

Analysis and Design of a Tap to Pay Protocol for On-chain Cryptocurrency Payments – Bachelor's Thesis

Haokun Zheng

October 2nd 2023, Bachelor's Thesis Final Presentation

Chair of Software Engineering for Business Information Systems (sebis)
Department of Computer Science
School of Computation, Information and Technology (CIT)
Technical University of Munich (TUM)
www.matthes.in.tum.de

Motivation & Problem Statement

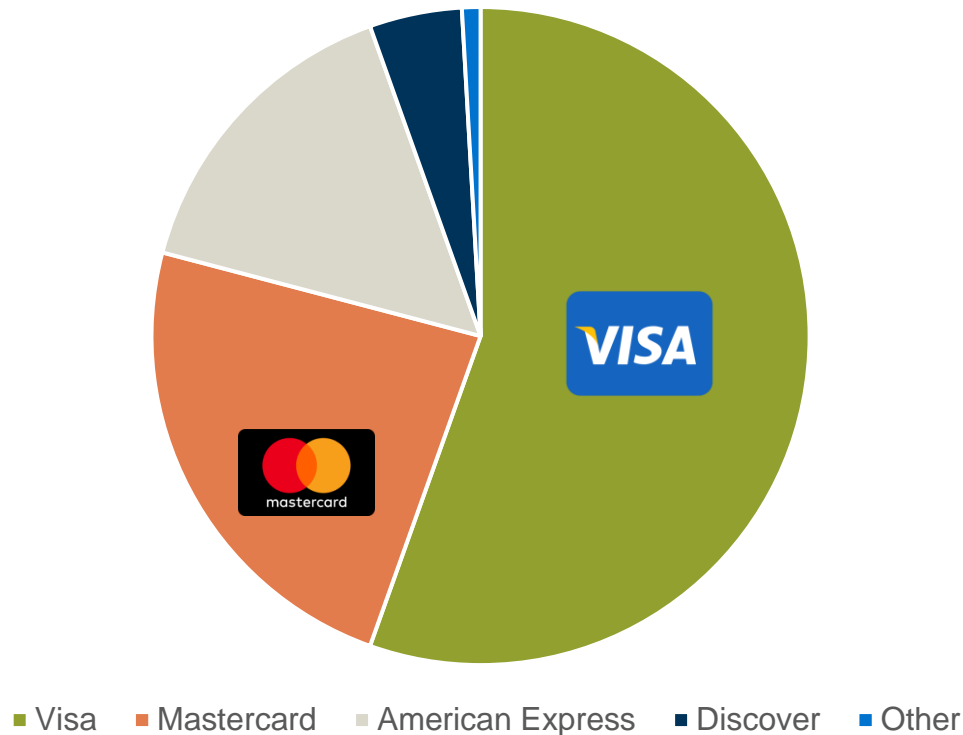
Existing Fiat & Cryptocurrency Payment Methods

Design of the proposed Cryptocurrency Tap to Pay Protocol

Reference Implementation Overview & Demo

Analysis and Comparison to existing State of the Art Payment Methods

Card payment processors by transaction volume, USA
2022



Visa Consumer interchange fees USA 2022

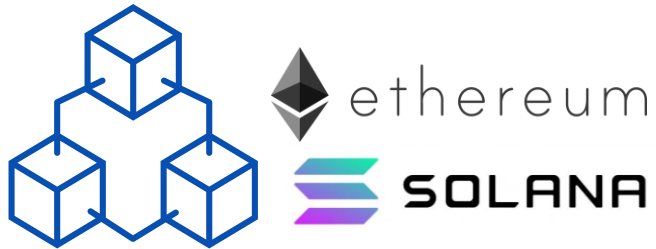
Lower end:
\$0.21 + 0.05% (Regulated Debit Card)

all the way to high end:
\$0.10 + 2,40% (Consumer Credit Card - Travel)

with non-consumer cards having even higher fees

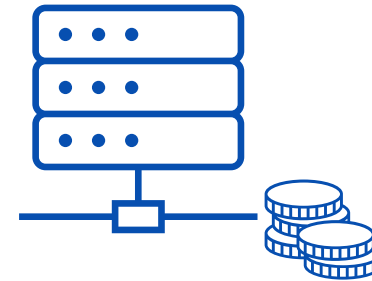
Modern payment networks are charging incredibly high fees, pressuring merchants and affecting consumers.

On paper...



Modern public blockchain infrastructure supports high enough capacity for mainstream payment volume...

- + Decentralization & Self-custody of funds
- + Higher degree of transparency

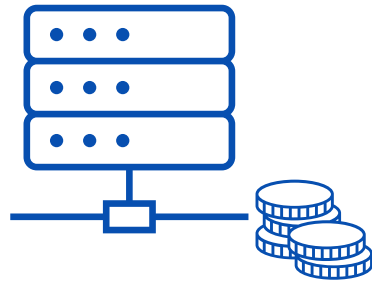


... with potentially orders of magnitude lower transaction fees than Visa & Mastercard

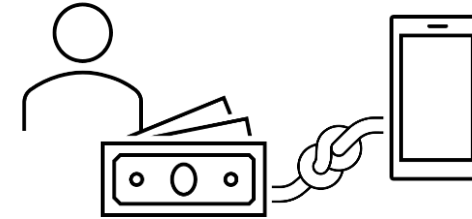
- + Improved security through immutability
- + Greater inclusion & democratized access



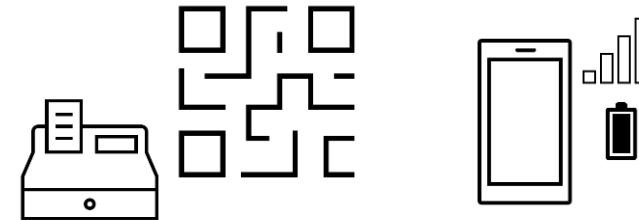
Modern public blockchain infrastructure supports high enough capacity for mainstream payment volume...



... with potentially orders of magnitude lower transaction fees than Visa & Mastercard



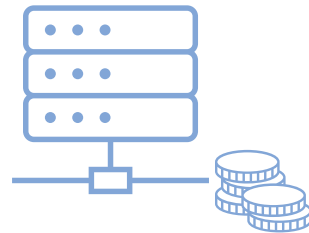
- Wallets complex to set up
- Seedphrases & Keys are difficult to understand



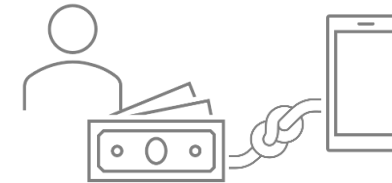
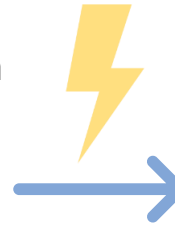
- Slow QR code-based payments
- Incompatible with current PoS hardware
- Client must process tx & have battery + service



Modern public blockchain infrastructure supports high enough capacity for mainstream payment volume...



... with potentially orders of magnitude lower transaction fees than Visa & Mastercard



Crypto wallets are **complex to set up** and **transactions only possible on a previously configured device**



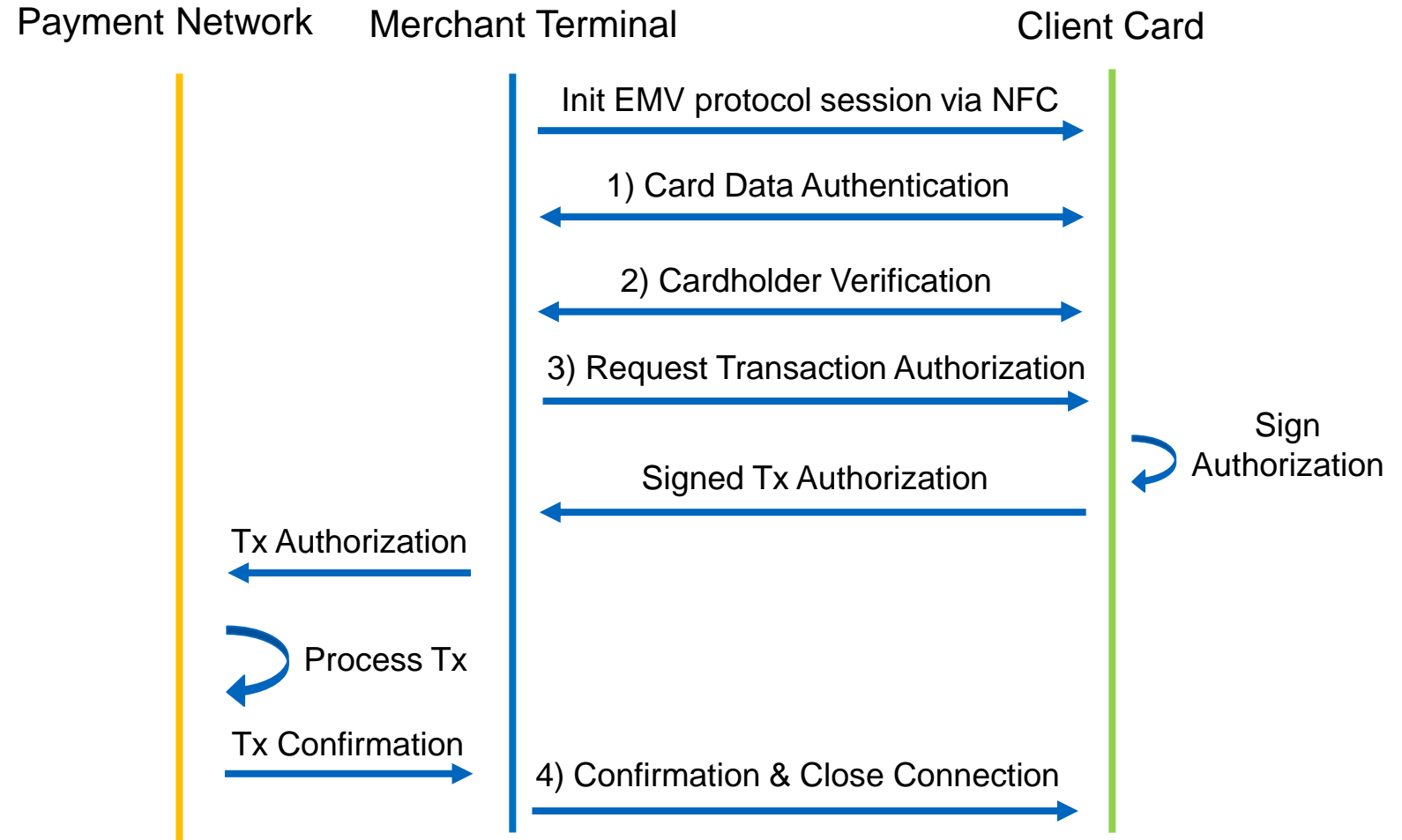
Slow QR code-based payments & incompatible with current POS hardware
Users must process tx and have battery & service

 **Development of a fiat-comparable tap to pay protocol for cryptocurrency transactions.**

EMV Fiat Payment Contactless Protocol Session



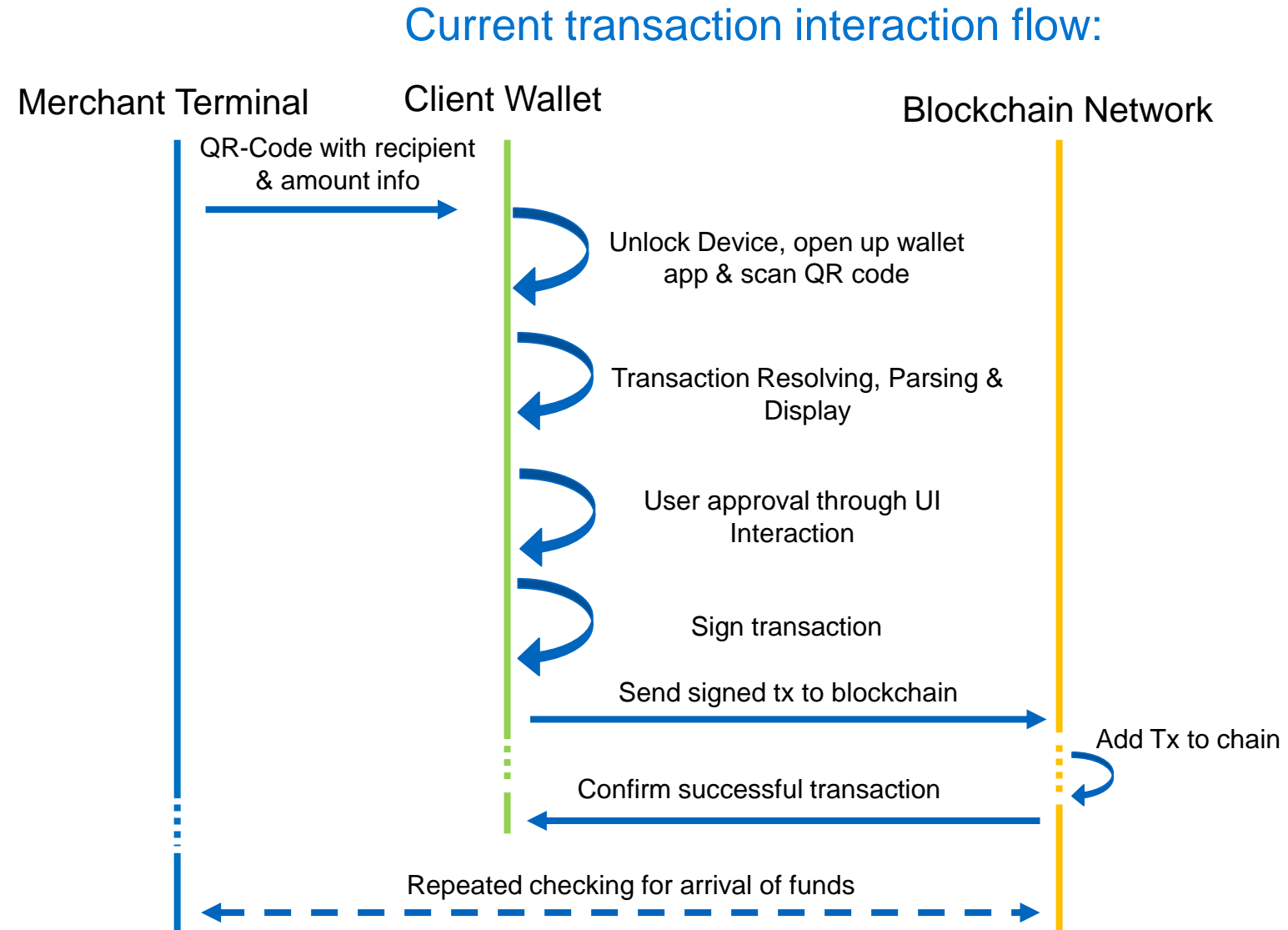
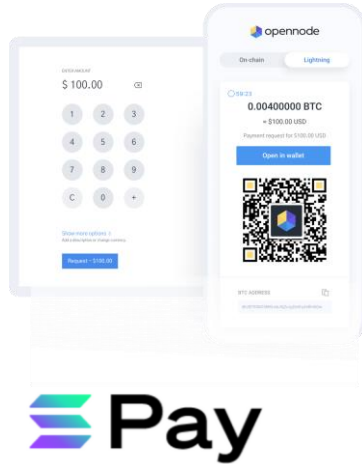
Current tap to pay interaction flow:



Preliminary takeaways:

- **PKI-based authorization scheme**
- **Merchant-side processing**
- **Phone and smart card based infrastructure**

State of the art cryptocurrency payment methods in comparison

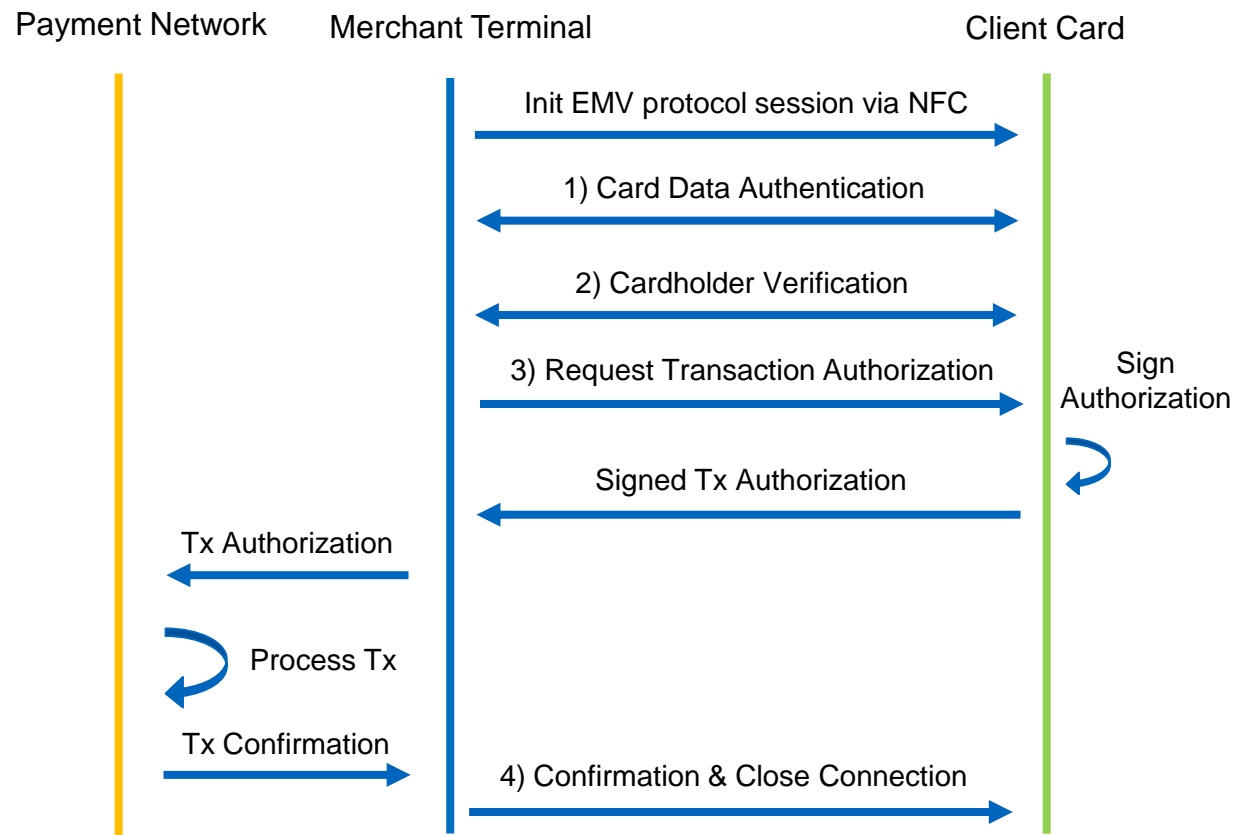


Relevant Standards for URI encoding:

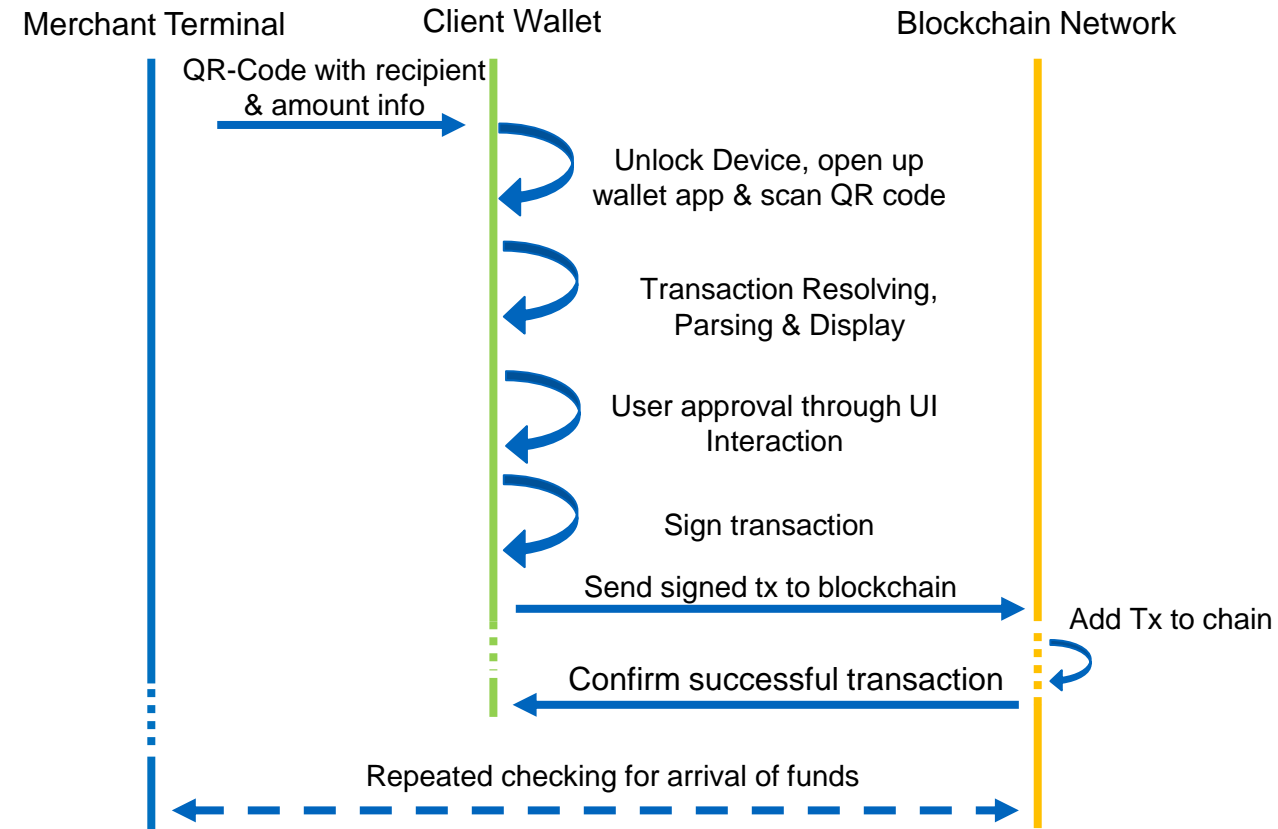
BIP 21 (Bitcoin)
Ethereum ERC-681
Solana Pay (Solana)

Shortcomings of existing Cryptocurrency payment methods

Fiat payment protocol session

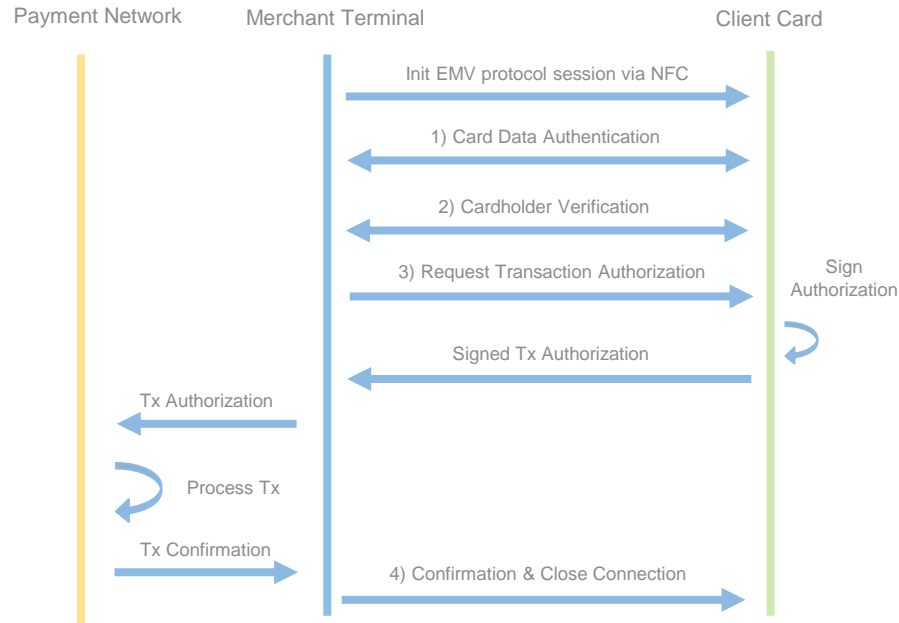


Cryptocurrency payment protocol session:

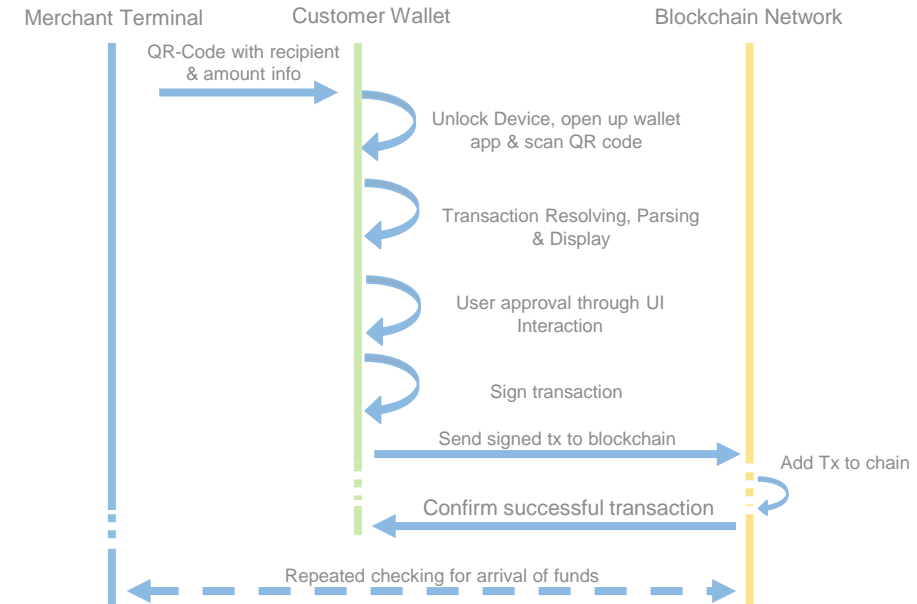


Shortcomings of existing Cryptocurrency payment methods

Fiat payment protocol session



Cryptocurrency payment protocol session:



↓ Client-side transaction initiation & processing

- Transaction status unknown to merchant until funds arrive
- Client has to pay transaction fees
- Client needs online device with sufficient battery charge

↓ Lengthy & uncompetitive QR code interaction:

1. Unlock phone
2. Open/Unlock Wallet App
3. Select QR code scanning function
4. Align phone to scan QR code
5. Authorize transaction

Requirements for a cryptocurrency tap to pay protocol

Selection of determined Functional Requirements:

FR1: Contactless (proximity-based) Transaction Initiation and Processing

FR2: Merchant-side Initiation & Protocol + Device Authentication

FR3: Client Wallet Ownership/Authorization Verification (PIN/biometrics)

FR4: Configurable Transaction Limitations (e.g. max no PIN/max Tx)

FR5: Merchant-side Transaction Processing

...

Selection of determined Non-Functional Requirements:

NFR1: Built on top of familiar UI & UX

NFR2: Compatibility with existing Software and Hardware

...

NFR5: Required NFC proximity under 2 seconds

NFR6: Client hardware requirements satisfiable with non-powered NFC capable smart card

NFR7: Protocol must be scalable

Protocol Session Design (chain agnostic)

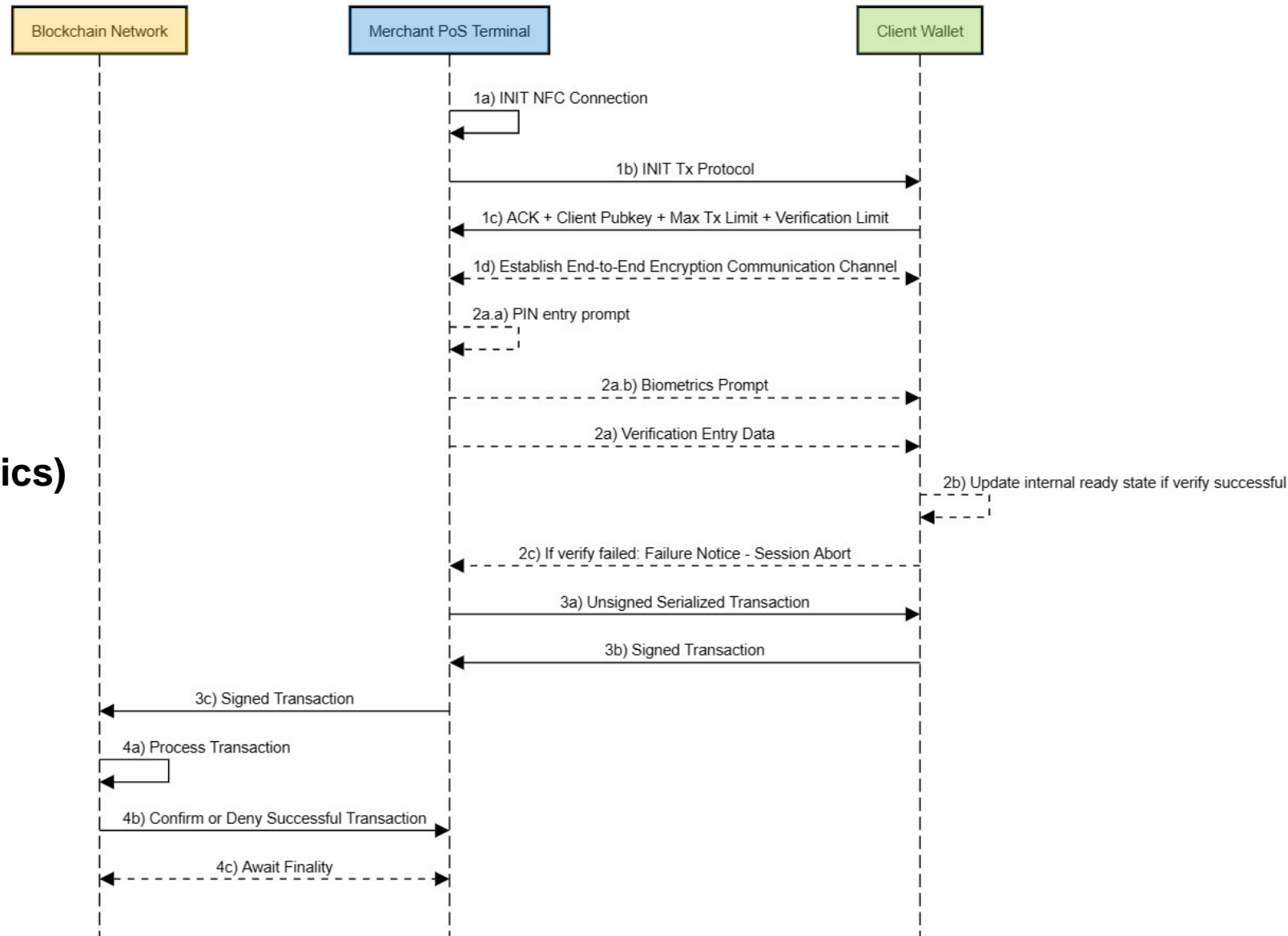
Following EMV protocol session scheme:

1) Session Initiation & Load Limit Configuration

2) OPT: Client Wallet Ownership/ Authorization Verification (PIN/biometrics)

3) Transaction Authorization

4) Transaction Processing



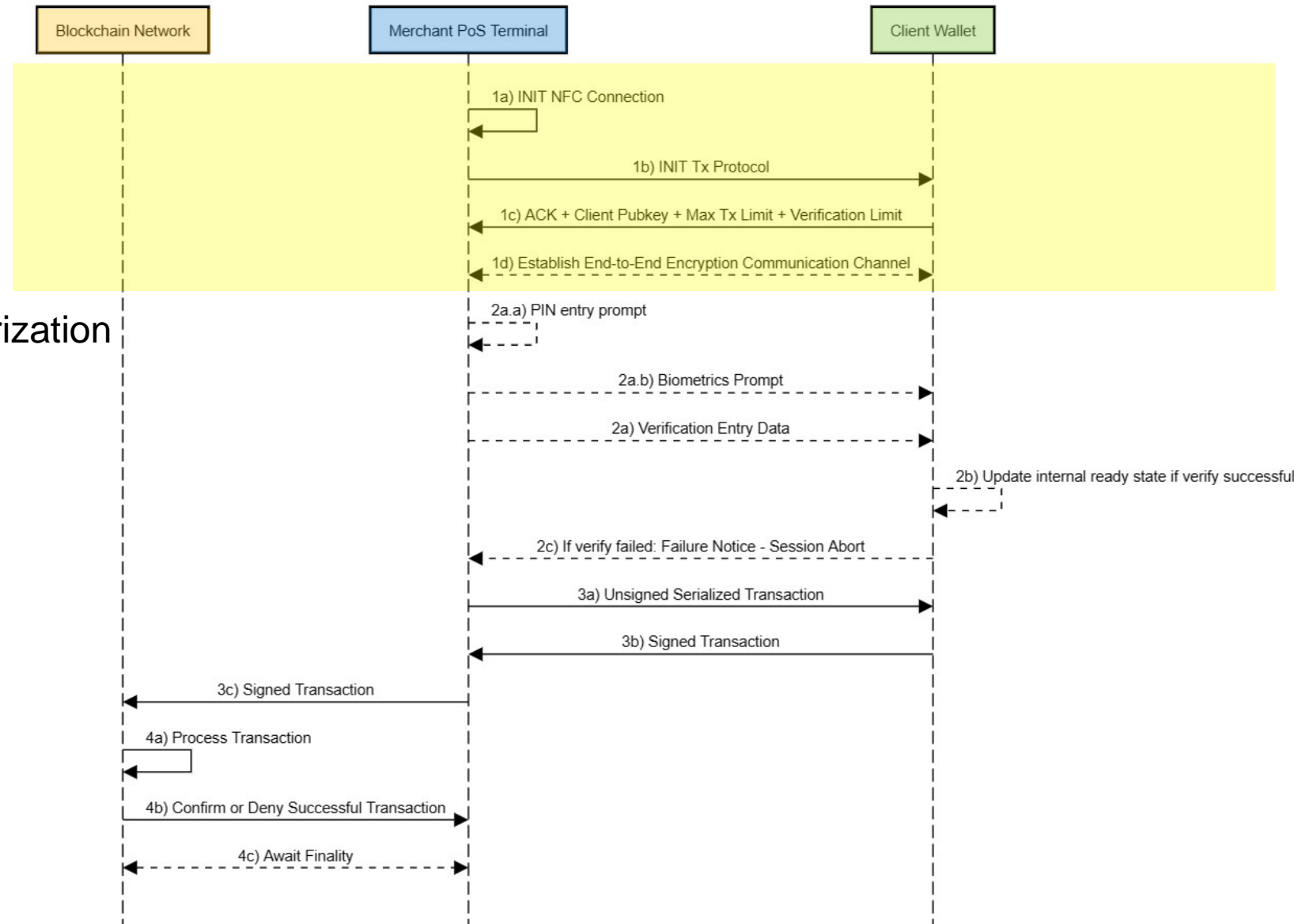
Proposed Protocol Session

1) Session Initiation & Load Limit Configuration

2) OPT: Client Wallet Ownership/ Authorization Verification (PIN/biometrics)

3) Transaction Authorization

4) Transaction Processing



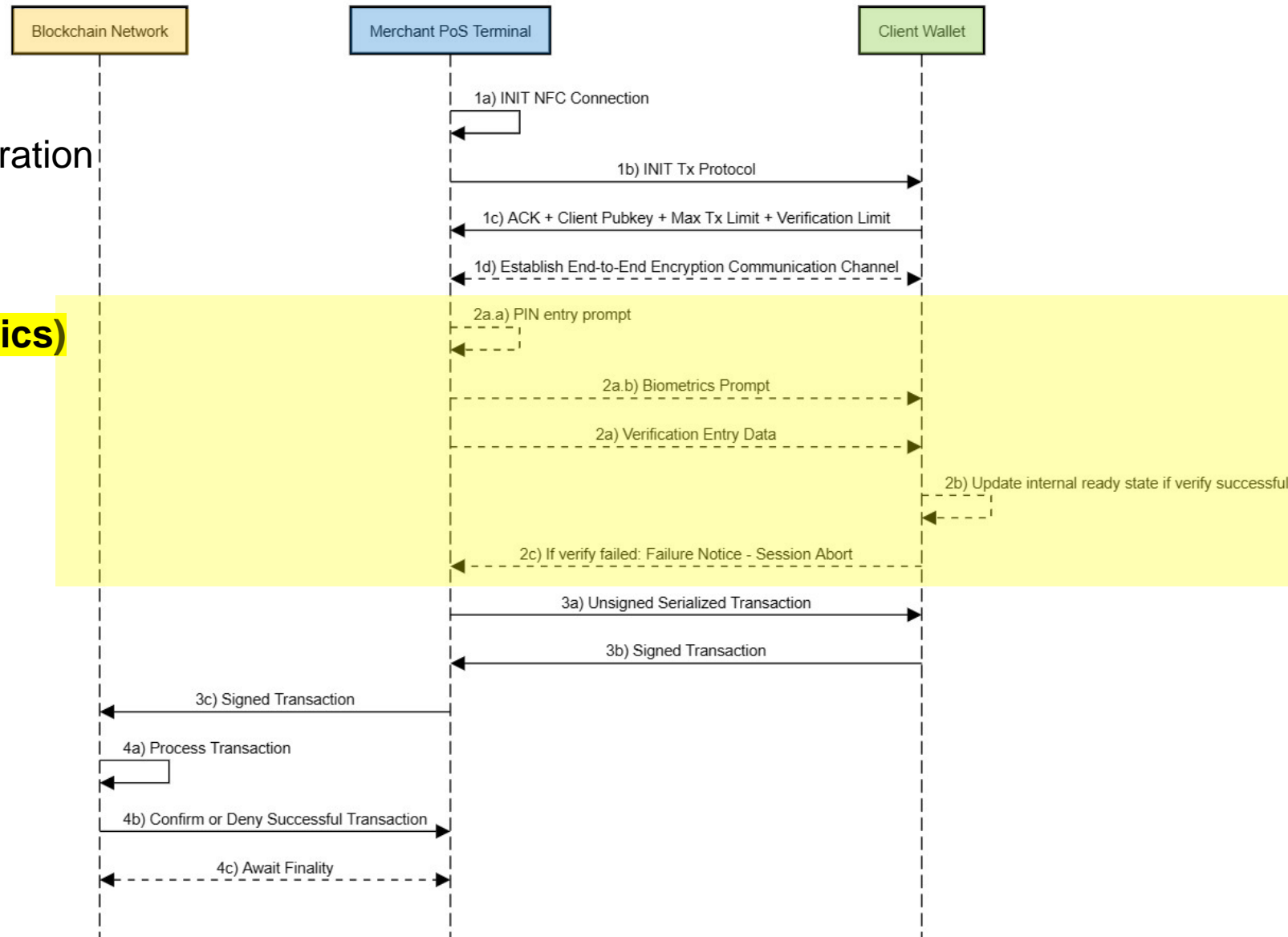
Proposed Protocol Session

1) Session Initiation & Load Limit Configuration

2) OPT: Client Wallet Ownership/ Authorization Verification (PIN/biometrics)

3) Transaction Authorization

4) Transaction Processing



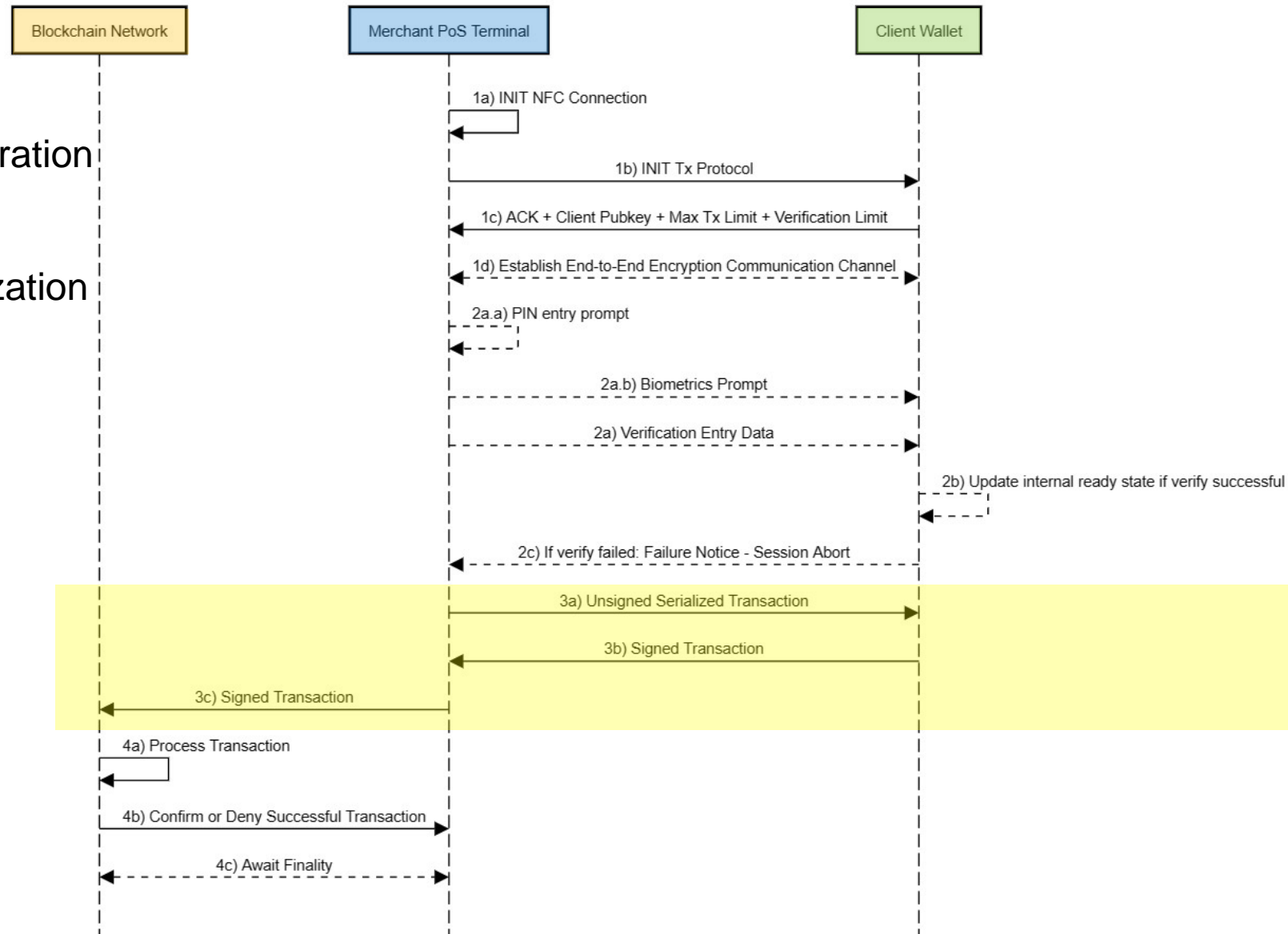
Proposed Protocol Session

1) Session Initiation & Load Limit Configuration

2) OPT: Client Wallet Ownership/ Authorization Verification (PIN/biometrics)

3) Transaction Authorization

4) Transaction Processing



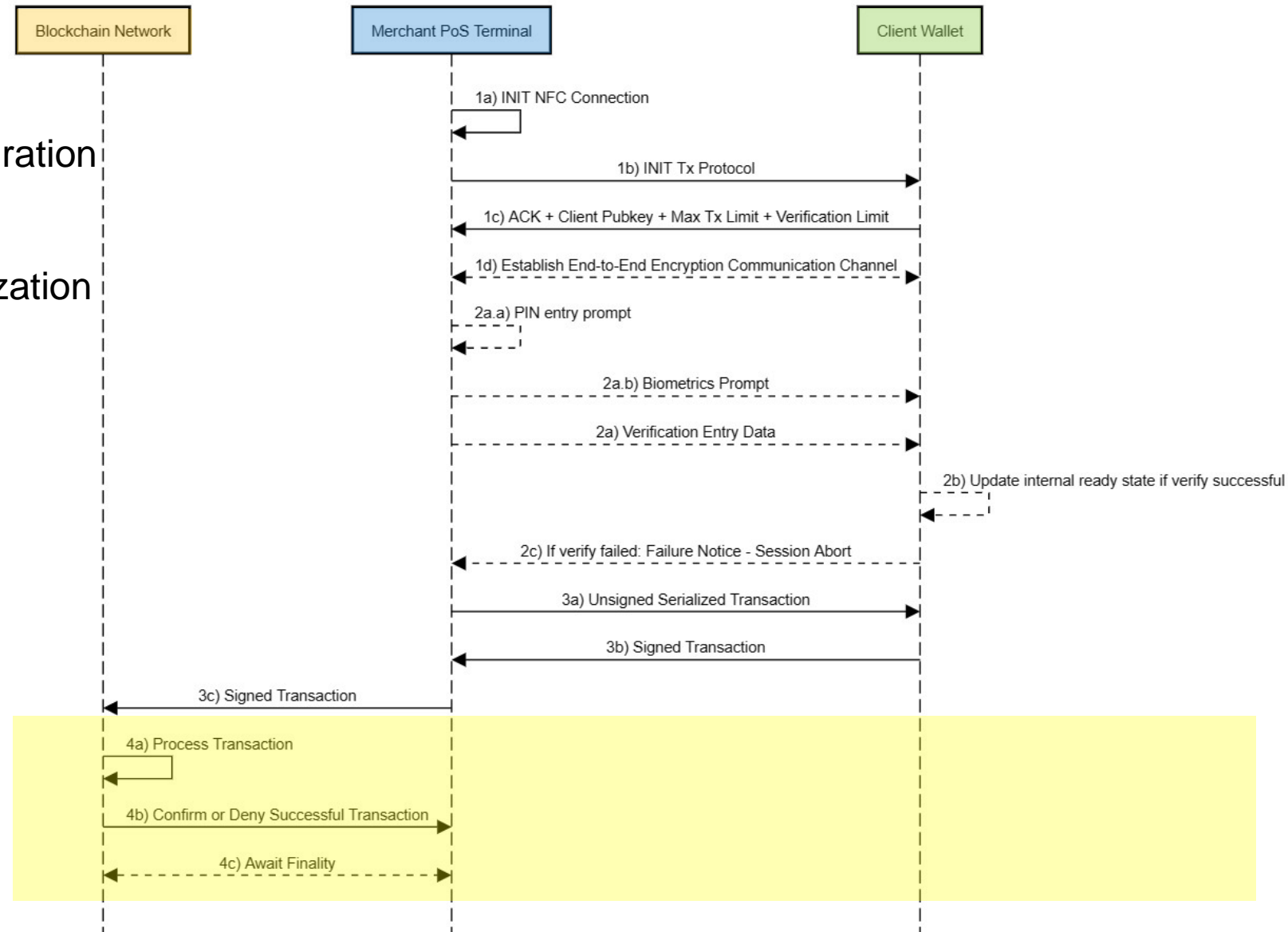
Proposed Protocol Session

1) Session Initiation & Load Limit Configuration

2) OPT: Client Wallet Ownership/ Authorization Verification (PIN/biometrics)

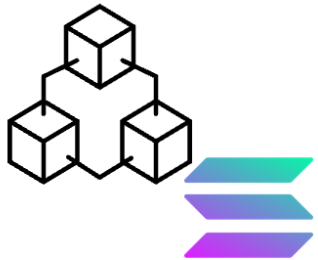
3) Transaction Authorization

4) Transaction Processing



Reference Implementation System Architecture

Solana Network



Merchant PoS System Webapp



PoS NFC Terminal



Client Wallet App (HCE)

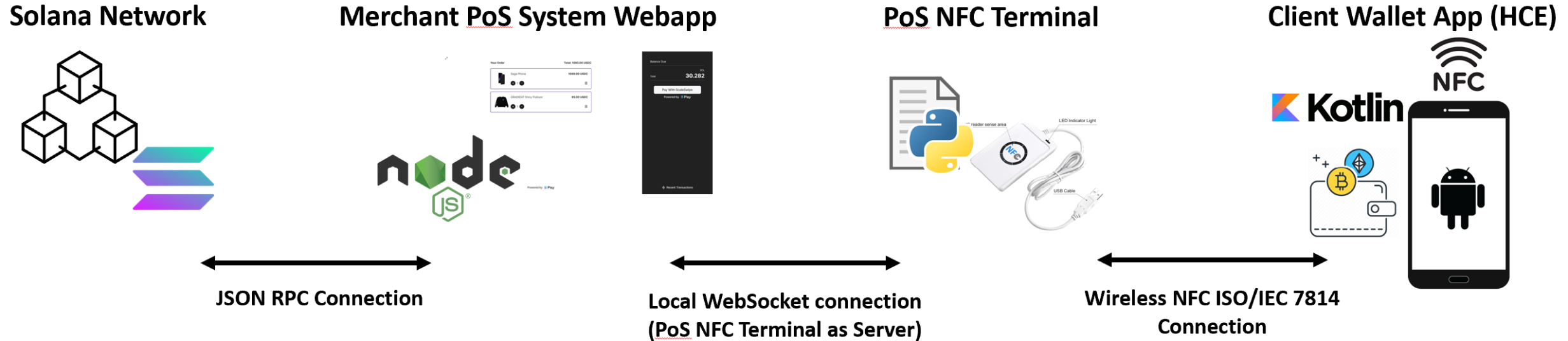


↔
JSON RPC Connection

↔
Local WebSocket connection
(PoS NFC Terminal as Server)

↔
Wireless NFC ISO/IEC 7814
Connection

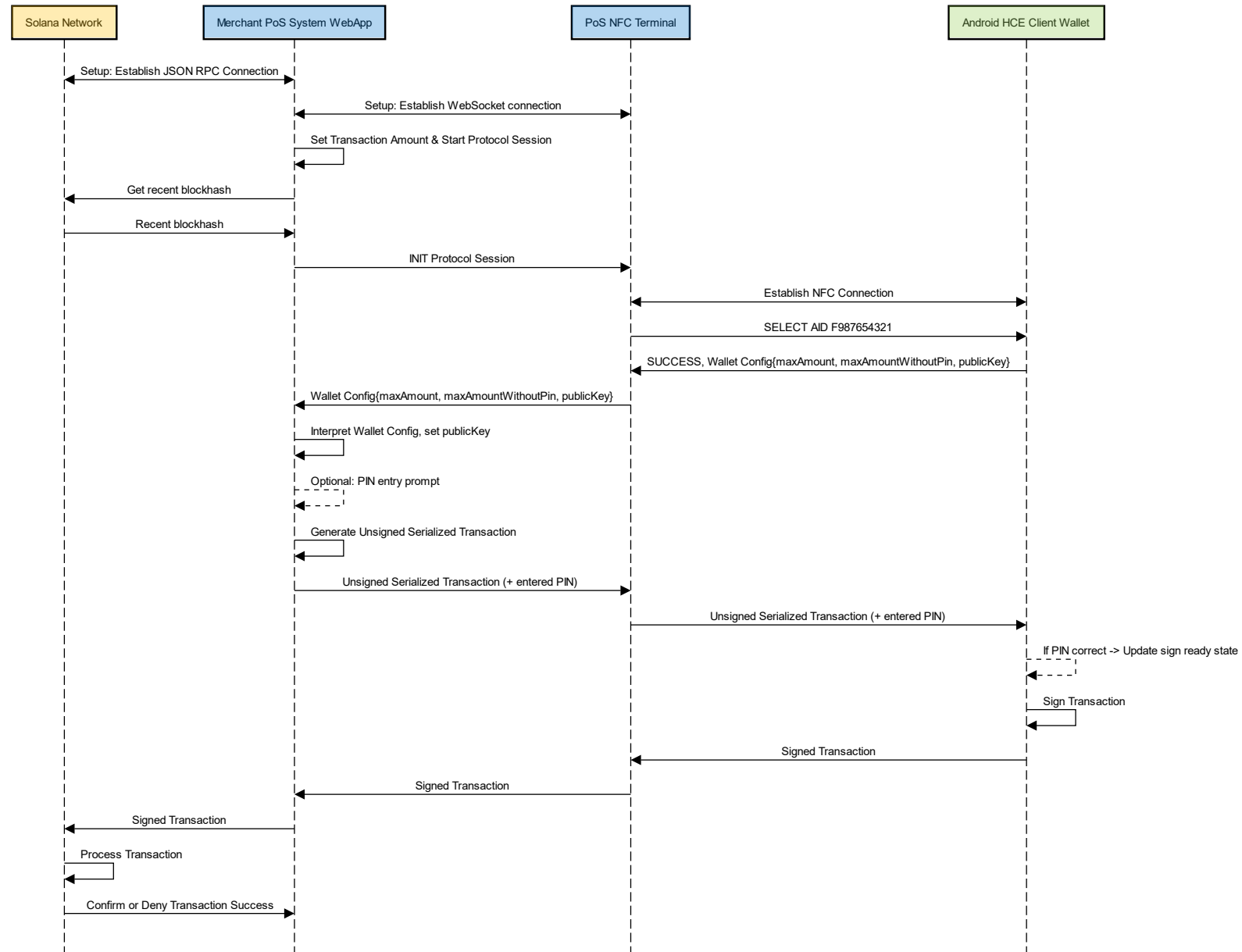
Reference Implementation System Architecture



Some characteristics of the Solana Blockchain:

- **Extremely low gas fees** (\$0.00001 per elemental Tx)
- **Extremely fast block time** (~400ms)
- **High TPS capacity** (currently 5k TPS, capable of up to 65k)
- **Very fast finality time** (~12s)

Reference Implementation Protocol Session






Reference Implementation Demo (EMV equiv.: PIN verification disabled)



Emulated Merchant Checkout System:

Your Order

Total: 20.85 USDC

	TUM Cotton Bag	4.95 USDC	<div>+ 1 -</div> <div>🗑</div>
	TUM Umbrella	9.95 USDC	<div>+ 1 -</div> <div>🗑</div>
	TUM Cap	5.95 USDC	<div>+ 1 -</div> <div>🗑</div>

Emulated Merchant Terminal:

Balance Due

SOL

Total1.15

Make Contactless Payment

Recent Transactions



Merchant address: AYJQ6o82Tr...wfdvLoJwSq

Client address: GA26NywR5a...rGdrD9GEEM

Performance of proposed Tap to Pay Protocol

Our protocol has a comparable performance to existing contactless fiat payment methods!

Segment	Duration	Standard Deviation
Entire transaction duration	2.765s	0.052s
Required contact duration	0.893s	0.0073s

As reference: VISA advertises a required tap-duration of “1-2 seconds”.



Performance of proposed Tap to Pay Protocol

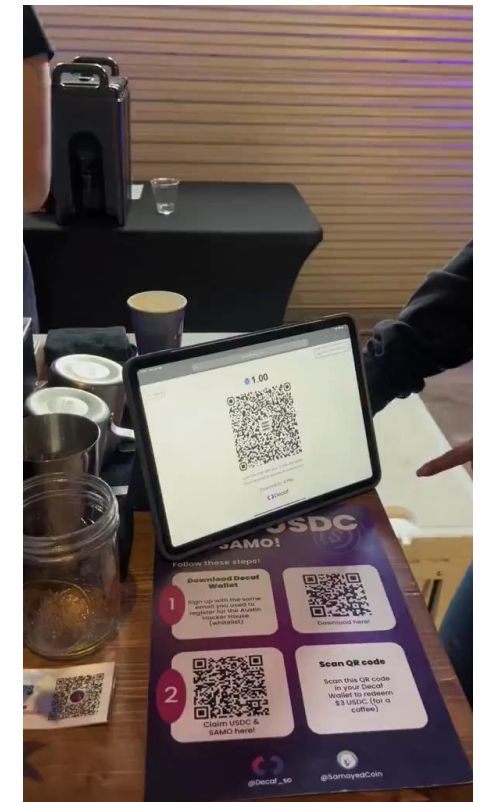
Our protocol has a comparable performance to existing contactless fiat payment methods!

Segment	Duration	Standard Deviation
Entire transaction duration	2.765s	0.052s
Required contact duration	0.893s	0.0073s

Benchmarking against existing State of the Art Cryptocurrency QR Code Payment System on Solana:



Segment	Duration	Comparison to our Impl.
Entire transaction duration Video 1	7.59s	2.75x slower
Entire transaction duration Video 2	8.97s	3.24x slower
Required client interaction duration Video 1	3.84s	4.30x slower
Required client interaction duration Video 2	5.48s	6.14x slower



Usability comparison of proposed Tap to Pay Protocol

	Our Protocol	Decaf QR	Visa EMV contactless
Processing Duration	2-3s	7-9s	2-10s
Funds Settlement Duration	0.4-2s	0.4-2s	1-3 days
No Client Input Interaction Required	✓	✗	✓
Supported Client Hardware Platforms	Card & Phone	Phone	Card & Phone
Offline Client Wallet Support	✓	✗	✓
Compatibility with existing Merchant Hardware	✓	(✓)	✓
Transaction Fees (Sept. 2023)	\$0.00001	\$0.00001	\$0.10–\$0.35 + 0.2%–3.15%

Our protocol provides the same user experience for merchants and clients as fiat payment methods!

Security soundness of protocol also demonstrated in thesis!

→ Proposed protocol proves to be competitive in all major categories:

- ✓ **Performance**
- ✓ **Usability**
- ✓ **Security**

QR code vs Tap to Pay:

- QR codes emerged from historic wallet application development, “simple addition”
- QR code methods guarantee no wrong fraudulent charges at cost of UX
- Tap to Pay protocol departs from sparse wallet use to everyday mass use case

Limitations & Constraints:

- Processing performance & fees dependent on underlying blockchain network
- On- & Offramping of funds not discussed
- Legal & Regulatory constraints

Future Work & Expandability:

- Support for multiple blockchains & tokens
- Smart contract based Anti-Fraud Whitelisting/Staking requirements/Refunds etc.
- Two-Tap Hybrid for all transaction amounts
- Public Key linked Customer Rewards Programs

Security soundness of protocol also demonstrated in thesis!

→ Proposed protocol proves to be competitive in all major categories:

- ✓ **Performance**
- ✓ **Usability**
- ✓ **Security**

QR code vs Tap to Pay:

- QR codes emerged from historic wallet application development, “simple addition”**
- QR code methods guarantee no wrong fraudulent charges at cost of UX**
- Tap to Pay protocol departs from sparse wallet use to everyday mass use case**

Limitations & Constraints:

- Processing performance & fees dependent on underlying blockchain network**
- On- & Offramping of funds not discussed**
- Legal & Regulatory constraints**

Future Work & Expandability:

- Support for multiple blockchains & tokens**
- Smart contract based Anti-Fraud Whitelisting/Staking requirements/Refunds etc.**
- Two-Tap Hybrid for all transaction amounts**
- Public Key linked Customer Rewards Programs**

Security soundness of protocol also demonstrated in thesis!

→ Proposed protocol proves to be competitive in all major categories:

- ✓ **Performance**
- ✓ **Usability**
- ✓ **Security**

QR code vs Tap to Pay:

- QR codes emerged from historic wallet application development, “simple addition”**
- QR code methods guarantee no wrong fraudulent charges at cost of UX**
- Tap to Pay protocol departs from sparse wallet use to everyday mass use case**

Limitations & Constraints:

- Processing performance & fees dependent on underlying blockchain network**
- On- & Offramping of funds not discussed**
- Legal & Regulatory constraints**

Future Work & Expandability:

- Support for multiple blockchains & tokens**
- Smart contract based Anti-Fraud Whitelisting/Staking requirements/Refunds etc.**
- Two-Tap Hybrid for all transaction amounts**
- Public Key linked Customer Rewards Programs**

Security soundness of protocol also demonstrated in thesis!

→ Proposed protocol proves to be competitive in all major categories:

- ✓ **Performance**
- ✓ **Usability**
- ✓ **Security**

QR code vs Tap to Pay:

- QR codes emerged from historic wallet application development, “simple addition”**
- QR code methods guarantee no wrong fraudulent charges at cost of UX**
- Tap to Pay protocol departs from sparse wallet use to everyday mass use case**

Limitations & Constraints:

- Processing performance & fees dependent on underlying blockchain network**
- On- & Offramping of funds not discussed**
- Legal & Regulatory constraints**

Future Work & Expandability:

- Support for multiple blockchains & tokens**
- Smart contract based Anti-Fraud Whitelisting/Staking requirements/Refunds etc.**
- Two-Tap Hybrid for all transaction amounts**
- Public Key linked Customer Rewards Programs**



Haokun Zheng

haokun.zheng@tum.de

Technical University of Munich (TUM)
TUM School of CIT
Department of Computer Science (CS)
Chair of Software Engineering for Business
Information Systems (sebis)

Boltzmannstraße 3
85748 Garching bei München

+49.89.289.17132
matthes@in.tum.de
www.matthes.in.tum.de

