# THE QR CODE PAYMENTS LANDSCAPE

## A LEVEL ONE PROJECT PERSPECTIVE

## OCTOBER 2019


THE LEVEL ONE PROJECT IS AN INITIATVE OF THE BILL AND MELINDA GATES FOUNDATION

GLENBROOK **PARTNERS**

# CONTENTS

This is a landscape review of QR Payments models around the world, with an emphasis on developments in emerging economies.

In this report, we describe the various models, with particular attention to how QR code implementations connect with the underlying payments systems used to process the payments.

We also assess how the various models are aligned with the Level One Project design principles and key concepts.

For this report we looked at the following market developments:

- Singapore SGQR
- Indonesia QRIS
- India BharatQR and BHIM QR
- Thailand Standardized QR Code
- Alipay w/ Europe Wallet Providers
- Mexico CoDi
- China Alipay
- South Africa SnapScan
- Asia GrabPay

This document is a continuation of prior research done for the Level One Project. The 2017 report “Research on QR Code-Based Payments and its Application in Emerging Markets”, which provides a detailed history on how QR codes were introduced, can be downloaded from leveloneproject.org.

# CONTENTS

# Executive Summary

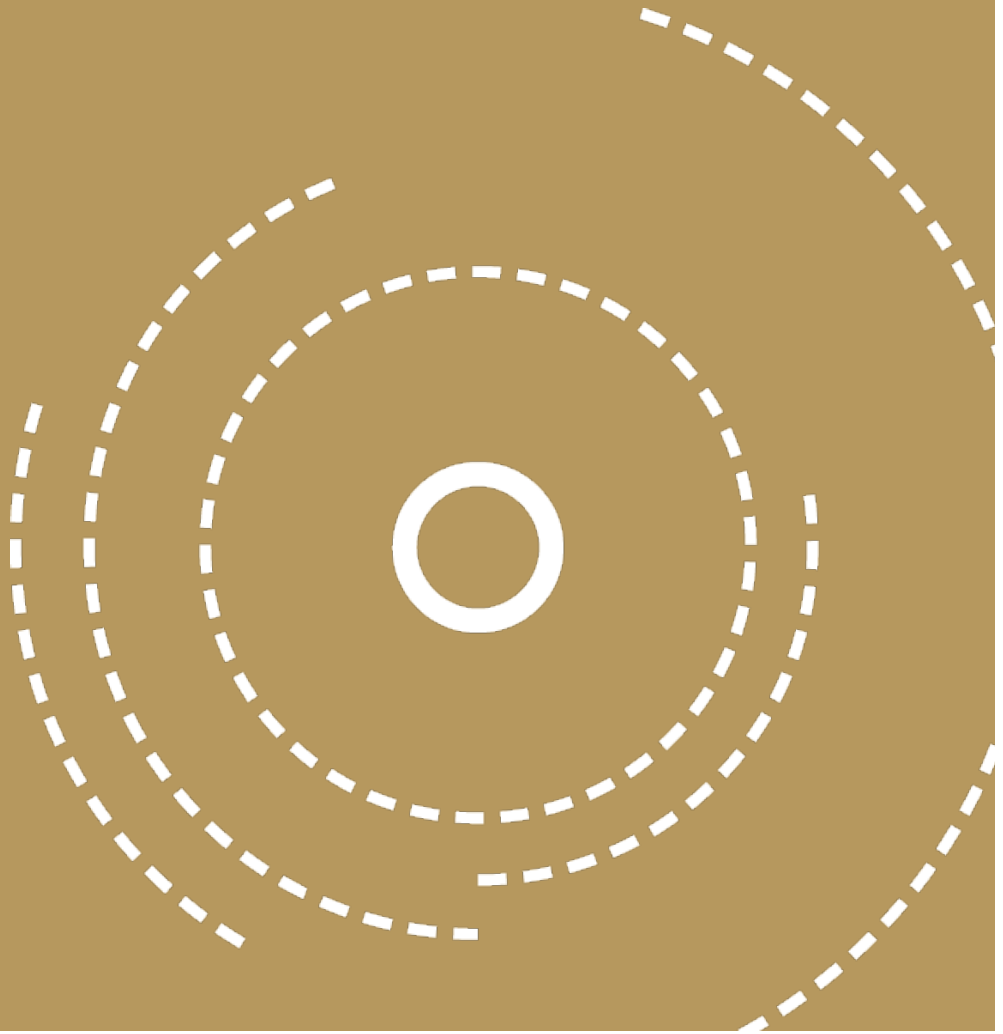
**QR Codes used for merchant payments are gaining rapid traction worldwide. These payments in general support Level One goals of growing the digital ecosystem: those that work in conjunction with interoperable payments systems are particularly well-aligned. But the market is still in its infancy, and important questions remain.**

The convenience and ease-of-use of the technology offers the promise of unlocking high volume merchant payments, and achieving goals important to financial inclusion. These goals include making digital money usable for consumers, and providing the high volumes necessary for low cost systems.

Early implementations are largely using static QR code protocols, and most use a Shared QR Code model implemented with EMVCo standards. It is not yet clear whether this is the right long term approach, as there are issues with control, fraud, and the ability to smoothly transition to dynamic QR code protocols.

Other models are emerging in the marketplace as well. Single QR Codes, used with either interoperable or closed-loop payment systems, are gaining dramatic share in countries such as China. And the “tech giants” are introducing alternatives to QR Codes which may impact the development of the market.

# INTRODUCTION



THE LEVEL ONE PROJECT

# QR Codes Are A Key Enabler Of Merchant Payments

**Particularly in emerging economies, QR code-enabled merchant payments can bring critical transaction volumes to the underlying payments system, thereby lowering transaction processing per unit costs.**

The ease of use of QR code payments – for both the consumer and the merchant - are breaking open the merchant payments market in many countries. This has been an intractable problem in the past – with neither merchants nor consumers being interested in paying electronically.

Without a developed card acceptance infrastructure, emerging economies have generally not had a means of converting cash merchant payments to digital payments. Some of these countries, however, do have the "rails" of a real-time retail payment system in place. These rails to date have been used primarily for person-to-person payments.

In countries with a real-time retail payments system in place, QR codes can be an "overlay" on those systems – the means to easily initiate payments that are cleared and settled over those rails.

# Merchant Payments are Critical for Financial Inclusion

**Enabling merchant payments makes digital money "spendable", and can reduce the rate of cash-out of digital balances.**

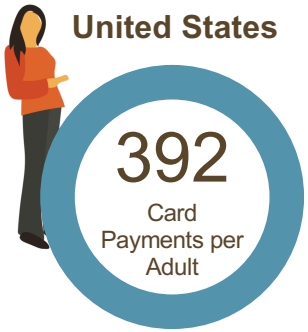

Enabling merchant payments is critical for a number of reasons. Making digital money "spendable" is necessary if we want consumers to leave their money in their account – rather than cashing-out upon receipt of digital funds. This can lead to a state of "digital liquidity" – where a consumer (or a merchant!) will be content to leave their funds in digital form.

With "spendable money" in a transaction account, consumers and merchants can develop a transaction history that can lead to the use of other financial services, including borrowing and investing.

A consumer who is using her transaction account for merchant payments will also be better positioned to participate in the developing digital economy – she is enabled to purchase a wide range of government and commercial services.

# Payments Opportunities in Emerging Economies

What will payments volumes look like once merchant payments “take off” in a country? We used the U.S. payments market as a reference point for a mature payments market. In the U.S., the most common form of electronic merchant payment is the debit card – but this may be a good proxy for what QR code based merchant payments could look like in other economies.




**Reference Point**

In this highly developed electronic payments market, card payments account for approximately 62% of all retail purchases, measured by the number of transactions.

Debit card payments were introduced in the 1970’s, but really began to gain traction in the 1990’s.

About 9 million merchants in the U.S. accept card payments.

All figures annual

*mPesa launched in 2007*

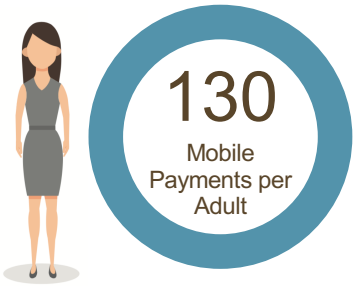
*PromptPay launched in 2017*

Source: Glenbrook analysis

# Payments Opportunities in Emerging Economies

So far, only China has truly realized the potential of QR payments, but other emerging economies have the infrastructure in place and are positioned for rapid growth. The numbers shown for India, Kenya and Thailand represent mostly P2P payments at this time, but the same payments systems are now also supporting QR code payments.

## China

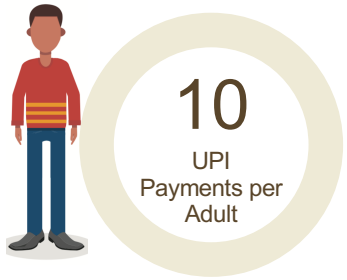



~ 40 million merchants enabled for QR

WeChat Pay and Alipay form a duopoly with dramatic payments volume growth. Most of these payments are QR code based

*Alipay launched in 2004*

## India

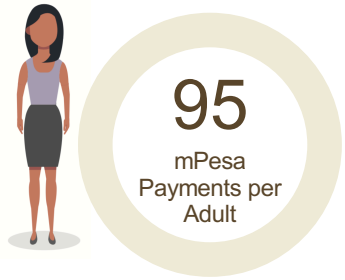



~ 10 million merchants enabled for QR

The BharatQR program has been linked to the UPI "rails"

*UPI launched in 2016*

## Kenya

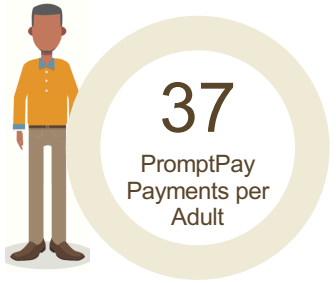



~ 100,000 merchants enabled

The established mPesa platform has been slowly adding QR code payments

*mPesa launched in 2007*

## Thailand




~ 5 million merchants enabled for QR

The new PromptPay system has been QR code enabled and is growing quickly

*PromptPay launched in 2017*

All figures annual

Source: Glenbrook analysis

# The Level One Project

This landscape review is done from the perspective of the Level One Project.  The Level One Project, an initiative of the Bill & Melinda Gates Foundation,  is a vision for a new digital payments platform that supports inclusive, interoperable digital economies. The QR payments models discussed in this report will be evaluated against the concepts that are central to this vision.

### Design Principles

- Open-loop
- Real-time, push payments
- Irrevocable, same day settlement
- Pro-poor governance
- Cost-recovery model
- Shared investment in fraud detection

### Key Concepts

- A collaborative/competitive spectrum
- Low cost
- Multiple Use Cases
- Government Support

### User Requirements

- Secure
- Affordable
- Convenient
- Open
- Robust

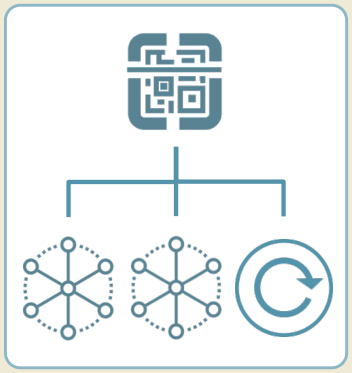
# QR CODE MARKET MODELS

# QR Code Payment Models In Market

**There are multiple different QR code models that are either live or in implementation in markets across the world.**

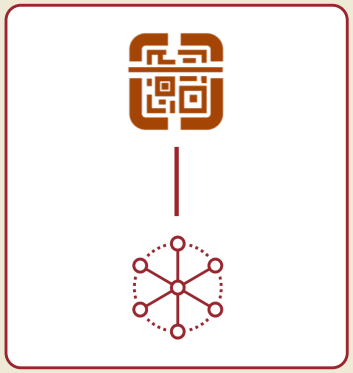
### Shared QR Code
***Multiple Payments Systems***

This multi-tenanted approach allows multiple schemes to initiate payments on their own “rails”, using a single QR code. The schemes may include both interoperable and closed-loop systems.



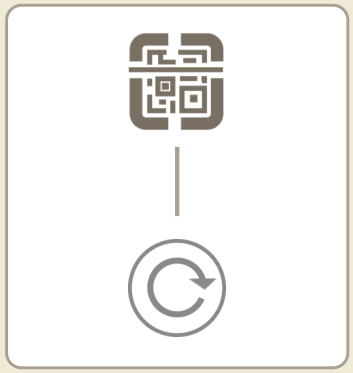
### Single QR Code
***Interoperable Payments System***

One QR code enables payments on a single interoperable payment scheme. Consumers and merchants using different participating DFSPs can send and receive payments using the QR code.



### Single QR Code
***Closed-Loop Payments System***

One QR code enables payments in a closed-loop payment system. These enable payments only for the payment system that provides them and requires both consumers and merchants to participate directly in the scheme.

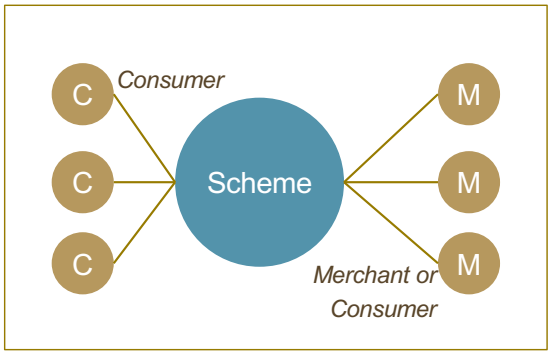


# A Note on Payments System Terminology

"***Open-loop***" and "***closed-loop***" are terms used to describe different types of payments systems. An "open-loop" system can also be described as an ***interoperable*** system. We use the term "***scheme***" to specify a payment system with its own business and operating rules, which bind participants in the system.

### Closed-Loop Payments Schemes

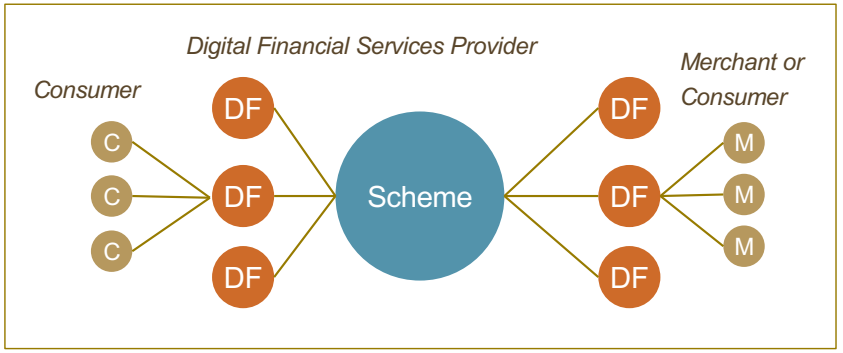
In a closed-loop scheme, each customer and merchant has a direction relationship with the scheme.




The scheme may access open-loop, or other closed-loop schemes, as funding sources for its customers.

### Open-Loop Payments Schemes

In an open-loop system, digital financial services providers belong to the scheme, and deliver interoperable payments transactions through the scheme to their consumer and merchant customers.



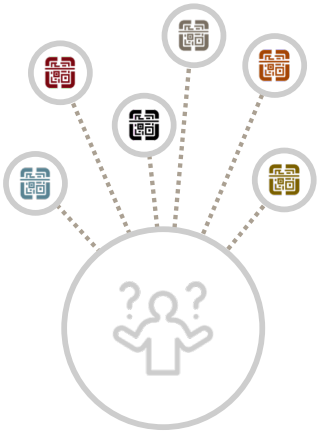

Depending on regulation and scheme rules, an open-loop system may allow both banks and licensed non-banks to be digital financial services providers and participate in the scheme.

# “QR Code Interoperability”

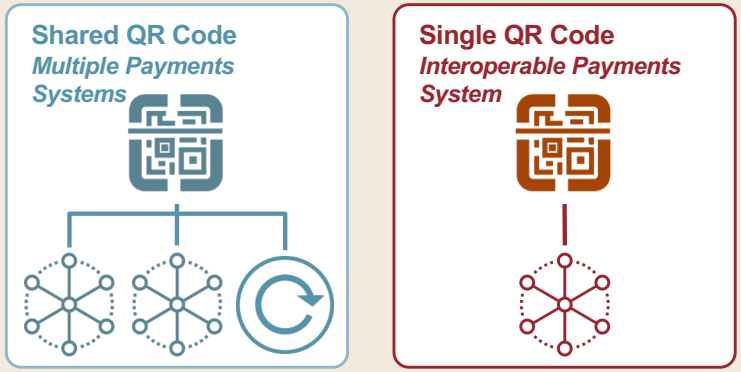
## It is common to hear “QR Code Interoperability” as an objective. But what does that mean?

The understandable goal is to avoid having multiple QR codes at a merchant’s counter: this can create a cluttered, confusing experience for consumers and merchants. The term “QR Code Interoperability” is used to to describe ways to address this issue. The term, however is a misnomer: payments systems, not QR codes, interoperate.

In market, the term “QR code Interoperability” can refer either to a multiple payments system, Shared QR Code or a Single QR Code for an Interoperable Payments System. Depending on the implementation, either approach can address the issue of point-of-sale clutter.

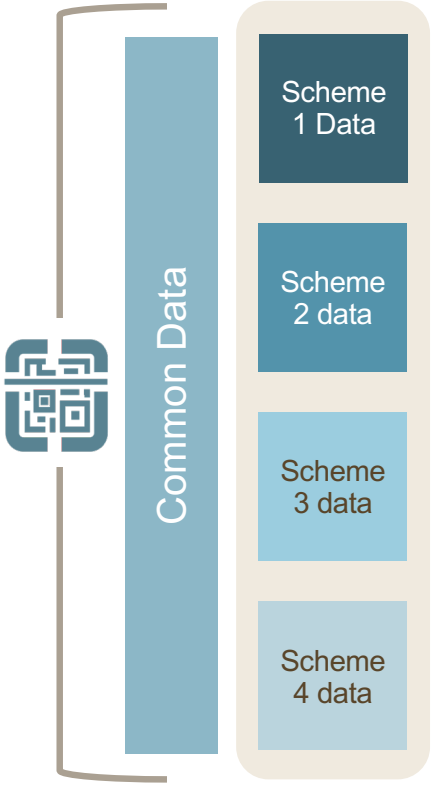


***Two approaches to fewer QR codes at the Point of Sale***



# The Shared QR Code Model

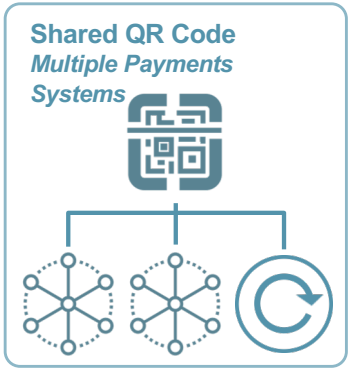
**This model is the most common seen in market today.**




In this model, the QR code data string contains a block of common data along with a “stack” of scheme-specific payments addresses. The common data block contains data that persists between schemes, such as the merchant’s name, while the stack contains data that is only necessary for each individual scheme, such as the merchant’s payments address.

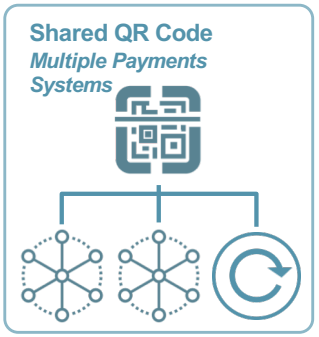
The scanner reading the QR code reads the encoded data objects to pull the common data required, and then interrogates the stack and extracts the scheme-specific data.

Seen in Singapore, India, Indonesia and Thailand



# The Shared QR Code Model and EMVCo Specifications

**The EMV QR code standard is the way that most of shared QR implementations are choosing to format the QR code data.**




The EMV specifications provide details of the formatting of the QR code and the payment address data in the “stack”. Each shared QR arrangement may customize the standard to some degree.

EMV® QR Code

Most of the implementations we see in market are merchant-presented, static QR codes. The EMV specification supports dynamic QR codes as well; this is discussed in the “Future Directions” section.

The EMVCo specification covers consumer-presented QR codes as well as merchant-presented. Merchant-presented is the more common model in the emerging economies, so that is what we discuss in this report.

Specifications

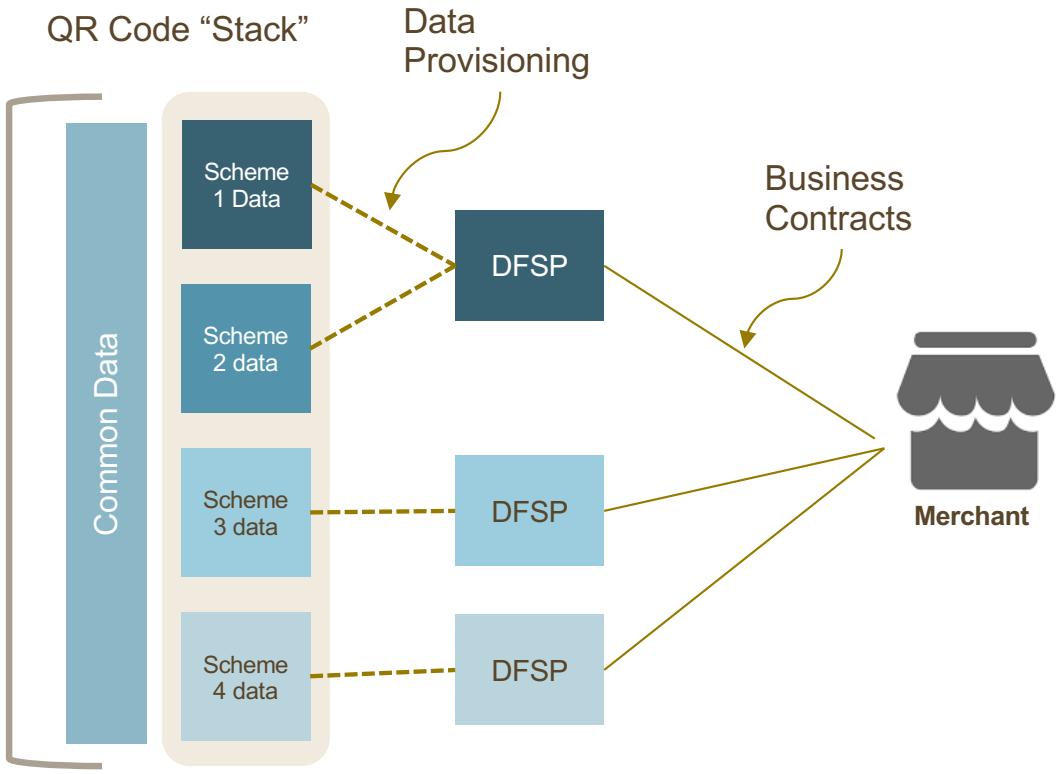
| Version | Published | Description |
|---|---|---|
| 1 | 31 Jul 2017 | EMV® QR Code Specification for Payment Systems: Merchant-Presented Mode |
| 1 | 13 Jul 2017 | EMV® QR Code Specification for Payment Systems: Consumer Presented Mode |

# Shared QR Code: Business Relationships

The QR code contains a “stack” of merchant payment addresses, one for each scheme the merchant accepts payments from.

This model relies on a merchant having  a business relationship with a DFSP for each scheme it supports. In some markets, one DFSP may represent several schemes to a merchant.

The term “scheme” as used here could be an RTRP credit transfer system, a card system, or a wallet of some sort.



# The Shared QR Code Model: Consumer Experience

This model relies on the consumer to choose the payment method used, based on the methods the merchant is accepting. This implies that the QR code display (physical or digital) needs to show the payment methods accepted.

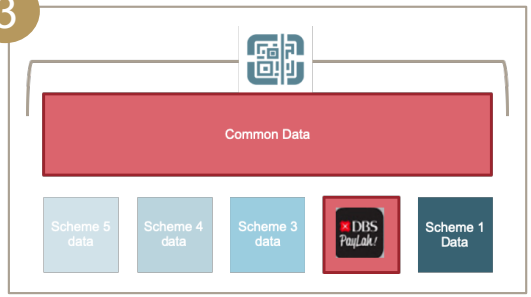
1


The consumer chooses which payment app she wants to use.

2


She scans the QR code using the payment app she chose.

3

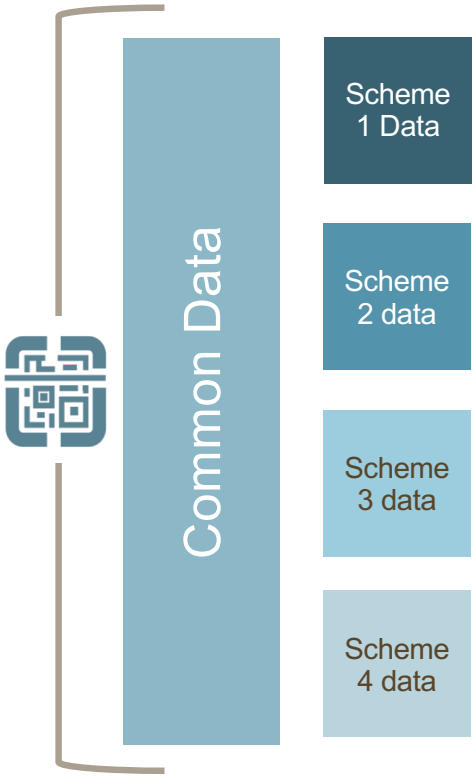



The consumer's chosen payment app interrogates the stack encoded into the QR code, which contains the merchant's payment address at each of the schemes they accept. If the app finds a compatible scheme payment credential in the QR code, it will begin the payment initiation process.

*How the payment process works depends on the specific scheme. Some schemes are "pull payments", such as card payments; others are "push payments" – such as RTRP payment networks.*

# The Shared QR Code: Merchant Provisioning

**How does the merchant get this multi-tenanted QR code?**




The merchant has separate business agreements with various DFSPs, aggregators, or wallet providers. In a single (non-shared) QR code scheme, the merchant would simply get the QR code from the DFSP (or self-provision using the DFSP's app). In a shared QR code model, there are a variety of options:

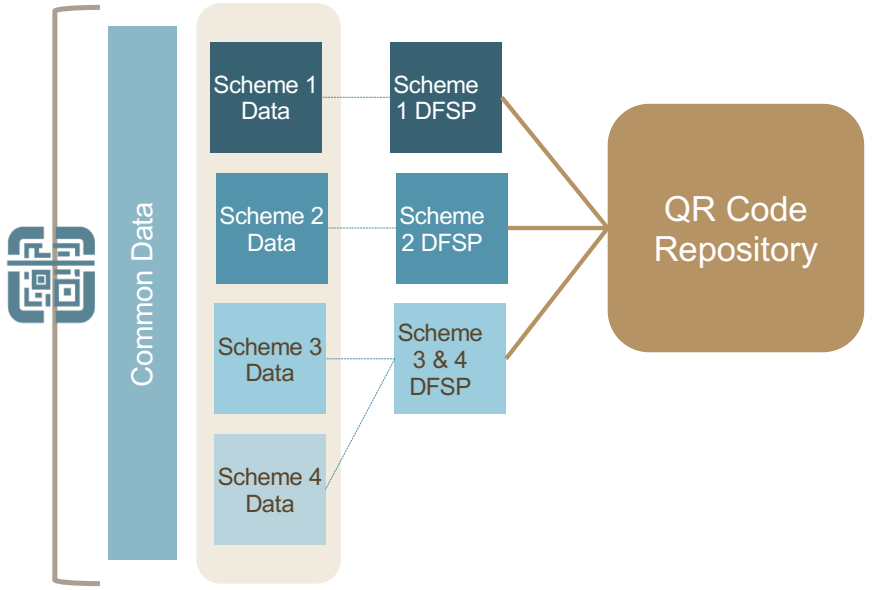
1. One DFSP is chosen as the lead; they create the QR code including data from other DFSPs. There are obvious issues here – who chooses the "lead" DFSP? Who ensures that the other DFSPs are correctly shown in the QR code?
2. Each new DFSP provisioned can create the "full stack" QR code, reading the old QR code to get the existing data. This model also has issues: how are changes managed, how do you delete inactive merchant relationships, etc.
3. The most common model is to use some central entity that tracks all of the payment methods accepted by each merchant, and is involved in some way in the generation of the QR code or the data string that is used to generate the QR code. For the purposes of this study, we are referring to this as the "QR Code Repository"

# Shared QR Code Model: the QR Code Repository

**A QR Code repository is a concept still in development in the market.**

- The repository keeps a record of every payment method a given merchant accepts
- The repository then either renders the QR code itself, or the data string which can render the code
- It is most likely that DFSPs, rather than merchants, would interface with the repository –but we have seen at least one major implementation where the merchant works directly with the repository
- Any DFSP can then render the QR code for the merchant, or make it available in the merchant app for the merchant to render.
- Who owns or controls this entity? By definition, it is greater than a single scheme. It may be some government agency, or a DFSP owned clearinghouse of some sort that handles multiple types of payments.

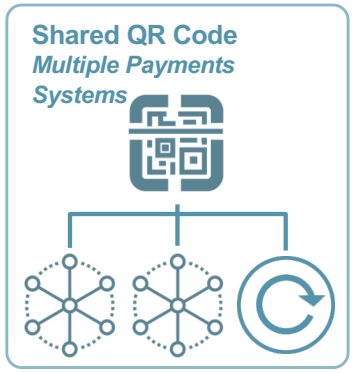
*A QR Code Repository, almost by definition, uses or creates some kind of national merchant identifier.*



# The Shared QR Code Model: Future Repository Functions

**QR Code Repositories may play a key role in fraud management.**

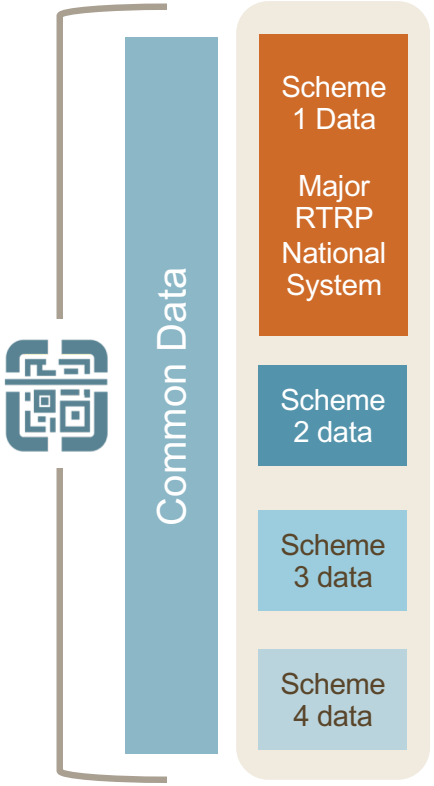
- If the Repository is generating the QR Code (or the data string used to render the QR code), it may enable – or require – validation of the QR code before a payment is effected.
- This may be done either by a hash function, with the repository taking an active role in validation at the time of transaction execution, or by a digital signature validation, which could be done at the consumer app.
- This is an important fraud mitigation step, and can ensure that at a minimum the QR code contains only payment credentials that are on file at the repository
- A QR Code Repository is also in a good position to add other pan-scheme, value-added services, including other fraud management services, in the future.




*Many countries are implementing – or trying to improve – the process of business registration. QR Code Repositories are a logical player in this process, and could feed – or be fed by – a national business registry.*

# A Shared QR Code Variation:

## Multiple Payment Methods, but a Dominant National RTRP System in the "Stack"




In some countries, there is a single RTRP credit-push platform with strong government support behind it. Although the QR code approach enables a "stack" of payment acceptance possibilities for a merchant, it may turn out that the RTRP platform is the dominant system used.

This is particularly likely in situations where the government is playing a role in setting merchant and consumer payment fees – in some cases, requiring them to be zero.

***India*** *and* ***Thailand*** *appear to be examples of this approach. Both are using the shared QR code EMVCo standard. But India's UPI payment scheme, and Thailand's PromptPay payment scheme, have strong government backing and are showing rapid growth. It appears possible that the two systems will become the default system for most merchants.*

# Implications of the Shared QR Code Model

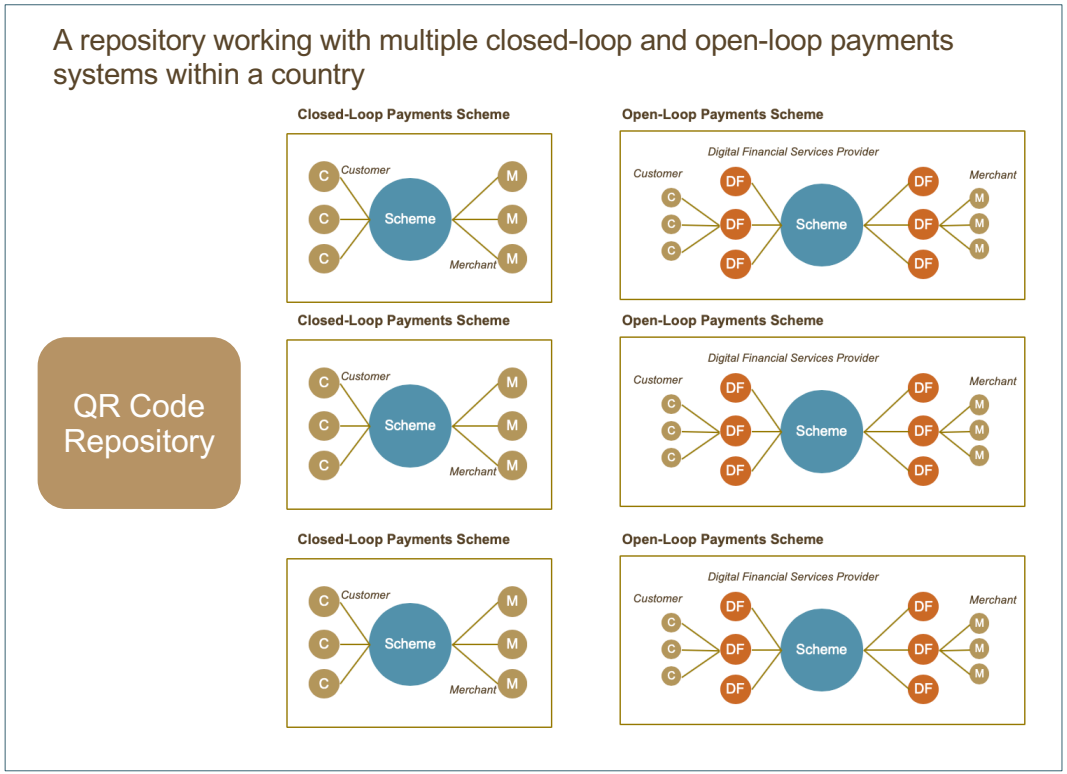
**This model promotes *competition among schemes.***

Each scheme enabled by the shared QR code has its own operating and business rules.

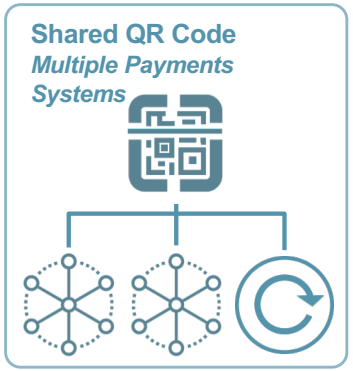
The QR Code Repository may become a “meta-scheme”, with repository rules that may over-write some of the underlying rules of individual schemes sharing the QR Code.

This approach may be the most appropriate in markets with already well-developed electronic payments ecosystems.

In emerging economies without such developed ecosystems, it may provide a degree of choice – and concomitant confusion for consumers and merchants – that could slow adoption.



# Challenges with the Shared QR Code Model




- The EMVCo standard uses what we call “in-code” payment credentials – the actual payment data is in the QR Code data string. Any change requires re-provisioning a QR code – a burden when used with static, paper-sticker QR codes. Other approaches use a “referred” model, in which the consumer payment app is directed, once the QR Code is scanned, to another location in order to find the payment data. This may prove more flexible in the future.
- The shared QR model inherently requires users to navigate to their chosen payment app in order to choose which payment scheme they would like to use. This could be perceived as an area of friction for the end user.
- This shared QR code approach also requires a consumer to use a smart phone: it does not easily accommodate the “QR Code plus pay-to till number” that some single-scheme approaches use.
- Cross-scheme fraud control is possible, particularly if there is a strong QR Code Repository function: but this is more complex and difficult than with the single-scheme approaches.

# The Single QR Code Model

## Implemented with a Closed-Loop Payments System

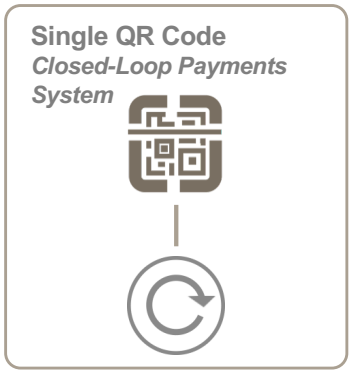
This has been the predominant method used in early implementations of QR code payments: a single, closed-loop wallet provider offering QR codes for ease of payments.  These remain in place in a number of markets.

These closed-loop systems work equally well in consumer-presented and merchant-presented mode: and consumer-presented codes can work with a printed sticker on a feature phone.

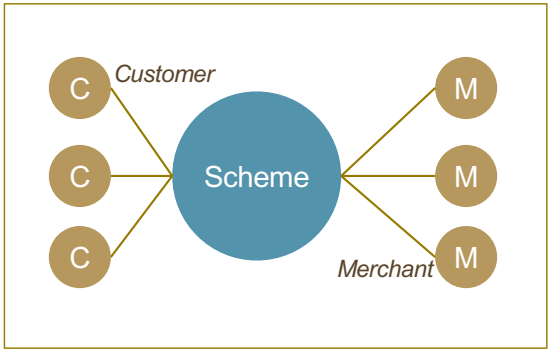
By definition, these implementations tightly couple the QR code protocols and rules with the rules of the underlying payment system.

In recent years, attention has focused primarily on China, where the duopoly of WeChat Payments and Alipay have accomplished broadly adopted QR code payments.

Seen in China and South Africa

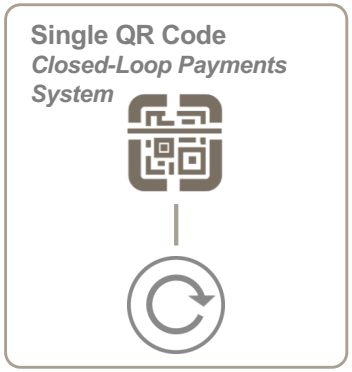



**Closed-Loop Payments Scheme**



# Implications of the Single QR Code Model

## Implemented with a Closed-Loop Payments System




This model promotes ***competition among schemes.***

In some respects, these implementations are easier to accomplish than are shared QR implementations. The closed-loop payment scheme can make unilateral decisions about formatting and related issues.

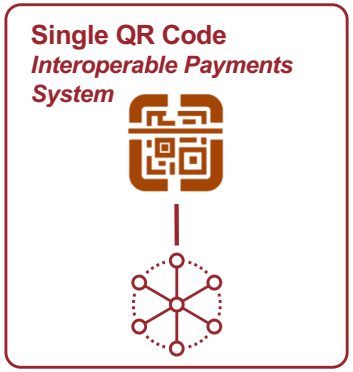
However, success depends on penetration of this underlying closed-loop payments scheme. Although China shows clear success with this model, it is questionable whether or not this is replicable in other markets.

Single QR Code, closed-loop implementations are also free to use proprietary formatting approaches – some of which leverage the URI and URL structures which arguably will provide greater flexibility, in the long term, than the relatively static in-code approaches, such as that demonstrated by the EMVCo standard.

Like with single QR code models for an open loop system, if other QR codes are used in any given market, multiple single scheme QR codes likely created clutter, and possible confusion, at the checkout.

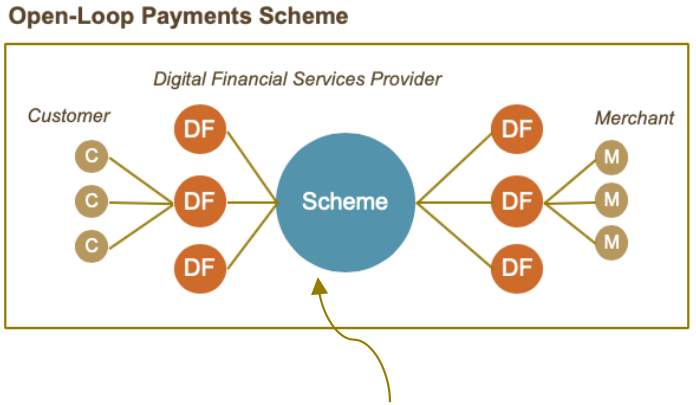
# Single Scheme QR Code Model

## Implemented with an Open-Loop Payment System




- This model can best be thought of as QR Code-enabling an existing interoperable payment system.
- The rules, processing capabilities, and fee structures are an extension of those that exist in the underlying payment system.
- The payment system can use whatever data formatting approach it favors: there is no need to use the shared QR code capabilities provided for in the EMVCo standard.
- ***QR code enablement of payments over an open-loop scheme is a relatively simple addition to existing form factors, whether those be card or mobile payments.***

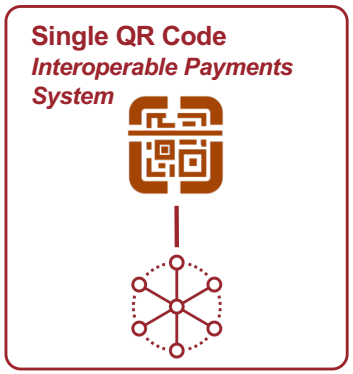
Seen in Mexico




QR code rules are added to existing scheme rules

# Implications: Single QR Code Model

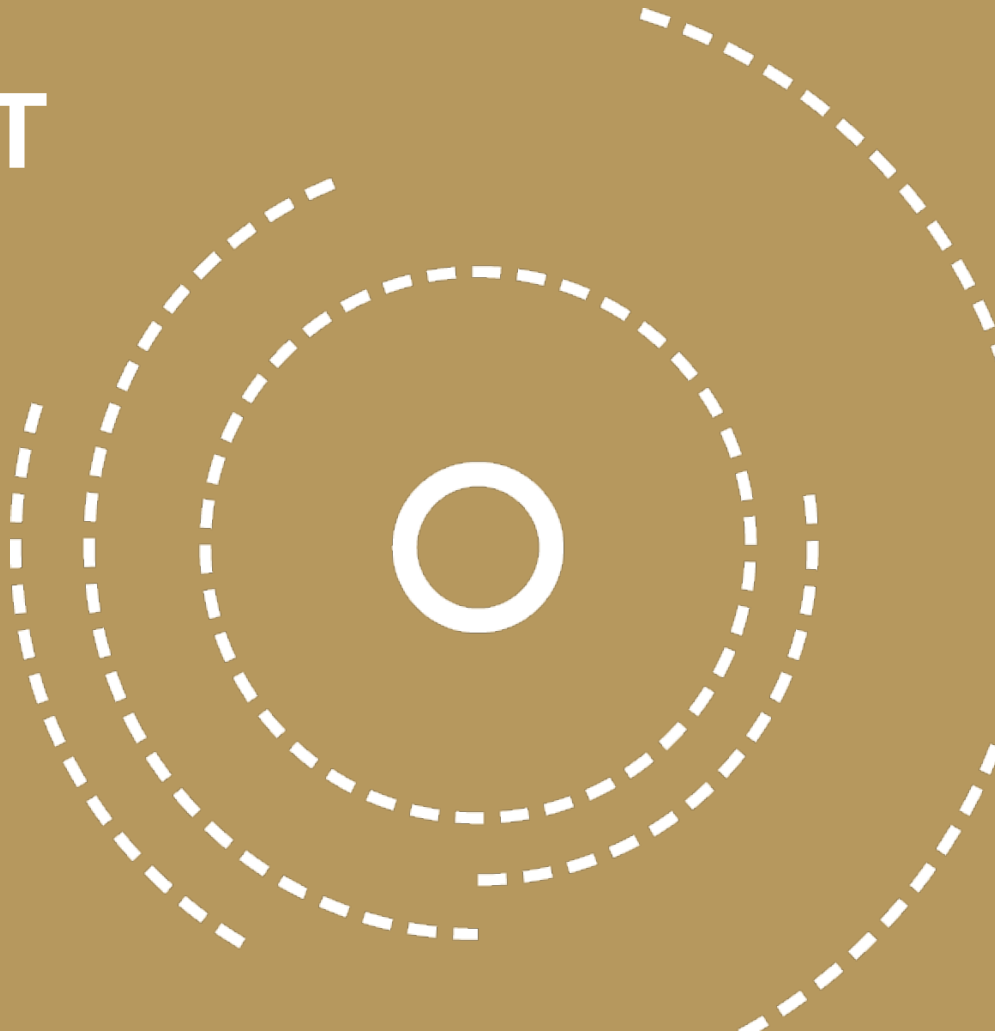
## Implemented with an Interoperable Payments System




- This model promotes ***competition among providers*** within the single scheme.
- It enables tight coupling of QR code rules and payment system rules.
- Logically, it requires a centralized merchant registry, or at a minimum centralized control over merchant payment addresses. This centralized authority can be an active participant in transaction processing, when that is required – for example, this may come into play with dynamic QR code implementations.
- Lastly, if other QR codes are used in any given market, multiple single scheme QR codes likely created clutter, and possible confusion, at the checkout.

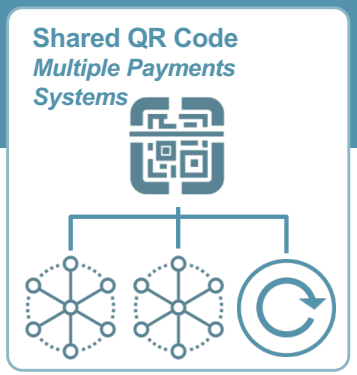
- *This approach appears to be used in countries where the primary objective of regulators (or payments authorities) is to build a single national payments platform.*
- *Concentrating volume on a single platform can provide economic efficiencies, and reduce marketplace confusion.*
- *Note that shared QR code implementations with a dominant RTRP share some characteristics of the Single-Scheme implementations.*

# QR CODES: MARKET LANDSCAPE



THE LEVEL ONE PROJECT

# Singapore SGQR




## A Shared QR Code Approach

### Country Payment System Overview

Singapore has a highly developed payment system, with a mostly banked population. Card penetration is extensive, and there are multiple mobile payment applications and FinTechs in market.

Recently, Singapore's banks introduced FAST, a real-time credit push electronic transfer system.

Singapore's central bank, The Monetary Authority of Singapore (MAS) oversees the payments ecosystem in the market. MAS has a Payments Council to drive the adoption of e-payments, and foster innovation and collaboration in the industry

### QR Code Market

Singapore has had many QR solutions in market, fueled by relatively high smartphone penetration.

MAS's Payments Council has stepped in to help streamline the multiple QR solution by launching SGQR, a shared QR code that combines the data elements necessary to conduct payments with multiple providers.

Participating payment schemes are currently in the process of migrating their merchant customers to the new shared QR code.

# Singapore SGQR

## A Shared QR Code Approach

SGQR is an implementation led by the central bank – the Monetary Authority of Singapore.

- SGQR is a shared QR code implementation using the EMVCo QR code specification.
- MAS contracted with BCS – a payments services operator – to operate the QR code repository
- The initial implementation is for merchant-presented, static QR codes only
- SGQR is not involved with payments processing, nor with the business agreements between merchants and payments providers

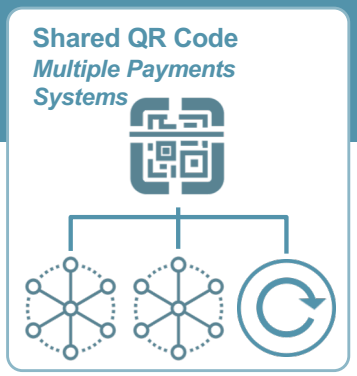
*Announced by MAS in September 2018: "SGQR will be adopted by 27 payment schemes including PayNow, Nets, GrabPay, Liquid Pay and Singtel Dash, and will be deployed progressively over the next six months."*

When the shared QR code is printed out on a paper sticker, it carries the brand icons of all of the payment schemes supported by that merchant. That helps the consumer choose what payment app to open.


*The initiative is apparently a reaction to a proliferation of single-scheme, closed loop QR codes offered in the market – which were creating clutter and confusion at merchants.*

.

# Indonesia QRIS




## A Shared QR Code Approach

### Country Payment System Overview

Nationally, only 49% of adults have a transaction account in Indonesia. Payments systems and availability are unevenly distributed and accessed. Cash and convenience store payments remain common for both point of sale and remote purchases.

Bank Indonesia (BI), the country's central bank, oversees the domestic payments market.

In 2017, BI recently announced the launch of the National Payments Gateway (NPG). Prior to the NPG initiative, debit cards issued by one of the nations more than 140 banks could only be used on terminals from the same bank.

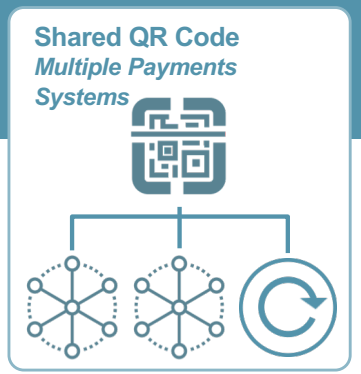
NPG is made up of a consortium of four local interbank switching companies who now jointly manage and operate the shared payment infrastructure.

Though smartphone penetration remains low in Indonesia, the market does have several QR providers.

These include OVO, GO-JEK, Dimo Pay, and Yap!

Recently, BI announced **QRIS**, a shared QR code approach aimed at reducing the use of cash in the country.

# Indonesia QRIS




## A Shared QR Code Approach

QRIS uses the EMVCo standard for QR codes. However, BI is taking a novel approach to the QR Code implementation, intending that a merchant who has a payment acceptance account with one payment scheme will be able to accept payment from consumers using any other scheme.

To do this, it appears that BI will put in place a "gatewaying" switch that will move a payment order from one system to another. The details behind this, including how settlement is effected, and how business rules are rationalized across system, is not yet clear.

This approach is conceptually similar to what Visa and MasterCard do in the United States with their "credit push" products: which use a variety of protocols to enable a payment initiated by a Visa bank, for example, to be received by a MasterCard bank. This is complicated, however, and requires both message protocols and business rules to effect.

*"QRIS allows QR-code-facilitated payments [in Indonesia] to be interconnected and interoperable through a single standardized code," said BI governor Perry Warjiyo during the launch ceremony in Jakarta.*

# India

## Multiple QR Code Approaches in a Country With Strong National Payments Systems

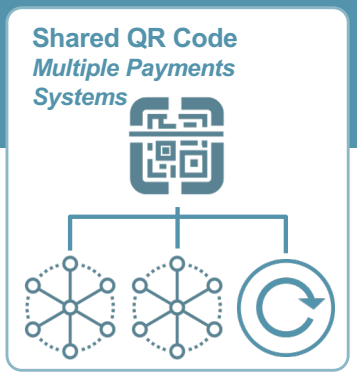
### Payments Systems

- India has a well-developed, broadly available set of payment systems. Most are operated by the National Payments Corporation of India (NPCI), a non profit company owned by a consortium of major banks. NPCI has led the charge in fostering innovation and building out the national digital payments infrastructure.
- NCPI has two RTRP systems: the IMPS system for interbank transfers and the UPI system. UPI, notably, allows non-bank, non-transaction account providing PSPs to initiate payments orders that transfer money from one bank account to another. This has allowed so-called "technology giants" (Google, as one example) to play a major role in payments systems initiation.)

### QR Market

- Historically, QR payments in India were limited to closed loop wallets, such as Paytm, Freecharge and Mobikwik.
- NPCI has introduced both Bharat QR and BHIM QR to reduce the problem of multiple QR codes.
- Bharat QR is a Shared QR Code Model with a dominant underlying RTRP system (UPI)
- BHIM QR is a Single QR Code Interoperable Payment System model, intended primarily for P2P payments.
- Single QR Code, closed-loop payment system models are also still in the market in India, as are non-standard, QR code like systems such as Google's Spot Pay – described in more detail in the "Future Directions" section of this report

# India: Bharat QR

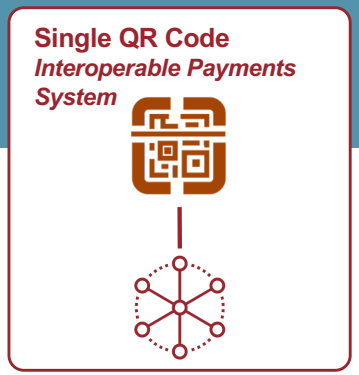



## A Shared QR Code Model

- BharatQR is a shared QR code implementation, using the EMVCo QR Code specification
- Bharat QR supports static and dynamic QR codes and both push and pull payment schemes. It appears to be used primarily with merchant-presented QR codes.
- It was launched in 2016, in cooperation with global card networks and the domestic RuPay card, operated by NPCI.
- NPCI appears to be operating the "Repository" function for Bharat QR


It remains to be seen if the most popular payment method used with Bharat QR will be RuPay Debit Cards or UPI. Both debit a consumer's bank account. UPI payments are less expensive to the merchant, but there are more RuPay enabled bank accounts.

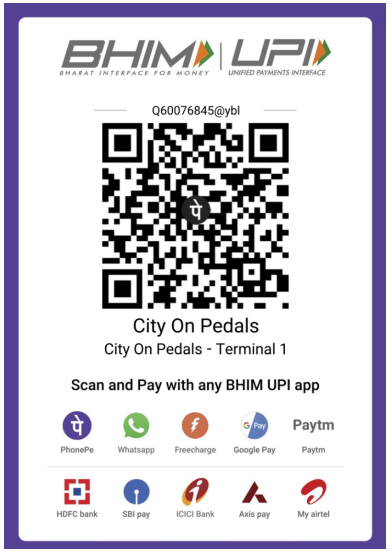
# India BHIM QR




## A Single QR Code Model Implemented with an Interoperable Payment System Model

- BHIM is provided by NPCI, and intended to be used by consumers to initiate P2P transfers over UPI.
- BHIM QR Codes can be created within the application and either displayed digitally or printed out
- BHIM QR Codes are used for payment only on the UPI payment system. UPI is an interoperable payment system supported by all banks in India.

From NPCI: "BHIM QR is UPI Based QR. It is preferably used for P2P or P2M dynamic Transaction using Virtual Payment Address. Bharat QR is specifically used for P2M transaction wherein payment is done via cards i.e., Debit card/Credit Card/Pre-paid Card."



# Thailand's Standardized QR Code

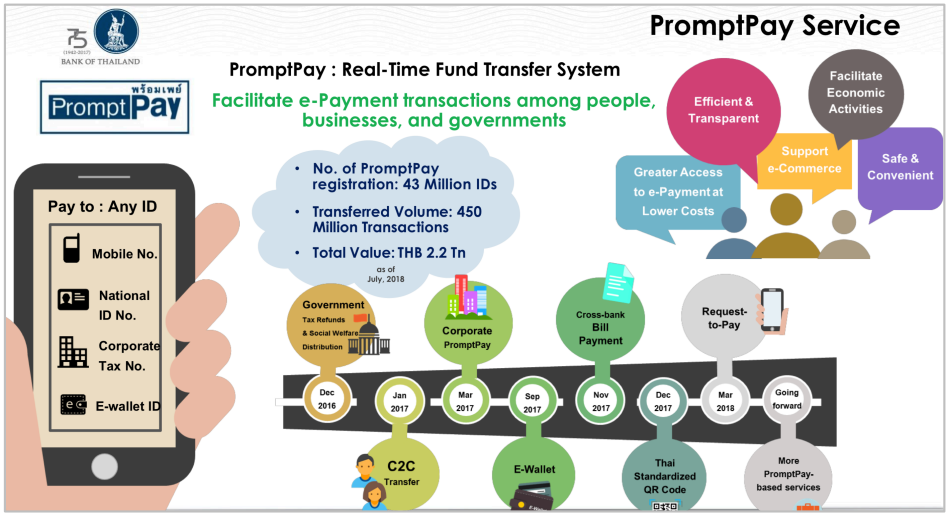
Thailand has a thriving economy and, at 77% a relatively high rate of adults with financial accounts.

The Bank of Thailand (BoT) oversees payments systems and regulation in the country, and maintains a National e-Payment Master Plan.

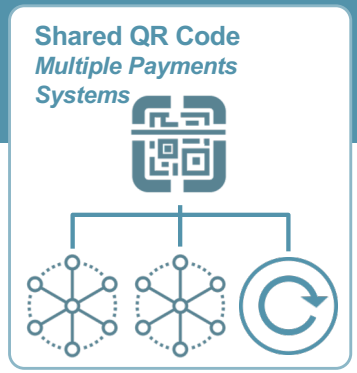
In 2017, BoT launched PromptPay, an electronic retail payments system, to enable real time payments between users. The open-loop system uses a social token, such as a phone number or national identification number, as a payment alias.

The Thai government has encouraged adoption of PromptPay by paying out government benefits using the system.

**Bank of Thailand's PromptPay Vision**
Includes multiple use cases and multiple payments addresses



# Thailand's Standardized QR Code

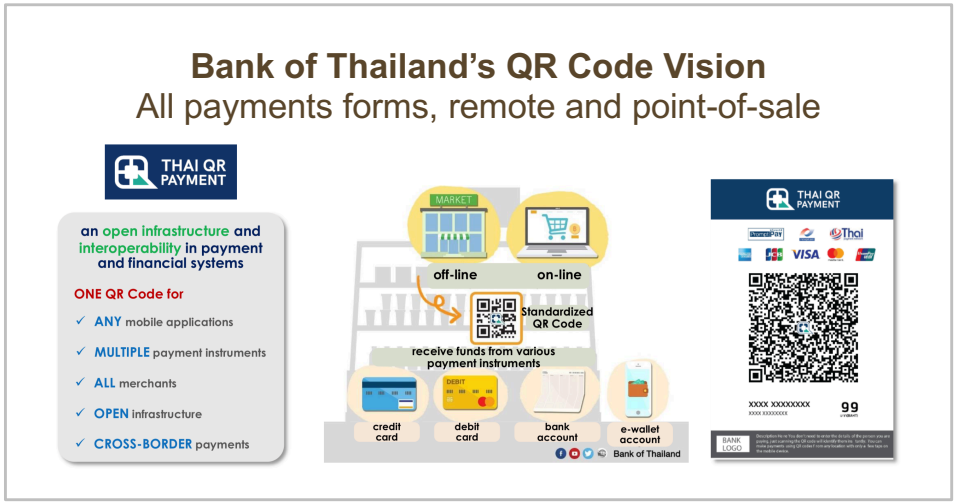



## A Shared QR Code Model with a Dominant RTRP (PromptPay)

Thailand launched a shared QR code payment system in 2017, operated by the Bank of Thailand. This implementation uses the EMVCo Merchant Presented Standards. All information is formatted using TLV and is readable to any scanner.

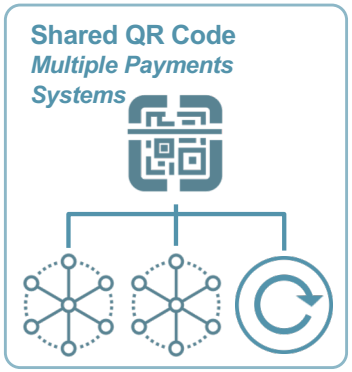
The implementation is for merchant presented QR codes, with both static and dynamic modes supported, as well as the ability to create a request for payment tied to an invoice.

Although the system does not rely on any single payment rail, it does enable payments via PromptPay, Thailand's real time retail payment system. PromptPay is expected to become the dominant underlying payment mechanism used with the QR code implementation.



# Alipay's Implementation with European Wallet Providers

## A Shared QR Code Model Variation




Alipay recently announced an integrated QR code with six European wallet providers.

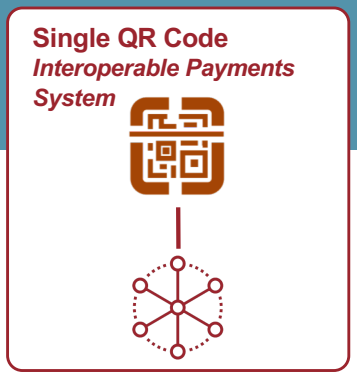
Alipay is using a variation of their China closed-loop model, which uses a URL in the QR code to resolve the merchant payment address. The European implementation uses a URL, but in consumer-presented mode. The merchant's application identifies the customer's wallet type via its URL structure and resolves the payment on the back end. The relationship between the European wallets and Alipay is likely governed by business agreements.

In this implementation, Alipay acts as the Depository, and can manage the other scheme's payments credentials on the back-end: a "referred" data model.

The URL embedded in the QR code creates and embedded user simplification. The QR code will cause the payments experience to launch in the correct app, rather than requiring the end user to choose and navigate to a payments application.

*This model, by using a "referred" data location, should be more flexible and arguably may be simpler as QR code enabled payments move towards a dynamic model. But the other schemes participating have to trust Alipay as the leader of the QR ecosystem.*

# Mexico's CoDi




## A Single QR Code Model Implemented with an Interoperable Payments System

### Payments Systems

Banco de México, Mexico's central bank, oversees the country's domestic payments systems.

In 2004, Banco de México launched SPEI, an open-loop RTRP electronic funds transfer system. The system is owned and operated by the central bank.

SPEI's participants can transfer Mexican pesos by own account and on behalf of their accountholders, in near real-time, 24 hours per day, every day of the year.

### QR Market

Banco de México has begun trials of its QR and NFC Cobro Digital (CoDi) electronic payment system in 2019. The system works by using QR codes to initiate electronic transfers on SPEI rails.

Participation in CoDi will be mandatory system for all Mexican banks above a certain size.

The initial pilot was conducted with employees of financial institutions including BBVA Bancomer, Citibanamex, Santander, Banorte, Banregio and Fincomun.

A handful of wallet providers, such as Mercado Pago, have also introduced closed-loop payment QR codes.

# Mexico’s CoDi

## A Single QR Code Model Implemented with an Interoperable Payments System

### Single Scheme, Open Loop

Mexico’s CoDi QR payment system runs on top of the RTRP “rails” of Bank of Mexico’s SPEI system, which has been in operation since 2004

SPEI is both the RTGS wholesale payment system and the retail real-time payment system. Transactions are credit-push, real-time, and use gross settlement.

The Bank of Mexico provides the notification service for all QR payments, including on-us transactions.

### Proprietary Data Format

Data objects contained in CoDi QR codes are formatted using specific, proprietary rules. They do not follow any international standard. All information contained in the QR code is encrypted; Banco de Mexico provisions shared symmetrical keys with the relevant parties.

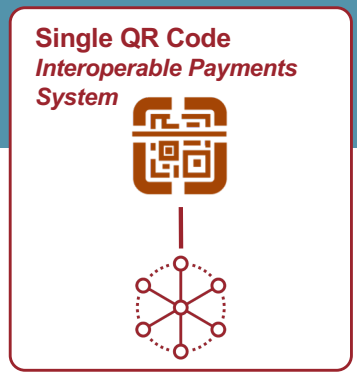
This means that every CoDi payment message must pass through Banco de Mexico.

CoDi is part of a major new initiative to reform and extend the financial sector in general:

The project, which touches on technology, services, market incentives, fees and financial inclusion, is the product of months of discussions between the heads of Mexico's private financial institutions, the central bank and the incoming finance ministry.

BN Americas, January 2019

# Mexico's CoDi




- CoDi is Merchant Presented, with Dynamic and Static Capabilities
- The merchant's CoDi app either generates payment message with full transaction details (amount and reason for payment) – OR – presents a static QR code to consumer.
- Banco de Mexico serves as as the CoDi "Administrator" and requires certification for merchants and service providers. It also maintains a legal agreement with merchants on CoDi usage.

## NOTABLE:

- CoDi began pilot testing to begin operations in April 2019. All banks must be capable of receiving CoDi payments by September 30, 2019, and banks with > 3,000 deposit accounts must have app certified and in market.
- The central bank of Mexico, as operator of the system, prohibits banks from charging merchants or consumers for transactions below a set value. Bank of Mexico has indicated that suppliers of the CoDi functionality will be allowed to charge customers for additional or associated services.
- CoDi plans include integration of NFC payments: this would enable consumers to "tap to pay" as well as "scan to pay"

# China and QR Codes

**Payments Systems**

China's population is heavily banked, and the national payments systems are well developed and tightly regulated.

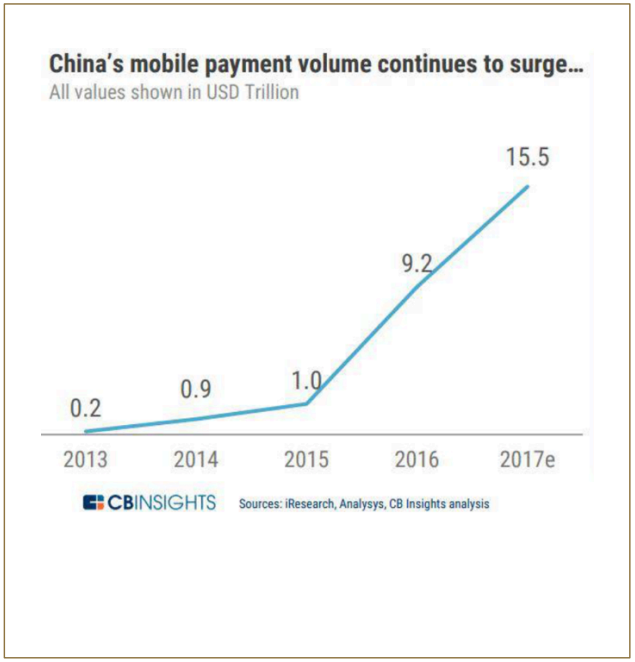
The People's Bank of China (PBOC), the country's central bank, passed reactive regulation in 2017 requiring all digital payments to clear through its platform, Wanglian. This data flow allows the government to monitor domestic money movement.

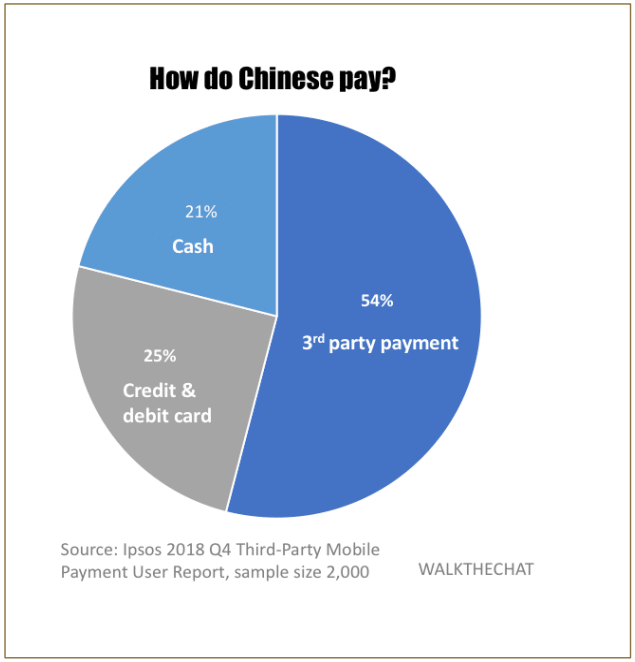
**QR Market**

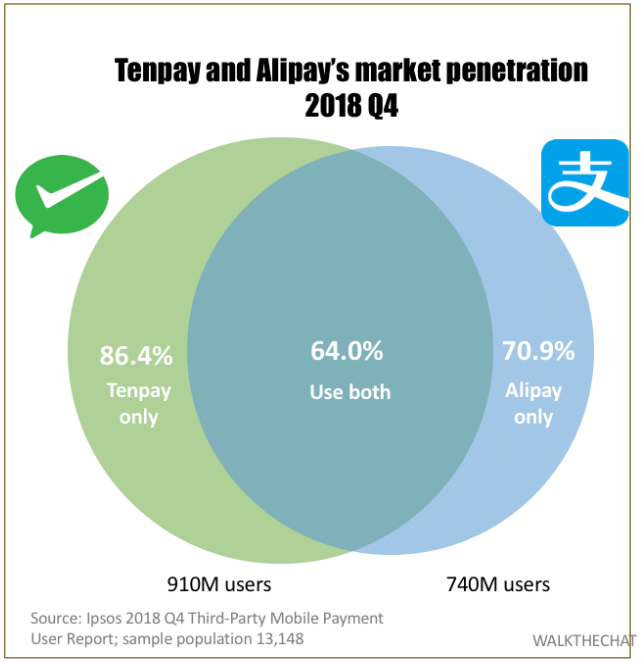
- China is arguably one of the most heavily penetrated QR markets globally, particularly in its urban centers. Penetration and usage are so high that merchants outside China are clamoring to enable Chinese tourists to use the payments systems to shop while abroad.
- Alipay and WeChat pay are the dominant QR payments systems in China. Though Alipay has nearly of the domestic 50% market share, WeChat still commands a significant 38%.
- Both Alipay and WeChat pay offer closed loop wallets. If merchants participate in multiple systems, they must display multiple QR codes. Customers can choose which one to scan with their phone. Closed loop wallets are funded by transfers from bank accounts, using the Wanglian platform.
- In 2018, the PBOC passed additional QR payment regulations and enacted daily transaction limits, encryption and verification requirements, data protection, and transaction verification controls. Additionally, all QR payments must be settled via a newly formed QR Code clearing house supervised by the PBOC.

# China's Mobile Payments Volume Growth

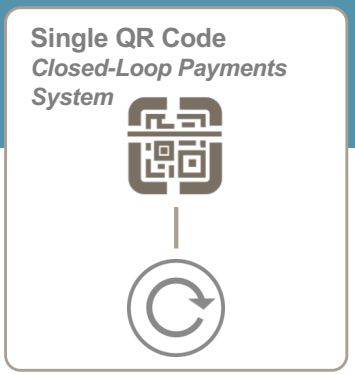
**Alipay (and WeChat Pay) are hugely successful, with QR Code merchant payment a clear enabler.**



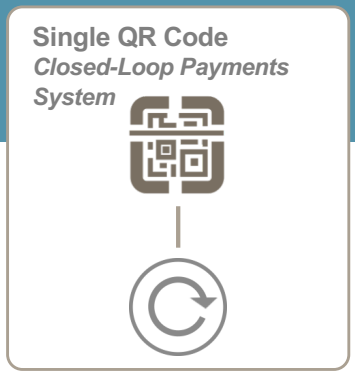
# China's AliPay




## A Single QR Code Model, Implemented with a Closed-Loop Payments System

- Alipay, a payment service owned by Ant Financial, works as a closed loop wallet. The service is run by Ant and only uses national payments rails/infrastructure to load funds in and out of the service.
- Alipay also provides additional financial services ranging from bank account management to insurance.
- QR Codes are mostly merchant presented, although consumer-presented is also supported. QR Codes can be implemented on either a static or a dynamic basis.
- The Alipay QR code contains only a URL; only the company can resolve an encoded web address into a payment instruction. Conveniently, any QR scanning application can read and direct the user to the encoded web address, which then summons the correct screen within the Alipay app.
- Most merchants in China reportedly have both WeChat Pay and Alipay QR codes displayed. The consumer chooses which app to pay with.
- Famously, both payment apps are embedded in consumer "Super Apps" which provide multiple other services – financial and non-financial.

# South Africa's SnapScan



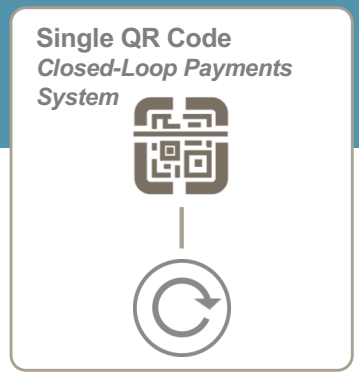

## A Single QR Code Model Implemented with a Closed-Loop Payments System

Launched in 2013 in partnership with Standard Bank

- 50,000 merchants enabled
- 3% transaction fee
- Broad range of merchant use cases incorporated: till point, online, in print (on posters, flyers, parking tickets), bill payment, invoices, etc.
- Both static and dynamic modes
- Allows customer to enter tips
- Also customer to enter "reference" in static mode– can be seen as a bridge towards dynamic QRs


*In 2016, SnapScan announced a partnership with Mastercard, enabling Masterpass wallet holders to scan a SnapScan QR code and effect a payment through whichever instrument is in the Masterpass wallet… making this an (indirect) cross-scheme implementation.*

# Asia's GrabPay




## A Single QR Code Model implemented with a closed-loop Payments System

**A closed-loop wallet introduced by a ride hailing platform**

- ~9 million merchants enabled
- 8 markets
- Static QR code, merchant presented
- Cash-in can be done electronically, or by Grab drivers that essentially function as an agent network
- Partner with local wallets in some geographies to reduce licensing burden
- Grab evolving to super-app model with additional financial services including offering loyalty, credit, and even investing

*Grab's vision is to ultimately create a "single ASEAN eWallet that will deepen financial inclusion for the region's growing middle-class consumers and micro-entrepreneurs."*

*Grab currently offers local wallets in 8 countries in Asia, and launched a remittance offering in 2018. This wallet-to-wallet product allows users to send money to other countries, with instant receipt and access for receivers.*

# QR CODES: FRAUD MANAGEMENT

THE LEVEL ONE PROJECT

# Fraud Risk in QR Code Payments

**All payment systems involve a level of fraud risk, and QR payments are no exception.**



While we cannot predict the future, we believe that some level of fraud is unavoidable; bad actors will attempt to exploit vulnerabilities for financial gain in a QR payment system.

In this section, we will explore some possible fraud vectors in QR payments. Most fraud attempts seen in market to date are, at their core, similar to fraud vectors that are present in other payment systems today. Their primary goal is to effect unauthorized transactions. Importantly, we will also explain the core design decisions that can help a QR payment system prevent these types of fraud.

Though fraud should be a design consideration when building a QR system, they also contain several unique features that help combat fraud more effectively than other payment systems. The presence of a mobile device in the transaction flow enables a system to enact powerful fraud controls including device identification, multi-factor authentication, and geolocation.

QR code scams strike China, from merchants to traffic tickets - Ni…
https://asia.nikkei.com › Economy › QR-code-scams-strike-China-from-me...
May 3, 2019 - TOKYO/SHANGHAI -- **QR** payment **codes**, a mainstay in **China's** cashless society , have presented con artists with yet another avenue to secure ...

# Securing QR Code Payments

QR codes present some unique security advantages compared to other instruments. Whether the QR code is merchant or consumer-presented, at least one of the transaction participants must use a mobile device. Either the central repository or an individual scheme could validate the transaction using one or more of the data points below:



### Device Identification

Every mobile device has unique characteristics that can be used to fingerprint, or identify, it within a reasonable level of certainty. If this information is recorded by a scheme or repository, it can be used to block or flag potentially fraudulent transactions.



### Multi-Factor Authentication

Increasingly, mobile devices use a biometric or PIN based authentication mechanism to allow users to control device access. QR based payment apps can leverage these built-in authentication mechanisms, or require users to set an additional, app-specific PIN.



### Device Geolocation

Mobile apps can be designed to monitor the device's location using methods such as GPS or cell-tower triangulation. This data can be submitted along with the payment message to ensure that the location of the transaction is in pattern with the user's typical behavior.

# Fraud in QR Code Payments: Misdirected Payments

Though QR codes can certainly increase some aspects of transaction security, they also present some security challenges. The the two-dimensional matrix format was not designed to be readable to the human eye and could allow bad actors to avail themselves of novel fraud vectors.

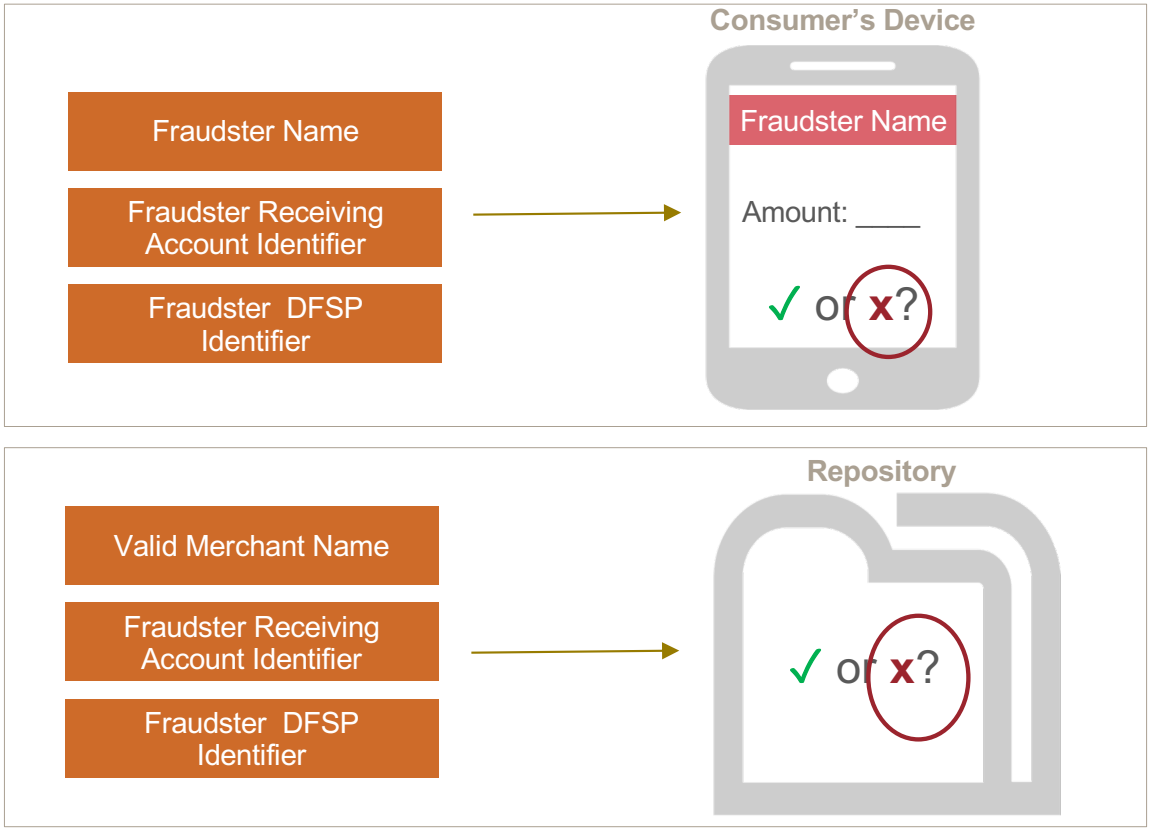
### Misdirected Payments

In static QR codes, bad actors can simply cover a “good” QR code with a fraudulent QR code that directs payments to them, rather than the intended merchant.

This type of fraud requires more technical sophistication to enact in a dynamic QR code environment. Fraudsters must gain control of the merchant device to redirect the payment.

One way to address this problem is a strong notification system with a verification step. However, in an irrevocable credit-push environment, the notification might come too little too late.

# Misdirected QR Code Payments: Mitigation



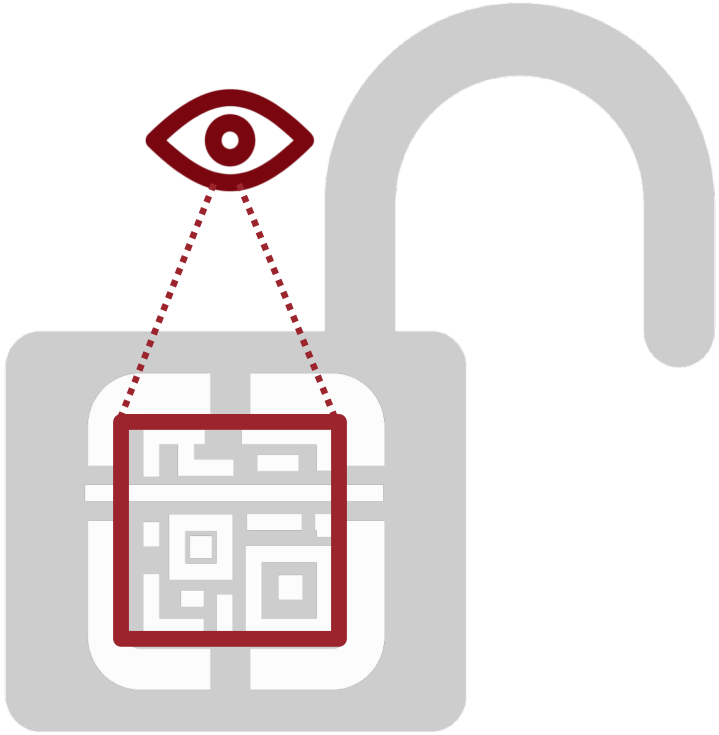

## Basic Control: Consumer Validation

- If data objects are available directly in the QR code, the app can be designed to display the encoded merchant name along with the transaction confirmation message. Upon seeing the wrong name, the consumer can decline the transaction.

## Enhanced Control: Repository Validation

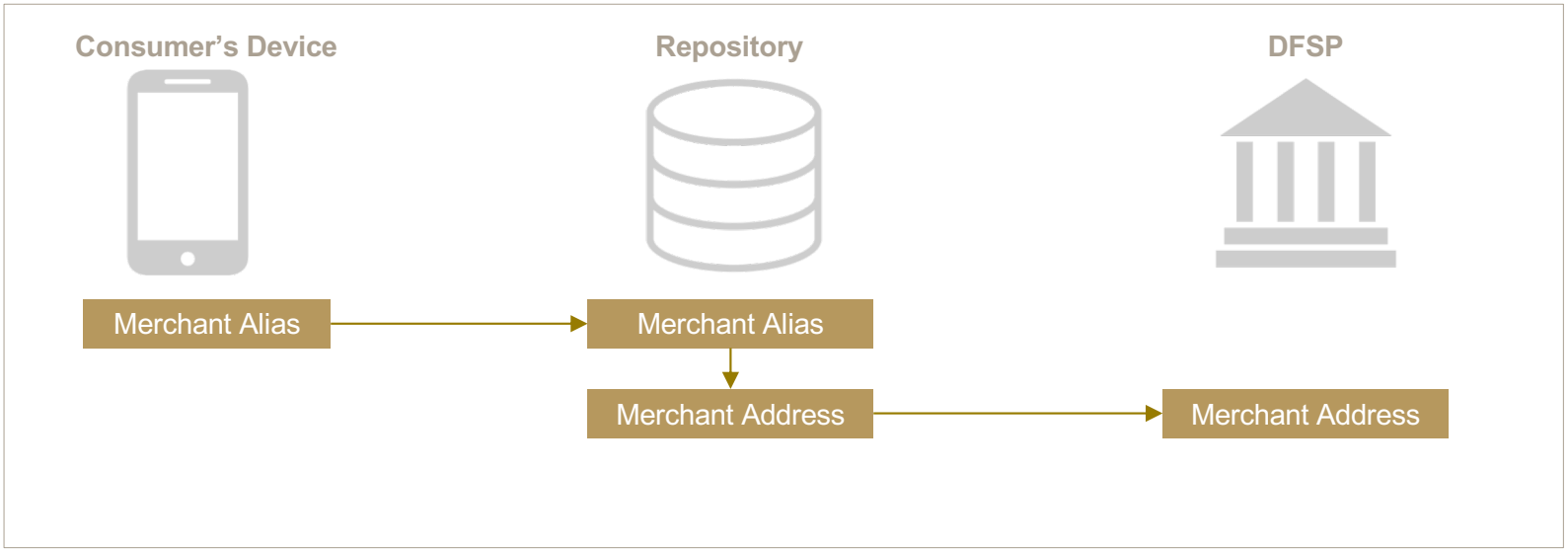
- If the data objects are available in a readily manipulated format, the fraudster could alter the payload to include the real merchant's name with the fraudster's address. However, if a central repository exists, it can be used to validate the payment by interrogating the hash or digital signature.

# Fraud in QR Payments: Exposing Sensitive Account Information



- QR codes are formatted based on internationally recognized ISO 18004 standards. Any information directly encoded into the QR can be read by any readily available QR scanner.
- Therefore, if the underlying data string contains sensitive information, anyone who reads the code can capture that information.
- This is not a risk if the information revealed could only be used to receive payments e.g. a credit-push only system. However, if the same information could be used to debit the account, it presents a security concern. Tokenization, if properly implemented, can manage that risk.

# Exposing Sensitive Account Information: Mitigation



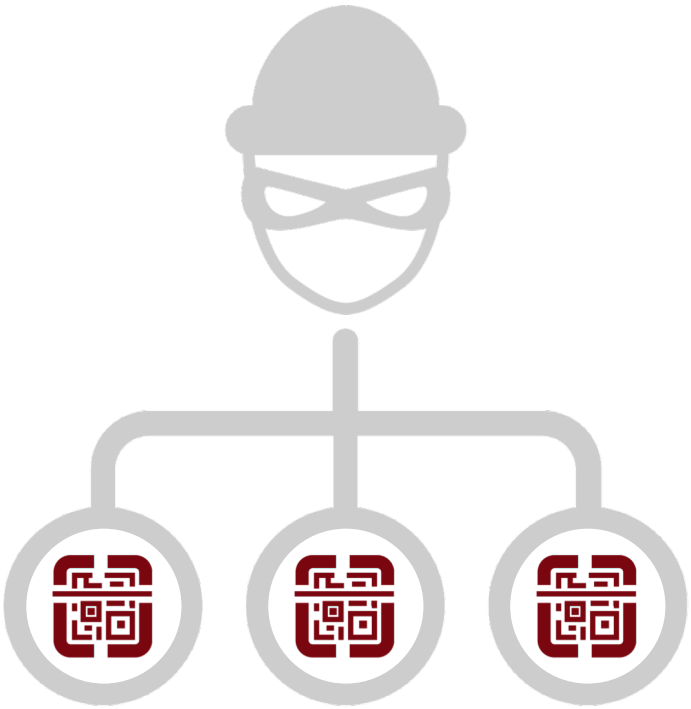

The QR Code repository can serve a directory role to aid in masking sensitive account information. Instead of encoding the information into the QR code, the QR would only contain an alias. At some point in the transaction, the message will flow through the repository which will "translate" the alias into the data format required to route the transaction correctly.

# Fraud in QR Payments: Redirecting Scanner to a Malicious URL

- Particularly for QR payments that use a URL or URI data format, users may become accustomed to scanning the QR code directly with their camera app.
- In this case, a fraudster could maliciously direct the users to a URL that is outside of the payment service. Fraudsters could do this to either:
  - Mimic the login interface of the payment service, in a phishing-like attack that gathers the user's login credentials
  - Install malware on the user's device to force payments, or track the device

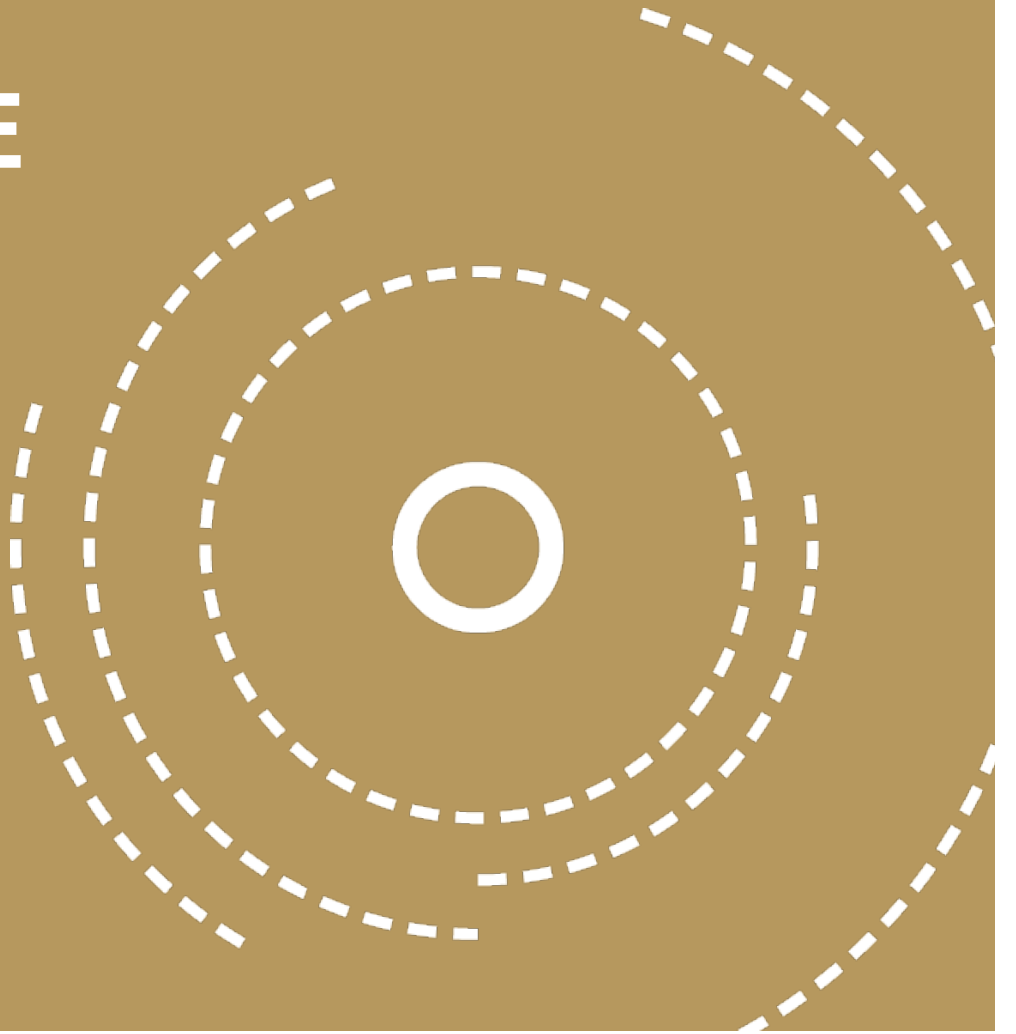
To mitigate malicious URL risk, the app should contain functionality to recognize valid URLs that are set up with the appropriate structure and parameters. Printed QR codes can also include standard counterfeiting controls such as foil over or other anti tampering features. Lastly, it is critical to educate users on the risks involved with scanning unknown URLs and reviewing them for suspicious elements before visiting them.

# Fraud in QR Code Payments: Fraudulent Merchants Scamming Consumers



- Scamming is a very common occurrence in the developed world with card payments. Fraudulent merchants sell false or damaged goods – or – in a remote commerce scenario – fail to deliver at all. Ponzi schemes are another variation of this.
- Closing fraudulent merchant accounts is fairly easy to do. But the fraudulent merchant will often simply open another merchant account. This may be within the same payment scheme, or in another scheme.
- The best mitigation for this is a persistent merchant identity, that can "see" the same bad actor when they pop up with a different account.
- Single RTRP schemes, and QR Code Repositories in shared QR implementations, have the opportunity to implement this. Tying it to biometric national identity of business owners is a further step that can address this type of fraud.

# QR CODES: FUTURE DIRECTIONS



THE LEVEL ONE PROJECT

# QR Code Payments: Future Directions

**QR Code payments are gaining traction rapidly worldwide. By many measures, however, they are in their infancy. The following considerations may influence their forward path:**

- How broadly will merchants adopt QR codes? Will adoption be greater for dynamic QR codes, that allow merchants to integrate payment receipt data into their sales systems? Logically, medium and larger merchants will do this – but will small (and poor) merchants begin to adopt this in scale, or will they remain with static QR codes?
- How will the integration of dynamic QR codes and "request to pay" messaging happen? Either will allow online and remote merchants to enable customers to pay in ways that integrate with their sales systems: but will these be parallel paths, or two ways of doing the same thing?
- At the point of sale, will merchants accept both NFC "tap and pay" payments and QR code payments? Will these be integrated into merchant acceptance services? How will consumer preference play out here?

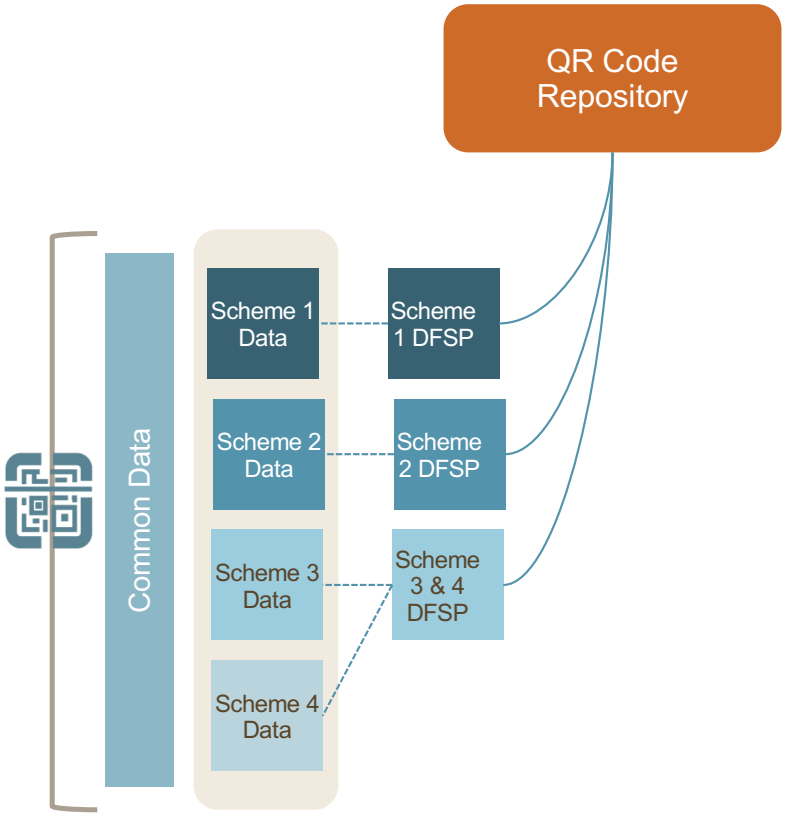
*In the developed world, the EMVCo "Secure Remote Commerce" standard is creating a "virtual payment terminal" allowing remote merchants to effect one integration to accept a variety of consumer payment wallets.*

*How might this complement or converge with QR code payments at the point of sale? In the online domain?*

# QR Code Payments: Future Directions and Questions

- Will the EMVCo member organization evolve to accept true interoperable QR code payments by supporting URL or URI formatting approaches?
- Today, there is a spectrum of control by schemes over consumer and merchant payments apps. How will this play out in the future – and how will it advantage (or disadvantage) the single-scheme vs. shared QR approach?
- What role do OS platforms play in helping to secure the system by verifying or otherwise securing the connection?
- Will cross-border QR payments work? This appears to be an objective of the EMVCo standard, but we note that each country appears to be implementing a somewhat customized version of this – which could hamper the ability to make this happen

# QR Codes: Future Directions and Questions




**Does the QR Code Repository Become a "Meta-Scheme"?**

The shared QR code model appears to be dominating in implementations world-wide. How will the role of the QR Code repository evolve? Will it become a center for meta-scheme fraud detection and control? If so, will the underlying payment schemes need to concede rules authority to the QR Code repository? Will single-scheme implementations have an advantage here?

.

# QR Code Variants

**Two initiatives have introduced QR Code like form factors for closed-loop wallets. Will these be more attractive to consumers?**

These initiatives enable a deep connection between the user and the merchant or platform, enabling far more than transactions.

The graphic that is rendered is based on proprietary standards rather than the standard ISO QR formatting conventions. Because of this, these codes can only be used to initiate payments using the closed loop system. Furthermore, the information they contain is unreadable to an outside party unless the company chooses to release the formatting conventions used

**Amazon Smile Codes**

"SmileCodes will allow you to instantly use Amazon benefits wherever you've scanned the code. So, if you visit an Amazon Locker, you might see a SmileCode that offers you the ability to retrieve the secure code for that locker. SmileCodes will reportedly also be used for things like getting a discount in Amazon Restaurant. Obviously, the opportunities are endless. We may even see these on Amazon boxes one day."

**Google Spot Codes**

*(Currently only in India)*

A Spot Code is a Google-branded visual code that works similar to a QR code but is unique to Google Pay India.

Users can discover a Spot online or at a physical location, and transact with the merchant easily and securely within the Google Pay app.

# QR CODES: A LEVEL ONE PERSPECTIVE

THE LEVEL ONE PROJECT

# THE LEVEL ONE PROJECT VISION

## What is the Level One Project Vision?

- The Level One Project is a vision for a new digital payments platform that supports inclusive, interoperable digital economies. Level One-aligned payments systems need to meet key user requirements:


To meet these requirements, a Level One Project-aligned payments system needs two core features:

- ***Interoperability***, enabling any licensed provider of transaction accounts in the country to connect to the system
- ***Low processing costs*** to the transaction account providers. This makes it possible for the providers to charge zero or near-zero transaction prices to their customers. Level One anticipates providers making most of their revenue through financial or commercial adjacencies.

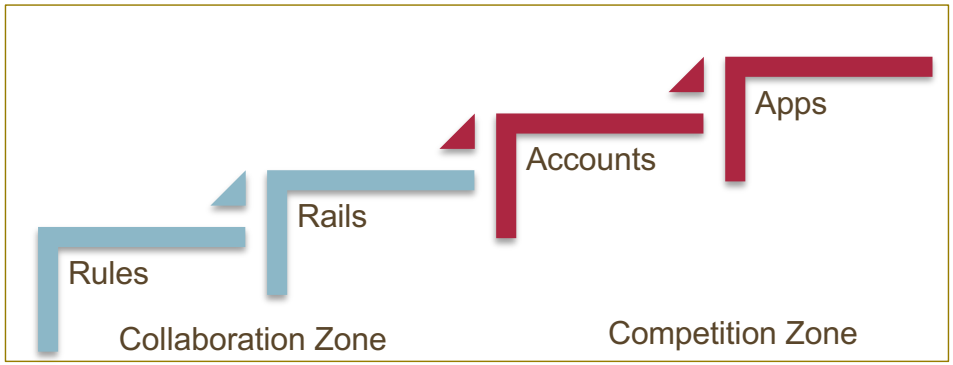
# How do the QR Code Payments Models Align with the Level One Project vision?

- At a high level, all of the models are supportive of the basic goals of the Level One project. In particular, ”waking up” merchant payments in many markets which have previously been exclusively cash-based is a very good development. It has the potential of moving consumers using these payments into a state of ”digital liquidity” – where they are content to leave money in digital form, rather than “cashing out”, because the digital form of their money is now spendable.

- We also note that in many (but not all) of the implementations that merchant payments are free to both consumers and merchants. This is a highly Level One aligned development.

- Other aspects of the QR Code implementation models need to be looked at more closely, to determine whether or not they support the broader goals of a digital payments ecosystem that will support the poor.

# The collaborative-competitive spectrum




- A key foundation of the Level One concept is the belief that the right collaborative-competitive spectrum is essential to develop the long term financial ecosystem of a country.

  This model holds that collaboration is appropriate on the “rails” and “rules” of a payments ecosystem; and that competition should occur above those rails, on “accounts” and “apps”.

*more aligned* ← → *less aligned*

**Single-Scheme QR Code implemented with an interoperable payment system: strong alignment based on the underlying RTRP system**

**Shared QR Code: may include some Level One aligned systems and other non-aligned systems.**

**Single-Scheme QR Code implemented with a Closed Loop System: not aligned**

# Comparison of Implementation Approaches and L1P Principles

| | QR Code Market Model | | |
|---|---|---|---|
| **Level One Design Principle:** | **Single QR Code,** ***Interoperable Payments System*** | **Shared QR Code,** *Multiple Payments Systems without Dominant RTRP* | **Single QR Code** *Closed-Loop Payments System* |
| *Open loop payment systems* | Yes | Possible | No |
| *Real-time, push payments* | Yes | No | n/a |
| *Pro-poor system governance* | Yes | Possible | No |
| *Cost-recovery model for payment system* | Yes | Depends on underlying payment systems | No |
| *Shared investment in fraud detection and management* | Possible | Repository could evolve to support this | n/a |

# QR Code Payments Pricing to Consumers and Merchants

**Having zero to low end-user pricing for payments (the fees or other charges to consumers and poor merchants) is a foundational goal of the Level One Vision.**

- In most countries, the fees charged to consumers or merchants for payments transactions are most typically set by the providers themselves: the DFSP who is serving each customer.
- In some countries, however, payments authorities are looking at the potential of QR enabled merchant payments and taking steps to set limits on these fees, in the hopes of encouraging adoption.
- In these countries the effective price to both the merchant and the consumer for low-value QR code enabled payments is zero. This may be accomplished by government mandate, by agreement among a group of providers, or simply by market practice.

*The Level One philosophy is that providers will be able to make money by providing services that are adjacent to payments: these may be either financial adjacencies (lending, investment, etc.) or commerce adjacencies (margins on selling goods and services online, enabled by electronic payments.*

# Fraud Management

**A shared investment on fraud at the hub is more efficient than replicating it at each provider.**

- As with any merchant payment system, we need to assume that there will be significant levels of fraud – and attempted fraud – on any QR based payment system.
- A key design principle of Level One is a shared investment in fraud management. The idea is that a centralized service will have access to more data, and can do a single investment in the algorithms and artificial intelligence programs necessary to detect and manage fraud.
- Level One supports scheme-level fraud management in addition to provider-level fraud management. If a country has a national, meta-scheme merchant registry, even further collaborative gains are possible.

*In looking at the various QR Code implementation models, it is clear that centralized fraud management is possible – and planned for – in the single-scheme model. In a shared QR implementation, the central QR repository (if there is one) could become the place for centralized fraud reporting, at least on an after-the-fact basis.*

# The Digital Mainstream

**Electronic merchant payments may help consumers – and merchants – become part of the digital mainstream.**

- Developed and emerging economies alike share an enthusiasm for the idea of a digital economy: an ecosystem in which people, businesses, and governments can easily and inexpensively exchange information and transact.
- Emerging economies are particularly concerned that poor citizens and residents are able to take advantage of these emerging ecosystems.
- With this in mind, we can look at the various QR Code implementation models to see how they might scale, and how they might support this vision.

# A Mojaloop Perspective on QR Codes

**Mojaloop is open-source software for financial services companies, government regulators, and others taking on the challenges of interoperability and financial inclusion.**

*The Bill & Melinda Gates Foundation has funded the initial development of Mojaloop code, and continues to support its ongoing development by a community of software and implementation partners.*

- The initial Mojaloop code provides capabilities for schemes (or bilateral partners) to implement secure transfer “switching” and settlement.
- The Mojaloop community is building on this base to create additional capabilities – these include capabilities relevant to merchant payments, including “request to pay” and QR codes.
- Mojaloop has a flexible addressing architecture that supports a variety of merchant payments addressing capabilities
- Depending on the implementation, the merchant’s payment address may be a mobile phone number, and address, or a scheme-specific alias – a “merchant ID”
- In a scheme implementation of Mojaloop, the scheme would exert overall control over the addressing protocol – ensuring uniqueness of addresses and regulatory visibility in merchant identity.

# A Possible Mojaloop QR Code Payment Flow

**This shows a static QR Code, merchant presented implementation. Rather than using EMVCo specifications, this approach uses URI formatting to effect the payment.**


*The consumer has a smart phone app that is enabled for QR code payments for the scheme.*

*The scheme supports centralized merchant registration.*

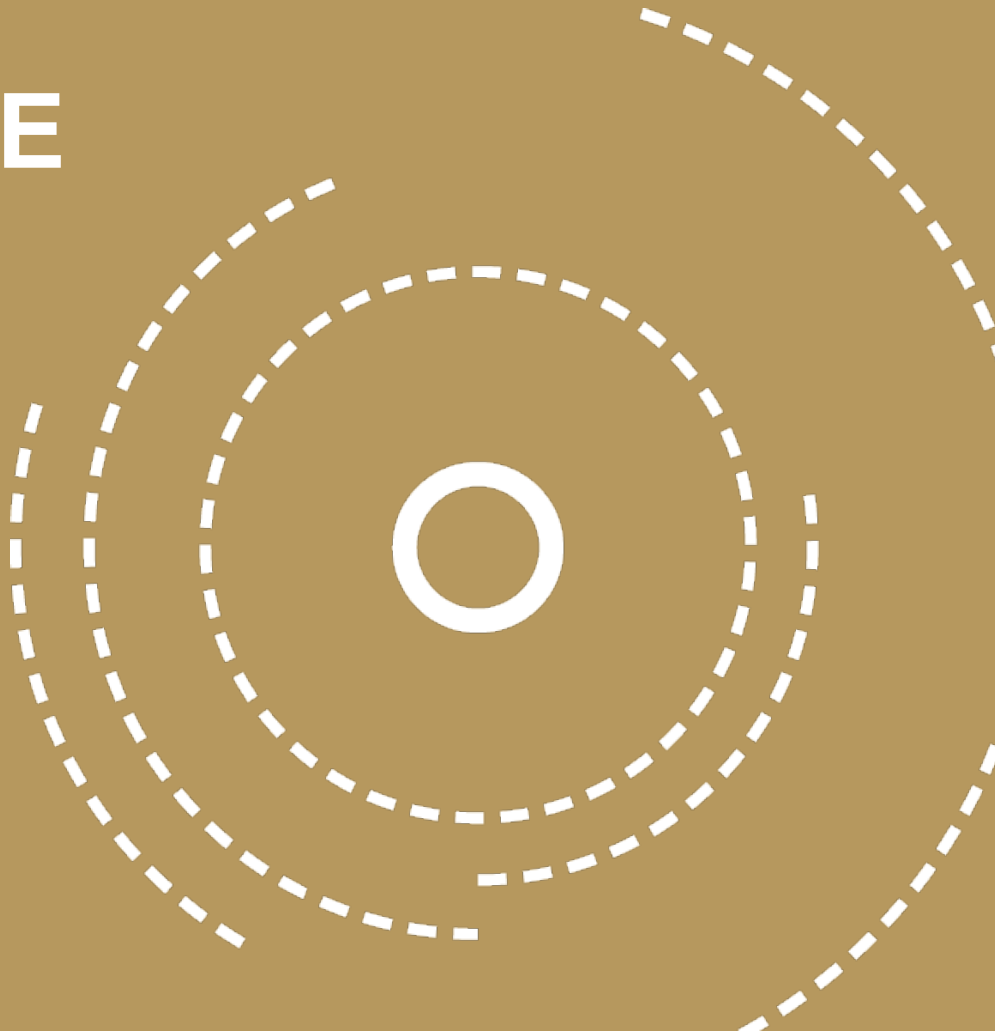
*The merchant has a scheme payment address and a QR code for display which embeds this.*

1. Consumer App Scans Code
2. URI-formatted Message Sent to Consumer DFSP and on to switch
3. Merchant ID Validation process occurs at switch

4. Consumer Enters Amount, payment request is sent by Consumer DFSP to switch
5. Mojaloop Quote Process confirms with Merchant DFSP that merchant's account is ready to receive funds

6. Consumer approves purchase
7. Transfer of funds is initiated by Consumer DFSP
8. Switch manages transfer and settlement process
9. Consumer and Merchant receive confirmations

# APPENDIX: QR CODE FORMATTING



THE LEVEL ONE PROJECT

# QR CODE DATA FORMATTING

**What data objects are included in a QR payment?**

- A QR scheme must establish what data elements are required for every payment message.
- For a static QR code, the data objects typically include:

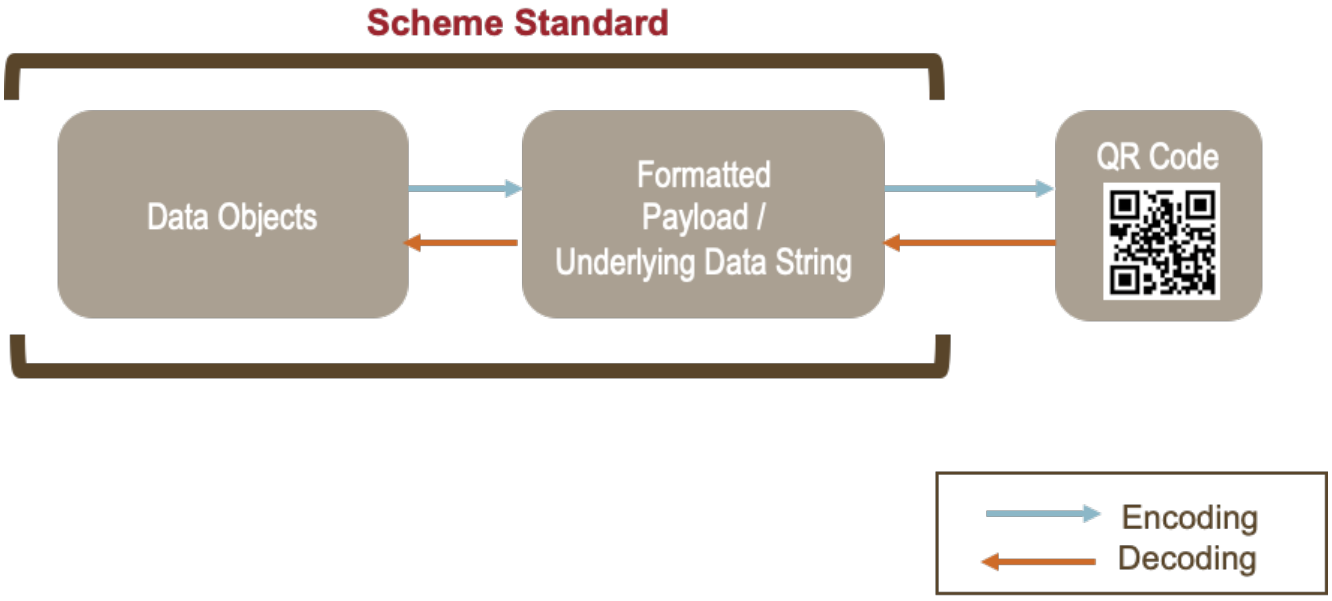
| Receiving Account Identifier | Receiving DFSP Identifier | Payment Network Identifier (for shared QR implementations) |
|---|---|---|

- If using dynamic QR code, schemes can opt to include additional data elements that vary from transaction to transaction:

| Invoice Detail | Order Reference Number | Transaction Amount | Tip Indicator | Data Validation |
|---|---|---|---|---|

# QR CODE DATA FORMATTING

The QR scheme standards dictate the data objects included in a QR payment and how they are formatted. These scheme standards are used to create the formatted payload, which we sometimes refer to as the underlying data string. Like any other formatted payment message, comprehensive standards are key to ensuring all scheme participants can consistently interpret the data and processing and 'action' the payment message.



# QR CODE DATA FORMATTING OPTIONS

**This is what is most commonly meant when discussing "QR Code Standardization". There are various approaches : proprietary, URL and URI formats.**

**Proprietary formats**

- Data objects are formatted using specific, proprietary rules. These may be set by an individual company (as with a closed-loop implementation) or by an industry body or group. the **EMVCo QR standard is a proprietary format, and the most frequently used QR code format in the market today**.
- On scanning, the app parses and validates the data objects, and constructs a payment message.
- The data string produced by the proprietary formatting is available to any QR scanner but can only be resolved by an app which holds the logic to create a payment message

# QR CODE DATA FORMATTING OPTIONS

**URL format**

- This approach uses a global standard for a resource locator to format the payload in the QR code. The data string encoded into the QR code is a URL.
- On scanning, the URL points the scanner to a webpage, which contains code to redirect the user to the intended screen within the payment application on the consumer's phone. The consumer's application then "knows" the merchant's payment address, and is ready to create the payment order.

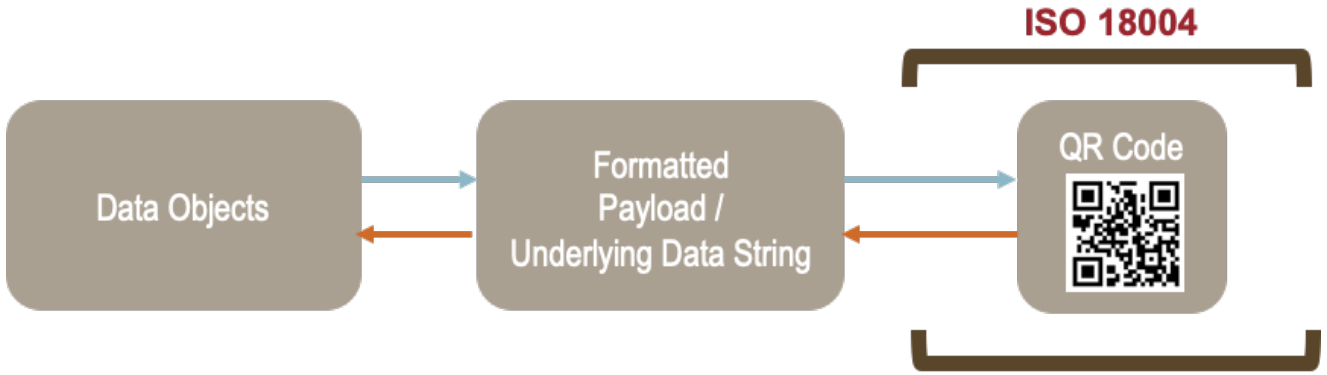
- If it is a static QR code, the consumer will enter the payment amount into the application.
- If it is a dynamic QR code, the payment amount will be prepopulated on the screen the consumer sees, and additional transaction-specific data may also be prepopulated
- Though the URL is available to any QR scanner in plain text, no payment data is directly readable; the payment address is held at the URL location. The consumer app needs to be able to use the address found at the URL location to create the payment order.

# QR CODE DATA FORMATTING

**URI format**

- This approach also uses a global standard for a resource locator to format the payload in the QR code.
- The data string encoded into the QR code is a URI. The data payload, including the merchant's payment address, is in the encoded data string; other data may be in the string or may be held elsewhere, as described in the string. All data in the string is formatted and labelled according to global standards.
- The URI approach allows a consumer to use either a generic reader application or a proprietary payment application. The chosen app parses and validates the data objects, and constructs a payment message.
- The data string produced by the proprietary formatting is available to any QR scanner but can only be resolved by an app which holds the logic to create a payment order

# QR CODE DATA FORMATTING: DATA ENCODING




- Once formatted, the underlying data string is encoded into a machine-readable visual representation using ISO 18004 standards. The results of this process is the familiar form of black squares arranged on a white background.
- When scanned, the imaging device recognizes this visual format and uses a standard algorithm to decode it back into the underlying data string using a standard algorithm

# QR CODE DATA FORMATTING: ENCRYPTION AND HASHES

**Which, if any, of the data elements are encrypted and/or hashed for validation purposes?**

- **QR Code Implementations may either:**
  - Create a hash of the QR code data string. The string is read when the consumer app scans the QR code. If the rules then require the consumer app to validate the data string with the QR code issuer (either the merchant DFSP or, more probably, the central authority – for example, the QR code repository in a shared QR implementation), the QR code issuer can validate that the data string is properly issued and not tampered with.
  - Encrypt some or all of the data elements in the QR code data string: the QR code issuer would digitally sign the elements with a private key; the consumer application would then use a public key to validate the signature. This can be done locally, and does not require the consumer app to connect to the issuer/central authority
- **There is debate within the industry about the merits – or need – for the use of encryption to disguise merchant payments credentials.**
  - This would be a good idea if a card or bank account number – which could be used to fraudulently "pull" a payment – was exposed in the QR data string. However,
  - Merchant payments addresses that are aliases, or tokenized forms of card numbers or bank accounts, arguably cannot be used for fraudulent "pulls" and therefore do not need to be encrypted. It appears that most QR code implementations are taking this direction

For more information about the Level One Project, visit leveloneproject.org

For more information about the Bill & Melinda Gates Foundation's Financial Services for the Poor, visit gatesfoundation.org


Report Authors

Carol Coye Benson, Glenbrook Partners
carol@glenbrook.com

Rebecca Rasis, Glenbrook Partners
rebecca@glenbrook.com

October 2019