May 2023

CREATING THE NEXT GENERATION OF PAYMENT RAILS: **LESSONS FROM PIX**

HOW TO BUILD A REAL-TIME PAYMENTS PLATFORM AT ITS FULL POTENTIAL

CTPI

CENTER FOR TECHNOLOGY AND PUBLIC INTEREST

ISBN: 978-84-09-51038-2
https://doi.org/10.59262/swcj93

TABLE OF CONTENT

1.

INTRODUCTION

ABOUT PIX

PIX IS THE REAL-TIME PAYMENTS RAIL created by the Brazilian Central Bank (BCB). Since its launch in late 2020, Pix has been gaining notoriety for its numbers and its early impacts on the lives of Brazilians of all social groups. According to BCB data, until February 2023, Pix reached the mark of over 148 million unique users (136 million individuals and 12 million legal entities). In the last three months, Pix processed 8 billion transactions, amounting to R$ 3.4 trillion (~USD 650 billion).

These numbers alone are enough to recognize the success of Pix as a fast payment system. Additionally, its systemic effects are just as impressive. Since the Pix launch, Brazil has reduced the total cash circulation by 10%, as stated in Brazilian Central Bank. It is the first time in history that the volume of Reais, the official currency of Brazil, circulating declined instead of increasing. A survey released in October 2021 by PayPal also reveals that almost 80% of Brazilians welcome abandoning cash in favor of electronic payment methods.

The rail's social-economic impacts also started to show early on. Numbers from BCB show the effect Pix had on financial inclusion. During the first year of Pix operation, over 45 million Brazilians, who did not make electronic transfers using the old infrastructures, started using Pix frequently. BCB also estimates that Brazilian businesses saved almost R$ 5 billion (~USD 1 billion) in card fees in the same period.

ABOUT THE AUTHORS

WHATEVER ASTONISHING MILESTONES PIX HAS collected so far, they were only possible due to a collection of governance and technical decisions the internal team at the Brazilian Central Bank has been making since 2018. These brilliant public servants worked tirelessly to build something extraordinary that would benefit all Brazilians.

Due to our professional affiliations at the time, we had a once-in-a-lifetime opportunity to benefit from the governance structure put in place and contribute to the technical design of Pix from the very beginning until the pre-launch. All this work was recognized by the regulators as instrumental in defining the design of Pix and many of its important features. Since 2018, we have been immersed in the Pix ecosystem in Brazil and are now ready to share our insights on what makes Pix what it is and how to introduce the same concept to other countries.

MARIANA CUNHA E MELO

JONAS ABREU

ABOUT THIS PAPER

THIS PAPER'S GOAL IS TO PROVIDE a comprehensive deep dive into the works of Pix, the critical decisions that enabled Pix's most essential features, and why they matter so much. The paper also indicates where the authors would recommend a different approach from the one the Central Bank implemented, always highlighting the tradeoffs between them.

Finally, this paper provides an in-depth technical description of Pix's design and protocol. We expect this paper will help stakeholders worldwide to navigate through design and architecture decisions while building fast payment systems. Furthermore, we hope countries can benefit from the positive impacts an effective real-time payments platform can bring to their people and economies.

2.

PROPERTIES AND PLATFORMS: **A HIGH-LEVEL VIEW OF PIX**

Before getting into how Pix works, it is worth making a few general remarks about Pix's properties and the fundamental decisions. These will help contextualize the payment system as a whole.

2.1.
PIX'S ESSENTIAL PROPERTIES AND THEIR SYSTEMIC CONSEQUENCES

a. Nine properties of Pix

1 → Government-driven

The Brazilian Central Bank was responsible for creating the rail, its rules, and its systems. It is also who operates the system and provides the necessary infrastructure. BCB is the financial and payments market regulator. The fact it was the financial system regulator that drove the whole project had many advantages in Brazil's case. Although it might be possible to make different arrangements work in other countries, there are few incentives for a market-driven solution to strive for global optimization and build a truly open, cost-effective, and flexible rail. To facilitate the process of extrapolating Pix's case to a broader set of circumstances, however, the role the BCB plays in the Pix rail may be identified in this paper more generally as a Payment System Operator or PSO.

2 High availability

Pix is, of course, available 24 hours a day, 7 days a week, 365 days a year, with no downtime on payment or any other key services.

3 Instant gross settlement

Pix offers instant payments, with settlement and clearing in up to 10 seconds (P50 = 6s; P99 = 10s). After that period, there is a timeout and the transaction fails. So in 10 seconds either the money is in the payee's account or the payer can safely try the transaction again.

4 Reliability

For both end-users and PSPs. For Payer users, all information about the transaction comes from accredited sources and is presented on their screens for confirmation before the money flow starts. So payers can trust the information that is presented and verify the destination and amount are correct before hitting send. For Payee users, the fact all Payee PSPs are mandated to notify the Payee every time a transaction is received also contributes to the trust and reliance in the system. After

all, the Payee can trust the notification from their bank that the money is already available in their accounts.

For PSPs, both Payer PSP and Payee PSP can know with certainty the status of a payment order at any given time for two reasons: every transaction is assigned a unique end-to-end ID that allows tracking the transaction throughout the flow; and the Payments Systems Operator (BCB in the Pix rail) is the single source of truth about the status of the payment so that any PSP can query the status of any individual transaction. Apart from that, every message in the payment flow is signed using digital certificates, so there is always cryptographic proof of every event from end to end, increasing the system's reliability.

5 → Ubiquity

Over 90% of all active Brazilian accounts are linked to Pix, according to Brazilian Central Bank. For PSPs with more than 500,000 active accounts, joining the Pix rail to allow end-users to make and receive Pix transactions is mandatory. No registration is needed from end-users to join the service — they simply send or receive funds as they would in any other online banking system.

6 → Cost-effectiveness

PSPs are charged nothing to send payments and around $0.0002 to receive Pix transactions.

7 Standardized user experience requirements

An additional factor that aided Pix's growth is the existence of a minimum user experience standard on all PSPs. Brazil's Central Bank mandated it because they want clients from all PSPs to use Pix easily. All participants must offer payment services using QR Codes, manual input, and alias keys. However, they are only required to generate static QRCs (and just for instantly natural persons).

8 Flexibility, extensibility, and evolvability

Pix is both a transfer and a payment rail and was built to absorb all existing use cases with multiple payment initiation capabilities (P2P, P2B, P2G, B2P, B2B, B2G, G2P, G2B, etc). Pix's extensibility and evolvability allow the protocol to adapt easily without the need to change the base protocol. It was also built to last.

Besides, Pix's simplicity, extensibility, and potential for data richness make it a powerful tool. The entire system was designed to function as a platform — not just one payment product. Instead of relying on QR Codes with the payment information in plain text, Pix "dynamic" QR Codes contain a URI that grants access to the routing information directly from the Payee PSP's servers. The consistency and accuracy of the data are ensured by frequent updates, as well as a formal communications protocol that allows Payee PSPs to send virtually any extra information relevant to the payment.

BCB set up specific fields as mandatory, but it also created an "additional fields" schema where the Payee PSP could make any additional information appear on the Payer PSP app on the payment confirmation screen. That is: BCB did not try to specify all the admissible fields but one admissible schema to add any other field.

9 Security by design

Pix was also projected to be secure by design, managing sources of truth, allowing confirmation of information before transfers are initiated, and reducing the complexity of the rail. Furthermore, Pix's design is anchored in the best practices of distributed systems. The Pix rail is idempotent, meaning that the same transaction can be performed multiple times without the risk of the value being credited multiple times.

Additionally, the BCB is used as a source of truth when there are disputes about where the money went — providing cryptographic proof to resolve such questions. Another example is Pix's use of powerful abstractions and tools such as replication logs to ensure that centralized data (alias keys) can be replicated into each relevant PSP's system without downtime.

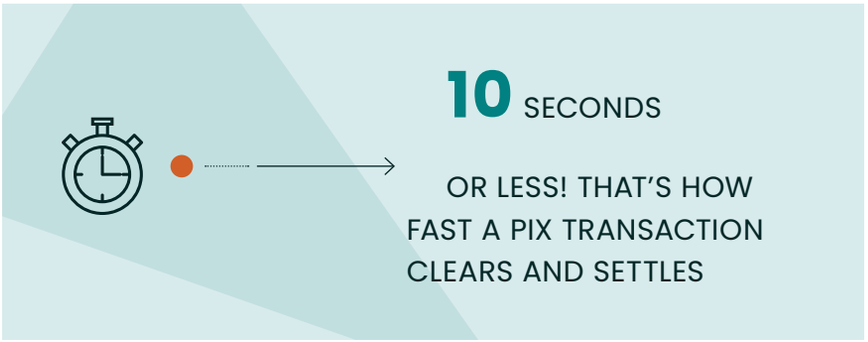
b. Systemic consequences that follow

THE CRITICAL PROPERTIES OF PIX have many systemic consequences. No longer is it a competitive advantage for companies to have been in the market for a long time and to have built up large customer bases. Any recently created payments institution can now enable its users to send money to as many recipients as the big incumbent networks do — without paying for access or being pre-approved by the gatekeepers.

Furthermore, the payee can use the end-to-end ID generated by a payment request to keep track of which payments have been fulfilled and which haven't, thus improving the management of cash flow and inventory.

In addition, the Payee PSP can create virtually any content to be rendered in the Payer PSP app — meaning it has a newfound capability of creating features without owning that relationship with both payer and payee. Traditionally, on credit card payments, the primary interface between merchants and customers is a credit card terminal (also called a point-of-sale device) owned by the merchant. However, with QR

Code payments, payment interfaces are controlled directly from the Payer PSP's app on the Payer's phone. That allows Payer PSPs to offer POS credit and other previously impossible features. It can also gather much more information about the payment.



To summarize, Pix is a payment and transfer scheme that operates and settles transactions in less than 10 seconds. The system operates 24/7/365 and is data-rich, extensible, and ubiquitous. The Brazilian Central Bank is the Pix scheme's settlor, managing its operation and defining the rules governing Pix. The scheme operates over an infrastructure consisting of a real-time gross settlement chamber and an alias database, both of which are under the Central Bank's direct operation. Pix was created to foster innovation, competition, and the digitalization of payments and the economy as a whole.

2.2.

FAST PAYMENT RAIL AS A PLATFORM, NOT A SPECIFIC PRODUCT IMPLEMENTATION

ONE OF THE MOST IMPORTANT traits that make Pix unique is the nature of its design core. Typically, when a company or a government sets out to build a payment rail, the focus is to solve a handful of use cases. And in doing so, communications protocols fall prey to over-specification and over-standardization, resulting in unnecessary complexity and inefficiency. And whenever a new use case emerges, those responsible for the rail need to either make workarounds in the already existing fields and messages or build an entirely new rail to accommodate the additional needs.

To take Brazil as an example, before Pix, the Brazilian Central Bank already operated the two settlement chambers through which all money flow in Brazil has to go through one for the movement of funds (STR) and the other for custody and trade of federal bonds (SELIC). On top of those two, however, the Central Bank has authorized fifteen other centralized settlement infrastructures to deal with several different financial products: there is one for paper checks, one for card schemes settlement, another for payroll accounts, another for transfers of less than R$ 1 million in one business day, another for transfers in D+2, a number of others to register credit cards receivables, another for bill payments, etc. Each of these rails was built separately, as needed. So they implemented their own

communications protocols, created their criteria for entry, and – as a general rule – are expensive to join and operate.

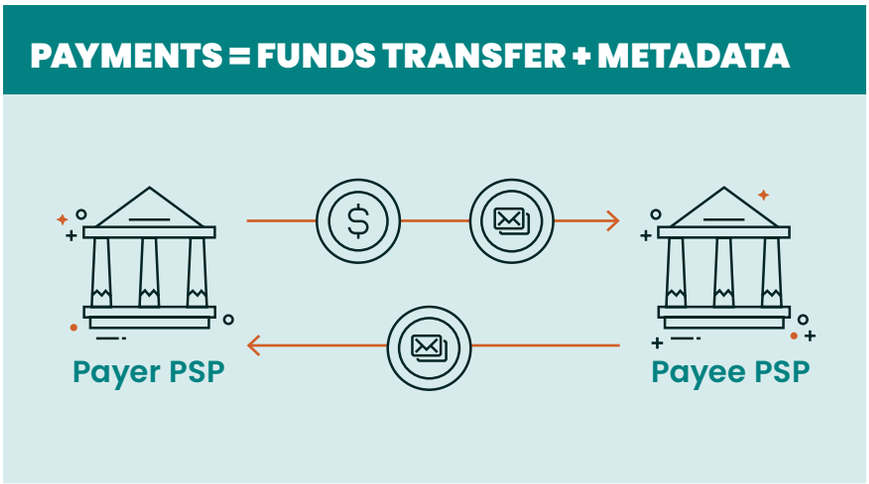
Pix takes a fundamentally different approach to systems design. The rail was built not as a specific product implementation but as a true platform. In fact, Pix was built to accommodate every payment method existent in Brazil at the time of launch and *any other that might come to play after*. That was only possible because all payment solutions and products necessarily share two foundational aspects:

1.

A MONEY FLOW: IT MOVES FUNDS FROM ACCOUNT A TO ACCOUNT B;

2.

A DATA FLOW: EACH TRANSACTION IS ASSOCIATED WITH SOME METADATA.



Therefore, any effective payment system should be predicated on enabling a money flow and a flow of arbitrary metadata between any two participants. That statement gives rise to three problems that need solving: an issue of protocol, an issue of trust, and an issue of reach. Let's go through each of these separately.

a. The protocol issue

The system needs a communication method that fulfills four main objectives.

1

Firstly, it must be standardized but not over-specified. The communications protocol of many payment rails suffers from over-specification. Over-specification happens when, during the protocol design process, one establishes all the use cases to be supported instead of creating a backward-compatible extensible structure that is able to represent all those use cases through extension. A familiar example in the world of payments is the ISO 20022 payment messages. Everything that goes into the payment needs to have a specific and already specified field in one of the messages. When another type of payment appears, instead of simply extending the message in a backward-compatible way, you need to standardize the new type of payment and fully specify it in the protocol, which can take years to happen.

The need for standardization is apparent. Without it, the many participants of the system cannot communicate with each other. But once the protocol is built to accommodate one specific need with specific fields and flows, it has to be extended by adding more specific fields and re-signifying old fields to evolve. The result is an intricate, inexpugnable web of old grammar with new semantics to decipher, and a big pile of unnecessary data travels in the system. That is, on the off-chance that the new functionalities can be hammered into the old protocol and a brand new infrastructure is not called for to "simplify matters".

That is not to say that a genuinely future-proof protocol is possible. But an effort to identify the primitives from a system and translate them into the communications protocol is possible and was paramount to the success of Pix.

2

Secondly, the protocol must be accessible to all potential participants in the ecosystem. Connecting every account in a given country through one payment system entails connecting all account service providers in the area. In that group, all kinds of institutions, big and small, newcomers and incumbents, must be able to communicate using the same protocol.

For that reason, the newest buzzword piece of tech or a patented technology only a selected few are licensed to use might get in the way of accessibility. Another issue is the cost. A protocol that requires expensive certifications may exclude smaller players. The same goes to a protocol that is so complex to operate, it requires huge teams of specialists to navigate.

3

Thirdly, the protocol must be secure, and security requires simplicity. Saying this about the communications protocol of the system that moves trillions of dollars every quarter may sound too obvious. But what it means and what it takes to ensure that goal often needs to be clarified. In the context of protocol security, simplicity is the key (or the lock, so to speak). Complex protocols are harder to secure because complex interactions are harder to analyze and ensure that no harmful interactions can happen.

4

Finally, the protocol must be efficient. This is where great opportunities lie for building something truly transformative for the lives of every citizen. The protocol bears a great share of the cost of infrastructure operation as a whole. The decisions made at the protocol level impact the cost of processing, memory, disk, bandwidth, and maintenance in general.

The size, frequency, and flows of messages exchanged between participants profoundly impact the overall price of each transaction. A protocol that demands unnecessary data to travel, uses a data-heavy format, or requires hiring proprietary services or a big team to run it is likely unable to serve a system that is supposed to cost micro cents per event and enable its use for any possible need to transfer funds. If it costs more than a loaf of bread to complete a transaction, the system would not be suited to accept payments in a bakery – and the goal is to create a solution for all needs.

b. The trust issue

The trust issue is twofold. From a regulatory standpoint, moving money around requires the guarantee that money will not disappear or multiply by mistake or by malicious design. For financial system regulators, that is an issue of systemic resilience and of currency stability. If a player is able to print digital currency or loses track of where someone's money is located, the value of the national currency or the trust in the financial system may be severely affected. The risk of a systemic failure is at the heart of the Brazilian Central Bank's concerns in regard to payment systems.

The second aspect of trust in this context is that connecting the financial system takes an arrangement between any two account service providers in the land. This requirement unfolds into several issues, from the complexity of business arrangements to the technical arrangements and issues, such as determining the source of truth.

c. The issue of reach

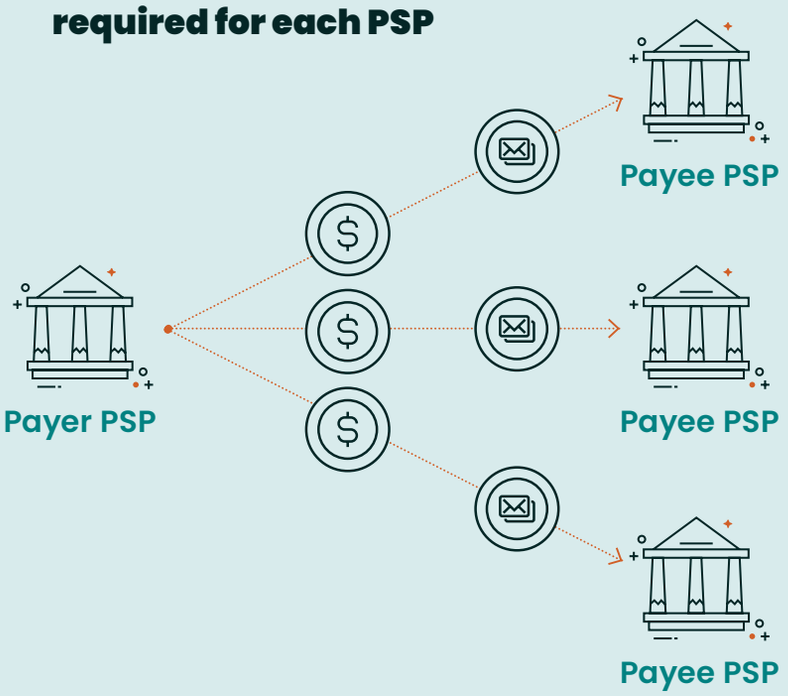
The issue of reach comes from the fact the payment system needs to connect any two accounts, from any two account services providers. Solving this issue is the difference between having a walled garden where only a few member institutions can provide access to the payment service and having an ecosystem where every user knows that whatever economic transaction they are making, they can use the payment service to liquidate the price because everyone is reachable. That is what enables users to leave their houses with only one payment method, because they know they will be able to use it for their every need.

As with the issue of trust mentioned above, the exponential nature of the task of integrating every institution (n) to every other institution (n-1) also makes the issue of reach all the more complex. What might be a daunting feat to bootstrap the ecosystem right out of the gate, may become an even bigger problem as the ecosystem evolves. It may effectively increase the cost of entry for new players to a point where only big, consolidated institutions can effectively join the ecosystem at a competitive price.

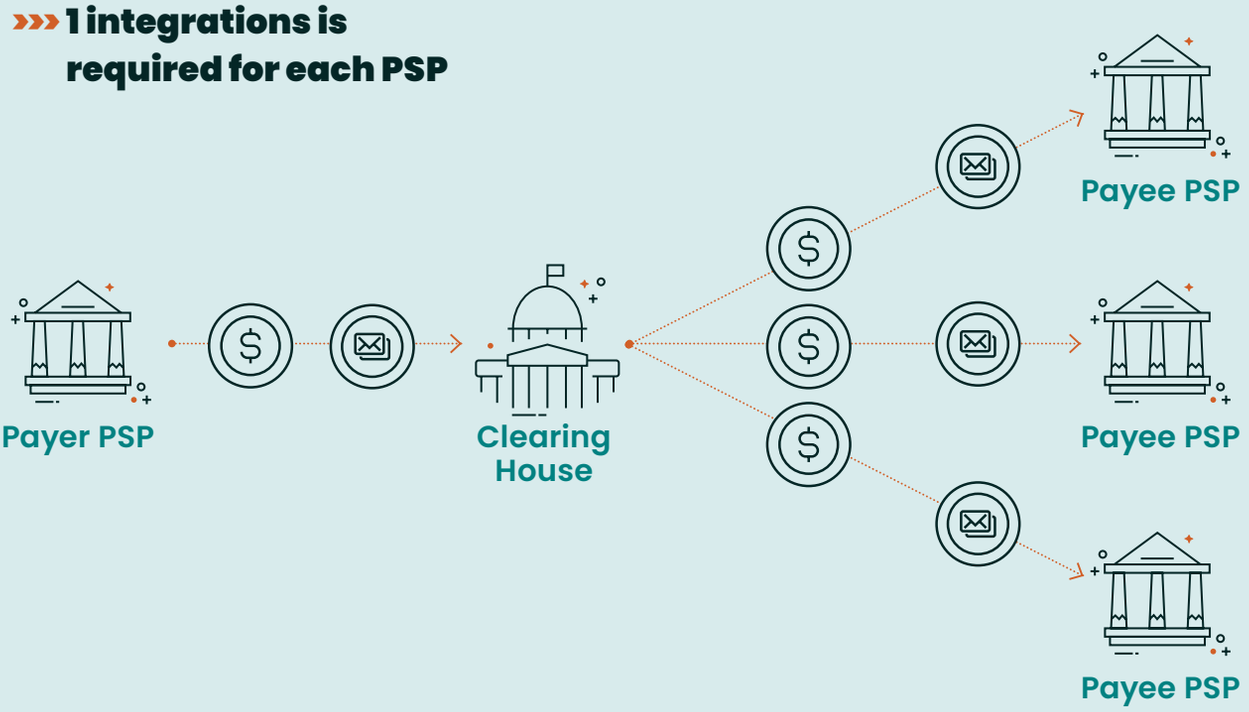
Left unsolved, this issue also gives rise to the emergence of intermediaries empowered by the impracticality of either competing with or operating without them.

4 PSPS IN THE ECOSYSTEM

»» 3 integrations are required for each PSP



»» 1 integrations is required for each PSP



2.3. LESSONS FROM PIX

TO ORCHESTRATE THE THREE ISSUES raised above, the Brazilian Central Bank took an approach that can be summarized in four main propositions:

1st

To create a centralized infrastructure built and run by the BCB itself that is in charge of the clearing and settlement service. This ensures that new members connect to all current and future participants in the ecosystem with a single integration into the centralized infrastructure. That enables reducing the integration cost, allowing greater reach, centralizing the issue of trust, and reducing the need for intermediaries.

2st

To favor open source protocols, such as HTTP and RESTful APIs over proprietary solutions that were traditional in the industry until then, such as the messaging software IBM MQ. This reduces the overall operating cost, as well as the integration cost, which also favors a greater reach.

3st

To create a messaging abstraction that was tailor-made for payments, in a way that enables the ecosystem to evolve at a much faster rate, thus ensuring the evolvability of the ecosystem while also reducing the computational and upfront investment from the infrastructure operator.

4st

To embed in the system design and protocol some of the best practices of distributed systems, such as eventual consistency, idempotency, a unified source of truth, and replication logs, thus creating a symbiosis between security and trust features and the inner works of the system.

These are the main characteristics that make Pix a successful case. In line with that assumption, the few critiques we have about BCB's choices in building Pix are in the areas where BCB deviated from these four north stars or missed the chance to take full advantage of them.

3.

HOW PIX WORKS: ARCHITECTURE AND PARTICIPANTS

3.1. ARCHITECTURE AND PARTICIPANTS

a. Pix infrastructure

THE PIX INFRASTRUCTURE WAS BUILT and is operated by the Brazilian Central Bank, the country's financial markets regulator.
To support the new instant payments system, BCB created two entities:

- **SPI (Instant Payments System)**, an RTGS settlement system that processes transactions;
- **DICT**, a payment alias database that facilitates payment addressing within the system.

Besides these two entities, the Brazilian Central Bank also leverages a broader infrastructure that supports all of its operations, the National Financial System Network (RSFN in Portuguese).

SPI is a settlement chamber that holds settlement accounts from some of the members of the Pix rail. These settlement accounts are called instant payment accounts (IP Account or Conta PI, in Portuguese). The institutions with IP Accounts are named "direct participants" to Pix. Those who choose not to have these accounts or who are excluded from having them are called "indirect participants" and must partner with a direct participant to be able to make and receive Pix transactions.

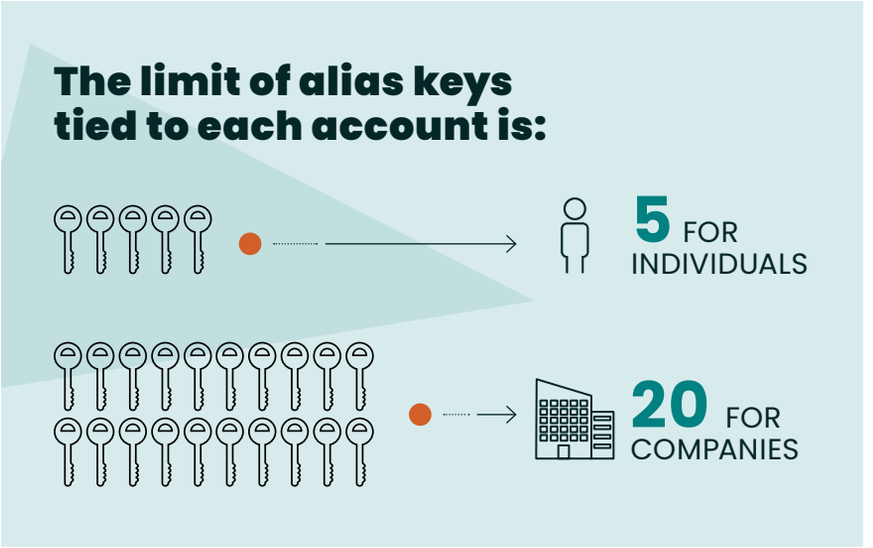
DIRECT PARTICIPANTS =
INSTITUTIONS WITH IP ACCOUNTS

INDIRECT PARTICIPANTS =
WHO CHOOSE NOT TO HAVE THESE ACCOUNTS OR WHO ARE EXCLUDED FROM HAVING THEM

The IP Account is managed through the older RTGS system BCB built called Reserves Transfer System (STR), which runs only on working days and hours. The direct participants must manage the cash flow from their IP Accounts to make sure they don't run into a liquidity problem, especially at night and on weekends. The Brazilian Central Bank provides a limited liquidity credit line for direct participants and allows other players to offer similar services to the participants. The lines of credit, however, are tied to the SELIC infrastructure, which is also limited to working hours of working days. To reduce the cost and the risk of managing the IP Account, BCB later introduced modifications to the regulation to instate a yield to be paid on top of the overnight deposits on the IP Accounts.

DICT is an alias base that enables payees to link a key — their tax ID, phone number, e-mail address, or a random UUID — to a single account so that payers can make payments using just this one piece of information.

Only one account can be linked to each alias key. I.e., users can have only one account linked to their tax ID, primary email, or phone number. However, Payees can have multiple alias keys related to the same account, and Payees can have various keys linked to multiple accounts. Payees can generate a random UUID and embed it in a QR Code — so they don't have to share their tax ID, e-mail address, or phone number with someone they've never met.



Because Payees can have only one account linked to each of their keys, there's a process that institutions must follow when they want to change which account is linked with a user's email or phone number. Payees can also remove the alias on their original institution's interface and link to a new account on a different PSP.

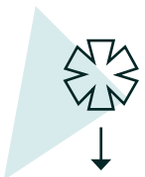
Users do not need to register an alias key at DICT in order to send or receive Pix. However, doing so makes using Pix much more seamless because instead of entering the account number and other personal details for each transaction, the users only have to use alias keys.

The National Financial System Network (RSFN in Portuguese) is the Brazilian Financial System's private network that supports data exchange to all critical financial infrastructures in the country, including SPI and DICT. To connect to RSFN, institutions must hire a direct link to the private network, as well as hold a digital certificate that meets certain criteria.

b. Pix participants

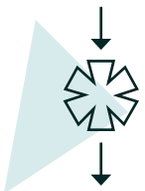
The Pix rail allows five different types of participants.

1 → Direct participants



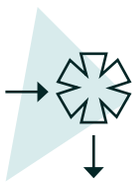
Their role is to provide account services to end-users. They are connected directly to SPI. That means it holds a "PI Account" with the Central Bank, used to settle Pix transactions. It is important to remember that direct participants may use IT service providers to integrate SPI. However, what matters most in being a direct participant is that the entity holds a PI Account and engages in BCB's settlement of transactions.

2 → Indirect participants



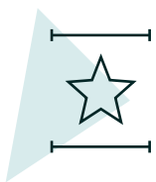
They provide customer service to end users and are indirectly connected to SPI via a direct participant. The direct participant mediates all Pix transactions and has access to unencrypted data from the indirect player transactions.

3 → Settlement service provider



It is a special type of participant on the Pix system that doesn't provide account services to end users. It enables participants who are not direct members themselves to settle transactions through it.

4 → Payment initiation service provider (PISP OR ITP, IN PORTUGUESE)



A PISP does not provide account services. It is a third party that operates between the payer and its account service provider, allowing transactions to happen outside the interface offered by those systems. Some account service providers can ask for special authorization from BCB to operate as a PISP, in addition to the other services they already deliver.

5 → IT Service Provider (PSTI)

PSTIs are integrators that facilitate connections to the broader Financial System Infrastructure (RSFN). These providers offer various levels of solutions (including all the systems to start operating with Pix).

3.2.
A DEEP-DIVE INTO THE KEY FEATURES OF PIX ARCHITECTURE AND PROTOCOL

a. Payment state and error handling

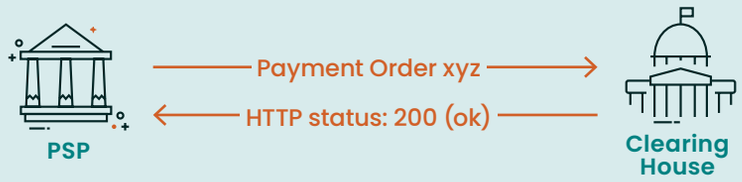
PIX'S CLEARING HOUSE HAS MODELED a payment in an eventually consistent way. This means that, after a period of time (in this case, 10 seconds for payment timeout, plus time for PSPs to query the information), all participants will agree on the final state of the payment.

Even though this can look like an obvious and necessary property for a payment rail, that is not the reality of most payment systems. It is not uncommon for a money movement to get to an inconsistent state (PSPs disagree on the final payment state), which requires manual intervention from specialized professionals manually operating the funds. Another evidence of the necessity of this property is how many rails or PSPs decline identical transactions in origin, destination, and value when they are too close in time (usually same minute), even if they are not the same.

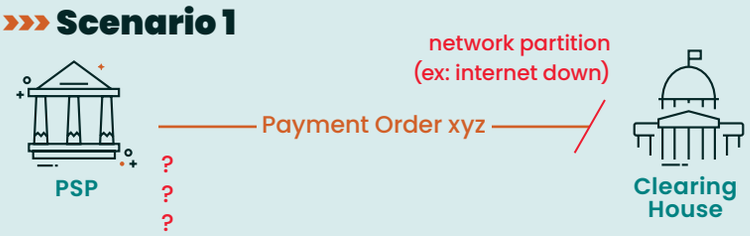
One important enabler of this property in Pix is a Universally Unique Identifier (UUID), an alphanumeric key that identifies the transaction in the rail and serves to query state or retry operations in case of errors.

Another key enabler is the clearing house, established as the source of truth for all payments. Whenever an error happens, the way for the PSP to recover is to retry the payment (which is safe because of the UUID) or to query the clearing house for the UUIDs it received confirmation the clearing house accepted. No manual intervention is necessary whenever an error occurs.

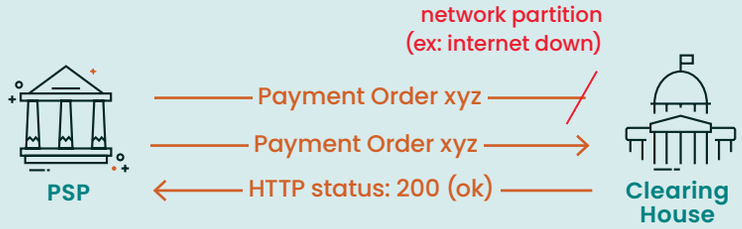
FLOW OF THE HTTP MESSAGING



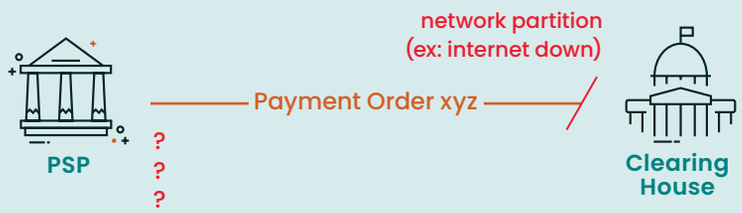
Scenario 1



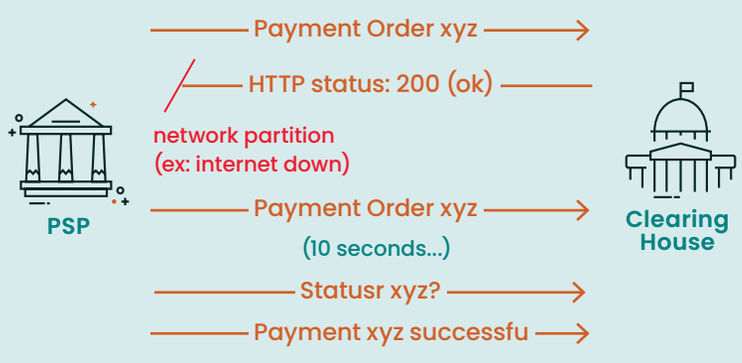
Retries + idempotency + timeouts = eventual consistency



Scenario 2



Retries + idempotency + timeouts = eventual consistency



In the image above, the normal flow of the HTTP messaging shows a payment order being sent from a PSP to the clearing house followed by a successful response — 200 response code. There are two different network partition error scenarios where the PSP does not receive the 200 status code after sending the payment order, explained bellow:

- **1st scenario:** the payment order never reached the clearing house;
- **2nd scenario:** the first message arrived at the destination, but the response was cut off.

If the system was not idempotent, any retry from the PSP could result in a doubled or tripled transaction. However, since all transactions are identified by an end-to-end identifier (e2e ID) unique to that transaction, the PSP can resend the given payment order as many times as it wants. The clearing house will always make sure to not process two transactions with the same e2e ID.

Note that the end-to-end ID should always be a UUID because it avoids collision and guarantees a specific pattern for all e2e IDs. Therefore, the Payer PSPs should be required to check if the payment metadata already contains an e2e ID. If it does not, the Payer PSPs would have to generate the UUID at the start of every money flow. Initially, BCB did not allow for this possibility, but later versions of the technical specification incorporated a similar provision. The adjustment is essential because Payee PSPs can leverage Pix's digital signatures to provide cryptographic proof that a specific QR Code was paid or not.

Regardless of the scenario, the PSP can retry the transaction in the absense of a response. Additionally, the whole payment flow has timeouts for each step and for the transfer of funds to be finalized. Since the settlement chamber is the one in charge of making the actual funds transfer happen, it is the only source of truth about the payment's status. If the funds are exchanged, it means the transfer was successful; if they are not, the

transaction will fail after the timeout period runs out and the payer will be instructed to initiate it again. Thus, even if the communication between the Payer PSP or the Payee PSP and the settlement chamber fails, they can query the settlement chamber as to the status of the transaction after the 10 seconds run out.

b. Payment description and metadata

ONE KEY DISTINCTION BETWEEN PIX and other payment rails is its strict separation of the money movement and the metadata definition. Money movement messaging is completely controlled by the clearing house, but the metadata messaging is flexible and can be defined by the Payee PSP.

This distinction has powerful implications. While in most payment systems every single participant must process and understand fields related to all kinds of transactions — moving in lockstep —, with Pix, the Payee PSP can independently define and then interpret the transaction, enabling new types of payments to be created unilaterally by the Payee PSP.

Unlike the Payer PSP, the Payee PSP is in the perfect position to define what a payment is about (its metadata), since it is the payee who understands which parameters are necessary for each use case. The role of the Payer PSP in this process is to show the payment metadata sent by the Payee PSP to the payer, without needing to process it in any meaningful way.

Another really interesting consequence of this segregation is the friction reduction to create new payment products. Most regulator's concerns fall on the

money's destination, not the specifics of their use cases. Most frauds, money laundering, and other payment restrictions are related to the money movement. Since this is handled in the same way in Pix, a new payment product will always have those capabilities enabled.

c. Account definition

SIMILARLY TO STR, PIX ALSO identifies accounts through information such as bank routing number, bank account number, and account owner tax ID, which allows participants to easily migrate customer transfers from STR to Pix without having the end user take active action for that to happen.

Pix also supports a mechanism to define an account alias, named Pix Key ("chave Pix" in Brazilian Portuguese). It can be:

- A **phone** number;
- An **email** address;
- A **tax ID** (CPF or CNPJ);
- A **social security** number;
- Or a random **UUID**.

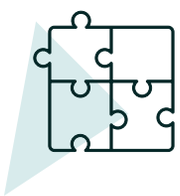
The goal is to facilitate the use of Pix so people can share information that is commonly memorized with other people to make a transaction. In Brazil it is really common to have your tax ID memorized and to broadly share it, contrary to SSN in the US.

Contrary to the UPI model for account aliases that is distributed and is local to the institution, BCB opted to have a centralized alias database, called DICT. This added a nice functionality: being able to provide only the alias and not an alias/PSP combo. In doing so, however, the DICT model also brought four issues that needed to be addressed.

1st issue → **Key scarcity**

Having only the possibility of having three aliases and those needing to be unique on the system, could eliminate possible use cases for Pix. The UUID alias was a good solution for this issue.

2nd issue → **Allowing for change in the account associated to each alias**

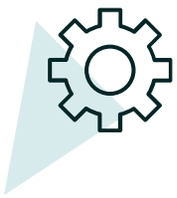


A second issue was creating processes for changing the account an alias points to. Since the change could be for accounts of different PSPs, a process needed to be defined to ensure both PSPs have the same data. That process had to be robust against attacks, such as account takeovers and identity frauds.

3rd issue → **Ensuring consistency of data between DICT and the PSPs**

Because the state of the alias is critical to define where the payment goes, this could not be implemented with a simple daily dump of information being sent to PSPs. This was solved by establishing DICT as the source of truth for alias state and having the change of data on aliases being propagated through events to the PSPs by the use of a write-ahead log.

4th issue → **DICT needs to be working correctly at all times**



This is necessary for a transaction to go through, instead of this requirement being present only for the clearing house. From a distributed system design perspective, the smaller the number of systems required for an operation, the easier it is to maintain that operation working. This is a direct consequence of the centralization of the alias information and, as such, is not solvable even though it is possible to mitigate the risk of the service stop working, such as having the service deployed to multiple physical locations, an active-active approach to high availability and other high availability practices. BCB is very well versed in these practices since it has been operating and maintaining critical country-wide infrastructure services for decades.

d. Extensibility and sub-standardization

AS A PLATFORM, PIX WAS intentionally designed to be extended. Its main extension point is the metadata field on the dynamic QRCode payload. This field specifies what that payment is about and is meta-modeled, meaning that only the way of presenting information is defined and not which information can be added there.

Many Brazilian government organizations have already started to use this metadata field to encode the information they need for their payment processes, starting to substitute other rails such as DARFs (a federal tax-specific payment rail named "Documento de Arrecadação de Receitas Federais" in Brazilian Portuguese). Utility companies are starting to use this field to create utility bill payments, replacing the barcode rail they use today. Many companies are replacing their barcodes for the Boleto (electronic bill payment method used extensively across Brazil) rail by adding the required information to the metadata field. Merchants are starting to include the items bought in this field, so their customers can later check what that payment was about directly from their banking app.

The examples above were developed unilaterally or along their PSP. In other words, the BCB, the clearing house, and other parties did not have to participate in or validate the creation process nor had to develop any additional code for it to work. This indicates that Pix is more extensive than most payment rails; however, there is space for improvement.

It is possible to develop standards on how to interpret specific information in this metadata field, effectively creating sub-standards that interested PSPs can choose to participate in while all the others will still be able to execute the payment without the added functionality. All that without the need to change the underlying rail.

e. Protocols, standards, and interoperability

IT IS NOT FEASIBLE TO build a platform without relying on several protocols or standards. The strategy of reuse is fundamental for the speed and price of creating something new, so it is not a surprise that some of the hardest decisions in designing Pix were choosing a protocol or standard for a specific part of it.

These decisions may seem innocuous, but they have a direct impact on the final price of the platform, cost of integration for the PSPs, possible functionality for the platform, and implementation time. Depending on the choices made, you are choosing who can participate in the ecosystem.

BCB's audacious goal of Pix was to enable all entities regulated by BCB to become a PSP. This includes multi-billion dollar full-blown banks with thousands of software engineers to the smallest credit cooperatives, with all systems outsourced, passing through small and medium banks that have internal systems which are integrated and maintained by external companies.

Another characteristic of Brazil's banking industry is that service provider contracting can take six months or more to happen. Banks tend to be quite conservative and perform strict due diligence to ensure the service provider complies with all relevant regulations while granting the service at the level needed. These characteristics and requirements substantially limited which protocols or standards could be applied in Pix, but they were also essential for the rail's success.

Open protocols and standards play a big role in Pix because they are cheaper than the alternatives available, while being widely used and familiar to most software engineers. Additionally, they are generally

easier to extend for specific use cases. Instead of choosing IBM MQ, licensed by IBM, the BCB opted for using the HTTP protocol, which is free.

Some other choices favored proprietary standards, such as the use of ISO 20022 data formats and the EMVco QRCode format. Even though that is not necessarily the case, both standards introduced additional complexity and limitations to the ecosystem.

The choice of ISO 20022 data format was mainly motivated by the possibility of interoperability with rails that also use the message format. Interoperability is an interesting goal to have but in the case of a payment platform that is far from solved by the data format. Authentication, authorization, connectivity, data requirements, and many other aspects need to be established before the data format can have an impact on interoperability.

The other motivation for ISO was not having to define a message format, which is perfectly valid since it takes a lot of effort to define and maintain a standard. Unfortunately, Pix is substantially different from other payment rails, so the ISO format had to be

Benefits of open protocols and standards in Pix's design

OPERATIONAL COST:
THEY ARE CHEAPER THAN THE ALTERNATIVES AVAILABLE

ADOPTION COST:
THEY ARE WIDELY USED AND FAMILIAR BY MOST SOFTWARE ENGINEERS

EXTENSIBILITY:
THEY ARE GENERALLY EASIER TO EXTEND FOR SPECIFIC USE CASES

adapted for Pix and is now maintained independently from the ISO format.

It was possible to define a much simpler standard than ISO 20022 that is strictly tailored for Pix, which could have reduced costs and implementation time even further.

The choice of EMVco QRCode standard also introduced unnecessary limitations for no apparent gain. Once more, the goal was to achieve interoperability but it failed. Apart from the unclear mapping of some IDs (26 through 51 that are inconsistently and incompatibly used in many different rails across the world) a choice of data format will not enable interoperability.

Moreover, the many restrictions in the EMVco QRCode format introduced additional complexity. One example is the need to encode information like the merchant's name on the QRCode. This does not make sense for Pix because such information must come from DICT. Pix had to add specific rules that PSPs need to follow in case the information on the QRCode diverges from what gets returned from DICT.

Another limitation added is the 99-character limit of a data field in the format. Pix uses Capability URIs to represent more complex payments. Even though 99 characters is sufficient for most use cases, it is too small to use Payload URIs. If there was enough room for Payload URIs, PSPs would be able to have the full payment information directly encoded in the URI, which could be used to avoid a round trip to the Payee PSP or be able to have a stateless and offline approach to generating payment QRCodes.

It is important to note once again that interoperability is a great goal to have but that needs to be one of the main goals for it to work and everything needs to be designed to be interoperable with other systems. If that is not the case, attempts to drive interoperability will mostly bring additional complexity without the benefits.

f. Joining Pix: certification and compatibility

FOR AN INSTITUTION TO BE part of Pix, it must undergo a process filled with certifications and technical validations. The Brazilian Central Bank created a sandbox environment where aspiring Pix participants can implement their internal systems against a test environment, facilitating the implementation process. Once finished, new participants must take an extra step: pass a series of technical tests to make sure the implementation works with the BCB's systems and that payments can be successfully made, received, or initiated. This reduces the risk of having compatibility issues going into production, which could damage the Pix brand.

The Brazilian Central Bank also defined multiple Service Level Agreements regarding API quality (latency and others) that PSPs must comply with. BCB closely monitors this requirement, helps guarantee Pix's excellent levels of availability and reliability.

3.3. LESSONS FROM PIX

AS MENTIONED PREVIOUSLY, ONE OF the most important lessons from Pix's architecture is the pivotal role of a centralized settlement chamber operated by a centralized Payment System Operator — the SPI and the Brazilian Central Bank, respectively. The possibility of having institutions joining the rail as either direct or indirect participants was also critical to reduce the cost of entry for smaller players who can enjoy the advantages of Pix without the need for a full-blown infrastructure. Yet, the value of the payment initiation service provider role in Brazil is still very questionable, given the restrictions imposed by the regulation and the strength of alternative solutions on top of Pix. The role of PISPs and the impacts of the Open Finance agenda on Pix is not, however, the main focus of this paper and should be discussed at a future opportunity.

The first valuable lesson worth replicating is that Pix was intentionally designed to be eventually consistent. This decision permeates the entire infrastructure and APIs, facilitating all error handling in the system. That approach impacts most Pix's key properties, such as 24/7 availability, reliability, and cost-effectiveness.

Eventual consistency was chosen as the most suitable consistency model for Pix, based on the CAP theorem. The theorem states that any distributed data store can provide only two of the following three guarantees:

- **Consistency**
- **Availability**
- **Partition Tolerance.**

For Pix, the possible 10s delay in payment consistency is a small price to pay to have the highest possible levels of Availability and tolerance to network failures (Partition Tolerance).

1st LESSON

Is that Pix was intentionally designed to be eventually consistent.

Another place where we can see the power of this consistency model is on the DICT. In the initial proposal, DICT was supposed to have a two-hour update downtime every day so all participants would be able to synchronize the data. By using a write-ahead log and the change for an eventual consistency model, the DICT can now operate with all functionalities 24/7, without periodically scheduled periods of unavailability.

The second feature that makes Pix the current protagonist of the instant payment disruption is the approach that allows arbitrary metadata to be associated with any given transaction, opening the rail up to extensibility and evolvability.

2st LESSON

Is the approach that allows arbitrary metadata to be associated with any given transaction, opening the rail up to extensibility and evolvability.

It is worth reiterating that security was a central aspect when designing Pix. Besides improving the system's safety, the ample use of digital signatures across the infrastructure made it easier to identify the responsible for adding bad data in the system – be it because of a bug or in consequence of an attack –, helping to solve issues promptly.

4.

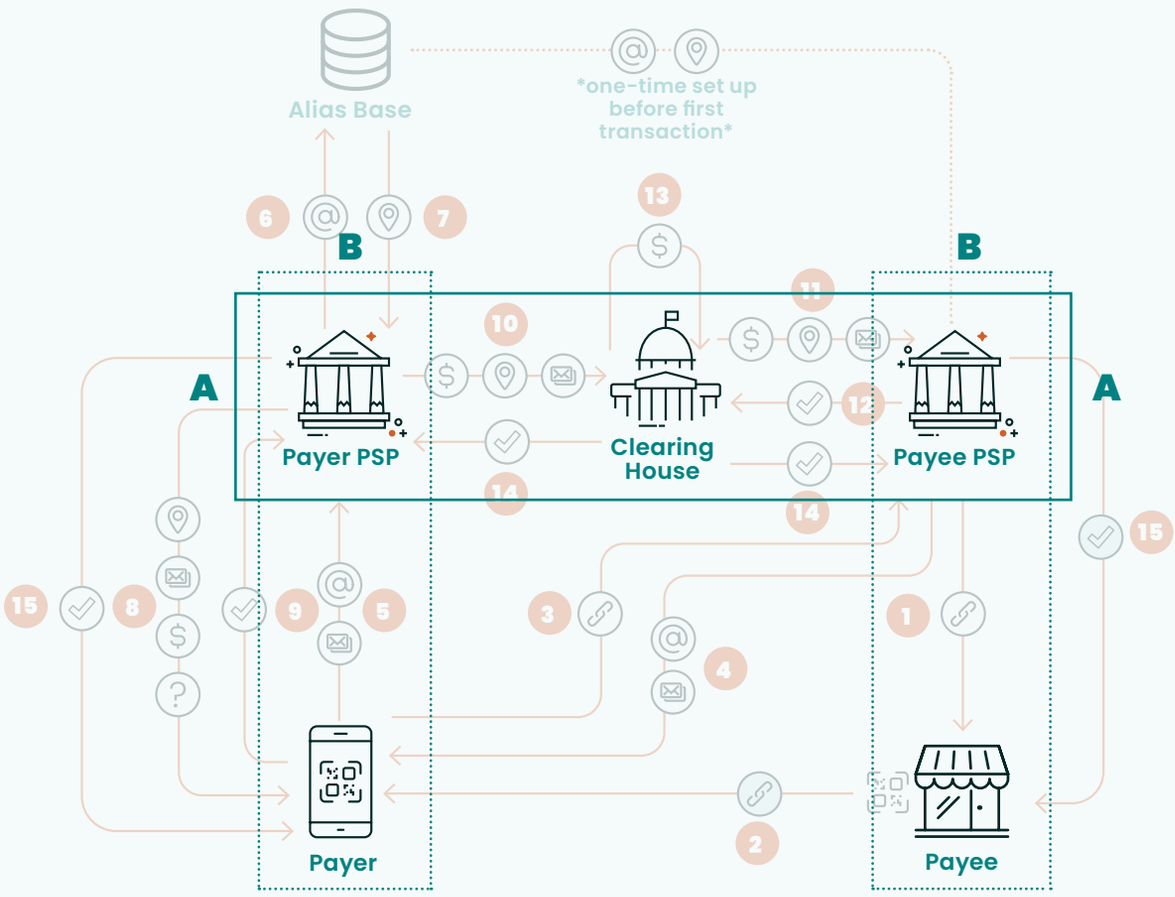
HOW PIX WORKS: PAYMENT FLOW

THE DATA FLOW CONSISTS OF sending the Payer PSP all necessary information to start the money transfer along with other details required by a particular payment method. For a financial transaction to happen, it is mandatory to have the following information:

- **Origin**
- **Amount**
- **Data and time**
- **Authorization from the account holder**

This is true for any kind of electronic payment use case debit and credit cards, vouchers, bill payments, tax payments, payroll, etc. Apart from those, the various use cases mentioned before

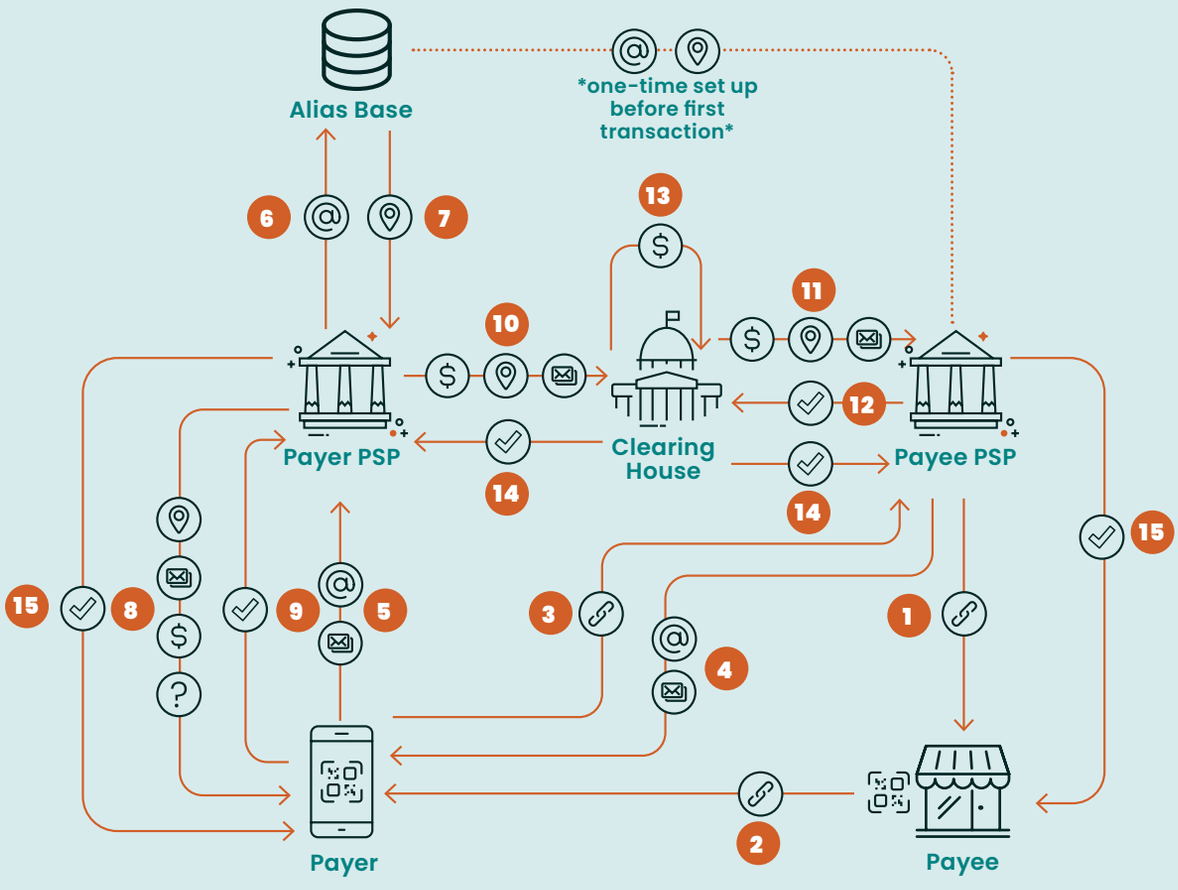
TWO KINDS OF COMMUNICATION



require additional metadata to fulfill the users' needs. For example, food vouchers need to verify if the payee is registered as a restaurant; credit cards have to defer the settlement of transactions. The proper protocol abstraction accounts for both of these kinds of use cases.

The flow of information can vary greatly, but at the end of the day, all payments use cases require mandatory and additional information to reach the Payer PSP. And that information flows through two kinds of channels: (A) the one between the PSPs and the settlement chamber (steps 10 through 14 in the diagram below), and (B) the communication channel between the end-users and the PSPs (steps 1, 5, 8, 9, and 15).

COMPLETE PIX COMMUNICATION FLOW: DYNAMIC QR CODE



COMPLETE PIX COMMUNICATION FLOW: DYNAMIC QR CODE

The diagram above illustrates one possible use of the Pix rail in the case of a Dynamic QR Code. The particularities of this kind of payment initiation, as well as other possible flows, will be discussed in a later section, as will the inner works of the clearing and settlement chamber, called SPI (Instant Payments System, in Portuguese). For now, it is worth going through the flow end to end to understand the whole better.

In the example given, the Payee is a merchant who generated a Dynamic QR Code with the Payee PSP (1) and presented it for the Payer to scan (2). When the Payer selects their Payer PSP app on their device and scans the QR Code, the Payer PSP app decrypts the QR Code image into text. Then, the Payer PSP app accesses the link embedded in the QR Code and uses it to access the Payee PSP´s servers (3). The Payee PSP replies to the call with the Pix Key and any other kind of information needed for the payment (4). The Payee PSP app forwards all the information to the Payer PSP´s servers (5). The Payer PSP then accesses the Pix Key Database (DICT) to look up the routing number associated with the Pix Key (6 and 7).

The Payer PSP then renders all the payment information to the Payer (8), who confirms the information and authorizes the payment (9). After the confirmation, the Payer PSP sends a message to the Settlement Chamber with the amount, the routing information, and any other data the Payer PSP might have added to the payment message(10). The Clearing House forwards the payment message to the Payee PSP using the routing information provided by the Payer PSP (11). If the Payee PSP confirms the account information is correct and the payment can be received (12), the Clearing House settles the transaction by transferring the amount from the Payer PSP´s account to the Payee PSP´s account (13) and notifies both the Payee PSP and the Payer PSP of the success of the transfer (14). Once the payment is confirmed, the Payee PSP notifies the Payee (15), and the Payer PSP notifies the Payer.

4.1. PAYMENT FLOW: COMMUNICATION BETWEEN PSPS AND THE SETTLEMENT CHAMBER

A TYPICAL PAYMENT MONEY FLOW STARTS when the Payer PSP receives the payment request from the Payer. As mentioned previously, all types of payment solutions have that in common. The method through which this communication happens, on the other hand, can vary depending on the use case and will be discussed in length in the next section. For now, the focus should be on the moment the Payer PSP receives the payment request and starts the money flow.

On Pix, the money flow always goes through the clearing and settlement chamber, called SPI. The existence of the Settlement Chamber is what enables the massive reach that Pix enjoys. It also plays a crucial role as the source of truth about the status of any given payment. The Settlement Chamber is, therefore, a fundamental piece of the system that guarantees the eventual consistency of the whole platform and the idempotency of all payments.

The communication between the PSPs and the Settlement Chamber happens through HTTP protocol, RESTful APIs implemented by the Settlement Chamber, and the long polling technique. From an operational

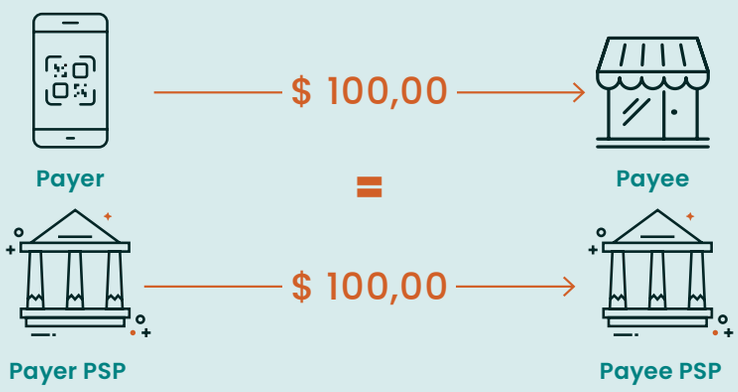
standpoint, this is not the most efficient choice but it avoids the inconvenience of having all PSPs implement and certify APIs on their end. After two years, this approach seems to have paid off since the integration of new members to Pix is relatively agile and the payment flow works seamlessly.

The reason why the Settlement Chamber can function as the single source of truth of payment status is a simple but powerful concept. All PSPs members of the Pix rail must be connected to the SPI, directly or via a partner who, in turn, is connected directly to the SPI. That direct connection means two things:

1. The PSP is integrated to SPI's APIs;
2. And the SPI holds an account in the name of the PSP that is then used to settle the gross transactions in real-time.

If the Payer transfers $ 100,00 to the Payee, the Settlement Chamber transfers $ 100,00 from the Payer PSP's account to the Payee PSP's account. From that moment forward, the payment is definitive and cannot be canceled.

INSTANT GROSS SETTLEMENT



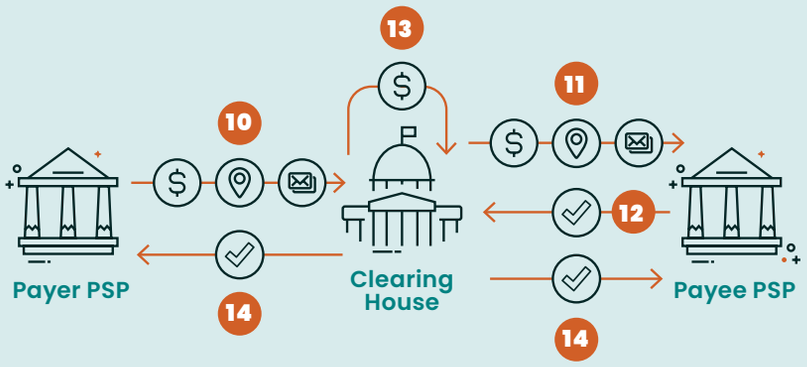
As a result, and since every transaction is identified through a UUID, if for any reason either of the PSP does not receive a payment success confirmation, they can send a request at any time to the settlement chamber and query whether the transfer between the PSPs was successful or not. Since the whole flow has a timeout of 10 seconds, the PSPs know that they can query the status of the payment and get a definitive answer if they have not heard back from the Settlement chamber in 10 seconds. According to the rail regulations, the Payer PSP and the Payee PSP have to communicate the success or failure of every transaction to their clients, which closes the loop of information regarding the payment status.

AT ALL TIMES, BOTH PSPS CAN KNOW WHERE THE MONEY IS, WHICH IS NOT TRUE FOR MANY OTHER TRANSFER OR PAYMENT RAILS

That is a crucial feature for the system as it provides a more secure and trustworthy rail. When someone uses Pix to pay for their groceries, the store knows the payment will either undoubtedly work, and they will instantly see the money in their account, or it will just as surely fail, and the person will need to retry the payment.

The image below shows the communications between the PSPs and the settlement chamber. It is a subset of the complete payment flow depicted above.

COMMUNICATIONS BETWEEN THE PSPS AND THE SETTLEMENT CHAMBER



10 Comes after all payment metadata has been collected and the Payer PSP is ready to send the payment order to the settlement chamber with the amount, destination, and any additional information that might be relevant to the transaction (e.g., reconciliation ID). At this point, the Payer PSP generates an end-to-end ID to guarantee the idempotency of the money transfer.

11 The settlement chamber forwards the payment order to the Payee PSP, as indicated by the Payer PSP. At this stage, the Payee PSP can also check if the payee account is available to receive funds. That is,
if the routing number is correct, if the account exists, is active, and is not subject to any sanctions.

12 Once completed the verification, the Payee PSP informs the settlement chamber if the transfer can be accepted.

13 If the money transfer is accepted, the appropriate funds will be transferred between the Payer PSP IP Account and the Payee PSP IP Account. From that moment forward, the Pix transaction is settled and cannot be undone. The payee can easily refund the payment if they choose to, however, from the Settlement Chamber's point of view, it is processed as a new money transfer in the opposite direction.

14 The settlement chamber informs the success or failure of the transfer to the PSPs.

So far, this payment flow has been working well. However, we believe that a minor adjustment could unlock many opportunities in Pix. Between Steps 11 and 12 — when the Payee PSP verifies if the payment can be accepted, BCB presents a very limited list of valid reasons to reject a transaction. The reason, among other things, could have been a concern that incumbents could use it to degrade the Pix experience, thus damaging its brand. Notwithstanding this is a reasonable concern, we believe that if Payee PSPs could block the transfer for other reasons, new use cases could arise.

There are cases where a Dynamic QR Code can have an expiration date or accept payment only once and therefore prevent a double payment by mistake. That feature, however, could also be built into the money flow if Payee PSPs could refuse payment when detecting a duplicate payment, avoiding errors. Another use case could be the possibility of refusing a payment before the payer digitally signs a contract or accepts the terms of Service (ToS).

4.2. PAYMENT FLOW: COMMUNICATION BETWEEN END-USERS' DEVICES/INTERFACES AND THE PSPS

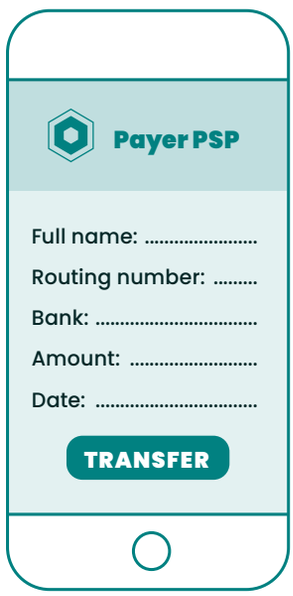
IN THE PIX ECOSYSTEM, THE different kinds of flow of mandatory and additional information toward the Payer PSP are called "payment initiation methods". They are data flows that ensure all required information is delivered to the Payer PSP. The BCB created several types of payment initiation methods and structured a roadmap for future implementations, which are detailed in the following image:

It is important to observe that most payment initiation methods listed above are *payer-initiated* — a significant difference between real-time payment rails and card rails. In the later system, the payment initiates in the merchant's device (the POS machine). That leads to several security issues since all sensitive payment information will be input into a single device. The risk of credit card cloning, of replay attacks on the POS machine, and other frauds are a constant concern regarding card rails. This issue is even more critical in locations where crime and fraud rates are elevated. Moreover, many people are wary of using credit and debit cards for security reasons, curbing the adoption rate of those payment methods in several countries, such as Germany or Argentina.

Apart from the direct debit, the customer-presented QR Code standard, and an eventual API-enabled payment initiation, all other bank-to-bank payment mentioned above begins on the payer's phone. That is a gigantic shift in the payment dynamics and may have implications for reducing skepticism and building trust in the system.

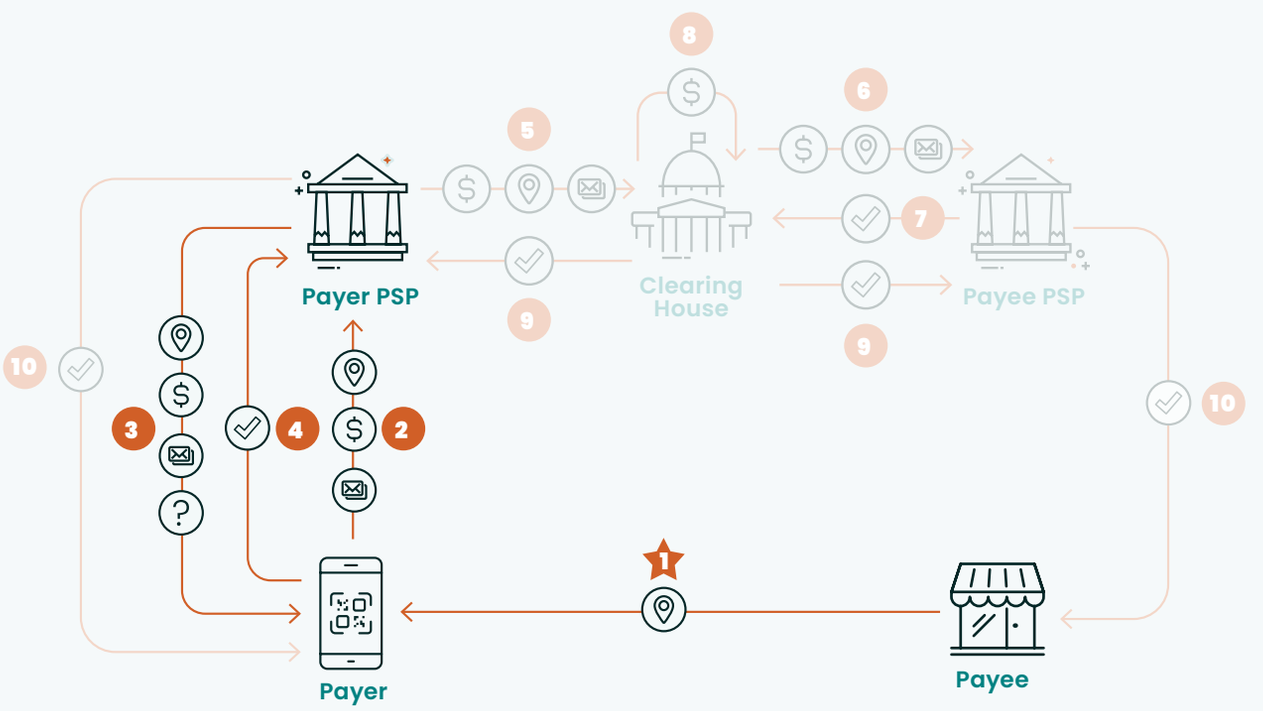
a. Full account information input certification

IN PIX'S CONTEXT, THE FULL account information input has been called "manual input". It consists of the Payer opening the Payer PSP's app and inputting all mandatory transaction information directly into the app. In essence, the user experience is very similar to the traditional rails used all over the world to make account-to-account transfers.



It may seem innocuous to account for a payment initiation method filled with so much friction while more sophisticated alternatives are available. However, to expressly recognize this as a valid form to initiate real-time payments has its virtues. Since the end-user step-by-step is strictly the same, the adoption cost for those customers is reduced to zero. The advantage of such an approach is, therefore, very clear. No matter the age of the user or where they are in the technology adoption lifecycle, everyone can start using the new rail as soon as it's live. That was, in fact, the case with Pix. Payment Service Providers started pushing for the adoption of Pix in a scenario where the cost of a Pix transaction was much lower than what existed before, and the user experience was, at worst, strictly the same as the previous, more costly solutions. Another advantage is that there is always a baseline fallback in case of issues with any other payment initiation method.

PAYMENT FLOW: FULL INFORMATION INPUT



PAYMENT FLOW: FULL INFORMATION INPUT

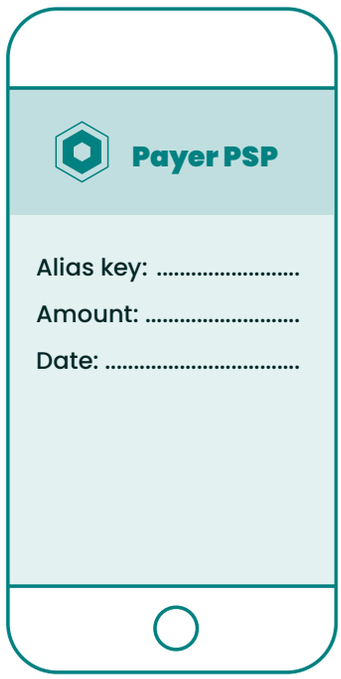
1. The merchant sends the full banking routing details to the payer

2. The payer inputs all the information in their PSP interface, along with the transfer amount and, if needed, a small message.

3. The Payer PSP sends all the information to the and presented it for the Payer to scan (2). When the Payer selects their Payer PSP app on their device and scans the QR Code, the Payer PSP app decrypts the QR Code image into text. Then, the Payer PSP app accesses the link embedded in the QR Code and uses it to access the Payee PSP's servers (3). The Payee PSP replies to the call with the Pix Key and any other kind of information needed for the payment (4). The Payee PSP app forwards all the information to the Payer PSP's servers (5). The Payer PSP then accesses the Pix Key Database (DICT) to look up the routing number associated with the Pix Key (6 and 7).

   The Payer PSP then renders all the payment information to the Payer (8), who confirms the information and authorizes the payment (9). After the confirmation, the Payer PSP sends a message to the Settlement Chamber with the amount, the routing information, and any other data the Payer PSP might have added to the payment message (10). The Clearing House forwards the message to the Payee PSP using the routing information provided by the Payer PSP (11). If the Payee PSP confirms the account information is correct and the payment can be received (12), the Clearing House settles the transaction by transferring the amount from the Payer PSP's account to the Payee PSP's account (13) and notifies both the Payee PSP and the Payer PSP of the success of the transfer (14). Once the payment is confirmed, the Payee PSP notifies the Payee (15), and the Payer PSP notifies the Payer.

b. Account alias

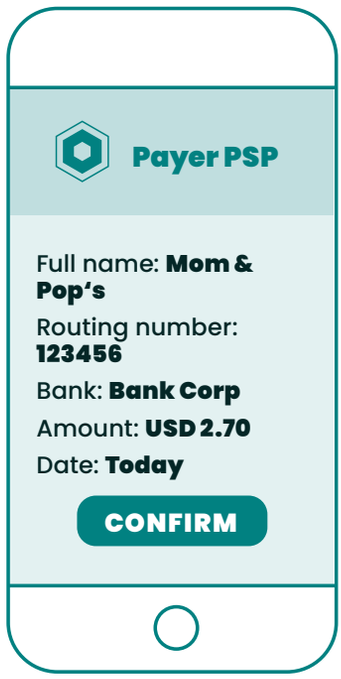


THE ACCOUNT ALIAS IS REFERRED to in Brazil as Pix Keys. These are stored in an alias database called DICT – Transactional Account Information Database. DICT, as mentioned before, was built and is maintained by the Brazilian Central Bank and allows payee users to link the information about a certain account to an alias so that, instead of sending the full routing information to the payer, they can inform just the alias and receive the transfer. The alias can be a telephone number, the payee tax ID (CPF), an e-mail address, or what is referred to as a "random key", which consists of a UUID generated by the Payee PSP and registered as a Pix Key.

The registration of any alias, however, is not a requirement to start sending or receiving funds through Pix. As mentioned above, payees can receive Pix transactions by providing their complete account information, and the payers can pay through any kind of payment initiation method without prior registration.

The Pix Key offers a vital feature to the ecosystem by facilitating the process of inputting mandatory information about the payee. Besides, the payment routing information comes from a secured source of truth, adding an extra layer of security to the transaction. After typing the Pix Key, the payer can double-check the name of the payee retrieved from

the alias base, making sure the money is going to the correct account. As noted previously, the mechanism of ensuring all relevant information comes from a trusted and verified source is present in all Pix payment initiation methods. It is one of the main features responsible for building trust in the system.



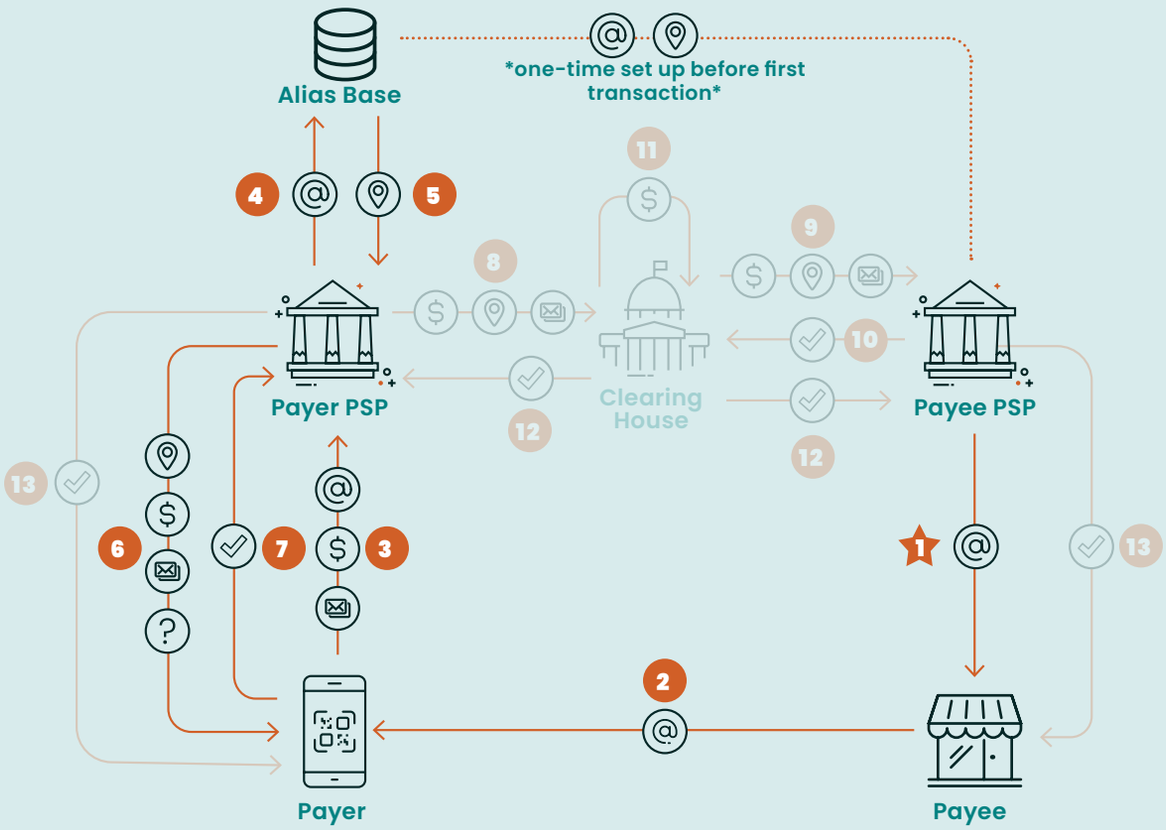
When debating on account aliases, the Brazilian Central Bank had a clear outcome in mind. It was important to the institution that any payer could make a transaction just by knowing the payee's telephone number. To accomplish this goal, creating the alias database was the only solution available.

However, it is worth noting that other options could have been implemented to provide the rail with an alias feature without the need to build a highly centralized database. A model based on a unique identifier of the account coupled with the information about who the Payee PSP is could have been a simpler solution. In such a model, similar to the UPI ID, the alias could follow a format similar to that of an email address, such as "payee-jane-doe@payer-psp". The information to the right would indicate to the settlement chamber to which PSP to route the request. Once the message got to the intended Payee PSP, they could check on their internal registry which account is identified by the "payee-jane-doe" handle.

However, an alias base and the power of the default option on important keys like the tax ID and the phone number triggered a race between PSPs to persuade payees to register these aliases to accounts held by each of them.

PAYMENT FLOW: PIX KEY

1. The Payee PSP registers the Payee's Pix Key
2. The merchant sends the Pix key to the payer
3. The payer inputs the Pix key in their PSP interface, along with the transfer amount and, if needed, a small message.
4. The Payer PSP accesses the alias database and asks for the full routing information associated to the Pix Key
5. The alias database provides the full routing information
6. The Payer PSP sends all the information back to the payer for confirmation
7. The payer confirms the transaction.
8. The Payer PSP starts the money flow



c. QR Codes

QR CODE IS, PERHAPS, PIX'S most noticeable feature. In fact, many of the Brazilian Central Bank's decisions regarding QR Codes made it possible to create secure and powerful tools that enable Pix to work well for P2M use cases instead of just the P2P transfers the first two mechanisms are more suited for. However, through a detailed assessment, we found this decision has been proven suboptimal for BCB's own goals in building Pix. Firstly, it is necessary to explain how QR Codes work in general and how they apply to the Pix scheme.

QR CODES ARE TEXT STRINGS ENCODED AS IMAGES.

When a QR Code reader scans a QR Code printed on a piece of paper, it decodes the image back to the original string. Therefore, they are a protocol designed to share information between two different means. The text that was in the paper is now on the device that scanned the image. In that sense, QR Codes are somewhat similar to protocols like Bluetooth, NFC, and WiFi. Conversely, QR Codes cannot transfer large datasets nor establish a continuous data exchange.

They also do not need to create a programmatic connection with the source of the original data. In fact, the data source does not need to be electronic; it can be a piece of paper. It is a protocol for the passive exposure of information for extraction by a different device. All of these aspects make QR Codes very powerful in the payment's ecosystem .

Additionally, there is no need to worry about the security of end-user devices, and the entire process can be done by using a smartphone camera.

The limit of data that is possible to encode as a QR Code is an issue that deserves attention. Since they are a special way of encoding text, the more text it is encoded, the bigger the code will be.

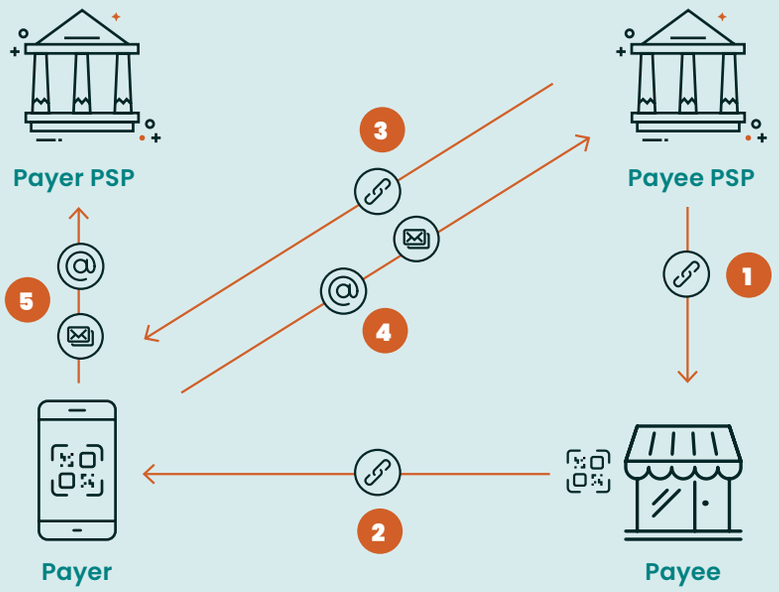
Take both QR Codes as an example. The one on the left, is a title of a beloved poem written by John Donne. On the right side, the entire poem is encoded as an image. It is possible to observe that the additional characters make the code much bigger and harder to read with a medium-quality camera than the QR Code on the left.

Depending on the amount of information a specific payment use case requires, the limitations of the protocol could considerably impact the system's functionality. Besides, such limited data capacity could make it difficult to incorporate any security mechanism to guarantee the integrity of the data, such as digital signatures. Attacks commonly involve pasting fraudulent QR Codes with the wrong payment routing information on top of the original one so that the payer makes the transaction to the attacker's account instead of the intended recipient.

Both problems can be solved with a simple solution: instead of embedding the payment metadata in the QR Code itself, a URI must be used in its place. By doing so, the payer will be sent to an environment containing all the information needed.

This is how it works in the context of payments:

DYNAMIC QR CODE IN THE PIX RAIL



1. The Payee PSP generates a URI containing a domain they own and a UUID. The presence of a UUID adds a security layer by making it virtually impossible for anyone to guess the URI, shielding it from attacks. This type of URI is commonly known as "capability URIs". After generating the URI, the Payee PSP creates a Pix QR Code and sends it to the payee.

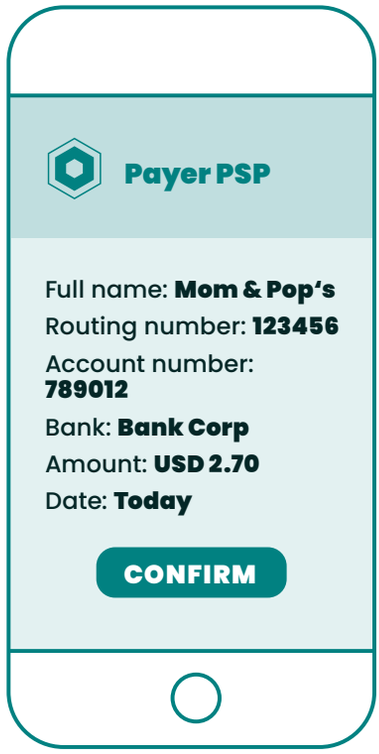
2. The payee presents the QR Code to the payer, who scans it with their phone using their Payer PSP app.

3. The Payer PSP app accesses the Payee PSP URI. This communication is secured by HTTPS and requires a signed response from the Payee PSP to be completed. It is worth mentioning that the signature must use a previously registered certificate on a database controlled by the Payment System Operator (BCB, in the Pix rail).

4. Then, the API call returns all data pertaining to the transaction: account number, payee identification, and other information that the payee may find helpful to present to the payer or to help the process of payment reconciliation.

5. The Payer PSP's app on the payer's device sends the routing and additional information to the Payee PSP's servers to initiate the money flow.

This mechanism defines a Dynamic QR Code in the Pix rail. It is dynamic because even if the QR Code itself does not change (it has the same URL), the data the Payee PSP returns to the Payer PSP — as shown in step 4 — can be renewed several times. That enables a merchant to print and display one QR Code in front of a cashier and update the payment information to show the amount due by each customer.



d. Static QR Codes versus Dynamic QR Codes

STATIC QR CODES ARE THE counterpart of Dynamic Codes. They are called static because they do not contain a link but rather the information directly; that means the amount of data inserted into the image is far more limited. However, similarly to the Dynamic type, Static

QR Codes also have a mechanism to ensure the integrity of the information about the payee and the routing information with a slight difference. Instead of adding the routing information in plain text, the protocol determines that the Static QR Codes must have a Pix Key so the Payer PSP can obtain the routing information in a trusted source, the Alias Base (DICT).

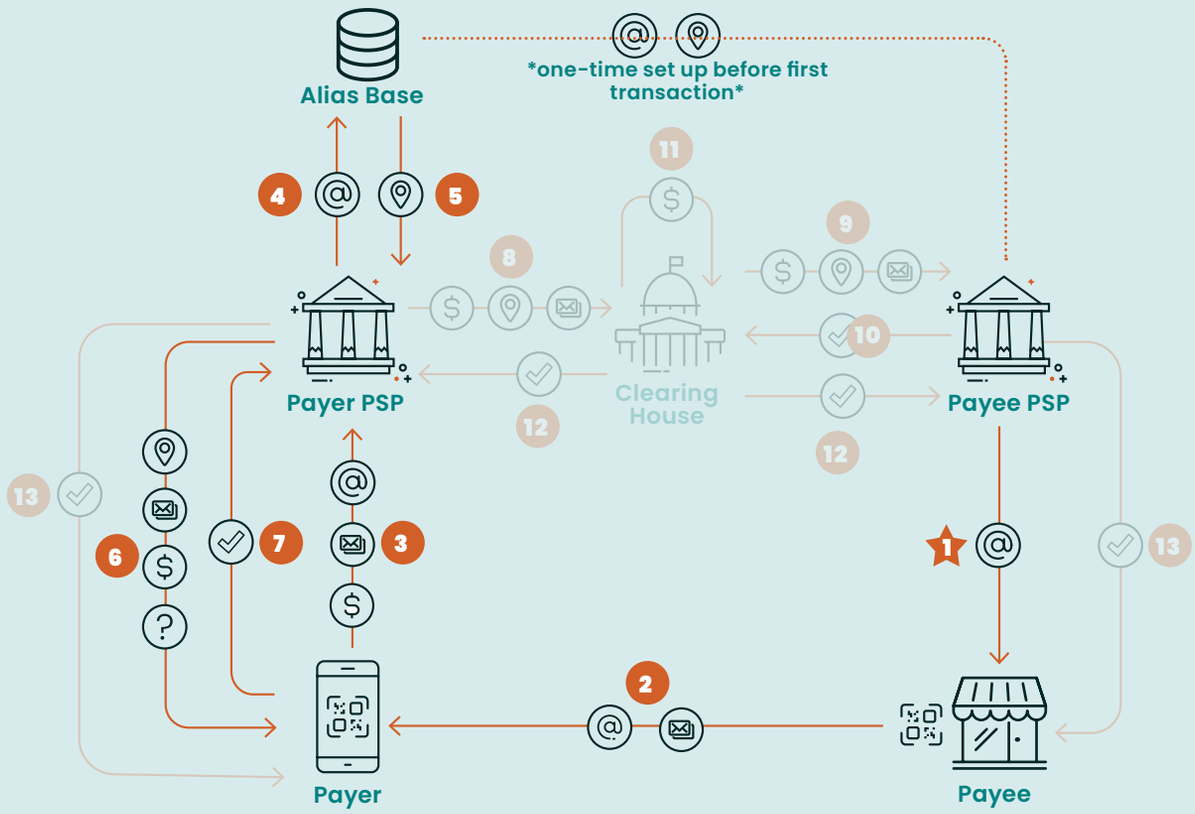
{
"pix_key_type": "tax_id",
"pix_key": "99999999999",
"amount": 2.7,
"identifier": "mp-10-06-2022-00050"
}

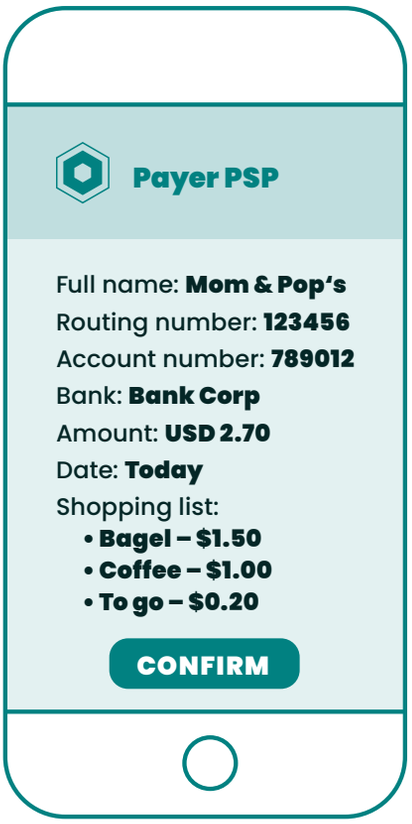
Static QR Codes also have some range of flexibility and functionality. Pix's technical specifications state that if the QR Code's "amount" field is blank, the Payer PSPs must render a field for the payer to fill with the total due. That is a simple but effective feature that allows some flexibility in QR Codes' payments. In Brazil, it is being largely used by street vendors and cab drivers, who benefit from the convenience of QR Codes without needing a fancy sales system.

Pix documentation also prescribes an optional field on Static QR Codes where payees can add an identifier, facilitating the reconciliation of payments. However, the system presents challenges; it identifies the QR Code, not each payment individually. Nevertheless, it has been proven good enough for several use cases.

PAYMENT FLOW: STATIC QR CODE

1. The Payee PSP registers the Payee's Pix Key. Either the Payee PSP, a third party, or the Payee themselves generates a Static QR Code, containing optional fields for an identifyer and a message to the Payer.
2. The Payer scans the QR Code using the Payer PSP app. If the QR Code did not contain a payment amount, the Payer inputs it.
3. The Payer PSP app sends the Pix key, the optional fields, and the amount to the Payer PSP server.
4. The Payer PSP accesses the alias database and asks for the full routing information associated to the Pix Key.
5. The alias database provides the full routing information.
6. The Payer PSP sends all the information back to the payer for confirmation.
7. The payer confirms the transaction.
8. The Payer PSP starts the money flow.

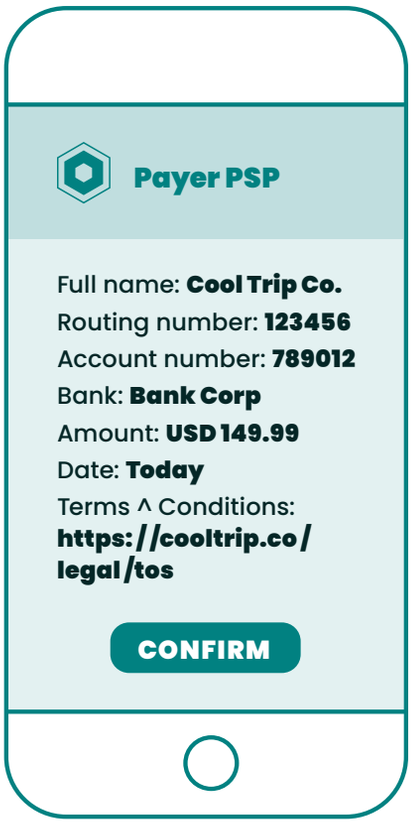




Another benefit of Static QR Codes is the level of autonomy it gives payees regarding their PSPs. To implement card payments, merchants must contact a bank and firm a deal, which can be rather expensive. Then, they have to buy or rent a specific hardware and follow the operation rules established by the bank. Static QR Codes empower merchants and other payees to start receiving and managing their pay-ins independently from their PSPs. Since virtually all PSPs in Brazil must accept Pix payments and register Pix Keys for their customers, any payee can print a Static QR Code to begin to accept Pix payments seamlessly. Since the QR Code standard is widely available on the Brazilian Central Bank's website, anyone can generate Pix QR Codes through free softwares.

On the other hand, Dynamic QR Codes include interesting additional properties by virtue of storing the information directly in the Payee PSP's servers. For instance, Payee PSPs can guarantee the same bill will never be charged twice by returning a 410 HTTP status code ("gone") if the Payer PSP calls the URI in the QR Code after the bill is paid. Payee PSPs can also return, along with the payment information, an end-to-end ID that is then transmitted through the whole payment flow. So, instead of being generated by the Payer PSP, the Payee PSP sends the e2e ID along with the other payment metadata through the Payer, then the Payer PSP, then the Settlement Chamber, and then back to the Payee PSP. That allows for a much more accurate reconciliation of payments.

Another pivotal property of Dynamic QR Codes is that they can potentially transmit any kind or amount of data since the QR Code image itself contains nothing but an address where to get the information the Payer is after. So the Pix documentation can easily add features to the Dynamic QR Codes. One of such features was the creation of specific rules to generate and read QR Codes with the due date, information about eventual late fees, and whether or not overdue payment may be received.



Moreover, the Brazilian Central Bank developed a special field to receive arbitrary information. It's a field type array where Payee PSPs can create extra fields following the overall Pix field syntax. Because the syntax is standardized, Payer PSPs can correctly render the arbitrary additional fields in the payment confirmation screen without needing a revised Pix specification. This strategy of specifying how to create fields instead of developing an exhaustive list of possible fields opens Pix for innovation, evolvability, and extensibility.

Even though the Brazilian Central Bank decided not to allow these additional fields to be returned to the Payer to fill out any information needed, the capability of rendering arbitrary information to payers that are not necessarily their clients is groundbreaking for Payee PSPs. They can find other ways of delivering value to payees by exploring this new communication channel. It is now possible to send the payee a link with the terms and conditions of a service they are paying.

Another path to be explored with the flexibility of Dynamic QR Codes is the development of over-the-top products such as point-of-sale credit, loyalty programs, as well as other partnerships between Payer PSPs and Payee PSPs, without the need to create a new communication channel, with another integration to develop and maintain.

- The possibilities are truly endless. All because of two key features:

- A URI that contains an address where all the information can be found;

And a protocol describing how to create additional fields in a way that any Payee PSP can return arbitrary information that any Payer PSP can parse and render to the payer, no additional integration needed.

It is important knowing that QR Codes should be understood as mere means of communication along the payment flow. What is truly important is that the URI gets to the Payer PSP. If that happens by the payer's device scanning a QR Code or any other way should not be relevant. The same result could be reached with a connection via Bluetooth, NFC, API, or even through a Payee PSP-initiated flow with the Settlement Chamber. They should all work in the exactly same way.

e. The problem with the EMVCo standard

THE BRAZILIAN CENTRAL BANK DECIDED to implement the EMVCo Merchant-Presented QR Code standard as mandatory for all QR Codes payments-related, including those in the context of Pix. The reasoning behind this decision was the ease of implementing a standard that was already

in effect across several countries, the concern about the emergence of several QR Code standards for each payment solution and the international interoperability. Although the reasons might be understandable, we believe they do not justify the use of EMV Co.

Firstly, EMVCo is a form-like QR Code standard with mandatory and optional fields that then have to be mapped out to match the needs of each particular payment system. Thus, although the standard exists, the effort to unravel the meaning of each field still burdens the regulators and the institutions that need to implement the extended standard.

Secondly, the EMVCo standard was created to encompass a multitude of specific payment use cases, overspecifying some fields, including the mandatory ones. That means the regulator in charge of setting the standard must make workarounds to avoid pieces of the original standard that do not fit perfectly with the payments system that is being developed. At the same time, the prolific standard limits the size of other relevant fields to accommodate unnecessary ones. The result is an inefficient standard that has too much and too little data at the same time.

Thirdly, no EMVCo QR Code standard implementations are alike, so international interoperability is not possible without a translation layer. That means field 26 in the EMVCo implementation in Singapore is drastically different from what it means in India, which is different from the one in Brazil. In other words, if a Brazilian PSP scans an EMVCo QR Code from Singapore, it will not be able to parse the information correctly.

Finally, the fact the EMVCo standard can support several payment options in one single QR Code does not mean merchants will be able to display one single QR Code on their counter. After all, the EMVCo standard is just a form template. In order to assemble multiple payment solutions in one QR Code (e.g., Pix, Mastercard, or PayPal), there must be an intermediary

generating the multi-rail QR Codes. Furthermore, it would be possible to do that even in the lack of an overarching standard, provided there was a clear need in the market to do so.

On the other hand, a standard tailor-made for Pix would have taken less time to craft and could have been much more efficient and flexible. Below is the table with the Pix Static QR Code fields and the corresponding EMVCo fields.

ID	Nome BR Code	Tam	Valor			
00	Payload Format Indicator	**02**	**01**			
26	Merchant Account Informations[22]	**58**	**ID**	**Nome**	**Tam**	**Valor**
			00	GUI	**14**	br.gov.bcb.pix
			01	chave	**36**	123e4567-e12b-12d1-a456-426655440000
52	Merchant Category Code	**04**	**0000** (não unformado)			
53	Transaction Currency	**03**	**986** (R$)			
58	Country Code	**02**	**BR**			
59	Merchant Name	**13**	**Fulano de Tal**			
60	Merchant City	**08**	**BRASILIA**			
62	Additional Data Field Template	**07**	**ID**	**Nome**	**Tam**	**Valor**
			05	**txid**	**03**	***
63	CRC16[23]	**04**	0x**1D3D** – incluindo "6304" (ID 63 e tamanho 04)			

00020126580014br.gov.bcb.pix0136123e4567-e12b-12d1-a456-4266554400005204000053039865802BR5913FulanodeTal6008BRASILIA62070503***63041D3D

Note that the fields merchant category code, merchant name, and merchant city are useless for the Pix use case since all information comes from a trusted source, and not the QR Code itself (e.g., the Alias Base or the Payee PSP). In Pix Static QR Code's documentation, there are only four pieces of information relevant to the payment:

- The Pix Key;
- The BRL amount;
- An additional information field;
- A transaction ID for reconciliation purposes.

The superfluous mandatory fields and the restrictions from the EMVCo standard also limit the amount of data that can be stored for those fields that are functionality-defining for Pix. If BCB were to create a standard based on URIs instead of the EMVCo, the Pix Static QR Code could look like this:

```
https://pay-pix/pix-key/BRL/amount/
additional-information-field/transaction-id
```

This standard uses the HTTPS URI scheme for a reason: in case the Payer scans the QR Code with their phone camera instead of their payment app, they could be redirected to a page hosted by the Brazilian Central Bank where they could find instructions on how to scan the QR Code correctly. However, the scheme could also be something new, such as "pix-bcb" or "pay-pix".

The relevant part of adopting URIs is the fact it is a simple, flexible, well-known communication URI scheme that has survived the test of time and mass implementation. The specifics of how to use the standard — e.g., if the Pix Key should be placed before

or after the amount or if the protocol should be HTTPs or anything else — are far less relevant to the outcome we expect with the use of URIs in this context and can be adapted to the proper context of each payment system.

Here is an example of the application of such standard:

https://pay-pix/0136123e4567-e12b-12d1-a456-42665544000/BRL/100/mom-and-pops-cookie/99999999999

As to the Dynamic QR Codes, their content should be a URI that can be used to access all payment information directly from the Payee PSP servers. That means these QR Codes can communicate more relevant information from a trusted source, which significantly amplifies the possibilities of applications. Besides, Dynamic QR Codes allow Payee PSPs to update the information as convenient for each use case.

https://payee-psp-domain/sub-domain/uuid

A Dynamic QR Code standard should not be much more different than the Static QR Code proposed above:

The application of HTTPS URI scheme is also valid in this case. The relevant part is using a registered Payee PSP domain and a UUID to complete the URI. Both measures increase the security of Dynamic QR Codes.

Payee PSPs should register their domains with the Payment System Operator so Payer PSPs can validate if the URI is related to a participant PSP. Also, the Dynamic QR Code becomes a capability URL by using a UUID as the identification key of the URI. That feature protects the information the Payee PSP returns to the Payer PSP from enumeration attacks since it is virtually impossible to guess any valid URI.

https://the-bank/pay-pix/418a34b8-4e5a-11ed-bdc3-0242ac120002

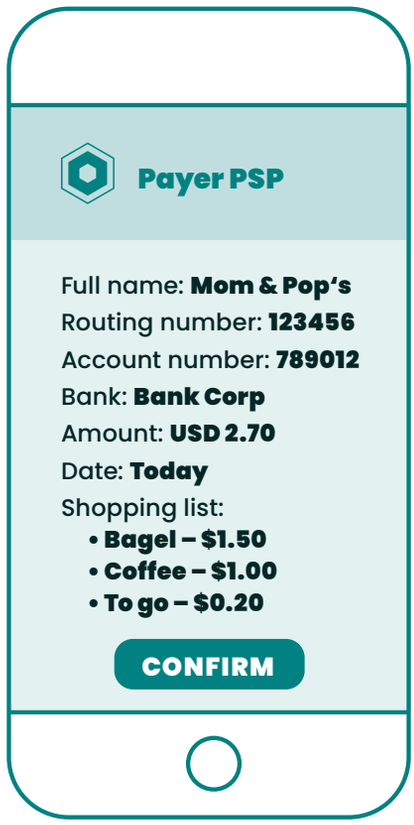
Because Dynamic QR Codes contain no information about the payment itself, an additional standardization is required: a return message from the Payee PSP with all payment information.

As mentioned before, the mandatory information for all kinds of payments are:

- Routing information (account, Payee PSP, Payee identification)
- Amount
- Date

However, there are extra fields that may be relevant for each type of payment. For instance, while paying the electricity bill, it may be relevant for the Payee to link a QR Code to an internal ID for the house or to send the monthly electricity consumption to the Payer. A loyalty program may want to limit the use of specific accounts so that they can be used exclusively at affiliated establishments by arranging that a passcode

should be sent on the related QR Codes. When paying for taxes and other state fees, the Payer might need to fill out a form with additional information to guarantee the money will be routed to the correct agency.



Even if it were possible to list all existing payment use cases and the extra fields they may require from the Payments System, the result would be a convoluted, over-specified, over-engineered, and dated protocol. It would not take long until a new use case is created, and the Payment System protocol would have to be changed to support it.

A better approach is to specify the schema of additional fields in the communication between Payee PSP and Payer PSP and how the Payer PSP renders the information to the Payer. In the context of Pix, the Brazilian Central Bank created a "free field" enabling Payee PSPs to add as many fields as they may require. The type of this field is an array and can therefore contain multiple other fields. As long as the fields follow the same schema as the other fields, Payer PSPs should have no problem parsing the additional information, even if they do not know what the fields mean.

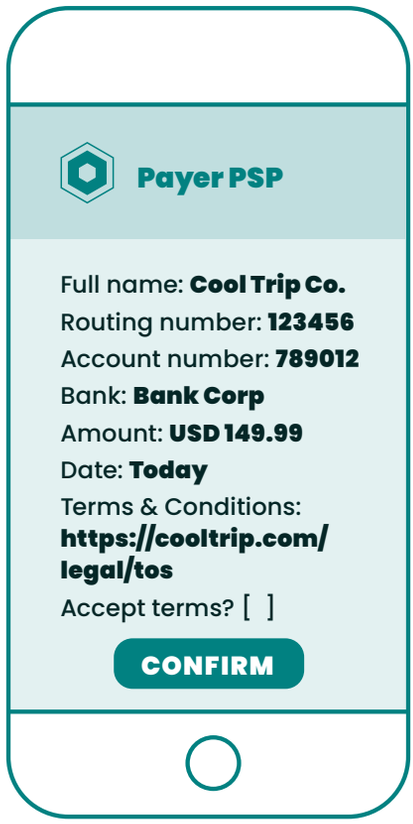
To live up to its full potential, our recommend that the additional information field of Dynamic QR Codes should follow this schema:

```
{
'field': type,
'name': string,
'value': string,
'visible': boolean
}
```

It is important that the fields created can accept multiple types, as the use cases may have different needs. Apart from that, there are two critical nuances in this proposal. Although the additional field exists as an array Pix's documentation, and they can receive multiple value types, they do not support the following functionality.

The first is giving the Payee PSP an option to ask the Payer PSP to hide the field from the Payer. Recall that all mandatory and additional information the Payee PSP sends to the Payer PSP can be rendered to the Payer for confirmation before the money flow actually begins. It is an extra security layer to ensure the Payer knows where and how much money they are sending and confirms it is indeed the intended recipient and amount. The Payer does not have to see all the information exchanged between Payee PSP and Payer PSP. For instance, Payee PSPs may want to send Payer PSPs a code related to a loyalty program or other feature built on top of the Payment System for their business partners.

Thus, the first nuance is to allow for hidden fields traveling with the payment information. That wouldn't be the only way for Payee PSPs to communicate with Payer PSPs without polluting the payment confirmation screen. Since all the communications between Payee PSP and Payer PSP are through HTTP protocols and RESTful APIs, Payee PSPs could (as they can in the Pix rail) send hidden tags or ids in the header of the HTTP messages. We believe, however, that embedding the functionality into the protocol is a preferable choice to PSPs having to rely on workarounds such as this one.

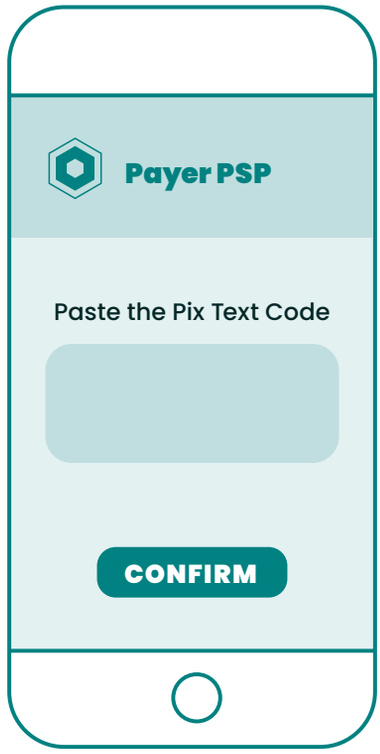


The second nuance of the proposal above is that the protocol should stipulate that, if the 'value' field of the additional field is empty, the Payer PSP should interpret that as an input field for the Payer to fill out. There are multiple use cases where the Payee requires from the Payer additional information to facilitate reconciliation or other post-payment processes – such as delivery of goods. The possibility of having the Payer filling out information to be later delivered to the Payee opens up new avenues of opportunity for innovation. If this functionality is coupled with the ability of the Payee PSP to create a curated list of rules to reject payments, the possibilities are even more promising. The Payee PSP could reject payments, for example, if the appropriate fields are not filled out or do not meet certain conditions.

f. The limits to QR Code application

ALTHOUGH QR CODE PAYMENTS ARE powerful tools, they have a significant limitation: users cannot scan their own screens, restricting the use of QR Codes in mobile commerce.

Going back to the basic primitives of payment methods, the core of any payment initiation is communicating the payment information to the Payer PSP. To address this, the Brazilian Central Bank instructed all PSPs to create a section on their app where users could paste the plain text content of the QR Code. That way, payers can copy the "text code" at the checkout, manually paste it on their Payer PSP app, confirm the payment information, and go back — also manually — to the merchant's website or app.



In this flow, the Payer does by hand what the Payer PSP app can do by scanning the QR Code and parsing its image into text. That is far from being an ideal user experience. However, the fact is that this small change in Pix's rules enabled its use on mobile ecommerces, which have been growing exponentially since the launch of the real-time payment system in Brazil.

There are several alternatives Payment System Operators can consider in order to optimize the checkout experience on mobile commerce. One of

them is the use of payment links for bank-to-bank transfers. However, the Brazilian Central Bank decided against creating a mandatory standard for payment links, opting for a more straightforward workaround. Before diving into the Pix solution and the payment link alternative, it is worth explaining the reason behind the BCB's decision. A parallel with the card industry may help clarify the matter.

As mentioned before, in credit card rails the payment flow starts necessarily with the merchant through the acquirer. Thus, on m-commerce, the acquirer asks the payer for their card information and sends the payment request to the card issuer through the network's communication system. On bank-to-bank payments, however, the transaction usually initiates with the payer, which requires the existence of a protocol so the payment information can travel from the merchant's website to the Payer PSP.

The goal of the payment link alternative is to create an app-to-app experience where the payer goes from the mobile commerce website to their payment app with one click to then confirm the payment information — just as they would after scanning a QR Code. That solution places the onus on the Payer PSP and the Payee PSP to make the payment information travel from one to the other.

The Brazilian Central Bank studied the possibility of adding such functionality on Pix but ultimately decided against it. One of the proposals discussed the development of a prefix for Pix Links, such as *pix.bcb.gov.br/pay*, so that all PSPs could register their apps with smartphone operating systems to open links with the *pix.bcb.gov.br/pay* prefix. This approach presented two problems:

- **1st problem:** any app – not only from the Pix-registered PSPs – could register to open the links;
- **2nd problem:** the definition of the default app to open the links would vary depending on the smartphone's operating system and would not

necessarily be compatible with the Payer user's best interest and the fundamental principles of Pix, especially related to increased competition.

However, there is a better alternative to improve the user experience on m-commerces payments: having a database of registered domains that can be used to open each participating Payer PSP app on both Android and iOS devices. The Payee PSP, then, could present the list of Payer PSPs participating on Pix. After selecting their preferred app, the user would be redirected accordingly to confirm the payment and return to the original screen. The Payees could also store the information of the Payer PSP used in the last payment so that the Payer could benefit from a default option that is convenient to them from their second payment onwards. In comparison with the card rails, where merchants can maintain a "card on file", here they could store a "bank on file".

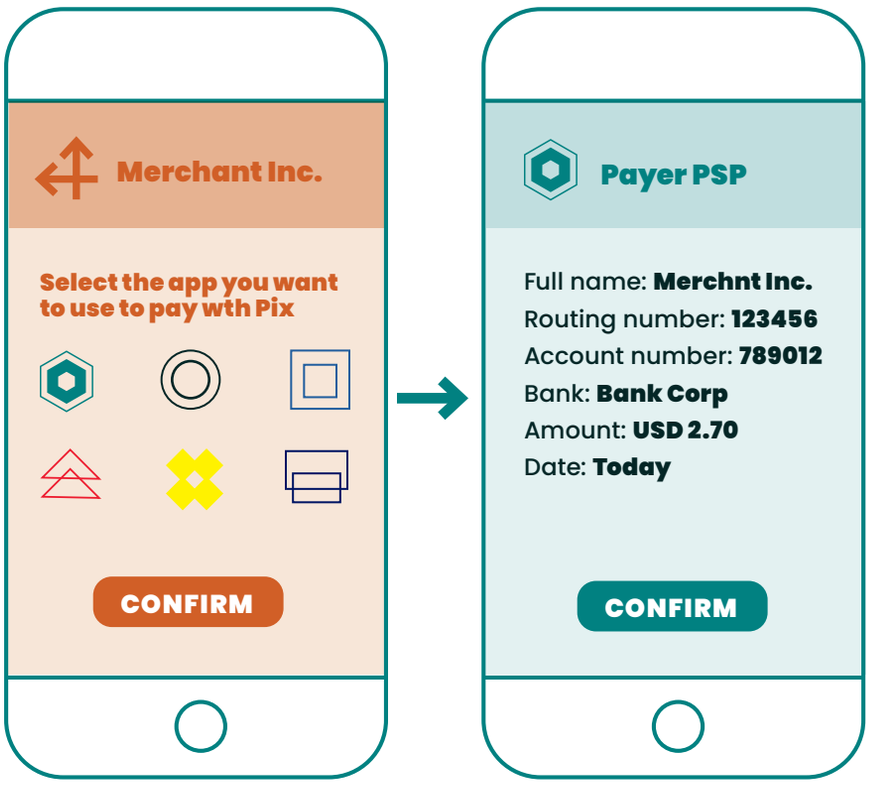
The Brazilian Central Bank also entertained this option but decided not to implement it because the private companies would be in a good position to do it themselves.

Note that the experience the Payer has in this context is very similar to that of the QR Code payment. The process of selecting their Payer PSP (browsing on their phone or on the merchant's website), confirming the payment on the Payer PSP interface, and going back to the context of the purchase is present in both flows.

This flow is similar to the one supported by Open Finance Payment Initiation Service Providers. However, while the Open Finance solution requires one-to-one back-end integrations, the payment link communications can be implemented on top of the app-to-app communication protocols already existing on Android and iOS (universal links/app links). Therefore, the solution would demand solely one integration with the registered links database so that each PSP can register their universal link/app link address and look up those of the other PSPs.

In terms of the front-end adaptation to support the payment universal link/app link, it would also not be very onerous. As mentioned, the payment confirmation screens would be exactly like the ones of the QR Code flow. The only additional effort this solution would require is processing the universal link itself in order to trigger the payment confirmation screen and then redirect the payer back to the merchant's interface. See below one example of how the payment link standard could be implemented:

www.payer-psp-domain/standardized-path
/qr-code-string/return-url



The payment link is a URL Payee PSP creates to prompt the Payer PSP app to open, thus ensuring app-to-app communication and redirect. For that

to happen, the Payment System Operator – or any other interested party – can define a path to every payment link. That would be the case of "pix-link" in the context of Pix. The way universal/app links work is that the Payer PSP would register a universal link/app link such as *"www.payer-psp.com.br/pix-link/*"* so that all links following that pattern prompt the app to open. This registration varies depending on the Operating System and is common knowledge among mobile front-end specialists. It is what guarantees app-to-app communication. Once the app is prompted by the payment link call, the Payer PSP app would be configured to process the link and navigate through the appropriate screens.

The link also contains the QR Code string, which in the context of Pix is an EMVCo-compliant data form (the copy/paste text code mentioned above). However, in the alternative proposal detailed above the string could be a RFC 3986-compliant URI. In any case, either the link or the URI should contain what the Payer PSP app would extract from the image if they were scanning the QR Code. After being prompted to open, the Payer PSP app would obtain the QR Code string from the payment link and process it as if it was a QR Code scanning or a copy/paste operation.

After the QR Code string, there should be a return URL to redirect the Payer to the original app once the payment is completed, avoiding the need for a second database of returned links.

One last alternative is having the whole URL signed by the Payee PSP using the digital certificates registered with the Payment System Operator, allowing the Payer PSP to process the link only if it is signed by another registered PSP. We do not believe this would increase the system's overall security since the customer has to review all the payment information before confirming the transaction on the Payer app. After all, the mechanics is equivalent to scanning a QR Code with a payment app, which is also not typically signed. The recommendation is that the security

guarantee should rest on the source of the data – either the PSP or a centralized alias base.

However, this approach can make sense depending on the specific requirements around how payment orders can be generated. See below two examples of how it could succeed:

Following the URI QR Code standard

https://payer-psp.com.br/pix-link
/payee-psp.com.br/pay-pix/418a34b8-4e5a-11ed-bdc3-0242ac120002
/www.payee-psp.com.br/return-url/6a101a34-82ed-4dbd-b734-0b85e63fbd6c
/fc11bbe5-180a-462d-b33f-56df7d61fb02

Following the EMVCo standard

https://payer-psp.com.br/pix-link
/00020126580014br.gov.bcb.pix0136123e4567-e12b-12d1-a456-426655440000520400005303986540510.005802BR5913Fulano deTal6008BRASILIA62070503***63041D3D
/www.payee-psp.com.br/return-url/6a101a34-82ed-4dbd-b734-0b85e63fbd6c
/fc11bbe5-180a-462d-b33f-56df7d61fb02

It is important to notice that we believe that restrictions on how payment orders can be created can have unintended consequences, even eventually impacting adoption.

g. Beyond QR Codes

TAKING THE CONCEPT OF PAYMENT initiation as a communication protocol to the next level, the idea of building payment solutions by creating new ways of sending the payment information from the Payee PSP to the Payer PSP can stretch into several additional applications. One example is contactless payments via Bluetooth, NFC, or other wireless communication. As long as the Payee PSP is available to send the payment information in EMVCo or URI standard, the payment initiation will follow the same flow as when the payer scans a QR Code.

However, vast the pool of applications of this concept, it is also worth mentioning another type of payment initiation: merchant-initiated payment. In this kind of payment initiation, the role of the Payer PSP is reduced or displaced. Use cases vary from direct debit, customer-presented QR Codes, variable recurring payments, and other implementations of the Open Finance concept of third-party payment initiation (3PI).

In each of these transactions, the payment flow starts with the Payee PSP – either the Payee's account holder or a third party commonly known as a Payment Initiation Service Provider, PISP. In either case, the first step of the payment flow, where the payer agrees to transfer a certain amount to a specific account, happens in the Payee's interface.

There are two ways to make this shift in the payment flow:

- By creating a new type of message the Payee PSP can send the Payer PSP through the Settlement Chamber indicating they want to initiate a payment;
- Or by establishing a new protocol for one-to-one integration between the participating PSPs.

The first solution is how the Brazilian Central Bank is implementing direct debit into Pix. The second approach is often used in Open Finance ecosystems.

In a scenario where all PSPs in the country are connected through one centralized Settlement Chamber, it does not seem reasonable to create a separate protocol for one-to-one integrations. However, it is worth noting that the Brazilian Central Bank did that by creating a one-to-one Open Finance protocol for payment initiation even after creating Pix.

To make matters worse, the Open Finance payment initiation flow is required by law to be subject to confirmation on the Payer PSP app before the payment is processed. As mentioned above, however, this level of experience could be attained using app-to-app communications via universal links/app links without needing to create complex standards or one-to-one API integrations.

An alternative approach could have been to specify the messaging between Payee PSP and Payer PSP via Settlement Chamber and allow PISPs to play the role of Payee PSPs in this context. The one-to-one integration protocol should only be used on two occasions:

- If the PISPs are allowed to initiate payments without the confirmation step on the Payer PSP app;
- And if it is either impossible or too inefficient to route the communication flow through the Settlement Chamber.

4.3. LESSONS FROM PIX

PIX'S PAYMENT FLOW HAS UNDOUBTEDLY proven its success. There are a few minor improvements that could be made, such as:

- Allowing the Payer to input information on the additional fields in Dynamic QR Codes;
- Creating a standard for redirect links for mobile payments;
- And relying more heavily on URIs to simplify the payment initiation standard for QR Codes and beyond.

All of which the Brazilian Central Bank had good reasons to leave out of Pix, but could be considered and eventually incorporated into new real-time payment rails with little additional specification efforts.

REFERENCES

- 79% dos brasileiros gostam da ideia de abrir mão do dinheiro vivo, diz PayPal (Época Negócios)
- A Plea for Simplicity (Schneier on Security)
- Banco Central do Brasil – Instant Payment System
- Ciro Nogueira infla prejuízo dos bancos e engana ao dizer que Bolsonaro criou Pix (Aos Fatos)
- Com o Pix, circulação de dinheiro em espécie caiu R$ 40 bi (Terra)
- Complexity and Security (Schneier on Security)
- Em um ano, Pix 'bancariza' 45,6 milhões de pessoas e pode poupar R$ 4,8 bi em tarifas para empresas (O Globo)
- Fim do dinheiro: Pela primeira vez na história valor do dinheiro em circulação cai no Brasil (Cointelegraph Brasil)
- Pesquisa do PayPal revela: 80% dos brasileiros não querem mais usar dinheiro e 93% adotariam o Real Digital (Cointelegraph Brasil)
- What is Pix? (Banco Central do Brasil)

AUTHORS

MARIANA CUNHA E MELO

Mariana Cunha e Melo is a NYU-educated lawyer with almost 15 years of experience in strategic litigation, public policy, legal research, and regulated markets. In her early career as a lawyer in Brazil, Mariana worked with Supreme Court justices, participated as a guest researcher in the Supreme Court public hearing about the right to be forgotten, and built the internet law team at a top law firm, representing Google on high courts and strategic litigation cases.

Mariana joined Nubank in 2018, where she helped structure the Public Policy team and developed the company's regulatory positioning and key advocacy thesis. She then transitioned to business and product strategy, leading Nubank in its efforts to work with the Brazilian Central Bank on designing its Real-Time Payments rail. She has since worked in early-stage startups as a strategic projects owner and director of regulation and strategy.

She is also a writer, having published books and articles on privacy, free speech online, and regulation of fintech companies. As a speaker, she has numerous international events.

AUTHORS

JONAS ABREU

Jonas de Abreu is a seasoned security engineer with deep experience in software engineering and security engineering. In his early career, he worked on several projects as an external consultant and was an instructor in various training programs.

Jonas dedicated almost a decade to helping build and scale Nubank, LATAM's leading financial technology company. He joined Nubank in early 2015 as one of the first engineers onboard. He served as the company's Chief Information Security Officer for several years. In late 2019, he switched to a Principal Engineer position, where he continued to make significant contributions to the company's security strategy.

Besides his role in shaping Nubank's infosec team and strategy, one of Jonas's most notable achievements at Nubank was his instrumental impact on the Brazilian Central Bank's decisions regarding the technology adopted in the Pix rail. He was the engineer responsible for Nubank's technical proposals during the Pix Forum. His contributions were highly valued by the industry experts and played a pivotal role in shaping the future of payment systems in Brazil.

ABOUT CTPI

THE CENTER FOR TECHNOLOGY AND Public Interest is a subscription-based research center. We are here to transform the future of the tech industry through information, training, and research toward a systemic and sustainable approach to technology. Our purpose is to bridge the gap between technology, business, and regulation to create systemic and sustainable solutions to the problems that neither the industry nor the regulation can solve on their own.

www.ctpi.io

https://www.linkedin.com/company/ctpi-io/

Email addresses:

- mariana@ctpi.io
- jonas@ctpi.io
- hello@ctpi.io

Address:

- CENTER FOR TECHNOLOGY AND PUBLIC INTEREST, SOCIEDAD LIMITADA
  Carrer de Bailèn, 11, Barcelona,
  Spain, 08010

CTPI

CENTER FOR TECHNOLOGY AND PUBLIC INTEREST