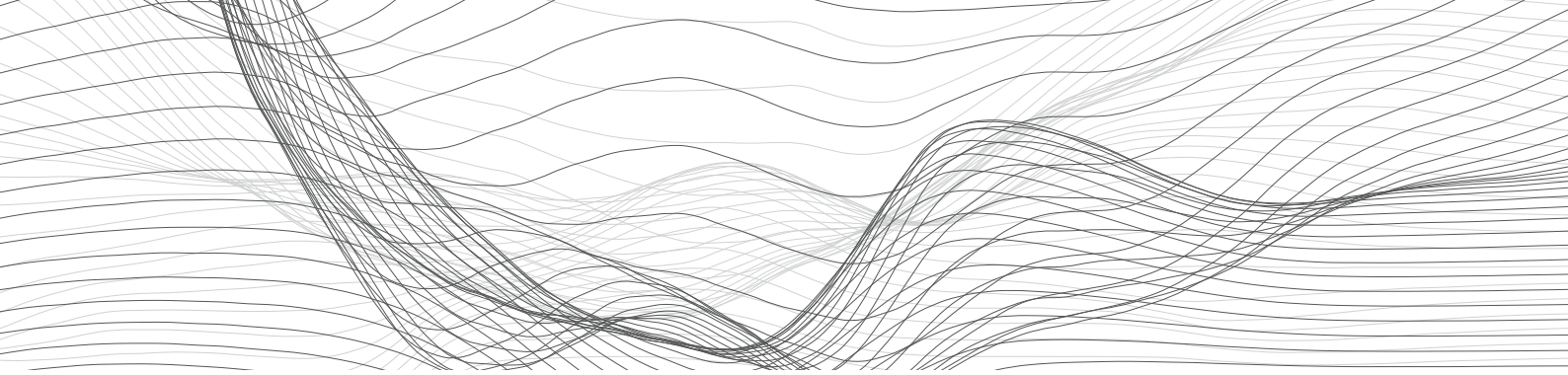


Comment émettre une monnaie numérique de banque centrale

David Chaum, Christian Grothoff, Thomas Moser

SNB Working Papers
3/2021

SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIUNALA SVIZRA
SWISS NATIONAL BANK

ASPECTS JURIDIQUES

CLAUSE DE NON-RESPONSABILITÉ

Les opinions exprimées dans cet article sont celles de l'auteur ou des auteurs, et ne reflètent pas nécessairement celles de la Banque nationale suisse. *Les Working Papers* présentent la recherche en cours. Leur objectif est de susciter les commentaires et la discussion.

COPYRIGHT

LIMITATION DE LA RESPONSABILITÉ

ISSN 1660–7716 (version imprimée)
ISSN 1660–7724 (version électronique)

Comment émettre une monnaie numérique de banque centrale*

Par David Chaum [a], Christian Grothoff [b] et Thomas Moser [c]

[a] xx Network
[b] Haute Ecole spécialisée bernoise et Projet GNU
[c] Banque nationale suisse

Présente version: février 2021
Première version: mai 2020

Résumé

Avec l'émergence du Bitcoin et des cryptomonnaies stables des géants du web (comme le Diem, anciennement Libra), les banques centrales doivent faire face à une concurrence accrue des acteurs privés qui développent leur propre solution numérique en vue de contourner les espèces. Nous ne nous penchons pas sur la question normative de savoir si les banques centrales devraient émettre une monnaie numérique de banque centrale (MNBC). Nous contribuons au débat actuel de la recherche en montrant comment une banque centrale pourrait réaliser un tel projet si elle le souhaitait. Nous proposons un système par jetons, sans registre distribué, et montrons comment les monnaies électroniques purement logicielles émises par le passé peuvent être améliorées pour préserver la confidentialité des transactions, répondre aux critères réglementaires et offrir une protection de niveau post-quantique contre les risques systémiques pour la protection de la vie privée. Ni la politique monétaire ni la stabilité financière ne seraient réellement affectées par ce système puisque la MNBC imiterait les espèces plutôt que les dépôts bancaires.

JEL: E42, E51, E52, E58, G2

Mots clés: monnaies numériques, banque centrale, CBDC, signatures aveugles, cryptomonnaies stables, *stablecoins*

*David Chaum (david@chaum.com), Christian Grothoff (christian.grothoff@bfh.ch), Thomas Moser (thomas.moser@snb.ch). Nous souhaitons remercier Michael Barczay, Roman Baumann, Morten Bech, Nicolas Cuche-Curti, Florian Dold, Andreas Fuster, Stefan Kügel, Benjamin Müller, Dirk Niepelt, Oliver Sigrist, Richard Stallman, Andreas Wehrli, et trois relecteurs anonymes pour leurs commentaires et contributions. La traduction française a été faite par Marie Walrafen et Emmanuel Benoist. Les vues, opinions, résultats et conclusions ou recommandations exprimées dans cet article sont strictement celles des auteurs. Elles ne reflètent pas nécessairement les positions de la Banque Nationale Suisse (BNS). La BNS décline toute responsabilité pour les erreurs, imprécisions ou omissions que pourrait contenir le présent document.

I. Introduction

Dès l'avènement de l'ordinateur personnel dans les années 1980, et plus spécifiquement depuis la levée par la National Science Foundation des restrictions sur l'usage commercial de l'Internet en 1991, la création d'espèces numériques pour les paiements en ligne a été une quête. La première proposition a été faite par Chaum (1983). Bien que de tels processus aient été mis en œuvre, ils ne se sont pas popularisés; par contre, les cartes de crédit sont devenues le moyen de paiement en ligne le plus répandu. La proposition par Nakamoto (2008) d'une monnaie virtuelle intégralement de pair à pair et le succès du lancement du Bitcoin qui en a résulté ont ouvert une nouvelle ère de recherche et développement sur les monnaies numériques. CoinMarketCap recense plus de 5 000 cryptomonnaies. Dernièrement, les banques centrales ont commencé à envisager ou au moins étudier l'émission de monnaies numériques (voir Auer et al. 2020, Boar et al. 2020, Kiff et al. 2020, et Mancini-Griffoli et al. 2018).

A l'heure actuelle, les banques centrales émettent deux types de monnaie: (i) des réserves sous forme de comptes de règlement à la banque centrale pour des acteurs agréés des marchés financiers et (ii) des devises sous formes de billets de banque disponibles pour le public. Par conséquent, la littérature sur la monnaie numérique de banque centrale distingue (a) la MNBC de gros dont l'accès est limité et (b) la MNBC de détail accessible à tous (voir par exemple Bech et Garratt 2017). Une MNBC de gros serait moins déstabilisante pour le système actuel puisque les banques et les acteurs du marché ont déjà accès à une monnaie de banque centrale numérique avec laquelle ils effectuent les règlements interbancaires. Ici, la question sera de voir si, par rapport aux systèmes de règlements bruts en temps réel (RBTR) existants, la MNBC sous forme de jetons numériques et la technologie des registres distribués (TRD, ou DLT en anglais) offrent des avantages. Jusqu'ici, la conclusion est négative, tout au moins pour les paiements interbancaires nationaux (voir Chapman et al. 2017).

Une MNBC de détail, qui serait une nouvelle forme de monnaie de banque centrale accessible à tous, pourrait être beaucoup plus déstabilisante pour le système actuel, selon la

façon dont elle est conçue. Plus une telle MNBC sera en concurrence avec les dépôts des banques commerciales, plus elle menacera leur financement, avec des effets potentiellement négatifs sur les crédits bancaires et l'activité économique (voir Agur et al. 2019). Pour autant, une MNBC de détail pourrait également être bénéfique (voir Bordo et Levin 2017, Berentsen et Schär 2018, Bindseil 2020, Niepelt 2020, Sveriges Riksbank 2020, et Bank of England 2020). Emettre une monnaie numérique de banque centrale exempte de risque de contrepartie et accessible à tous pourrait aussi améliorer la stabilité et la résilience du système de paiement de détail. Cela pourrait également fournir une infrastructure de paiement neutre permettant d'encourager la concurrence, l'efficacité, et l'innovation. Globalement, les coûts et les avantages d'une MNBC de détail sont susceptibles de varier d'un pays à l'autre. Pour le point de vue de la Banque nationale suisse (BNS), qui n'a aucun projet d'émission de MNBC de détail, voir Jordan 2019.

Dans la présente analyse, nous étudions la MNBC de détail, sans aborder la question de savoir si une banque centrale *devrait* émettre une MNBC. Nous nous concentrons sur une architecture technique. L'intérêt pour la conception des MNBC s'est dernièrement considérablement accru (voir par exemple Allen et al. (2020), Bank of England (2020)). La conception que nous proposons est singulièrement différente des propositions existantes. Notre système poursuit et développe la technologie d'eCash décrite par Chaum (1983) et par Chaum et al. (1990). En particulier, nous proposons une MNBC purement logicielle, par jetons, sans registre distribué. La DLT est une architecture intéressante lorsqu'il n'existe pas d'acteur central ou si les parties prenantes ne souhaitent pas s'accorder sur un acteur central de confiance. Ce qui n'est cependant pratiquement jamais le cas pour une monnaie numérique de détail émise par une banque *centrale*. Recourir à un registre distribué ne fait qu'augmenter les coûts de transaction; cela n'apporte aucun avantage dans une mise en place par une banque centrale. L'utilisation d'une DLT

est pertinente en l'absence de banque centrale (voir par exemple le projet Sovereign des îles Marshall) ou si l'intention est de se passer de banque centrale (par exemple Bitcoin)[1].

La présente proposition de MNBC par jetons permet la préservation d'une propriété clé de la monnaie physique: la confidentialité des transactions. Il est habituellement considéré que la cryptographie permettant de garantir la confidentialité requiert tellement de puissance de calcul que son utilisation sur des appareils portables est infaisable. (voir Allen et al. 2020). Bien que cela puisse être vrai dans le cas d'une DLT où la traçabilité des transactions est nécessaire pour éviter les doubles dépenses (Narayanan et al. 2016), ce n'est pas le cas d'un processus de signature aveugle de type Chaum avec une banque centrale, comme exposé dans cet article. Notre MNBC, basée sur les signatures aveugles et une architecture à deux niveaux, garantit parfaitement la protection post-quantique de la confidentialité des transactions, tout en fournissant à la société des protections contre le blanchiment d'argent (AML) et le financement du terrorisme (CFT) qui sont de fait plus fortes que celles des billets de banque.

La confidentialité des transactions est importante pour trois raisons. Premièrement, elle protège d'une surveillance et d'un contrôle potentiellement abusifs par les gouvernements. Même si l'on pense n'avoir rien à cacher, la surveillance de masse reste problématique, ne serait-ce qu'à cause du risque d'erreur et d'abus, surtout si elle s'effectue sans transparence ni responsabilité (voir Solove 2011). Deuxièmement, la confidentialité des transactions protège les utilisateurs de l'exploitation des données par les prestataires de services de paiement. Enfin, elle protège l'utilisateur contre toute autre partie à une transaction, en empêchant un comportement opportuniste ex-post ou une protection des données défaillante ou négligée par l'autre partie (voir Kahn et al. 2005).

1 Il peut y avoir des cas opportuns d'utilisation de la DLT pour des infrastructures de marchés financiers, comme les échanges numériques, lorsque la question se pose de savoir comment intégrer de l'argent de banque centrale au sein d'une structure DLT pour effectuer des règlements. Toutefois, dans ces situations, les avantages potentiels de la DLT, à savoir une baisse des coûts ou un rapprochement automatique, n'ont aucun lien avec l'émission décentralisée de monnaie de banque centrale.

Le présent document est structuré comme suit: dans la section II, nous rappelons la différence entre une monnaie de banque centrale et les autres monnaies. Dans la section III, nous passons en revue les conceptions habituelles de MNBC avant d'exposer notre conception dans la section IV. Nous discutons ensuite les aspects règlementaires et stratégiques et les travaux liés (VI) avant de conclure (VII).

II. Qu'est-ce que la monnaie de banque centrale ?

La monnaie est un actif qui peut être utilisé pour acheter des biens et services. Pour être une monnaie, l'actif doit être accepté par des acteurs autres que l'émetteur. C'est pourquoi les bons par exemple, ne sont pas considérés comme monnaie. Une réelle monnaie doit être *communément* acceptée comme moyen d'échange. Bien que la monnaie possède également la qualité d'unité de mesure et de stockage de valeur, sa caractéristique spécifique est sa fonction de moyen d'échange. Normalement, l'unité de compte (soit le moyen par lequel se fait l'établissement des prix et l'enregistrement des dettes) coïncide avec le moyen d'échange pour des raisons pratiques. Ils peuvent être cependant séparés, si le moyen d'échange vient à manquer de stabilité en valeur par rapport aux biens et services échangés[2]. La monnaie doit également être une réserve de valeur afin de garder son pouvoir d'achat entre le moment où elle est reçue et le moment où elle est dépensée. Pour autant, il existe de nombreux autres actifs servant de réserve de valeur, tels que les actions, les obligations, les métaux précieux ou les biens immobiliers. La réserve de valeur n'est pas une propriété exclusive de la monnaie.

Dans une économie moderne, la population utilise deux types de monnaies: (a) la monnaie d'Etat et (b) la monnaie privée. Généralement, la monnaie d'Etat est émise par la

[2] Cela peut se produire spontanément dans un environnement à forte inflation, par exemple lorsque les prix sont indiqués en dollars mais que les paiements sont effectués en monnaie locale. Il en va de même pour les paiements en bitcoin, où les prix sont généralement affichés en dollars ou dans d'autres monnaies locales en raison de la forte volatilité du bitcoin. Une séparation peut également se faire à dessein, comme dans le cas de la Unidad de Fomento (UF) au Chili ou du droit de tirage spécial (DTS) du Fonds monétaire international (FMI). Toutefois, là aussi, l'objectif est de disposer d'une unité de compte plus stable.

banque centrale agissant comme un agent de l'Etat. La monnaie de banque centrale est disponible pour des acteurs sélectionnés sous forme de dépôts à la banque centrale (les réserves), et pour la population sous forme de monnaie fiduciaire (billets de banque et pièces) également appelée «espèces». Dans une économie moderne, la monnaie fiduciaire n'a pas de valeur intrinsèque. Juridiquement, c'est un passif de la banque centrale, bien qu'elle ne soit pas remboursable. Dans la plupart des pays, la monnaie de banque centrale a cours légal et doit donc être acceptée pour le paiement de toute dette monétaire, dont les impôts et amendes. Bien que cela assure une certaine valeur à la monnaie de banque centrale, le fait d'avoir cours légal ne suffit pas au maintien de la stabilité de sa valeur. C'est la politique monétaire de la banque centrale qui maintient la valeur de la monnaie. La stabilité des prix – à savoir la valeur de la monnaie par rapport à celle des biens et services échangés – est en effet l'une des principales responsabilités des banques centrales.

Dans une économie moderne, la plupart des paiements sont effectués à partir de fonds privés émis par des banques commerciales. Cet argent est constitué des dépôts à vue que les personnes détiennent auprès des banques commerciales. Ces dépôts à vue peuvent être utilisés avec des chèques, des cartes de paiement, de cartes de crédit et d'autres moyens de transfert d'argent. Ils sont inscrits au passif des banques commerciales concernées. Une caractéristique essentielle de ces dépôts est que les banques commerciales garantissent leur conversion en monnaie de banque centrale à la demande à un prix déterminé, en l'occurrence à leur valeur nominale. Les déposants peuvent retirer leurs fonds en espèces ou les transférer au taux fixe de 1:1. Les banques commerciales maintiennent la valeur de leur argent en l'adossant à la monnaie banque centrale.

Néanmoins, dans un système de réserve fractionnaire, une banque commerciale – même solvable – peut manquer de liquidités pour honorer sa promesse de conversion en monnaie de banque centrale (par exemple en cas de panique bancaire) jusqu'à voir ses clients dans l'impossibilité de retirer leur argent. Une banque peut également devenir insolvable, faire faillite et par conséquent ses clients peuvent perdre de l'argent. C'est pourquoi les banques commerciales sont soumise à une réglementation destinée à limiter ces risques.

Une différence notoire entre la monnaie de banque centrale et la monnaie émise par les banques commerciales est donc que cette dernière comporte des risques de contrepartie. Une banque centrale peut toujours répondre à ses engagements en utilisant sa monnaie non remboursable. La monnaie de banque centrale est la seule valeur monétaire d'une économie domestique qui ne présente aucun risque de crédit ou de liquidité. C'est ainsi la valeur préférée pour effectuer les règlements au sein des infrastructures des marchés financiers (cf., CPMI-IOSCO Principles for Financial Market Infrastructures (2012)). Une autre différence réside dans la capacité de la monnaie de banque centrale à fournir un ancrage au système monétaire domestique en fournissant une valeur de référence avec laquelle les banques commerciales maintiennent une convertibilité totale.

En dehors des banques commerciales, d'autres acteurs privés tentent parfois d'émettre de la monnaie. Les cryptomonnaies n'en sont que les plus récentes tentatives. Mais contrairement aux dépôts à vue, ces monnaies ne sont pas communément admises comme moyen d'échange. Ceci vaut même pour le Bitcoin, qui est pourtant la cryptomonnaie la mieux acceptée. La forte volatilité de leur valeur est l'une des entraves à leur usage comme moyen d'échange. La récente émergence des cryptomonnaies stables (*stablecoins*) s'est faite en réponse à ce problème. Les *stablecoins* tentent d'asseoir leurs valeurs par l'une des deux méthodes suivantes: soit ils imitent les banque centrales (*stablecoins* algorithmiques), soit ils imitent les banques commerciales et autres fonds privés (*stablecoins* adossés à des actifs)[3].

Les *stablecoins* algorithmiques s'appuient sur des algorithmes pour ajuster l'offre. En d'autres termes, ils tentent d'accéder à la stabilité des prix grâce à leur propre «politique monétaire algorithmiques». S'il en existe un certain nombre d'exemples (comme le NuBits), aucun d'entre eux n'a réussi à stabiliser sa valeur sur une longue période.

Les *stablecoins* adossés à des actifs varient selon les types d'actifs utilisés et les droits accordés à leurs détenteurs. Les types d'actifs généralement utilisés sont monétaires (réserves de banque centrale, billets ou dépôts bancaires), des matières premières (comme

[3] Pour une taxonomie détaillée des *stablecoins*, voir Bullmann et al. (2019).

l'or), des valeurs mobilières et parfois d'autres cryptomonnaies. Le succès de telles stratégies pour stabiliser la valeur du *stablecoin* par rapport à celle des actifs dépend essentiellement des droits qu'acquièrent les détenteurs de *stablecoins*. Si le *stablecoin* est remboursable à prix fixe (par exemple 1 *coin* = 1 USD ou 1 *coin* = 1 once d'or), sa stabilité peut être en théorie réalisée. Cette stratégie reproduit alors celle des banques commerciales en garantissant à la demande la convertibilité dans la valeur choisie[4]. Cependant, contrairement aux dépôts bancaires qui ne sont en général que partiellement couverts par des réserves de banque centrale, les *stablecoins* sont le plus souvent entièrement couverts par des réserves dans les actifs choisis afin d'éviter les risques de liquidité, et ce surtout à défaut des avantages de garde-fous publics tels que les fonds de garantie et le prêteur en dernier ressort dont bénéficient les banques réglementées.

Les *stablecoins* couverts en monnaie fiduciaire sont aussi appelées *fiat-currency stablecoins*. La couverture à 100% en monnaie fiduciaire (billets ou dépôts bancaires) n'est cependant pas très rentable. Par conséquent, les détenteurs de *stablecoins* sont fortement incités à économiser leur détention d'actifs pour se tourner vers des systèmes de réserves fractionnaires ainsi que l'ont fait les banques commerciales[5]. Ceci implique de réduire leurs actifs les moins rentables au minimum estimé nécessaire pour garantir leurs engagements de convertibilité et d'augmenter à la place leurs actifs liquides à fort rendement tels les obligations d'état. Ce qui augmente leur rentabilité mais accroît leur niveau de risque. Cependant, même si un *stablecoin* est entièrement adossé à des dépôts bancaires il reste vulnérable aux risques de défaut de crédit ou de liquidité de la banque correspondante. Ce risque peut être écarté si les dépôts sont faits à la banque centrale ou si le *stablecoin* est

[4] La stabilisation de la valeur du *stablecoin* par rapport aux biens et services échangés dépend essentiellement de la stabilité de la valeur des actifs auxquels il est adossé par rapport aux biens et services échangés.

[5] L'incertitude concernant les garanties d'un *stablecoin* peut être l'une des raisons pour lesquelles on voit des *stablecoins* échangés en dessous de leur valeur sur le marché secondaire (voir Lyons et Ganesh Viswanath-Natraj, 2020). Des cas similaire ont également pu se présenter à l'époque où les banques commerciales émettaient les billets de banque. Ces billets s'échangeaient à des taux variables sur le marché secondaire jusqu'à ce que l'émission de billets de banque soit nationalisée et transférée aux banques centrales avec un monopole.

adossé aux réserves de banque centrale. Les *stablecoins* ont été appelés «MNBC de synthèse» (*synthetic CBDCs*, Adrian et Mancini-Griffoli 2019). Il est important de souligner que de tels *stablecoins* sont distincts de la monnaie centrale et ne constitue donc pas une MNBC, puisqu'ils ne sont pas inscrits au passif de la banque centrale et donc toujours exposés aux risque de contreparties, notamment au risque de faillite de l'émetteur du *stablecoin*.

Si un *stablecoin* n'est pas remboursable à un prix déterminé, sa stabilité relative à l'actif auquel il est adossé n'est pas garantie. Si le *stablecoin* représente une part de propriété de l'actif sous-jacent, le schéma ressemble alors à celui d'un fonds commun de placement fermé ou à un fonds négocié en bourse (ETF ou FNB) et inclut les risques de ceux-ci. La valeur du *coin* va dépendre de la valeur liquidative du fonds, laquelle valeur peut dériver. S'il existe des acteurs autorisés à créer et rembourser des *stablecoins* et ainsi se placer en arbitres, comme dans les cas de FNB, et comme cela est prévu pour Diem (Libra Association 2020), la dérivée est supposée être minime.

Globalement les *stablecoins* ont plus de chance de devenir monnaie que les cryptomonnaies, surtout s'ils sont correctement règlementés. Cependant, la disponibilité de MNBC limiterait considérablement l'utilité de ces *stablecoins*.

III. Conceptions simples de MNBC

Comme nous l'avons exposé, une MNBC serait un passif de la banque centrale. Les deux conceptions différentes dans la littérature sur le sujet sont (a) une MNBC basée sur des comptes et (b) une MNBC par jetons (ou basée sur la valeur). Elles correspondent aux deux types existant de monnaies de banque centrale et des systèmes de paiement y afférents (Kahn et Roberds 2008): les réserves de banque centrale (système basé sur des comptes) et les billets de banque (système basé sur des jetons). Un paiement a lieu lorsqu'une valeur monétaire est transférée d'un payeur vers un receveur. Dans un système basé sur des comptes, le transfert a lieu en débitant le compte du payeur et en créditant celui du

receveur. Dans un système basé sur des jetons, le transfert a lieu en transférant la valeur elle-même, à savoir un jeton qui représente la valeur monétaire. Les espèces, pièces ou billets, sont les premiers exemples de jetons. Payer en espèces signifie donner une pièce ou un billet de banque. Aucun besoin d'enregistrement du jeton, la simple possession suffit. Ainsi, les parties n'ont à aucun moment de la transaction besoin de s'identifier, et ils peuvent tous deux rester anonymes. Cependant, le receveur doit pouvoir vérifier l'authenticité du jeton. C'est la raison pour laquelle les banques centrales investissent des moyens considérables dans les éléments de sécurité de leurs billets de banque.

Il a été suggéré que la différence entre les systèmes basés sur des comptes et ceux basés sur des jetons n'est pas applicable aux monnaies numériques (Garratt et al. 2020). Nous pensons au contraire qu'il existe une différence significative. La différence essentielle est l'information portée par l'actif informatique. Dans un système basé sur des comptes, les actifs (comptes) sont associés à un historique de transactions qui comprend toutes les opérations de débit et de crédit du compte. Dans un système basé sur des jetons, les actifs (jetons) ne comportent que les informations sur leur valeur faciale et sur l'entité qui a émis le jeton. Les systèmes par jetons sont donc la seule façon de garder la confidentialité des espèces[6].

A. Une MNBC basée sur des comptes

La façon la plus simple de lancer une MNBC serait de permettre au public de détenir des comptes de dépôt à la banque centrale. Ceci impliquerait une responsabilité de la banque centrale pour les vérifications liées à la connaissance du client (*know your customer*, KYC) ainsi qu'aux luttes contre le blanchiment (*anti money-laundering,* AML) et le financement du terrorisme (*combating financing of terrorism* CFT). Ce qui inclurait

[6] Bien que le nom Bitcoin suggère l'utilisation de jetons, il s'agit d'un système de comptes. Le fait que les comptes ne soient pas gardés dans une seule base de données centralisée mais dans une base de données décentralisée est la seule différence entre un système habituel de comptes et une chaîne de blocs.

non seulement la gestion du processus initial de connaissance du client, mais aussi l'authentification des clients des transactions bancaires et la gestion de la fraude et des faux positifs ou négatifs de l'authentification. Compte tenu de la faible présence physique des banques centrales dans la société et du fait qu'elles ne sont vraisemblablement pas préparées à effectuer une authentification des citoyens à une très large échelle, une telle MNBC demanderait que la banque centrale sous-traite ces vérifications. La totalité du service et de son entretien pourrait être confiée à des fournisseurs tiers (Bindseil 2020), ou la législation pourrait autoriser les banques commerciales à ouvrir des comptes auprès de la banque centrale pour leurs clients (Berentsen et Schär 2018).

Une telle MNBC comptable donnerait potentiellement à la banque centrale accès à beaucoup de données supplémentaires. L'un des problèmes étant que les gouvernements pourraient facilement opérer une surveillance de masse et exécuter des sanctions sur les détenteurs individuels de comptes. Leur nature centralisée rend ces opérations faciles et très peu coûteuses. Même dans les démocraties, il existe de nombreux exemples de surveillance abusive ciblant critiques et opposants politiques. On peut s'imaginer que les banques centrales pourraient protéger ces informations de l'intrusion des gouvernements et de l'abus politique, mais cela ouvrirait néanmoins une nouvelle brèche pour des pressions politiques menaçant l'indépendance des banques centrales. De plus, une base de données centrale serait une cible évidente pour des attaques: l'accès en lecture seule d'un fragment de celle-ci pourrait créer des risques concrets pour les personnes dont les données seraient exposées.

En fournissant des comptes bancaires au public, les banques centrales feraient concurrence aux banques commerciales. Cette concurrence présenterait deux risques. Premièrement, cela menacerait la base de dépôts à vue des banques et pourrait même à l'extrême entraîner une désintermédiation du secteur bancaire. Ceci pourrait affecter la disponibilité du crédit pour le secteur privé et par suite l'activité économique (Agur et al. 2019). La désintermédiation des banques pourrait aussi mener à la centralisation de l'allocation de crédit au sein de la banque centrale, ce qui influerait négativement sur la productivité et la croissance. Deuxièmement, permettre aux personnes de transférer leurs

dépôts pour profiter de la sécurité des dépôts de banque centrale accélèrerait les paniques bancaires lors de crises économiques.

Il y a cependant des contre-arguments. Brunnermeier et Niepelt (2019) soutiennent que les transferts de fonds depuis des comptes de dépôts à vue vers des comptes MNBC entraîneraient, de fait, la substitution d'un financement via les dépôts par un financement via les banques centrales. Cela refléterait la qualité de prêteur en dernier ressort jusque-là implicite des banques centrales. Berentsen et Schär (2018) pensent même que la concurrence avec la banque centrale pourrait avoir un effet vertueux sur les banques commerciales du fait que ces dernières se verraient obligées de consolider la sécurité de leur modèles économiques afin d'éviter les paniques bancaires.

Il y a aussi des propositions pour réduire le risque de désintermédiation en limitant ou en décourageant l'utilisation de la MNBC comme réserve de valeur. Une des propositions est de plafonner la MNBC qu'une personne peut détenir. Une seconde proposition est d'appliquer aux comptes MNBC un taux d'intérêt variable afin que leur rémunération soit toujours suffisamment inférieure à celle des comptes dans les banques commerciales, allant jusqu'à des taux négatifs, pour que la MNBC ne soit pas attrayante pour la conservation de valeur (Kumhof et Noone 2018, Bindseil 2020). Au-delà, pour éviter les paniques bancaires Kumhof et Noone (2018) suggèrent que la MNBC ne soit pas émise en échange de dépôts bancaires, mais seulement en échange de titres tels que des obligations d'Etat. Quoiqu'il en soit, une MNBC basée sur des comptes demanderait une plus ample analyse de ces sujets.

B. Une MNBC par jetons matériels

Une banque centrale pourrait aussi émettre des jetons électroniques plutôt que de tenir des comptes. Cela exigerait que le système puisse prévenir la copie des jetons électroniques. Des fonctions physiquement non clonables (voir Katzenbeisser et al. 2012) et des zones sécurisées dans le matériel (voir Alves et Felton 2004, Pinto et Santos 2019) sont deux technologies envisageables pour prévenir les copies numériques. Toutefois, les fonctions physiques non clonables ne peuvent pas s'échanger sur Internet (éliminant de fait

l'usage principal de la MNBC) et les tentatives précédentes de verrous matériels pour empêcher la copie ont été compromises de façon répétée. (voir par exemple Wojtczuk et Rutkowska 2009, Johnston 2010, Lapid et Wool 2019).

Un des avantages principaux de la MNBC par jetons est que les systèmes par jetons pourraient marcher hors ligne, c'est à dire que les utilisateurs pourraient s'échanger des jetons (de pair à pair) sans impliquer la banque centrale, ce qui protègerait la vie privée et les libertés fondamentales. Toutefois, la désintermédiation − qui se produit lorsque les utilisateurs échangent des jetons électroniques sans recourir à des intermédiaires réalisant les vérifications de connaissance du client (KYC) et les procédures (AML / CFT) − serait problématique pour limiter les abus criminels.

La carte SIM est aujourd'hui le verrou matériel potentiel le plus répandu pour déployer un système avec sécurisation matérielle, mais elle comporte aussi des risques. L'expérience (par exemple Soukup et Muff 2007, Garcia et. al. 2008, Kasper et. al. 2010, CCC 2017) suggère que tout matériel économiquement reproductible qui peut stocker des jetons à valeur monétaire qu'un individu peut détenir et qui permet des transactions hors ligne − et par là-même le vol par clonage des informations − fera l'objet de contrefaçons réussies dès que la valeur économique de l'attaque sera conséquente. De telles attaques viennent également d'utilisateurs qui forcent leurs propres équipements (voir aussi Allen et al. 2020). Les systèmes de cartes de paiement qui ont été déployés précédemment reposent sur la résistance à la copie combinée à la détection de fraude afin de limiter l'impact d'une compromission. La détection de fraude requiert cependant une capacité d'identification du payeur et le traçage des clients, ce qui est incompatible avec le respect de la confidentialité de la transaction.

IV. Une MNBC par jetons conçue pour respecter la vie privée.

La MNBC proposée ici est purement logicielle, une simple application pour smartphone qui ne requiert aucun matériel supplémentaire. La MNBC s'appuie sur eCash et GNU Taler.

Taler fait partie du projet GNU, dont le fondateur Richard Stallman a inventé le terme de logiciel libre (*free software*) aujourd'hui fréquemment appelé *free/libre and opensource software* (FLOSS)[7]. Un logiciel est considéré libre lorsque sa licence accorde quatre libertés essentielles à son utilisateur: la liberté de l'exécuter comme il le souhaite, la liberté de l'étudier et de le modifier, la liberté d'en distribuer des copies et la liberté d'en distribuer des copies modifiées. Le logiciel libre n'empêche pas une commercialisation; l'assistance logicielle est un modèle commercial standard pour FLOSS.

Compte-tenu du nombre important de parties prenantes impliquées dans une MNBC de détail, la banque centrale, le secteur financier, commerçants et clients, ainsi que l'envergure critique de l'infrastructure, une MNBC de détail devrait être basée sur un logiciel libre ou ouvert. Imposer une solution propriétaire qui entraînerait une dépendance à un fournisseur spécifique pourrait vraisemblablement constituer dès le départ un obstacle à son adoption. Avec un logiciel FLOSS, toutes les parties prenantes ont accès à chaque détail de la solution et le droit d'adapter le logiciel à leurs besoins. Ceci facilite l'intégration, améliore l'interopérabilité et la concurrence entre fournisseurs[8]. Cela permet également à la banque centrale de répondre aux exigences de transparence et de responsabilité. Les avantages des logiciels libres en matière de sécurité sont également très largement reconnus. La disponibilité du code source et la liberté de le modifier facilite le repérage de failles et leur correction rapide[9].

[7] Pour plus d'informations sur GNU, voir https://www.gnu.org et Stallman (1985). GNU Taler est publié sous la licence GNU Affero General Public License par le Projet GNU. Autres projets GNU connus auprès des économistes: «R» et «GNU Regression, Econometrics and Time-series Library» (GRETL). Pour une discussion sur les bénéfices du FLOSS sur le logiciel propriétaire pour la recherche, voir Baiocchi et Distaso (2003), Yalta et Lucchetti (2008), et Yalta (2010). Sur les licences ouvertes, voir Lerner et Tirole (2005).

[8] Le matériel privé peut avoir son rôle à jouer. Par exemple pour la protection des stockages de clés et certaines fonctions d'audit, un matériel dédié évalué par un nombre restreint d'experts peut avoir des avantages, à condition qu'une telle sécurité soit un ajout.

[9] Par exemple, le bulletin de cybersécurité publié par la U.S. National Security Agency en avril 2020 incite les utilisateurs à préférer le logiciel libre ou *open source* dans le choix et l'usage des services collaboratifs en ligne: «Le développement open source permet une transparence sur la robustesse du code et sa conformité aux meilleures pratiques, évitant d'offrir des failles ou des vulnérabilités qui mettraient les utilisateurs et données en danger.» (U/OO/134598-20).

Dans l'architecture proposée, toutes les interactions de consommateurs et de commerçants se font avec les banques commerciales. Toutefois, la création d'argent et la base de données sont exclusivement gérées et fournies par la banque centrale. Les banques commerciales identifient le client lorsqu'il retire de la MNBC ainsi que les commerçants lorsqu'ils reçoivent de la MNBC. En revanche lorsqu'il paye, le client n'a besoin que d'autoriser la transaction, et non de s'identifier lui-même. Ceci rend les paiements moins chers, plus faciles et plus rapides tout en prévenant une ingérence trop facile dans la vie privée (Dold 2019). De plus, l'identification des clients lorsqu'ils retirent de la MNBC ainsi que des commerçants ou bénéficiaires lorsqu'ils reçoivent de la MNBC permet la conformité avec les exigences de connaissance de ses clients (KYC) et de lutte contre le financement du terrorisme (CFT).

La MNBC proposée dans ce document est un véritable instrument numérique au porteur puisque lorsque l'utilisateur retire une somme d'argent sous forme d'un nombre, ce nombre est «caché» ou obstrué par le smartphone avec un chiffrement spécifique. Dans le système lui-même, une pièce (*coin*) est une paire de clés publique/privée, la clé privée n'étant connue que du seul détenteur de la pièce[10]. Sa valeur réside dans la signature de la banque centrale. Cette signature figure sur la clé publique de la pièce. La banque centrale signe avec sa propre clé privée et détient une multitude de paires de clés pour signer des pièces de différentes valeurs. Un commerçant peut utiliser la «clé publique» correspondante de la banque centrale pour vérifier la signature. Néanmoins, afin de s'assurer que la pièce n'a pas été copiée et déjà retirée (à savoir «double dépensée»), le commerçant doit déposer la pièce afin que la banque centrale puisse la comparer à sa liste de pièces retirées. Car ni la banque commerciale, ni la banque centrale ne voient le numéro de la pièce; plus tard, lorsque le commerçant dépose la pièce, on ne sait quel utilisateur l'a retirée. L'invisibilisation et la confidentialité en résultant font de ce type de MNBC un véritable instrument numérique au porteur.

[10] Dans Bitcoin, système de comptes, la paire de clés est un compte, avec la clé publique qui est l'adresse du compte et ainsi une sorte d'identité, même s'il s'agit d'un pseudonyme.

Dans l'exposé qui suit, nous apportons une présentation approfondie de la technologie et montrons comment celle-ci peut être intégrée dans le système bancaire actuel pour créer une MNBC. Dold (2019) apporte des détails supplémentaires.

A. Blocs de construction de clés

Décrivons maintenant les principales composantes du protocole, qui comprend notamment les bases mathématiques d'une instanciation possible des primitives cryptographiques, pour illustrer comment une implémentation pourrait fonctionner. Notant qu'il existe d'autres conceptions mathématiques équivalentes pour chacun des éléments, nous ne présentons que les plus simples des solutions sûres dont nous avons connaissance.

Signatures numériques – L'idée de base d'une signature numérique dans un schéma de clé publique de signature est de s'assurer que le détenteur de la clé privée est le seul capable de signer un message, alors que la clé publique permet à n'importe qui de vérifier la validité de la signature[11]. Le résultat de la fonction de vérification de la signature est binaire («vrai» ou «faux»). Si le message est signé avec la clé privée qui appartient à la clé publique de vérification, le résultat est «vrai»; si ce n'est pas le cas, il est «faux». Dans notre proposition, le message est une pièce ou un billet avec un numéro de série, et la signature de la banque centrale atteste de sa validité. Alors que GNU Taler utilise les signatures EdDSA modernes (voir Bernstein 2012), nous présentons un plan simple de signature cryptographique basée sur RSA, système cryptographique bien étudié (Rivest et al. 1978)[12]. Toutefois, en principe, toute technologie de signature (DSA, ECDSA, EdDSA, RSA, etc.) peut être utilisée.

Pour générer une clé RSA, le signataire prend d'abord deux grands nombres premiers p et q et calcule $n = pq$ ainsi que la fonction indicatrice d'Euler $\phi(n) = (p-1)(q-1)$.

[11] La cryptographie à clé publique a été introduite par Diffie et Hellmann (1976), et les premières réalisations de signatures numériques ont été celles de Rivest, Shamir et Adleman (1978).

[12] Pour une discussion sur l'historique du système de chiffrement RSA et une revue des attaques sur ce système, voir Boneh (1999).

Alors, tout e avec $1 < e < \phi(n)$ et $pgcd(e, \phi(n)) = 1$ peut être utilisé pour définir une clé publique (e, n). La condition que le plus grand dénominateur commun (gdc) de e et $\phi(n)$ soit 1 (à savoir qu'ils doivent être premiers entre eux) assure que l'inverse de $e \bmod \phi(n)$ existe. Cet inverse est la clé privée correspondante *d*. Etant donné $\phi(n)$, la clé privée *d* peut être calculée en utilisant l'algorithme d'Euclide étendu tel que $d \cdot e \equiv 1 \bmod \phi(n)$.

Etant données la clé privée *d* et la clé publique (*e*, *n*), la signature RSA *s* d'un message *m* est $s \equiv m^d \bmod n$. Pour vérifier la signature, $m' \equiv s^e \bmod n$ est calculé. Si m' et *m* correspondent, la signature est valable, ce qui prouve que le message a été signé par la clé privée qui correspond à la clé publique de vérification (authentification du message) et que le message n'a pas été modifié durant le transit (intégrité du message). En pratique, les signatures sont posées sur les empreintes (*hash*) des messages plutôt que sur les messages eux-mêmes. Les fonctions de hachage calculent des nombres qui sont des identifiants uniques et courts pour chacun des nombres. Signer un *hash* court est beaucoup plus rapide que de signer une longue série de chiffres; la plupart des algorithmes de signatures ne fonctionnent que sur des entrées relativement courtes[13].

Signatures aveugles – Nous utilisons les signatures aveugles imaginées par Chaum en 1983 pour protéger la confidentialité. Une signature aveugle est employée pour créer la signature cryptographique d'un message sans que le signataire ne puisse lire le contenu du message qu'il signe. Dans notre proposition, cela empêche que la banque commerciale et la banque centrale puissent remonter l'achat jusqu'à l'acheteur. En principe, notre solution fonctionne avec n'importe quel mécanisme de signature aveugle, mais la meilleure solution reste la version basée sur RSA décrite par Chaum (1983).

Le masquage est effectué par les clients qui cachent leurs pièces avant de les transmettre à la banque centrale pour signature. Le client n'a donc pas besoin de faire confiance à la banque centrale. Plus encore, l'obfuscation avec RSA fournit également une

[13] Dans le cas du système RSA, la limite de taille est $log_2 n$ bits.

protection contre les attaques post-quantiques. La banque centrale pour sa part établit une multitude de paires de clé disponibles pour signer des pièces de valeurs variées et publie les clés publiques *(e, n)* pour ces valeurs.

Soit f la valeur de hachage d'une pièce et ainsi l'identifiant unique de cette pièce. Le client retirant une pièce génère tout d'abord un facteur de masquage aléatoire b avec lequel il calcule $f' \equiv fb^e \bmod n$ avec la signature de banque centrale pour cette valeur. La pièce masquée f' est alors transmise à la banque centrale pour signature. La banque centrale signe alors f' avec sa clé privée d en calculant la signature aveugle $s' \equiv (f')^d \bmod n$, attachant s' à la pièce masquée f'et renvoie la paire (s', f') au client. Le client peut alors démasquer la signature en calculant $s \equiv s'b^{-1} \bmod n$. Ceci est rendu possible parce que $(f')^d = f^d b^{ed} = f^d b$ et, donc, multiplier s' avec b^{-1} donne f^d, est une signature RSA valide de f puisqu'auparavant: $s^e \equiv f^{de} \equiv f \bmod n$.

Dans la proposition originale de Chaum, les pièces n'étaient que de simples jetons. Ici, nous voulons que les signatures numériques puissent permettre de signer des contrats. Pour ce faire, dès qu'un portefeuille numérique retire une pièce, il crée d'abord une clé privée de pièce aléatoire c et calcule la clé publique correspondante C pour créer la signature numérique avec les outils habituels de signature cryptographique (comme DSA, ECDSA; EdDSA et RSA). Puis, f est dérivée de la clé publique C par une fonction de hachage cryptographique , avant d'être signée en aveugle par la banque centrale (avec un facteur aveuglant aléatoire par pièce). Maintenant l'acheteur peut utiliser c pour signer des achats électroniques, dépensant ainsi la pièce.

Comme vu plus haut, la banque centrale établirait des paires de clés différentes pour chaque valeur de pièce et publierait la clé publique que les clients peuvent utiliser pour retirer de l'argent. Ces clés d'énumération, et donc les pièces, auraient une date d'expiration avant laquelle elles doivent être changées pour de nouvelles pièces si elles n'ont pas été dépensées. Les clients auront un certain temps pour changer les pièces après leur expiration. Les billets de banque sont eux aussi régulièrement renouvelés afin d'être

équipés des derniers dispositifs de sécurité, sauf que les billets restent en circulation des décennies plutôt que quelques mois ou années[14].

D'un point de vue technique, une date d'expiration a deux avantages. Tout d'abord elle améliore l'efficacité du système puisque la banque centrale peut évacuer les données expirées en s'épargnant ainsi d'avoir à parcourir une liste toujours plus longue de pièces (dépensées) pour détecter une double-dépense. Ensuite, cela réduit les risques de sécurité, parce que la banque centrale n'a pas à s'inquiéter d'attaques sur les clés de valeur (*d*). De plus, dans le cas où une clé privée serait compromise, la période pendant laquelle l'attaquant peut utiliser la clé est limitée. En outre, ajouter des frais de change permettrait d'intégrer des taux d'intérêts négatifs. La banque centrale pourrait également, si elle le souhaite, imposer une limite de conversion, pour des raisons de lutte contre le blanchiment ou le financement du terrorisme (*cash limits*) ou pour des raisons de stabilité financière (éviter la thésaurisation ou les paniques bancaires).

Protocole d'échange de clés – GNU Taler utilise un protocole d'échange de clé pour établir un lien entre la pièce et sa monnaie rendue pour un achat. Ceci garantit que la monnaie peut être rendue sans compromettre la transparence des revenus et la vie privée des consommateurs. Le même mécanisme peut être utilisé pour des remboursements. Le protocole gère également les échecs de matériel ou de réseau en assurant que le paiement est définitivement effectué ou définitivement annulé et que toutes les parties ont une preuve cryptographique du résultat. Ceci correspond approximativement aux swaps atomiques des protocoles inter-registres ou *fair exchange* dans les systèmes de e-cash habituels.

La construction mathématique la plus commune pour un protocole d'échange de clé est la construction Diffie-Hellman 1976. Il permet aux deux parties de dériver une clé

[14] En Suisse par exemple, la Banque Nationale Suisse a commencé à retirer de la circulation sa huitième série de billets en avril 2016. Cette série avait été mise en circulation à la fin des années 90. Cependant, à compter du 1er janvier 2020, tous les billets à partir de la sixième série (émise en 1976) jusqu'aux futures séries, resteront indéfiniment valables et échangeable contre des billets de la série en cours.

partagée secrète. Pour cela, ils partagent deux paramètres du domaine p et g, qui peuvent être publics, où p est un grand nombre premier et g une racine primitive modulo p[15].

Maintenant, les deux parties choisissent leurs clés privées a et b, qui sont deux grands nombres entiers. Avec ces clés privées et les paramètres du domaine, ils génèrent leurs clés publiques respectives $A \equiv g^a \bmod p$ et $B \equiv g^b \bmod p$. Chaque partie peut maintenant utiliser sa propre clé privée et la clé publique de l'autre partie pour calculer la clé partagée $k \equiv (g^b)^a \equiv (g^a)^b \equiv g^{ab} \bmod p$[16].

Pour obtenir la monnaie, le client commence par la clé privée de la pièce c. Prenons C comme clé publique correspondante, à savoir: $C = g^c \bmod p$. Lorsque la pièce a précédemment été partiellement dépensée, la banque centrale a enregistré la transaction concernant C dans sa base de données. Pour simplifier, nous choisissons qu'il existe une valeur de pièce correspondant au montant résiduel. Dans le cas contraire, le protocole se relance jusqu'à ce que toute la monnaie soit rendue. Soit (e, n) comme clé de valeur pour la monnaie à rendre.

Pour obtenir la monnaie, l'acheteur crée d'abord κ clés de transfert privées t_i pour $i \in \{1, \ldots, \kappa\}$ et calcule les clés publiques correspondantes T_i. Ces κ clés de transfert sont simplement des paires de clés publiques-privées qui permettent au client de lancer le protocole d'échange en local – jouant les deux côtés du procédé – κ fois entre c et chaque t_i. Si Diffie-Hellman est le protocole d'échange de clé, alors $T_i \equiv g^{t_i} \bmod p$.

[15] Un nombre entier g est un racine primitive modulo p si pour tout entier a coprime à p, il y a un entier k pour lequel $g^k \equiv a \pmod p$. En pratique, g devrait être racine p-1^e primitive, aussi appelé un générateur, ce qui permet d'éviter les attaques de sous-groupes comme les attaques de Pohlig-Hellman (voir Lim et Pil 1997).

[16] Le même mécanisme pourrait être employé pour s'assurer que les pièces ne sont pas transférées à un tiers pendant la transaction. Pour ce faire, les utilisateurs doivent conserver une clé d'identité semi-permanente. Alors, le processus de retrait pourrait être construit de la même façon que celui que GNU-Taler utilise pour rendre la monnaie, à la différence que la clé d'identité semi-permanente du client serait utilisée plutôt que celle de la pièce pour effectuer le retrait sur le compte bancaire du client. Toutefois, une compromission de la sécurité de sa clé d'identification semi-permanente par le client remettrait en cause les protections de la vie privée et permettrait le vol de toutes les pièces du portefeuille. Compte tenu des limites au vol par des tiers lors du retrait des pièces, il n'est pas clair que cette réduction du risque serait un bon compromis.

Le résultat est κ clés de transfert $K_i \equiv KX(c, t_i)$. Le protocole d'échange de clé peut être utilisé de plusieurs façons pour obtenir la même valeur de $K_i \equiv KX(C, t_i) = KX(c, T_i)$. Soit K_i, le client utilise une fonction de hachage cryptographique *H* pour dériver les valeurs $(b_i, c_i) \equiv H(K_i)_{,,}$ où b_i est un facteur de masquage valable pour la clé de valeur (e, n) et c_i est une clé privée pour la nouvelle pièce obtenue comme monnaie résiduelle. c_i doit pouvoir être utilisée pour créer la signature cryptographique et servir à nouveau dans le protocole d'échange de clé pour pouvoir rendre la monnaie de la pièce.

Soit C_i la clé publique correspondant à c_i. Le client demande alors à la banque centrale de créer la signature aveugle sur C_i pour tout $i \in \{1, \dots, \kappa\}$[17]. Par cette requête, le client ajoute également aux clés publiques T_i. La requête est autorisée par une signature effectuée grâce à la clé privée *c*.

Au lieu de renvoyer directement la signature aveugle, la banque centrale demande d'abord au client la preuve que la construction ci-dessus a été correctement utilisée en donnant un $\gamma \in \{1, \dots, \kappa\}$. Le client doit alors montrer t_i pour tout $i \neq \gamma$ à la banque centrale. La banque centrale peut alors calculer $K_i \equiv KX(C, t_i)$ et dériver les valeurs (b_i, c_i). Si pour tout $i \neq \gamma$, les t_i fournis prouvent que le client a correctement utilisé la construction, la banque centrale renvoie la signature aveugle sur C_γ. Si le client ne renvoie pas une preuve correcte, la valeur résiduelle de la pièce est corrompue. Ceci punit effectivement ceux qui essayent d'échapper à la transparence des revenus avec un taux d'imposition estimé de $1 - \frac{1}{\kappa}$.

Pour empêcher un client de s'arranger avec un commerçant qui veut dissimuler des revenus, la banque centrale permet à toute personne qui connaît *C* d'obtenir, à tout moment, les valeurs de T_γ et la signature aveugle de toutes les pièces liées à la pièce d'origine *C*. Ceci permet au détenteur de la pièce d'origine – qui connait *c.*– de calculer $K_\gamma \equiv KX(c, T_\gamma)$ et, de là, de dériver (b_i, c_i) pour, enfin, retirer le masque de la signature aveugle. Par

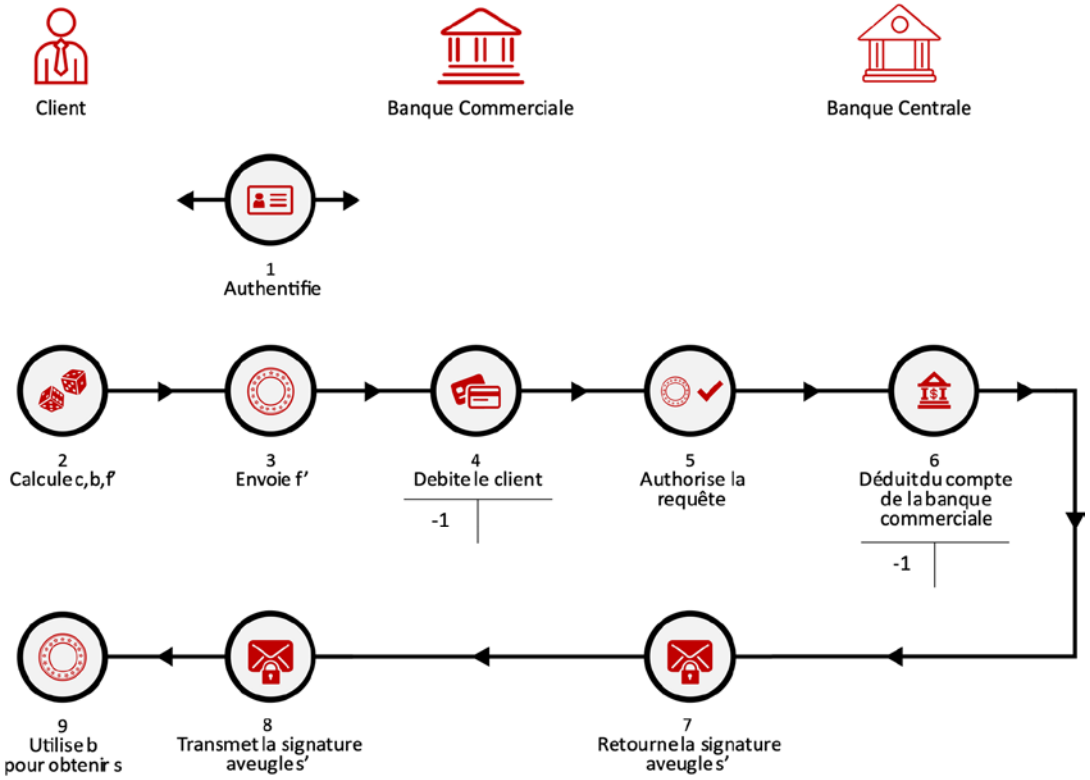
[17] Si les signatures aveugles étaient faites avec un chiffrement de type RSA, nous aurions $f \equiv FDH_n(C_i)$, où $FDH_n(\,)$ est le hachage de domaine complet sur *n*.

conséquent, un commerçant dissimulant ainsi ses revenus ne pourrait que former une entente économique limitée au lieu d'obtenir le contrôle exclusif.

B. Architecture du système

Un objectif clé de notre architecture est d'assurer que les banques centrales n'aient pas besoin d'interagir directement avec les payeurs (clients) ou de garder quelque information sur eux, mais seulement de maintenir une liste de pièces dépensées. L'authentification est déléguée aux banques commerciales qui ont déjà l'infrastructure nécessaire en place. Les protocoles de retraits et de dépôts parviennent aux banques centrales en passant par les banques commerciales. Du point de vue du client, le procédé est analogue au retrait d'espèces à un distributeur de billets. La transaction entre la banque commerciale d'un utilisateur et la banque centrale se fait en arrière-plan. Le procédé de retrait de MNBC est décrit dans le schéma 1.

Schéma 1: retrait de MNBC



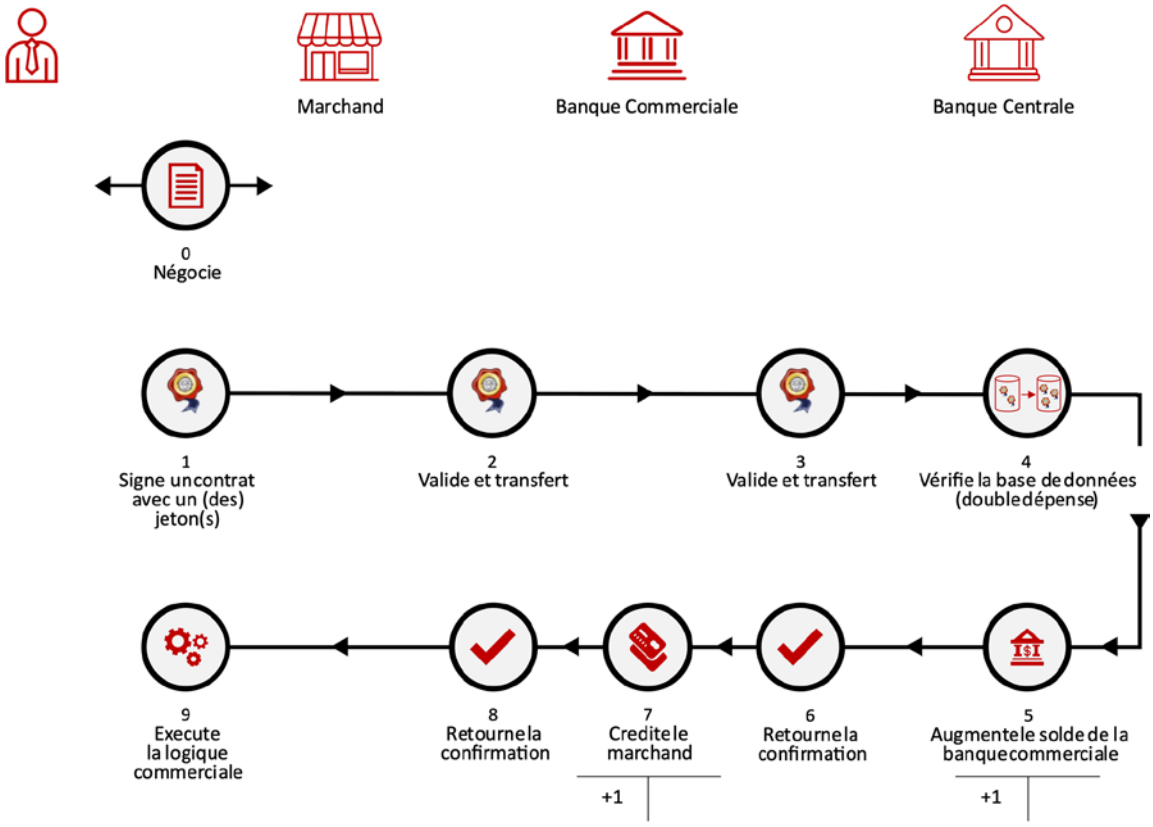
Un client (1) s'authentifie auprès de sa banque commerciale en utilisant les procédures d'authentification et d'autorisation de celle-ci. Ensuite, le smartphone (ou l'ordinateur) du client obtient la clé de valeur publique (*e, n*) fournie par la banque centrale pour cette valeur; il calcule ensuite (2) une paire de clés pour la pièce, avec une clé publique *c* et une clé privée *C*, et choisit un facteur de masquage *b*. La clé de la pièce est ensuite hachée. ($\rightarrow f$) et masquée ($\rightarrow f'$). Alors (3), l'appareil du client envoie *f'* avec une autorisation de retrait de la pièce et de débit du compte du client à la banque commerciale par un canal sécurisé. La banque commerciale débite alors (4) le montant du compte de dépôt de son client, puis (5) autorise la requête grâce à la signature propre à son groupe bancaire et transmet la requête et la pièce masquée à la banque centrale pour signature. La

banque centrale déduit (6) la valeur de la pièce du compte de banque centrale de la banque commerciale, signe en aveugle la pièce avec la clé de banque centrale pour la valeur concernée, et renvoie (7) la signature aveugle *s'* à la banque commerciale. La banque commerciale transmet (8) la signature aveugle *s'* au portefeuille électronique du client. Enfin, l'appareil du client (9) utilise *b* pour enlever le masque de la signature ($\rightarrow s$) et enregistre la pièce fraîchement «frappée» (c, s).

Pour dépenser les pièces, le procédé est analogue au paiement à un commerçant en espèces. Cependant, pour consolider la transaction, le commerçant doit déposer la pièce. Dépenser de la MNBC s'effectue comme décrit dans le schéma 2.

Un client et un commerçant négocient un contrat. Le client (1) utilise une pièce numérique pour signer le contrat de vente avec la clé privée de la pièce *c* et transmet la signature au commerçant. La signature d'une pièce sur un contrat avec une pièce valable est une instruction du client pour payer le commerçant identifié par le compte bancaire dans le contrat. Les clients peuvent signer un contrat avec plusieurs pièces si une pièce unique est insuffisante pour payer le montant total. Le commerçant valide alors (2) la signature de la pièce sur le contrat et la signature *s* de la banque centrale sur *f* qui correspondent à celle de la pièce *C* avec les clés publiques respectives et transmet la pièce signée (ainsi que les informations du compte du commerçant) à la banque commerciale du commerçant. La banque commerciale du commerçant confirme (3) que le commerçant est un de ses clients et transmet la pièce signée à la banque centrale. La banque centrale vérifie (4) les signatures et vérifie sa base de données pour s'assurer que la pièce n'a pas déjà été dépensée. Si tout est en ordre, la banque centrale ajoute (5) la pièce à la liste des pièces dépensées, crédite le compte de la banque commerciale à la banque centrale et envoie (6) à cet effet une confirmation à la banque commerciale. Ensuite, la banque commerciale crédite (7) le compte du commerçant et informe ce dernier. Le commerçant délivre (9) le produit au client. L'ensemble de l'opération prend quelques centaines de millisecondes.

Schéma 2: dépenser et déposer de la MNBC



C. Considérations de sécurité

Notre proposition nécessite que la banque centrale puisse mettre en œuvre des services et des bases de données à forte disponibilité. Seule des vérifications en ligne peuvent prévenir la double dépense, car des utilisateurs peuvent copier les pièces électroniques. Bien qu'il existe des solutions pour identifier à posteriori les utilisateurs qui font des doubles dépenses (voir Chaum et al. 1990), ces solutions créent un risque, autant pour les utilisateurs que pour la banque centrale, du fait des délais d'identification des transactions frauduleuses. La détection de doubles dépenses en ligne élimine ce risque mais rend donc les transactions impossibles si la connexion Internet de la banque centrale est indisponible.

La banque centrale devra également protéger la confidentialité des clés privées qu'elle utilise pour signer les pièces et les autres messages du protocole. Si les clés de signature de la banque centrale sont compromises par un ordinateur quantique, par une attaque physique sur les boucles des *data centers*, voire même par quelque algorithme imprévu, les utilisateurs peuvent en toute sécurité, sans lever la confidentialité, être remboursés de l'ensemble des pièces non dépensées. La banque centrale annoncerait alors une clé de révocation via l'interface de programmation applicative (API) qui serait détectée par les portefeuilles, entraînant alors le lancement du protocole de rafraîchissement suivant: l'utilisateur dévoile C la clé publique de la pièce ainsi que le facteur de masquage b à la banque centrale, ce qui permet à la banque centrale de vérifier le retrait légitime et ensuite de rembourser la valeur non dépensée de la pièce. Pour détecter la possible compromission de ses clés, la banque centrale peut surveiller les dépôts excédant les retraits dans ses bases de données.

D. Coûts et montée en charge

Le procédé proposé serait aussi efficace et économique que les systèmes modernes de RBTR couramment utilisés par les banques centrales.

La montée en charge concerne le coût de l'augmentation de la capacité de traitement effectuée afin que le nombre croissant de transactions puisse être finalisé dans un temps adéquat. Le coût global du système peut être faible puisque la MNBC proposée ici est purement logicielle. Les pièces dépensées peuvent être stockées jusqu'à ce que la clé de valeur utilisée pour signer les pièces soit périmée, suivant par exemple un roulement annuel, ce qui garde la base de données limitée. La quantité de bande passante et de capacité de calcul nécessaires augmentent de façon égale pour chaque transaction supplémentaire, dépense ou dépôt, car les transactions sont par essence indépendantes les unes des autres. La puissance supplémentaire est facilement atteinte par l'ajout de matériel, pratique fréquemment appelée cloisonnement ou partitionnement. Grâce à ce que nous appellerons le hachage cohérent, les ajouts de matériel ne sont pas disruptifs. Tous les types de bases de données peuvent être utilisés.

Plus concrètement, la partie guichet de la banque centrale n'a besoin de conduire que quelques opérations de signature, et un simple processeur peut en exécuter quelques milliers par seconde (voir Bernstein et Lange 2020). Si un système unique est insuffisant, il est facile de déployer de nouveaux serveurs frontaux et d'orienter les diverses banques commerciales pour qu'elles ajustent les trajets de leurs requêtes à travers les fermes de serveurs, ou d'utiliser un équilibreur de charge pour distribuer les requêtes dans l'infrastructure de la banque centrale.

Les serveurs frontaux doivent communiquer avec une base de données pour effectuer les transactions et éviter les doubles dépenses. Un seul serveur de base de données moderne devrait pouvoir gérer des dizaines de milliers de transactions par seconde. Les opérations peuvent facilement être réparties sur plusieurs serveurs de base de données en assignant simplement à chaque serveur de base de données une plage de valeurs à gérer. Cette construction garantit que les transactions individuelles ne traversent jamais les partitions. Ainsi, les systèmes de back-end connaîtront également une montée en charge linéaire

suivant celle des ressources de calcul qui, commençant avec un serveur unique, ont déjà une solide base de départ.

Les serveurs frontaux doivent également communiquer avec les serveurs back-end grâce à une interconnexion. Ces interconnexions peuvent supporter un grand nombre de transactions par seconde. Une seule transaction est habituellement de 1 à 10 kilooctets. Les *data centers* d'aujourd'hui, échangeant des informations à 400 Gbit/s, peuvent supporter des millions de transactions par seconde.

Pour finir, le coût total du système est très économique. Le stockage sécurisé de 1 à 10 kilooctets par transaction pour de nombreuses années sera vraisemblablement le coût principal du système. Des expériences menées sur une précédente version de Taler en utilisant les tarifs d'Amazon Web Service ont établi un coût du système (stockage, bande passante et capacité de calcul) qui à l'échelle serait de 0,0001 dollar des Etats-Unis par transaction (pour les détails concernant les données, voir Dold 2019).

V. Considérations réglementaires et stratégiques

Dans la solution proposée, les banques centrales n'ont pas connaissance de l'identité des clients ou du montant total des transactions. Les banques centrales ne voient que lorsque les pièces électroniques sont libérées ou quand elles sont remboursées. Les banques commerciales continuent à fournir l'authentification des clients et commerçants, restant donc les gardiennes de la connaissance client (KYC). Les banques commerciales ont vue sur les fonds que les commerçants peuvent recevoir et peuvent si besoin limiter les montants de MNBC que les commerçants peuvent recevoir par transaction. De plus, les transactions sont associées à leurs contrats client. Cela crée une transparence des revenus qui permet au système d'être compatible avec les dispositifs réglementaires de lutte contre le blanchiment et le financement du terrorisme (AML et CFT). Si des anomalies apparaissent dans les revenus des commerçants, la banque commerciale et les autorités fiscales ou judiciaires peuvent obtenir et inspecter les contrats liés aux paiements suspects afin de vérifier leur légitimité ou mettre à jour leur irrégularité. La transparence des

encaissements est aussi un dispositif fort de lutte contre l'évasion fiscale, puisque les commerçants ne peuvent pas sous-déclarer leurs revenus ou les soustraire au fisc. Globalement, le système intègre les principes de confidentialité par conception et par défaut (comme par exemple requis par le RGPD de l'UE). Les commerçants n'apprennent pas nécessairement l'identité de leurs clients, les banques commerciales n'ont que les informations nécessaires sur les activités de leurs clients, et les banques centrales n'ont pas accès aux détails des activités de leurs citoyens.

Dans certains pays, il existe des plafonds réglementaires pour les retraits ou les paiements en espèces. De telles restrictions pourront être intégrées dans l'architecture proposée. Les clients pourraient par exemple être limités dans les sommes qu'ils peuvent retirer par jour, ou bien la totalité des sommes de MNBC convertibles par les banques commerciales pourraient être plafonnées.

La désintermédiation du secteur bancaire est l'un des risques d'instabilité financière souvent soulevés quant à la MNBC de détail. Cette dernière pourrait notamment faciliter l'accumulation de grandes quantités de monnaie de banque centrale, ce qui pourrait avoir un impact très négatif sur le financement des banques commerciales par les dépôts, notamment parce que le public détiendrait moins d'argent en dépôts bancaires. Pour les pays dont la monnaie est une valeur refuge, cela pourrait de plus entraîner de fortes augmentations d'apport de capitaux dans les périodes de repli donnant lieu à des pressions sur les taux de change. Ce qui serait donc un vrai problème avec une MNBC basée sur des comptes devrait l'être beaucoup moins avec une MNBC par jetons. Premièrement, la thésaurisation de MNBC en jetons comprend des risques de vol ou de perte similaires aux risques entourant la thésaurisation d'espèces. Détenir quelques centaines de dollars sur un smartphone est probablement un risque acceptable pour beaucoup, y détenir des sommes bien plus importantes constitue vraisemblablement un risque beaucoup moins acceptable. Ainsi, nous ne nous nous attendons pas à une augmentation sensible du volume de thésaurisation d'espèces physiques.

Cependant, l'accumulation ou la conversion massive de dépôts bancaires en MNBC deviendrait-elle préoccupante que la banque centrale aurait plusieurs moyens pour réagir.

Comme exposé, l'architecture proposée contient une date de péremption des clés de signature, ce qui implique qu'à une date donnée les pièces signées par ces clés ne sont plus valables. Quand une clé de valeur expire, les clients doivent changer leurs pièces signées avec ces clés caduques contre de nouvelles pièces; le régulateur peut imposer une limite de conversion par client pour créer une limite franche de la quantité de MNBC qu'un individu peut accumuler. De plus, les banques centrales pourraient si nécessaire faire payer des frais. Des frais de rafraîchissement lorsque les pièces vont expirer signifieraient concrètement des taux d'intérêt négatifs sur la MNBC permettant de limiter son attrait en tant que réserve de valeur, comme le suggère Bindseil (2020). Ce serait dans les faits une application directe de l'idée de Silvio Gesell d'une taxe au porteur sur la monnaie, notoirement défendue par Keynes (1936) et reprise par Goodfriend (2000), Buiter et Panigirtzolou (2003), ainsi que par Agarwall et Kimball (2019).

Quant aux implications en termes de politique monétaire, il ne devrait pas y avoir de changement réel puisque notre MNBC est conçue pour répliquer les espèces plutôt que les dépôts bancaires. L'émission, le retrait et le dépôt de notre MNBC correspondent exactement à ceux des billets de banque. Il est possible que la vitesse de circulation d'une MNBC de détail puisse être différente de celle des espèces physiques, mais cela ne devrait pas être un problème significatif pour la politique monétaire.

VI. Travaux liés

Comme noté plus haut, la MNBC proposée dans ce document est basée sur eCash et GNUTaler[18]. Depuis la proposition originelle d'eCash de Chaum, la recherche s'est penchée sur trois problèmes principaux. Premièrement, dans la proposition de Chaum, les pièces avaient une valeur fixe et ne pouvaient qu'être entièrement dépensées. Le paiement de sommes importantes en centimes aurait été inefficace. Okamoto (1995), Camenisch

[18] La mise en œuvre de eCash par la société DigiCash dans les années 90 est documentée dans https://www.chaum.com/ecash.

(2005), Canard et Gouget (2007) et Dold (2019) ont par la suite inventé des façons de traiter ce problème. Ces solutions contiennent des protocoles permettant de rendre la monnaie, ou de faire en sorte que les pièces soient divisibles.

Le deuxième problème concerne les échecs de transactions dus par exemple aux coupures de réseau. Dans ce cas, le système doit faire en sorte que les fonds restent en possession du consommateur sans affecter la confidentialité. Les e-cash endossés proposés par Camenisch et al. (2007) et Dold (2019) s'attaquent tous deux à ce problème. Plusieurs de ces solutions lèvent les garanties de protection de la vie privée des consommateurs, et toutes sauf Taler violent les conditions d'une transparence des revenus.

Le troisième problème principal, souvent négligé, est en effet la transparence des revenus et donc les conformités AML et KYC. Fuchsbauer et al. (2009) ont délibérément conçu leur système de désintermédiation pour fournir une sémantique plus proche des espèces physiques. Cependant, la désintermédiation totale est assez difficilement cohérente avec la règlementation en matière de lutte contre le blanchiment et contre le financement du terrorisme, puisqu'il devient impossible d'atteindre le niveau de responsabilité requis. Un exemple d'une telle conception est celle de ZCash, un registre distribué qui cache le payeur, le receveur et le montant de la transaction. Seul Taler offre tout à la fois: une protection constante de la vie privée et de la transparence des revenus tout en fournissant un rendu de monnaie efficace, des swaps atomiques (voir Camenisch 2007) ainsi que la possibilité de récupérer les portefeuilles à partir d'une sauvegarde.

Sur les systèmes de paiement pour MNBC, Danezis et Meiklejohn (2016) ont conçu un registre extensible pour RSCoin. C'est globalement un système de RBTR sécurisé avec la même cryptographie que Bitcoin. Comme Taler, ce concept utilise l'éclatement de base données pour permettre une extensibilité linéaire. Cependant, la conception de Danezis et Meiklejohn n'inclut aucune protection de la vie privée et manque d'éléments pour la mise en œuvre pratique de la solution avec les procédés et systèmes bancaires existants.

L'EUROchain de la Banque Centrale Européenne (voir ECB 2019) est un autre prototype de MNBC avec un registre distribué. Semblable à la conception proposée dans le présent document, EUROchain utilise une architecture à deux niveaux avec les banques

commerciales comme intermédiaires. Avec une différence fondamentale dans la façon dont le système combine confidentialité et conformité AML. Si dans notre conception, le régulateur peut imposer un montant limite d'espèces électroniques qu'un détenteur de compte bancaire peut retirer sur une période donnée, EUROchain émet un nombre limité de «coupons d'anonymat» qui permettent un nombre limité de transactions sans vérifications AML. Comme ces coupons semblent totalement dépourvu de tout symbole de valeur, le moyen d'éviter un marché noir de «coupons d'anonymat» n'est pas clair. De plus, la notion d'anonymat d'EUROchain est très différente puisqu'elle permet tout juste d'éliminer certaines vérifications AML, mais maintient la capacité pour les banques commerciales de savoir comment leurs clients dépensent leurs espèces numériques. Là où les payeurs de Taler interagissent avec les commerçants pour dépenser leurs espèces électroniques, le système EUROchain demande aux payeurs d'ordonner à leur banque commerciale d'accéder à leur MNBC. Ainsi l'EUROchain n'émet pas directement de symboles de valeur aux consommateurs, mais compte sur les clients pour qu'ils s'authentifient auprès de leur banque commerciale afin d'accéder à la MNBC que la banque centrale détient en dépôt. Les bénéfices de l'EUROchain en termes de confidentialité, de performance ou de sécurité par rapport à la monnaie de dépôt actuelle ne sont donc pas évidents.

VII. Conclusion

Avec l'émergence du Bitcoin et des monnaies numériques récemment proposées par les géants de la tech (comme le Diem, anciennement Libra), les banques centrales font face à une concurrence accrue des acteurs privés proposant leur propre solution numérique en vue de contourner les espèces. Les décisions de banques centrales d'émettre ou non une MNBC dépendent de leur évaluation des bénéfices et des risques d'une MNBC. Ces risques et bénéfices, tout comme le cadre juridique qui définira le champ de la MNBC, sont susceptibles de changer d'un pays à l'autre.

Si une banque centrale décide d'émettre une MNBC de détail, nous proposons une MNBC par jeton qui combine la confidentialité des transactions avec la connaissance client

(KYC) et la conformité AML/CFT. Une telle MNBC ne concurrencerait pas les dépôts bancaires mais imiterait plutôt les espèces physiques, limitant ainsi les risques d'instabilité financière et de perturbation de la politique monétaire.

Nous avons montré que la conception proposée ici serait aussi efficace et économique que les systèmes de RBTR mis en œuvre par les banques centrales. Les paiements électroniques avec MNBC ne nécessiteraient que de simples transactions de base de données sur des quantités infimes de bande passante. L'efficacité et l'économie de cette solution, de même que la facilité d'utilisation induite par le passage de l'identification à l'autorisation, en font probablement la première solution qui atteint l'objectif de longue date de permettre les micro-paiements en ligne. De plus, l'utilisation de pièces pour signer cryptographiquement des contrats permet également l'emploi de contrats intelligents. Cela pourrait entrainer l'émergence de nouvelles applications pour les systèmes de paiement. Bien que la solution ne soit pas basée sur une technologie de registres distribués, elle peut facilement intégrer cette dernière si cela était requis par les infrastructures du marché financier.

Dernier point, et non des moindres: une MNBC de détail doit rester, tout comme les espèces physiques, un bien commun respectueux de la vie privée, sous le contrôle individuel des citoyens. L'architecture proposée dans la présente étude remplit cette exigence, et permet aussi aux banques centrales d'éviter de sérieuses remises en cause de leur politique monétaire ou de la stabilité financière susceptibles d'être entrainées par la numérisation.

RÉFÉRENCES

Adrian, Tobias et Tommaso Mancini-Griffoli (2019), «The Rise of Digital Money», IMF Fintech Note 19/01.

Agarwal, Ruchir et Miles S. Kimball (2019), «Enabling Deep Negative Rates to Fight Recessions: A Guide», IMF Working Paper 19/84.

Agur, Itai, Anil Ari et Giovanni Dell'Ariccia (2019), «Designing Central Bank Digital Currencies», IMF Working Paper 19/252.

Allen, Sarah, Srđjan Čapkun, Ittay Eyal, Giulia Fanti, Bryan A. Ford, James Grimmelmann, Ari Juels, Kari Kostiainen, Sarah Meiklejohn, Andrew Miller, Eswar Prasad, Karl Wüst et Fan Zhang (2020), «Design Choices for Central Bank Digital Currency: Policy and Technical Considerations», NBER Working Paper nº 27634.

Alves, Tiago et Don Felton, 2004, «TrustZone: Integrated hardware and software security», *ARM IQ*, vol. 3, nº 4, pp 18-24.

Auer, Raphael et Rainer Böhme (2020), «The technology of retail central bank digital currency», *BIS Quarterly Review*, mars 2020, pp 85-96.

Auer, Raphael, Giulio Cornelli et Jon Frost (2020). «Taking stock: ongoing retail CBDC projects», *BIS Quarterly Review*, mars 2020, pp 97-98.

Bank for International Settlements (2018), «Central Bank Digital Currencies», Joint Report of the Committee on Payments and Market Infrastructures and Markets Committee.

Bank of England (2020), «Central Bank Digital Currency: Opportunities, Challenges and Design» Discussion Paper, mars.

Baiocchi, Giovanni et Walter Distaso (2003), «GRETL: Econometric Software for the GNU Generation», *Journal of Applied Econometrics*, vol. 18, pp 105-110.

Bech, Morten et Rodney Garratt (2017), «Central bank cryptocurrencies», *BIS Quarterly Review*, septembre, pp 55-70.

Berentsen, Aleksander et Fabian Schär (2018), «The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies», *Federal Reserve Bank of St. Louis Review*, vol. 100, nº 2, pp 97-106.

Bernstein, Daniel J. et Tanja Lange (2020), «eBACS: ECRYPT Benchmarking of Cryptographic Systems», https://bench.cr.yp.to, consulté le 17 mars 2020.

Bernstein, Daniel J., Niels Duif, Tanja Lange, Peter Schwabe et Bo-Yin Yang (2012),

«High-speed high-security signatures», *Journal of Cryptographic Engineering*, vol. 2, pp 77-89.

Bindseil, Ulrich (2020), «Tiered CBDC and the financial system», ECB Working Paper 2351, janvier.

Boar, Codruta, Henry Holden et Amber Wadsworth (2020), «Impending arrival – a sequel to the survey on central bank digital currency», BIS Papers, nº 107.

Boneh, Dan (1999), «Twenty Years of Attacks on the RSA Cryptosystem», *Notices of the AMS*, vol. 42, nº 2, pp 202-213.

Bordo, Michael D. et Andrew T. Levin (2017), «Central bank digital currency and the future of monetary policy», NBER Working Papers, nº 23711.

Brunnermeier, Markus et Dirk Niepelt (2019), «On the Equivalence of Private and Public Money», Journal of Monetary Economics, vol. 106, pp 27-41.

Buiter, Willem H. et Nikolaos Panigirtzoglou (2003), «Overcoming the Zero Bound on Nominal Interest Rates with Negative Interest on Currency: Gesell's Solution», *The Economic Journal*, vol. 113, nº 490, pp 723-746.

Bullmann, Dirk, Jonas Klemm et Andrea Pinna (2019), «In search for stability in crypto-assets: are *stablecoins* the solution?», ECB Occasional Paper Series, nº 230.

Camenisch, J., Aanna Lysyanskaya, et Mira Meyerovich (2007), «Endorsed E-Cash», dans *2007 IEEE Symposium on Security and Privacy (SP '07)*, mai, pp 101-115.

Camenisch, Jan, Susan Hohenberger et Anna Lysyanskaya (2005), «Compact E-Cash», dans Ronald Cramer (éd.), *Advances in Cryptology – EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Aarhus, Danemark, 22-26 mai, Berlin, Heidelberg: Springer.

Canard, Sébastien et Aline Gouget (2007), «Divisible e-cash systems can be truly anonymous», *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp 482-97.

CCC (2017), «Chaos Computer Club hacks e-motor charging stations», 34c3.

Chapman, James, Rodney Garratt, Scott Hendry, Andrew McCormack et Wade McMahon (2017), «Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet?», Banque du Canada, *Financial System Review*, juin, pp 59-69.

Chaum, David (1983), «Blind signatures for untraceable payments», *Advances in Cryptology: Proceedings of Crypto '82*, vol. 82, nº 3, pp 199-203.

Chaum, David, Amos Fiat et Moni Naor (1990), «Untraceable electronic cash» *Advances in Cryptology: Proceedings of CRYPTO '88*, pp 319-327.

Danezis, George et Sarah Meiklejohn (2016), «Centrally Banked Cryptocurrencies», dans *23nd Annual Network and Distributed System Security Symposium*, NDSS2016, San Diego, Californie, Etats-Unis, 21-24 février, The Internet Society.

Diffie, Whitfield et Martin Hellmann (1976), «New Directions in Cryptography», *IEEE Trans. on Inf. Theory*, IT-22, pp 644-654.

Dold, Florian (2019), *The GNU Taler System: Practical and Provably Secure Electronic Payments*, thèse, Université de Rennes 1.

European Central Bank (2019), «Exploring anonymity in central bank digital currencies» *In Focus*, nº 4, décembre.

Fuchsbauer, Georg, David Pointcheval et Damien Vergnaud (2009), «Transferable constant-size fair e-cash», dans *International Conference on Cryptology and Network Security*, Springer, pp 226-47.

Garcia, Flavio, Gerhard de Koning Gans, Ruben Muijrers, Peter van Rossum, Roel Verdult, Ronny Wichers Schreur et Bart Jacobs (2008), «Dismantling MIFARE Classic», *European Symposium on Research in Computer Security*.

Garratt, Rod, Michael Lee, Brendan Malone et Antoine Martin (2020), «Token- or Account-Based? A Digital Currency Can Be Both», *Liberty Street Economics*, Federal Reserve Bank of New York, 12 août 2020.

Goodfriend, Marvin (2000), «Overcoming the Zero Bound on Interest Rate Policy», *Journal of Money, Credit, and Banking*, vol. 32, nº 4, 1007-35.

Johnston, Casey (2010), «PS3 hacked through poor cryptography implementation», *Ars Technica*, 30 décembre.

Jordan, Thomas J (2019), «Monnaie et jetons numériques», exposé donné au 30e anniversaire du Centre de sciences économiques et de l'Association des économistes bâlois, Université de Bâle, septembre. Disponible sous: www.snb.ch/fr/mmr/speeches/id/ref_20190905_tjn/source/ref_20190905_tjn.fr.pdf

Kahn, Charles M. et William Roberds (2009), «Why Pay? An Introduction to Payments Economics», *Journal of Financial Intermediation*, nº 18, pp 1-23.

Kahn, Charles M., James McAndrews et William Roberds (2005) «Money is Privacy» *International Economic Review*, vol. 46, nº 2, pp 377-399.

Kasper, Timo, Michael Silbermann et Christof Paar (2010), «All you can eat or breaking a real-world contactless payment system», *Financial Cryptography and Data Security, Lecture Notes in Computer Science*, vol. 6052, pp 343-50.

Katzenbeisser, Stefan, Ünal Kocabaş, Vladimir Rožić, Ahmad-Reza Sadeghi, Ingrid Verbauwhede et Christian Wachsmann (2012), «PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonable Functions (PUFs) Cast in Silicon», *Cryptographic Hardware and Embedded Systems – CHES 2012, Lecture Notes in Computer Science*, vol. 7428, pp 283-301.

Keynes, John Maynard (1936), *The General Theory of Employment, Interest and Money*, Londres, Macmillan.

Kiff, John, Jihad Alwazir, Sonja Davidovic, Aquiles Farias, Ashraf Khan, Tanai Khiaonarong, Majid Malaika, Hunter Monroe, Nobu Sugimoto, Hervé Tourpe et Peter Zhou (2020), «A Survey of Research on Retail Central Bank Digital Currency», IMF Working Paper 20/104.

Kumhof, Michael et Clare Noone (2018), «Central bank digital currencies – design principles and balance sheet implications», Bank of England, Staff Working Paper nº 725.

Lapid, Ben, et Avishai Wool (2018), «Cache-Attacks on the ARM TrustZone Implementations of AES-256 and AES-256-GCM via GPU-Based Analysis», International Conference on Selected Areas in Cryptography, *Lecture Notes in Computer Science*, vol. 11349.

Lerner, Josh et Jean Tirole (2005), «The Scope of Open Source Licensing», *Journal of Law, Economics & Organization*, vol. 21, pp 20-56.

Libra Association (2020), *Libra White Paper v2.0*, https://libra.org/en-US/white-paper/

Lim, Chae Hoon et Phil Joong Lee (1997) «A key recovery attack on discrete log-based schemes using a prime order subgroup», CRYPTO 1997, *Lecture Notes in Computer Science*, vol. 1294.

Lyons, Richard K. et Ganesh Viswanath-Natraj (2020), «What Keeps Stablecoins Stable?" NBER Working Paper nº 27136, mai.

Mancini-Griffoli, Tommaso, Maria Soledad Martinez Peria, Itai Agur, Anil Ari, John Kiff, Adina Popescu, et Céline Rochon (2018), «Casting Light on Central Bank Digital Currency», IMF Staff Discussion Notes 18/08, International Monetary Fund.

Nakamoto, Satoshi (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*

https://www.bitcoin.com/bitcoin.pdf

Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder (2016), *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton: Princeton University Press.

Niepelt, Dirk (2020), *Digital money and central bank digital currency: An executive summary for policymakers*, VOX/CEPR. https://voxeu.org/article/digital-money-and-central-bank-digital-currency-executive-summary.

Okamoto, Tatsuaki (1995) «An Efficient Divisible Electronic Cash Scheme», dans *Advances in Cryptology — CRYPT0'95: 15th Annual International Cryptology Conference* Santa Barbara, Californie, Etats-Unis, 27-31 août 1995, actes édités par Don Coppersmith, Berlin, Heidelberg: Springer, pp 438-451.

Pinto, S. et N. Santos (2019), «Demystifying Arm Trust Zone: A Comprehensive Survey» ACM Computing Surveys, article nº 130, janvier.

Rivest, Ronald L., Adi Shamir et Leonard Adleman (1978), «A Method for Obtaining Digital Signatures and Public Key Cryptosystems", *Comm. ACM*, vol. 21, nº 2.

Solove, Daniel J. (2011), *Nothing to Hide: The false tradeoff between privacy and security*, New Haven & London: Yale University Press.

Soukup, Michael et Bruno Muff (2007), «Die Postcard lässt sich fälschen» *Sonntagszeitung*, 22 avril.

Stallman, Richard (1985), «The GNU manifesto», *Dr. Dobb's Journal of Software Tools* 10(3), pp 30-35.

Sveriges Riksbank (2020), *The Riksbank's e-krona project*, février, https://www.riksbank.se/globalassets/media/rapporter/e-krona/2019/the-riksbanks-e-krona-pilot.pdf

Wojtczuk, Rafal et Joanna Rutkowska (2009), «Attacking Intel Trusted Execution Technology», BlackHat-DC 2009.

Yalta, A. Talha et A. Yasemin Yalta (2010), «Should Economists Use Open Source Software for Doing Research?», *Computational Economics*, vol. 35, pp 371-94.

Yalta, A. Talha et Riccardo Lucchetti (2008), «The GNU/Linux Platform and Freedom Respecting Software for Economists», *Journal of Applied Econometrics*, vol. 23, pp 279-86.

Working Papers récents

2021-03 David Chaum, Christian Grothoff, Thomas Moser:
How to issue a central bank digital currency

2021-02 Jens H.E. Christensen, Nikola Mirkov:
The safety premium of safe assets

2021-01 Till Ebner, Thomas Nellen, Jörn Tenhofen:
The rise of digital watchers

2020-25 Lucas Marc Fuhrer, Marc-Antoine Ramelet, Jörn Tenhofen:
Firms' participation in the COVID-19 loan programme

2020-24 Basil Guggenheim, Sébastien Kraenzlin, Christoph Meyer:
(In)Efficiencies of current financial market infrastructures – a call for DLT?

2020-23 Miriam Koomen, Laurence Wicht:
Demographics, pension systems, and the current account: an empirical assessment using the IMF current account model

2020-22 Yannic Stucki, Jacqueline Thomet:
A neoclassical perspective on Switzerland's 1990s stagnation

2020-21 Fabian Fink, Lukas Frei, Oliver Gloede:
Short-term determinants of bilateral exchange rates: A decomposition model for the Swiss franc

2020-20 Laurence Wicht:
A multi-sector analysis of Switzerland's gains from trade

2020-19 Terhi Jokipii, Reto Nyffeler, Stéphane Riederer:
Exploring BIS credit-to-GDP gap critiques: the Swiss case

2020-18 Enzo Rossi, Vincent Wolff:
Spillovers to exchange rates from monetary and macroeconomic communications events

2020-17 In Do Hwang, Thomas Lustenberger, Enzo Rossi:
Does communication influence executives' opinion of central bank policy?

2020-16 Peter Kugler, Samuel Reynard:
Money, inflation and the financial crisis: the case of Switzerland

2020-15 Sébastien Kraenzlin, Christoph Meyer, Thomas Nellen:
COVID-19 and regional shifts in Swiss retail payments

2020-14 Christian Grisse:
Lower bound uncertainty and long-term interest rates

2020-13 Angela Abbate, Sandra Eickmeier, Esteban Prieto:
Financial shocks and inflation dynamics

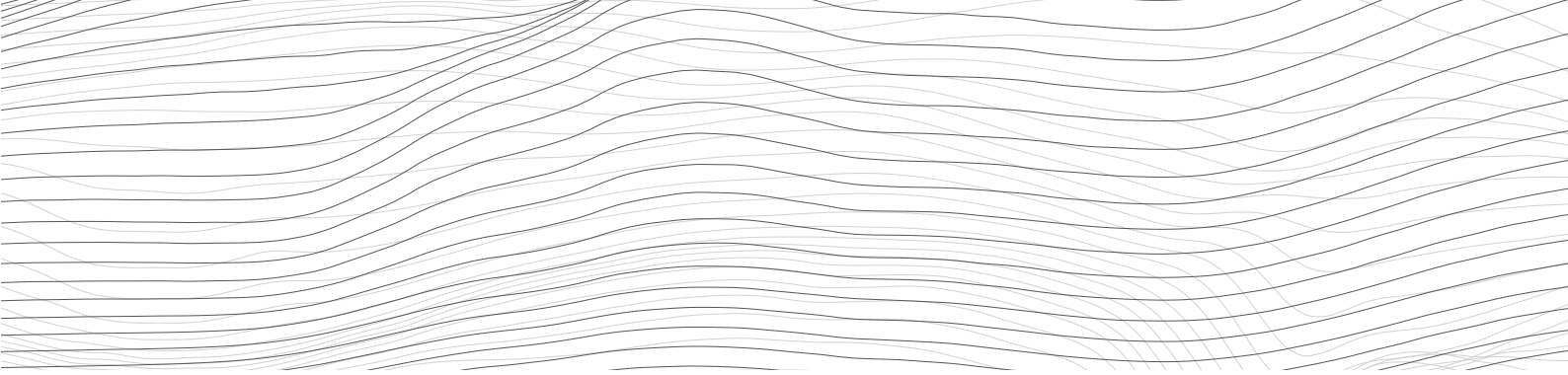
2020-12 Toni Beutler, Matthias Gubler, Simona Hauri, Sylvia Kaufmann:
Bank lending in Switzerland: Capturing cross-sectional heterogeneity and asymmetry over time

2020-11 Sophie Altermatt, Simon Beyeler:
Shall we twist?

2020-10 Tim D. Maurer, Thomas Nitschka:
Stock market evidence on the international transmission channels of US monetary policy surprises

2020-9 Romain Baeriswyl, Kene Boun My, Camille Cornand:
Double overreaction in beauty contests with information acquisition: theory and experiment

2020-8 Albi Tola, Miriam Koomen, Amalia Repele:
Deviations from covered interest rate parity and capital outflows: The case of Switzerland



SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIUNALA SVIZRA
SWISS NATIONAL BANK