WORLDLINE

# The future of autonomous and invisible transactions

White Paper

Digital Payments
for a Trusted World

# Contents

# Forwards

**Drs Henkkuipers**

**Innovation Manager at Strategy & Innovation Rabobank Tech Lab**

“Thanks to its well-structured and thorough approach, this white paper gives you an excellent overview of IoT payments. It explains many of the different types of technology that are applied within this field, and it also discusses the varying business opportunities that arise.
Not only does it bring you up to speed with what IoT payments are about, but it also highlights which developments can be expected in the coming years and what challenges lie ahead.”

**Franck Leveque**

**Partner & Mobility Practice Head for Europe, Founding Member of Mobility Practice Frost & Sullivan**

“This white paper provides insightful, practical perspectives into IoT payment solutions, and highlights the core necessity for trust and accountability.
These trusted automated payment solutions will be a fundamental component of the transformation of the automotive industry as its business model shifts from a one-time sale to value creation throughout the vehicle life cycle, whether one talks about electric vehicle charging, the download of new vehicle features on demand and other connected services, or shared mobility.”

# Executive summary

## We are currently witnessing three trends that are combining to drive the IoT payment revolution:

**Acceleration of digital payments,** with 779 billion transactions conducted digitally in 2020.

**Massive growth in connected devices,** tripling in five years to 38.5 billion in 2020.

**The increased use of Artificial Intelligence,** driven by growing compute power and better algorithms.

**Given this backdrop, perhaps it is not surprising that the IoT payments market is expected to be : worth $27.6 billion by 2023, impacting every industry and disrupting the current payment model landscape. Indeed, we believe that the IoT Payment Revolution is no longer a mere possibility, but a certainty, driven by the significant benefits that it will deliver:**

**For consumers,** a truly frictionless experience for repetitive or low-value purchases, saving them time and effort, and reducing stress.

**For merchants,** a seamless experience for their customers leading to higher conversion rates, increased revenues and more repeat custom

**For all businesses creating new offerings based on IoT and Artificial intelligence,** the ability to embed automated payments into their value propositions to create truly innovative, end-to-end solutions for their clients.

However, to achieve these benefits, managing the topics of trust and accountability will be crucial. People need to trust the device triggering a payment, and the delegation of the person or organisation accountable for the payment must be verifiable. We therefore believe that regulatory frameworks will need to evolve rapidly to accommodate Object-Initiated Transactions (which will exist alongside the Merchant and Customer-Initiated Transactions of today).

To harness the power of IoT payments, businesses will have to understand and master several technological aspects, including device authentication, lifecycle management, interoperability, communications, and Artificial Intelligence.

Those organisations which successfully understand the possibilities created by IoT payments and how these could transform their industry, and which develop the right capabilities needed to leverage their true potential, will be able to gain significant competitive advantage in the coming years. Many attractive use cases exist: from electric vehicle charging, to highly convenient walk-in/walk-out shopping experiences, through to sustainable commerce solutions enabled via the sharing economy.

In this paper, which draws on Worldline's extensive payments experience and research in this area, together with the insights gained through working with our clients and partners, we seek to help you understand the potential of IoT payments in your industry, and to identify the key actions you need to take today to position your organisation for this future.

# Introduction

The first physical currency was minted by King Alyattes of Lydia over 2,600 years ago. These simple coins evolved into banknotes in 1661[1]. However, up until 1871, the monetary transactions enabled by these currencies remained physical: a tangible exchange of cash. The first electronic money transfer was made in 1871 by Western Union using a telegram[2]. Nearly 150 years later, in 2020, 779 billion digital transactions were completed worldwide[3].
And yet, the fundamental basis of these transactions has not changed: they are triggered by one person (sometimes representing an organisation) making a payment to another person (or organisation).

More recently, there has been a huge growth in the number of devices connected to the Internet, from an estimated 200 million globally in the year 2000[4] up to 38.5 billion in 2020[5]. Twenty years ago, a small percentage of households may have had a single device connected via a modem or router. Now, a vast range of objects are connected, from toasters and watches, to light bulbs and thermostats, through to cars and trains.

In the last decade, we have also seen a rise in the use of Artificial Intelligence (AI), fuelled by the increased availability of compute power coupled with readily available state-of-the-art open source algorithms. We are now starting to see

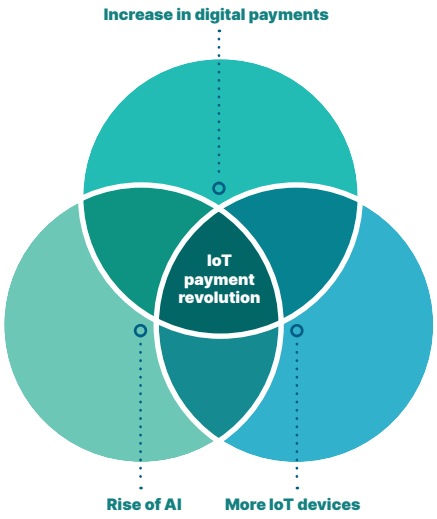


**Figure 1:** Drivers of the Iot payment revolution.

AI being used to make decisions on behalf of people or organisations and to take actions fully autonomously[6].

In this paper, we explain how these three trends are combining to create what we call "The IoT Payment Revolution". With electronic payments already ubiquitous, and with increasingly powerful connected devices able to run AI algorithms, we are on the verge of a world in which these devices will autonomously trigger payments to organisations, people and even other devices.

The question now facing business leaders in all sectors is not whether IoT payments will become pervasive, but rather how this change will impact their products and services, and what they need to do now to prepare for this future.

Drawing on Worldline's extensive payments experience and research into this area, together with the insights we have gained through working with our customers and partners, in this paper, we seek to help you answer these questions.

We start by defining exactly what is meant by IoT payments and detailing what is driving their growth. We then cover three important topics for which businesses need to be ready: the impact on underlying payment models, the challenges of trust and accountability, and the technologies that need to be understood and mastered. Finally, we describe some of the main use cases which can provide inspiration as to how your industry may be transformed.

There has been a huge growth in the number of connected devices, from an estimated 200 million globally in the year 2000 up to 38.5 billion in 2020.

1. https://www.telegraph.co.uk/finance/businessclub/money/11174013/The-history-of-money-from-barter-to-bitcoin.html
2. https://blog.forte.net/electronic-payments-history/
3. https://www.capitalontap.com/en/blog/posts/the-rise-of-digital-wallets/
4. https://paxtechnica.org/?page_id=738
5. https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020
6. https://worldline.com/content/dam/worldline-new/assets/documents/whitepapers/hyperautomation_in_payments.pdf

# What are IoT payments?

**We define IoT payments as payment transactions that are triggered by IoT devices with a certain degree of autonomy (requiring low or zero human interaction), as shown in Figure 2.**

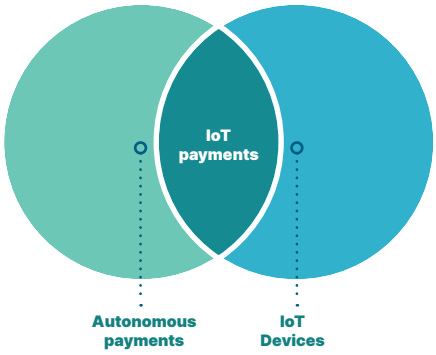


**Figure 2:** Autonomous payments triggered by IoT devices.

## What are IoT devices?

ARM has defined IoT devices as "pieces of hardware, such as sensors, actuators, gadgets, appliances, or machines, that are programmed for certain applications and can transmit data over the internet or other networks. They can be embedded into other mobile devices, industrial equipment, environmental sensors, medical devices, and more[7]."

This is a very broad definition, which encompasses small devices (such as a thermometer or light switch) with limited compute power, through to general purpose devices such as mobile phones (when they are used to sense our environment), through to large objects such as a fridge, a car or industrial machinery. In all cases, these devices are both connected and exist in our day-to-day world (rather than running software in a data centre).

## How autonomous are IoT payments?

One defining characteristic of IoT payments is that they are triggered by IoT devices with a certain level of autonomy, based on data that they are collecting and analysing. This is why, for example, we would not consider a person using a mobile app to make an account-to-account bank transfer to be an example of an IoT payment. However, if the mobile phone uses its knowledge of the person's location to trigger a payment automatically (with limited or no user interaction), then this would be considered an IoT payment. Similarly, if connected cameras are used to detect who is boarding and disembarking from a train and the correct fares are then automatically charged to the individuals, we would also class this as an example of an IoT payment.

Compared with other sectors, the payments industry is already highly automated and digitised, relying on the secure connection of millions of devices (such as payment terminals, contactless cards, cash machines and smartphones). As such, the technologies to support this are already well established. However, today, these payments are still predominantly triggered by humans. Tomorrow, with the advent of the IoT Payment Revolution, these payments will increasingly be triggered autonomously by machines.

As shown in Figure 3[8], we have defined four levels of increasing autonomy for payments. IoT payments must operate at levels 1-3. Here we explain the characteristics of each level of autonomy in more detail:

IoT payments are payment transactions that are triggered by IoT devices with a certain degree of autonomy.

### Level 1 (Informational)

The device has permission to access a user's bank account. The outcome of such a transaction is only to provide information regarding the permissible data available in this bank account around payments.
***For example:*** *a smart speaker at home configured to access a user's bank account through a voice service to offer information such as their account balance, last month's main transactions, or how much a specific device has paid in the last month on behalf of the consumer.*

### Level 2 (Permissioned)

The device must request the explicit consent of the user before triggering a payment. Payment permission must be granted by authentication means (e.g. biometric or non-biometric).
***For example:*** *at a fuel station, the device asks the user for their consent with a push notification to their smartphone before triggering the refuelling payment directly from their (bank) account in a system based on reading the vehicle's licence plate, to ensure that it is the authorised user who is refuelling the vehicle.*

### Level 3 (Conditional)

The device makes a payment automatically (without asking the explicit consent of the user) under pre-defined deterministic conditions set by the user to trigger the payment.
**For example:** *a smart printer in an office is configured so that when it is low in toner, an order and payment for the toner replacement is automatically triggered.*

### Level 4 (Fully Autonomous)

The device conducts a payment automatically using a combination of pre-defined deterministic conditions (as per Level 2) and, additionally, uses adaptive behaviours of the device depending on the context.
**For example:** *a system in a smart city that manages an annual repair budget initiating prioritised purchases and payments to suppliers based on the elements that need attention or repair in the city at any moment such as streetlights, garbage containers, etc.*

7. https://www.arm.com/glossary/iot-devices
8. First published by Worldline here: https://worldline.com/en/home/knowledgehub/blog/2020/march/from-automatic-to-autonomous-payments-can-things-pay.html

## Advanced IoT payments

Today, we see IoT payments being applied to relatively simple cases (for example, where the location of a person or object is used to trigger a payment). However, we can imagine scenarios where devices use multiple data sources and sophisticated AI algorithms to transform people's day-to-day lives.
An example of this could be a connected fridge that orders food automatically when it detects that supplies are low, based on an assigned budget and taking into account the changing preferences of the household and even dietary recommendations provided by a nutritionist. The fridge might also interact with various e-commerce solutions to find the best option in each case and book a delivery slot, after confirming availability for receiving the order by a member of the household.
This example shows how an IoT device combined with Artificial Intelligence and some rules can fully replace the existing modus operandi in which a human completes the order and makes the payment from their smartphone.
There are many other situations in which we will see how payment capacity can be transferred to things with different levels of autonomy.

### Full autonomous — Level 4

Smart IoT Payments
Machine-to-machine payments based on adaptive, context-aware,behaviour-based algorithms in a transparent and autonomous way.
***Example:*** *EV charging. Smart fridge stocking food. Self-maintaining street lamps.*

### Conditional — Level 3

Event-driven Payments
Payments based on pre-programmed deterministic conditions set by humans (e.g. smart contract clauses enforcement).
***Example:*** *Smart printer ordering ink. Smoke alarm ordering battery*

### Permissioned — Level 2

Pay-per-Use Payments
Pre-programmed periodic payments based on metered business model from IoT.
***Example:*** *Connected Appliance. Tolling/Pay-as-you-drive.*

### Informational — Level 1

Access to accounts
Leverage on PSD2 directives to consult user's bank account.
***Example:*** *Bank's voice assistant.*

**Figure 3:** Model developed by Worldline for the four levels of increasing autonomy for IoT payments.

# The drivers for Iot payments

## Frictionless and invisible payments

Consumers and merchants are expecting payment experiences to be increasingly frictionless, or even invisible. Frictionless payments are where the transaction can be completed easily by the customer with limited additional interactions beyond those already needed to access the product or service. An example of this is an in-app purchase authorised by facial recognition. Invisible payments take this one step further: here the customer does not need to take any specific additional action to trigger and complete the payment. For example, they may simply connect their electric vehicle to a charging point and then drive off when the charge is complete; payment is handled fully automatically.

Driving this expectation, on the consumer side, are the attitudes of Gen-Z, who are expected to increase their per-capita spending by more than 70% over the next five years[9]. Gen-Z is characterised as the first "digitally native" generation, which means they expect a smooth digital customer experience, and that payments become increasingly frictionless and invisible.


**Figure 4:** IoT to enable frictionless and invisible payments.

At the same time, merchants are looking for ways to increase conversion rates in their stores, whether bricks-and-mortar, online or omnichannel. Amongst the top five reasons for why customers abandon their shopping cart are if their preferred payment option is not offered or if the payment process is perceived as unsafe[10]. Merchants are increasingly accepting payment via mobile applications such as Apple Pay, AliPay, PayPal, Samsung Pay and WeChat Pay. At Worldline, we have developed WL Scan & Pay[11], which is a digital self-checkout that puts cashier functions into any smartphone with a camera. This solution offers benefits to retailers by addressing this need for a seamless omnichannel shopping with an integrated payment experience.

## IoT for next-level seamless experiences

Moving from frictionless to invisible payments often requires IoT payments, as illustrated in Figure 4. In physical stores, we see merchants exploring the "walk-in/walk-out" concept, where shoppers simply enter a store, pick up the goods they require, and leave (with payment automatically processed in the background). An example of this is Amazon Go which has successfully opened tens of stores. Even though there are discussions around privacy due to the use of image tracking technology and AI, it does seem that customers are adopting Amazon Go as they enjoy the seamless experience it provides[12].

And IoT payments are not only applicable in a retail setting. They can enable payments to be initiated by connected devices such as coffee machines, washing machines, agricultural equipment and cars. By 2023, this new market of IoT payments is expected to reach $27.6 billion and the market segments that will benefit from this development include retail, automotive, smart city and smart housing, to name just a few[13].

9. https://www.bcg.com/publications/2020/how-marketers-can-win-with-gen-z-millennials-post-covid
10. https://www.b2ceurope.eu/how-to-avoid-lost-ecommerce-sales-at-checkout/
11. https://worldline.com/content/new-worldline-com/en/home/solutions/pos-and-terminals/scan-and-pay.html
12. https://www.pymnts.com/news/retail/2020/how-amazons-cashierless-tech-will-or-wont-change-the-physical-retail-landscape/
13. https://www.intellias.com/iot-payments-what-s-ahead-for-contextual-commerce/

# IoT payment models

**The payment landscape is shifting towards a new world where a variety of models that support payment will co-exist, mixing domestic payment schemes, international card schemes, digital wallets, and distributed cryptocurrency networks. Figure 5[14] illustrates three alternative payment models that can potentially be used for IoT payments, which we describe in more detail below.**

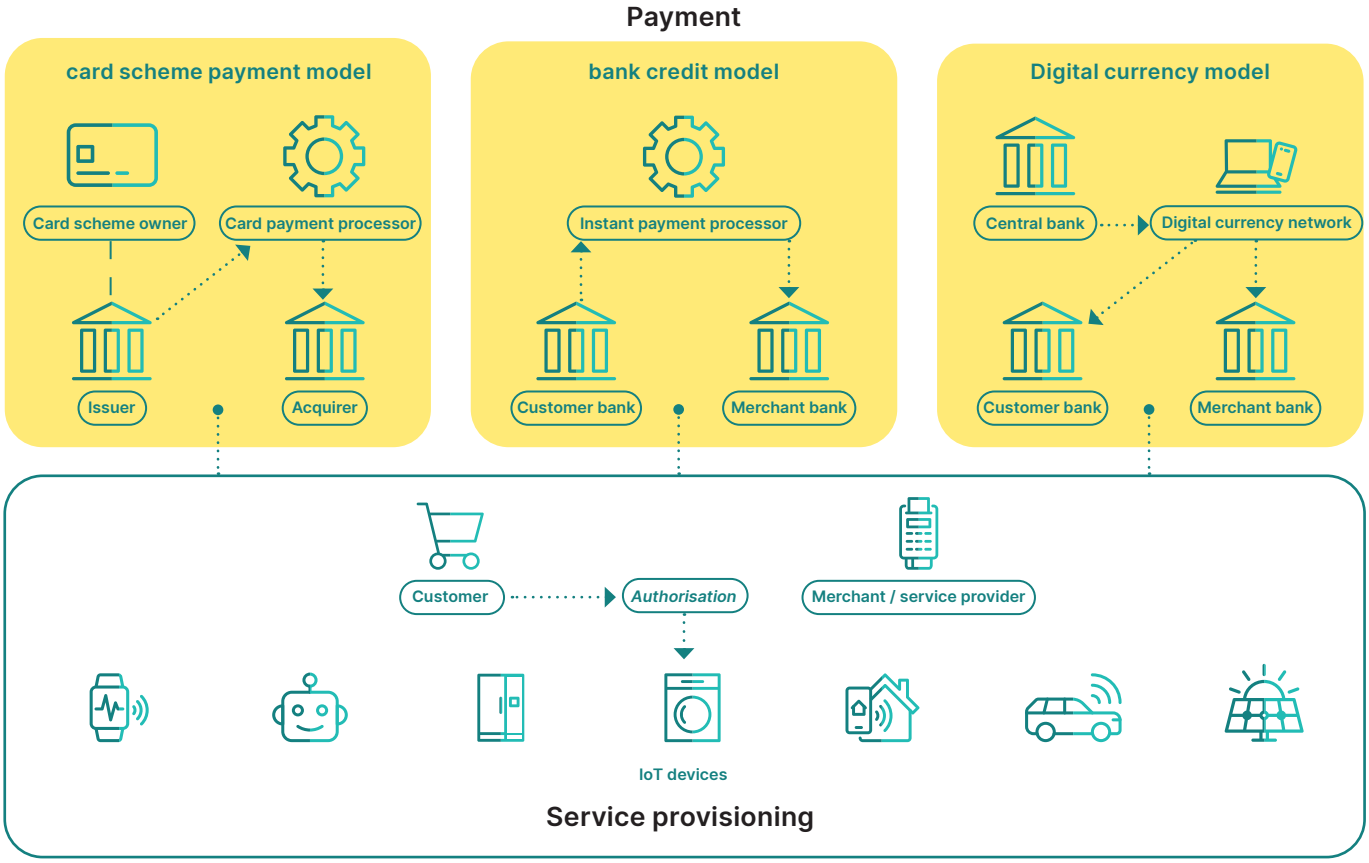


**Figure 5:** Payment models for IoT payments.

## Card scheme payment model

Major international card schemes have been successfully deploying non-card payment through payment tokenisation, which is the process of replacing sensitive data with a unique identifier that refers to, but does not disclose, confidential data.
Today, one of the most common uses of debit and credit card tokenisation is to emulate a payment card with a mobile phone, using Near Field Communication (NFC) to initiate a transaction, where the tokenisation replaces the Primary Account Number (PAN). As an extra security measure, the card emulation software (that resides in a smart phone or in the cloud) can generate a dynamic card verification value, which is uniquely bounded to a single transaction. This card tokenisation can also be used to turn IoT devices into payment-enabled devices. For example, a connected car can host a tokenised payment card, which enables payments from the car. The standardisation of this model is mainly driven by the card schemes.

## Bank credit transfer model

Instant Payments are currently an exciting development in many parts of the world. With Instant Payments, banks are able to execute money transfers in near-real-time. This means that, if a payer wants to pay someone in Europe, the beneficiary is able to receive the money within seconds, assuming that both the payer and the beneficiary are customers of banks participating in the SCTinst (SEPA Instant Credit Transfer) scheme. The SCTinst covers both person- to-person payments and person-to- business payments. Payment Initiation Services (PIS), enabled by PSD2- mandated third party access to accounts (XS2A), bring tremendous opportunities with or without Instant Payments and support most of the IoT payment use cases that are already feasible via card scheme payments.

## Digital currency payment

One of the most discussed technologies for IoT payments today are cryptocurrencies, based on a distributed ledger, which bring attractive technical features to an IoT environment. Since the ledger is distributed, it allows IoT devices to perform peer-to-peer transactions with or without the involvement of a trusted third party. It is still uncertain whether or how the current development of numerous digital currency initiatives will lead to some becoming mainstream in the future. Nevertheless, a possible scenario would be a move towards regulated digital currency networks where central banks will play a crucial regulating role, and where the exchange of different currencies will be possible. Another scenario could be multiple closed loop cryptocurrencies that optimise both transaction handling and cost inside one or multiple IoT payment ecosystems, ideally in an interoperable way.

Source: Worldline authors of this report

# Trust & accountability

## Consumer resistance

As described earlier, many people (especially younger generations) are positive about the smooth payment experience that IoT payments can enable. However, others will be resistant to such a change, perhaps due to a fear of new technologies that is often deeply linked to the local historical and/or societal context.

Beyond this fear of technology, many unbanked consumers have a justified concern about the proliferation of such "unmanned services" because they are excluded if only digital payments are accepted[15]. In response to this, we have already seen states in the US legislating against cashless businesses[16], requiring these stores to accept cash payments. Furthermore, even customers who have bank accounts may prefer to have the option to use cash, for reasons of privacy and anonymity.

In cases where there is no resistance to autonomous digital payments per se, a consumer still needs to trust a device with their financial assets (i.e. have confidence in its purchase decisions and spending control) even if it is a wallet with a fixed limit. For example, the concern that the system may be fooled by someone intending to steal from it may be very significant. In the longer term, understanding and trusting these systems will be key; auditability and interpretability of machine decisions is required in order to make them transparent[17] and win the trust of the user. Even with such transparency, ultimately the factor that increases acceptability and adoption may be the ability to easily roll back those transactions that consumers are not happy with.

**Auditability and interpretability of machine decisions is required in order to make them transparent.**

Not only do customers need to trust the device to make an autonomous payment on their behalf, they also have to trust that the device is secured against malicious threats. Given the huge variety of devices potentially involved in IoT payments and that the exchange of data often takes place in an open Internet environment, assuring security is especially challenging. Fraudsters are targeting IoT devices more aggressively than ever before[18]. In particular, in IoT payment use cases, where there is not a visible human control, cyber criminals could try to seize an advantage. It is therefore up to the payment ecosystem as a whole to ensure that the security of IoT payments can be guaranteed, that the consumer is able to easily control what devices do with their payment credentials, and that the consumer is fully aware of the security and control that is provided to them.

The key aspects that need to be considered are how payment credentials are stored securely on a device, how access to the device is controlled (to prevent hacking), and how the user of the device will authenticate themselves. We believe that regulations such as the EU's Second Payment Services Directive (PSD2) will need to evolve in order to cater for these challenges. Furthermore, monitoring to detect and prevent fraudulent IoT payments is also crucial. We will now discuss each of these in more detail.

## Securing payment credentials

The frictionless payment experience created by payment card tokenisation has made it the preferred approach for securing payment account information in IoT payment transactions, thanks to its standardisation and its adoption in the payment industry. EMVCo[19] mandates a user identity and verification step before granting any token request. A similar mechanism is necessary to ensure that device owners are aware of token requests originating from their devices and that such requests are legitimate. Major payment companies and card scheme owners are beginning to address these concerns. For example, Visa secures payment functionality for IoT using their Visa Token Service[20] for provisioning a token to a device to activate payments.

## Ensuring strong authentification

The basic requirements of PSD2 state that strong customer authentication (SCA) has to be based on the use of two or more possible authentication elements, categorised as:

**Knowledge**

(i.e. something only the user knows, such as a password).

**Possession**

(i.e. something only the user has, such as a token).

**Inherence**

(i.e. something only the user is, such as a fingerprint or face scan).

In IoT payments, authentication is more complex than in "traditional" payments because both device authentication and customer authentication need to be addressed, yet often the ambition is to make payments frictionless or invisible. We believe that regulations will need to evolve to cater for these Object- Initiated Transactions, and now we describe this in more detail below.

15. https://www.pymnts.com/wp-content/uploads/2020/03/Commerce-Connected-Playbook-Mar20.pdf
16. https://www.wsj.com/articles/philadelphia-is-first-u-s-city-to-ban-cashless-stores-11551967201
17. https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf#page=58
18. https://blog.f-secure.com/attack-landscape-h1-2019-iot-smb-traffic-abound/
19. https://www.emvco.com/
20. https://usa.visa.com/partner-with-us/payment-technology/visa-token-service.html

## Device authentification

A large proportion of IoT devices are deployed with a weak security level; sometimes devices are even preconfigured with an easy to guess 4-digit password (e.g. 0000), which remains unchanged during operation. The lack of a common security framework poses serious problems for device manufacturers, service providers and consumers.

Existing payment authentication methods are not suitable for many IoT devices due to resource constraints such as low power and limited storage capacity. It is important to determine and to reach the desired level of trust without overburdening the computing capacity of IoT devices. Today, there is an increasing adoption of standard authentication methods such as PKI, OAuth and OIDC to serve IoT use cases of a specific scope and scale. Further standards from OAM DM, LWM2M and TR-069 are also being deployed to secure the communication between nodes in an IoT network[21].

## Consumer authentification

As stated earlier, an IoT payment transaction must be trusted and accountable. An IoT device by itself cannot be held accountable: ultimate accountability will instead rest with the person or organisation that has delegated payment tasks to it. This necessitates consumer authentication. The key challenge is to apply the most convenient authentication method to a specific payment use case.

As illustrated in Figure 6, there are various forms of customer authentication methods and, depending on the type of usage and the acceptable level of risk, certain methods are more suitable than others. When it comes to customer convenience, biometric authentication is becoming increasingly acceptable, as long as privacy is assured.
For example, voice recognition is a good candidate for in-car payment, since voice control is already a common technology used in connected cars.
In retail, we are seeing examples of contactless palm scans being used to authenticate a payment[22].

It should be noted that solutions like face recognition and a palm scans by themselves still only offer 1-factor authentication. Consumer authentication could be improved through the use of continuous multimodal biometrics and contextual information checking, where several sources of biometric information (such as gait, face, etc.) are combined with other information (such as where the person is and what they are doing) to provide a more rigorous and harder-to-fool authentication of the individual.

## Objet-initiated transactions

PSD2 defines two ways for initiating a transaction: Merchant- Initiated Transaction (MIT) and Customer-Initiated Transaction (CIT).

With MIT, the user has enrolled their credit card, IBAN or other payment instrument with the merchant, and then the merchant initiates the transaction, for example for one-click orders or recurring orders. This is not always appropriate for IoT payments as the consumer may want to pay for services for which they have not yet enrolled, such as toll fees in a foreign country.

With CIT, PSD2 requires strong authentication and, as described previously, this is not something an object can do autonomously for us.

As a result, a new kind of transaction initiation with its own authentication requirements is needed. We believe that regulations will be updated to cater for these Object-Initiated Transactions (OIT). Failure to do so could see a proliferation of entities providing services by acting as third parties using MIT. These could become de-facto standards for Object-Initiated payments, but they may not ultimately protect the best interests of consumers and merchants.

The key challenge is to apply the most convenient authentication method to a specific payment use case.

## IoT payment fraud prevention

As previously discussed, IoT devices are particularly vulnerable to cyber-attacks and therefore the continuous monitoring of IoT payment transactions is essential to detect and prevent fraud. As IoT devices also have the potential to offer many more data sources, fraud detection algorithms can have a more complete picture of user actions (including before, during and after the payment is made). For example, by knowing that an individual has travelled to a shop in their car and then used their phone to scan products in the store, the legitimacy of the final payment transaction could be assured with greater confidence.

**Figure 6:** Various biometric authentication methods.

21. https://www.muutech.com/en/iot-device-management-protocols-lwm2m-oma-dm-and-tr-069/
22. https://www.a3bc.org/carrefour-green-court-first-store-in-romania/

# Key technology enablers

So far, we have described why we foresee a rise in IoT payments and how this will potentially impact the dominant payment models. We have also discussed the challenges associated with trust and accountability. Now we will describe some of the key technology enablers that businesses wishing to leverage IoT payments will need to master. These are illustrated in Figure 7, which shows our view on how soon they will need to be adopted and also the potential impact they will have on the IoT payment landscape.

## Trusted Iot devices

As seen in the previous section, IoT devices that trigger payments must be secure. Therefore, we see a strong need for these IoT devices to have embedded cryptographic hardware and enough computing power to ensure the integrity of data generated in the device itself before it is transmitted.

To guarantee device identity we must ensure integrity and confidentiality of information. This can be achieved with different levels of security: secure elements, trusted execution environments (TEE) or white boxes. The first two require hardware components and are not always available on IoT devices, while software-based white boxes may not offer sufficient security for payment applications[23].

Identity of an IoT device can also be provided by a Physically Unclonable Function (PUF) enclosed in trust zones or secure elements. These functions provide a unique identity to each specific device. They rely on small variations during the manufacturing process and give unique features that can be used to derive private and public keys to authenticate the device. Because the device does not store the private key, rather it is derived from an unclonable feature of the device, the security and the integrity of such devices is greatly improved.

## Authentification

As already discussed, in order to process payments on behalf of the device owner, there is a need to authenticate the IoT device. We see three authentication protocols that could prove useful for application in IoT environments. The first option is the FIDO Universal Authentication Framework (or UAF)[24], which provides strong authentication through public key cryptography. The second option is the recently published EMVCo specifications for 3-D Secure (3DS)[25], which is a messaging protocol that enables consumers to authenticate themselves to a card issuer when performing card-not-present (CNP) transactions. The third candidate is OpenID Connect, which is an identity layer on top of the OAuth 2.0 authorisation protocol[26]. It allows devices to verify the identity of the end user based on authentication performed by an authorisation server.

## Device lifecycle

An IoT payment device must ensure that all communications and processes are secured end-to-end, from the device's own security component to the payment issuer back-end system. Device manufacturers and service providers need to be aware that, even after the device has been delivered to the end user and the payment credential has been provisioned, there is still a need to manage the lifecycle of the payment application and the IoT device itself. Key considerations include changes of ownership, expiration of payment credentials, application end-of-life and device end-of-life.

## Interoperability

The diversity of IoT platforms and network protocols complicates system interoperability between IoT applications, preventing the IoT from reaching its full potential. The interoperability issue and the lack of standards lead to complex and costly integrations between platform applications and device data, or the prevalence of proprietary rather than open APIs (Application Programming Interfaces). To address IoT interoperability it is necessary to build middleware platforms or IoT hubs, enabling intermediary IoT services to communicate in a common language and assure security levels for the connectivity and exchange of data across different platforms.

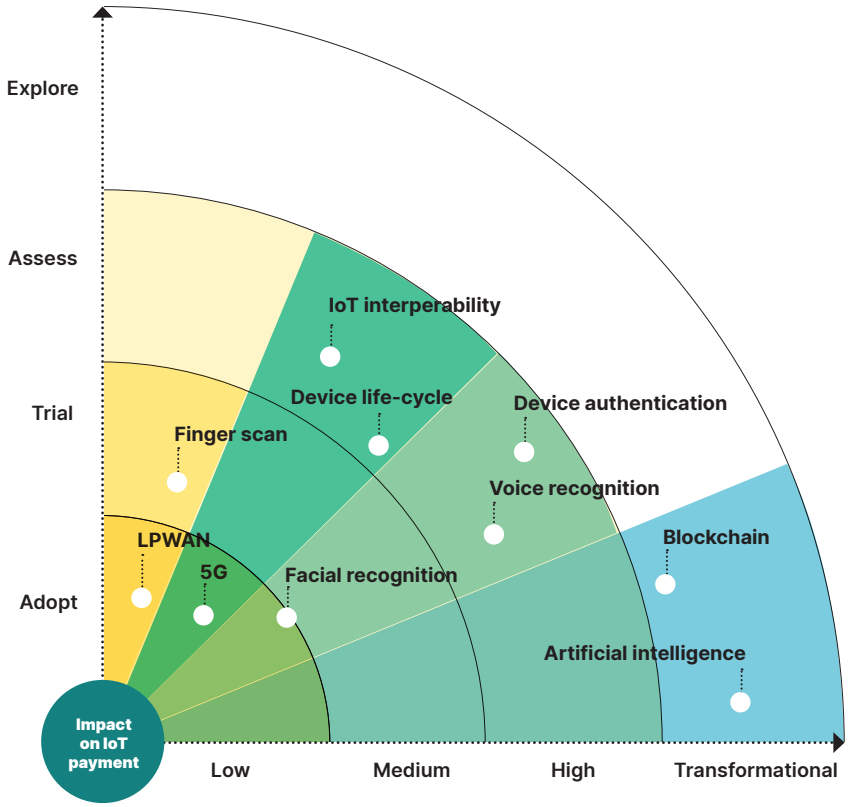


**Figure 7:** Key technology enablers for IoT payments.

23. For example, in this competition, all white boxes were cracked in 27 hours or less: https://eric-diehl.com/white-box-cryptography-an-open-challenge/
24. https://fidoalliance.org/
25. https://www.emvco.com/emv-technologies/3d-secure/
26. https://oauth.net/2/

## Communication technology

Most IoT devices rely on wireless communication technology. Different wireless technologies are emerging, each with their own characteristics, advantages and disadvantages from both a technical and commercial point of view.

The two major categories that we see are LPWAN (Low-power Wide-area Network) and 5G. LPWAN can operate on both the licensed and unlicensed radio spectrum. On the other hand, 5G (consisting of NB-IoT, LTE-M, LTE cat x) operates only in the licensed radio spectrum. Depending on the use case, and the corresponding business case, one technology will be more suitable than the other. Therefore, it is likely that LPWAN and 5G will co-exist.

LPWAN is designed for IoT applications that only send and receive small amounts of data (i.e. a few tens of hundreds of bytes per day). The main advantage of LPWAN is its low power consumption, enabling the battery life of sensors to last 10+ years depending on data transmission frequency.

The first implementations of 5G are providing a better bandwidth and lower latency and enabling the connection of a very high number of IoT devices. The low latency will enable increasingly frictionless payments as it will speed up person-to-person instant payments and mobile payments in general. Increased bandwidth will enable much more data to be collected from a much wider range of sources, which can feed the AI algorithms that will boost the level of autonomy of IoT payments. We can imagine many possibilities that this will enable. For example, in a 5G empowered smart city infrastructure, streetlights could autonomously order and trigger payments for repairs and replacements as recently shown in a demo from Worldline.

## Artificial Intelligence (AI)

AI has tremendous potential to boost efficiency and enable innovative service development. Worldline has addressed these topics in detail in our white paper Hyperautomation in Payments: Automating complexity at scale[27]. This notes that despite its great potential, AI has not yet been widely adopted in many areas, including the IoT landscape.

IoT devices collect large amounts of data that can fuel AI machine learning algorithms and neural network systems to predict consumer behaviour. Extensive training on user behaviour and the transactional context is needed to effectively implement the capability to execute truly autonomous payments (at level 3) on behalf of and with the full confidence of a human user.

Today, most of the information collected from IoT devices is processed by a central server in the cloud and only 20% is processed locally[28]. In the future, we will see a shift from centralised to decentralised processing. More advanced AI- enabled devices with greater edge computing capabilities together with more resource optimised AI models will be needed to run autonomous algorithms.

## Blockchain

Blockchain technology is a cryptography-driven solution with the potential to use a distributed decision model to replace existing centralised architectures. It provides an innovative technological approach to manage data and execute transactions in an indisputable way, where accuracy and reliability is paramount, without the explicit need for a trusted third party. As it is based on peer-to-peer technology, distributed ledger technology stacks can perfectly fit a highly distributed IoT ecosystem.

In a 5G empowered smart city infrastructure, streetlights can autonomously order and trigger payments for repairs.

The essentials of using blockchain technology consist of data that cannot be altered (integrity), no single point of failure (availability), identity managed by public/private key pair (authentication), cryptographic primitives that deny data access to unauthorised users (confidentiality), and that all transactions are signed and can be audited (non-repudiation).

27. https://worldline.com/content/new-worldline-com/en/home/knowledgehub/publications/download-ai-hyperautomation.html
28. https://atos.net/wp-content/uploads/2019/11/digital-vision-for-cyber-security-2-2.pdf

# Business impact

**IoT payments will help accelerate the development of sharing economy platforms.**

As mentioned in the introduction, there were over 38.5 billion connected devices in 2020[29] (triple the number in 2015). From this growth trajectory, billions of additional IoT payment transactions can be expected, yet most of these opportunities still remain untapped today. For example, a smart "personal shopper" could search for a specific product and close the deal automatically at the given permissible price on behalf of the consumer.

Solar panels could sell spare energy to other consumers/machines, with dynamic pricing and corresponding payment transactions being handled autonomously between two devices, enabled by blockchain technology. With so many potential use cases, it is important to identify which ones offer the greatest business opportunities for your organisation now and in the future. Figure 8[30] provides our assessment of the expected adoption and business potential for many IoT payments use cases. You may find it useful to prepare your own version of this radar for your company, taking into account factors like market traction (as assessed thorough interactions and discussions with your partners and your clients), market size, expected transaction volumes and expected customer adoption.

We will now describe in more detail two of the more promising examples of IoT payment use cases: electric vehicle charging and the sharing economy.

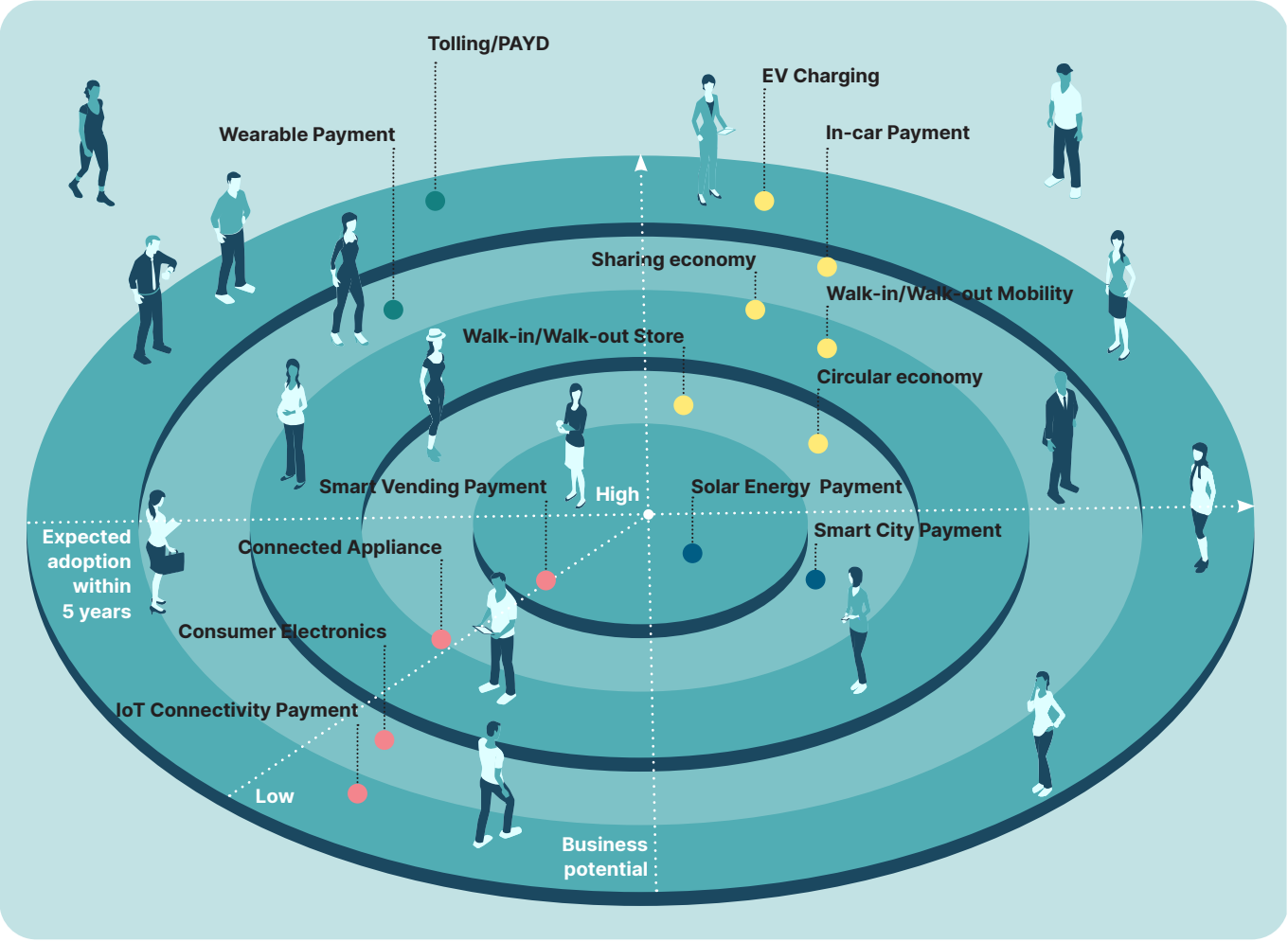


**Figure 8:** IoT payments business radar.

29. https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020
30. Source: Worldline authors of this paper

## Use case: electric vehicle charging

The market for Electronic Vehicle (EV) charging infrastructure in Europe is gaining strong traction[31]. We believe that EV charging will bring short and mid-term business opportunities. Here we briefly describe an exemplary customer journey supported by IoT payments (as illustrated in Figure 9).

Imagine enjoying future rides in your electric vehicle without worrying about where to recharge the battery, whether or not you will have a charging station made available for you, or where to get a good meal on the way. In this idealised customer journey, payments would become invisible, disappearing completely into the background. In such a use case, the car could use information such as the current battery level, the number of miles left to complete the journey, how long the driver has been driving non-stop, and their usual habits for taking breaks and their food preferences. Using all of this contextual information, the car can determine what would be the best location and time for it to be charged. The car could reserve the charging point, and potentially even a table at the food outlet, for the expected arrival time.

The driver can relax and enjoy a coffee or some food, which will be paid for automatically using a walk-in/walk-out model. When the car is sufficiently charged, the driver will receive a notification on their phone (or wearable device such as a watch).When the driver disconnects their car from the charging point, the payment for the charging session is automatically triggered by the car as the journey is resumed.

This kind of journey could be implemented based on the card payment or bank transfer models described earlier. However, it could also be possible to use a decentralised ledger for payments[32], where blockchain enables a payment to be made directly from the car to the charging station, even if neither is connected to a centralised infrastructure.

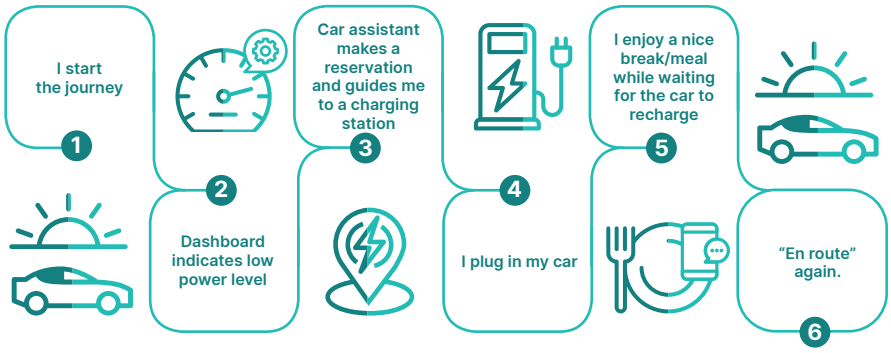


**Figure 9:** Exemplary customer journey for EV charging.

## Use case: the sharing economy

Among younger generations we are seeing a shift in attitudes as to how they consume goods and services. For them, "consumption means having access to products or services, not necessarily owning them."[33] Due to this, servitisation (the trend of delivering more and more products "as-a-service" with charging models closely linked to the value gained by the consumer) is becoming an increasingly standard business model. However, servitisation requires that you can monitor and control usage — something that is easy to do for cloud-based software but harder to do for physical goods.

Gen-Z are also extremely concerned about climate change[34], which we expect will drive them to prioritise sustainable ways of living. We see that this drive for sustainability, combined with growth in servitisation, will propel the sharing economy forward: individuals who are less concerned with ownership will be able to share access to material products with others, leading to a lower cost for everyone (paying only for what they need), while also minimising the environmental impact. IoT payments will help accelerate the development of sharing economy platforms, because they help to enable pay-per-use business models for physical products.

These new models are also interesting for financial institutions. Many have already developed long-term visions driven by sustainability, looking at social as well as environmental benefits. Today, banks, insurers, pension funds and asset managers are developing sustainable finance practices, which are becoming the new standard. In simple terms, sustainable finance means defining and deploying investment plans which take into account criteria for Environment, Society and corporate Governance (the "ESG criteria").

A good example of sustainable finance is the Circular Service Platform[35] (CiSe), initiated by Rabobank, Sustainable Financial Lab[36], Unc Inc and Allen & Overy. This blockchain-based platform helps service providers and manufacturers develop pay-per-use business models, driven by IoT[37], at the same time promoting the sharing economy. It is important to note that one of the reasons why banks have a great interest in making pay-per-use business models successful is because they are expected to finance service providers (and therefore the associated financial risks have to be managed properly and effectively). Another useful example is FINN[38] (a spin-off from ING) that is developing "Banking of Things" services by adding payment capabilities to smart devices. It is a thought-provoking initiative which shows a possible direction for how financial institutions can innovate through business platforms that are driven by IoT.

31. Information based on recent announcement of many public tenders for EV charging
32. https://www.finextra.com/blogposting/16658/blockchain-and-disruption-in-the-financial-world-will-banks-survive
33. https://www.mckinsey.com/industries/consumer-packaged-goods/our-insights/true-gen-generation-z-and-its-implications-for-companies
34. https://www.forbes.com/sites/emanuelabarbiroglio/2019/12/09/generation-z-fears-climate-change-more-than-anything-else
35. https://www.cise.network/
36. https://proofingfuture.eu/2021/03/15/sharing-e-mobility-an-interview-with-henk-kuipers/
37. https://bundles.nl/
38. https://makethingsfinn.com/

# Conclusion

**As we have seen, the IoT Payment Revolution is now a certainty rather than a possibility. Stemming from the rise in digital transactions, the growth in the number of connected devices, and advances in AI, we see that IoT payments will become a key enabler for increasingly sought after frictionless and invisible payments.**

**This will impact payment models. In particular, we expect a rise in the use of bank transfers and digital currencies for making payments.**

**Key to the increased adoption of IoT payments will be trust: in the device, in the environment in which the transaction takes place, in accountability, in security, in retaining control, and in being able to reverse a transaction if anything goes wrong.**

**At Worldline, we continue to research these new growth drivers together with our clients and partners, exploring and testing innovative use cases and technical solutions. We hope this paper has helped you to understand the potential that IoT payments can offer as well as helping you to formulate the actions you need to take now to prepare for this future.**

## Key takeaways

### IoT payments

There is increasing growth in digital transactions, connected devices and the use of AI. This is resulting in the IoT Payment Revolution where more and more connected devices will make payments autonomously on behalf of people.

### Frictionless and invisible payments

IoT payments can enable increasingly sought-after frictionless and invisible payment experiences, where consumers have to take very few (or no) actions to conduct a payment transaction.

### IoT payment models

We expect that IoT payments will drive the adoption of bank transfer and digital currency payment models.

### Trust

Specific considerations must be addressed relating to trust. In particular, both the device and the consumer must be authenticated. We expect that regulations will need to evolve to cater for Object-Initiated Transactions.

### Accountability

Accountability for transactions will continue to rest with individuals or organisations who delegate devices to make payments on their behalf. Verification of delegation and the ability to roll back unwanted transactions will be important factors to address.

### Technology enablers

Use our radar of IoT payment technology enablers to assess your current readiness.

### Business impact

Assess use cases based on the expected adoption and the business potential for your company in order to determine where you should invest now.

# Authors and acknowledgments

This paper was prepared by the Worldline Scientific Community and authored by the following experts from across the business:

**David Daly,**
Worldline Scientific Community Editor-in-Chief, UK

**Tony Ducrocq,**
France

**Louise Freer-Jones,**
Competitive Intelligence, UK

**Dalila Hattab,**
Head of Financial Services Lab, France

**Colombe Herault,**
Research Development and Innovation Manager, France

**Gregory Herpe,**
Project Manager IoT, France

**Minh Le (Lead Author),**
Head of Connected Vehicle & Emerging IoT Offerings, Netherlands

**Jose Maria Lopez,**
Head of Business Development Mobile Competence Center, Spain

**Santi Ristol,**
Mobile Competence Center Director, Spain

**Joan Vicent Orenga Serisuelo,**
Technical Director Mobile Competence Center, Spain

**Peter Timmermans,**
Innovation Champion New Technologies, Belgium

**Tomas Garcia Zaragoza,**
Product Management, Spain

We are also grateful to Gilles Grapinet, Wenlin Jin, Karim Jouhari, Yacine Kessaci, Nicolas Kozakiewicz, Denis Lesieur, Olivier Maas, Johan Maes, Sebastian Ramatowski and Jeroen Vershuuren, who all provided valuable insights and feedback during this paper's preparation.

**About the Worldline Scientific Community**

The Worldline Scientific Community identifies and analyses key trends in society, business and technology. By predicting how these trends will evolve, the community creates valuable strategic insights for our clients, helping them to prepare for this future.

The community is personally chaired by Worldline's CEO and Deputy CEO and is made up of diverse technology and business experts from across the Group.

Scientific Community

# About Worldline

Worldline [Euronext: WLN] is the European leader in the payments and transactional services industry and #4 player worldwide. With its global reach and its commitment to innovation, Worldline is the technology partner of choice for merchants, banks and third-party acquirers as well as public transport operators, government agencies and industrial companies in all sectors. Powered by over 20,000 employees in more than 50 countries, Worldline provides its clients with sustainable, trusted and secure solutions across the payment value chain, fostering their business growth wherever they are. Services offered by Worldline in the areas of Merchant Services; Terminals, Solutions & Services; Financial Services and Mobility & e-Transactional Services include domestic and cross-border commercial acquiring, both in-store and online, highly-secure payment transaction processing, a broad portfolio of payment terminals as well as e-ticketing and digital services in the industrial environment. In 2020 Worldline generated a proforma revenue of 4.8 billion euros.

worldline.com

**For further information**
WL-marketing@worldline.com