専門家支援プログラム

専門家の意見

デジタルユーロとそのトークンベースのオフライン方式

ティボール・ヤーガー教授（工学博士）

SPE プログラムの一環として、EDPB は特定のテーマに関する報告書やツールの提供を請負業者に委託することがある。

成果物に記載された見解は、その作成者のものであり、必ずしも欧州データ保護委員会（EDPB）の公式見解を反映するものではない。EDPB は、成果物に含まれる情報の正確性を保証しない。EDPB も、EDPB に代わって行動する者も、成果物に含まれる情報のいかなる利用についても責任を負わない。

成果物の一部は、その公開が正当な利益の保護を損なう可能性があるため、削除または編集されることがある。これには、とりわけ、規則（EU）2018/1725 に基づく個人データの保護に関する個人のプライバシーおよび完全性、ならびに自然人または法人の商業的利益が含まれる。

概要

本稿は、デジタルユーロ向けに現金類似匿名性・二重支払い防止機能を備えたオフライン方式を開発する際の技術的実現可能性、固有の制限、可能なアプローチ、およびセキュリティ上の考慮事項を探るものである。

主な考察点：

- 物理的な現金の匿名性、安全性、利便性を完全に再現するオフライン**デジタル通貨の構想**は概念的には魅力的だが、**物理的制約の欠如、強固な二重支払防止の必要性、匿名性**と**追跡可能性**の間の緊張関係が重大な技術的課題となっている。
- 実践においてオフラインで安全かつプライバシーを保護するデジタル通貨を実現するには、複雑な技術的トレードオフの領域をナビゲートする必要がある。非常に強力な方法で偽造防止性と匿名性を達成するために使用できる暗号技術は多種多様である。これらを二重支払防止のための適切な技術と組み合わせる必要がある。例えば、安全なハードウェア要素を利用するか、オフライン要件を慎重に緩和するといった方法である。
- 設計は明確な要件、現実的な脅威モデル、そして暗号技術、システムセキュリティ、ハードウェア工学、法的枠組み、政策といった分野横断的な緊密な連携によって導かれる必要がある。全てのシステム構成要素の設計と実装における公開透明性は不可欠である。独立した専門家による精査が脆弱性を早期に発見するのに役立ち、システムの公衆の信頼、広範な採用、長期的な正当性を育む上で重要だからだ。

結論として、デジタルユーロの匿名モードは、技術とトレードオフの適切な組み合わせに基づく設計がなされれば実現可能である。現在利用可能な暗号技術は、プライバシーを保護し安全なオフラインモードのデジタルユーロ設計に向けた信頼できる道筋を提供している。

概要：

本文書は第 1 節で提示された 5 つの質問を軸に構成される。第 2 節では「現金類似性」通貨など、必須用語と概念の**定義**を記載する。第 3 節では分散システム全般に適用される**既知の根本的制約**と、オフラインデジタル通貨への**適用可能性**を論じる。第 4 節ではこの制約を克服するための**セキュアハードウェア活用の可能性と課題**を考察する。第 5 節では「現金類似性」を実現するための**固有の課題と技術、ハイブリッド解決策の可能性**を論じる。第 6 節では**二重支払いの防止**について考察する。第 7 節では、標準的な暗号技術に基づく現金類似のオフラインデジタル通貨を**設計するための技術的アプローチ**に焦点を当てる。利用可能な全ての暗号手法を網羅的に概説することは本稿の範囲外であるが、特に影響力があり理解が進んでいるツールの一つである**ブラインド署名**に焦点を当て、技術的に実現可能なことを示すことを目的とする。また、その機能性、利点、限界、およびこれらの限界に対処するアプローチについて論じる。

2025 年 9 月提出文書

目次

1. 検討事項 4

2. 用語の定義 5

2.1 物理的な現金 5
2.2 「オンライン」取引と「オフライン」取引 5
2.3 「トークン」はデジタルコインである 6
2.4 「現金類似」デジタル通貨 6
2.5 セキュアハードウェア 9

3. CAP 定理とオフラインデジタル通貨への応用 11

3.1 分散システムと CAP 定理 11
3.2 オフラインデジタル通貨における CAP 定理 11
3.3 CAP 定理の妥当性について 12

4. セキュアハードウェアによる一貫性の実現 14

4.1 二重支払い攻撃とセキュアハードウェア 14
4.2 多層防御による二重支払いの軽減 15
4.3 結論 17

5. 代替技術的解決策 18

5.1 オフラインデジタル通貨における現金類似特性の実現課題 18
5.2 解決策の検討 20
5.3 結論 22

6. 譲渡可能なデジタルトークンにおける二重支払いの防止 23

7. 匿名トークンベースのオフライン方式のための技術的解決策 24

7.1 ブラインド署名 24
7.2 プライバシー保護型デジタルキャッシュにおけるブラインド署名の利用 26
7.3 機能性、利点、制限の分析 28
7.4 プライバシー保護型デジタルトークン向けその他の暗号技術 32
7.5 結論 33

8. 結論 35

1. 検討事項

本専門家意見は、欧州データ保護委員会（EDPB）の委託により、以下の問題に対処するために作成されたものである：

1. **CAP 定理**が有効である場合、デジタルユーロのトークンベースのオフライン方式の設定・設計にどのように適用できるか。また、その 3 つの特性（一貫性、分割耐性、可用性）は、電子決済サービスの文脈においてそれぞれ何を意味するのか。
2. セキュア（ハードウェア）要素に対する過去の（成功した）攻撃の歴史を考慮すると、多重支出は考えられるか。もし考えられる場合、オフラインのデジタルユーロインフラストラクチャのエンドユーザーデバイス（例：スマートフォン）を侵害しようとする試みに対するさらなる防御ラインを構築するために、どのような技術的対策を追加できるか。
3. デジタルユーロのオフライン方式を「現金類似」ものにする実現可能な代替技術ソリューションは存在するのか。つまり、二重支払いに耐性がありながら同時に匿名性のある使用を可能にするもの…
   (a) CAP 定理を遵守しつつ、
   (b) 例えば「可用性」を犠牲にしてオフラインモードを実現するなど、3 つの特性のうち 1 つを満たさないことを受け入れつつ、実用的な実装と使い勝手への影響は？
   (c) 匿名性は全ての当事者ではなく、消費者／支払先（自然人）のみ／少なくともそれらに対して適用され、販売者（「送信者匿名性」）とは対照的であり、ハイブリッドソリューションとなる可能性があるか？
4. トークンベースのオフライン方式は、複数の取引が連続し、その間に何らかの調整がない状況で、二重支払いをどのように防止できるか？逆に、トークンベースのオフライン方式の現金類似性を維持しながら、調整プロセスをどのように実装できるか？
5. デジタルユーロの設計選択に関する既存の研究を踏まえ、匿名性を維持しつつトークンベースのオフライン方式を実装するのに有用な技術的解決策は何か？

2. 用語の定義

「オフライン」「トークンベース」「現金類似」のデジタル通貨に関する疑問に答えるためには、これらの用語をより明確に定義する必要がある。物理的な現金を簡略化した観点から始めることが有用だろう。

2.1 物理的現金

図 1 は物理的現金の簡略化・抽象化された図解である。これは、通貨の発行と償還に関わる金融機関と、個人ユーザー間の価値移転との分離を示している。この図では 3 種類のユーザーを考慮している：

- 最初の支払者は、銀行から現金を引き出し、それを別のユーザー（最終的な受取人、あるいは一連の支払者と受取人の間の仲介ユーザー）に送金することで現金を使うユーザーだ。
- 無制限の数の仲介者が存在し得る。仲介者とは、あるユーザーから価値を受け取り、別のユーザーへ移転するユーザーである。これらの仲介者は支払先と支払者の両方の役割を果たす。

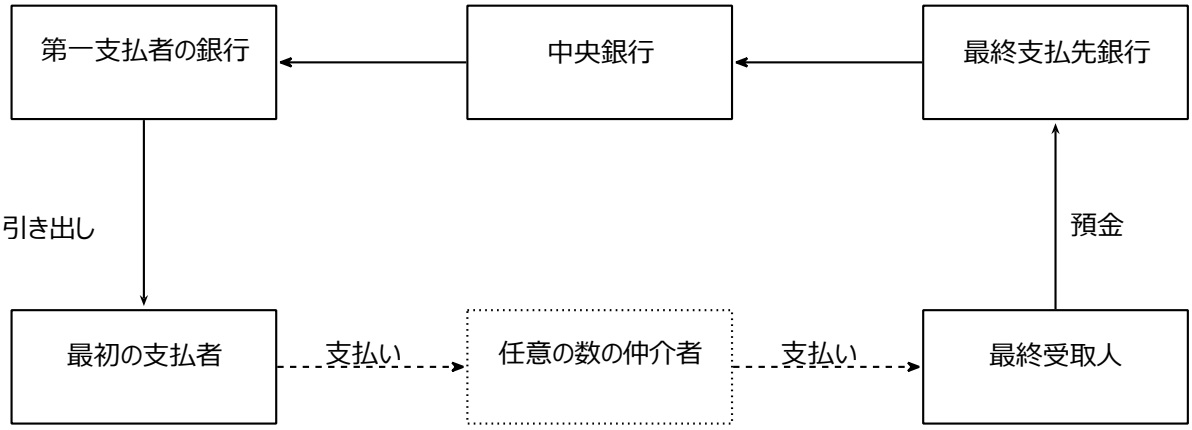

図 1：現金の流れの図解。実線は「オンライン」とみなされる取引、つまり（中央）銀行などの中央機関との通信経路が確立されている取引を示す。破線は「オフライン」取引を示し、中央機関との通信なしに実行できる取引である。

- 最終支払先は現金の最終受取人であり、その後その現金は銀行に預け入れられる。

図 1 の破線矢印は、最初の支払者から最後の受取人まで、任意の数の仲介者を経由して流れる現金支払いを表す。これは現金の核心的特徴を浮き彫りにする：一度引き出された現金は、銀行や中央当局の関与・監視なしに当事者間で自由に移転できる。点線の仲介者ノードは、現金が最終受取人に到達する前に、任意の数の仲介者（例：企業、個人ユーザー）の手を経由する可能性を抽象化している。機能上、仲介者を特定したり記録したりする必要はない。

物理的な現金は、いかなる仲介者も特定・記録する必要なく使用できる。通常、最初の支払者は引き出し時に特定され、最後の受取人は入金時に特定される場合がある。

2.2 「オンライン」と「オフライン」取引

「オンライン」および「オフライン」取引の定義については、欧州委員会によるデジタルユーロ創設に関する規制案[Eur23]の定義に従う。

- [Eur23]第 2 条第 14 項は、「オンラインデジタルユーロ決済取引」を「決済がデジタルユーロ決済インフラにおいて行われるデジタルユーロ決済取引」と定義する。

- [Eur23]第 2 条第 15 項は、「オフラインデジタルユーロ決済取引」を「物理的に近接した状態で実行され、支払者と受取人の双方のローカルストレージデバイスにおいて承認と決済が行われるデジタルユーロ決済取引」と定義している。

このアプローチに従い、現金を対象に適用すると、「オンライン」取引とは中央機関（利用者の銀行または中央銀行）への能動的な通信経路を必要とする取引を、「オフライン」取引とはそれを必要としない取引と定義する。すると現金は以下の性質を持つ：

- 最初の支払者は現金を引き出す際にオンラインでなければならない。しかし、現金が中間または最終の受取人に移転される際には、アクティブな通信は不要である。したがって、支払者は現金を別のユーザーに移転する際にオフラインであってもよい。
- 仲介者は、現金を受け取る時や他のユーザーに送金する時にオフライン状態であっても構わない。
- 支払先は支払いを受け取る際にオフラインであっても構わないが、預金を行う際にはオンラインでなければならない。

2.3 「トークン」とはデジタルコインである

以下では、「トークン」を物理的な硬貨や紙幣のデジタル版と理解する。つまり、ユーザー間で直接転送可能な独立した価値単位であり、即時的なオンライン接続を必要としない。各トークンは特定の額面を表し、有形の現金と同様に、それ自体が持つ貨幣価値を体現する。簡略化のため、以下では主に固定額面（例：1 ユーロ）のトークンを扱う。これにより核心概念の説明が明確になる。拡張については 7.3.3 節で論じる。

2.4 「現金類似」デジタル通貨

この節では、物理的な現金が満たすいくつかの異なる特性と、それらが「現金類似」デジタル通貨に期待される可能性を明らかにする。これは、デジタル の世界でこれらの特性を実現する上での可能性と限界を議論するための基礎となる。また、物理的な近接性は現金の特性であり、デジタル通貨で確実に実現するのは非常に困難であることも説明する。

2.4.1 現金類似通貨に求められる特性

現金類似通貨には、少なくとも以下の 4 つの特性が必要であり、これらは物理的な現金が満たしている：

1. **偽造不可能性**とは、支払先や銀行が本物と高い確率で受け入れるような偽造通貨を作成することが不可能な（あるいは少なくとも、偽造コストが偽造通貨の価値を上回るため非合理的な）性質を指す。

   物理的な現金は、以下の意味で偽造不可能である。中央銀行は、偽造を非常に困難にする、あるいは少なくとも費用対効果が悪いものとするために様々な対策を講じている。これには、透かし、ホログラム、特殊な印刷技術、特殊な紙、紫外線や磁気による特徴などが含まれる。これらの特徴は、特に複数の特徴を組み合わせた場合、複製が非常に困難になるように設計されている。偽造通貨の生産コストがその価値を上回る場合、通貨の偽造は法外な費用がかかる（したがって非合理的である）。したがって、特に大規模な偽造は起こり得ないと考えられる。

   物理的な現金とは異なり、デジタルデータは容易に複製またはクローン化できる。したがって、この文脈における偽造不可能性とは、新たなトークンを生成できないことのみを指す。デジタルトークンの複製は偽造とは見なされない（ただしトークンの二重支払いは防止する必要がある、下記項目 3 参照）。デジタル環境では、デジタル署名方式などの暗号技術や、ブラインド署名[Cha82, Cha86, CFN90]などのプライバシー保護プリミティブを用いて偽造防止を実現できる（第 7 節参照）。

2. **匿名性**とは直感的に、ユーザーの身元が可能なユーザー集合（いわゆる匿名性集合）の中に隠されることを保証する性質である。具体的な応用文脈によって、「匿名性」という総称が正確に何を指すか解釈が異なり、それを達成するには全く異なる技術を用いる必要がある。例えばデータベース分野では統計的集約、差分プライバシー、データ最小化、ノイズ添加が標準的手法だが、デジタル通貨は異なる形態の匿名性を求めるため別の手法が必要となる。

   デジタル通貨の文脈における匿名性とは、ユーザーが身元を明かさず、取引が特定されない状態で支払いを行えることを指す。したがって匿名性を、個人に追跡不可能な仮名と、行動の非関連付け可能性の組み合わせと定義する：

   - **仮名性**とは、ユーザーが実の身元と直接結びつかない識別子（仮名）の下で活動する性質を指す。

     現金の支払いのほとんどは、身分証明書を提示したり取引参加者の情報を開示したりする必要なく行われるという点で、現金は仮名性を有している。

     非常に重要な点として、単なる仮名性だけでは匿名性を達成できないことに注意せよ。仮名自体が実体を明かさなくても、同一ユーザーによる異なる取引を特定できる可能性があるからだ。例えば同一仮名で複数行動を行う場合、それらの行動は関連付けられる。時間の経過とともに、行動パターンや相互作用から十分な文脈情報が明らかになり、高い確率で仮名背後の個人を特定できる可能性がある。匿名性を実現するには、匿名集合内でユーザーが区別不能であること、そして彼らの行動が相互に、あるいは永続的な識別子に確実に結びつけられないことが必要だ。これは仮名を使用するだけでは達成されない。したがって、仮名性は身元保護の一層を提供できるが、それだけでは長期的な追跡やプロファイリングを防ぐことはできない。

   - **非連結性**とは、個々の取引が互いに、あるいは特定の主体と関連付けられない性質を指す。デジタル通貨の文脈では、取引の非連結性により、観察者や攻撃者が同一ユーザーに属する複数の活動を、たとえ異なる取引や時間軸にまたがって発生しても結びつけることが妨げられる。

     現金の非連結性は以下の意味で成立する。紙幣の固有シリアル番号を通じて多くの現金取引は理論上連結可能だが、個人・企業・銀行が日常取引でシリアル番号を記録しない限り、現金支払いは実質的に非連結と見なせる。さらに、紙幣が多くの仲介者を経由する場合、各仲介者が紙幣の元の出所と最終的な行き先について不確実性を生じさせるため、（複数の）仲介者を跨ぐ異なる取引の関連付けが著しく困難になる。したがって、ある時点で支払いが観察されたとしても、それを同一ユーザーの他の取引と関連付けることは事実上不可能である。関与する仲介者が多ければ多いほど、考えられる出所と終点の数は増え、匿名性の範囲が実質的に拡大する。ただし例外は存在する。例えば、特殊なケースでは法執行機関が銀行と協力し、犯罪に関与した特定の紙幣を追跡するためにシリアル番号を使用することがある。

   仮名性（Pseudonymity）はユーザーの身元を隠し、非連結性（Unlinkability）は同一ユーザーによる異なる活動を結びつけられないことを保証する。つまり、これらの活動が同一ユーザーに属するか異なるユーザーに属するかを検出することは不可能だ。これらの特性が組み合わさることで、行動を個人に遡及したり行動プロファイルを構築したりすることが不可能となり、ユーザーの匿名性を効果的に保護する。したがって、ユーザーが仮名であり、その行動がリンク不可能な場合に匿名性が達成される。

   実体のある現金は、この仮名性と非連結性の特性により、匿名決済システムの典型例と言える。第 5.1 節では、実体のある現金のデジタル版には、さらに強力な匿名性が求められる理由についても説明する。

   > 偽造防止性と匿名性を同時に達成できる、ブラインド署名などの強力な暗号技術がある。これらは第 7 節で論じる。

3. **二重支払いの防止**とは、同じ硬貨や紙幣を複数回使用することが事実上不可能であるという特性である。

   物理的な現金の場合、二重支払いの耐性は、それが唯一無二の物理的実体として存在することの直接的な結果として自然に生じる。この実体が取引で引き渡されると、元の所持者はもはやそれを所有せず、再び使用することは不可能になる。硬貨や紙幣の物理的な移転は、本質的に同じ通貨単位が二度使用されることを防ぐ。ただし、唯一無二の物理的実体としての存在は、デジタルデータには当てはまらないことに注意せよ。

   デジタル通貨システムにおいて二重支払いの防止は、以下の二つの方法で実現できる：

   (a) 技術的に同一トークンの複数回使用を防止する（例：悪意あるユーザーによるトークンの二重使用を防止するため安全なハードウェアコンポーネントを使用する、あるいはオンライン接続を用いて特定トークンの使用履歴を確認する）。

   (b) 二重支払いが発生した後にそれを検出する監査メカニズムを採用することで、当局が攻撃者を特定し法的措置で罰することができる。

   検出が用いられる場合、非誣告可能性[Bra94]も関連してくる。これは、誠実なユーザーが二重支払いの虚偽の告発を受けないという保証を指し、銀行による告発すら含まれない。二重支払いを検出する仕組み（追跡や身元開示プロトコルなど）が導入されている場合、非誣告可能性は、実際の二重支払い者だけが特定され、悪意のある者やシステム運営者を含む第三者が、無実のユーザーを不当に巻き込むためにシステムを操作できないことを保証する。

4. **移転可能性**とは、銀行を介さずに複数のユーザー間でトークンを交換できる可能性を指す。つまり、図 1 に示されたプロセスにおいて少なくとも 1 つの仲介者が存在しない方法である。

   非移転性通貨でも、オフライン環境では 2 ユーザー間（具体的には図 1 の最初の支払者から最後の受取人へ、仲介者なしに直接）で価値を移転できる場合がある。しかし、ユーザーからコインを受け取ると、別のユーザーへ転送できず、銀行に預けることしかできない。

   物理的な現金は本質的に譲渡可能である。なぜなら、銀行を介さずに、あるユーザーから別のユーザーへ、さらに別のユーザーへと直接手渡すことができるからだ。

   デジタル通貨の文脈では、安全なハードウェアに依存する方法（第 4 節参照）や暗号技術を用いる方法[CHL05, FPV09, BCFK15, BFQ21]（第 7.3.2 節参照）によって移転可能性を実現する技術が存在する。なお、移転可能性はデジタル通貨にとって必須要件ではない場合もある。回避策を設計することが可能だからだ。例えば、端末には二種類の残高を表示できる：(1) 他のユーザーから受け取った支払い（銀行との最終決済まで「凍結」され、他のユーザーへの支出不可）、(2) 銀行から受け取ったデジタルトークン（他のユーザーへの支出可能）。移転性を要求しないことで、システム設計の簡素化やハードウェア部品のセキュリティ要件削減が可能となる。

物理的な現金は、偽造防止性、二重支払い耐性、匿名性、移転可能性を提供する。続編では、（オフラインの）デジタル通貨が「現金類似」性質を実現するために、これらの特性をどの程度達成できるかについて議論する。

2.4.2 デジタル通貨における物理的近接性の実現難しさ

物理的な現金のもう一つの顕著な特徴は、移転を行うために何らかの**物理的な近接性**を必要とすることだ。これにより、特に多額の移転や移転が秘密裏に行われる場合（例えば当局から隠す場合）、長距離移転はかなり困難になる。同時に、物理的近接性は容易に確認できる。現金取引に関わる全ての当事者は、単に紙幣

を直接交換するだけで、相手方が物理的に存在していることを即座に確認できるからだ。物理的現金では当然のこの特性は、デジタル通貨では容易に再現できない。

デジタルシステムは距離を「認識」できない。データ通信で届く 1 バイトのデータは、2 センチ先から来た場合も別の大陸から来た場合も、同じように見える。したがって、デジタル通貨において物理的な近接性を強制することは（オンラインかオフラインかを問わず）本質的に困難だ。デジタル通信経路は位置を特定できないからだ。この特性は、NFC や Bluetooth といった短距離通信プロトコルを使用するデバイスで通貨が実装される場合にも当てはまる。バイトデータ自体には、送信者と受信者が実際に同じ場所に存在していることを証明する要素は何もない。

この隙を突くのが中継攻撃だ。攻撃者は一方の端末（支払者側）の近くにプロキシを配置し、もう一方の端末（受取人側）の近くにも別のプロキシを置く。プロキシは高速接続でメッセージを中継するため、各端末は相手端末が直接近接していると「信じ込む」のだ。こうした中継攻撃はよく知られている。例えば、車泥棒はリレーを利用して、家の中から車庫の車に向けて車のキーフォブの信号を転送できる[FDC11]。電子身分証明の文脈では、リレー攻撃によって遠隔のパスポートがリーダーの近くに存在しているように見せかけることが可能だ[KW05]。

残念ながら、利用可能な対策は非常に限られている。距離制限プロトコル（例：[BC94, ABB+ 18]）は、高速なチャレンジ・レスポンス交換の時間を計測することで距離の上限を推定しようとする。その核心的な考え方は、信号が光速 を超える速度で伝播できないという事実にある。したがって、あるデバイスがチャレンジを発行し、他のデバイスが応答する速度を測定すれば、距離の上限を推定できる。なぜなら、真に近接したデバイスは極めて迅速に応答できるはずだが、中継されたメッセージはより長い時間を要するからだ。しかし実際には、これを確実に実施するのは極めて困難だ。市販デバイスは予測不能な処理遅延を生むため、検証者は物理的な伝播時間だけを分離できない。攻撃者は特殊な低遅延ハードウェアを使って中継遅延を削減し、遠隔デバイスの応答を許容閾値内に収めることも可能だ。

別のアプローチとして、近接性に基づくペアリング[ZPZ+ 16]が考えられる。これは 2 つのデバイス間の物理無線チャネルの特性を、鍵導出および認証プロトコルの追加入力として利用する手法だ。近接性を強制する興味深い手法ではあるが、現時点では技術成熟度がかなり実験的な段階にあるようだ。

> 日常的なデバイスにおいて中継攻撃を確実に防止することは、依然として大きな課題である。オフラインのデジタルユーロに近接性が本質的な要件であるならば、それを保証する効果的な技術を開発・導入するか、あるいはこの制限を認識し中継攻撃のリスクを考慮したシステム設計を行う必要がある。

本稿では、物理的近接性をデジタル通貨において確実に強制可能な現金の特性とは見なさない。

2.5 セキュアハードウェア

以下において、「**セキュアハードウェア**」という用語は、スマートカードのような専用ハードウェア、あるいはスマートフォンなどの汎用コンピュータ内のセキュア環境を指す。これらは特定の不正操作に対して耐性があると想定される。

重要なのは、「セキュアハードウェア」という用語を、システムが実際に安全であること、すなわち特定のセキュリティ特性を達成していることを示すために使用しない点だ。これは、ハードウェアが「安全である」という概念が絶対的かつ永続的な状態ではなく、脅威や技術の進化によって形作られる流動的な目標だからである。システムが要求されるセキュリティ特性を達成しているかどうかは、新たな攻撃や脆弱性が発見されるにつれて時間とともに変化する可能性がある。

代わりに、我々は「セキュアハードウェア」という用語を、デバイスを利用するシステムがデバイスに要求する特定のセキュリティ形態を示すために使用する。この要求は時間経過とともに安定している。例えば、システムがユーザーデータの機密性や取引記録の完全性を要求する場合、これらの要求自体は（システムが変更されない限

り）変わらない。達成方法が新たな攻撃技術に対応して適応する必要があっても、要求自体は不変である。こうした想定されるハードウェアのセキュリティ特性に関する議論については、第 4 節を参照のこと。また、異なるアプローチが異なるハードウェアのセキュリティ特性を要求する様子を図示した表 2 も参照されたい。

ハードウェアに求められるセキュリティ要件が増えるにつれ、期待されるハードウェアのセキュリティ特性は次第に強化される（つまり、現実的ではなくなり、保証が困難になる）点に留意する必要がある。あるアプリケーションの文脈において 特定のセキュリティ特性を達成するハードウェアは、異なるアプリケーションの文脈ではセキュリティを提供するには不十分である可能性がある（4.1 節参照）。既存のハードウェアを、デジタル通貨のサポートに特化した追加機能で拡張することは、特に下位互換性が要求される場合、技術的に困難あるいは不可能な場合がある。既存プラットフォームの適応が不可能な場合、新たなハードウェアの設計と導入が必要となることがあり、これは往々にして費用と時間を要する。

ハードウェアデバイスには、共通基準認証などのセキュリティ認証が存在する。こうした認証は、特定のハードウェアデバイスが期待されるセキュリティ特性を確かに満たすことを保証する要素と見なせる。しかし重要なのは、こうした認証は特定の基準を満たすことを確認するだけであり、デバイスが実際に安全であり、今後も安全であり続けることを保証するものではない点だ。なぜなら、それは現在および将来のあらゆる攻撃が存在しないことを保証する必要があるからである。[1]

「セキュアハードウェア」における「セキュア」という用語は、デバイスが実際に安全であることを指すのではなく、デバイスに対して特定のセキュリティ特性を要求し、前提とする事実を指す。異なるセキュリティ要件の数が増えるにつれ、期待されるハードウェアのセキュリティ特性は現実離れし、保証が困難になる。

[1]例えば、これは GDPR 第 25 条(3)項および第 32 条(3)項にも反映されている。ここでは、認証がコンプライアンス達成の要素となり得るが、一般的にそれだけでは十分とは見なされないことが述べられている。

3. CAP 定理とオフラインデジタル通貨への応用

検討すべき問題

1. CAP 定理が有効である場合、デジタルユーロのトークンベースオフライン方式の設計・構築にどのように適用できるか。また、その三つの特性（一貫性、分割耐性、可用性）は電子決済サービスの文脈でそれぞれ何を意味するか。

3.1 分散システムと CAP 定理

CAP 定理[Bre00, GL02]は分散システム理論における基礎的な数学的命題である。これらのシステムは、要求と応答を通じてネットワーク上でデータを交換するノードを含む。この定理は、このような分散システムが以下の 3 つの特性の中から同時に保証できるのは 2 つだけだと述べる：

- 一貫性（C）：全てのノードが同時に同一のデータを見る。
- 可用性（A）：すべてのリクエストが応答を受ける。ただし、最新のデータを含まない場合もある。
- 分割耐性（P）：ネットワーク分割や通信障害が発生した場合でも、システムは動作を継続する。「分割」とは、ノード *A* と *B* が存在し、*A* から *B* への通信経路が一切存在しない時点を指す。

本節で検討する問題に答えるためには、まず「一貫性」「可用性」「分割耐性」という用語をオフライン型デジタル通貨の文脈に適用する必要がある。

CAP 定理は、リクエストとレスポンスを通じてネットワーク上でデータを交換するノードで構成される特定の分散システムを対象とする。具体的には、このモデル外のシステム、例えば追加でセキュアハードウェアを使用するシステムなどは対象外である。

3.2 オフラインデジタル通貨における CAP 定理

例えばデジタルユーロのトークンベースのオフライン形態のようなオフラインデジタル通貨は、取引時に中央機関へのリアルタイム接続を必要とせず、ピアツーピア取引を可能にする。CAP 定理は、このようなシステムに対して次のように適用される。

- **一貫性（C）**とは、システム全体（ウォレット、デバイス、分散型ノードなど）が流通する通貨について共有され正確な認識を維持する状態を指す。

  これには、デジタル資金が二重に支出される（「二重支出」）ことを防ぎ、ユーザーが実際よりも多くの資金を保有しているとシステムを欺くことを防止することが含まれる。取引がオフラインで行われる場合（例えば、インターネット接続のない 2 台のスマートフォン間の ）であっても、システムは各取引の有効性を保証し、残高が正しく更新されるようにしなければならない。

  一貫性のあるオフライン通貨システムは、オフライン端末が後で再接続した際、オフラインで実行された取引が広範なネットワークに矛盾なく正確かつ一貫して統合されることも保証する必要がある。結局のところ、システムのあらゆる部分が、誰が何を所有しているかについて合意しなければならない。たとえその情報の異なる部分が一時的にオフラインで保存または交換されていたとしてもだ。

- **可用性（A）**：オフラインデジタル通貨において可用性とは、デバイスがインターネットや中央システムに接続されているかどうかにかかわらず、いつでも支払いが行えることを意味する。したがって、システムはオンライン検証を待たずに、二者が直接かつ即時的にデジタル通貨を交換できるようにしなければならない。

可用性は**オフライン対応通貨に本質的に備わる特性**である。接続問題によって支払いが阻害・遅延せず、オフライン時でも通貨システムが利用可能であることを保証する。これによりユーザーは通貨の継続的な機能性を信頼でき、実物現金と同様に日常利用に実用的なものとなる。

- **分割耐性（P）**：オフライン取引は必然的にネットワーク分割を生む。つまり、インターネットやネットワーク接続の欠如により、デバイスやユーザーがシステムから隔離される状況だ。こうした分割状態でも、オフライン通貨はサーバーとの即時通信に依存せず、ユーザーが安全な支払いを実行し残高を管理できるようにしなければならない。

  分割耐性は、オフライン対応通貨に本質的に求められる特性である。中央機関へのオンラインアクセスなしに動作できることが「オフライン」の定義そのものだからだ。分割耐性のあるシステムは、接続が途切れないとは限らない現実世界において、回復力と実用性を保証する。

CAP 特性	デジタル通貨における意味	オフライン対応デジタルユーロへの適用
一貫性（C）	全ての端末が同一データを反映する	オフライン時は犠牲となり、オンライン時に復元される
可用性（A）	取引はいつでも処理される	オフライン利用の基本要件
分割耐性（P）	接続の喪失に耐える	オフライン利用の基本要件

表 1：オフラインデジタル通貨における一貫性、可用性、分割耐性の意味と適用

分割耐性と可用性が基本要件であるため、CAP 定理はオフラインデジタル通貨に根本的な制約を課す。すなわち、システムは一貫性を保証できない。

ただし、この帰結は限定的であることに留意すべきだ。なぜなら、オフラインデジタル通貨を特定の分散システムと見なした場合にのみ適用されるからである。安全なハードウェア要素や半オフライン環境（5.2.3 節）といった追加の安全策を考慮することで、この定理を回避できる。

CAP 定理は分散データベースの文脈でよく議論されるが、これは分散システム全般への広範な適用性の一例に過ぎない。特に CAP における「一貫性」とは、全てのデバイスがデータセット全体を冗長に保存しなければならないという意味ではない。むしろ、指定された整合性モデルに従って、全てのノードがシステム状態の一貫したビューを提示することを保証することを指す。例えばローカルなトランザクション履歴など、ノードが部分的なデータのみを保存する場合でも、システム全体でデータが論理的に一貫していることが重要であるため、この保証は成立する。したがって、CAP 定理は、システムが全データをあらゆる場所に複製する場合でも、データの一部を構成要素間で分散させる場合でも適用される。

3.3 CAP 定理の妥当性について

本節で検討する問題は、CAP 定理が「有効である場合」の適用可能性について問うものである。ただし、上記の議論と結論は、分散システム理論における一般的な数学的命題としての CAP 定理の有効性とは独立して成り立つ可能性があることに留意すべきである。つまり、仮に将来的に定理の証明に不備が見つかったり、定理が曖昧であることが判明したり[Kle15]、主張されているほど一般的でなかったり、あるいは誤りであることが判明した場合でも（それは予想されないが不可能ではない）、本節で論じた主な議論は、上記の意味で分散システムと見なされるオフラインデジタル通貨には依然として適用可能である。**この問題は CAP 定理に焦点を当てて**

いるが、オフラインデジタル通貨という特例に適用された推論と導かれた結論は、それ自体で成立し、CAP 定理とは独立して有効であり続ける可能性がある。

4. セキュアハードウェアによる一貫性の達成

検討課題

2. セキュア（ハードウェア）要素に対する過去の（成功した）攻撃の歴史を考慮すると、多重支出は考えられるか。もし考えられる場合、オフラインのデジタルユーロインフラのエンドユーザーデバイス（例：スマートフォン）を侵害しようとする試みに対して、さらなる防御ラインを構築するためにどのような技術的対策を追加できるか。

4.1 二重支払い攻撃とセキュアハードウェア

スマートカード、モバイルセキュアエンクレーブ、信頼実行環境（TEE）などのセキュアハードウェア要素に対する成功した攻撃には長い歴史がある。詳細は[Koc96, KJJ99, KJJR11, OP11, MIE17, WCP+ 17, DDE+ 18, VMW+ 18、CCX+ 19、MOG+ 20、CYS+ 21、CVM+ 21、vSY+ 24、SMvH+ 21、FQF+ 24]およびそれらの参考文献を参照のこと。これらの研究論文は、最小限の物理的アクセス、あるいはサイドチャネルやソフトウェアベースの手法によって、暗号鍵の抽出、認証メカニズムの回避、セキュアエレメントの複製、悪意のあるコードの注入、ハードウェアからの機密データの流出が可能であることを示した研究の一部である。より具体的に言えば、スマートカードに対するサイドチャネル攻撃により、攻撃者は暗号処理中の消費電力の変動を分析することで秘密鍵を復元できるようになった[KJJ99, KJJR11]。モバイルセキュアエンクレーブや TEE においては、研究者らがマイクロアーキテクチャ攻撃を用いて隔離保証を破り秘密情報を抽出する能力を実証している。Foreshadow[VMW(+) 18]や Plundervolt[MOG(+) 20]は、Intel の SGX のような TEE が一時的実行や電圧フォルト注入によって侵害される可能性を示した。iOS デバイス向けブートロム脆弱性 Checkm8（https://github.com/axi0mX/ipwndfu 参照）のような攻撃は、何百万ものスマートフォンを侵害し得る低レベルで永続的、かつ修正不可能な脆弱性の潜在性を示している。

特にモバイル端末のセキュアエンクレーブや TEE に対する攻撃は根本的な課題を浮き彫りにしている。安全とされる端末内で動作するアプリケーションロジックが複雑になればなるほど、脆弱性からの防御は困難になるのだ。注目すべきは、これらの攻撃の一部が攻撃者が基盤ハードウェアに直接アクセスしなくても、遠隔で実行可能だということだ。物理的な端末を実際に所持する攻撃者に対する防御はさらに困難である。物理アクセスは通常、より強力な攻撃ベクトルを可能にするからだ。

これらの事例は、ハードウェアセキュリティに関する膨大な研究の中から、ごく一部をランダムに選んだものに過ぎない。技術的知識と適切なツールを備えた熟練した攻撃者が、「セキュア」なハードウェアコンポーネントによって実装された防御を突破した攻撃例は、他にも数多く存在する。

したがって、暗号鍵管理などの機密操作を保護するために設計されたセキュアなハードウェアコンポーネントであっても、学術研究と実世界の両環境において、**多種多様な攻撃に対して脆弱**であることが繰り返し示されてきた。スマートフォンやスマートカードのようなエンドユーザーデバイスが、オフラインデジタル通貨のようにリアルタイム監視なしに自律的に価値を保管・ 転送することが想定される環境では、安全とされたが実際には脆弱なハードウェア要素が侵害されると、悪意ある主体がトークンの複製、カウンターの改ざん、残高のリセットを可能にし、二重支払いやその他の攻撃を許容する恐れがある。

この文脈では、デジタル通貨の場合、**「攻撃者」と「ユーザー」が同一の個人である可能性**を認識することも極めて重要だ。攻撃を行うユーザーは自身のデバイスを改ざん・分析するために無制限のアクセス権と十分な時間を持つ可能性があるため、セキュリティ確保の難易度が大幅に高まる。

さらに、標準的なハードウェアセキュリティモジュールは、基本的な暗号機能のための安全な鍵保管庫など、特定のデータ機密性・完全性の確保に焦点を当てている。しかし、複雑なトランザクションプロトコルロジックの強

制や、悪意のある（技術的に高度なスキルを持つ可能性もある）ユーザーに対するオフライン価値移転の一意性の保証は、達成がはるかに困難である。

ここで提示した例は、より広範な脅威の存在を示す具体的な攻撃の事例として理解すべきである。これらの攻撃の一部は、現行のハードウェア設計では既に十分に緩和されているが、それでも根本的な脅威は依然として現実のものだ。歴史が示すように、新たな攻撃手法は頻繁に出現し、たった一つの巧妙な新発想が新たな実用的なエクスプロイトを生み出すことも多い。したがって、今日安全と見なされているハードウェアが永遠に安全であり続けると想定するのは賢明ではない。

脆弱なハードウェアの交換は、不安全なソフトウェアへのパッチ適用よりもはるかに困難で、時間がかかり、費用がかかる点も考慮すべきだ。ハードウェアベースのセキュリティ前提に依存するシステム、特にデジタルユーロのような大規模なケースでは、この動態を慎重に検討しなければならない。

二重支払いは明らかに想定可能であり、ハードウェア要素を追加の保護層として使用する場合でも、非常に慎重に検討しなければならない。ハードウェアが安全な鍵保管といった従来の暗号利用ケースでは安全と見なされていても、オフラインデジタル通貨における二重支払い攻撃のようなより複雑な不正シナリオに対しては、十分な保護を提供しない可能性がある。

4.2 多重防御による二重支払いの軽減

オフラインのデジタル通貨システムにおいて二重支払いのリスクを軽減し、より強固な防御ラインを構築するには、技術的、アーキテクチャ的、運用的な安全対策を統合した包括的なアプローチが必要だ。これには以下が含まれる：

1. ハードウェアベースの安全対策：

   (a) **安全なハードウェアの使用。**物理的・論理的攻撃に対する耐性を提供する改ざん防止ハードウェア要素を採用する。

   (b) **安全かつ監査可能な起動プロセス。**暗号署名付きファームウェアを用いて、エンドユーザーデバイスが検証済みかつ信頼できる状態で起動することを保証する。不正なソフトウェアがセキュアモジュールにアクセスしたり変更したりするのを防ぐための適切な措置を実施する。

   (c) **ハードウェアの多様性か均質性か？** 多くのシステムが同一または極めて類似したプラットフォームに依存する均質なハードウェア環境は、単一障害点を作り出す可能性がある。広く展開されたハードウェアアーキテクチャの単一インスタンスに対する攻撃が成功した場合、その攻撃は大規模に複製され、エコシステムの大部分を危険に晒す。デバイス種別を跨いだ多様なセキュアハードウェア設計・実装を採用することで、単一ハードウェア設計の普遍的脆弱性によるシステム的障害のリスクを低減できる可能性がある。

   しかし多様性には重大な欠点もある。普遍的な障害リスクを軽減する一方で、システムの複雑性を著しく増大させる。多様なハードウェア環境は、設計・実装・サプライチェーン・更新メカニズムの違いから、より広範な潜在的脆弱性を生み出す可能性がある。これにより、断片化したパッチ適用慣行や攻撃者が探索できる攻撃対象領域の拡大といった弱点がさらに増大する。

   エンドユーザーデバイスが主に少数のメーカーが製造するスマートフォンやスマートカードで構成される技術環境では、エコシステム全体でのハードウェアの均質性が高いため、プラットフォーム固有の脆弱性の潜在的な影響が大きくなる。これはシステム設計において考慮されなければならない。

2. 例えば以下のような概念を実装することで、回復力のあるシステム設計が可能となる：

(a) 将来のハードウェアやプロトコルレベルの攻撃に対する堅牢性を最大化し、多様なデバイスやメーカー間での広範な互換性を確保するためには、**ハードウェアの仮定への依存を最小限に抑え、ヘッジされたセキュリティ**を採用することが望ましい。

特定のケース（特にオフライン環境での二重支払い防止の強制）ではハードウェアベースの解決策が必要となる場合もあるが、それらは必然的に重大なリスクをもたらす。具体的には、デバイス侵害への脆弱性、信頼できる製造プロセスへの依存、サイドチャネル攻撃への感受性などである。したがって、安全なデジタル通貨の設計では、可能な限りこうした依存関係を最小限に抑えるべきである。

ブラインド署名（第 7 節参照）のような暗号プリミティブは、偽造防止性や匿名性（および追加のセキュリティ特性）について、ユーザーのデバイスにおけるハードウェアのセキュリティ仮定とは独立して成立し得る、十分に理解され厳密に分析された保証を提供し得る。

理想的には、システム構成要素は、ハードウェア層または暗号層のいずれかが侵害されない限りセキュリティが維持されるように設計されるべきである。これにより、一方の層が失敗した場合に他方が安全装置として機能する。この二重層アプローチは、ハードウェアと暗号技術が互いに補完し合い、相互の回復力を提供し、全体的な堅牢性を高める「多重防御」を実現する。

(b) オフライン取引に関連するリスクを管理するための制御を実装する、**転送制限**やその他のリスクベースのルール。これには、オンライン接続なしで取引できる価値の上限や、取引が発生できる頻度の制限などが含まれる可能性がある。さらに、ユーザーが保持できる最大オフライン残高の上限設定や、ピアツーピア取引のホップ数制限といった設定可能なポリシーは、デバイスまたはデバイス群が侵害された場合の潜在的な損害を抑制するのに役立つ。これらのルールは、利便性とプライバシー・セキュリティのバランスを取り、システムを重大なリスクに晒すことなくオフライン機能を利用可能にしなければならない。

(c) **遅延確定**とは、オフライン取引が再接続時に確認されるまで暫定的なものとみなす手法を指す。これは、適切な検証が行われるまで当該取引の最終決済が遅延することを意味する。このプロセスを支援するため、デバイスは取引ログを維持し、後日の監査を可能にする。これらのログは、オフライン活動中の紛争や不正の疑い発生時に、説明責任と追跡可能性を確保するのに役立つ。ただし、こうしたログの維持はユーザープライバシーへのリスクをもたらすため、慎重に検討すべきトレードオフとなる。

(d) **有効期限や鮮度制約を伴うトークン設計**では、短命または時間制限付きのトークンを使用し、盗難や複製されたトークンに関連するリスクを低減する。これらのトークンには有効期限タイムスタンプが含まれ、限定期間のみ有効であることを保証する。これにより、特にオフラインや半接続環境において、トークンの悪用による潜在的な損害を制限し、全体的なセキュリティを強化できる。ただし、この手法は可用性、ユーザー体験、長期的な価値保存手段としてのデジタル通貨の利用との潜在的な衝突を回避または最小化するよう設計されなければならない。

(e) 全てのシステム構成要素の設計と実装における**透明性**は不可欠である。これには、システム全体の設計仕様の公開、各構成要素の正確なセキュリティ目標と攻撃者モデルの明示、オープンソースソフトウェア実装とハードウェア設計の公開、そして独立したセキュリティ研究者や倫理的ハッカーがシステム設計を精査し脆弱性を特定し、セキュリティ強化に貢献できるよう公開されたアーキテクチャ文書が含まれる。不透明性や独自仕様のブラックボックス設計に依存するシステムは、隠れた欠陥が放置される恐れがある。こうした欠陥は国家レベルの攻撃者や組織犯罪集団といった手練れの攻撃者に発見・悪用される可能性があり、採用すべきではない。外部レビューを可能にし、オープンな文化を育むことで、より強固なセキュリティを実現できる。また、新たな脅威や変化する攻撃者の能力への迅速な適応も可能となる。

3. 技術的・体系的なレベルでの監視には以下が含まれる：

(a) **新たなハードウェア脆弱性や攻撃手法の監視。**システム運用者は、進化する脅威や攻撃手法を継続的に監視する仕組みを構築しなければならない。この監視により、暗号解読攻撃、ハードウェア改ざん、その他のシステム侵害手法が早期に検知され、適切に対応されることが保証される。これにより 脆弱性が露呈する期間が短縮され、デバイスに保存された価値の完全性が維持され、デジタル決済システムの信頼性が支えられる。

(b) **異常検知。**同一のデジタルトークンが複数回使用されるなど、二重支払いを示唆する不審なパターンをシステムで監視する手法が考えられる。重要なのは、この種の分析をプライバシー保護方式で実行する技術が存在することだ。これにより、二重支払いが検出されない限り、ユーザーID や取引詳細は隠蔽されたままとなる。この場合のみ、システムは不正取引に関連する ID を特定する。第 7.3 節および第 7.4 節も参照のこと。デジタルユーロ規模のオフライン通貨への適用可能性を含む、こうした具体的なシステム設計の詳細な分析は膨大な労力を要し、本稿の範囲外である。しかしながら、デジタルユーロの安全なオフライン方式設計においては、こうした技術を検討・評価すべきである。

(c) **責任ある開示の枠組み。**脆弱性の責任ある開示のための枠組みを確立することは不可欠である。セキュリティ問題を報告するための明確な連絡経路を提供し、発見された脆弱性についてシステム運営者に慎重に通知され、パッチまたは緩和策が開発され、問題が公になる前にユーザーとシステムが保護されることを保証しなければならない。責任ある開示に適切に対応する組織は、セキュリティ態勢の成熟度、改善への開放性、ユーザー保護への取り組みを示している。

脆弱性を発見したセキュリティ研究者は、法的責任を恐れることなく報告できるべきだ。責任ある開示を奨励することは、より安全なエコシステムを促進するだけでなく、研究者とシステム開発者の間の信頼を築く。バグ報奨金プログラムなどの報酬制度は、欠陥の特定と報告を促し、セキュリティ問題の発見と解決を加速させる可能性がある。安全で構造化された開示プロセスを支援することで、開発者とシステム運用者は、システムのセキュリティと回復力を向上させるために協力する、より広範で関与するセキュリティコミュニティの恩恵を受けるだろう。

適切なセキュリティメカニズムの組み合わせは、具体的な要件、プロトコル、前提条件、脅威モデルと攻撃者モデル、セキュリティ目標、システム設計に依存する。前述の手法のサブセットまたは全て、および追加の手法を含む場合がある。

4.3 結論

セキュアなハードウェア要素は、オフラインのデジタルユーロを二重支払いその他の攻撃から保護する上で重要な役割を果たす可能性がある。しかし、潜在的な脆弱性は現実的かつ信憑性のあるリスクである。したがって、回復力のある設計はハードウェアセキュリティのみに依存すべきではなく、ハードウェア保証と暗号技術、ソフトウェア保護策、分析、リスクを意識した運用制約を組み合わせた多層防御アプローチを採用すべきである。透明性と脆弱性を信頼性高く責任ある形で開示する枠組みが不可欠である。これらの対策を組み合わせることで、攻撃の実行可能性と影響を大幅に低減でき、システムのセキュリティと耐障害性を大幅に向上させることが可能となる。

5. 代替技術的解決策

検討事項

3. デジタルユーロのオフライン形態を「現金類似」もの、すなわち二重支払いの観点で耐性があり、同時に匿名性のある使用を可能にする実現可能な代替技術的解決策は存在するのか…

   (a) CAP 定理を遵守しつつ、

   (b) 例えば「可用性」を犠牲にしてオフラインモードを実現するなど、3 つの特性のうち 1 つを満たさないことを受け入れつつ、実用的な実装と使い勝手への影響はどうか？

   (c) 匿名性は全ての当事者ではなく、消費者／支払先（自然人）のみ／少なくともそれらに対して適用され、販売者（「送信者匿名性」）とは対照的であり、ハイブリッドソリューションとなる可能性があるか？

5.1 オフラインデジタル通貨における現金類似特性の実現課題

オフラインデジタル通貨において、偽造防止性、二重支払い防止性、匿名性、移転可能性を実現することは、技術的・概念的に重大な課題をもたらす。これらの特性は相互に矛盾する可能性があり、またデジタル環境には、従来の現金で自然にこれらの特性を強制する物理的制約が存在しないため、課題が生じる。デジタル情報は、硬貨や紙幣のような物理的対象とは異なり、本質的に非常に容易かつ完全に複製可能である。この固有の物理的制限の欠如が、デジタル現金システムに核心的な課題を創出する：

- デジタル通貨における**二重支払いの防止**には技術的な安全策が必要だ。なぜなら、物理的な物体が本来持つ唯一性――同じ硬貨や紙幣が二度以上使われるのを防ぐ特性――はデジタル領域には存在しないからだ。これを実現するには、二重支払いを防止するシステム設計（7.3.1 節参照）か、不正利用者を追跡・特定するメカニズムを実装し事後的に検出可能にする（7.3.2 節参照）かのいずれかが必要だ。

  オンライン型デジタル通貨では、取引ごとに信頼できる機関（中央銀行やブロックチェーン型暗号通貨の分散型台帳など）への通信経路が存在する。この場合、信頼できる機関が取引承認前にリアルタイムで検証を行うことで二重支払いを防止できる。ユーザーがデジタルトークンを支出しようとするたびに、その取引はオンラインシステムに送信され、トークンが既に支出されていないか確認される。支出済みでなければ取引は承認・記録され、そうでなければ拒否される。このプロセスにより、中央機関（分散型合意形成プロトコルで実装される可能性あり）が最新かつ一貫性のあるグローバル記録を保持するため、各デジタルトークンは一度しか支出できないことが保証される。重要なのは、第 7 節で説明した技術を用いれば、全取引のグローバルログを持たずにプライバシーを保護する形でこれを実現できる点だ。これにより、トークン自体に物理的な唯一性や安全なハードウェアへの紐付けを要求せずとも、二重支払いを防ぐ強力な保証（ ）が得られる。ただし、ユーザー（より正確には取引の受取人）が信頼できる機関にオンライン接続していることが本質的に必要となる。

  オフラインのデジタル通貨では、取引時に中央機関へのアクセスがないため、二重支払いの防止ははるかに困難である。デジタルデータは容易かつ完全に複製可能なため、システムはリアルタイム検証なしに二重支払いを防止または検出する技術的メカニズムを採用し、匿名性を確保する方式を採用しなければならない。

  – 一つのアプローチは、トークンが一度だけ使用されることをデバイス上でローカルに強制するセキュアハードウェアに依存することだ。このハードウェアは、トークン、秘密鍵、取引データを漏洩しないことが信頼されなければならない。第 4 節で議論されたこのアプローチに関連するリスクを考慮すると、セ

キュアハードウェアは他の技術的・体系的な対策で補完されるべきである。例えば第 7 節では、ハードウェアのセキュリティに依存せず強力な匿名性を実現する暗号技術を用いた手法を説明する。関連手法は[ACK(+) 24]などで採用されている。

– あるいは、トークンに暗号的特徴を埋め込み、後から不正なユーザーを特定できるようにすることで、二重支払いを事後的に検出するシステムも考えられる。これにより、ネットワークが再接続された際に二重使用されたトークンを攻撃者に結びつけて追跡できる一方、正当な使用時にはユーザーの匿名性を維持できる（セクション 7.3.2 参照）。

ただしこの手法は追加リスクを生むことに注意が必要だ。二重支払いの発生から検出までの時間が長ければ長いほど、攻撃者が不正取引から利益を得て罰則を回避する機会が増大する。攻撃者が意図的にデバイスやネットワークを隔離してこの機会を拡大するなど、オフライン状態が敵対的に誘導される可能性すらある。これらの課題は、オフライン取引の一方が EU の監督外で活動し、執行が不確実となるような越境環境ではさらに複雑化する。

さらに、国家主体が二重支払い攻撃に関与または支援する可能性は新たな次元を加える。国家主体はネットワーク可用性の操作、ハードウェアの侵害、あるいは管轄区域の隙間をはるかに大規模に悪用する資源を保有している可能性があるからだ。

したがって、オフライン環境では物理的な唯一性の制約やオンライン環境の同期記録の制約が欠如しているため、二重支払いの耐性は暗号技術、ハードウェアの仮定、あるいはその両方の組み合わせによって慎重に設計されなければならない。

- **デジタルキャッシュは、物理的な現金よりも強い非連結性を必要とする。**物理的な現金は、その擬似匿名性と実質的な非連結性から、匿名決済システムの典型例と見なされることが多い。しかし重要なのは、紙幣のシリアル番号が個人、商人、銀行によって日常的に記録されていないという前提で、現金は 非連結と見なされている点である。

  一方、デジタル通貨は内部構造がユーザーに透明でないデバイス上で動作するため、隠れた追跡を実装しやすく、検出を困難にする。結果として、オフラインのデジタル通貨が物理的な現金と同等の「現金類似」匿名性を保証するには、はるかに強力な非関連性保証が必要となる。第 7 節では、ブラインド署名などの高度な暗号技術を用いて、こうした強力な非関連性を実現する方法について論じる。

  物理的な現金が実質的に匿名性を保つのは、（隠密な）紙幣追跡が、特に大規模では実施が困難だからだ。これに対し、デジタル通貨は内部構造が不透明なデバイス上で動作するため、隠れた監視がより容易に、かつはるかに大規模に実施できる。このため、デジタル通貨にはより強固な匿名性が求められる。これは適切な暗号技術によって確実に実現可能である（第 7 節参照）。

- **二重支払いの検出と匿名性の間の緊張関係。**攻撃を事前に確実に防止できず、事後的にしか検出できない場合、攻撃者を罰するために悪意のあるユーザーを特定する必要がある。これには何らかのユーザー追跡可能性が必要であり、匿名性をある程度損なう可能性がある。しかし、高度な暗号技術を用いて検出タグを実装するプロトコルも存在する。このタグはコインが二重に支出された場合にのみ明らかになる。こうしたプロトコルについては第 7.4 節で論じる。

- **長期的な安全性。**オフライン型デジタル通貨は、改ざん防止性、匿名性、安全なハードウェアコンポーネント間の認証といった特性を保証するために暗号技術が必要だ。デジタルユーロのオフラインモードは長年にわたる使用を想定して構築されるため、全システムコンポーネントの長期的な安全性を考慮しなければならない。

セキュアハードウェアの仮定に関しては、デバイスのライフサイクル、改ざん耐性の堅牢性、時間の経過に伴う進化する攻撃手法への耐性を慎重に検討する必要がある。これには、ハードウェアセキュリティモジュール、セキュアエレメント、信頼実行環境が導入時に強力な保護を提供するだけでなく、脆弱性が発見された場合に更新、交換、または失効できることも含まれる。さらに、ハードウェアの信頼性に関する仮定は現実的であり、単一障害点を最小限に抑え、一部のデバイスが侵害されてもシステムリスクが封じ込められるようにしなければならない。

暗号アルゴリズムに関しては、稼働中のシステムにおいてアルゴリズムを容易に交換可能な設計（「暗号的俊敏性」）を強く推奨する。これは特に将来の量子攻撃の可能性を念頭に置いたものである。システムは、（量子）暗号解読技術の進歩により暗号アルゴリズムの交換が 必要となる潜在的な状況に備えるべきである。

物理的な現金と同等の匿名性、安全性、利便性を完全に再現するオフラインデジタル通貨という構想は概念的には魅力的だが、これを実践で実現するには複雑な技術的トレードオフの領域を慎重に検討する必要がある。物理的制約の欠如、堅牢な長期セキュリティの必要性、隠れた監視を容易かつ大規模に実施する可能性、匿名性と追跡可能性の間の緊張関係は、プライバシー保護暗号技術の慎重に設計された組み合わせを要求し、信頼できるハードウェアが必要となる場合がある。

5.2 解決策の検討

5.2.1 CAP 定理下における「現金類似」ソリューションの実現可能性

第 3 節で概説したように、オフライン対応のデジタル通貨システムは定義上、分割耐性（P）と可用性（A）を必要とする。したがって、CAP 定理は、一貫性（C）を達成するためには、CAP 定理が考慮するシステムモデルの範囲を超えたツールや技術を用いる必要があることを示唆している。したがって、現金類似システムを設計する一つのアプローチは、オフライン使用時の一時的な不整合（すなわち二重支払い）のリスクを受け入れ、システムレベルの安全対策を通じてこれらのリスクを管理することである。このような解決策には、例えば以下が含まれる：

- **セキュアハードウェアによる強制：**デバイスがローカルな一貫性を強制し、セキュアハードウェアを用いて二重支払いを防止する。ただし、これは第 4 節で論じたセキュアエレメントの制限や攻撃ベクトルの影響を受ける。
- **取引制限の利用**：デバイスごとの取引回数や金額に上限を設けることで、デバイスが侵害された場合のリスクを低減する。ただし、この解決策は慎重に設計する必要がある。制限値が低すぎると、特にオフライン決済が日常的な幅広い支出をカバーする環境では、実用性が大幅に低下する可能性がある。したがって、セキュリティと実用性の適切なバランスを見極めることが重要である。制限が厳しすぎると採用が阻害され、逆に緩すぎると侵害時の潜在的な損害が増大する。さらに注意すべき点は、これらの制限の施行が侵害された端末自体にのみ依存する場合、攻撃者がそれを回避する可能性があることだ。特に中央機関が即時的な遵守確認を行えないオフライン環境では顕著である。このような技術を導入する際にはこの点を考慮しなければならない。例えば、堅牢なセキュアハードウェアの仮定が必要となる場合があり、端末がセキュアハードウェア要素と通信していることを検証可能なリモート認証インフラとの組み合わせが求められるかもしれない。
- **調整と検出**：一つの解決策は、不整合が発生する可能性を受け入れつつ、再接続時に検出・追跡を可能にすることだ。具体的には、ユーザーの匿名性を保護しつつ、二重支払いのユーザーを信頼性高く、偽装不可能な形で追跡できる暗号技術が考えられる。

CAP 定理の下で現金類似体験を実現するには、一貫性に関する妥協が必要であり、代わりにハードウェアによる強制、事後的な不正検出、取引制約に依存して生じるリスクを管理しなければならない。

5.2.2 CAP 特性の選択的違反

CAP 定理を選択的に破ることは、以下の結果をもたらす：

- **一貫性（C）の違反：**これはハードウェアの仮定が失敗した場合に二重支払いが一時的に発生する可能性を受け入れるケースに相当する。この場合、リスクは送金限度額や監査可能性といった安全策で対処できる。この道は、ある程度のシステムリスクを代償として使いやすさを優先する。
- **可用性（A）の違反：**一貫性と分割耐性を優先すると、オフライン期間中は取引が進行できなくなる。実質的にオンライン専用システムとなり、オフライン決済が不可能となるため、オフライン環境でのデジタルユーロには適さない選択肢だ。また、例えば通信環境が限られる地方や緊急時などにおいて、強いユーザビリティ制限をもたらす。
- **分割耐性(P)の違反：**これもオフラインモードの放棄に等しい。ただし、折衷案として半オフラインモードも検討可能であり、これは第 5.2.3 節で最初のハイブリッドアプローチとして、また第 7 節でより具体的な文脈で説明する。

完全なオフライン環境での現金類似決済を実現しようとする分散システムは、ネットワークプロトコルレベルだけでは一貫性を達成できないことを受け入れなければならない。この不可能性は、オフライン要件やセキュアハードウェアの仮定におけるトレードオフによって回避できる（5.2.3 節および 7 節も参照）。

5.2.3 ハイブリッドソリューション

プライバシー、説明責任、規制順守のバランスを取るために、ハイブリッドな手法も用いられることがある。

1. 二重支払いを防止する一つの手法は、半オフライン環境を考慮することだ。この環境では、取引の送信者はオフラインであるが、支払いの時点で受信者はオンラインである。このモデルでは、送信者がデジタル署名付きトークン（価値を表す）を受取人に転送し、受取人は直ちに「検証サービス」として中央のオンライン機関に照会してトークンの有効性と一意性を確認する。トークンが既に使用済みの場合、取引は拒否される。そうでない場合、中央機関によって承認され償還済みとしてマークされ、再利用と二重支払いを防止する。この場合の通信モデルは、従来のクレジットカードや POS システムのアーキテクチャに似ている。そこでは、取引を承認するためにオンラインアクセスが必要なのは加盟店のみである。重要なのは、発行者が内容を開示せずにトークンに署名できるブラインド署名[Cha82]などの暗号技術を用いることで、送信者の強力なプライバシーを依然として保持できる点だ。この手法については第 7 章で詳細に論じる。結果として発行者と検証者は、トークンの正当性を確認しつつ、その所有者 を特定せずに済む。このアプローチは実用的なトレードオフを提供する：完全なオフライン決済はサポートしないが、受取人がオンライン接続を維持している限り、強力なプライバシー保証を伴う堅牢な二重支払防止を実現する。
2. 別のアプローチとして、二重支払いを事後的に検出する方法がある。これは監査役を指定機関として導入し、二重支払いが発生した場合にのみユーザーの身元を明らかにできるようにするものである。この設定では、暗号技術により、通常の状態では正直なユーザーが（監査役に対しても）完全に匿名性を保つことが可能となる。これにより正直なユーザーの追跡は不可能だ。ただし、ユーザーが同一トークンを複数

回使用した場合、その身元は明らかにされる[Bra94, CHL05, FPV09]。条件付き追跡可能性は、正直なユーザーの匿名性を損なうことなく説明責任を提供しうる。しかしこれはトレードオフであり、新たなリスクも生む。例えば二重支払いの発生から検出までに大幅な遅延が生じた場合、特に攻撃者が既に別の管轄区域に移動している場合、攻撃者の逮捕や処罰が困難になる可能性がある。

5.3 結論

基本的な制約とトレードオフを受け入れることを前提に、「現金類似」オフラインデジタルユーロを実現する技術的解決策のアイデアと基本概念は存在する。あらゆるオフライン方式は本質的に分割耐性と可用性を必要とするため、ハードウェアによる強制やセミオフライン方式の採用といった追加技術・仮定を用いて一貫性を達成するか、あるいは一貫性の欠如を容認し、不正利用監査メカニズムによって緩和する必要がある。

プライバシー保護暗号ツールとセキュアハードウェア、半オフラインシステム設計、条件付き追跡可能性を慎重に組み合わせることで、ユーザーとセキュリティの期待、規制要件に沿ったシステム設計が可能となるかもしれない。半オフライン環境を考慮したハイブリッド設計や、誠実なユーザーの匿名性を保持する検知手法を用いる設計は、セキュリティ・匿名性・ユーザビリティのトレードオフを改善し、より実用的な解決策をもたらす可能性がある。ただし、こうした設計は実践において堅牢な保証を提供することを確実にするため、慎重に研究・評価されねばならない。最終的には、現実的な脅威モデルに基づき、社会的目標に沿って、異なる要件間の慎重に調整されたバランスを反映した設計が求められる。

トレードオフを受け入れるならば、現金類似オフラインのデジタルユーロは実現可能だ。二重支払い攻撃を防ぐためにハードウェア仮定を考慮することもできる。

半オフライン環境を考慮したり、正直なユーザーへの匿名性を保ちつつ悪意あるユーザーの検出を可能にするハイブリッド手法は、CAP 定理が示す不可能性を回避する実用的な方法となり得る。

CAP 定理が示唆する不可能性を回避する実用的な方法となり得る。

6. 移転可能なデジタルトークンにおける二重支払いの防止

検討すべき問題

4. トークンベースのオフライン方式は、複数の取引が連続し、その間にいかなる調整も行われない状況で、どのように二重支払いを防止できるのか？逆に、トークンベースのオフライン方式の現金類似性を維持しながら、調整プロセスをどのように実装できるのか？

トークンベースのオフライン方式は、複数の取引が連続し、その間にいかなる形の調整も行われない状況で、二重支払いをどのように防止できるか？完全オフラインのデジタル通貨における二重支払いの防止は、現時点では、ユーザーのデバイスが二重支払い制約を確実に強制できる安全なハードウェアを備えているという前提、あるいはセミオフライン環境のようなより弱い形の「オフライン」利用可能性を考慮する場合にのみ可能と思われる。これは、単一の取引であれ複数の取引の連続であれ、あらゆる形態のオフライン取引に適用される。

ハードウェア自体が安全であっても、システムはユーザーが真正で侵害されていないデバイスと通信していることを保証しなければならない。これには通常、リモートアテステーションが必要となる。これは暗号プロトコルであり、デバイスが検証者（例えば他のユーザーのデバイス）に対して、信頼できるハードウェア環境で認可されたソフトウェアを実行していることを証明するものである。安全で信頼性の高いリモートアテステーションの実装自体が複雑な課題であり、特に多様で敵対的なデバイス環境では困難を極める。したがって、オフライン二重支払いの防止にはハードウェアベースの強制が不可欠だが、これには慎重に対処すべき重大な技術的・運用上の課題が伴う。

安全なハードウェアがなければ、悪意のあるユーザーがトークンを複製し、デバイスが再接続するまで検出不可能な二重支払いを可能にする。システムがリアルタイムの照合に依存して整合性を強制できない場合、オンラインシステムにおける中央機関の代理として機能するデバイスの内部保護機能を完全に信頼せざるを得ない。

複数の取引が連続し、その間にいかなる調整も行われない状況における二重支払いの防止は、ハードウェアの安全性、および改ざん・複製・侵害に対する耐性に完全に依存する。ただし、ハイブリッドなアプローチも検討の余地がある。

逆に、トークンベースのオフライン方式における現金類似性を維持しつつ、どのように照合プロセスを実装できるだろうか。現金類似性を保つには、システムは偽造不可能性、二重支払い耐性、匿名性、そして（場合によっては）移転可能性という主要な特性を維持しなければならない。

トークンベースのオフライン通貨における偽造不可能性と匿名性は、例えばブラインド署名[Cha82]などの標準的な暗号技術を用いて達成できる（第 7.2 節参照）。したがって、照合プロセスは、譲渡可能通貨と非譲渡可能通貨の両方において、二重支払い耐性に焦点を当てる必要がある。詳細な議論は第 7.3 節を参照のこと。

7. 匿名トークンベースのオフライン方式に対する技術的解決策

検討すべき課題

5. デジタルユーロの設計選択に関する既存の研究を踏まえ、匿名性を維持しつつトークンベースのオフライン方式を実装するために、どのような技術的解決策が有用と考えられるか？

プライバシー保護型のトークンベースデジタル通貨を支えるため、様々な暗号技術が提案されている。特に影響力があり、理解されやすく、容易に入手可能なツールとして、基本的なブラインド署名に焦点を当て、技術的に実現可能なことを説明する。この技術は、匿名デジタル決済に対する最も初期かつ基礎的なアプローチの基盤を形成している。その機能性、利点、限界を検討することで、暗号技術がデジタルユーロの匿名トークンベースオフライン方式の実装をどのように支援できるかについて、具体的な知見を得ることができる。

以下では、ブラインド署名の仕組み、プライバシー保護型トークンベースオフラインデジタル通貨構築への応用方法、二重支払い・移転可能性といった課題解決に必要な追加メカニズムについて説明する。

7.1 ブラインド署名

ブラインド署名は古典的で、非常に研究が進んだ暗号技術である。これは匿名デジタル決済を可能にするデジタル署名の一形態だ。「デジタルコイン」を表すトークンは、ランダム ID のデジタル署名に対応し、署名者（例：銀行）は特定の署名と特定のユーザーを結びつけることができない。

7.1.1 基本機能

ブラインド署名方式には二つの当事者が関わる。メッセージ m に署名を求めたいユーザーと、秘密署名鍵 sk と対応する公開鍵 pk を保持する署名者だ。署名者は sk を使って m に対するデジタル署名 s を作成するが、メッセージ m や署名 s を一切見ることはない。公開鍵 pk を使えば、誰でも s が確かに m に対する有効な署名であり、署名者によって発行されたものであることを検証できる。

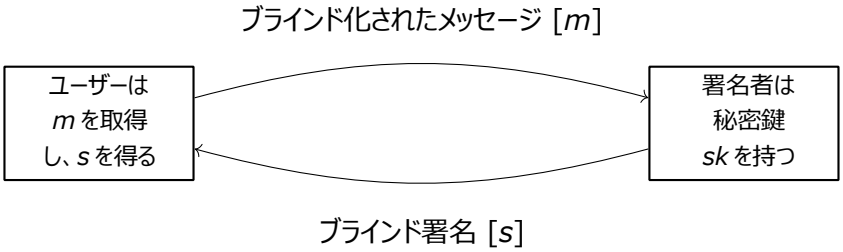

図 2：基本的なブラインド署名機能。s は署名者秘密鍵 sk によるメッセージ m のデジタル署名である。対応する公開鍵 pk はあらゆる当事者が利用可能である。

7.1.2 ブラインド署名プロトコル

ユーザーと署名者は、基本ブラインド署名プロトコル（図 2 参照）において以下のようにやり取りする：[2]

[2]このブラインド署名プロトコルは、特定のブラインド署名構造に対しては正確であるが、他の特定の構造については基本機能の簡略化された説明に過ぎない。一部のブラインド署名方式ではプロトコルがより複雑であり、例えば複数回の相互作用を必要とする場合がある。

1. **ブラインド化：**ユーザーはメッセージ m を用意し、ブラインド変換を適用してメッセージの隠蔽版 $[m]$ を作成する。このブラインド化されたメッセージが署名者に送信される。

   概念的には、メッセージを手紙に書き、その手紙を封筒に入れることに似ている。

2. **署名：**署名者は秘密署名鍵 sk を保持しており、元のメッセージに関する情報を一切知ることなく、ブラインド署名アルゴリズムをブラインド化されたメッセージ $[m]$ に適用する。その結果として生成されるブラインド化された署名は $[s]$ と表記され、ユーザーに返される。

   この比喩を続けると、このステップは署名者が封筒を開けずに手紙に署名する行為に相当する。例えば、ユーザーがメッセージ m とカーボン紙を封筒に入れると想像できる。署名者は封筒の外側に署名し、カーボン紙が封筒を通して内側のメッセージに署名を転写する。デジタル世界では、ブラインド署名方式は既知の実用的な標準暗号技術を用いてこれを実現できる。

3. **開封：**ブラインド署名$[s]$を受け取ったユーザーは、ブラインド処理を解除して元のメッセージ m に対する最終的な署名 s を得る。

   これは封筒を開封し、署名 s とともに元のメッセージ m を得ることに相当する。

署名者は、自身が署名するメッセージ m も署名 s も見えず、ブラインド処理された値 $[m]$ と [s] のみを見ることに注意せよ。

7.1.3 ブラインド署名の安全性

ブラインド署名方式に求められる二つの標準的な特性は次の通りだ：

- **追加の不偽造性**：ユーザーは署名者から任意のメッセージに対する署名を取得できることに注意せよ。ユーザーが署名者と N 回やり取りして N 個（異なる）メッセージの署名を取得した場合、N+1 個目の異なるメッセージに対する署名を取得することは不可能であるべきだ（つまり、追加のメッセージに対する署名を偽造することは不可能であるべきだ）。

  この特性は**署名者に対するセキュリティ**を提供する。つまり、ユーザーは署名者とやり取りせずに署名付きメッセージを作成できない。デジタル通貨で利用すれば、トークンの偽造不可能性が保証される。

- **ブラインド性：**署名者が、ユーザーがブラインド署名プロトコルの過去の実行で取得したメッセージ m と対応する署名 s からなるペア (m,s) を受け取った場合でも、署名者は (m,s) を特定のブラインド署名プロトコル実行、ひいては特定のユーザーに結びつけることができない。

  この特性は、署名者が与えられたペア(m,s)を、m を選択し署名者から s を受け取ったユーザーと結びつけることができないという意味で、**ユーザーにセキュリティ**を提供する。デジタル通貨で使用される場合、この特性はユーザーの匿名性を提供する。

7.1.4 ブラインド署名の実現

ブラインド署名は多様な方法で実現可能であり、様々な暗号技術に基づいている。例えば、RSA 方式に基づく構造[Cha82]、離散対数技術に基づく構造[Sch91, Sch90]、格子技術に基づく構造[BLNS23]など、多くの手法が存在する。

5.1 節で既に述べたように、量子攻撃の脅威を考慮する必要がある。現在、量子コンピュータは現代のブラインド署名スキームの偽造不可能性に対する現実的な脅威とは見なされておらず、多くのスキームは無条件に（つまり将来の量子攻撃に対しても）ブラインド性を達成している。こうした方式については、現時点で量子耐

性は必須ではない。しかし、使用中の方式の安全性を破る量子コンピュータが登場すれば、状況は即座に変わる。したがって、全ての暗号アルゴリズムは、最初から量子耐性を備えるか、少なくとも稼働システム内でアルゴリズムを更新・置換可能な形で実装し、将来的に置換が必要となる状況に備えるべきである（「暗号の俊敏性」）。量子攻撃とは独立して、暗号解析技術の進歩に備えて方式を置換できるようにするため、暗号の俊敏性は強く推奨される。

7.2 プライバシー保護型デジタルキャッシュにおけるブラインド署名の利用

ブラインド署名技術は、プライバシー保護型トークンベースのオフラインデジタルキャッシュシステム設計における基盤的構成要素として活用できる。このシステムでは、（中央）銀行がトークンを発行し、ユーザーは匿名で支出が可能となる。この概念は、匿名電子決済スキームの基礎的成果である David Chaum [Cha82]の画期的研究で初めて提唱された。以下では、Chaum のプロトコルの中核となる考え方を概説する。これは、デジタルユーロのトークンベースのオフライン方式を実装する上で有用な技術的解決策としてのブラインド署名の適用可能性を示すとともに、追加のツールを必要とする制限事項に関する議論の基礎となるものである。

7.2.1 基本的なトークンベースのデジタル通貨

基本的なトークンベースのオフラインデジタル通貨については、以下のシステム構成を想定する：

- （中央）銀行は、ブラインド署名方式用の秘密署名鍵 *sk* を保有する。この秘密鍵 *sk* は、物理的な硬貨のデジタル相当物として、暗号的に認証されたトークンを生成するために使用される。対応する公開鍵 *pk* は公に知られている。
- 各トークンには固有のトークン *ID* が付与され、トークンを「ラベル付け」するとともに一意の識別子として機能する。新規トークンは銀行からの引き出し時に生成され、預け入れ時に破棄される。中央銀行は「破棄済み」トークン ID、すなわち流通後に銀行へ預け入れられた全トークンのリストを管理する。
- 簡略化のため、トークンは固定価値を持つと仮定する。例えば、各トークンは 1 ユーロといった固定価値に対応する。この一般化については後述する。

この仕組みに基づき、トークンの発行・移転・預け入れは以下の通り行われる。

- **ブラインド引き出しによるトークンの生成。**引き出しプロセスは新しいトークンを生成する。ユーザー（より正確には図 3 の「最初の支払者」）は支払者の銀行とやり取りし、その銀行は中央銀行と以下のようにやり取りする。

  1. 支払者はトークン ID *m* を選択する。これはトークンを一意に識別する乱数である。

     十分に広い範囲から乱数を選択することで、トークン *ID* の一意性を保証できる。つまり、ごくわずかな誤差確率を除き、異なるトークンが同一のトークン ID を共有することはない。この誤差確率は、実際には発生しないと合理的に期待できるほど十分に小さく設定可能だ。例えば、*m* を 32 バイトの乱数として選択すれば、実用上は十分である。

     トークン ID のリストは無限に増え続けるため、非常に大きくなる可能性があることに注意せよ。ただし、リストのサイズを縮小するためのトレードオフが存在する。例えば、トークン ID に引き出し月などのタイムスタンプを埋め込み、デジタルトークンに有効期限を設ける方法がある。そうすれば、現在の有効期間に属するトークン ID のリストのみを保存すればよい。ただし、これは利便性（有効期間のサイズによってパラメータ化されるデジタルトークンの有効期限が限定されるため）と匿名性の両面でトレードオフとなる。トークン ID にタイムスタンプを埋め込むことで、匿名性集合が「システムの利用者全員」から「トークン ID のタイムスタンプと一致する時期にトークンを引き出したシステムの利用者全

員」へと縮小されるのだ。より細かいタイムスタンプはリストサイズと匿名性集合を縮小し、より粗いタイムスタンプは匿名性とリストサイズの両方を増加させる。

2. 最初の支払者は、支払者の銀行で引き出しプロセスを開始する。この過程で、支払者銀行は中央銀行とブラインド署名プロトコル（例えば第 7.1 節で説明したようなもの）を実行する。この際、支払者と中央銀行間のメッセージは支払者銀行によって中継される（図 3 参照）。これにより、ユーザーはランダムなトークン ID m と、中央銀行によるトークン認証署名 s から成るトークン (m,*s*) を入手する。

3. 支払者の銀行は、ユーザーの口座から対応する金額を請求する。

重要なのは、この引き出しが「ブラインド」である点だ。つまり、支払者の銀行も中央銀行も、トークン ID m や対応する署名 *s* を見ることはない。彼らが目にするのは、対応するブラインド化された値 [*m*] と [s] だけである。

支払者と受取人の間のリンクはブラインド署名によって隠蔽される。ただし、引き出し（「ブラインド」であるにもかかわらず）もコインの預け入れも匿名である必要はない。むしろ、資金が正しい銀行口座から引き出されることを保証するためには、引き出しはユーザーの身元に紐付けられる必要があるように思われる。したがって、引き出しプロセスにおけるトークン ID と署名のブラインド化は、支払者と受取人の関連付けを不可能にするためのものであり、匿名での引き出しを実現するためのものではない。直感的に言えば、トークン ID は紙幣のシリアル番号に似ており、引き出し時のブラインド化は技術的に、銀行が顧客に渡した紙幣のシリアル番号を記録できないことを保証する。

- **トークン移転による支払い。**あるユーザーから別のユーザーへ、つまり図 3 の「支払者」から「受取人」へトークン(m,s)を移転するには、支払者は単に(m,s)を受取人に送信する。受取人は(m,s)を受信後、中央銀行の公開鍵 pk に対して s が m の有効な署名であることを確認して初めてトークンを受け入れる。これにより(m,s)が中央銀行によって認証された有効なトークンであることが保証される。この場合、受取人はトークンを受け入れ、取引は完了する。

  二重支払い攻撃。ここで考慮すべき重要かつ根本的な技術的課題は、二重支払い攻撃である。これは、ユーザーが同一のトークンを二つの異なる主体（他のユーザーや銀行）に送金しようとする攻撃を指す。この攻撃に対処する方法は、完全な防止か事後検知の二通りである。この課題には様々なアプローチが可能だが、各手法の機能性、利点、限界について詳細な議論が必要となる。これについては第 7.3 節で説明する。ここでは、トークンが二重に支出されないことを保証する何らかの方法が存在すると仮定する。

- **トークンの預け入れと破棄。**最終的な受取人は、トークンを自身の銀行口座に預け入れるため、(m,s)を銀行に送信する。銀行は、s が中央銀行の公開鍵 pk に対して m に対する有効な署名であることを確認した後で初めてトークンを受け入れる。この確認が通れば、受取人の銀行はトークンを受け入れ、対応する金額を受取人の銀行口座に入金する。さらに、受取人の銀行は中央銀行に対し、トークン ID m を持つトークンを「破棄済み」として記録するよう通知する。

  ここでも二重支払い攻撃を考慮することが重要だ。ただし、銀行が「オンライン」状態にあると仮定すれば、トークン預入時の二重支払いの検出は格段に容易になる。例えば、偽名 m を持つトークン (m,s) が以前に銀行に預けられていないか確認するため、受取人の銀行は中央銀行と通信し、ID m のトークンが「破棄済み」かどうかを照合できる。もし破壊済みであれば、二重支払い攻撃が検出され、トークンの受け入れ拒否によって防止される。

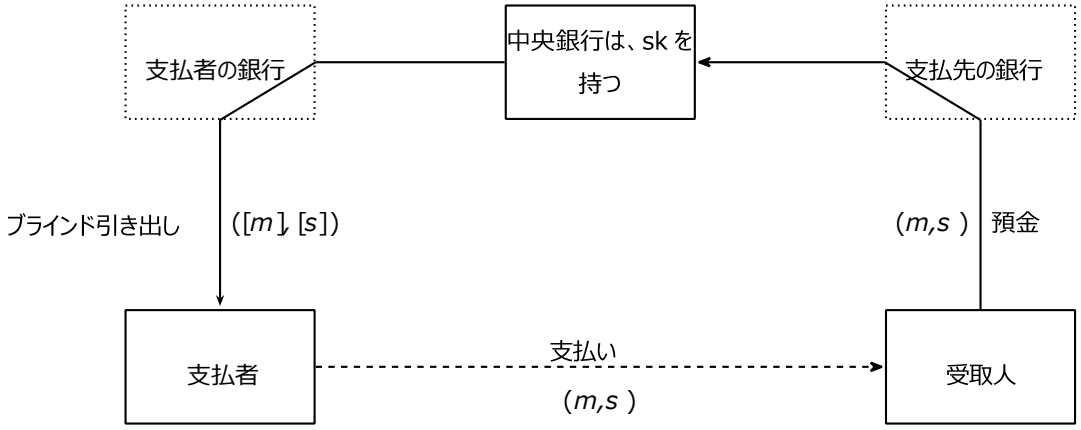

図 3：ブラインド署名を用いたデジタルキャッシュの図解。実線は「オンライン」とみなされる取引、すなわち中央銀行とのアクティブな通信チャネルを介した取引を表す。ユーザーが取引銀行と通信している間、取引銀行は特定の操作において中央銀行を関与させる場合がある。これは中央銀行と直接通信するか、ユーザーと中央銀行間のメッセージを中継するかのいずれかである。破線は「オフライン」取引を表し、これは中央機関との通信なしに、2 人のユーザー間で直接実行される可能性がある。

本節で説明するデジタル通貨は、完全な設計ではない。匿名性を維持しつつトークンベースのオフライン方式を実装する技術的解決策の有用性を示す簡略例として意図されている。また機能性、利点、限界に関する議論の基盤を提供する。

7.3 機能性、利点、限界の分析

上記で説明した基本的なブラインド署名ベースのデジタル通貨が、セクション 2.4 で定義された意味においてどの程度「現金的」であるかを検証する。偽造不可能性、二重支払い耐性、匿名性、移転可能性という 4 つの特性を考慮する必要がある。まず偽造不可能性と匿名性について考察する：

1. **偽造不可能性**：偽造不可能性とは新たなトークンを生成する能力を指す。ブラインド署名方式の「追加生成不能性」特性により、正当に認証されたトークンは中央銀行との相互作用、すなわち中央銀行の承認を得てのみ生成される。いかなるユーザーも、中央銀行が署名したトークン数、すなわち銀行から引き出した額を超えるトークンを生成することはできない。

   ブラインド署名方式が偽造不可能なものであれば、基本的なデジタル通貨は偽造不可能である。

2. **匿名性**：セクション 2.4 で説明したように、匿名性にはトークンが偽名性であり、関連付け不能であることが求められる。なお、上記の基本 デジタル通貨は両特性を達成している。個々のトークンを識別するトークン ID m は、ユーザーやシステム内の他のエンティティを参照しない乱数である。引き出しプロセスでトークンを作成する際、銀行が把握するのはユーザーがトークンを引き出した事実のみであり、これをユーザーの銀行口座に反映できる。しかし、ブラインド署名の盲目性特性により、銀行は引き出しプロセスをトークンのトークン ID m に結びつけることができない。さらに、署名方式の盲目性特性により、ユーザーに転送された、あるいは銀行に預けられたトークン (m,s) を、がトークンを引き出したユーザーに結びつけることも不可能となる。

   基本的なデジタル通貨は匿名性を持つ。ただし、ブラインド署名方式がブラインド性というセキュリティ特性を備えている場合に限る。

二重支払いの防止と移転可能性については、まだ議論が残っている。

7.3.1 二重支払いの防止

二重支払いを防止する仕組みを理解するため、以下の 3 つの異なる設定を考察する：

1. 完全オフライン、ハードウェア前提なし：この設定では、ユーザーはインターネット接続なし、かつセキュアハードウェアに依存せずに操作する。ユーザビリティを確保するため、システムは可用性を保証しなければならず、オフライン動作のためネットワーク分割に耐えなければならない。CAP 定理（第 3 節参照）によれば、これら二つの特性は必然的に一貫性を犠牲にする。

   この一貫性の欠如は単なる理論上の懸念ではなく、一貫性を破る具体的な二重支払い攻撃が存在する。この攻撃は次のように機能する：ユーザーがトークン(m,s)を引き出し、それを二つの異なる受取人に転送する。両受取人がオフラインであるため、トークンが既に使用されたかどうかを確認できない。結果として、両者が同じトークンを受け入れる。後で受取人が銀行にトークンを預け入れようとした時、最初の受取人だけが成功する。2 人目はトークンが既に「破壊」されているため拒否される。

   > セキュアハードウェアのない完全オフライン環境では、二重支払いを防ぐことはできない。これは CAP 定理の直接的な帰結である。

2. 完全にオフラインで、セキュアハードウェアを前提とする場合：上記の制限を克服するには、セキュアハードウェアに依存できる。このセキュアハードウェアは、スマートカードのような専用デバイスか、スマートフォン内のセキュア環境のいずれかである（2.5 節参照）。

   この環境では、トークンは完全にセキュアハードウェア内で保管・管理される。ハードウェアは以下のことを保証する：

   - トークンが信頼できない環境にエクスポートされることは決してない。
   - すべての操作（引き出し、送金、預け入れ）はセキュアハードウェアを介して行われる。
   - トークンが使用されると、支払者のハードウェアはそれを永久に削除する。
   - 受取人のハードウェアも、別のユーザーへの転送や銀行への預け入れ時に削除を強制する。

   これにより、たとえ全ての関係者がオフライン状態であっても、トークンの複製や二重使用が不可能となる。さらに、銀行を介さずにユーザー間でオフラインでの移転が可能となる。

   この手法の安全性は、トークンが信頼できない環境に決して晒されないことを保証することに大きく依存している点を強調しておく必要がある。さらに、トークンが引き出され、送金され、または預け入れられる際には、常に安全なハードウェア内に留まっていることが保証されなければならない。これは、これらの操作に参加できるのは安全なハードウェア要素のみであることを意味する。したがって、各セキュアデバイスと銀行は、通信相手が同様に信頼できるセキュアハードウェアモジュールであり、通信経路が暗号的に安全であることを検証できなければならない。これを実現するには通常、システムの完全性と安全性を維持するために不可欠な、リモート認証プロトコルなどの追加インフラが必要となる。

   これはセキュアハードウェアに対する非常に厳しいが不可欠な要件である：システムは、デバイスを所有し任意の改ざんを試み得る悪意のある（かつ潜在的にリソース豊富な）ユーザーに対しても安全性を維持しなければならない（第 4 節参照）。この要件は、あらゆる時点において、全てのデバイスが、非常にリソースを投入した攻撃に対しても満たさなければならない。既知のハードウェア攻撃が多岐にわたるため、こ

のアプローチは追加のシステムレベルのセキュリティ対策と組み合わせて実装する必要があると思われる（セクション 4 参照）。

> 二重支払いを確実に防止する安全なハードウェアを前提とすれば、「現金類似」特性、すなわち偽造不可能、二重支払い耐性、匿名性、譲渡性を備えたオフラインデジタル通貨の実装が可能である。ただしこの手法は、悪意がありリソース豊富なユーザーの手中にあってもハードウェアが安全性を維持するという非常に強い仮定に依存している。

3. セミオフライン、ハードウェア前提なし：この設定では、支払者はオフラインだが、受取人は取引時にオンラインである。この構成は、クレジットカードや POS 端末のような従来システムに似ている。そこでは販売者（受取人）はオンラインだが、顧客（支払者）はオフラインである（セクション 5.2 参照）。

   支払者からトークンを受け取ると、受取人は直ちに銀行に預け入れるか、中央システムに照会してトークンが既に使用・破棄されていないか確認できる。未使用であればシステムはトークンを受け入れ破棄処理を行うため、二重支払いを防止できる。

   この設定では、トークンがユーザー間で直接渡せる真の移転性はないが、この機能は効果的にエミュレートできる。受取人はオンライン状態のため、受け取ったトークンを預け入れた直後に新しいトークン を引き出せる。これにより、二重支払いの防止というセキュリティを維持しつつ、移転可能な デジタル通貨の挙動を模倣する。

   > この半オフライン設定により、非常に強力なハードウェアを前提とせずに、「現金類似」、すなわち偽造不可能、二重支払いの防止、匿名性、譲渡性を備えたデジタル通貨を実現できる。これはオンライン要件と安全なハードウェアへの信頼とのトレードオフである。重要な点として、トークンの有効性にはある程度のオンライン検証があるにもかかわらず、半オフライン設定は匿名性を提供することを留意すべきだ。

7.3.2 二重支払いの検出

二重支払いを完全に防止するのではなく、その検出と説明責任（二重支払いを行ったユーザーを確実に特定する能力）に焦点を当てる代替アプローチがある。検出された不正使用に対する罰則の脅威は抑止力として機能しうる。このアプローチの基本的な考え方は、二重支払いの場合にのみユーザーの身元を明らかにできる監査役を導入することである。一方、通常の使用時には誠実なユーザーは（監査役に対しても）完全に匿名性を保つ。

第 7.2 節で概説した基本プロトコルに基づくデジタル通貨は、基盤となるブラインド署名方式をより高度な構造に置き換えることで、こうした検出メカニズムをサポートできる。一例として、ブランズによる電子現金方式[Bra94]がある。これは匿名デジタル決済のための暗号プロトコルであり、強力なプライバシー、偽造防止性、二重支払い検出と説明責任を提供する。また、[CHL05]や[FPV09]など、いくつかの後続研究も存在する。これらのスキームでは、同一トークンが複数回使用されない限り、トークンはユーザーの身元と結びつかない。二重支払いが発生した場合、その行為は検知され、不正ユーザーの身元は冤罪を被らせない形で明らかにされる。オリジナルの Brands スキームはユーザー間でのトークン移転をサポートしないが、後続の研究では移転可能な変種が提案されている[BCFK15, BFQ21]。

しかしこの手法には、追加のセキュリティ特性である非フレーム可能性[Bra94]が必要となる。これは、いかなる主体（中央銀行でさえも）が、誠実なユーザーを不当に二重支払いの証拠に巻き込むことができないことを保証するものである。

二重支払い検出に基づくアプローチの主な欠点は、悪意あるユーザーの身元を明らかにすることだ。ここでは、強力なハードウェア仮定に依存せず（表 2 参照）、誠実なユーザーに匿名性を提供する完全オフライン環境を実現する別の選択肢として提示する。これにより、CAP 定理が暗示する制限を回避する別の道筋が得られる。

たとえ誠実なユーザーが無条件に保護されたとしても、グローバルレベル（すなわちユーロシステム）での不正ユーザーの匿名性解除が許容できないと考える場合、より分散化されたアプローチ、例えば小売銀行や決済サービスプロバイダーを通じた方法が検討される可能性がある。

さらに、秘密分散やしきい値暗号といった暗号技術を用いることで、不正利用者の匿名化解除には複数の独立した当事者の協力が必要となるように設計することも可能だ（ ）。このような解決策の設計は、既知の暗号技術を用いて原理的には可能だが、具体的な設計を進めるにはまず要件を明確に定義する必要がある。

不正ユーザーの匿名化解除が一般的に許容されない場合、セキュリティ、プライバシー、システム設計要件のバランスを取る代替アプローチを検討できる。

7.4.3 固定価値トークンを超えて

我々は基本のブラインド署名で実現される固定価値トークンに焦点を当ててきた。その概念的単純さにより、偽造不可能性と強固な匿名性の達成可能性、二重支払い耐性の実現における課題と選択肢を容易に説明・具体化できるためである。しかし、この基本アプローチの機能を拡張できる暗号技術は多岐にわたる。

例えば、7.2 節で説明した Chaum の基本プロトコルはブラインド署名に基づき、固定額面のトークンを発行する。任意の支払い（例：5 ユーロトークンで 2.75 ユーロを支払う）をサポートするには、トークンの分割、あるいは釣り銭用の新規トークン生成が必要となる。同時に、余分な価値が生成・悪用されないこと、そして匿名性が保持されることを保証しなければならない。トークンの価値未満の支払いを可能にし、残額を新たなトークン（複数可）として受け取ることを許可しつつ、プライバシー・偽造防止・二重支払い検知を損なわない課題に対処する暗号技術は複数存在する。例えば［Oka95, CHL05, CG07, CPST15b, CPST15a, BPS19］などが挙げられる。

別の実用的なアプローチとして、異なる額面のトークン（例：1 セント、5 セント、1 ユーロ、2 ユーロ、10 ユーロ、50 ユーロなど）を導入し、ユーザーがそれらのトークンを組み合わせて引き出せるようにする方法がある。ユーザーの端末上のセキュアハードウェアが、使用されるトークンの総額が引き出し総額を超えないことを保証すれば、引き出されるトークンの総額が希望の引き出し額を超えることさえ可能だ。支払い時には、端末が支払い額に合うトークンの組み合わせを選択・転送し、残ったトークンが未使用のまま残ることを強制する。この手法はリアルタイムのトークン分割を回避しつつ、偽造不可能性と匿名性を維持するが、ハードウェアの安全性を前提としている。

7.3.4 利点と制限に関する考察

ブラインド署名に基づくアプローチにはいくつかの利点があるが、制限も伴う。最も重要な利点は以下の通りだ：

1. **偽造不可能性：**ブラインド署名ベースのトークンの偽造不可能性は、確立された標準的な暗号技術に基づいて非常に強固に実現できる。
2. **匿名性**：ブラインド特性により、銀行はトークンの識別子を知らずに署名する。これにより特に、預け入れられたトークンが引き出しプロセスに遡及的に関連付けられないことが保証され、非関連性と強力なユーザープライバシーを提供する。

3. **簡潔性**：基本設計は概念的に単純で、標準技術で実現可能だ。この簡素な基盤は高度な技術で拡張できる。例えば、システム設計全体で必要とされれば、二重支払い検出、特定の説明責任形態、柔軟な額面設定などをサポートすることが可能だ。
4. **現金類似支払いフロー**：ユーザーは銀行からトークンを引き出し、後で直接加盟店で使用できる。これは物理的な現金の仕組みに非常に近い。

以下の制限事項を考慮する必要がある：

1. **二重支払い耐性**：CAP 定理はブラインド署名ベースのプロトコルにも適用される。したがって、他のオフライン対応デジタル通貨と同様に、ブラインド署名ベースのアプローチも安全なハードウェア、半オフライン検証、あるいはその両方の組み合わせを必要とする。
2. **移転可能性**：基本スキームでは、銀行を介さずに同一トークンをユーザー間で自由に移転することはできない。移転可能性が要求される場合、追加のメカニズムまたはセキュアハードウェアの仮定が必要となる。
3. **説明責任**：説明責任は本質的にユーザーの匿名性解除を必要とするため、匿名性と根本的に矛盾する。これは物理的な現金と同様にデジタル現金にも当てはまる。ただしデジタル環境では、ユーザーのプライバシーと当局による追跡可能性のバランスを取るための異なるトレードオフが可能だ。必要であれば、組織的・技術的措置の両方が検討できる。

ブラインド署名を用いてトークンを実現するデジタル通貨は、これらの特性を達成するためにセキュアハードウェアを必要とせず、強力な匿名性と偽造防止性を保証できる。基本プロトコルは概念的に単純で、現金類似支払いフローを実現する。二重支払い耐性、移転可能性、説明責任はシステム設計の選択に大きく依存する。完全オフライン環境では基本的にセキュアハードウェアが必要となる。半オフラインアーキテクチャは信頼性と利便性の面で異なるトレードオフを提供し得る。より高度なスキームは説明責任や柔軟な額面設定を可能にすることで機能を拡張でき、真に「現金類似」デジタル通貨を構築するための豊かな設計空間を示している。

7.4 プライバシー保護型デジタルトークン向けその他の暗号ツール

本節で検討するブラインド署名方式の種類は、Chaum が[Cha82]で導入したブラインド署名の本来の概念に対応する。この概念には数多くの拡張が開発されており、その中には非対話型ブラインド署名[Han23, BCGY24, HPZ25]や部分的ブラインド署名[MS98, AO00, Oka06, BPV12, dPK22, KLLQ23]など、ごく最近のものも含まれる。さらに、プライバシー保護型デジタル通貨の設計に有用な「プライバシー保護型で偽造不可能なデジタルトークン」を実現する、その他の暗号技術も非常に多く存在する。例えば、匿名認証情報[CL01, CV02, CL04, BCGS09, CKLM14]、ゼロ知識証明[GMR89, BFM88, Gol01, GOS06, GS08, Gro16, BBB$^+$ 18]、いわゆる OPRF [CHL22]、一般的なセキュア計算プロトコル [EKR18] などである。

適切な暗号ツールの選択は、検討中のデジタル通貨システムの具体的な要件と制約に大きく依存する。特定のシステム設計に固執することなく、これらの異なる概念の微妙な違いを掘り下げることは、おそらく非生産的である。このため、ここではデジタルユーロのオフラインモードで使用可能な暗号ツールの具体例として、基本的なブラインド署名に焦点を当てる。ここでは主に、その本質的な仕組みを伝え、プライバシー保護暗号が提供し得る保証と限界を明らかにすることを目的とする。

システムアーキテクチャに適切に統合されれば、現代の暗号技術はデジタルキャッシュに、偽造不可能性や匿名性といった物理的現金の主要な特性を実現させることができる。

7.5 結論

安全なプライバシー保護型デジタル通貨の設計には、様々なツールや技術を慎重かつ包括的に統合する必要がある。例えば、ブラインド署名を用いれば、偽造不可能かつ匿名のデジタル通貨を容易に構築できる。あらゆるオフライン型デジタル通貨が直面する根本的な課題は二重支払いの防止であり、これは本質的にトレードオフを伴う。完全なオフライン環境では、二重支払いを防止する安全なハードウェアが必要となる（7.3.1 節で検討した第二の設定を参照）。あるいは、匿名性を犠牲にすることなく取引の受取人によるオンライン検証を利用する半オフライン環境（7.3.1 節の第三の設定）を検討することもできる。両アプローチの組み合わせも考えられる。例えばデフォルトで半オフライン方式を採用し、ハードウェア仮定をフォールバックとして用いる方法などだ。

これらのツールの適切な選択と統合は、システム全体の設計と、システムが要求する特定のセキュリティおよび機能特性に依存する。したがって、堅牢な設計では、適切な暗号ツールを選択し、使いやすさ、効率性、脅威への耐性のバランスを取りながら、システムアーキテクチャ内で正しく構成されていることを保証しなければならない。

> デジタルユーロの匿名オフライン方式は、適切な暗号ツールの組み合わせに基づくシステム設計により実現可能である。完全なオフライン方式では、二重支払いを防止し移転性を確保するため、安全なハードウェア（4.3 節参照）が必要となる。一方、半オフライン方式は、安全なハードウェアを前提としない、あるいはより弱い前提に基づく場合でも実現可能かもしれない。重要な点として、デジタルユーロの安全かつ匿名のオフライン方式を実装することは技術的に可能に見えるが、その実現には多大な研究開発努力が必要となる。

デジタルユーロのオフライン方式を開発するには、システム設計の基礎となる、全ての機能要件とセキュリティ要件を正確かつ包括的に規定する必要がある。このシステム設計では、基盤となる暗号プリミティブと関与するセキュアハードウェアコンポーネントについて、 な仮定を明確に述べなければならない。

要件仕様とシステム設計の両方は、外部からの精査と独立したレビューを支援し積極的に促すため、透明性のある方法で開発されるべきだ。

表 2 には、さまざまなアプローチの概要と、それらが偽造防止性、匿名性、二重支払い防止性、および移転可能性をどのように達成できるかが示されている。

スキーム	支払者オフライン	受取者オフライン	偽造不可能	匿名性	二重支払い防止譲渡可能	
セキュアハードウェアのみ	✓	✓	HWA	HWA	防止、HWA	HWA
ブラインド署名＋セキュアハードウェア	✓	✓	暗号化	暗号化	防止、HWA	HWA
ブラインド署名（半オフライン）	✓	✗	暗号化	暗号化	防止	✓(*a*)
オンラインでのブラインド署名	✗	✗	暗号化	暗号化	防止	✓(*a*)
譲渡可能な電子現金	✓	✓	暗号化	暗号化[(*b*)]	検出のみ	✓

表 2：異なる基本アプローチの特性と必要な前提条件の比較。重要な点として、この表はいくつかの可能なトレードオフを示すことを目的としており、異なるトレードオフや追加の特性を持つ多くのバリエーションが考えられる。特

定のバリエーションに関する具体的な推奨は、全ての機能要件、セキュリティ要件、許容可能なリスクと前提条件を正確に定義した上でしか行えない。

「支払者オフライン」および「受取人オフライン」の列は、取引時にそれぞれのユーザーがオフライン状態にある可能性を指す。「HWA」は、考慮される特性が安全なハードウェアの仮定によって強制されなければならないことを意味する。ハードウェアが提供しなければならない異なる特性が増えるほど、期待されるセキュリティ特性は強化される（すなわち、現実的ではなくなり、達成が困難になる）ことに注意せよ。既存のハードウェアにデジタル通貨が要求する追加機能を拡張することは、特に下位互換性を保つ方法では困難あるいは不可能である。新規ハードウェアの開発は高コストかつ時間を要する。[(a)] ユーザーに対してエミュレート可能。[(b)]誠実なユーザーのみ対象。

8. 結論

本報告書は、デジタルユーロの匿名性を持つ現金類似のオフライン形態は技術的に実現可能であると結論づける。ただし、暗号技術、ハードウェアの仮定、システム的な安全策を慎重に組み合わせる必要がある（第 5.1 節）。

特定の特性（特に偽造不可能性と匿名性）は、確立された暗号手法を用いて非常に強固に保証できる。適切な暗号ツールを用いれば、一見匿名性と矛盾する特定の説明責任形態さえも、誠実なユーザーを保護し、悪意あるユーザーのみが匿名解除を可能とする形で実現できる（第 7.3.2 節）。一方、二重支払い耐性や移転可能性といった他の主要要件は、CAP 定理に根ざした本質的な制約に直面する（第 5.1 節、第 6 節）。これらの制約は解決を不可能にするものではないが、安全なハードウェア仮定の使用や、半オフライン環境を考慮したオフライン要件の緩和といった、慎重かつ現実的な選択を必要とする（第 5.2.3 節）。重要なのは、必要なセキュリティ仮定は可能な限り弱く（つまり現実的に）、本質的に必要な場合にのみ使用すべきだということだ（セクション 2.5、セクション 4.3）。例えば、匿名性を達成するためにセキュアハードウェア仮定を用いるべきではない。この特性は、十分に理解された暗号技術を用いることでより確実に達成できるからである（セクション 7.5）。また、特定のハードウェアデバイスが、セキュアな鍵保管といった従来の暗号利用ケースでは安全と見なされていても、二重支払い攻撃のようなオフラインデジタル通貨におけるより複雑な不正シナリオに対して十分な保護を提供しない可能性があることも考慮しなければならない。物理的近接性は、デジタル環境において確実に実施することが困難な特性として浮上しており、したがって、堅牢な距離制限に依存しない設計を追求する方が有望である（セクション 2.4.2）。

デジタルユーロの設計は、明確な要件と堅牢な脅威モデルをもって、これらのトレードオフを透明性をもってバランスさせる必要がある。

匿名性・オフライン・現金類似性を備えたデジタルユーロは実現可能な構想だが、同時に困難な設計課題でもある。これを達成するには、強固な暗号保証と現実的で理解されたハードウェア前提、トレードオフ、透明かつオープンな設計を組み合わせた多面的なアプローチが必要だ。これらの要素が整合すれば、期待されるセキュリティ・プライバシー・ユーザビリティ特性を備えたオフラインモードの構築は可能と思われる。

オープンで透明なシステム設計の必要性について。現金類似匿名性の欠如と攻撃リスクは、デジタル通貨システムにおける現実的で信憑性のある脅威であり、その普及を著しく阻害する可能性がある。これらのリスクを民主的で信頼できる方法で軽減し対応する最善の方法は、システム全体を公の監視に開放することである。デジタル通貨システムは以下を必須とする：

1. 各コンポーネントの要件、セキュリティ目標、攻撃者モデルを明確に文書化すること。
2. プロトコルと基礎となるセキュリティ前提を公開すること。
3. ソフトウェアとハードウェアの両方のオープンソース実装を提供すること。
4. 独立した専門家や倫理的ハッカーがシステムをテスト、分析し、改善を支援するよう積極的に促すこと。

オープンで透明性のある設計は、より強固で将来性のあるセキュリティを実現するだけでなく、市民の目に正当性を保証する。デジタルユーロが欧州の伝統である開放性と基本的人権の保護に沿って構築されていることを示すことで、その成功に必要な信頼と受容を育むことができる。

透明性のある設計アプローチの成功例として、COVID-19 パンデミック時に開発された DP-3T（「分散型プライバシー保護近接追跡」）プロジェクト[TBB^{+} 22]が挙げられる。これはユーザーのプライバシーを保護しつつ

接触追跡を可能にするためのもので、中核プロトコル、暗号学的仮定、脅威モデルは当初から完全に公開され、実装はオープンソースとしてリリースされた。この透明性により広範な独立した分析と批判が可能となり、高い社会的信頼を獲得した。欧州の数政府が最終的に DP-3T ベースのシステムを採用したのは、まさにその公開性によって技術的堅牢性と社会的受容性の両方が促進されたためである。これは、透明性とコミュニティの関与が、安全で広く受け入れられるデジタルシステムのための実践的な前提条件であることを示している。

参考文献

[ABB+ 18] Gildas Avoine、Muhammed Ali Bingol、Ioana Boureanu、Srdjan¨ capkun、Gerhard Hancke、ˇ Suleyman Kardas¸、Chong Hee Kim、C¨ edric Lauradoux、Benjamin Martin、Jorge Munilla、´ Alberto Peinado、Kasper Bonne Rasmussen、Dave Singelee、Aslan Tchamkerten、Rolando´ Trujillo-Rasua、Serge Vaudenay。距離制限のセキュリティ：調査。*ACM Comput. Surv.*、51(5)、2018 年 9 月。

[ACK+ 24] Elli Androulaki、Angelo De Caro、Kaoutar El Khiyaoui、Romain Gay、Rebekah Mercer、Alessandro Sorniotti。セキュアエレメントを使用した、安全でプライバシーを保護する CBDC オフライン決済。Cryptology ePrint Archive、論文 2024/1746、2024 年。

[AO00] Masayuki Abe and Tatsuaki Okamoto。証明可能な安全性を備えた部分的にブラインドな署名。Mihir Bellare 編、*CRYPTO 2000*、*LNCS* 第 *1880* 巻、271–286 頁。Springer、ベルリン、ハイデルベルク、2000 年 8 月。

[BBB+ 18] ベネディクト・ブンツ、ジョナサン・ブートル、ダン・ボネ、アンドルー・ポールストラ、ピーター・ウィール、グレッグ・マクスウェル。Bulletproofs: 機密取引などのための短い証明。*2018 IEEE* セキュリティ・プライバシーシンポジウム、315-334 ページ。IEEE コンピュータ協会出版、2018 年 5 月。

[BC94] Stefan Brands と David Chaum。距離制限プロトコル（拡張要約）。Tor Helleseth 編集、*EUROCRYPT'93*、*LNCS* 第 765 巻、344–359 ページ。Springer、ベルリン、ハイデルベルク、1994 年 5 月。

[BCFK15] フォテイニ・バルディムツィ、メリッサ・チェイス、ゲオルグ・フックスバウアー、マルクルフ・コールヴァイス。匿名譲渡可能電子現金。ジョナサン・カッツ編、*PKC 2015*、*LNCS* 9020 巻、101–124 頁。シュプリンガー、ベルリン、ハイデルベルク、2015 年 3 月/4 月。

[BCGS09] パトリック・ビヒセル、ヤン・カメニッシュ、トーマス・グロス、ヴィクター・ショウプ。標準 Java カード上の匿名認証情報。エハブ・アルシャエル、ソメシュ・ジャ、アンジェロス・D・ケロミティス編『*ACM CCS 2009*』600–610 頁。ACM プレス、2009 年 11 月。

[BCGY24] フォテイニ・バルディムツィ、ジャイキ・チェン、リシャブ・ゴヤル、アユシュ・ヤダヴ。非対話型ブラインド署名：ポスト量子およびより強固なセキュリティ。カイミン・チョン、ユウ・ササキ編、*ASIACRYPT 2024*、*Part II*、*LNCS* 15485 巻、70–104 頁。Springer, Singapore, 2024 年 12 月。

[BFM88] Manuel Blum, Paul Feldman, Silvio Micali. 非対話型ゼロ知識証明とその応用（拡張要旨）. *20th ACM STOC*, 103–112 頁. ACM Press, 1988 年 5 月.

[BFQ21] バルタザール・バウアー、ゲオルグ・フックスバウアー、チェン・チェン。移転可能な電子現金：より明確なモデルと最初の実用的な具体化。フアン・ガライ編、*PKC 2021*、*Part II*、*LNCS* 第 *12711* 巻、559–590 頁。シュプリンガー、チャム、2021 年 5 月。

[BLNS23] Ward Beullens, Vadim Lyubashevsky, Ngoc Khanh Nguyen, Gregor Seiler. 格子ベースのブラインド署名：短く、効率的で、ラウンド最適である。Weizhi Meng, Christian Damsgaard Jensen, Cas Cremers, Engin Kirda 編, *ACM CCS 2023*, 16–29 頁. ACM Press, 2023 年 11 月.

[BPS19] Florian Bourse, David Pointcheval, Olivier Sanders. 制約付き擬似乱数関数からの分割可能電子現金. Steven D. Galbraith, Shiho Moriai 編, *ASIACRYPT 2019, Part I*, *LNCS* 11921, 679–708 頁. Springer, Cham, 2019 年 12 月.

[BPV12] オリヴィエ・ブラジー、デヴィッド・ポワントシュヴァル、ダミアン・ヴェルノー。コンパクトでラウンド最適の部分盲署名。イヴァン・ヴィスコンティとロベルト・デ・プリスコ編、*SCN 12*、*LNCS* 7485 巻、95–112 頁。シュプリンガー、ベルリン、ハイデルベルク、2012 年 9 月。

[Bra94] ステファン・ブランズ. 監視者が存在するウォレットにおける追跡不可能なオフライン現金 (拡張要約). ダグラス・R・スティンソン編, *CRYPTO'93*, *LNCS* 773 巻, 302–318 頁. スプリンガー, ベルリン, ハイデルベルク, 1994 年 8 月.

[Bre00] Eric A. Brewer. 堅牢な分散システムに向けて（要旨）. 第 *19* 回 *ACM* 分散コンピューティング原理シンポジウム論文集, 7 ページ. ACM, 2000. 招待講演.

[CCX+ 19] Guoxing Chen, Sanchuan Chen, Yuan Xiao, Yinqian Zhang, Zhiqiang Lin, and Ten-Hwang Lai. SgxPectre: 投機的実行による SGX エンクレーブからの Intel 機密窃取. *2019 IEEE European Symposium on Security and Privacy*, 142–157 頁. IEEE Computer Society Press, 2019 年 6 月.

[CFN90] David Chaum, Amos Fiat, Moni Naor.「追跡不可能な電子現金」. Shafi Goldwasser 編, *CRYPTO'88*, *LNCS* 第 *403* 巻, 319–327 頁. Springer, ニューヨーク, 1990 年 8 月.

[CG07] セバスチャン・カナール、アリーン・グージェ. 分割可能な電子キャッシュシステムは真に匿名性を保てる. モニ・ナオール編, *EUROCRYPT 2007*, *LNCS* 4515 巻, 482–497 頁. スプリンガー, ベルリン, ハイデルベルク, 2007 年 5 月.

[Cha82] David Chaum. 追跡不可能な支払いのためのブラインド署名. David Chaum, Ronald L. Rivest, Alan T. Sherman 編, *CRYPTO'82*, 199–203 頁. Plenum Press, ニューヨーク, アメリカ合衆国, 1982 年.

[Cha86] David Chaum. 身元証明なしでの認証情報の提示：無条件に非連結可能な仮名間で転送される署名. Franz Pichler 編, *EUROCRYPT'85*, *LNCS* 第 *219* 巻, 241–244 頁. Springer, Berlin, Heidelberg, 1986 年 4 月.

[CHL05] Jan Camenisch、Susan Hohenberger、Anna Lysyanskaya。コンパクトな電子キャッシュ。Ronald Cramer 編集、*EUROCRYPT 2005*、*LNCS* 第 3494 巻、302-321 ページ。Springer、ベルリン、ハイデルベルク、2005 年 5 月。

[CHL22] S´ılvia Casacuberta、Julia Hesse、Anja Lehmann。SoK: Oblivious pseudorandom functions。*2022 IEEE European Symposium on Security and Privacy*、625–646 ページ。IEEE Computer Society Press、2022 年 6 月。

[CKLM14] Melissa Chase、Markulf Kohlweiss、Anna Lysyanskaya、Sarah Meiklejohn。可鍛性署名：新しい定義と委任可能な匿名認証情報。Anupam Datta および Cedric Fournet 編、CSF 2014 コンピュータセキュリティ基礎シンポジウム、199-213 ページ。IEEE Computer Society Press、2014 年。

[CL01] ヤン・カメニッシュ、アンナ・リシヤンスカヤ。非譲渡性匿名クレデンシャルのための効率的なシステム：オプションの匿名性撤回機能付き。ビルギット・プフィッツマン編、*EUROCRYPT 2001*、*LNCS* 2045 巻、93–118 頁。Springer、ベルリン、ハイデルベルク、2001 年 5 月。

[CL04] Jan Camenisch および Anna Lysyanskaya。双線形写像による署名方式および匿名認証。Matthew Franklin 編集、*CRYPTO 2004*、*LNCS* 第 3152 巻、56-72 ページ。Springer、ベルリン、ハイデルベルク、2004 年 8 月。

[CPST15a] Sebastien Canard、David Pointcheval、Olivier Sanders、Jacques Traor´ e. 分割可能な E-cash´ の実用化。ジョナサン・カッツ編、*PKC 2015*、*LNCS* 第 9020 巻、77-100 ページ。Springer、ベルリン、ハイデルベルク、2015 年 3 月/4 月。

[CPST15b] セバスチャン・カナール、デヴィッド・ポワントシュヴァル、オリヴィエ・サンダース、ジャック・トラオレ e. スケーラブルな分割可能電子マネー。タル・マルキン、ウラジミール・コレスニコフ、アリソン・ビショップ・ルウコ、ミハリス・ポリクロナキス編、*ACNS 2015*、*LNCS* 9092 巻、287–306 頁。シュプリンガー、チャム、2015 年 6 月。

[CV02] ヤン・カメニッシュ、エルス・ファン・ヘレウェヘン. idemix 匿名認証システムの設計と実装. ヴィジャヤラクシュミ・アトルリ編, *ACM CCS 2002*, 21–30 頁. ACM Press, 2002 年 11 月.

[CVM+ 21] Zitai Chen, Georgios Vasilakis, Kit Murdock, Edward Dean, David Oswald, Flavio D. Garcia. VoltPillager: SVID 電圧スケーリングインターフェースを用いた Intel SGX エンクレーブに対するハードウェアベースの障害注入攻撃. Michael Bailey, Rachel Greenstadt 編, *USENIX Security 2021*, 699–716 頁. USENIX Association, 2021 年 8 月.

[CYS+ 21] Jinhua Cui、Jason Zhijingcheng Yu、Shweta Shinde、Prateek Saxena、Zhiping Cai。SmashEx：例外を用いた SGX エンクレーブの破壊。Giovanni Vigna と Elaine Shi 編、*ACM CCS 2021*、779–793 頁。ACM Press、2021 年 11 月。

[DDE+ 18] ファーガス・ダル、ガブリエル・デ・ミケリ、トーマス・アイゼンバース、ダニエル・ゲンキン、ナディア・ヘニンガー、アフマド・モギミ、ユバル・ヤロム。CacheQuote：キャッシュ攻撃による SGX EPID の 長期秘密の効率的回復。*IACR TCHES*、2018(2):171–191、2018 年。

[dPK22] Rafael del Pino と Shuichi Katsumata。トラップドアサンプリングによる、より効率的なラウンド最適格子ベース（部分）ブラインド署名のための新たな枠組み。Yevgeniy Dodis と Thomas Shrimpton 編、*CRYPTO 2022*、*Part II*、*LNCS* 13508 巻、306–336 ページ。Springer, Cham, 2022 年 8 月。

[EKR18] David Evans、Vladimir Kolesnikov、Mike Rosulek。安全なマルチパーティ計算の実用的な紹介。*Found. Trends Priv. Secur.*、2(2-3):70–246、2018。

[Eur23] 欧州委員会。欧州議会及び理事会によるデジタルユーロ創設に関する規則案。https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0369、2023 年 6 月。COM(2023) 369 final、CELEX: 52023PC0369。

[FDC11] オーレリアン・フランシヨン、ボリス・ダネフ、スルジャン・カプクン。現代自動車における「キーレスエントリー」および「キーレススタート」システムに対する中継攻撃。*NDSS 2011*。インターネット協会、2011 年 2 月。

[FPV09] ゲオルグ・フックスバウアー、デビッド・ポワントシュヴァル、ダミアン・ヴェルノー。移転可能な定サイズ公正電子現金。フアン・A・ガライ、宮地敦子、大塚明編、*CANS 09*、*LNCS* 5888 巻、226–247 頁。シュプリンガー、ベルリン、ハイデルベルク、2009 年 12 月。

[FQF+ 24] Dengguo Feng, Yu Qin, Wei Feng, Wei Li, Ketong Shang, Hongzhan Ma. 機密計算に関する研究の概観. *IET Commun.*, 18(9):535–556, 2024.

[GL02] Seth Gilbert と Nancy Lynch. ブリュワーの予想と、一貫性・可用性・分割耐性を備えたウェブサービスの実現可能性. *ACM SIGACT News*, 33(2):51–59, 2002.

[GMR89] シャフィ・ゴールドワッサー、シルヴィオ・ミカリ、チャールズ・ラコフ。対話型証明システムの知識複雑性。*SIAM Journal on Computing*、18(1):186–208、1989 年。

[Gol01] オデッド・ゴールドライヒ.『暗号の基礎：基本ツール』第 1 巻. ケンブリッジ大学出版局, 英国ケンブリッジ, 2001 年.

[GOS06] イェンス・グロート、ラファイル・オストロフスキー、アミット・サハイ。NP に対する完全非対話型ゼロ知識証明。セルジュ・ヴォードネイ編、*EUROCRYPT 2006*、*LNCS* 第 *4004* 巻、339–358 頁。シュプリンガー、ベルリン、ハイデルベルク、2006 年 5 月/6 月。

[Gro16] イェンス・グロート. ペアリングに基づく非対話型証明のサイズについて. マルク・フィシュリン、ジャン＝セバスチャン・コロン編,『*EUROCRYPT 2016*』第 *II* 部, *LNCS* シリーズ第 *9666* 巻, 305–326 頁. シュプリンガー, ベルリン、ハイデルベルク, 2016 年 5 月.

[GS08] イェンス・グロート、アミット・サハイ. 二重線形群のための効率的な非対話型証明システム. ナイジェル・P・スマート編, *EUROCRYPT 2008*, *LNCS* 4965, 415–432 頁. スプリンガー, ベルリン, ハイデルベルク, 2008 年 4 月.

[Han23] Lucjan Hanzlik. ランダムメッセージのための非対話型ブラインド署名. Carmit Hazay と Martijn Stam 編, *EUROCRYPT 2023, Part V*, *LNCS* 14008 巻, 722–752 頁. Springer, Cham, 2023 年 4 月.

[HPZ25] Lucjan Hanzlik, Eugenio Paracucchi, Riccardo Zanotto.「RSA 仮定とそれ以上に基づく非対話型ブラインド署名」. Serge Fehr, Pierre-Alain Fouque 編, *EUROCRYPT 2025, Part II*, *LNCS* 15602 巻, 365–394 頁. Springer, Cham, 2025 年 5 月.

[KJJ99] Paul C. Kocher, Joshua Jaffe, Benjamin Jun. 差分電力解析. Michael J. Wiener 編, *CRYPTO'99*, *LNCS* 1666, 388–397 頁. Springer, Berlin, Heidelberg, 1999 年 8 月.

[KJJR11] Paul C. Kocher, Joshua Jaffe, Benjamin Jun, Pankaj Rohatgi. 差分電力解析入門. *Journal of Cryptographic Engineering*, 1(1):5–27, 2011 年 4 月.

[Kle15] マーティン・クレップマン。CAP 定理の批判。*CoRR*、abs/1509.05393、2015 年。

[KLLQ23] 勝俣修一、Yi-Fu Lai、Jason T. LeGrow、Ling Qin。CSI-Otter：ひねりを加えたクラス群作用による等質群ベースの（部分的な）ブラインド署名。Helena Handschuh および Anna Lysyanskaya 編、*CRYPTO 2023*、*Part III*、*LNCS* 第 14083 巻、729–761 ページ。Springer, Cham, 2023 年 8 月。

[Koc96] ポール・C・コッチャー. ディフィー・ヘルマン、RSA、DSS 及びその他のシステムの実装に対するタイミング攻撃. ニール・コブリッツ編, *CRYPTO'96*, *LNCS* 第 1109 巻, 104–113 頁. スプリンガー, ベルリン, ハイデルベルク, 1996 年 8 月.

[KW05] ジブ・クフィルとアヴィシャイ・ウール. 非接触型スマートカードシステムに対する中継攻撃を用いた仮想ポケットの搾取. 暗号学電子印刷アーカイブ, 報告書 2005/052, 2005 年.

[MIE17] Ahmad Moghimi, Gorka Irazoqui, Thomas Eisenbarth. CacheZoom: SGX がキャッシュ攻撃の威力を増幅する仕組み. Wieland Fischer, Naofumi Homma 編, *CHES 2017*, *LNCS* 第 *10529* 巻, 69–90 頁. Springer, Cham, 2017 年 9 月.

[MOG+ 20] キット・マードック、デイビッド・オズワルド、フラビオ・D・ガルシア、ジョー・ヴァン・ブルック、ダニエル・グラス、フランク・ピエッセンズ。Plundervolt：インテル SGX に対するソフトウェアベースのフォールトインジェクション攻撃。*2020 IEEE* セキュリティ・プライバシーシンポジウム、1466–1482 頁。IEEE コンピュータソサエティプレス、2020 年 5 月。

[MS98] 宮崎慎吾、櫻井浩一。離散対数問題に基づく部分盲署名を用いた、より効率的な追跡不能電子キャッシュシステム。Rafael Hirschfeld 編、*FC'98*、*LNCS* 第 *1465* 巻、296–308 頁。Springer、ベルリン、ハイデルベルク、1998 年 2 月。

[岡 95] 岡本達明. 効率的な分割可能な電子キャッシュ方式. ドン・コッパースミス編, *CRYPTO'95*, *LNCS* 963 巻, 438–451 頁. シュプリンガー, ベルリン, ハイデルベルク, 1995 年 8 月.

[岡 06] 岡本達明. ランダムオラクルを必要としない効率的なブラインド署名と部分的ブラインド署名. Shai Halevi と Tal Rabin 編, *TCC 2006*, *LNCS* 3876 巻, 80–99 頁. Springer, Berlin, Heidelberg, 2006 年 3 月.

[OP11] David Oswald と Christof Paar. Mifare DESFire MF3ICD40 の破り方：実環境における電力解析とテンプレート. Bart Preneel と Tsuyoshi Takagi 編, *CHES 2011*, *LNCS* 6917 巻, 207–222 頁. Springer, Berlin, Heidelberg, 2011 年 9 月/10 月.

[Sch90] クラウス＝ペーター・シュノール. スマートカードのための効率的な識別と署名. ジル・ブラサール編, *CRYPTO'89*, *LNCS* 435 巻, 239–252 頁. スプリンガー, ニューヨーク, 1990 年 8 月.

[Sch91] クラウス＝ペーター・シュノール. スマートカードによる効率的な署名生成. *Journal of Cryptology*, 4(3):161–174, 1991 年 1 月.

[SMvH+ 21]カールトン・シェパード、コンスタンティノス・マルカントナキス、ニコ・ファン・ヘイニンゲン、ドリス・アブールカシミ、クレメント・ゲイン、ティボー・ヘックマン、デイビッド・ナカッシュ. モバイルデバイスに対する物理的故障注入とサイドチャネル攻撃：包括的分析. コンピュータセキュリティ, 111:102471, 2021.

[TBB+ 22] Carmela Troncoso, Dan Bogdanov, Edouard Bugnion, Sylvain Chatel, Cas Cremers, Seda F. Gurses, Jean-Pierre Hubaux, Dennis Jackson, James R. Larus, Wouter Lueks, Rui Oliveira, Mathias Payer, Bart Preneel, Apostolos Pyrgelis, Marcel Salathe, Theresa Stadler, Michael Veale.分散型でプライバシーを保護する近接追跡の展開。Commun. ACM, 65(9):48–57, 2022.

[VMW+ 18] Jo Van Bulck、Marina Minkin、Ofir Weisse、Daniel Genkin、Baris Kasikci、Frank Piessens、Mark Silberstein、Thomas F. Wenisch、Yuval Yarom、Raoul Strackx。

Foreshadow：一時的なアウト・オブ・オーダー実行による SGX の鍵抽出。ウィリアム・エンクとアドリアン・ポーター・フェルト編『*USENIX Security 2018*』991–1008 頁。USENIX 協会、2018 年 8 月。

[vSY+ 24] ステファン・ファン・シャイク、アレクサンダー・セト、トーマス・ユレック、アダム・バトリ、ベイダー・アルバサム、ダニエル・ゲンキン、アンドルー・ミラー、エイアル・ロネン、ユヴァル・ヤロム、クリスティーナ・ガーマン。SoK: SGX.fail: 情報がどのように暴露されるか。*2024 IEEE* セキュリティおよびプライバシーに関するシンポジウム、4143–4162 ページ。IEEE コンピュータ協会出版、2024 年 5 月。

[WCP+ 17] Wenhao Wang、Guoxing Chen、Xiaorui Pan、Yinqian Zhang、XiaoFeng Wang、Vincent Bindschaedler、Haixu Tang、Carl A. Gunter。暗い土地の漏れる大釜：SGX におけるメモリサイドチャネルの危険性を理解する。Bhavani M. Thuraisingham、David Evans、Tal Malkin、Dongyan Xu 編、*ACM CCS 2017*、2421–2434 ページ。ACM Press、2017 年 10 月/11 月。

[ZPZ+ 16] Christian T. Zenger、Mario Pietersz、Jan Zimmer、Jan-Felix Posielek、Thorben Lenze、Christof Paar。相関ランダムチャネルを利用した、リソースの少ないデバイス向けの認証付き鍵確立。*Comput. Networks*、109:105–123、2016 年。