

The background features a dark, stylized illustration. It includes a smartphone displaying a payment interface with a card labeled 'MEEP CARD' and a balance of '24810'. Overlaid on the phone is a dark rectangular box with the word 'Payment:' and a progress bar. Surrounding these elements are various icons: a large red dollar sign, a play button, a magnifying glass, and a circular arrow. Dashed lines and arrows suggest a flow or process. The overall theme is mobile payments and security.

Paielements Mobiles : Protocoles, Sécurité et Failles

Aymane AMESSEGHHER
Moataz ER-RAMI

Plan

1. Les paiement mobiles de nos jours
2. Architecture Technique des Paiements Mobiles
3. Les Principaux Protocoles de Communication
4. Mécanismes de Sécurité Fondamentaux
5. Comparaison des Plateformes Majeures
6. Failles Documentées et Cas Réels
7. Perspectives et Enjeux Futurs
8. Démonstration

L'Écosystème des Paiements Mobiles

2.1Md

Utilisateurs mondiaux

Adoptant les paiements mobiles en
2024

95%

Taux de croissance

Augmentation depuis 2019

\$1,68 T

Volume transactionnel

Transactions mensuelles uniquement
en 2024

Source: <https://www.mobileworldlive.com/gsma/mobile-money-accounts-surpass-2b/>

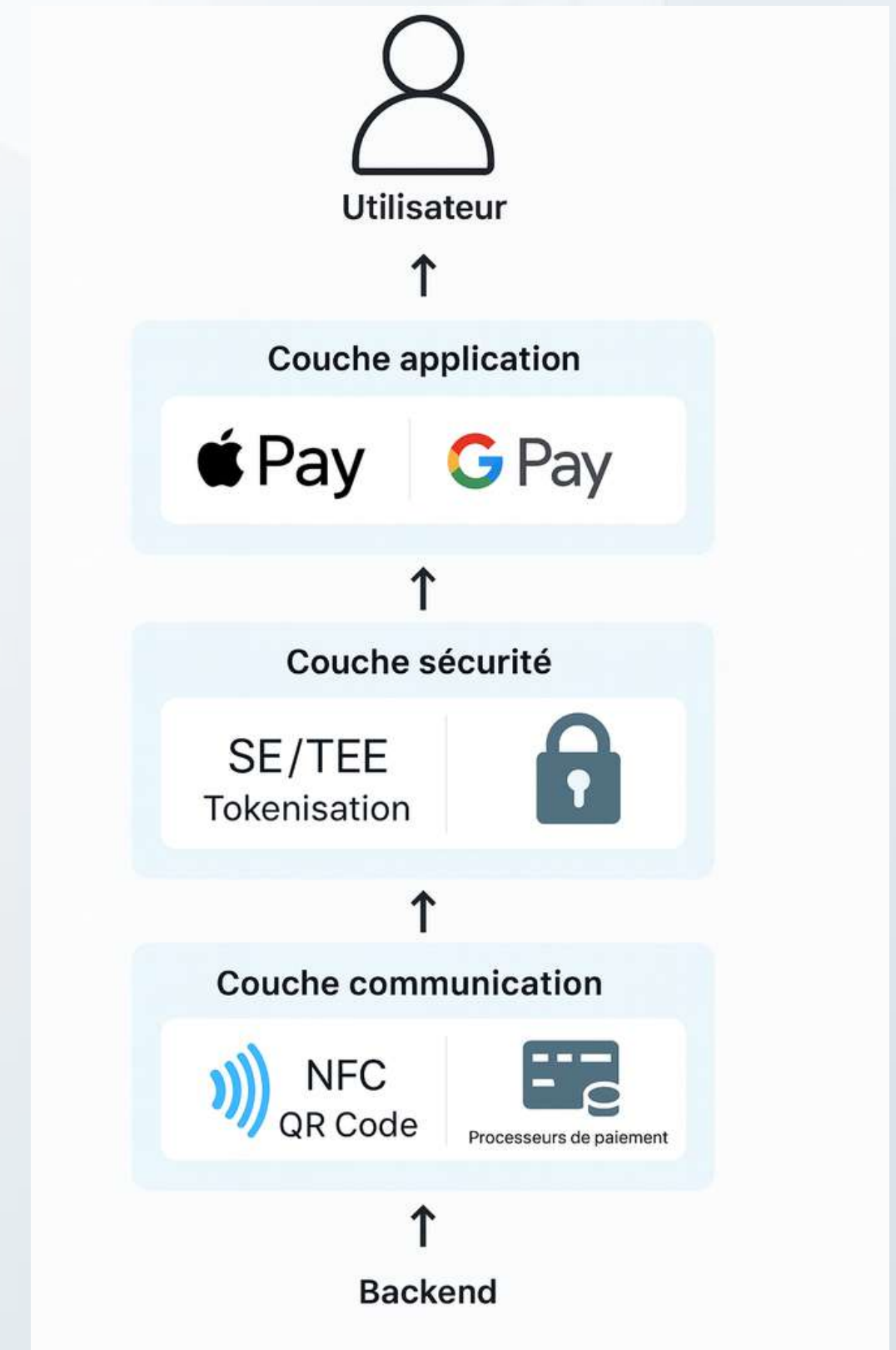
Architecture Technique des Paiements Mobiles

Composants essentiels :

- Terminal mobile (smartphone/tablette)
- Module de sécurité : SE ou TEE
- Système de tokenisation
- Plateforme du fournisseur (Apple, Google, Samsung)
- Infrastructure bancaire (Visa, Mastercard)

SE : Secure Element

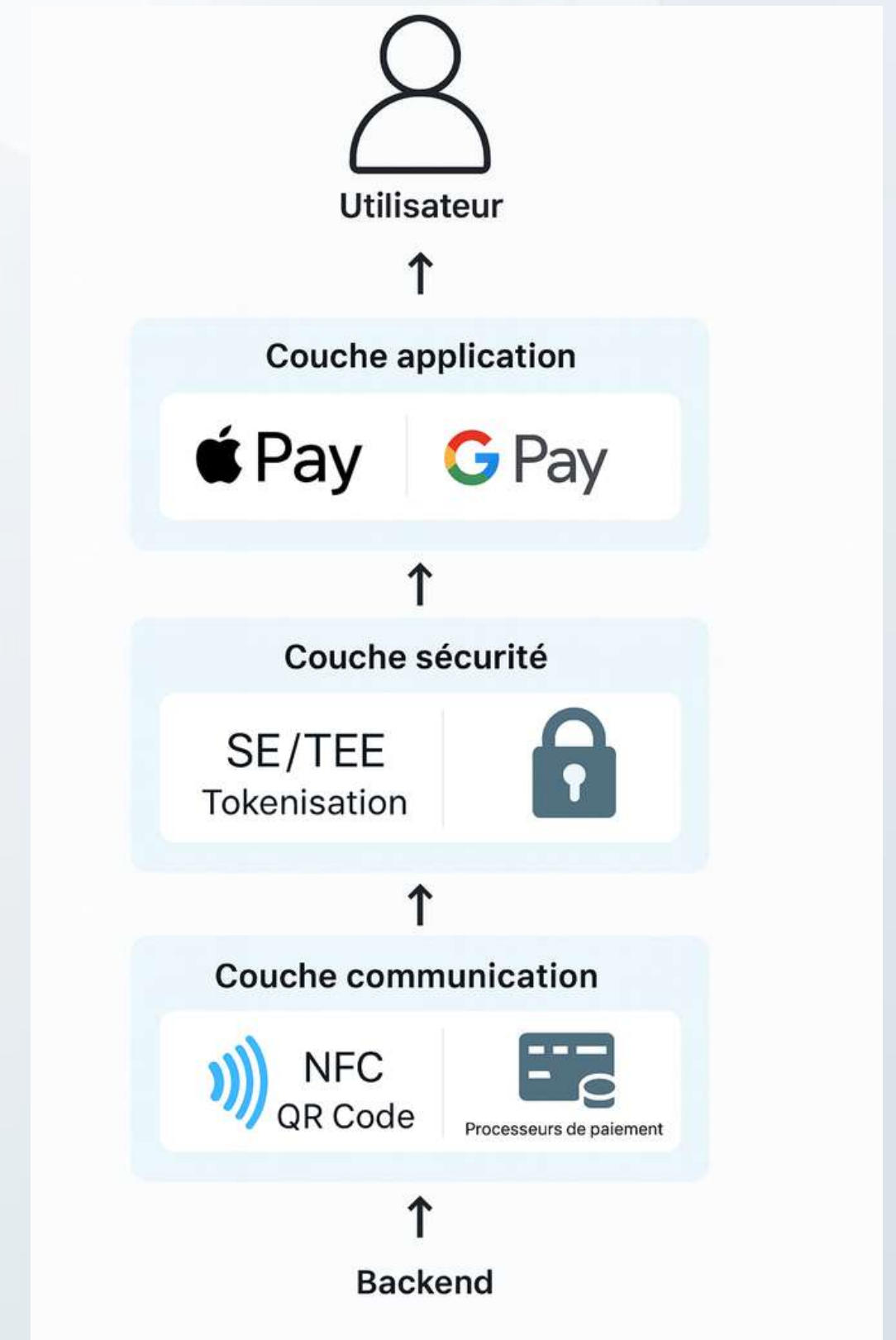
TEE : Trusted Execution Environment



Architecture Technique des Paiements Mobiles

Architecture de paiement :

- Sans contact (NFC) : Apple Pay, Google Pay
- À distance : Apps bancaires, QR codes

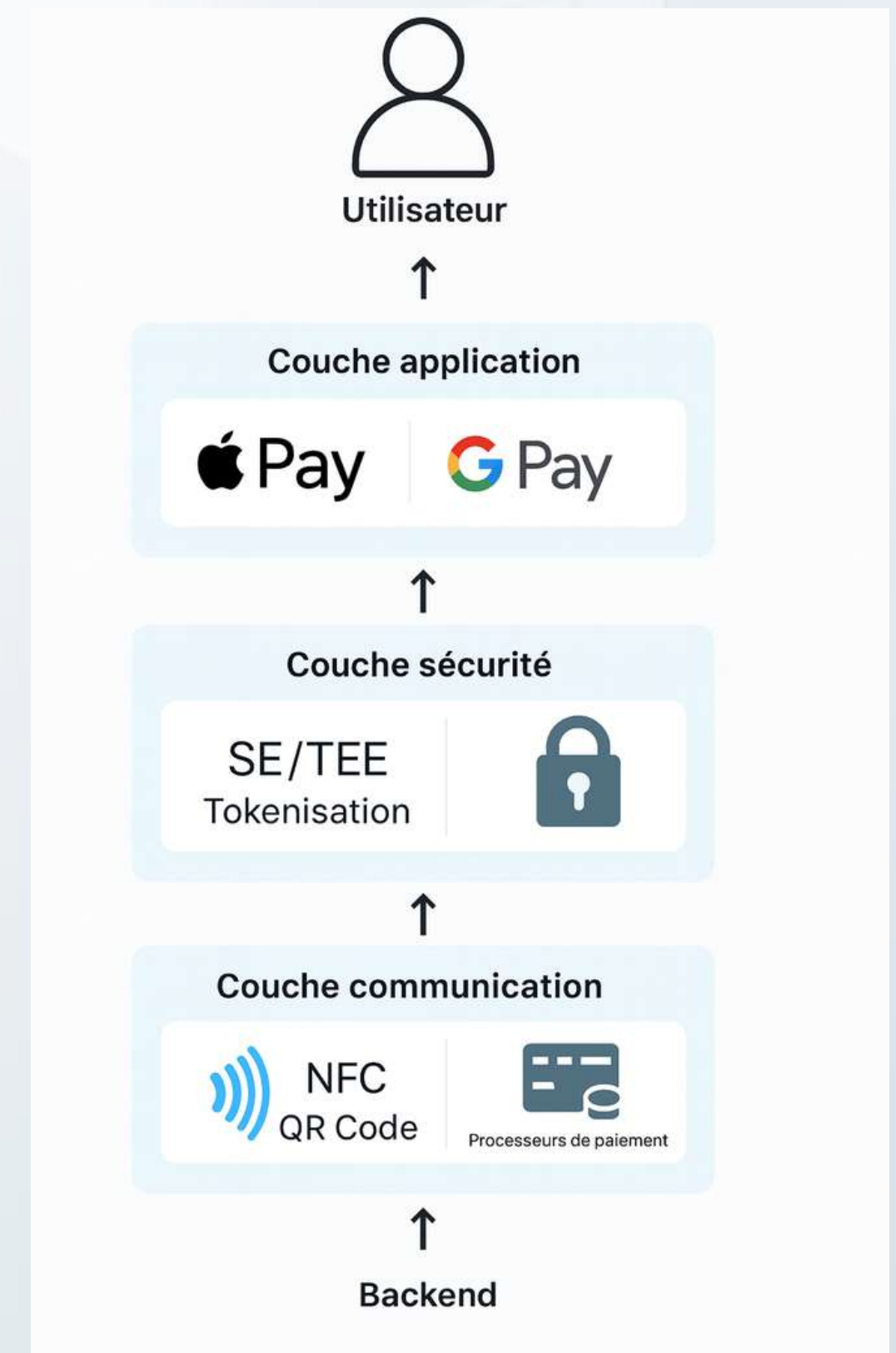


Architecture Technique des Paiements Mobiles

Sécurisation :

- Secure Element = puce virtuelle de carte bancaire
- Stockage chiffré des clés et tokens
- Communication NFC via HCE ou SE matériel

HCE: Host Card Emulation



Les principaux protocoles de Communication

NFC (Near Field Communication)

- Communication à courte portée (4-10 cm) à la fréquence de 13.56 MHz
- Permet l'échange sécurisé de données entre le terminal de paiement et le smartphone
- Mode émulation de carte (Card Emulation Mode)

EMV Contactless

- Standard international pour les transactions sans contact
- Basé sur les spécifications Europay, Mastercard et Visa
- Génération de cryptogrammes dynamiques uniques par transaction
- Vérification par méthode CVM (Cardholder Verification Method) : code PIN ou biométrie

QR Code

- Principalement utilisé par AliPay, WeChat Pay et systèmes asiatiques
- Encode les informations de transaction dans un code scannable
- Deux modes : actif (commerçant scanne le QR du client) et passif (client scanne le QR du commerçant)
- Chiffrement de bout en bout des données de transaction

Mécanismes de Sécurité Fondamentaux

Tokenisation

- Substitution du PAN (numéro de carte réel) par un jeton unique et limité dans son usage.
- Le jeton est inutilisable en cas d'interception : aucune donnée sensible n'est exposée.
- Réduit considérablement les risques de fraude.

Authentification Biométrique

- Vérification de l'identité via :
 - Empreinte digitale
 - Reconnaissance faciale (Face ID)
 - Scanner d'iris
- Obligation d'authentifier l'utilisateur avant chaque transaction.

Cryptographie Asymétrique

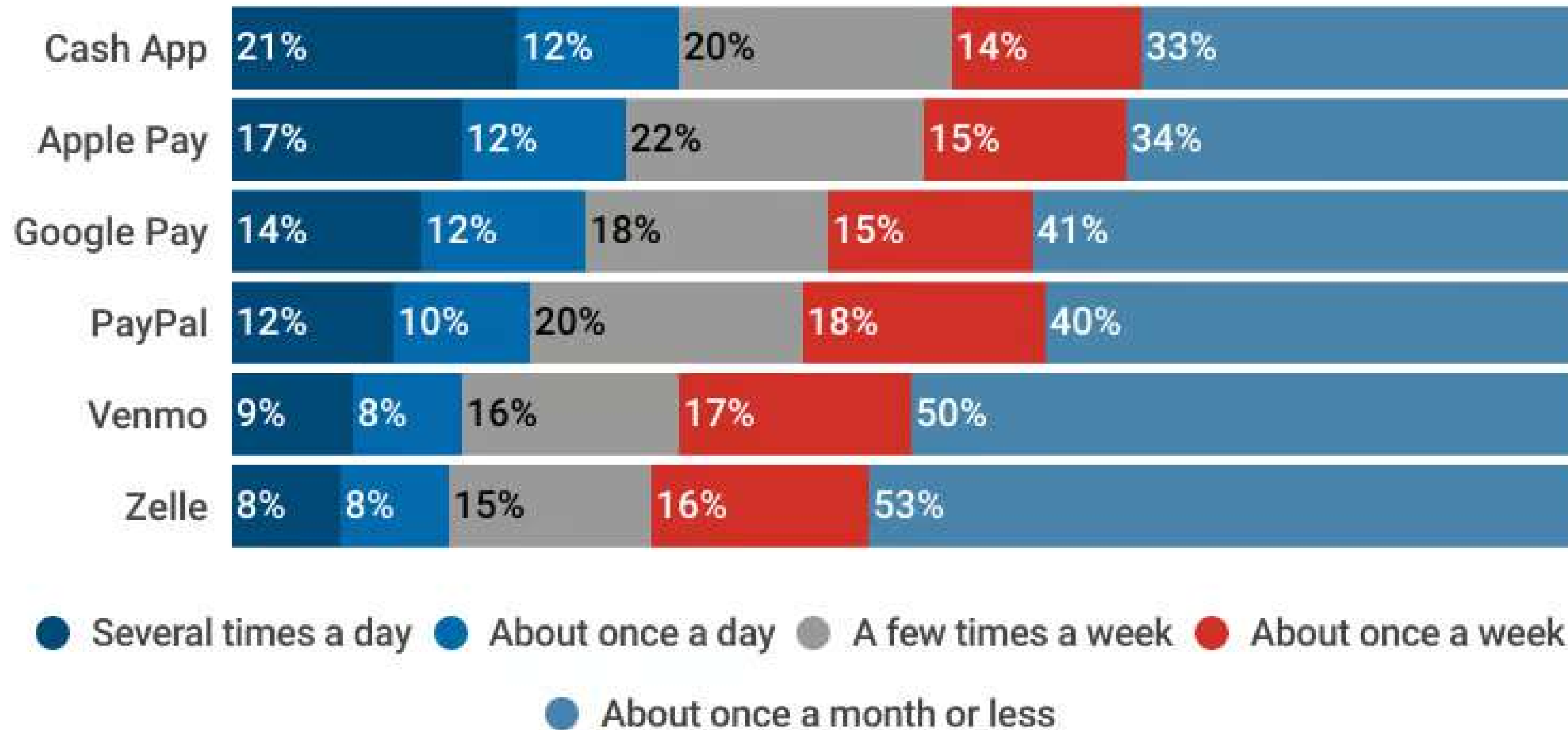
- Utilisation d'une clé publique et d'une clé privée.
- Permet le chiffrement et la signature des données sensibles.
- Garantit :
 - La confidentialité,
 - l'intégrité,
 - l'authenticité des messages échangés

Élément Sécurisé

- Puce matérielle ou enclave isolée du système d'exploitation.
- Stocke les credentials sensibles (clés cryptographiques, jetons).
- Conçue pour résister au root/jailbreak, aux attaques logicielles et physiques.
- Fonctionne comme une carte bancaire intégrée dans le smartphone.

Comparaison des Plateformes Majeures

Frequency of Use Among Digital Wallet Users



Source: Morning Consult

Source :<https://capitaloneshopping.com/research/digital-wallet-statistics/>

Failles Documentées et Cas Réels

2019 - Vulnérabilité Visa

Des chercheurs ont démontré qu'il était possible de contourner la vérification du PIN sur certaines transactions sans contact Visa en manipulant les données APDU.

1

2

2020 - Faille Samsung Pay

Une vulnérabilité du Trusted Execution Environment (TEE) permettait, via une attaque physique, d'extraire les tokens de paiement de Samsung Pay.

3

2021 - Attaque par Relais NFCGate

L'outil open-source NFCGate a montré qu'une attaque par relais NFC pouvait fonctionner sur plus de 100 mètres.

4

2022 - Exploit Google Pay HCE

Une faille dans l'implémentation HCE permettait à une application malveillante d'usurper Google Pay et d'effectuer des paiements.

5

2023 - AliPay QR Spoofing

Une campagne de phishing utilisait de faux QR codes, redirigeant les paiements AliPay vers des comptes frauduleux en Asie du Sud-Est.

An abstract digital background on the left side of the slide. It features a dark blue and purple gradient with glowing orange and yellow lines that resemble circuitry or data paths. Several glowing orange cubes are scattered throughout, some with circular patterns on their top faces. The overall aesthetic is futuristic and technological.

Perspectives et Enjeux Futurs

Cryptographie Post-Quantique

Migration vers des algorithmes résistants aux ordinateurs quantiques pour protéger les transactions futures.

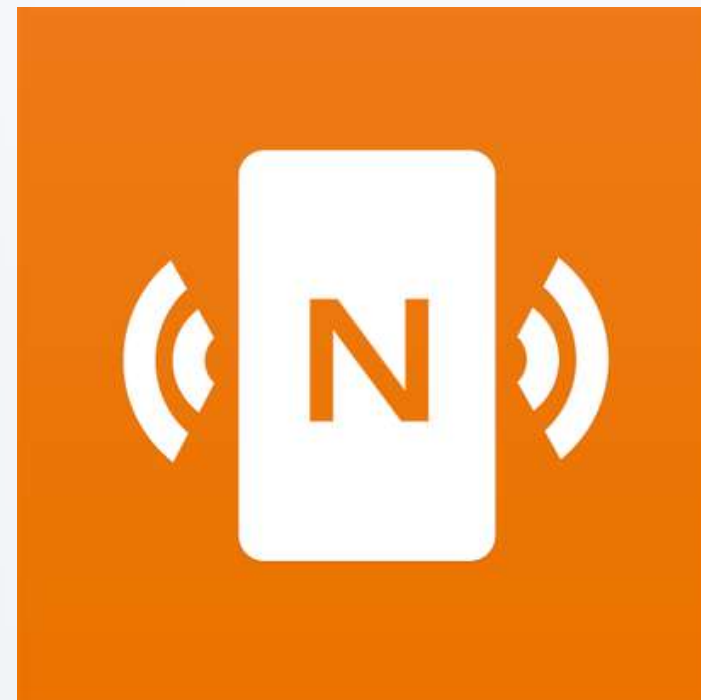
Blockchain et DLT

Intégration de registres distribués pour améliorer la traçabilité et réduire la fraude.

Biométrie Continue

Authentification comportementale permanente analysant la démarche, la frappe et les gestes.

Démonstration



NFC tools

Démonstration

relay attack



Démonstration

Protection
contre le
relay attack

Mesurent de temps exact que met un message à
revenir (distance bounding) ;

Déverrouillage et authentification biométrique ;

Capteurs : mouvement, proximité.