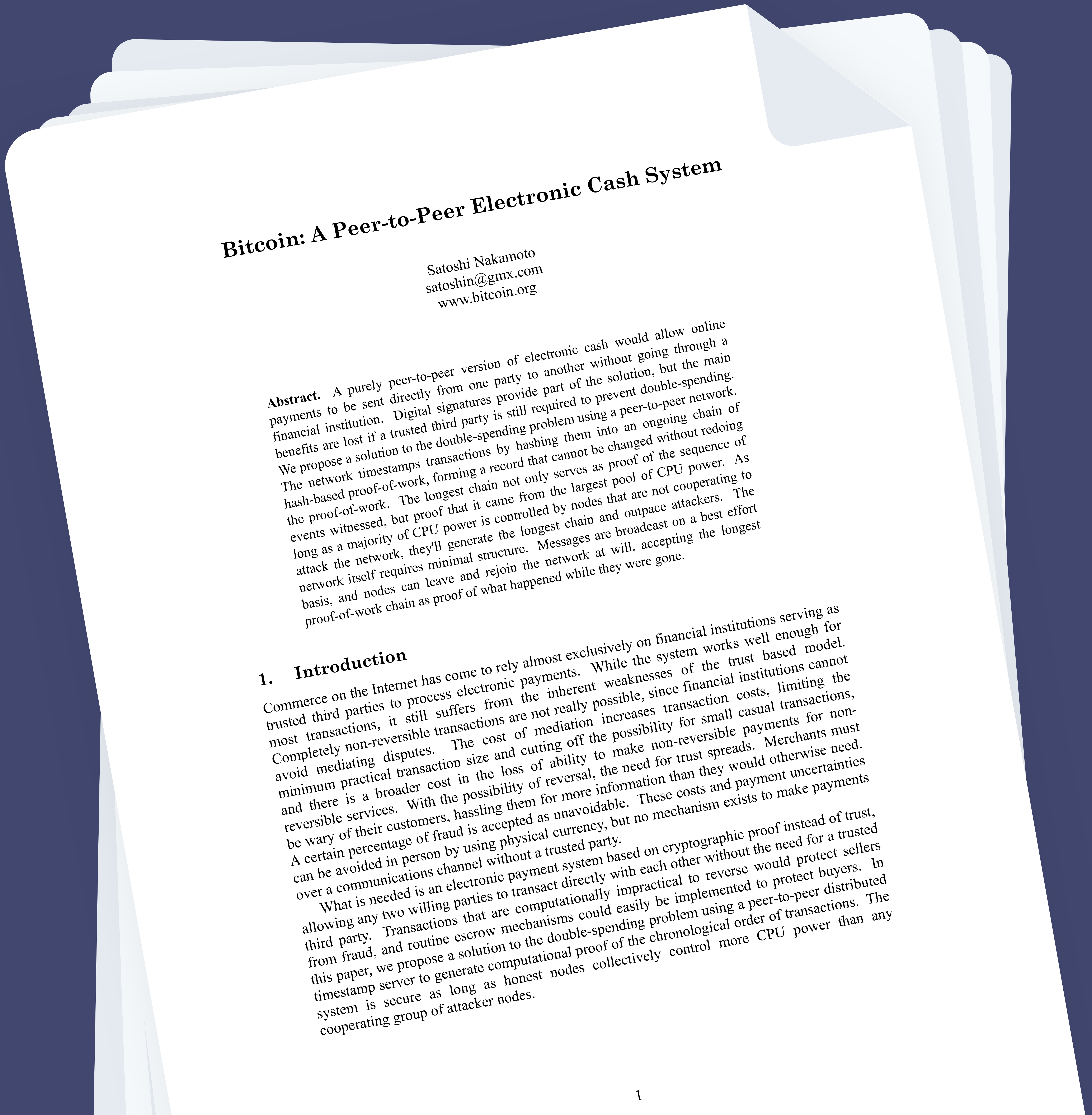
stripe

Florent Tardivel

HEAD OF SALES FRANCE, STRIPE



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

7B+ cards

Largest card network in the world

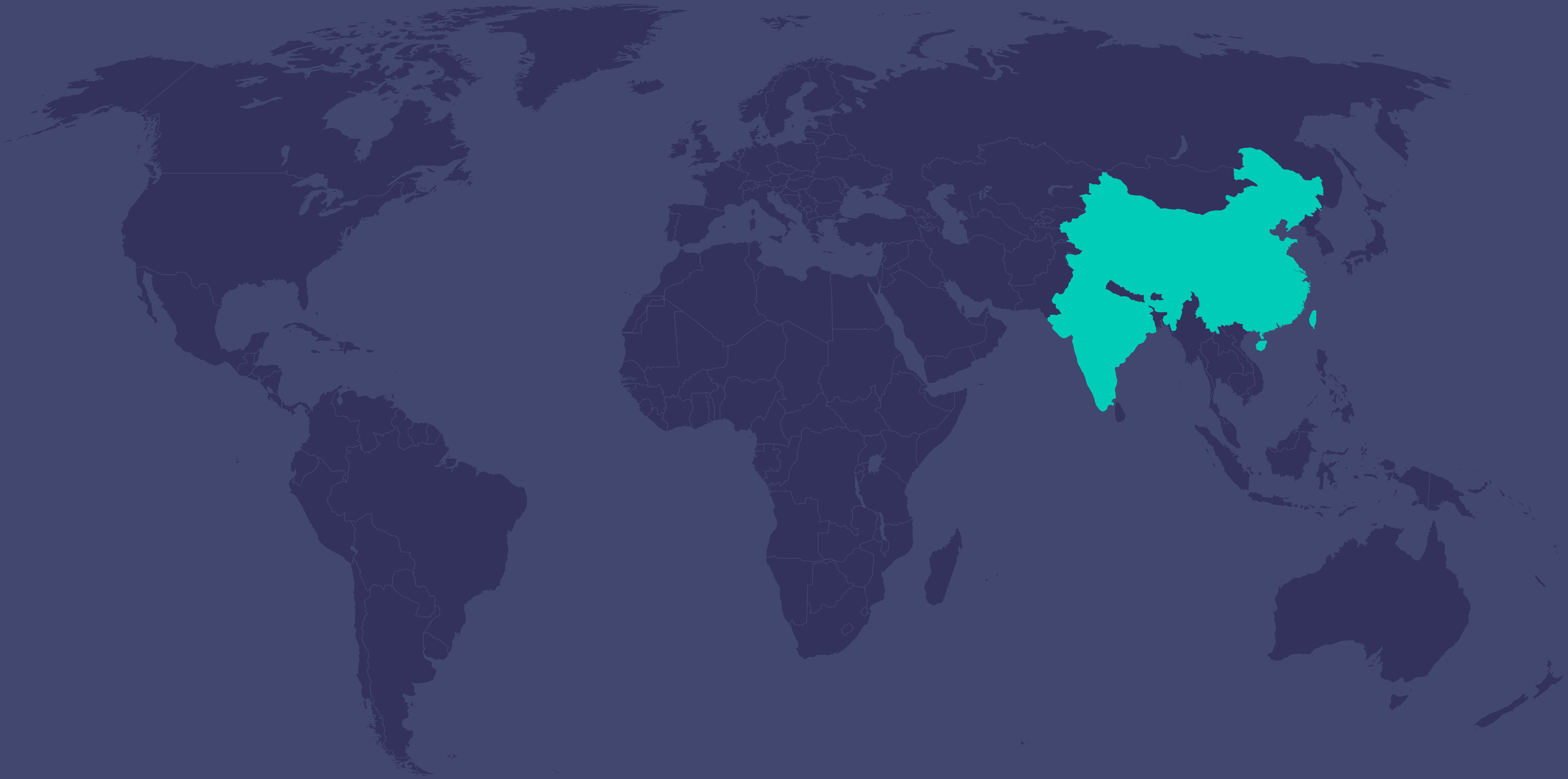
UnionPay 银联

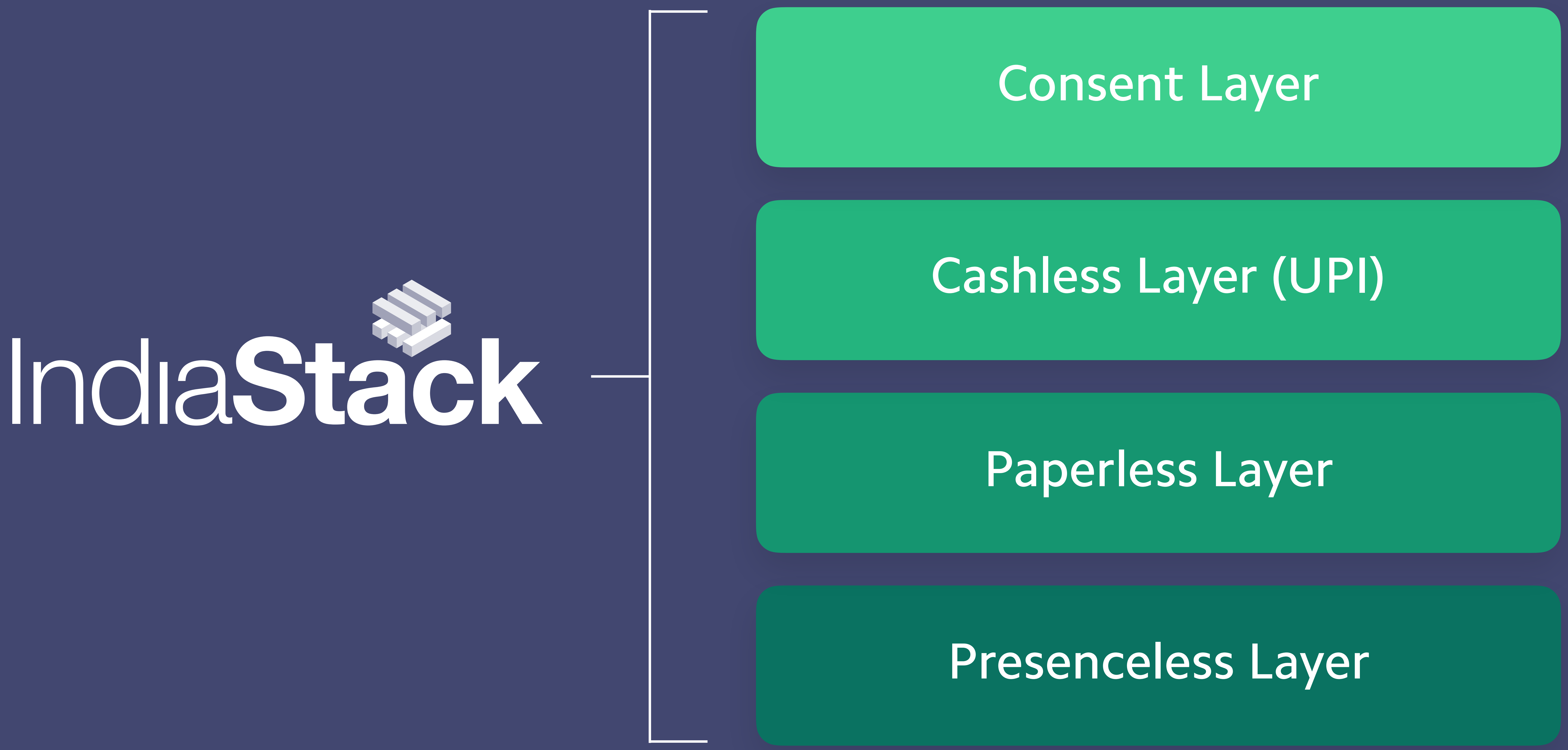
推荐使用微信支付
果诚水果店

1.1B

monthly active WeChat users

- Social network first, payments built on top





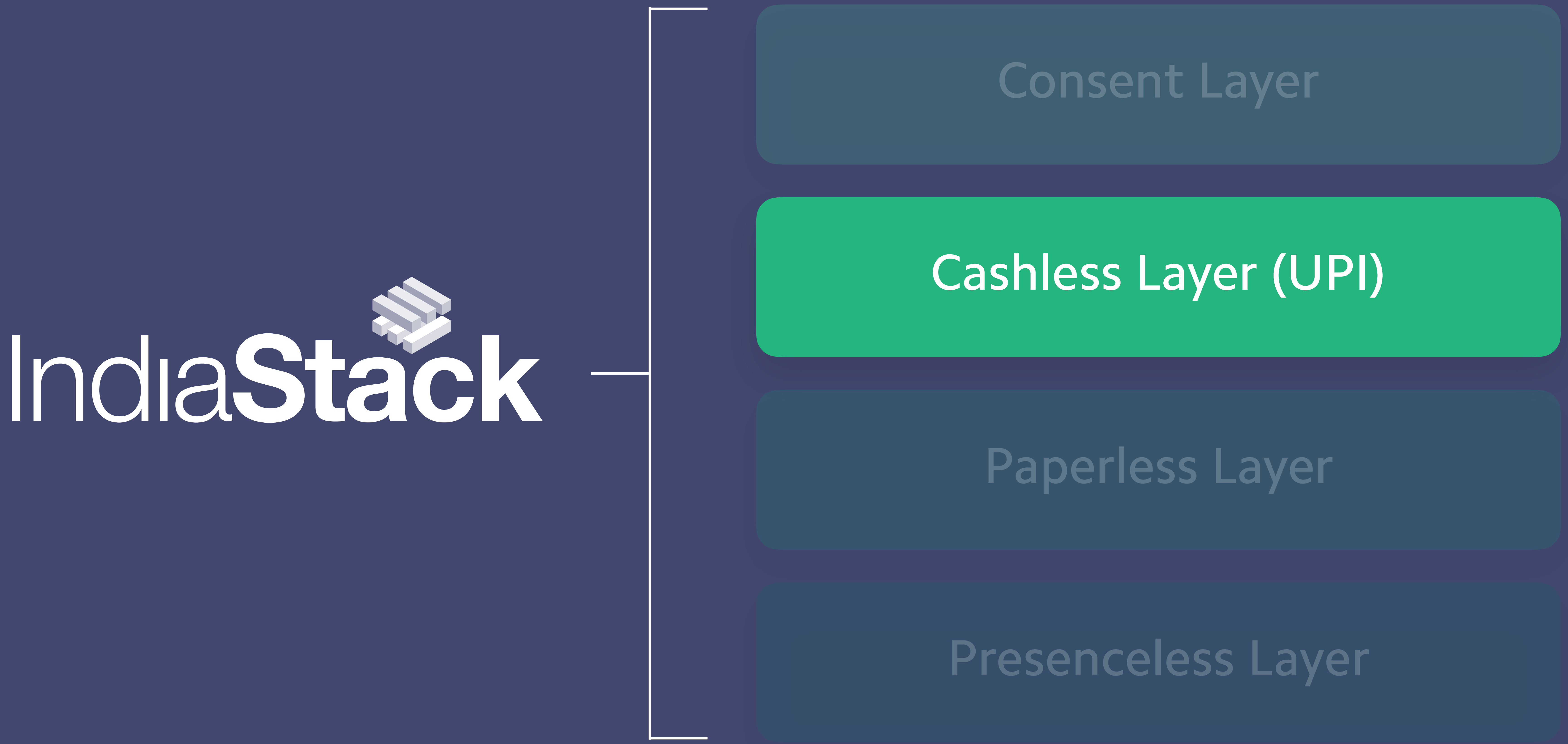
IndiaStack

Consent Layer

Cashless Layer (UPI)

Paperless Layer

Presenceless Layer



IndiaStack

Consent Layer

Cashless Layer (UPI)

Paperless Layer

Presenceless Layer

BENEFITS OF UPI

Public

Interoperable payment methods

Fast

Send payments instantaneously

Cheap

No additional intermediaries taking fees

Available

Open 24/7

TODAY

1.1B People

using the India stack

Cashless

due to demonetization in Nov 2016

$250B

payment volume run-rate

x50

payment volume in 2 years

afaricom
Care Des
m PESA
m PESA
afaricom
Desk

49%

of GDP is processed through M-Pesa

93%

of Kenyans have access to mobile payments

M-PESA

Orange Money

orange

airtel

money

Equitel

My money. My phone. My life.

MobilePay

mobicash

زبان کا پکا

VISA

mastercard.

Cards are dead.

Long live wallets?

venmo
支付宝 ALIPAY
coins.ph
GrabPay
m-pesa

HUAWEI pay
amazon pay
WeChat Pay
JioMoney
NETELLER

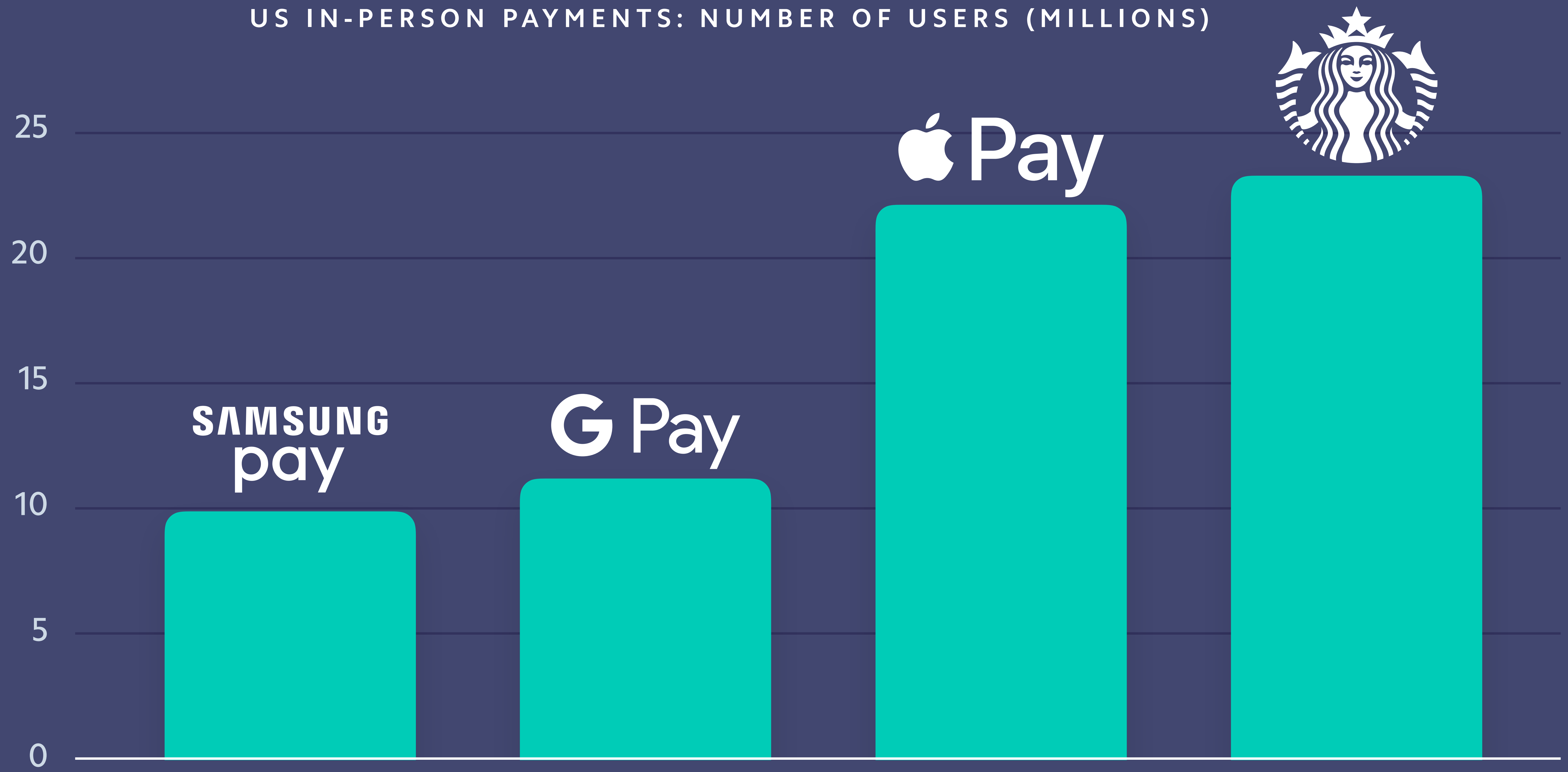
CashApp
PhonePe
masterpass by mastercard
yono SBI

WhatsApp
nexi
G Pay
DOKU Wallet

Zelle
Pay
SAMSUNG pay
gojek
Microsoft Wallet

Square
hike
BHIM
GoPay
PayPal

US IN-PERSON PAYMENTS: NUMBER OF USERS (MILLIONS)



eMarketer 2018

OPEN LOOP

Business-agnostic

CLOSED LOOP

Business-specific

OPEN LOOP

Business-agnostic

SAMSUNG pay

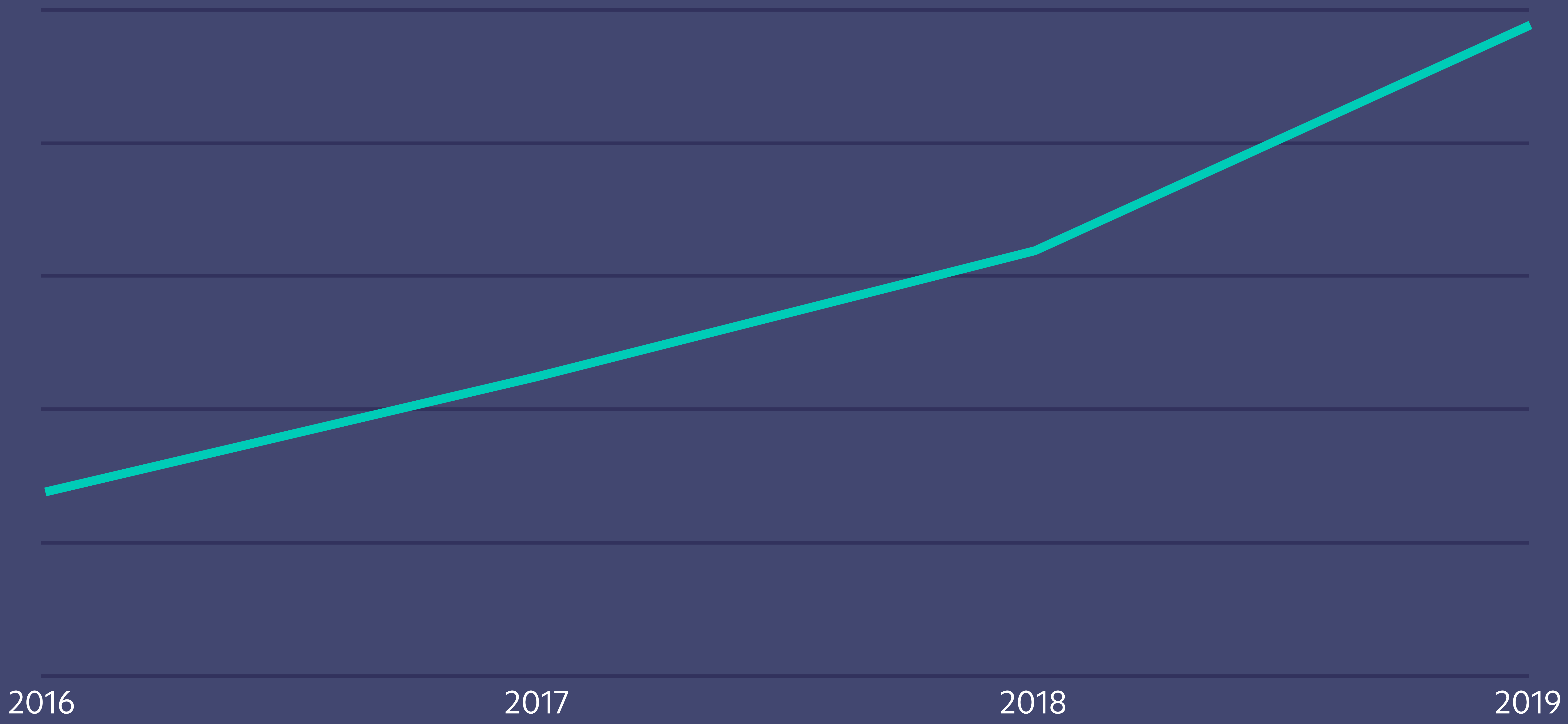
G Pay

Pay

CLOSED LOOP

Business-specific

APPLE PAY VOLUME ON STRIPE



OPEN LOOP

Business-agnostic

SAMSUNG pay

G Pay

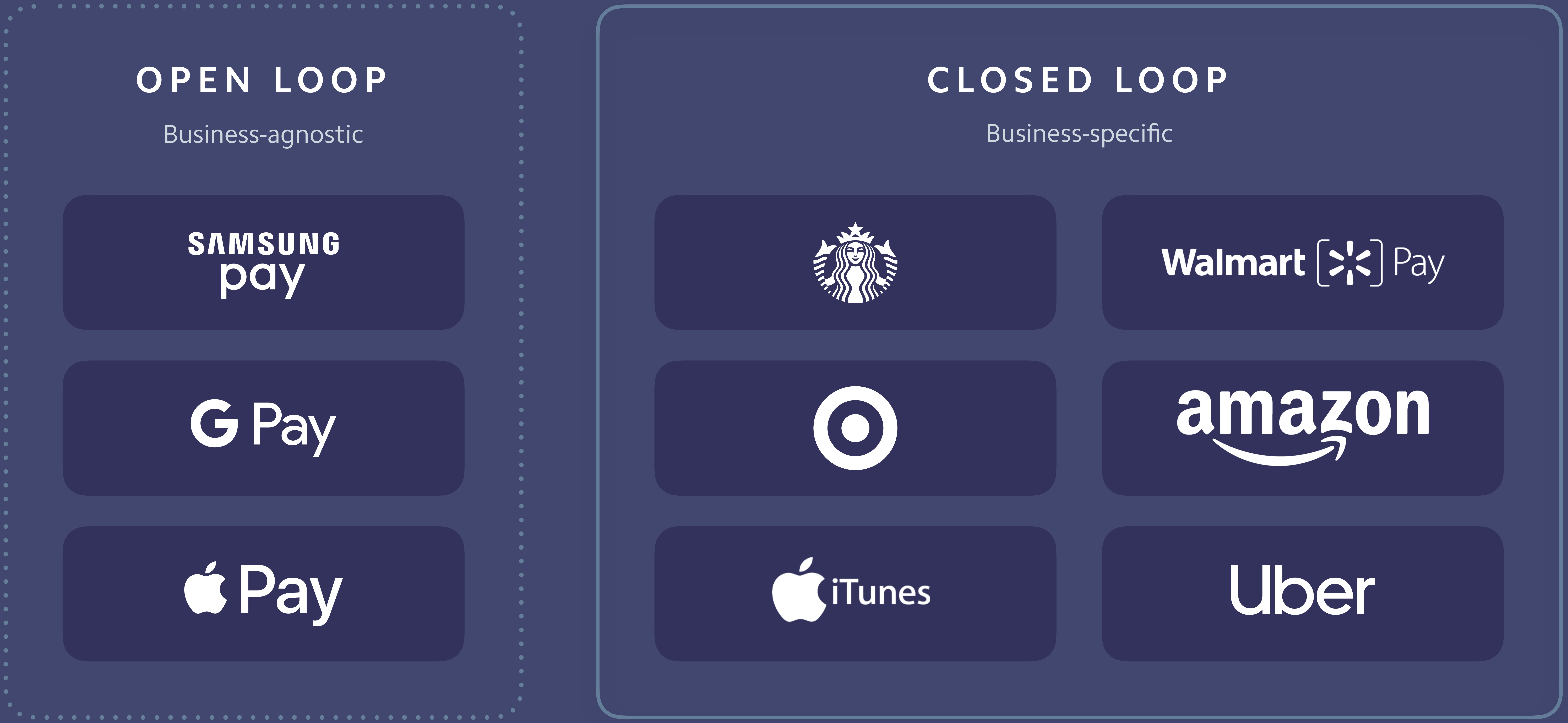
 Pay

CLOSED LOOP

Business-specific

$1.6B

stored value across gift cards and mobile app



OPEN LOOP

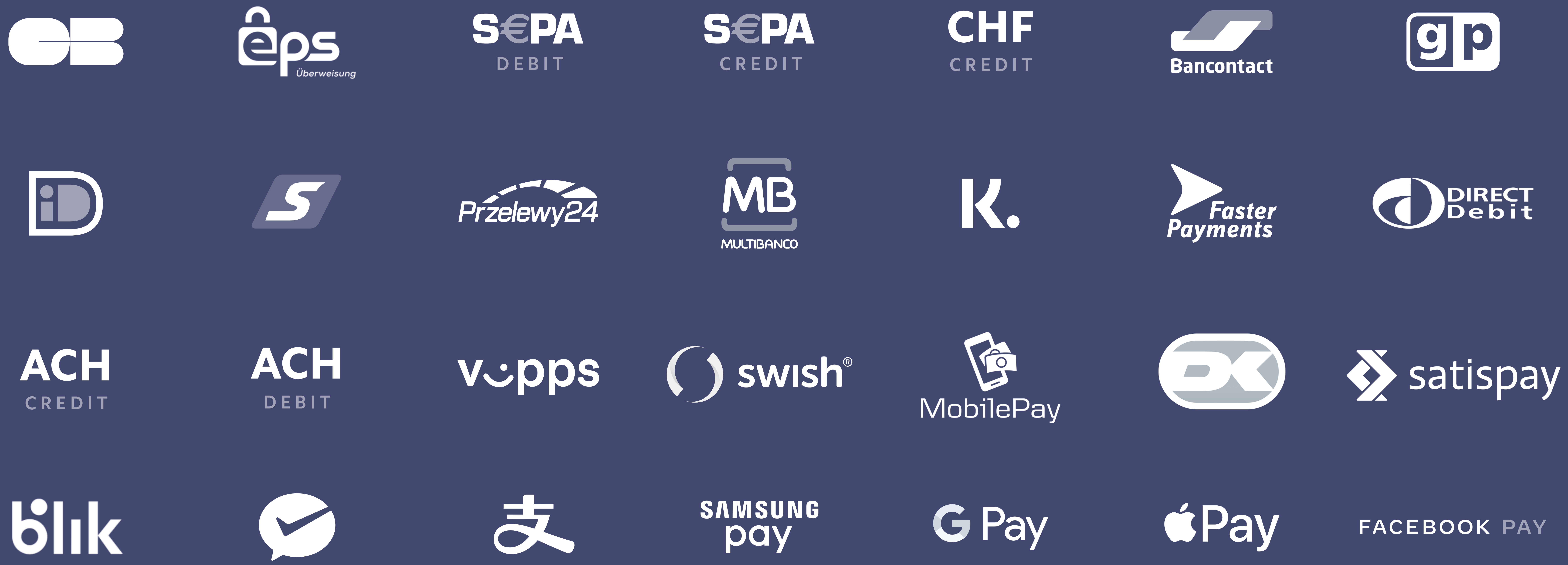
Business-agnostic

CLOSED LOOP

Business-specific

EMV

Standards have made chip and pin ubiquitous in Europe.


CB
eps Überweisung
SEPA DEBIT
SEPA CREDIT
CHF CREDIT
Bancontact
gp
iD
S
Przelewy24
MB MULTIBANCO
K.
Faster Payments
DIRECT Debit
ACH CREDIT
ACH DEBIT
vipps
swish®
MobilePay
DK
satispay
blik
支
SAMSUNG pay
G Pay
Pay
FACEBOOK PAY

European
Commission

The European Commission has proposed a revised Payments Services Directive (PSD2) and a Regulation on Multilateral Interchange Fees (MIFs) in order to **cater to the needs of the European payments market**.

The proposed bills are intended to create **more competition** in the market which in turn should lead to **innovation and higher security standards in the payments environment**.

Strong Customer Authentication

SCA

3DS

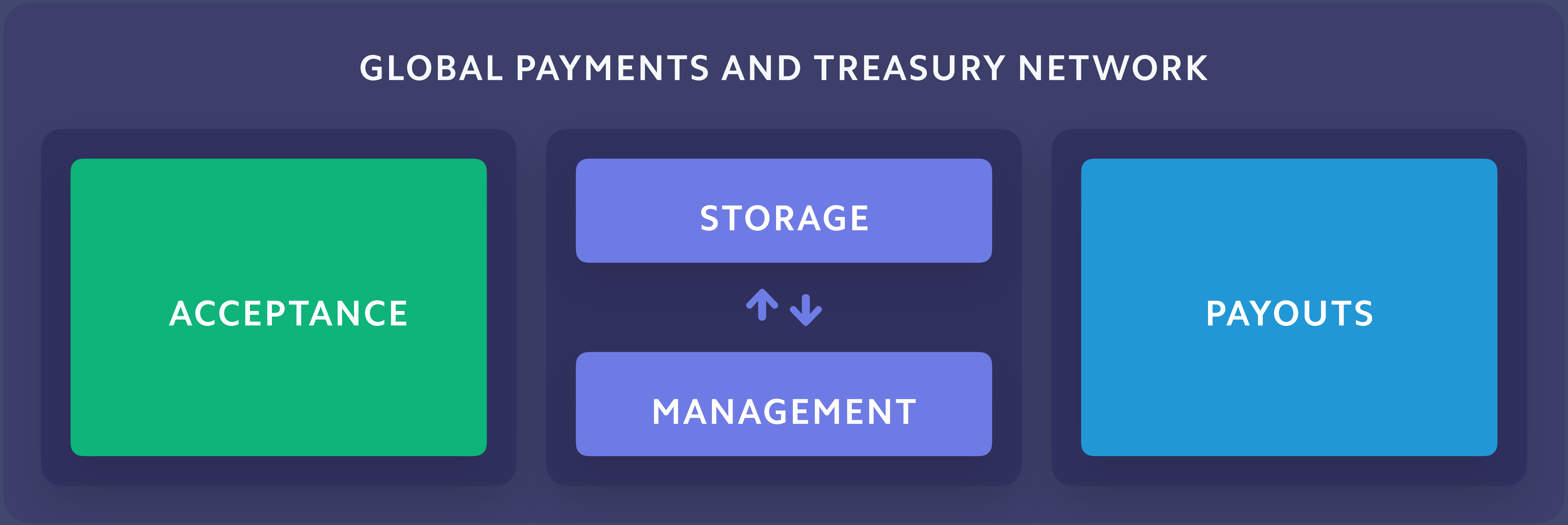
GLOBAL PAYMENTS AND TREASURY NETWORK

GPTN

$USD

🇧🇪

AMERICAN
EXPRESS



GLOBAL PAYMENTS AND TREASURY NETWORK

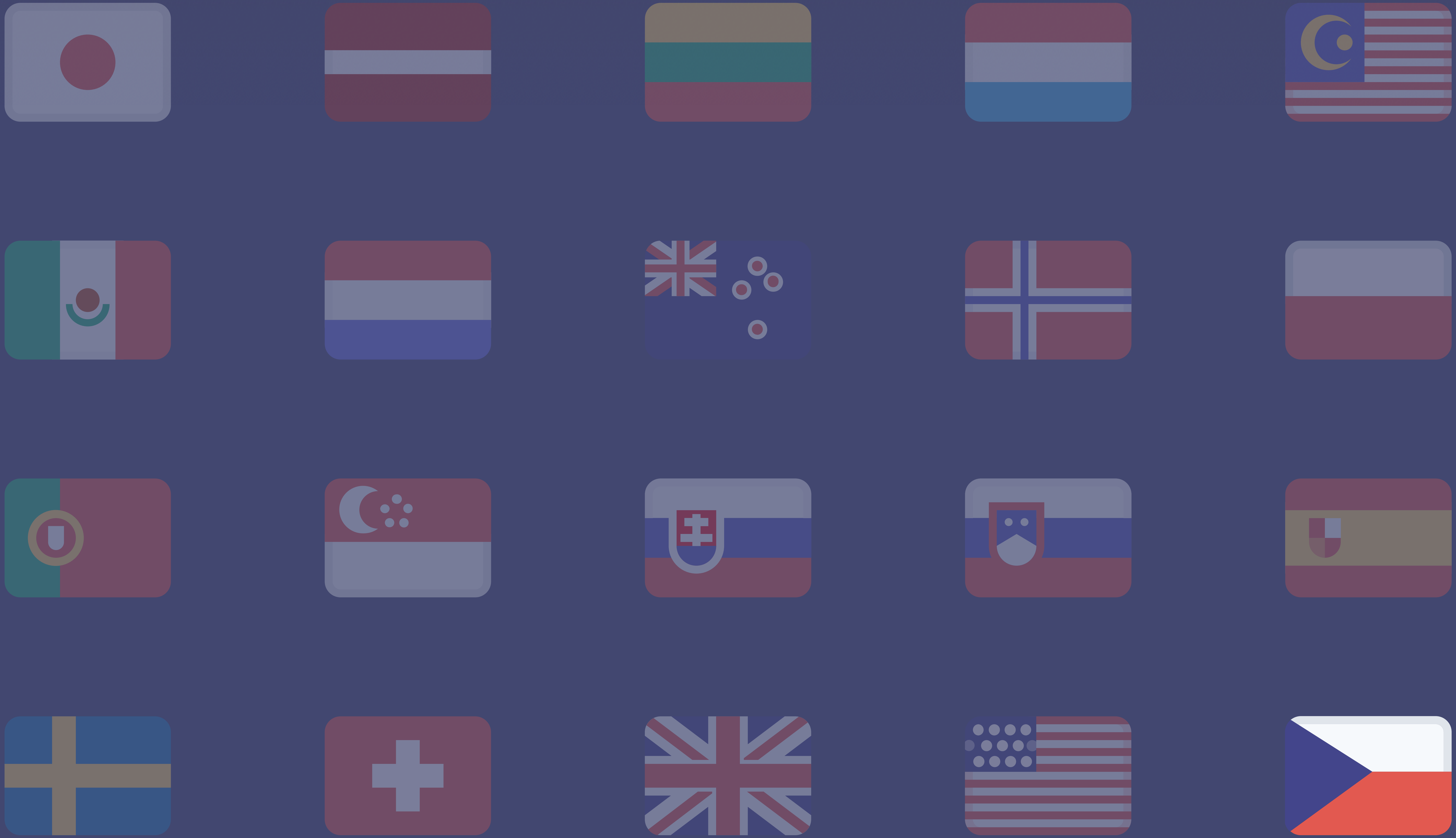
ACCEPTANCE

STORAGE

↑↓

MANAGEMENT

PAYOUTS



GLOBAL PAYMENTS AND TREASURY NETWORK

stripe