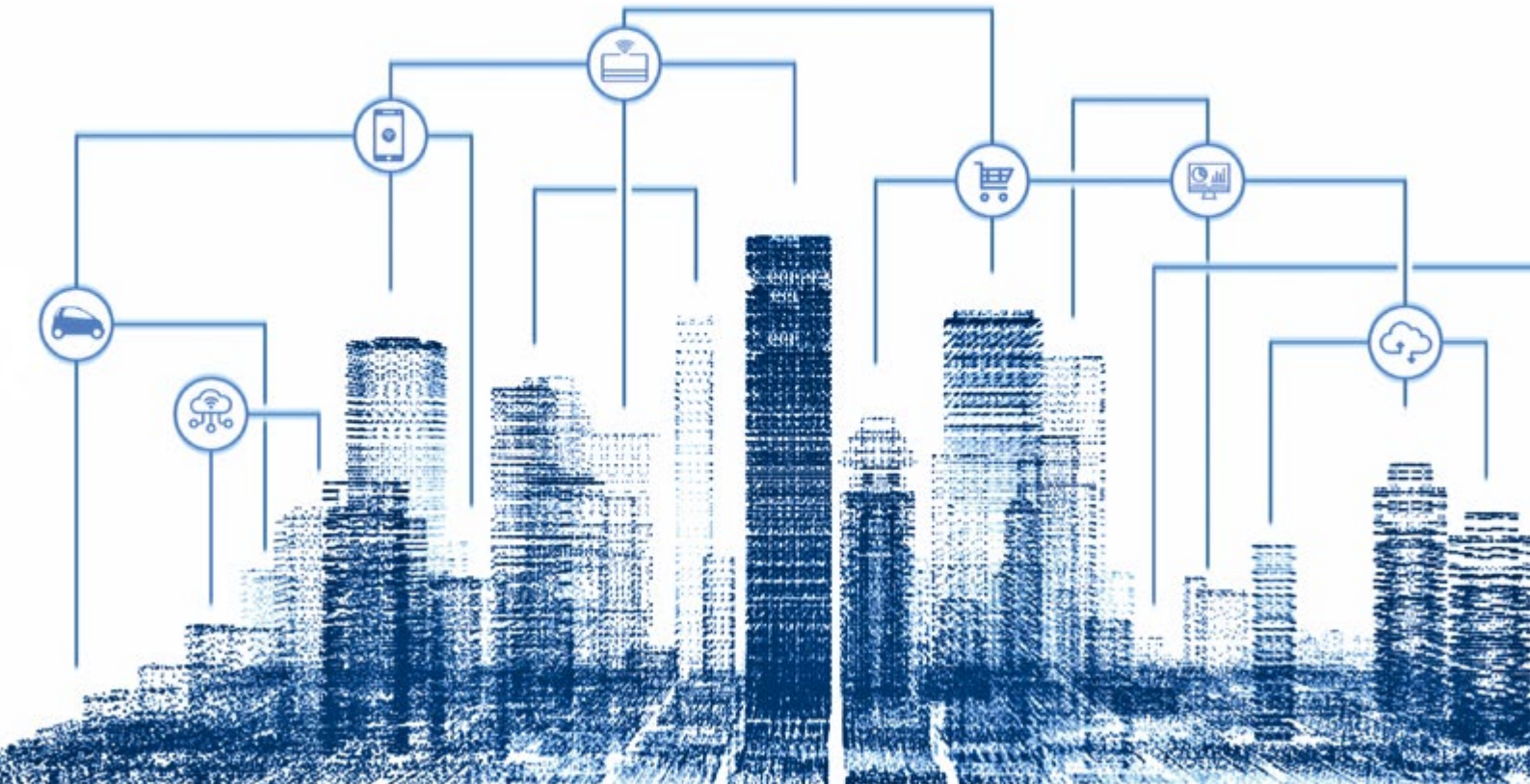
ABE EBA

EURO BANKING ASSOCIATION

Information paper

THE INTERNET OF THINGS AND SMART PAYMENTS

Cryptotechnologies and Smart Payments Working Group



The information contained in this document is provided for information purposes only and should not be construed as professional advice.

This information paper is the result of an analysis carried out by the Euro Banking Association's Cryptotechnologies and Smart Payments Working Group.

Information paper

THE INTERNET OF THINGS AND SMART PAYMENTS

Cryptotechnologies and Smart Payments Working Group

CONTENT

INTRODUCTION 5

INTERNET OF THINGS AND THE SMART ECONOMY 6

Defining the Internet of Things 6

Industries driving the development of IoT 7

IoT-compliant technologies 8

ADAPTING PAYMENT SERVICES TO THE SMART ECONOMY 11

Underlying principles essential for IoT development 13

Principles for IoT payment services 15

KEY SUCCESS FACTORS FOR BANKS IN THE MOVE TO IOT 17

Leveraging data in the IoT economy 17

Laying the foundations for digital identity 18

New business models for smart payments 19

CONCLUSION 22

INTRODUCTION

Of all the changes experienced in financial services in the twenty-first century, none has larger potential to fundamentally shift business and consumption models than the Internet of Things (IoT). At its core, IoT is about the expansion of internet connectivity to devices that allow for the monitoring and managing of processes digitally and remotely. This expansion is enabled by a combination of lower technology costs, mature network infrastructures, and new technologies that are pushing connectivity even further. Intel estimates that by 2020, there will be 40 times more connected devices than people on the planet (with over 200 billion devices).[1] The maturation of cloud computing, which is now an integral part of financial services, enables firms to store and analyse vast and ever-growing amounts of data. And the introduction of 5G in Europe and elsewhere promises to boost the scope and bandwidth of connectedness, further anchoring data as a cornerstone for businesses of all types. While the future state of IoT development is not necessarily clear, it is clear that IoT is far more than a buzzword; IoT merges machine and human agency, creating a new digital space with a new digital economy.

Banks and other stakeholders in the financial services industry have begun preparing for this new digital economy; initiatives such as Open Banking and instant payments have gained momentum and give a glimpse into the digital future of banking and payments. The core opportunity that the new digital economy will offer to banks is the massive wave of new data about consumers and businesses generated by IoT devices. Banks and other stakeholders will have unprecedented visibility into their customers' habits and needs. By leveraging these insights, banks can offer their customers more personalised services and better identify cross-service customer needs (e.g. in loans and financing). Improved data analysis will also help financial institutions reduce inefficient processes and detect fraud patterns more proactively. Data analysis and automation are also key in enabling smart payments, which leverage smart data to enable autonomous payments to be initiated in real time without manual intervention. To take advantage of these data opportunities, banks will need to invest in IT and business process rejuvenation to be able to efficiently handle the massive amounts of new data. While there are still challenges ahead, banks have the opportunity now, and they have already begun the transformation with the move to PSD2/ Open Banking and instant payments, to ready their systems for IoT and the new digital economy.

This report will examine the development of the Internet of Things and assess how payment services need to evolve in an IoT world. It will begin by looking at the technologies and industries driving the development of IoT today. Then, attention will shift to how payment services can become smart payments by utilising IoT. We will begin by outlining a set of principles driving IoT development, principles essential for adapting payment services to IoT, and principles for IoT payment services. In the end, we will examine key issues that the financial services industry (together with other industries leading the charge on IoT) will need to explore collaboratively in order to ensure that smart payments are fit for purpose in an IoT ecosystem.

1 https://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html

INTERNET OF THINGS AND THE SMART ECONOMY

The Internet of Things will have a significant impact on banks because it is poised to dramatically alter their customers' business and personal lives. While IoT is still in its early stages, its impact is already apparent with the increasing connectivity and digitalisation of things and processes. Understanding IoT and the principles behind it will be key to helping banks and other players respond and shape these developments, and ultimately help them develop fully IoT-compliant financial services in the future. This section will provide an overview of IoT, including the industries and technologies shaping IoT and future smart economies.

DEFINING THE INTERNET OF THINGS

IoT connects physical devices using sensors to digital networks to enable the tracking, monitoring, control, and management of devices and processes remotely via the Internet.[2] The combination of sensors embedded in physical devices and increased connectivity will result in exponentially more data being generated, shared, stored, and analysed by both people and machines. The result will be a further blurring of the lines between the physical and digital worlds. Insights generated by more granular data and detailed data analysis will be used to improve processes and make business decisions. A key element of IoT will be autonomous machines and humans working together in a data-rich ecosystem. IoT does not involve full automation of all processes. Rather, it will involve automation of specific tasks and processes, which will enable humans to focus on crucial decisions that are vital to their personal lives or business.

Two phases of IoT

In the area of payments and financial services, IoT is likely to develop in two phases of which the first is already underway. In this first phase an increase in internet-connected devices and the leveraging of legacy payment infrastructures and services will allow for greater automation of payments and new payment touchpoints for end users. Early stages can be seen in card networks with the tokenising of payment cards on devices such as smart watches, which can be used for contactless or in-app payments. In other industries, IoT is already more developed. For example, automobile companies and smart device manufacturers are already leveraging sensors and connectivity to receive new insights into supply chains and consumer behaviour and develop new processes, products, and services that rely on this information.

The second phase of IoT in the payments and financial services industry will come with the development of a machine-to-machine (M2M) economy, where machines and devices are capable of autonomously sending or requesting payments. The M2M economy will require a re-assessment of payment infrastructures and payment services by banks and other stakeholders. In this phase of IoT, transaction volumes are expected to greatly increase while transaction values decrease. Micropayment capability will be required. Centralised payment infrastructures with high transaction fees are likely not suited to this phase of IoT. Many view the use of new payment platforms based on distributed ledger technology (DLT) as a promising way forward in this space.

A full M2M IoT economy will feature some degree of decentralisation, which will make standards and interoperability key. In this second phase, IoT will likely resemble a network of networks, with various levels of access and control rights. While a bird's

2 What is IoT? https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/; IOT Agenda https://internetofthingsagenda.techtarget.com/

eye view of the Internet of Things may resemble a fully decentralised network, IoT will also feature centralised nodes of information (e.g. a large car manufacturer) interacting with other nodes and networks. The degree of centralisation and decentralisation of IoT will depend on how one looks at it. Within a large corporation, there may be a high degree of centralisation of information flows. Within a specific industry or national jurisdiction, there may be clusters of centralised nodes within (a) decentralised network(s) where information is shared on a continuous basis between different nodes in the network.

INDUSTRIES DRIVING THE DEVELOPMENT OF IOT

IoT is not being driven by the financial services industry. In other industries such as consumer and home goods, IoT-enabled devices are already on the market. Smart thermostats allow homeowners to remotely control temperatures and save on heating bills; connected cars using apps such as DriveNow allow for customers to reserve and pay for cars on an as-needed basis, and smart parking sensors allow for more efficient management of resources in dense urban areas and could be one of the pre-requisites for future smart cities. Many of these products and services rely on smart interfaces with consumers and granular usage data via sensors that allow for more exact pricing to end users.

But consumer-facing services are not the only area where IoT is on the rise. Indeed, there are multiple examples of industrial uses of IoT in high-tech industries that are changing the way supply chains are managed, maintenance schedules are devised, and products are delivered to market. Aircraft manufacturers have used data generated by IoT sensors in jet engines to obtain insights into engine performance that would have been impossible in a pre-IoT world. By aggregating and analysing the data via cloud computing, aircraft manufacturers can monitor performance, anticipate maintenance needs and optimise performance. This allows for "smart" maintenance that does not rely on pre-determined schedules, thereby improving performance and allowing airlines to optimise maintenance windows without sacrificing safety.[3] In the automobile industry, some car companies are using sensor-driven data to analyse and optimise supply chains, thereby lowering costs and allowing for business process optimisation within complicated, cross-border supply chains.[4]

The continued impact of IoT in a business context remains unclear for financial institutions, although increased investment suggests that IoT may be poised to transform how banks interact with their corporate clients. In a survey conducted by the Mobey Forum's IoT Expert Group as part of their report "IoT in Financial Services: Roles and Opportunities for Financial Institutions," respondents[5] were unsure about the impact of IoT devices in business contexts.[6] However, in consumer-facing activities, over 60% of respondents thought IoT had an impact on client interfaces, and almost 30% of respondents listed banking products for clients as impacted by IoT. In an industrial IoT context, the impact on client

3 How IoT is turning Rolls-Royce into a data-fueled business. https://www.i-cio.com/innovation/internet-of-things/item/how-iot-is-turning-rolls-royce-into-a-data-fuelled-business

4 The impact of Industry 4.0 on the Automotive Industry. https://blog.flexis.com/the-impact-of-industry-4.0-on-the-automotive-industry

5 Survey respondents were made up of members of the Mobey Forum, which includes major banks, technology vendors, telecommunications firms, and digital identity providers. For more information on Mobey members, please see: https://www.mobeyforum.org/about/

6 Mobey Forum, "IoT in Financial Services: Roles and Opportunities for Financial Institutions," June 2019, pp. 7-8. Available at: https://www.mobeyforum.org/iot-in-financial-services-roles-and-opportunities-for-financial-institutions/

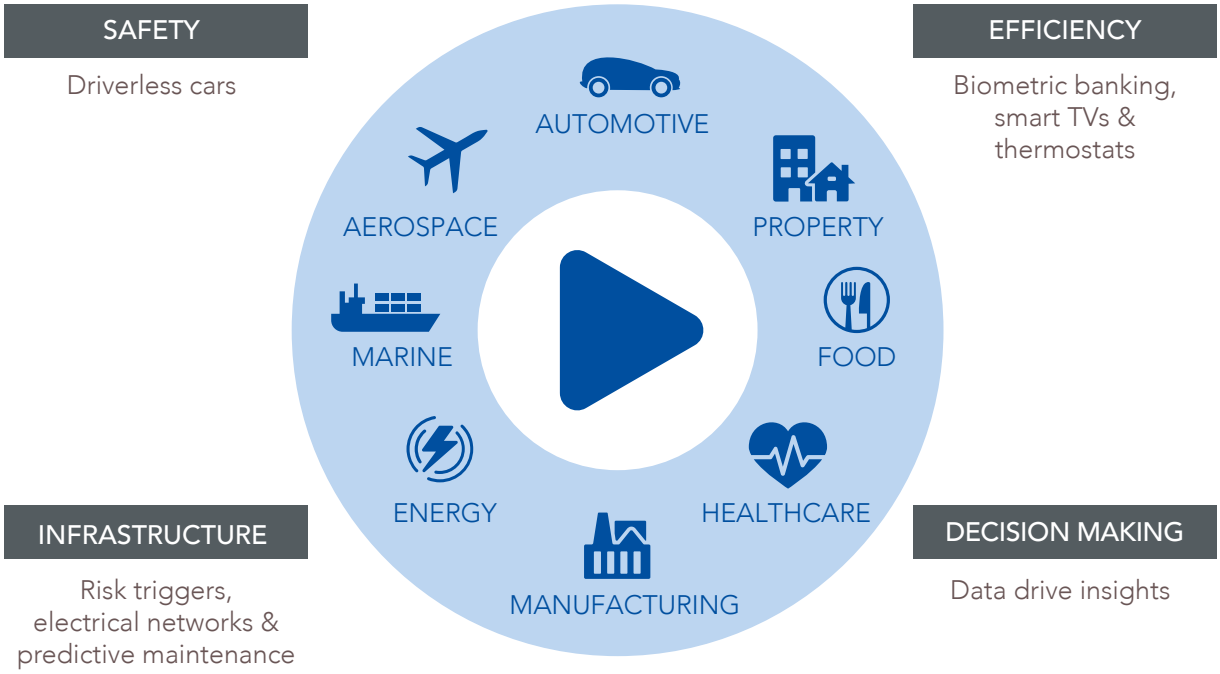


Figure 1: Industries driving development of IoT

Source: Intel

interfaces is likely to be strong, while the impact on banking products may be even higher than in a consumer context. With trade between businesses large and small becoming increasingly global and supply chains becoming ever more complex, banks may see opportunities in IoT for improved financing or cross-border payment capabilities, naturally embedded in smart devices and processes. While the financial services industry may not be driving these changes, it will be important for banks and other stakeholders to monitor and take part in these developments to continue providing value-added products and services to consumer and corporate customers alike.

IOT-COMPLIANT TECHNOLOGIES

At the core of IoT are new technologies that monitor devices and processes, and generate, exchange and store massive amounts of data, thus producing insights that manual analysis could never obtain. Some of these technologies such as cloud computing and application programming interfaces (APIs) are already used by banks today, while other technologies such as 5G or DLT are either still being developed or are at an early phase of use in the financial services industry.

Data generation technologies

Perhaps the biggest change brought about by IoT is the exponential increase of data generated by connected devices. Many consumer and business devices such as smart phones, wearables, home appliances, and containers have smart sensors as a core component today. These sensors generate data, often at a very granular level, in order to give a more detailed view of the performance of a device or process. The data generation may give new insights into the location of a shipping container in real time, the temperature of a perishable product in transit, or biometric information such as a person's pulse or temperature.

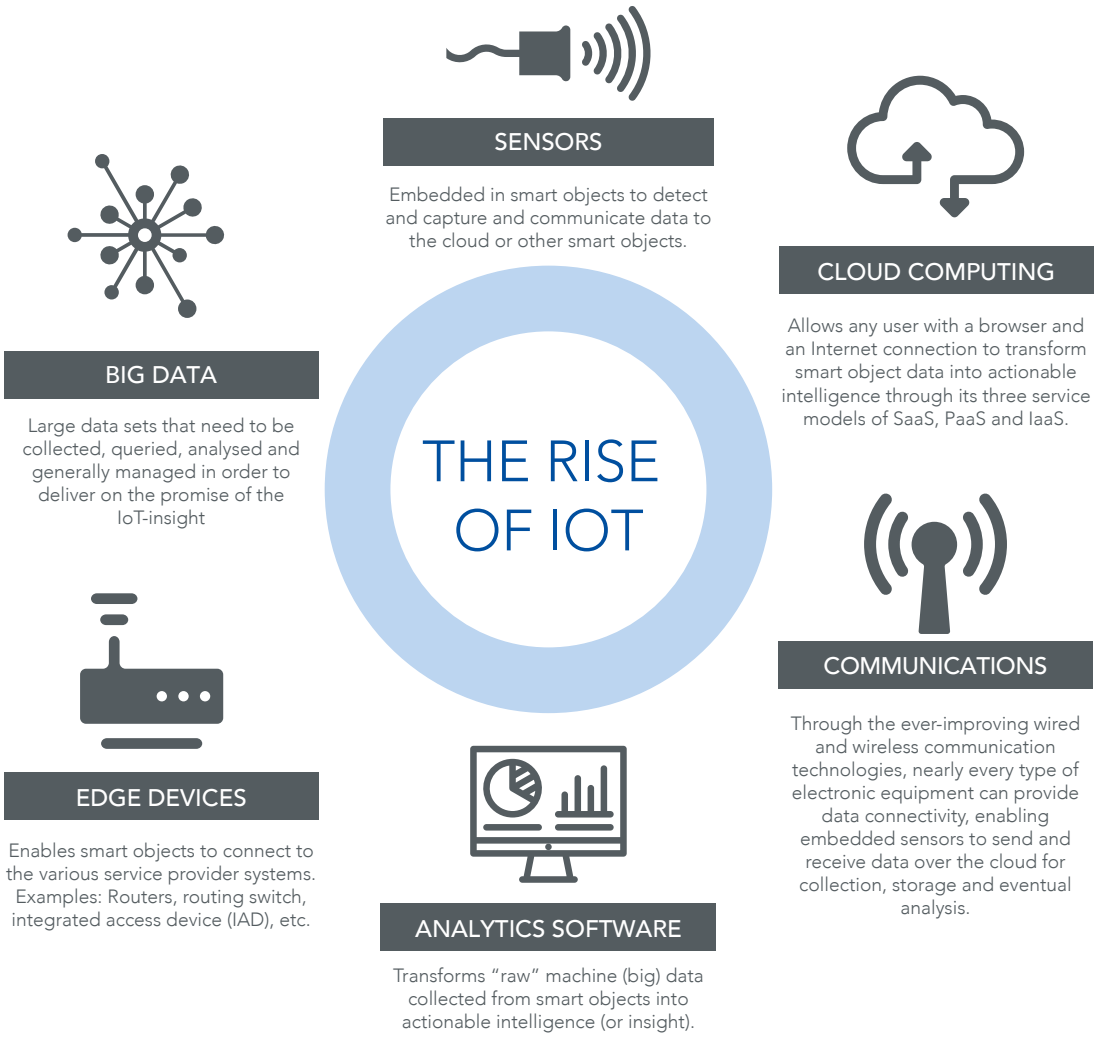


Figure 2: IoT-compliant technologies

Source: IPWatchdog

Connectivity and network technologies

Generating data is not particularly useful if that data cannot be shared as legally permissible within an organisation or between multiple organisations, and devices. The foundational infrastructure of IoT connectivity is the internet, with connectivity between devices enabled by edge devices such as routers and integrated access devices (IADs). The development of 5G network technology is also touted as a key enabler of IoT ecosystems in Europe and beyond. 5G has the potential to drastically increase data bandwidth and enable connected devices to download and share huge amounts of information without the need for a wired connection. The importance of 5G has also been recognised by government institutions such as the European Commission, which has developed a 5G Action Plan as part of its digital single market strategy.[7] Within and between organisations, the use of application programming interfaces (APIs) is likely to continue playing a crucial role in the secure exchange of information between networks.

Storage technologies

Businesses will have to securely store IoT data for processing and to meet regulatory requirements. Cloud computing, which has gained in importance for banks over the last decade, will be integral to the storage of such data. Individual organisations such as large manufacturers will need to store data in a centralised manner so that data can only be accessed by (authorised) divisions within that organisation. Any data that is exchanged or shared externally will have to go through checks. Particularly sensitive data such as a client's personal information retained in line with regulations such as the General Data Protection Regulation (GDPR), may require organisations to aggregate or anonymise data before sharing it. As IoT develops further, there may be an increasing need to store data that is used by multiple organisations. In a financial services context, this may include digital identity attributes that could be accessed by multiple organisations (provided client/data owner consent is previously obtained). For such decentralised data, DLT may offer a technological solution for storage. DLT could enable data to be encrypted and secured, and only accessed by authorised parties without the need for a centralised data controller or manager.

Analytics technologies

Its ability to enable the generation and enhanced analysis of huge datasets is what makes IoT valuable for businesses. The use of big data technologies such as artificial intelligence (AI) and machine-learning (a sub-set of AI) will be key to allowing organisations to make sense of large datasets and develop useful insights that can be used by consumers and businesses alike. These insights can be used to make decisions related to internal processes or as the basis for new products and services that can help increase revenue and customer satisfaction. As banks face downward pressure on legacy revenue streams such as transaction fees (due to a combination of regulation and competition), the development of value-added services derived from data analytics will be key to new revenue streams and business models in IoT-compliant financial services.

7 http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-5g-action-plan

ADAPTING PAYMENT SERVICES TO THE SMART ECONOMY

As IoT ecosystems and the "smart" economy develop further, payments will also need to become "smart." Smart technologies are usually defined as technologies that allow for autonomous connectivity and remote control of devices and processes through the use of sensors, wireless connections, and databases. Smart payments can thus be defined as payments that leverage smart data and that can be made autonomously in real time without manual intervention. Fully smart payments may not be prevalent in the early stages of IoT, but they offer a vision for banks and other payment service providers to work towards as the IoT economy develops further. Existing payment infrastructures such as instant payment systems, bulk payment systems (ACH), card networks, and others may be leveraged to develop IoT-compliant smart payments. In order to help guide this journey, this section will distil key principles of IoT, the underlying principles essential for organisations developing IoT ecosystems, and the principles guiding the development of payment services using IoT.

Principles of IoT and the smart economy

Current IoT developments share three main principles: connectivity, speed, and automation. These principles include a combination of technology and business innovations that are shaping the future of industry and commerce.

Connectivity

Connectivity is at the heart of all IoT developments; without it, there is no IoT. At the core of this is the internet, which is now the foundation of most consumer and corporate activity. The increasing

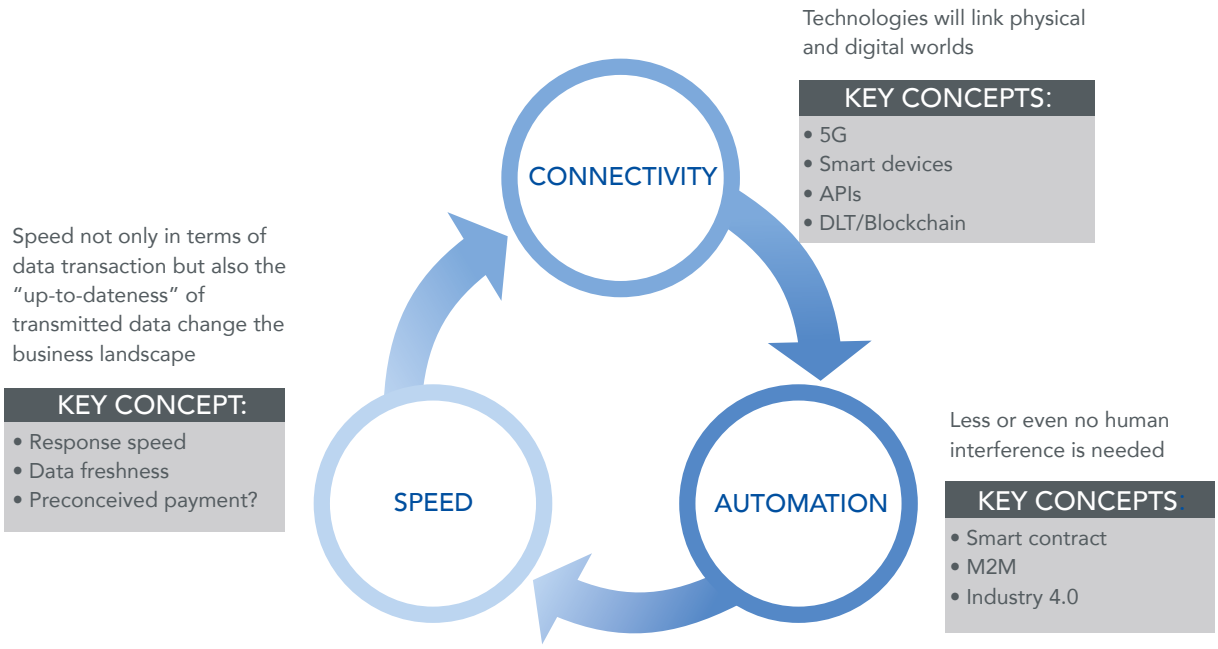


Figure 3: Principles driving IoT development

Source: Lipis Advisors

development of physical smart devices that contain sensors to measure and generate data is enabling an exponential increase in data shared over the internet. The development of 5G technology is expected to be a further catalyst here, as it will massively increase the bandwidth of wireless connections, setting the stage for truly interactive connectivity for both humans and machines. The European Commission has invested millions in the development of 5G technology and 5G standards to enable full machine-to-machine (M2M) communication in an IoT ecosystem.[8] The main result of this increase in connectivity is the continued blurring of the boundaries between the physical and digital worlds. In the future, the distinction between these two worlds will be less and less important, as IoT-enabled technologies enable physical processes to be controlled remotely, and more and more products and services are developed and distributed through digital networks.

Speed

Speed is not an exclusive characteristic of IoT. Indeed, the internet age has adjusted both consumer and business expectations of instant data transmission. With a world of knowledge at our fingertips – be it Wikipedia, Netflix, or Google – instant has become the new normal. With IoT, speed refers not only to data transmission (itself expected within seconds), but more crucially to the speed in which actions are taken. Industrial IoT players such as auto manufacturers rely on data that is updated within seconds to make decisions that may have downstream effects on a supply chain. In an IoT world, business processes need to adapt to the need to make decisions in real time based on freshly updated data, all on a continuous basis. The gap between a problem arising and a decision being made will increasingly be measured in seconds. Accomplishing this is beyond the control of humans alone. In an M2M economy, machines will have to make some decisions autonomously, with follow-up actions taken either by machines or by humans, depending on the importance of the decision. Deferring decisions until a later date (even if that means later in the same business day) will increasingly become untenable, particularly for more low-level tasks that can be automated.

Automation

Speed and connectivity enable increased automation, which itself is integral to the functioning of IoT ecosystems. Automation is already an important factor in many industries today, not least the financial services industry. Instant access to information is impossible without automation. Value-added services that leverage big data rely on automation to make sense of large datasets and analyse data to find new products and services. Automation does not, however, imply that all manual processes will be done away within an IoT ecosystem. While some processes within banks such as checks for sanctions screening or AML/CTF procedures that require human intervention today could be automated, other data analysis processes will still require human intervention. For instance, big data and automation could enable a company to analyse a large dataset and then present the analysis to a team of people who take in these insights and use them to make business decisions.[9] Banks have already begun doing this today, particularly in areas related to fraud detection and sanctions screening. While not all decision-making will be made by machines, automation will be key in enabling more fine-tuned and valuable decisions by analysts and business teams.

8 https://ec.europa.eu/digital-single-market/en/towards-5g

9 For example, Rolls-Royce leverages AI and Industry 4.0 for smarter manufacturing: https://internetofbusiness.com/rolls-royce-ai-industrie-4-0/

UNDERLYING PRINCIPLES ESSENTIAL FOR IOT DEVELOPMENT

The previously discussed principles of IoT can help companies understand the basic trajectory and key elements of IoT and the smart economy. However, new players entering the IoT space such as banks also need to be aware of key principles that will guide their own development of IoT-compliant products and services and enable them to serve consumers and businesses in a smart economy.

Big Data

Banks throughout Europe and beyond are already thinking about big data as a way to take their businesses into the future. The use of big data involves the storage, processing, and analysis of massive amounts of data with the goal of achieving valuable insights that can help reduce risk, increase security, boost efficiency, and support the development of new products and services. As Harvard Business Review points out, the key difference between big data and legacy analytics is in the volume, velocity, and variety of data being processed. [10] The volume of data produced by connected devices is already growing exponentially, and this trend will be even more prevalent in IoT ecosystems. For banks, leveraging big data for IoT will mean investing in new technologies, updating legacy processes, and fostering expertise internally. Without the ability to leverage big data, no player can succeed in an IoT ecosystem.

10 https://hbr.org/2012/10/big-data-the-management-revolution

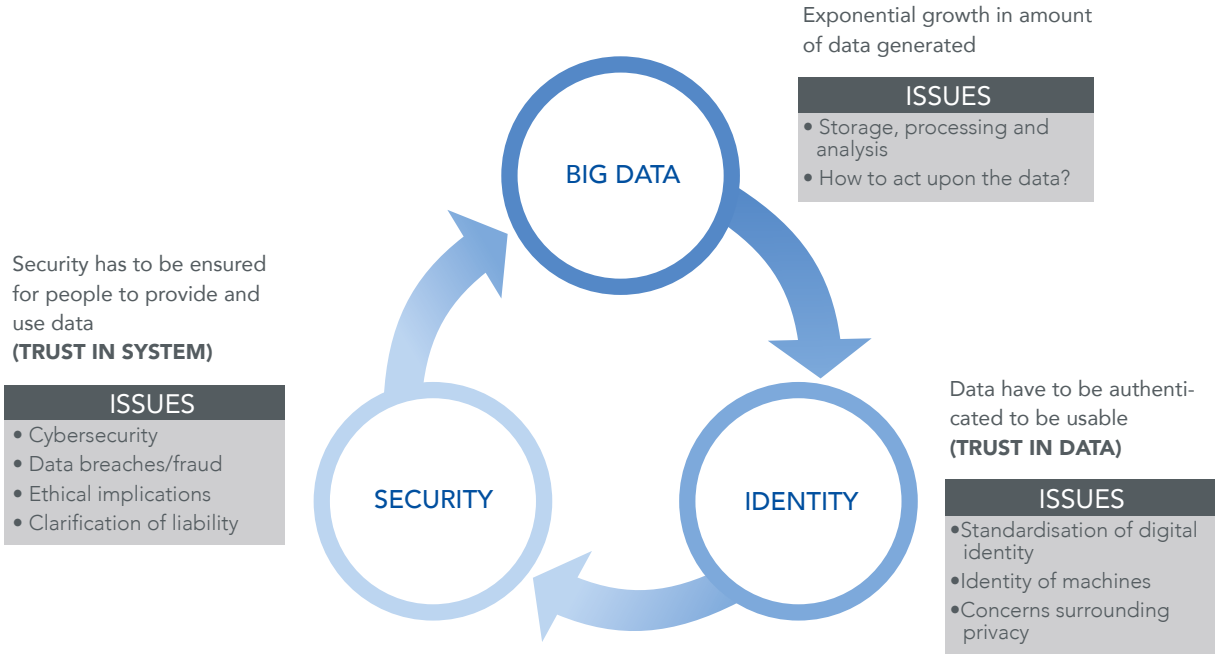


Figure 4: Underlying principles essential for IoT development

Source: Lipis Advisors

Identity

Data generated by IoT devices must be authenticated to be useable by banks and other players. Simply put, without trust in the data being generated, no IoT ecosystem can function. Digital identity is a key enabler of the automation at the core of IoT. Authenticating digital identity is a challenge that banks and other organisations are already facing today, and this challenge will become even more difficult with the inclusion of new people, organisations, and even devices in an IoT ecosystem. Achieving trustworthy digital identity will require the standardisation of digital identities and interoperability between digital identities. It is unlikely that there will be one overarching standard for digital identity globally. One could imagine different levels of digital identity based on a local jurisdiction, a specific industry, or for certain types of transactions. One key question here is which entity should provide and validate digital identifiers. Government-validated identification is typically relied on in many developed economies, while other markets rely to some extent on socially-validated identity such as occupation or connections on a social media platform. An IoT ecosystem may have to leave space for both types of identity authentication, and potentially accommodate multiple layers of identity. These multiple layers may also represent different end users: human, business, and machine. Initially, machines may not have sovereign identities, instead acting as agents or custodians on behalf of a person or business entity. As we move toward the M2M economy, this may have to be revised. Re-defining identity may require a revision of the technology used to facilitate digital identity. Distributed ledger technology (DLT) in particular offers attractive potential to enable fully self-sovereign digital identity.[11]

11 For more on DLT-based self-sovereign identity, see Hyperledger's Indy project at https://www.hyperledger.org/projects/hyperledger-indy

Security

With massive amounts of data being generated, shared, stored, and analysed, cybersecurity will become an even greater challenge in IoT ecosystems than it is in today's digital economy. As the speed of data transmission and financial transactions grows, hackers and fraudsters will develop more sophisticated ways to falsify and steal data. Data breaches and fraud can have adverse effects on end users' willingness to share data and could represent an obstacle to the further development of IoT. Individuals, organisations, industries, and governments will need to establish proper cybersecurity measures and look into other issues such as clarifying liability in IoT transactions. The ethical implications of data usage and data security should also be explored. With data of vital importance to the operation of IoT ecosystems, there is a risk that sensitive personal information could fall into the wrong hands or that the sharing of personal data becomes a necessary prerequisite for taking part in essential services such as banking or the use of internet platforms.

PRINCIPLES FOR IOT PAYMENT SERVICES

Adapting payment services to IoT will require updates to enable faster, automated, and data-rich transactions while maintaining the core principles that consumers and businesses have come to expect from financial institutions. The following section will outline core principles for IoT payment services.

Trust

Trust is the bedrock of financial services, and this will not change with the development of IoT. As the barriers between the physical and digital worlds continue to blur and automation and machine-generated payments grow, trust will be more important than ever to consumers and businesses. In payment services, banks are well placed to be the main providers of trust for their customers. Cybersecurity and data protection will continue to be key elements for fostering trust in payment services. Banks will also need to clarify liability frameworks for their customers in an IoT world. One of the key advantages that card payments hold for consumers today in an e-commerce and POS context is the ability of consumers to apply refunds and chargebacks in the case of mistaken or fraudulent payments. With the possibility of faster, more automated, and even autonomous payments made in IoT ecosystems, consumers and businesses may be wary of smart payments if liability attribution is unclear or insufficient for building trust. Payments initiation is another area where trust will be a key factor. Banks will need to ensure that payment initiation is secure (e.g. through the use of biometrics) while also balancing the need for convenience.

Convenience

In the realm of digital payments, customers value a fast and convenient experience. As a 2018 PwC report on customer experience showed, consumers are often willing to pay a premium for products and services that offer a great customer experience.[12] A key element of customer experience is convenience, which was deemed important by more than two-thirds of customers in the PwC survey. Creating a more convenient customer experience in digital payments is a challenge many banks are facing, and this challenge will be even greater in an IoT economy. Convenience is not just limited to customer-initiated payments; machine-initiated

12 https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/pwc-consumer-intelligence-series-customer-experience.pdf

payments made on behalf of an end user will also need to take into account the convenience factor. While end users will continue to value control over their payments, some low-value and recurring payments could be automated without the need for a customer to sign-off on each individual payment. This reduces the amount of "clutter" in their financial lives without raising the risk of lower security or decreased control.

Revenue from Smart Payments

With the introduction of new payment opportunities and autonomous payments made by machines, the volume of payments in an IoT economy are set to grow dramatically.[13] With ever-growing payment volumes, banks and other stakeholders facilitating smart payments may need to independently re-assess revenue models. The downward pressure on interchange fees today[14] will likely continue, and the interchange model itself may need re-thinking. Legacy payment streams such as direct debits may be leveraged for automated smart payments due to lower price and consumer protection around reversals. Transaction fees to end users will likely also face downward pressure. Pressure to lower or even eliminate transaction fees means that it will be necessary to fundamentally re-think how revenue from smart payments is driven. The development of micropayment capabilities as IoT ecosystems mature will provide further downward pressure on transaction fees. With new technologies enabling richer, faster, and automated payments and consumer and business expectations for low-cost or free core services, value-added services will have to be developed to counterbalance this downward trend.

13 Consumer demands and the impact of IoT on the Payment Industry. https://www.paymentsjournal.com/consumer-demands-and-the-impact-of-iot-on-the-payment-industry/

14 European Commission. http://europa.eu/rapid/press-release_IP-18-6655_en.htm

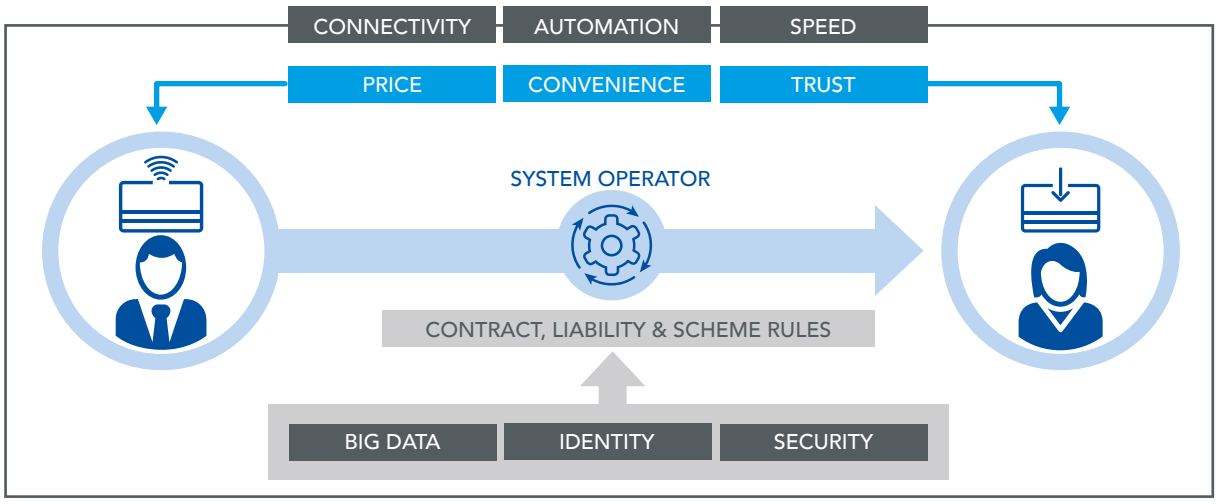


Figure 5: IoT principles and application for payments

Source: Lipis Advisors

KEY SUCCESS FACTORS FOR BANKS IN THE MOVE TO IOT

The development of IoT will present both opportunities and challenges for players in financial services. The expansion of data and more granular details about customers, businesses, and machines will give banks far more insight into how their customers (be they consumers or businesses) operate and interact with each other. By leveraging this data, banks can better serve their customers by offering them flexible and tailor-made products. Businesses in particular could benefit from this information, as banks could use these insights to provide improved financing or advisory services that can help improve or grow their customer's business. The need for payments and other financial services will not go away in an IoT economy, and banks are well placed to benefit from IoT and the smart economy.

But in order to realise these benefits, banks will have to successfully position themselves in IoT ecosystems. Agile new players such as fintechs or entrenched organisations such as large technology firms also see the opportunities arising from IoT. While some players may have more experience with leveraging new technologies such as AI for product development, banks have a wealth of knowledge in financial advisory, regulatory compliance, and know-how in payment services. Banks should focus on three key areas in the IoT economy: leveraging data and data insights; enabling digital identity; and developing new business models for payments and financial services. By concentrating on these three areas, banks can conceive potential use cases and products and thus develop the foundation for their future role in IoT. Focusing on the three key areas could also help banks with investment decisions and strategic planning in light of the transition to IoT while they are undergoing transformations that developments such as new regulations and instant payments have brought to the financial services industry.

LEVERAGING DATA IN THE IOT ECONOMY

Before banks can fully participate in IoT, they will have to develop the internal capabilities of exchanging, storing, and analysing data in real time. For many banks, this will require not only a significant investment in new technologies, but, even more crucially, a change in mindset and internal business processes as well. In Europe, banks have already begun this process, spurred in part by new regulations such as the second Payment Services Directive (PSD2) and the introduction and ramp-up of instant payment systems. For both PSD2 and instant payments, the exchange and evaluation of customer and business data is key. Nevertheless, the necessary upgrades to IT systems are moving slower than planned, in part because the data culture within banks has been slow to change. Within some banks, sharing data internally is still a challenge due to legacy infrastructure and siloed business processes. In an IoT world, banks will need to leverage this internal data on a continuous basis and use it to feed insights into business and compliance processes while maintaining data protection and cybersecurity.

As European banks continue to modernise internal processes and IT systems, some best practices have emerged. The introduction of regulatory sandboxes in markets such as the UK[15], as well as the development of innovation hubs by major banks, have given banks an opportunity to experiment in a low-risk, low-cost environment. In some cases, banks are partnering with fintechs and other third parties to develop new capabilities in a collaborative fashion. The open banking model may even be seen as a first step toward an IoT-compliant model of payment services. Banks have also begun investing in human resources with

15 https://www.fca.org.uk/firms/regulatory-sandbox

data expertise. Many major European banks now employ data scientists and have begun expanding their hiring processes to include people with experience outside of banking. Hiring people from larger technology firms or fintechs helps develop the internal know-how that will be essential to leveraging data to provide value-added services and develop new business models around payments and financial services more broadly. Another lesson banks can learn from more agile players such as fintechs is the need for an iterative approach to product development. Traditionally, banks tend to spend a lot of time testing products before having a big release once or twice a year. Smaller fintechs on the other hand tend to release new products and services far more quickly and then rely on customer feedback to update and adapt the product on a more frequent basis. When it comes to developing new products and services that leverage customer data, banks would be well-served to move away from big annual product releases and instead move toward more frequent releases on a continuous basis (monthly, weekly, or even daily). Lastly, banks have begun taking a more holistic view of payments, recognising that the siloed IT and business processes that have dominated in the past are not in line with the needs of the future. Having cross-functional teams work collaboratively to meet new requirements and develop new products can help banks better understand how data flows will affect all areas of the bank while ensuring that regulatory compliance and customer trust are assured. In this process, new technologies can be an enabler of IT and business process rejuvenation, ultimately helping banks compete now and in the future.

LAYING THE FOUNDATIONS FOR DIGITAL IDENTITY

As IoT progresses and the physical and digital worlds continue to merge, the issue of identity will be more acute than ever. As IoT develops further and both humans and machines take part in new digital infrastructures, digital identity solutions will be necessary to ensure the smooth and safe functioning of infrastructures and networks. Today, identity is one of banks' strongest propositions for both consumer and business customers. Due to strong KYC processes and regulatory checks, banks are seen as a trusted source for storing and sharing identity attributes. With the move to IoT, banks could leverage this advantage and add to it with the development of new digital identity frameworks that are fit for the digital economy and IoT ecosystems.

Digital identity is one of the promising areas for distributed ledger technology (DLT), which many see as an enabler of self-sovereign identity (SSI). SSI allows end users to have full control over their digital identity, allowing them to share identity attributes securely with authorised parties or revoke access at any time. The decentralised nature of DLT can allow users to share encrypted attestations of verified digital ID attributes with any party directly without the need to save ID attributes on a centralised ledger. KYC can be checked and approved by using public-private keys, and the storage of digital identity can be chosen by individual users. As custodians of customer identity and data today, banks would be well-placed to continue playing this role in IoT ecosystems. Banks can play numerous roles in enabling and managing their customers' digital identity. They can use ID attributes as a basis for developing a digital SSI collaboratively with banks and other stakeholders. Banks could also play a role in managing and securing public-private keys for their customers. While many consumers and

businesses will welcome having increased control of their data due to regulations such as GDPR and SSI enabled by new technologies, not everyone will want to manually manage their digital identity in all areas of business and personal lives. Banks could help their customers by storing public-private keys to help reduce fraud and by offering insurance products related to ID management. This will allow end users to focus on other areas while offering banks an opportunity to realise additional revenue streams related to digital identity.[16]

When developing digital identity frameworks and solutions, banks will need to keep interoperability at the top of mind. It is unlikely that a single global framework for digital identity and identity management will be feasible, as different national jurisdictions and industries have different legal and business requirements related to identity. One could imagine a network of (digital identity) networks interacting in real time across national borders and across industries. Banks already have experience working in cross-jurisdictional environments and are seen as a trusted source for identity and regulatory compliance by regulators and end users alike. Banks will also need to think about business models around digital identity, with a focus on how they can leverage trusted services such as KYC and regulatory compliance to develop new revenue streams. While end users may not be willing to pay a premium for identity services, banks may look to partner with entities such as retailers or businesses involved in international trade to grow revenue in this space. The issue of human vs. machine identity will also have to be explored in more detail as IoT develops further. It is possible that machine identities are initially linked to a person or business, but as the M2M economy develops, machines and devices may require their own digital identities that can be used to send or request payment.

NEW BUSINESS MODELS FOR SMART PAYMENTS

External pressure is already affecting bank business models today, and this trend will become even more pronounced as IoT develops further. New players have successfully entered the payments value chain, and new regulatory frameworks such as the PSD2 are compelling banks to re-think products and services and the

16 Collaborative approaches to SSI using DLT have already begun. Gemalto's Trust ID leverage the Corda platform from R3 to enable blockchain-based digital identity solutions, while Hyperledger Indy forms the basis for Sovrin's digital identity network.

business models that underpin them. In an IoT economy, these pressures on traditional business models will intensify, and banks will need to develop new business models for smart payments. At the core of these new business models will be data-driven insights that allow banks to bring value to their customers beyond the mere exchange of payments and transactional data.

The exponential growth in data with IoT will expand the potential revenue pool for banks. As data becomes more important for consumers and businesses, banks stand to gain from the additional services that can be provided through IoT ecosystems. But in order to profit, banks must individually re-think their business models in an IoT world. As the cost of processing lowers and competition increases (as has already begun under the PSD2 in Europe), banks may have to look beyond transaction fees for revenue from payment services. One area that could potentially make up for lower revenue from transaction fees is in monetising the use of data. Current initiatives such as the PSD2 and the Open Banking initiative in the UK remain unclear on whether banks can charge for access to customer data. Within IoT ecosystems, it is unlikely that banks or other players will be able to charge for simple access to data, as the efficient and quick flow of data will be crucial to the functioning of IoT networks. Bringing in charging models for access to low-level data may ultimately lower overall network efficiency and make it more difficult for ecosystem stakeholders to leverage crucial insights from customer data. Two areas that banks can look to is in finding new partnership models and in focusing on data-driven value-added services.

Partnership models

IoT ecosystems are necessarily interactive, and banks should not expect to go it alone as IoT ecosystems develop further. Spurred by competition, new technologies, and regulations such as the PSD2, European banks are already opening up and developing partnerships with new players such as fintechs and technology companies. There is widespread recognition in the financial services industry that open banking and partnerships will be crucial to the future of banking. In an IoT economy, banks should identify potential partners in areas of strategic value that can help add value to their customers' experience. On the consumer side, banks could partner with retailers or manufacturers of smart products (such as home appliance or cars) to facilitate payment as part of the customer journey. By becoming embedded in smart processes, banks can obtain a detailed view of consumer needs and identify areas where additional services may be needed. For instance, by partnering with automobile dealerships, banks could play an expanded role in consumer vehicle financing, thereby growing revenue from loans and credit to make up for potential losses in transaction fees. The automobile dealer can benefit by making the experience of buying a car as smooth as possible, potentially lowering the barrier for purchase and growing overall sales revenue. In this instance, both the bank and the car dealer can boost revenue while making the overall experience for consumers easier and faster.

On the corporate side, banks can play a key role in improving supply chains, crafting more flexible financing options, and helping facilitate payments to suppliers and from end users. This may be particularly valuable to businesses in the cross-border space, where the lack of international regulations and fragmented industry frameworks present an opportunity for banks to aid corporate clients and advise them on business expansion and trade financing. Corporates with complicated and global supply chains such as airlines could greatly benefit from big data insights gained from IoT ecosystems and could help reduce costs by rationalising supply chains. Banks could also

enter partnerships with other banks and groups of corporates to develop industry platforms that drive value for all players.[17]

One segment that may stand to benefit from data-driven insights using IoT in particular is small businesses. Many small businesses – be they independent retail shops in urban locations, small manufacturers embedded in local and global supply chains, or emerging technology firms – need help as they grow. Understanding when and where to expand their business, making connections to buyers and suppliers domestically and internationally, and obtaining financing for business expansion are all areas where banks could potentially serve a vital role in advising their small business clients as they grow their business. Data-driven insights derived from IoT ecosystems could be used by banks to develop business intelligence that can be sold to small businesses.

The end of transaction fees?

While transaction fees for payments will not go away overnight, banks might want to begin looking more holistically at their offerings to point a way forward for bank revenue in an IoT world. The massive increase in data and need for data-driven insights in all areas of business may create new opportunities for banks to earn revenue from other areas. As competition for payments increases, banks could use transactional data to better understand their customers' overall financial needs. This will provide opportunities to offer revenue-driving products such as loans. Banks can also lower the risk of lending by having a more detailed view of their consumer and corporate customers' financial flows and creditworthiness, which can help boost the stability of loan portfolios and lower overall risk in the ecosystem.

The reduction or eventual elimination of transaction fees will also require new pricing models for interbank payment infrastructures. Legacy pricing models such as interchange are not suited to IoT-compliant payment systems with exponentially increasing transaction volumes. Lower transaction values (including micropayments) also make high interbank fees unfeasible for banks and other system stakeholders. The introduction of micropayments may present a particular challenge around fees, as banks' current AML/compliance processes may make low-fee micropayments unfeasible at this time. Re-thinking and automating manual processes around compliance will be necessary to enable a low- or no-fee smart payment environment. New technologies can help drive the price of interbank systems down, while scheme rules and governance will continue to play a vital role in ensuring a level playing field for all players. In the M2M economy, the use of technologies such as DLT may be more realistic for interbank payments processing due to the need for high resiliency, low costs, and the inclusion of new players beyond banks.

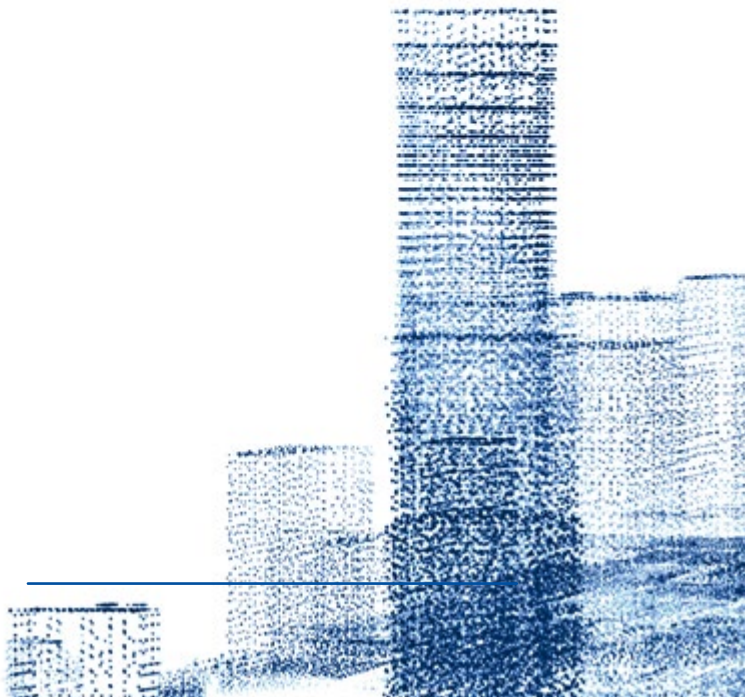
Ultimately, payments serve to facilitate trade and enable additional services. As banks look ahead to open banking, instant payments, and ultimately to IoT and smart payments, they should take a holistic approach to business models in payments and financial services more generally. As IoT develops further, the siloes between business areas within banks will have to be overcome in order to enable data-driven insights and smart products and services.

17 The we.trade initiative is one current example that may point to a way forward here. We.trade's trade platform uses blockchain technology and smart contracts to help identify parties to a transaction and facilitate the settlement of obligations between parties in a trade transaction. The transparency and automation provided by this platform will help drive expectations in the future in a way that is compliant with IoT ecosystems.

CONCLUSION

The development of IoT ecosystems presents both challenges and opportunities for banks. IoT has already arrived in industries such as smart manufacturing and home goods, and its continued development is poised to reach all areas of business and consumer lives. IoT-enabled smart payments will require banks to increase speed, automation, and flexibility in order to meet customer needs, leverage insights from big data, and develop new business models. European banks have already begun this journey with the development of instant payments and open banking in line with the PSD2. But there is much work left to be done. Banks need to begin thinking about what role they can play in decentralised IoT ecosystems. Partnering with an expanded list of players will be crucial. In addition to fintechs, banks may look to partner with retailers, corporates, and other banks to develop products and services that facilitate the secure transfer of data and payments. Achieving this will require banks to re-think investment decision and business models and focus on how they can add value to their customers in IoT ecosystems. Developing smart payment functionality will be a necessary enabler of a full M2M IoT economy, and banks are well-placed to take advantage of this.

Competition in payment services will become more intense as the needs of consumers and businesses evolve. Large technology firms are already competing in the payments space and while projects such as Facebook's Libra cryptocurrency will surely face major regulatory scrutiny, such efforts show that innovative payment services are now also coming from outside the traditional financial industry. As IoT ecosystems mature, banks stand to gain by positioning themselves at the intersection of data exchange, commerce, and financing. The development of smart payments, digital identity solutions, and new partnership models can help banks meet the evolving needs of consumers and businesses while adapting business models and operational requirements for the connected world of the Internet of Things.



IMPRINT

Euro Banking Association
40 rue de Courcelles
F-75008 Paris

Contact

association@abe-eba.eu

Graphic design

BOSSE UND MEINHARD, Bonn

Images

cokada/istock, BOSSE UND MEINHARD