

CBDCフォーラム
【ユーザーデバイスとUI/UX】WG（WG5）
第2回会合 事務局説明資料

オフライン決済に関する
海外の取り組みのご紹介

2024年5月

日本銀行 決済機構局



1. BISによるProject Polaris

1-1. Project Polarisの概要

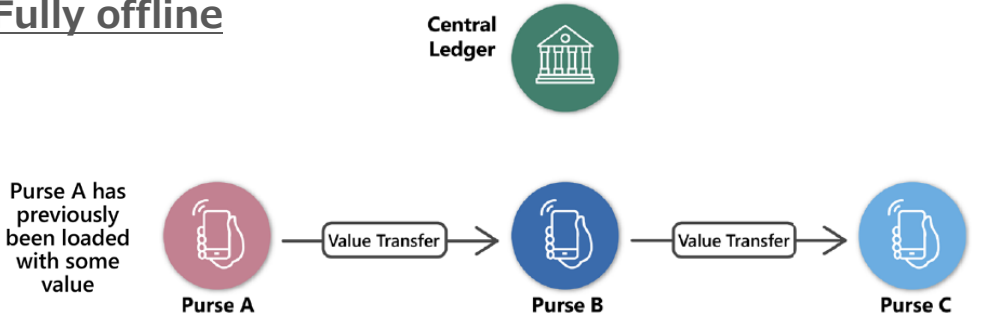
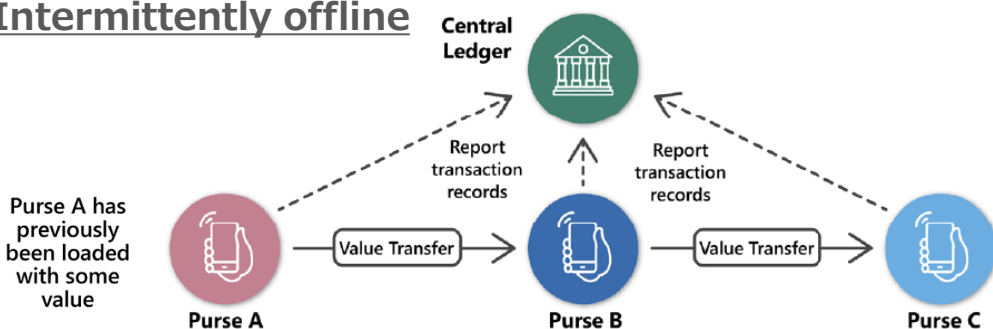
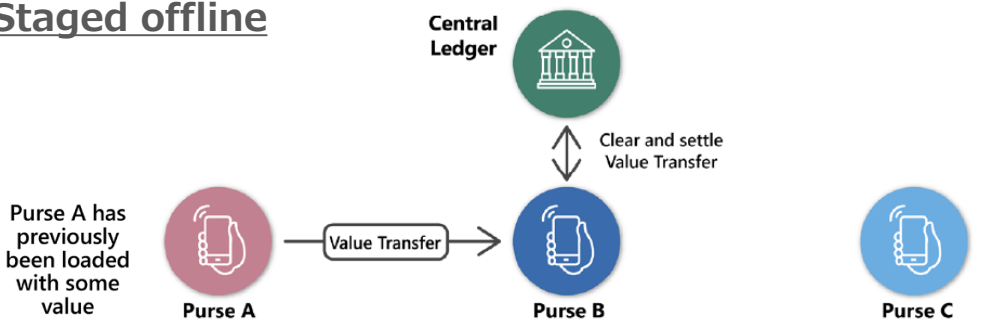
- CBDCシステムのレジリエンスとセキュリティについて調査するためのプロジェクト
- 報告書は4部で構成され、Part1と4がオフライン決済に関する内容
 - Part1：CBDCのオフライン決済の**3つの分類、想定されるリスクやその対策等を取りまとめたもの**で、導入を検討している各中央銀行の手引きとなることを目的とした報告書
 - Part4：Part1を掘り下げ、オフライン決済を検討するにあたり、考慮すべき**デザインを分類し、デザイン選択のアプローチを提示**した報告書

1-1. Project Polarisの概要

- Project Polarisにおける**オフライン決済の定義**
 - 中央の台帳システムへの接続を必要とせずに行われる、デバイス間※の価値移転
 - 支払人（payer）と受取人（payee）の両方とも台帳システムへの接続が不要だが、あくまでもデバイス間の“価値移転”が対象（チャージや払出以外）
- Project Polarisにおける**“Final settlement”の定義**
 - **技術的な観点から価値移転が完了した状態（受け取った価値を次に移転できる）**
 - 本報告書では、法的に価値移転が取り消し不能な状態の“Settlement finality”は、別途、法律の枠組等の手当てや考慮が必要であることから、あえて用いていない

*本報告書では、“Purse（財布）間の価値移転”と表現する場合もある。Purseは、スマホやスマートカード等のデバイス内で、オフライン決済機能を提供するアプリ。

1-2. オフライン決済の3つの分類

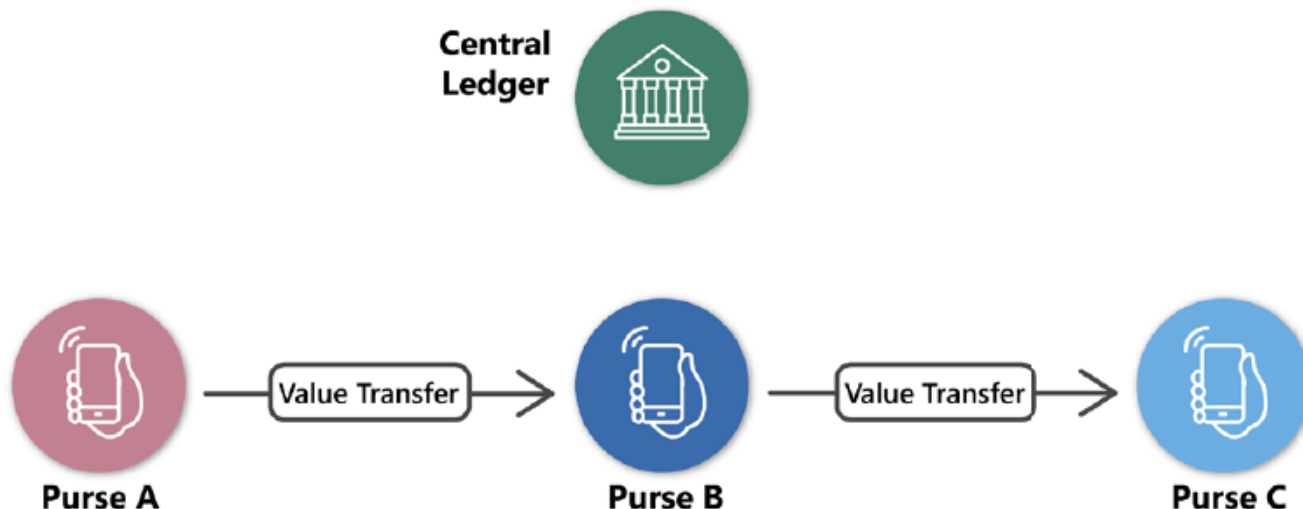
オフライン決済の分類	“Final settlement” における台帳システム への接続必要性	価値移転において 台帳システムへの接続が 必要なタイミング
Fully offline  Purse A has previously been loaded with some value Purse A Purse B Purse C Central Ledger	不要 接続せず取引可能な 回数 = ∞	
Intermittently offline  Purse A has previously been loaded with some value Purse A Purse B Purse C Central Ledger	不要 接続せず取引可能な 回数 = n	Purse機能に対する取引 回数等の制限のリフレッ シュのために、台帳シス テムへ接続しなければな らない場合がある
Staged offline  Purse A has previously been loaded with some value Purse A Purse B Purse C Central Ledger	必要	価値移転を行う際に台帳 システムへの接続は不要 だが、受取人が受け取っ た価値を次に移転するた めには、一度、台帳シス テムへ接続する必要があ る

1-2. オフライン決済の3つの分類

Fully offline

- 支払人と受取人が“**Final settlement**”する（以降、支払を完了するという）ために、台帳システムへ接続する必要はない
- 交換された価値*（value）は、すぐに受取人のデバイスに移転する
- 受取人が受け取った価値は、**すぐに次の支払いに使用できる**
- 支払人と受取人は、いつまでも “**Fully offline**”の状態を維持できる

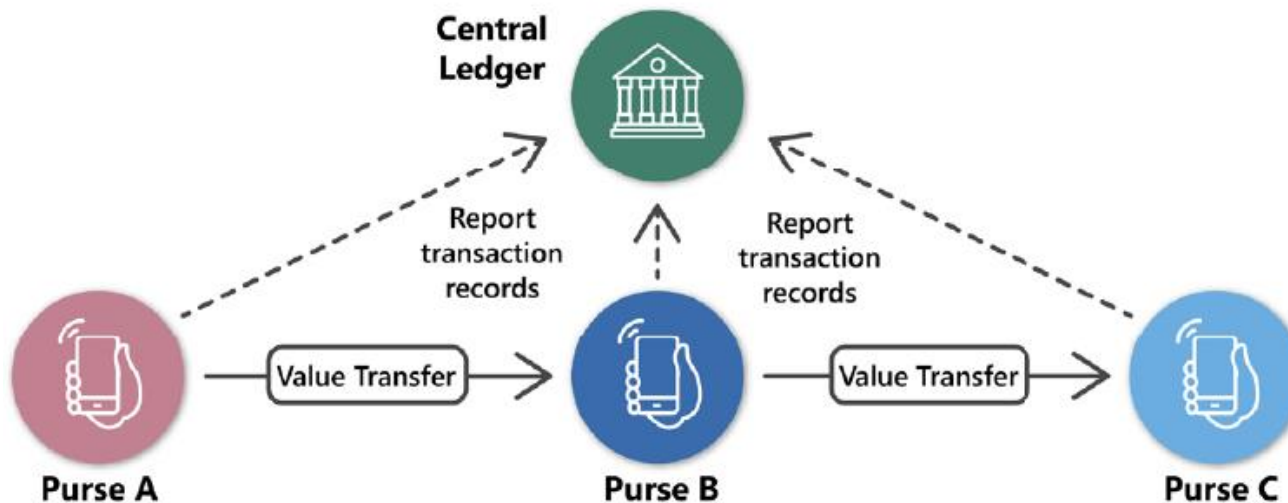
*ここでの「価値」とは、Purseに保存されている残高（balance）やトークンを指す



1-2. オフライン決済の3つの分類

Intermittently offline

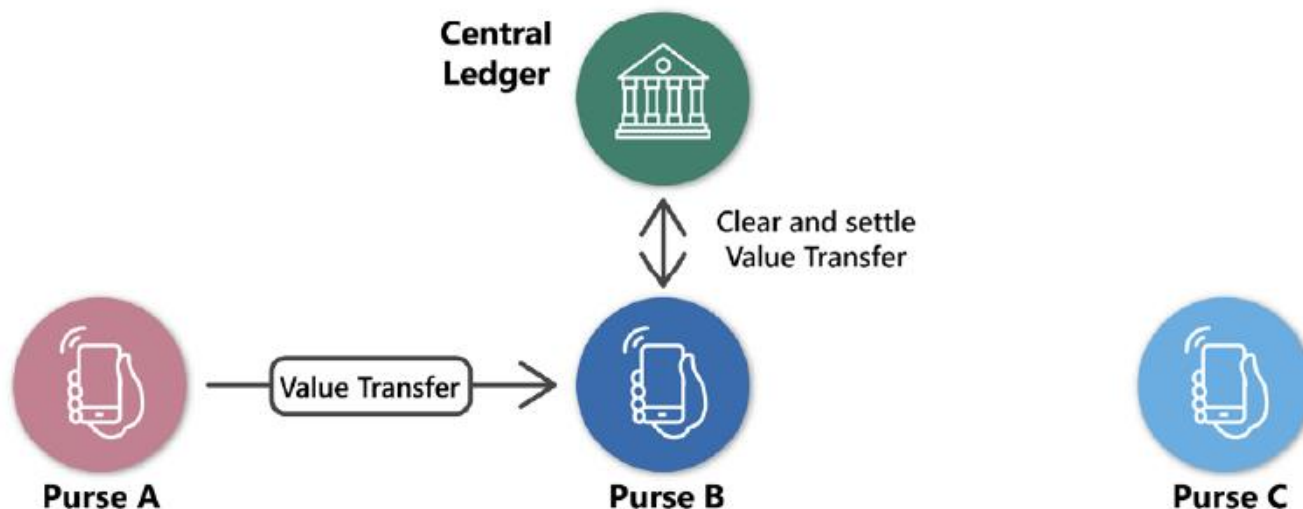
- 支払人と受取人との間の支払を完了するために、台帳システムへ接続する必要はない
- 交換された価値は、すぐに受取人のデバイスに移転する
- 受取人が受け取った価値は、**すぐに次の支払いに使用できる**
- 支払人と受取人は、リスク管理を目的として、Purse機能が制限（取引回数など）に達した場合のリフレッシュ等のために、台帳システムへ接続しなければならない場合がある（接続時に決済取引履歴等のアップロード等）
 - ただし、取引ごとに接続する必要はない前提



1-2. オフライン決済の3つの分類

Staged offline

- 支払人から受取人へ価値を交換する際に、台帳システムへ接続する必要はない
- 交換された価値は、すぐに受取人のデバイスに移転する
- 支払人と受取人との間の支払を完了するためには台帳システムへ接続する必要がある
- 受取人が受け取った価値は、**次の支払いに使用できず**、次の支払いに使用するためには、台帳システムへ接続する必要がある



1-3. オフライン決済の課題と対策

- Project Polarisではオフライン決済に対する考慮すべきリスクやその対策についてまとめている。リスクは技術的リスクだけでなくオペレーショナルリスクやレピュテーションリスクもあげられているが下表は主にユーザーデバイスの観点における技術的リスクの概要と対策となる。（前述の3分類に共通の課題だが、特に、Fully offlineについては全般的にリスクが大きい）

課題			対策例
二重支払		使用済みの価値を再利用されるリスク	- 受取人のPurseが二重支払を受け付けないように、確立した耐タンパー性の高いデバイスと暗号原理の元で確保された暗号鍵とデータの物理的安全性に依拠した設計 - オンラインとオフラインの残高を区別して管理する等
偽造	デバイスに対する不正	直接及び間接的にハードウェアにアクセスされる、デバイス自体が改ざんされる等の脆弱性により、偽の価値やメッセージの生成、Purseを偽造されるリスク	デバイスの耐タンパー性（特にFully offline）及びデータに対する暗号セキュリティを重視した実装 - データ及び暗号鍵の安全な保管と暗号化の実施 - 不正発生後に他デバイスへの波及を防ぐ工夫 - デバイスのセキュリティアップデートの管理
	暗号解読	Purse間の価値移転の通信が解読され、偽の価値等を生成されるリスク	- 専門家による暗号アルゴリズムの認定、レビューの実施 - 暗号鍵やアルゴリズムを必要に応じて変更・更新できる仕組みの導入
紛失	デバイス等の紛失	デバイスの紛失や忘失によって、他人が利用してしまうリスク	- オンライン接続で対象のPurseを使用不能とし、また、ブロックリストとして他Purseに共有する - ユーザーが端末等の盗難や紛失を申告し、それが信頼できると確認可能な場合は価値を回復する仕組みの導入等
	デバイス等の故障	故障や取引中断等によって、価値が消失したり、利用できなくなるリスク	未完了取引等をPurse内に保存する機能、その復元可能システムの構築、又は補償の枠組みの設定等

2. リクスバンクによる e-krona pilot Phase 4

2-1. リクスバンクにおけるオフライン決済の取組

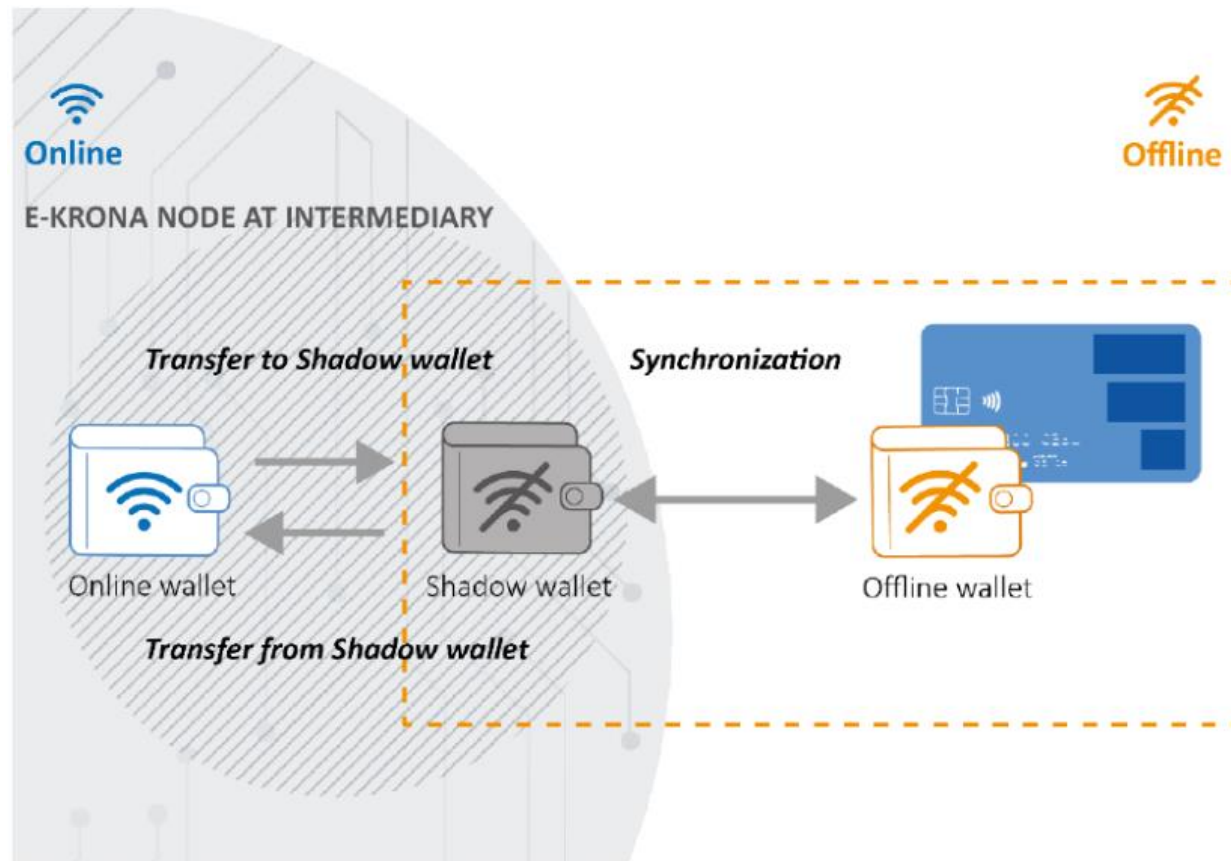
- リクスバンクでは、CBDC（一般利用型）に関する技術的ソリューションを検討するため、2020-2023年にe-kronaのパイロットプロジェクトを実施
- 最後に実施されたフェーズ4は、安全な残高（balance）ベースのオフライン決済ソリューションの設計可能性のテストおよび評価を実施
- 物理カード及びPOS端末にオフラインウォレット（機能）を搭載し、物理カードを利用する場合の通信手段は、スマホのNFC^{*1}リーダーを利用
 - － リクスバンクはスマホのsecure storageとTEE^{*2}を利用できなかったため、トランザクションを保護する目的で独自のソリューションを開発

*1 NFC: Near Field Communication（近距離無線通信）

*2 TEE: Trusted Execution Environment（信頼された実行環境）

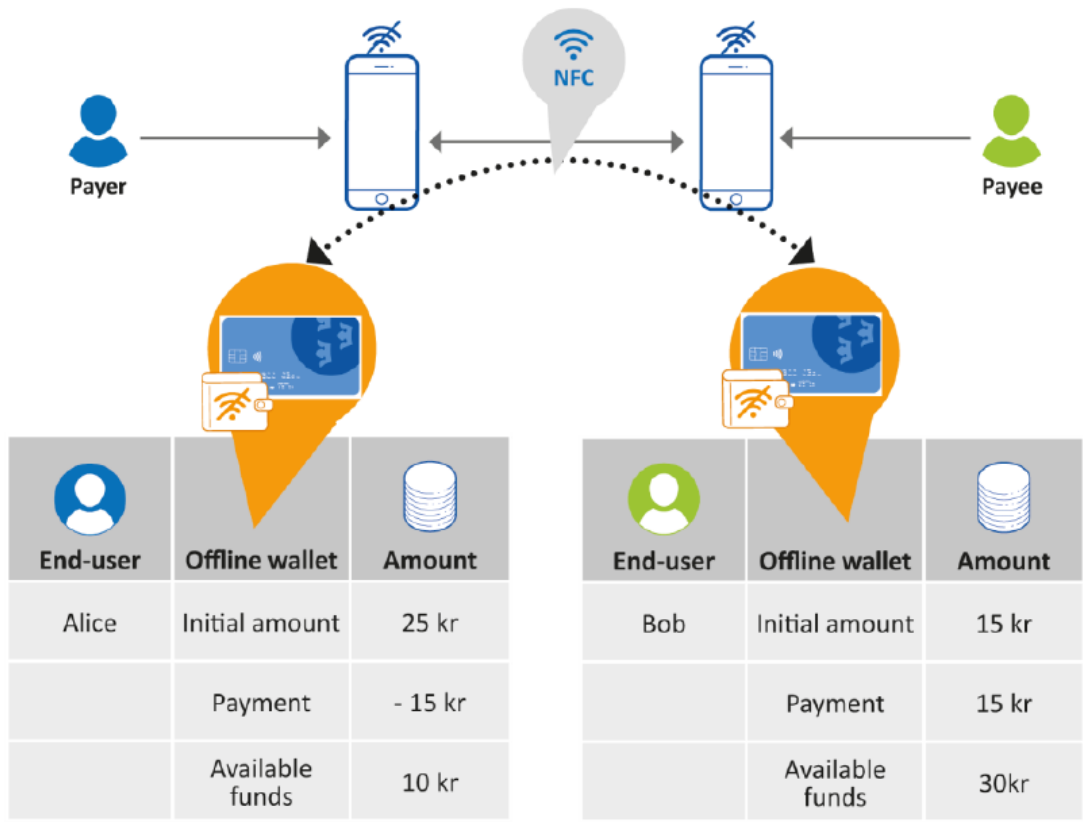
2-2. e-kronaのウォレット

- e-kronaをオフラインで利用するためには、**オンライン口座の残高を一部ロックする**
- ロックした残高は、スマホを通じて**物理カードへ記録**される
 - スマホは同期や記録するための通信手段として活用



2-3. 個人間のオフライン決済の流れ

- 個人間のオフライン決済では、ユーザーは、それぞれ物理カードとスマホを使用する

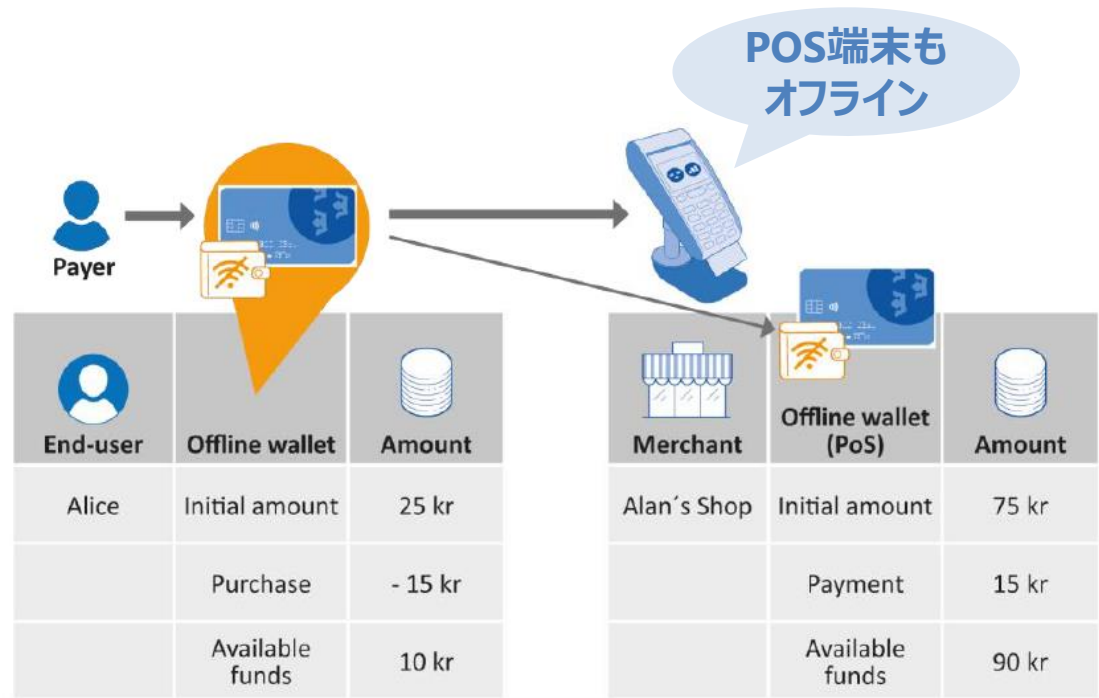


*カードをかざす：NFCを利用し、スマホ等のデバイスとカードの間でデータのやり取りを行う。

1. 受取人（Payee）が自身のe-kronaアプリに金額入力し、スマホにカードをかざす*。カードがデジタル署名された**“支払リクエスト”**（金額、受取人署名）を生成し受取人のスマホに返す。
2. 受取人のスマホから支払人（Payer）のスマホへ、NFC等で**“支払リクエスト”**を送付。
3. 支払人は、支払のリクエストを承認（アプリへカードのPIN入力、カードをかざす）。カードはPINを確認し、**カード残高を減額**させた上で、**“支払リクエスト”**へ署名し、支払人のスマホに返す。
4. 支払人から受取人のスマホへ、NFC等で**“支払リクエスト”**を返送。
5. 受取人は、この支払を受け入れる（アプリへカードのPIN入力、カードをかざす）。カードはPINと受取人及び支払人の署名を検証した上で**カード残高を増額**させ、取引成功の通知を受取人のスマホに返す。

2-4. 店舗でのオフライン決済の流れ

- 店舗でのオフライン決済では、ユーザーは物理カードのみ使用し、店舗はPOS端末（オフライン）を使用する



1. 店舗がPOS端末に金額入力。POS端末は、リクエスト（Request to Pay）を生成。
2. 支払人は、POS端末で支払のリクエストを承認（表示されている金額の確認、カードのPINを入力、カードをかざす）。カードは、PINを確認して**カード残高を減額**した上で、“**デジタル署名されたオフライン取引**”（金額、支払人、受取人）を生成して保存し、POS端末にも送付する。
3. POS端末は署名検証を行い、問題なければ“デジタル署名されたオフライン取引”を保存。取引完了を画面で通知*。

*店舗側がリクエストしていないのに価値移転が実行されてしまうことがないように、店舗側によって各取引が開始されることが重要であり、合わせて、今回の設計では、何度もカードをかざすことなく、カードとPOS端末間の処理が実施できるように考慮されている。

2-5. 決済の完了

- **決済の完了（finally settled）は、支払人が受取人のいずれかがオンラインでe-kronaネットワーク（*1）と同期したタイミング**
 - **同期とは、物理カードやPOS端末に保管されているトランザクションをe-kronaネットワークへアップロードして内容を検証することを指す**
 - アップロードされたトランザクションの検証（二重支払や偽造など）は、Notary Node（リクスバンクが管理）が実施
 - いずれかが同期した後に、残りの一方が同期したタイミングで、この取引がすでに決済完了しているかどうかのチェックが行われるが、二重支払や偽造等が発覚した場合の課題は未記載（*2）

*1 リクスバンクと仲介機関で構成されるネットワーク。e-kronaはこのネットワーク上で取引される。DLTプラットフォームはCordaを使用

*2 不正への対応等は制度面の検討も必要であり、技術的検証結果を報告する本書では言及しなかったと推察

2-6. オフライン決済の制限

- マネー・ローンダリングや詐欺を防止するため、オフライン決済機能に制限を課す想定

制限項目	物理カード	POS端末
最大取引回数	5回（支払、受取）	12回（受取）
金額上限	総残高：SEK3,000	総受取金額：SEK20,000
受け取った価値を次のオフライン支払いに利用	可能 —ただし、同期における流動性の課題が示唆されている（次ページ参照）	不可能

- 取引回数のカウント及びPOS端末の金額上限はe-kronaネットワークへ同期したタイミングでリセットされる（カード残高については、同期後の払出操作で減額される）
- 物理カードの制限のルールは、カード内のプログラムコードに直接実装され、**個別の書き換えはできない**
 - 制限のルールを変更する場合は、物理カードごと交換が必要

(参考) 同期における流動性の課題

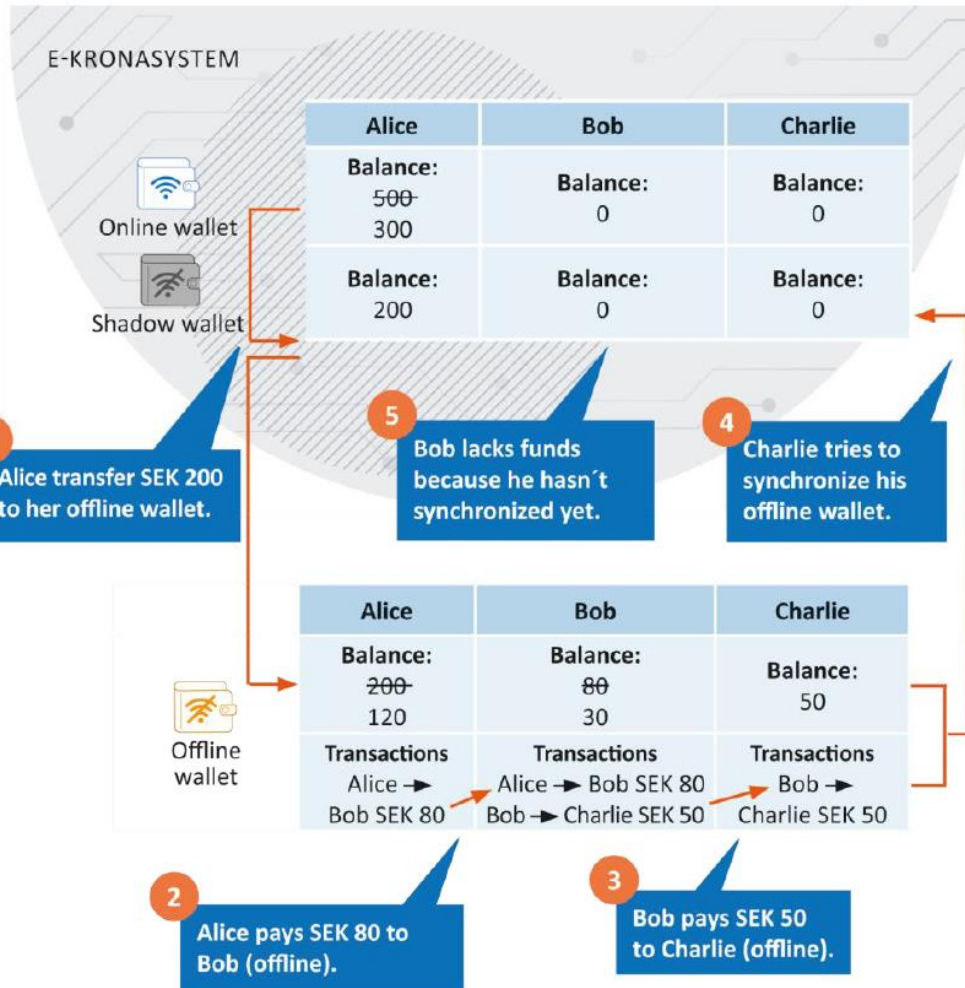
(流動性の課題)

前提：BobとCharlieはオンライン口座からオフライン決済用の残高をロックしていない

1. Aliceはオンライン口座からオフライン決済用の残高としてSEK200をロックする
2. そこからオフラインでBobへSEK80を支払う
3. Bobが、Aliceから受け取ったSEK80のうち、オフラインでCharlieへSEK50を支払う
4. **Charlieが最初にe-kronaネットワークへ同期**
5. Bobがロックしている残高（シャドウウォレット）は0のため、同期が成立しない（BobのシャドウウォレットがSEK50の資金不足）

(対策案)

- 中銀が支払いのための**流動性プール**を提供する
 - オフラインで受け取った資金は、**同期するまで再使用不可能とする等の制限を設ける**
- 本報告書では「対策案の詳細分析は未了であり実現可能性は言及できない」としている。



2-7. 検証から得られた教訓と結論

- プロジェクトから得られた教訓
 - 個人間のオフライン決済では、安全性を考慮した結果、多くの手順が必要になりユーザビリティが低下した
 - 店舗での決済では、POS端末（Androidを使用）のTEEを利用できないため、トランザクションの保存は暗号化に依存するが、不正に操作されないために十分なセキュリティレベルを完全には検証できていない など
- 最も重要な教訓は、**安全で機能的なオフラインソリューションには、技術・規制・プロセスにおいて多くの開発協力が必要**になること
 - そのうえでリクスバンクは、「（安全性とユーザビリティとの）適切な境界線と規制のフレームワーク（the right boundaries and regulatory framework）があれば、安全でユーザブルなオフラインソリューションを開発することは可能であろう」としている