SENATE SÉNAT

CANADA

Second Session
Forty-first Parliament, 2013-14

Deuxième session de la
quarante et unième législature, 2013-2014

Proceedings of the Standing Senate Committee on

BANKING, TRADE AND COMMERCE

Chair:
The Honourable IRVING GERSTEIN

Wednesday, April 2, 2014
Thursday, April 3, 2014

Issue No. 7

Third and fourth meetings on:

The use of digital currency

WITNESSES:
(*See back cover*)

Délibérations du Comité sénatorial permanent des

BANQUES ET DU COMMERCE

Président :
L'honorable IRVING GERSTEIN

Le mercredi 2 avril 2014
Le jeudi 3 avril 2014

Fascicule n° 7

Troisième et quatrième réunions concernant :

L'utilisation de la monnaie numérique

TÉMOINS :
(*Voir à l'endos*)

51302-51307

STANDING SENATE COMMITTEE ON
BANKING, TRADE AND COMMERCE

The Honourable Irving Gerstein, *Chair*

The Honourable Céline Hervieux-Payette, P.C., *Deputy Chair*

and

The Honourable Senators:

Bellemare	Greene
Black	Maltais
Campbell	Massicotte
* Carignan, P.C. (or Martin)	Ngo
	Ringuette
* Cowan (or Fraser)	Rivard
	Tkachuk

* Ex officio members

(Quorum 4)

Changes in membership of the committee:

Pursuant to rule 12-5, membership of the committee was amended as follows:

The Honourable Senator Tkachuk replaced the Honourable Senator MacDonald (*April 2, 2014*).

The Honourable Senator MacDonald replaced the Honourable Senator Tkachuk (*April 1, 2014*).

COMITÉ SÉNATORIAL PERMANENT DES
BANQUES ET DU COMMERCE

Président : L'honorable Irving Gerstein

Vice-présidente : L'honorable Céline Hervieux-Payette, C.P.

et

Les honorables sénateurs :

Bellemare	Greene
Black	Maltais
Campbell	Massicotte
* Carignan, C.P. (ou Martin)	Ngo
	Ringuette
* Cowan (ou Fraser)	Rivard
	Tkachuk

* Membres d'office

(Quorum 4)

Modifications de la composition du comité :

Conformément à l'article 12-5 du Règlement, la liste des membres du comité est modifiée, ainsi qu'il suit :

L'honorable sénateur Tkachuk a remplacé l'honorable sénateur MacDonald (*le 2 avril 2014*).

L'honorable sénateur MacDonald a remplacé l'honorable sénateur Tkachuk (*le 1er avril 2014*).

Published by the Senate of Canada
Available on the Internet: http://www.parl.gc.ca

Publié par le Sénat du Canada
Disponible sur internet: http://www.parl.gc.ca

MINUTES OF PROCEEDINGS

OTTAWA, Wednesday, April 2, 2014
(18)

[*English*]

The Standing Senate Committee on Banking, Trade and Commerce met this day, at 4:55 p.m., in room 9, Victoria Building, the chair, the Honourable Irving Gerstein, presiding.

Members of the committee present: The Honourable Senators Bellemare, Black, Campbell, Gerstein, Greene, Hervieux-Payette, P.C., MacDonald, Maltais, Massicotte, Ngo, Rivard and Tkachuk (12).

In attendance: Adriane Yong and Brett Stuckey, Analysts, Parliamentary Information and Research Service, Library of Parliament.

Also present: The official reporters of the Senate.

Pursuant to the order of reference adopted by the Senate on Tuesday, March 25, 2014, the committee continued its examination on the use of digital currency. (*For complete text of the order of reference, see proceedings of the committee, Issue No. 6.*)

WITNESSES:

Bank of Canada:

Grahame Johnson, Chief, Funds Management and Banking;

Lukasz Pomorski, Assistant Director, Funds Management and Banking.

The chair made an opening statement.

Mr. Johnson and Mr. Pomorski each made a statement and answered questions.

At 5:28 p.m., the Honourable Senator Tkachuk replaced the Honourable Senator MacDonald as a member of the committee.

At 6:13 p.m., the committee suspended.

At 6:15 p.m., pursuant to rule 12-16(1)(d), the committee proceeded in camera to consider a draft agenda (future business).

It was agreed that senators' staff be permitted to remain in the room provided they not use their blackberries, cellular phones or other electronic devices.

PROCÈS-VERBAUX

OTTAWA, le mercredi 2 avril 2014
(18)

[*Traduction*]

Le Comité sénatorial permanent des banques et du commerce se réunit aujourd'hui, à 16 h 55, dans la salle 9 de l'édifice Victoria, sous la présidence de l'honorable Irving Gerstein (*président*).

Membres du comité présents : Les honorables sénateurs Bellemare, Black, Campbell, Gerstein, Greene, Hervieux-Payette, C.P., MacDonald, Maltais, Massicotte, Ngo, Rivard et Tkachuk (12).

Également présents : Adriane Yong et Brett Stuckey, analystes, Service d'information et de recherche parlementaires, Bibliothèque du Parlement.

Aussi présents : Les sténographes officiels du Sénat.

Conformément à l'ordre de renvoi adopté par le Sénat le mardi 25 mars 2014, le comité poursuit son étude sur l'utilisation de la monnaie numérique. (*Le texte intégral de l'ordre de renvoi figure au fascicule nº 6 des délibérations du comité.*)

TÉMOINS :

Banque du Canada :

Grahame Johnson, chef, Gestion financière et Opérations bancaires;

Lukasz Pomorski, directeur adjoint, Gestion financière et Opérations bancaires.

Le président ouvre la séance.

MM. Johnson et Pomorski font chacun une déclaration, puis répondent aux questions.

À 17 h 28, l'honorable sénateur Tkachuk remplace l'honorable sénateur MacDonald au sein du comité.

À 18 h 13, la séance est suspendue.

À 18 h 15, conformément à l'article 12-16(1)d) du Règlement, la séance se poursuit à huis clos afin que le comité puisse examiner un projet d'ordre du jour (travaux futurs).

Il est convenu que le personnel des sénateurs soit autorisé à demeurer dans la pièce à condition de ne pas utiliser d'appareils BlackBerry, de téléphones cellulaires ou d'autres appareils électroniques.

At 6:20 p.m., the committee adjourned to the call of the chair.

ATTEST:

À 18 h 20, le comité s'ajourne jusqu'à nouvelle convocation de la présidence.

ATTESTÉ :

La greffière du comité,

Barbara Reynolds

Clerk of the Committee

OTTAWA, Thursday, April 3, 2014
(19)

[*English*]

The Standing Senate Committee on Banking, Trade and Commerce met this day, at 10:31 a.m., in room 9, Victoria Building, the deputy chair, the Honourable Céline Hervieux-Payette, P.C., presiding.

Members of the committee present: The Honourable Senators Bellemare, Black, Campbell, Gerstein, Greene, Hervieux-Payette, P.C., Maltais, Massicotte, Ngo, Rivard and Tkachuk (11).

In attendance: Adriane Yong and Brett Stuckey, Analysts, Parliamentary Information and Research Service, Library of Parliament.

Also present: The official reporters of the Senate.

Pursuant to the order of reference adopted by the Senate on Tuesday, March 25, 2014, the committee continued its examination on the use of digital currency. (*For complete text of the order of reference, see proceedings of the committee, Issue No. 6.*)

WITNESSES:

As individuals:

Jeremy Clark, Assistant Professor, Concordia Institute for Information Systems Engineering, Concordia University;

David Descôteaux, Associate Researcher, Montreal Economic Institute (by video conference).

The deputy chair made an opening statement.

Mr. Clark made a statement and answered questions.

At 11:28 a.m., the committee suspended.

At 11:34 a.m., the committee resumed, the chair, the Honourable Senator Gerstein, presiding.

Mr. Descôteaux made a statement and answered questions.

OTTAWA, le jeudi 3 avril 2014
(19)

[*Traduction*]

Le Comité sénatorial permanent des banques et du commerce se réunit aujourd'hui, à 10 h 31, dans la salle 9 de l'édifice Victoria, sous la présidence de l'honorable Céline Hervieux-Payette, C.P. (*vice-présidente*).

Membres du comité présents : Les honorables sénateurs Bellemare, Black, Campbell, Gerstein, Greene, Hervieux-Payette, C.P., Maltais, Massicotte, Ngo, Rivard et Tkachuk (11).

Également présents : Adriane Yong et Brett Stuckey, analystes, Service d'information et de recherche parlementaires, Bibliothèque du Parlement.

Aussi présents : Les sténographes officiels du Sénat.

Conformément à l'ordre de renvoi adopté par le Sénat le mardi 25 mars 2014, le comité poursuit son étude sur l'utilisation de la monnaie numérique. (*Le texte intégral de l'ordre de renvoi figure au fascicule n^o^ 6 des délibérations du comité.*)

TÉMOINS :

À titre personnel :

Jeremy Clark, professeur adjoint, Institut d'ingénierie des systèmes d'information de Concordia, Université Concordia;

David Descôteaux, chercheur associé, Institut économique de Montréal (par vidéoconférence).

La vice-présidente ouvre la séance.

M. Clark fait un exposé, puis répond aux questions.

À 11 h 28, la séance est suspendue.

À 11 h 34, la séance reprend sous la présidence de l'honorable sénateur Gerstein (*président*).

M. Descôteaux fait un exposé, puis répond aux questions.

At 12:01 p.m., the committee adjourned to the call of the chair.

À 12 h 1, le comité s'ajourne jusqu'à nouvelle convocation de la présidence.

ATTEST:

ATTESTÉ :

La greffière du comité,

Danielle Labonté

Clerk of the Committee

EVIDENCE

OTTAWA, Wednesday, April 2, 2014

The Standing Senate Committee on Banking, Trade and Commerce met this day, at 4:55 p.m., to study the use of digital currency.

Senator Irving Gerstein (*Chair*) in the chair.

[*English*]

The Chair: I want to mention to the members that I would appreciate it if you would be good enough to remain for about five minutes in camera at the conclusion of the meeting.

Today the committee is holding its third meeting as part of its study on the use of digital currency. The committee began its study last Wednesday with an appearance by officials from the Department of Finance, followed on Thursday by two members of academia, both of whom have worked in the areas of private and digital currencies.

This afternoon the committee will be receiving a presentation from the Bank of Canada. We are pleased to welcome Grahame Johnson, Chief, Funds Management and Banking; and Lukasz Pomorski, Assistant Director, Funds Management and Banking.

Thank you both for being here today. We apologize for being a little late in getting starting.

My understanding, Mr. Johnson, is that you will start with an opening statement and Mr. Pomorski will follow with a technical briefing on digital currency.

Mr. Johnson, the floor is yours.

Grahame Johnson, Chief, Funds Management and Banking, Bank of Canada: Thank you, Mr. Chair. Both Lukasz and I would like to thank all the committee members for the invitation to speak today. It is a subject that we both find to be complex but fascinating. As you know, the bank was asked to provide you with a briefing on digital currencies and we are happy to be here today to do so.

In discussing digital currencies, it might be helpful to put them in the context of advances in the payment system more broadly. Given that, I'll start by providing an overview of recent innovations and developments in payment systems and the role of the Bank of Canada. Then my colleague, Lukasz Pomorski, will provide you with more technical details about digital currencies and the needs they serve.

Our briefing today is intended to provide some background on what e-money is and how it is evolving. While we will introduce some of the policy issues that the broad adoption of e-money could raise for the Bank of Canada, it is important to stress that our research in this area is still very much a work-in-progress and many, if not all, of the policy issues remain open questions. We

TÉMOIGNAGES

OTTAWA, le mercredi 2 avril 2014

Le Comité sénatorial permanent des banques et du commerce se réunit aujourd'hui, à 16 h 55, pour étudier l'utilisation de la monnaie numérique.

Le sénateur Irving Gerstein (*président*) occupe le fauteuil.

[*Traduction*]

Le président : Je voudrais dire aux membres du comité que j'apprécierais beaucoup qu'ils restent à la fin de la séance pour que nous puissions tenir une réunion de cinq minutes à huis clos.

Le comité tient aujourd'hui sa troisième réunion consacrée à l'étude de la monnaie numérique. Nous avions commencé cette étude mercredi dernier en entendant des fonctionnaires du ministère des Finances. Jeudi, nous avons reçu deux représentants du monde universitaire qui s'étaient tous deux occupés de monnaies privées et numériques.

Cet après-midi, le comité entendra un exposé de la Banque du Canada. Nous avons le plaisir d'accueillir Grahame Johnson, chef de la Gestion financière et des Opérations bancaires, ainsi que Lukasz Pomorski, directeur adjoint de la Gestion financière et des Opérations bancaires.

Je vous remercie tous deux de votre présence au comité. Nous vous présentons nos excuses pour le retard que nous avons mis à commencer.

Je crois savoir, monsieur Johnson, que vous présenterez un exposé préliminaire et que M. Pomorski prendra la suite pour nous donner des détails techniques sur la monnaie numérique.

Monsieur Johnson, la parole est à vous.

Grahame Johnson, chef, Gestion financière et Opérations bancaires, Banque du Canada : Merci, monsieur le président. Lukasz et moi voudrions remercier tous les membres du comité de cette invitation à comparaître devant vous. C'est un sujet que nous trouvons tous deux complexe mais fascinant. Comme vous le savez, la banque a été sollicitée pour vous donner un aperçu des monnaies numériques, ce dont nous allons nous acquitter avec plaisir.

Quand on parle de monnaies numériques, il peut être utile de les situer dans le contexte plus général de l'évolution des systèmes de paiement. Cela étant, je vais commencer par un tour d'horizon des innovations et des développements récents touchant les systèmes de paiement et le rôle de la Banque du Canada. Ensuite, mon collègue, Lukasz Pomorski, vous présentera plus de précisions techniques sur les monnaies numériques et les besoins auxquels elles répondent.

Dans notre exposé d'aujourd'hui, nous avons l'intention d'expliquer dans les grandes lignes en quoi consiste la monnaie électronique et la façon dont elle évolue. Même si nous avons l'intention d'aborder certaines des questions de politique publique que l'adoption généralisée de la monnaie électronique pourrait soulever pour la Banque du Canada, il importe de souligner que

would, however, be pleased to return to this committee at a later date and speak to the policy questions in more detail once our work is further advanced.

As anyone who has visited the Currency Museum at our previous location on Sparks Street will know, systems of payment have evolved over time to meet the needs of the society they serve. Within this context, we can see that digital currencies, or e-money and similar innovations, are part of this broader historical continuum.

Before I discuss some of these innovations, I would like to start with some basic definitions about what exactly it is we mean by "money." Money serves three functions. First, it's a generally accepted medium of exchange. You can change your Canadian dollars for a coffee or a sandwich, for example, and the person who sells you the coffee can in turn use the money received to buy other goods. This general acceptance is a critical that money needs to play.

Second, it serves as unit of account. The dollar helps us to compare the value of different goods, for example, the cost of a Tim Hortons coffee compared with a Starbucks coffee.

Third, it can be used as a store of value. You can deposit your dollars in your bank account and then be confident that when you withdraw them, they still will have a similar value in terms of the goods or services that they can purchase.

[*Translation*]

We are all very familiar with money in the traditional sense, that is to say coins and bank notes. When we talk about Canadian dollars we usually have Canadian bank notes in mind. These notes, once paper and now polymer, remain popular among Canadians; the value of notes in circulation has been growing at more or less the same pace as the economy over the past two decades. So, despite a growth in electronic payments, cash is still important.

Important, but not always convenient. Carrying bank notes to pay for purchases, especially for transactions that have a relatively large value — like buying a refrigerator or a car — can be impractical. There is also the risk of loss or theft. Over the years, innovations in payment systems have addressed many of these problems.

[*English*]

In the modern financial system, people typically store their money as deposits in commercial bank accounts. This money is denominated in state currencies and issued by regulated financial

nos recherches dans ce domaine sont toujours en cours, et que de nombreuses sinon toutes les questions de politique demeurent floues. Nous nous ferions néanmoins un plaisir de revenir devant votre comité afin de traiter ces questions de politique d'une manière plus approfondie dès que nos travaux auront suffisamment progressé.

Comme le sait toute personne qui a visité le Musée de la monnaie de la Banque du Canada, à notre ancien établissement, rue Sparks, les systèmes de paiement évoluent au gré des besoins de la société. Dans ce contexte, il est clair que les monnaies dites numériques ou électroniques, et d'autres innovations similaires s'inscrivent dans cette lignée historique.

Avant de traiter de quelques-unes de ces innovations, je commencerai par définir des notions fondamentales liées à ce que nous entendons par « monnaie ». La monnaie a trois fonctions. Premièrement, c'est un moyen d'échange généralement accepté. On peut échanger des dollars canadiens contre un café ou un sandwich, par exemple. Et le vendeur du café peut à son tour utiliser l'argent qu'il reçoit pour acheter d'autres biens. Cette notion d'acceptation générale est un attribut essentiel que doit avoir la monnaie.

Deuxièmement, la monnaie sert aussi d'unité de compte. Elle nous aide à comparer la valeur de différents biens, par exemple le prix d'un café de Tim Horton par rapport à celui d'un café de Starbucks.

Troisièmement, la monnaie peut servir de réserve de valeur. On peut déposer de l'argent dans son compte en banque et être sûr qu'une fois qu'on le retirera, il aura à peu près le même pouvoir d'achat.

[*Français*]

Nous connaissons tous très bien la monnaie au sens classique du terme, c'est-à-dire les pièces et les billets de banque. Et lorsqu'on parle de dollars canadiens, ce qui nous vient d'abord à l'esprit ce sont les billets de banques canadiennes. Naguère en papier, désormais en polymère, ces billets demeurent un moyen de paiement prisé des Canadiens; au cours des 20 dernières années la valeur des billets en circulation a progressé à peu près au même rythme que celui de l'économie. En dépit de la croissance des paiements électroniques, l'argent comptant garde donc toute son importance.

L'argent comptant est important, mais pas toujours commode. On conviendra que ce n'est pas pratique pour certaines transactions, surtout celles de montants élevés, comme l'achat d'un réfrigérateur ou d'une voiture. Et puis, il y a aussi les risques de perte et de vol. Au fil des années, les innovations apportées aux systèmes de paiement ont permis de résoudre certains de ces problèmes.

[*Traduction*]

Dans le système financier moderne, les gens déposent habituellement leur argent dans des comptes en banque. Cet argent est libellé dans la monnaie nationale et émis par des

institutions through lending and the creation of demand deposits; that is, accounts that allow people to access their money on demand. Demand deposits are a medium of exchange and can be transferred from one account holder to another. Cheques were an early innovation that facilitated such transfers. They save us the hassle of going to the bank to withdraw large sums of cash.

Since the introduction of cheques, we have seen a number of other technological advances that allow the transfer of account balances between people and between people and businesses. These innovations include such things as debit and ATM cards, phone banking, Internet banking and mobile banking, all of which we refer to as access devices; that is, they provide access to our demand accounts, but they are not money per se.

I should also mention the innovation of the credit card, which we use to transfer funds from our credit account at a bank. Again, credit cards are access devices in that they provide us access to lines of credit.

For our discussion, we will refer to such access devices as electronic payments or e-payments. We continue to see innovation in e-payments. More recently, for example, we've seen the introduction of contactless debit and credit cards. These are the tap-and-go cards that you may have seen. Such improvements are driven by the evolving needs and expectations of consumers but also by advances in technology. Importantly, e-payments are the domain of banks and other deposit-taking institutions that are subject to prudential regulation.

From e-payments I will move to the main topic of our presentation: e-money. In contrast to e-payment technology, e-money is actual monetary value that is stored on an electronic device. This could be a computer, a mobile phone, a tablet, a chip card or even a server, in a cloud. It has a monetary value in a state currency, often from an issuer who assumes a liability for that value. In this way it's different from e-payments that don't have that intrinsic value but, rather, provide access to funds in a bank account.

Lukasz will provide you with a much more detailed analysis of what e-money is and what the main types of e-money are, but e-money was developed and is growing for reasons that are related to both demand and supply.

On the demand side, online commerce has clearly created the need to be able to transact over long distances using telecommunication technology. While existing e-payment

institutions financières réglementées, sous forme de prêts qu'elles consentent et de dépôts à vue qu'elles créent, c'est-à-dire des comptes qui permettent au déposant d'accéder à son argent à sa discrétion. Les dépôts à vue sont un moyen d'échange qui permet de virer de l'argent d'un détenteur de compte à un autre. Les chèques ont constitué une première innovation qui permettait de tels virements, en épargnant au déposant d'avoir à aller à sa banque pour retirer de l'argent liquide.

Depuis l'avènement des chèques, il y a eu bien d'autres innovations technologiques qui permettent de virer des fonds entre les comptes de particuliers, ou encore entre les comptes de particuliers et ceux d'entreprises. Ces innovations comprennent, par exemple, les cartes de débit ou de retrait au guichet automatique, les services bancaires par téléphone ou en ligne, voire les services bancaires mobiles. Tous ces moyens sont considérés comme des dispositifs d'accès parce qu'ils permettent d'accéder à son compte à vue, mais ne constituent pas de la monnaie en soi.

Je n'oublierai pas de mentionner aussi l'innovation de la carte de crédit, qu'on emploie pour virer des fonds de son compte de crédit bancaire. Les cartes de crédit sont aussi des dispositifs d'accès, puisqu'elles permettent à leurs utilisateurs d'accéder à des lignes de crédit.

Pour les besoins de notre exposé, nous allons ranger ces dispositifs d'accès dans la catégorie des paiements électroniques. Les innovations continuent de fleurir dans ce domaine, comme en témoigne le récent lancement des cartes de débit ou de crédit sans contact. Vous avez sans doute vu ces cartes qu'on agite simplement devant un récepteur. Ces améliorations sont essentiellement dues à l'évolution des besoins et des attentes des consommateurs, ainsi qu'aux avancées technologiques. Fait important à souligner, les paiements électroniques sont du ressort des banques et d'autres institutions de dépôt qui sont assujetties à une réglementation prudentielle.

Après cette parenthèse sur les paiements électroniques, permettez-moi d'entrer dans le vif du sujet : la monnaie électronique. Contrairement aux paiements électroniques, la monnaie électronique consiste en une valeur monétaire réelle stockée sur un support électronique, comme un ordinateur, un téléphone portable, une tablette, une carte à puce, ou encore un serveur en nuage. Elle a une valeur monétaire qui lui est attribuée dans une monnaie nationale, souvent par un émetteur qui s'en porte garant. Elle se distingue ainsi des paiements électroniques qui, sans avoir une valeur intrinsèque, donnent accès aux fonds détenus dans un compte bancaire.

Lukasz vous présentera une analyse beaucoup plus détaillée de la monnaie électronique, en en précisant la nature et les principaux types, mais la monnaie électronique a été mise au point et s'étend actuellement pour des raisons qui tiennent à des facteurs relevant tant de l'offre que de la demande.

Du côté de la demande, le commerce en ligne a clairement créé le besoin de consommer à distance à l'aide des technologies de télécommunications. Bien que les moyens de paiement

methods such as credit cards can and clearly are used for such online transactions, they carry with them a number of potential disadvantages, for example, inconvenience and, in the case of credit cards, the need to share a relatively large amount of information every time a transaction occurs. There are relatively high fees. Again in the case of credit cards, merchants get charged for every transaction, particularly for small-value transactions that can be prohibitive. Certainly, cross-border transactions or international remittances are expensive. Finally, there are potential security risks, many associated with the amount of information that needs to be disclosed.

On the supply side, there are things such as advances in technology, the growth of the Internet and the widespread adoption of technology such as mobile devices and smart phones, which give people the means to use these new payment products offered by technology companies. We now have firms such as PayPal, for example, that allow users to pay over the Internet without giving a full amount of personal information to the merchant with every transaction. E-money can also make payments more efficient and cheaper, especially across borders.

While e-payments are facilitated by regulated financial institutions offering new ways for individuals and businesses to transfer money, e-money itself is often issued by unregulated institutions. These include new players in the payments landscape: telecommunications companies, information processers and even, in some cases, social networks.

While banks still provide payment services, they often seek partnership with non-banks in providing innovative payment products such as mobile payment.

[*Translation*]

How important are these innovations to the Canadian economy? A 2009 study conducted by the Bank of Canada showed that two particular innovations, contactless credit cards and stored-value cards, accounted for three per cent of the number of transactions and about two per cent of the dollar value of all transactions. This relatively small share may have increased over the past few years, and the bank is currently updating this research.

Moreover, the Canadian Payments Association estimated that there were 24 million transactions of various e-money products in 2011, worth nearly $10 billion, up from $3 billion in 2008. These figures likely capture only a subset of all e-money transactions as the CPA tracked only e-wallet products and peer-to-peer transactions. Over the same period, the annual growth rate of these types of payments in terms of volume has averaged close to 40 per cent.

électronique comme les cartes de crédit soient utilisés pour le commerce en ligne, ils ont plusieurs inconvénients possibles. Ainsi, ils peuvent être malcommodes et, dans le cas des cartes de crédit, ils peuvent imposer d'échanger un important volume d'information à chaque transaction. De plus, les frais sont relativement élevés. Encore une fois, dans le cas des cartes de crédit, le marchand doit payer pour chaque transaction des frais qui, particulièrement dans le cas des transactions de peu de valeur, peuvent être prohibitifs. Il n'y a pas de doute que les transactions transfrontalières ou internationales sont coûteuses. Enfin, il y a des risques sur le plan de la sécurité, qui sont liés dans beaucoup de cas au volume d'information à communiquer.

Du côté de l'offre, les progrès techniques, l'essor d'Internet et la large adoption d'appareils mobiles tels que les téléphones intelligents ont donné à de nombreux utilisateurs les moyens d'employer les nouveaux produits de paiement offerts par des entreprises technologiques. Il y a maintenant des sociétés qui, comme PayPal, permettent aux consommateurs de payer leurs achats sur Internet sans avoir à communiquer autant de renseignements personnels aux vendeurs à chaque transaction. De plus, la monnaie électronique est de nature à rendre les paiements plus efficients et moins coûteux, en particulier les paiements internationaux.

Alors que les paiements électroniques sont le fait d'institutions financières réglementées qui offrent aux particuliers et aux entreprises de nouvelles façons de virer de l'argent, la monnaie électronique, elle, est souvent émise par des institutions non réglementées. Parmi ces dernières, on compte de nouveaux acteurs du secteur des paiements, tels que des entreprises de télécommunications ou de traitement de l'information, voire des réseaux sociaux.

Si les banques continuent à fournir des services de paiement, elles cherchent aussi souvent à nouer des partenariats avec des institutions non bancaires pour fournir des moyens de paiement novateurs, comme les paiements mobiles.

[*Français*]

Quelle est l'importance de ces innovations dans l'économie canadienne? Une étude de 2009, réalisée par la Banque du Canada, a montré que deux innovations en particulier, soit les cartes sans contact et les cartes prépayées, représentaient 3 p. 100 du volume, et environ 2 p. 100 de la valeur de l'ensemble des transactions. Ces proportions relativement faibles ont peut-être augmenté depuis, c'est pourquoi la banque s'emploie présentement à actualiser les résultats de cette étude.

En outre, l'Association canadienne des paiements a estimé qu'en 2011, il y avait eu 24 millions d'opérations effectuées à l'aide de monnaies électroniques diverses, d'une valeur avoisinant 10 milliards de dollars, comparativement à 3 milliards de dollars en 2008. Ces chiffres ne mettent probablement en évidence qu'une partie de toutes les transactions de monnaie électronique réalisées au Canada. L'Association canadienne des paiements s'étant concentrée sur les opérations de porte-monnaie électronique et

[*English*]

Despite this growth, there are relatively fewer e-money products in Canada relative to some other countries. Some of you may remember Mondex — although neither of us do — which was a stored value card that appeared in the mid-1990s but failed to get traction. This seems to suggest that Canadians are relatively well served by the existing methods of payment and existing methods of e-payment systems in particular.

In contrast, consumers in countries with retail payment systems that are not as well developed need to seek out alternative methods of payment. This leads to e-money innovations such as the mobile system M-Pesa in Africa or multi-purpose prepaid cards such as the Octopus card in Hong Kong.

E-money addresses important consumer needs but also raises potential risks and challenges. At present such risks have the largest impact on individual consumers and businesses rather than on the overall Canadian economy or financial system.

The most significant risk posed by e-money is probably inadequate user protection. This could include insufficient or inadequate information about a new payment service provider, especially about terms and conditions, fees or dispute settlement procedures. Moreover, users may not fully appreciate the potential privacy issues associated with these means of payment since some e-money providers have business models that depend on advertising revenue derived from sharing personal information about users.

Other e-money developments provide relative anonymity which entails additional risks such as money laundering and terrorist financing issues. I believe our colleagues from the Department of Finance, who appeared here last week, have discussed these aspects of e-money in a little more detail.

The Bank of Canada has several reasons to be interested in e-money developments. The bank designs, produces and distributes Canada's banknotes. One potential impact of recent developments in e-money is that they may lead to changes in the demand for cash. There are at present about $63 billion worth of banknotes in circulation and the bank invests the proceeds of issuing these notes in Government of Canada bonds. These bonds are held on the bank's balance sheet and generate interest income, which we refer to as seigniorage revenue. This revenue is used by

de P2P, ou entre pairs. Le taux de croissance annuelle de ces modes de paiement, en volume, s'est établi à près de 40 p. 100 en moyenne pendant cette même période.

[*Traduction*]

En dépit de cette forte croissance, il y a, toutes proportions gardées, moins de produits de monnaie électronique au Canada que dans d'autres pays. Certains d'entre vous se souviendront peut-être de Mondex — je dois admettre qu'aucun de nous deux ne s'en souvient —, une carte prépayée introduite au milieu des années 1990, mais qui n'a pas trouvé de créneau porteur. Cela donne à penser que les Canadiens sont bien servis par les moyens de paiement existants, à commencer par les systèmes de paiement électroniques.

Par contre, les consommateurs de pays où les systèmes de paiement ne sont pas aussi développés ont besoin de trouver des modes de paiement différents, ce qui donne lieu à des innovations dans le domaine de la monnaie électronique. On peut citer, par exemple, le système de paiement mobile M-Pesa, en Afrique, ou encore les cartes prépayées polyvalentes comme Octopus, à Hong Kong.

La monnaie électronique répond certes à d'importants besoins des consommateurs, mais elle recèle aussi certains risques. Pour le moment, ces risques sont supportés essentiellement par chacun des utilisateurs, qu'il s'agisse de particuliers ou d'entreprises, plutôt que par l'ensemble de l'économie et du système financier du Canada.

Le risque le plus important réside probablement dans le manque de protection de l'utilisateur. Il peut s'agir de renseignements insuffisants ou inadaptés au sujet d'un nouveau fournisseur de services de paiement, particulièrement en ce qui concerne les modalités, les frais d'utilisation ou les procédures de règlement des litiges. Il se peut en outre que les usagers ne se rendent pas entièrement compte de problèmes potentiels ayant trait à leur vie privée, car le modèle d'affaires de certains fournisseurs de monnaie électronique se fonde sur les recettes publicitaires tirées de la communication à d'autres des renseignements personnels de leurs utilisateurs.

D'autres monnaies électroniques assurent un anonymat relatif à leurs usagers et comportent, par le fait même, d'autres types de risques, comme le blanchiment d'argent et le financement de groupes terroristes. Je crois que nos collègues du ministère des Finances, qui ont comparu devant votre comité la semaine dernière, ont abordé plus en détail ces aspects.

La Banque du Canada a plusieurs raisons de s'intéresser à l'évolution de la monnaie électronique. Tout d'abord, elle conçoit, produit et distribue les billets de banque canadiens. Or, l'essor récent des monnaies électroniques pourrait faire baisser la demande de numéraire. Il y a en ce moment pour environ 63 milliards de dollars de billets en circulation, et la banque place le revenu tiré de l'émission de ces billets dans des obligations du gouvernement du Canada. Ces titres figurent au bilan de la banque et génèrent des intérêts que nous appelons revenus de

the Bank of Canada to pay our expenses and the balance is remitted to the federal government. In 2013 this seigniorage revenue was roughly $1.6 billion and the remittance to the government was about $1 billion.

Furthermore, the financial assets of these government bonds that we hold on the bank's balance sheet help support the bank's various mandates, including our monetary policy and financial stability functions. A substantial decrease in the demand for cash would mean a commensurate increase in the financial assets on the bank's balance sheet. This would, in turn, lead to reduced revenue for both the bank and the federal government. Furthermore, the lower level of financial assets held on the balance sheet might also have other effects on the bank's ability to do the work we do. Given that the demand for cash has been relatively stable over the past number of decades, these risks at present appear to be largely hypothetical.

The bank also has an interest in promoting safety and efficiency in the payment system. We work with other authorities in this area, and given the bank's responsibilities under the Payment Clearing and Settlement Act, we are collaborating with the Department of Finance to conduct a governance review of the payment system. This work addresses the oversight and governance of the national payments, clearing and settlement infrastructure and includes alternative payments technology.

Studying e-money and its implications for central banks is clearly a strategic priority for the Bank of Canada. The bank's research efforts in this area are focused on deepening our understanding of electronic money and payments as digital alternatives to cash, and analyzing the implication of an increased use of these alternatives for how the bank fulfills its mandates to provide secure banknotes, to promote financial stability, and to control inflation.

Our research will inform a number of important policy questions. These include: Should the Bank of Canada have a role as an issuer or operator of e-money? Could the broader adoption of e-money pose financial stability concerns? If so, how can these be best mitigated? What is the appropriate regulatory framework for e-money? Could increased reliance on e-money potentially have implications for monetary policy?

As I mentioned at the beginning, it is important to stress that our research in this area is very much a work-in-progress, and the issues I've raised remain open questions. Given the public interest and the importance of the topic, however, the bank intends to share its research with the public through a new section on our website dedicated to this subject, and the bank sees e-money within a broader continuum of payment system innovation. As with any innovation, looking back at where we have been is a lot easier than looking ahead to determine where we're going. With a

seigneuriage. Ces recettes servent à couvrir les dépenses de l'institution, le solde étant versé au Trésor fédéral. En 2013, par exemple, les revenus de seigneuriage se sont élevés à 1,6 milliard de dollars environ, dont un milliard a fini dans les caisses de l'État.

De plus, les actifs financiers inscrits au bilan au titre de ces obligations aident la banque à remplir ses diverses fonctions, notamment en ce qui concerne la politique monétaire et la stabilité financière. Une importante baisse de la demande de numéraire entraînerait donc une diminution du portefeuille d'actifs de l'institution, qui, à son tour, mènerait à un repli des recettes aussi bien pour la banque que pour le gouvernement fédéral. De surcroît, la baisse des actifs financiers inscrits au bilan pourrait avoir d'autres conséquences sur la capacité de la banque de s'acquitter de son mandat. Cela dit, étant donné que la demande de numéraire a été relativement stable ces dernières décennies, ces risques sont, pour le moment, purement théoriques.

La Banque du Canada s'efforce également de promouvoir la sûreté et l'efficience du système de paiement. Nous travaillons de concert avec d'autres autorités dans ce domaine et, compte tenu des responsabilités que lui confèrent la Loi sur la compensation et le règlement des paiements, la banque procède, en collaboration avec le ministère des Finances, à un examen de la gouvernance du système canadien de paiement. Ce travail couvre la surveillance et la gouvernance de l'infrastructure nationale des systèmes de paiement, de compensation et de règlement, y compris les nouvelles technologies de paiement.

L'étude de la monnaie électronique et de ce qu'elle implique pour les banques centrales est donc pour nous une priorité stratégique. Les recherches que nous effectuons dans ce domaine visent surtout à mieux comprendre la monnaie et les moyens de paiement numériques, comme produits de remplacement du numéraire, et à analyser l'incidence de leur essor sur la capacité de la banque à remplir ses grandes missions, en l'occurrence, procurer aux Canadiens des billets de banque sûrs, promouvoir la stabilité financière et maîtriser l'inflation.

Ces recherches aideront les décideurs à répondre à plusieurs questions stratégiques importantes. Par exemple : la Banque du Canada devrait-elle avoir un rôle dans l'émission ou l'exploitation de la monnaie électronique? L'adoption généralisée de la monnaie électronique comporte-t-elle des risques pour la stabilité financière? Si oui, quelle est la meilleure façon de les atténuer? Quel cadre réglementaire conviendrait le mieux pour la monnaie électronique? Le recours accru à cette monnaie peut-il se répercuter sur la politique monétaire?

Il importe de noter, comme je l'ai dit au début de mon exposé, que les recherches de la banque sont en cours et que les questions de politique que j'ai soulevées demeurent floues. Compte tenu de l'intérêt du public pour cette question et de l'importance qu'elle revêt, la Banque du Canada entend diffuser les résultats de ses recherches dans une nouvelle section de son site web qui sera consacrée à ce sujet. Pour la banque, la monnaie électronique fait partie du continuum plus vaste des innovations touchant les systèmes de paiement. Comme pour toute innovation, il est bien

solid research agenda and by monitoring and assessing e-money systems, the bank is committed to building our understanding so we continue to meet our mandate to promote the economic and financial welfare of Canada.

I will now turn it over to Lukasz for an in-depth explanation of e-money.

Lukasz Pomorski, Assistant Director, Funds Management and Banking, Bank of Canada: Let me start by saying that e-money is difficult to define. When you talk to people about it, multiple terms are used almost interchangeably: e-money, e-cash, digital money, digital currency, virtual currency and so on. The problem is that people would use these terms with sometimes very different meanings. We'll talk about that. Then we'll talk about whether and how e-money could potentially satisfy the roles of money and currency, as we understand it, in terms of a medium of exchange, a unit of account and a store of value.

As Grahame explained, e-money is monetary value stored on an electronic device, either a computer, mobile phone, tablet or chip card.

To analyze it more deeply, I would like to divide e-money into two categories: One is centralized e-money, that is, e-money that is issued and often managed by a central issuer who often assumes liability for the e-money; and decentralized, that is, based on a dispersed network of users, with no one user recognizing the e-money as his liability.

I will begin with centralized e-money. Centralized e-money is monetary value stored on an electronic device that is issued upon receipt of funds and accepted as a means of payment by entities other than the issuer.

This definition is used not only by us but also by multiple other institutions, for example, the European Central Bank or the Bank for International Settlements. The critical feature of centralized e-money is that it has a particular issuer who has liability for its value.

As an example, consider prepaid payment cards, for example, those issued by Visa or MasterCard. Consumers who are using these cards could use the card potentially to obtain a particular good or service from the issuer directly. They might use the card for goods and services provided by a third party — for example, a merchant — who will subsequently be reimbursed by the issuer. Lastly, the consumer might also be able to redeem the value of e-money perhaps using an ATM, and the cash will be subsequently reimbursed by the issuer to the bank.

plus facile de mesurer le chemin parcouru que de déterminer les voies qui pourraient s'ouvrir. Toutefois, grâce à un solide programme de recherches ainsi qu'à la surveillance et à l'évaluation des systèmes de monnaie électronique, la banque est résolue à parfaire ses connaissances dans ce domaine afin de continuer à remplir son mandat de promotion de la prospérité économique et financière du Canada.

Je vais maintenant céder la parole à Lukasz qui vous donnera des explications détaillées au sujet de la monnaie électronique.

Lukasz Pomorski, directeur adjoint, Gestion financière et Opérations bancaires, Banque du Canada : Je commencerai par dire que la monnaie électronique est difficile à définir. Quand on en parle, les gens lui donnent de multiples noms qu'ils utilisent comme s'ils étaient interchangeables : monnaie numérique, monnaie virtuelle, argent électronique, et cetera. Le problème, c'est que les gens emploient ces mots en leur attribuant parfois des significations très différentes. Nous parlerons de tout cela. Ensuite, nous déterminerons si la monnaie électronique peut remplacer l'argent, comme nous le connaissons, comme moyen d'échange, unité de compte et réserve de valeur.

Comme Grahame l'a expliqué, la monnaie électronique est un instrument dont la valeur monétaire est stockée sur un support électronique, comme un ordinateur, un téléphone portable, une tablette ou une carte à puce.

Pour en faire une analyse approfondie, je noterai d'abord que la monnaie électronique se répartit entre deux principales catégories : la monnaie électronique centralisée, c'est-à-dire émise et gérée, la plupart du temps, par une autorité centrale qui la comptabilise dans son passif, et la monnaie électronique décentralisée qui repose sur un réseau d'utilisateurs dispersés et qui ne figure au passif d'aucun d'entre eux.

Examinons tout d'abord la monnaie électronique centralisée. Il s'agit d'une valeur monétaire stockée sur un support électronique, émise contre une remise de fonds et acceptée comme moyen de paiement par des entités autres que son émetteur.

À part la Banque du Canada, de nombreuses institutions utilisent cette définition, dont la Banque centrale européenne et la Banque des règlements internationaux. Ce qui fait la particularité de la monnaie électronique centralisée, c'est qu'elle est émise par une autorité centrale qui comptabilise sa valeur dans son passif.

Prenons, à titre d'exemple, les cartes prépayées Visa et MasterCard. Un consommateur peut employer une telle carte pour acheter un bien ou un service directement à l'émetteur. Il peut également se procurer des biens et des services auprès d'un tiers, comme un marchand, qui sera ensuite remboursé par l'émetteur. Enfin, il lui est parfois possible d'échanger la valeur monétaire stockée sur sa carte contre de l'argent comptant, à un guichet automatique bancaire, par exemple. Dans ce cas, l'émetteur remettra à l'institution financière la somme correspondante.

Another important and key feature of centralized e-money is that it is multipurpose. Prepaid cards that are used for a particular store or coffee chain wouldn't qualify for that.

To give you an example of a very popular centralized e-money device, I would like to talk about the Octopus card, which is very popular in Hong Kong. The Octopus card is a contactless card that is prepaid and was originally issued by the Hong Kong mass transit system. Over time, the Octopus card has become more generally accepted by retailers, and nowadays people use it to make other purchases, not only transport. Value on the Octopus card is prepaid and it becomes a liability of the issuer. It can be used to make payments at a wide range of retail and transport venues, which satisfies multi-purpose criteria.

I would like to contrast the Octopus card with a similar card that we have in Canada, the PRESTO card. The PRESTO card is used for transport services in multiple municipalities in Ontario. At present, the acceptance of a PRESTO card is limited to the transport system. You can use it to pay for rides but not necessarily to make purchases for coffee, newspapers and so on.

When we compare the PRESTO and the Octopus card, there's an interesting question: Why did the Octopus card, quite similar to PRESTO, gain widespread adoption in Hong Kong and is used for a variety of purposes, whereas in Canada it's used almost exclusively for transport?

In Hong Kong, since the 2000s, consumers have been using the Octopus card not only for transport but also for small transactions. In Canada, this is not so. One reason is that in Canada, contactless debit and credit cards are already filling this economic need, this niche.

One last point that I want to make on the topic of centralized e-money is that sometimes when you talk to people about that, they would mention centralized digital currencies that are issued by particular Internet companies, for example, Facebook or Amazon, or used within some computer game systems, for example, World of Warcraft. Those currencies are actually centralized in the sense of being issued and controlled by a particular company.

We would argue, however, that they don't really qualify as e-money. The key reason why not is because they are intended to be used exclusively within those platforms and communities. They are in no sense generally accepted as a medium of exchange, as means of payment, and hence don't qualify as e-money.

Having talked about the centralized variety of e-money, let us move on to decentralized e-money and start with highlighting some of the key differences.

La polyvalence est une autre caractéristique importante de la monnaie électronique. Les cartes prépayées dont l'utilisation est restreinte à un seul magasin ou restaurant ne s'inscrivent pas dans cette catégorie.

Pour vous donner un exemple d'un instrument très populaire de monnaie électronique centralisée, je vous parlerai de la carte Octopus, qui est très utilisée à Hong Kong. Il s'agit d'une carte sans contact prépayée émise à l'origine pour faciliter le paiement à bord des transports en commun de Hong Kong. Avec le temps, les détaillants ont été de plus en plus nombreux à accepter les paiements effectués avec cette carte, de sorte qu'aujourd'hui, les gens s'en servent pour régler de multiples achats, et pas seulement leur transport. Une valeur monétaire est préalablement stockée sur la carte, qui devient ainsi un élément de passif pour l'émetteur. Elle peut être utilisée dans de nombreux commerces de détail et moyens de transport, ce qui fait d'elle un mode de paiement polyvalent.

Je voudrais maintenant comparer la carte Octopus à la carte PRESTO, assez semblable, que nous avons au Canada. La carte PRESTO est utilisée dans les transports en commun de plusieurs villes de l'Ontario. À l'heure actuelle, elle n'est reconnue que par les sociétés de transport. On peut s'en servir dans les transports en commun, mais pas nécessairement pour acheter un café ou un journal.

La comparaison de ces deux cartes nous amène à nous demander pourquoi la carte Octopus, très semblable à la carte PRESTO, a été largement adoptée à Hong Kong où elle sert à de multiples fins, alors que la carte canadienne est utilisée presque exclusivement dans les transports en commun?

Depuis le début des années 2000, les consommateurs de Hong Kong se servent de la carte Octopus non seulement pour se déplacer, mais aussi pour régler de menus achats, tandis qu'au Canada, les cartes de crédit et de débit sans contact satisfont déjà à ce besoin.

Un dernier point au sujet de la monnaie électronique centralisée. Quand les gens en parlent, ils mentionnent parfois des monnaies électroniques centralisées émises par des sociétés en ligne, comme Facebook et Amazon, ou par des concepteurs de jeux en ligne comme World of Warcraft. Ces monnaies sont effectivement centralisées, car elles sont gérées par une firme ou une entité particulière.

Toutefois, elles ne sauraient être considérées comme de véritables monnaies électroniques, puisqu'elles sont destinées à servir exclusivement sur leur plateforme d'origine. Elles ne sont donc pas généralement acceptées comme moyen d'échange ou de paiement par des parties autres que leur émetteur.

Abordons maintenant la question des monnaies électroniques décentralisées, pour lesquelles il n'y a pas d'émetteur officiel, afin de mettre en évidence les principales différences avec les monnaies centralisées.

The main difference is that for decentralized e-money there is no formal issuer. There is no central bank, financial intermediary or Internet platform.

E-money is decentralized over a peer-to-peer computer network but directly links users, in which no one user assumes control for the e-money. Maybe a good analogy would be to think about an Internet chat room that links users, but no one user has control over it.

The standard example for decentralized e-money is the bitcoin. The bitcoin was created in 2009, and since then there have been about 200 other similar currencies. We call them crypto-currencies, and I will explain why in a second. Many of them have been created over the last few months, and a few of them have been since discontinued.

As the best-known example of decentralized e-money, most of my remaining time will be focused on the bitcoin, and I will close by illustrating similarities and differences between the bitcoin and other crypto-currencies.

Until the creation of the bitcoin, so until 2009, the very idea of decentralized e-money was theoretical, and multiple specialists would argue that it's unsolvable, that it's only a theoretical construct that couldn't be implemented in practice. The biggest problem there was the issue of double spending. Let me explain why.

Suppose we develop a crypto-currency or digital currency that I would like to sell to Grahame. As I send this electronic record to Grahame, the first thing he will need to do is verify that this record is authentic or valid. This step is relatively straightforward and there are some tools in information technology that allow for this step. In a sense, it's similar to taking a banknote and verifying it's not counterfeit.

Problems will arise when I try to convince Grahame that this record I'm sending to him has not yet been sent to somebody else before him. How do I convince him I have not already sent information — the money I'm sending to him? This is not an issue for banknotes, because once you spend them, they're gone; you cannot spend them twice.

Moreover, when we talk about centralized e-money, it's not an issue either. That's because there is a centralized issuer who keeps a ledger that summarizes who holds how much of a currency, and it's continually updated with transactions.

With bitcoin and some of the decentralized currencies, this ledger is shared on a peer-to-peer network, and because of cryptographic tools the network uses, its validity is trusted despite the absence of a trusted third party — an issuer.

From the point of view of technology, being able to spread the trust across a peer-to-peer network was a major innovation. This means there is no single issuer of bitcoins. The bitcoin itself is nobody's liability and, in particular, it's not redeemable. Because bitcoin uses cryptographic tools to achieve this, we call it "crypto-currency."

La plus grande différence est qu'il n'y a pas d'entité émettrice à l'origine de ces monnaies : ni banque centrale, ni institution financière, ni plateforme Internet.

Elles sont émises de manière décentralisée dans un réseau informatique de pair à pair, sur lequel personne n'a autorité, et dont les utilisateurs sont en rapport direct les uns avec les autres, un peu comme dans un site de clavardage.

Le bitcoin est l'exemple type d'une monnaie électronique décentralisée. Il a fait son apparition en 2009. Depuis, quelque 200 monnaies semblables ont vu le jour. Elles sont appelées cryptomonnaies pour des raisons que je vous expliquerai dans quelques instants. Bon nombre d'entre elles ont été créées au cours des derniers mois et certaines ont déjà disparu.

Puisqu'il s'agit de l'exemple le mieux connu, je consacrerai l'essentiel du temps qui me reste à la description du bitcoin, puis je tâcherai, en conclusion, de faire ressortir les différences et les similarités qu'il présente avec les autres cryptomonnaies.

Avant la création du bitcoin en 2009, de nombreux experts considéraient la monnaie électronique décentralisée comme un concept théorique insoluble, impossible à réaliser en pratique, notamment en raison du phénomène de la double dépense. Je m'explique.

Imaginez que l'on mette au point une monnaie électronique et que je veuille transférer des fonds à Grahame. Une fois que je lui aurai transmis les renseignements électroniques, il voudra tout d'abord vérifier l'authenticité de ces renseignements. Cette étape est relativement facile à réaliser, car elle repose sur des techniques informatiques bien établies et parfaitement adaptées. C'est un peu comme de s'assurer qu'un billet de banque n'est pas contrefait.

Les ennuis surgissent lorsque je dois convaincre Grahame que je n'ai pas dépensé ailleurs la somme que je suis en train de lui transférer : comment puis-je lui prouver que je ne l'ai pas déjà envoyée à quelqu'un d'autre? Ce problème n'existe pas avec les billets de banque : il est impossible de les dépenser deux fois.

De la même façon, cela n'occasionne aucun souci dans le cas des monnaies électroniques centralisées, puisqu'il y a alors un émetteur qui dispose des moyens technologiques nécessaires pour tenir à jour, après chaque transaction, un livre comptable centralisé où sont clairement notés les avoirs de chacun.

Dans le cas des bitcoins, le livre comptable est partagé entre les utilisateurs du réseau, qui ont confiance en sa validité, malgré l'absence d'une tierce partie fiable, parce que le réseau fait appel à des procédés cryptographiques.

Il s'agit d'une innovation majeure dans le domaine des technologies de l'information. Cela a permis de créer une monnaie sans émetteur, qui ne constitue un élément de passif pour aucune entité et dont il n'incombe à personne de rembourser la valeur monétaire. L'appellation « cryptomonnaie » découle du fait que tout ce système repose sur la cryptographie.

There is a lot more to learn about the technical aspects of bitcoin and similar currencies, particularly the cryptographic tools they use. We understand that you will be hearing from an expert in information systems engineering who will be better able to provide you with this information.

For our talk, we would like to focus on the question within our field of expertise, starting with whether bitcoins and, by extension, other crypto-currencies can satisfy the functions of money. We would also like to discuss how innovations such as bitcoin might contribute to improving the efficiency of our payment systems, while raising some issues for policy makers.

As we saw in the discussion of centralized e-money, there were some cases where it met the criteria of money: It was a medium of exchange, a unit of account and had a store of value. Again, one of the key examples would be the Octopus card in Hong Kong.

How does decentralized e-money such as bitcoin hold up? We would argue that bitcoin and other crypto-currencies fall short of a definition of money and do not satisfy the functions of money, at least at present. First, for bitcoin to be currency, it would need to be generally accepted and it would need to be a medium of exchange. While there may be some potential here, it's not quite there yet.

We do see that the bitcoin network allows and facilitates transfers of bitcoin users. We also see a growing group of retailers — some of them global — that allow purchases in bitcoin. Our search of bitcoin-related enterprises reveals that there are anywhere between 100 and 200 retailers in Canada who accept bitcoins for transactions. Worldwide, all my sources would estimate there are in the neighbourhood of 15,000 goods and services that can be obtained for bitcoins. These are perhaps large numbers, but at the same time, in the context of the overall economy, we would argue that these numbers are not quite enough to persuade people that bitcoin is at present a generally accepted means of exchange.

In terms of a unit of account, bitcoin may have potential but is not quite there. Even in those cases where bitcoin is a means of exchange, the underlying value of a transaction seems to be always in terms of a state currency, such as the U.S. or Canadian dollar. Such value would then be trusted into bitcoins for the purposes of a transaction.

This is true of most merchants who market themselves as accepting bitcoins. In practice, such merchants rarely actually receive the crypto-currency. Instead, they contract with third parties that exchange bitcoins into international currencies at the moment of exchange of the transaction. An example of a

Il reste encore beaucoup à apprendre au sujet des aspects techniques du bitcoin et des monnaies semblables, et particulièrement des outils de chiffrement utilisés. Je crois savoir qu'un spécialiste de l'ingénierie informatique comparaîtra prochainement devant le comité pour vous fournir des renseignements à ce sujet.

Pour notre part, nous nous concentrerons sur les questions qui relèvent de notre domaine d'expertise, en cherchant d'abord à déterminer si le bitcoin et, par extension, les cryptomonnaies apparentées constituent bel et bien un type de monnaie. Plus particulièrement, nous verrons en quoi les innovations comme le bitcoin peuvent à la fois contribuer à accroître l'efficacité de notre système de paiement et poser des problèmes auxquels les décideurs devront s'attaquer.

Comme nous l'avons dit plus tôt, il existe des cas où la monnaie électronique centralisée possède tous les attributs d'une monnaie : elle peut servir de moyen d'échange, d'unité de compte et de réserve de valeur. Encore une fois, l'un des meilleurs exemples serait la carte Octopus utilisée à Hong Kong.

Mais qu'en est-il des monnaies électroniques décentralisées comme le bitcoin? Nous sommes d'avis que le bitcoin et les autres cryptomonnaies ne répondent pas tout à fait à la définition de la monnaie et ne remplissent pas ses fonctions, du moins pour le moment. Tout d'abord, pour que le bitcoin soit considéré comme une monnaie, il faudrait qu'il constitue un moyen d'échange généralement accepté. À cet égard, il présente un certain potentiel, mais il ne remplit pas encore toutes les conditions voulues.

Toutefois, il faut bien constater que le réseau Bitcoin permet bel et bien d'effectuer des virements entre utilisateurs. En outre, de plus en plus de détaillants, dont certains sont d'envergure mondiale, donnent l'option aux consommateurs de régler leurs achats en bitcoins. En faisant des recherches sommaires sur le Web, nous avons relevé entre 100 et 200 commerçants qui les acceptent au Canada. À l'échelle mondiale, d'après l'ensemble de nos sources, il serait possible de se procurer quelque 15 000 biens et services en payant avec des bitcoins. Cela dit, même si ces nombres semblent importants, ils ne le sont pas encore assez, à l'échelle de l'économie, pour convaincre la plupart des gens que le bitcoin constitue un moyen d'échange généralement accepté.

En ce qui concerne son aptitude à servir d'unité de compte, le bitcoin présente là aussi un certain potentiel, mais il n'est pas tout à fait à la hauteur. Même lorsque les bitcoins sont utilisés comme moyen d'échange, la valeur sous-jacente de la transaction semble toujours exprimée dans une monnaie nationale, comme le dollar américain ou canadien. Cette valeur est simplement convertie en bitcoins aux fins de la transaction.

C'est le cas chez la plupart des marchands qui se targuent d'accepter le bitcoin. En réalité, ils ne reçoivent que très rarement des paiements sous forme de cryptomonnaies, car ils font appel à des tierces parties qui les changent en monnaie nationale au moment de l'opération. BitPay, dont le siège est à Atlanta, est

company that offers such services is bitbay, an Atlanta-based company that provides the merchant with the option of accepting bitcoins but receiving the equivalent payment in state currency via bank transfer from bitbay.

Finally, when it comes to the store of value, here again we would argue that bitcoin falls short. The key reason is the variability of prices in terms of international currencies. For example, a recent report estimates the volatility of the value of bitcoin is about 108 per cent per year. In comparison, it's about 40 times greater than the volatility of the real value of a U.S. dollar.

To illustrate this, consider that in 2010, bitcoin traded at a third of a cent per bitcoin. It reached a high of about $1,200 in December. I checked this morning, and it now trades at about $430 per bitcoin. Imagine you're a merchant and you're receiving bitcoins for the good and services you provide your customers. You wouldn't know how much those bitcoins will be worth next week or next month. A typical merchant wouldn't be comfortable to accept a medium of exchange that varies in value so much.

There's an anecdote that illustrates this. An unfortunate soul in 2010 exchanged 10,000 bitcoins for two pizzas worth about $30 at the time, and the bitcoins were worth a third of a cent per bitcoin. In today's exchange rates, those 10,000 bitcoins would be worth $4.3 million, making those two pizzas really overpriced.

This volatility of bitcoin means that customers who store value in bitcoin are exposing themselves to a lot of variability and a great deal of risk in terms of what the savings could be worth, even in a relatively short period of time, like a week.

Because of these reasons, some would argue that crypto-currencies such as bitcoin are perhaps better understood and characterized as speculative investments rather than as a source of value worth a division of money. Some experts and some of our peers such as the Bank of England and Bank of Finland would suggest bitcoin is more similar to a commodity than a currency.

I want to spend a little more time on the store-of-value aspect, because the price volatility of bitcoin and other crypto-currencies signals an important difference between them and state currencies issued by banks. Many crypto-currencies have delegated the management of the money supply to algorithms. In bitcoin's case, the money supply is growing at a pre-specified rate. It will eventually level and remain constant forever after.

This fixed supply is at least partly responsible for the volatility of bitcoin in the presence of viable demand. In contrast, one of the key roles that central banks play is maintaining the price stability in terms of state currencies and specifically preventing price volatility of the type we are seeing in bitcoin.

l'une de ces sociétés qui permettent aux commerçants d'accepter en théorie les bitcoins, mais de recevoir en pratique des paiements en monnaie nationale par virement bancaire.

Finalement, le bitcoin ne saurait être considéré comme un instrument adéquat de réserve de valeur, principalement en raison de la forte variabilité de son cours par rapport aux monnaies nationales. Ainsi, un rapport récent estimait la volatilité du bitcoin à 108 p. 100 par année, ce qui est près de 40 fois plus élevé que le taux de variabilité associé à la valeur réelle du dollar américain.

Il est intéressant de noter, par exemple, que le bitcoin valait un tiers de cent en 2010, mais a atteint un sommet de plus de 1 200 $ en décembre dernier. Quand j'ai vérifié ce matin, le cours du bitcoin se situait aux alentours de 430 $. Imaginez un instant que vous êtes un marchand et que vous devez recevoir des paiements en bitcoins pour les biens et services que vous offrez. Vous ne sauriez pas combien cette monnaie vaudra dans quelques jours ou dans quelques semaines. Le marchand moyen est peu enclin à accepter un moyen d'échange dont la valeur est aussi volatile.

Une anecdote souvent évoquée à cet égard est celle du malheureux consommateur ayant déboursé 10 000 bitcoins en 2010 pour acheter deux pizzas qui coûtaient environ 30 $, puisque le bitcoin ne valait alors qu'un tiers de cent. Au taux de change d'aujourd'hui, les 10 000 bitcoins vaudraient 4,3 millions de dollars. Ces pizzas avaient donc été très chèrement payées!

Une telle volatilité signifie que les usagers qui se constituent des réserves de bitcoins sont susceptibles de voir leurs économies s'évaporer dans un laps de temps aussi court qu'une semaine.

Pour ces raisons, d'aucuns affirment que les cryptomonnaies telles que le bitcoin ressemblent davantage à des instruments de placement spéculatifs qu'à des réserves de valeur dignes d'être qualifiées de monnaies. De plus, certains experts et quelques-uns de nos homologues de la Banque d'Angleterre et de la Banque de Finlande avancent que le bitcoin constitue plus un bien qu'une devise.

Je voudrais consacrer un peu plus de temps à cet aspect de réserve de valeur, car la volatilité des cryptomonnaies met en évidence une importante différence qu'elles ont avec les monnaies nationales émises par des banques centrales. De nombreuses cryptomonnaies reposent sur un algorithme qui régule leur masse monétaire. Dans le cas du bitcoin, l'offre de monnaie augmente à un rythme préétabli qui finira un jour par devenir nul. La masse monétaire restera à jamais constante par la suite.

Il est probable que l'offre fixe est au moins en partie responsable de la forte fluctuation des cours. À l'opposé, l'une des principales responsabilités des banques centrales est d'assurer le maintien de la stabilité des prix exprimés en monnaie nationale, et plus particulièrement, de lutter contre le genre de volatilité qu'on observe dans le cas du bitcoin.

One of the tools that central banks have to achieve this goal is changing the supply of a state currency. This wouldn't be possible for bitcoin. Arguably, it was a feature that was attractive to some of the users of bitcoin, but we would argue it is a feature that has a negative consequence of contributing to price volatility. This volatility makes it difficult for bitcoin to be a reliable store of value and, consequently, a currency.

So if we argue that crypto-currencies at present don't really satisfy the key functions of money, why are they so popular? Why do we have them?

First, crypto-currencies may help reduce the cost of initial intermediation. Because they are decentralized, crypto-currencies sidestep the high cost of facilitating and processing electronic payments. That mediation is often expensive and too high for smaller-value payments to be processed, and this effectively limits the scope of e-commerce to higher-value transactions.

Another related feature that some consider positive is the irreversibility of payments. This allows crypto-currencies to look more like cash and allows merchants to accept payments for transactions without the risk that these transactions will be later reversed.

These two features, avoiding potentially costly intermediation and enforcing irreversibility of payments, could allow crypto-currencies and bitcoin, for example, to serve an important niche in the digital economy, and specifically for micropayments. Think about payments for individual songs over the internet or individual pictures. Such payments are too low to warrant merchants' investments in payment infrastructure or to justify the fees from existing instruments such as credit cards.

Finally, there's another feature of bitcoin's design that is attractive again, at least to some consumers, and that is the high degree of privacy, or to be technical, pseudonymity that bitcoin offers.

Transactions in bitcoin are publicly available, but at the same time, they do not reveal the transactor's true identity. Again, this feature was meant to make bitcoin more similar to cash and cater to consumers who value their privacy. However, as with cash, there are disadvantages of allowing such anonymity.

As we have seen, bitcoins can be stolen or defrauded from the owners. Moreover, the novel features of bitcoin, such as anonymity, irreversibility of transactions, makes it professionally attractive to people who are interested in, say, trading illicit substances or professional money laundering, particularly over the Internet.

L'un des moyens utilisés par les banques centrales pour atteindre cet objectif est justement de modifier l'offre de monnaie nationale, ce qui est impossible dans le cas du bitcoin. Bien que certains de ses adeptes y voient un avantage, la volatilité des cours est en fait un effet pervers de cette constance de l'offre. En somme, il est difficile de considérer le bitcoin comme une réserve de valeur fiable et, par voie de conséquence, comme une vraie monnaie.

Si les cryptomonnaies ne satisfont pas actuellement à notre définition de la monnaie, pourquoi sont-elles si populaires? Pourquoi existent-elles?

Tout d'abord, elles permettent de réduire les coûts liés à l'intermédiation financière. Comme elles sont décentralisées, les cryptomonnaies permettent d'éviter les frais, souvent élevés, associés au traitement des paiements électroniques. Le fait de passer par un intermédiaire coûte cher, parfois trop pour que les petites transactions soient rentables. Cela a pour effet de restreindre le commerce électronique aux opérations de grande valeur.

Le caractère irréversible des paiements est un autre attribut que certains considèrent comme un atout. Les transactions réglées en cryptomonnaies s'apparentent ainsi aux paiements en espèces, ce qui donne aux commerçants la garantie que les transactions ne risquent pas d'être annulées par la suite.

Ces deux caractéristiques — élimination potentielle d'un intermédiaire coûteux et irréversibilité des paiements — pourraient permettre à des cryptomonnaies comme le bitcoin de s'imposer dans un créneau important de l'économie numérique, à savoir les micropaiements. Songez par exemple aux paiements à effectuer pour télécharger une seule chanson ou une seule image sur Internet. Les sommes en cause sont trop petites pour que les commerçants jugent rentable d'investir dans une infrastructure de paiement ou de justifier les frais associés à l'utilisation d'instruments traditionnels comme les cartes de crédit.

Finalement, un autre attrait du bitcoin, du moins aux yeux de certains consommateurs, réside dans son caractère hautement confidentiel qui, dans le jargon technique de ce domaine, est appelé pseudonymat.

Les transactions en bitcoins sont publiques, mais la véritable identité des parties n'est jamais révélée. On a doté le bitcoin de cette caractéristique afin de renforcer sa similarité avec l'argent comptant et d'attirer les consommateurs pour qui la confidentialité est une priorité. Toutefois, comme c'est le cas avec les paiements en espèces, il y a un inconvénient à cet anonymat.

Comme nous l'avons vu, les détenteurs de bitcoins peuvent être victimes de vol ou de fraude. En outre, les caractéristiques novatrices du bitcoin — l'anonymat et l'irréversibilité des transactions — le rendent particulièrement attrayant dans le commerce de substances illicites ou le blanchiment d'argent, surtout sur Internet.

I believe our colleagues from the Department of Finance have already discussed some of these issues with you.

[*Translation*]

As I said earlier, bitcoin is the cryptocurrency we hear about the most often, but there are many others. Some of these have different features that try to improve perceived shortcomings, while others just copy the original formula under a different name.

I will give you a few examples. One such cryptocurrency, litecoin, was developed in 2011, largely based on bitcoin's specification. Some changes were introduced to try to improve the speed of transaction confirmation, the settlement, and the size of the total money supply was increased fourfold compared to the bitcoin. At present, litecoin is the second most popular cryptocurrency in terms of market capitalization.

A perhaps more interesting example is peercoin. This cryptocurrency is much less popular than bitcoin or litecoin, but it offers some distinctive new features. First, there is no hard limit on the total number of peercoins. Instead, the money supply will increase by one per cent per year. Second, the newly minted peercoins are partly awarded to users who do some particular tasks within the system, much as in bitcoin or litecoin, but also to existing holders of peercoin. Roughly speaking, if you hold one per cent of peercoins, your stake entitles you to one per cent of newly minted peercoins. You may perhaps think about this as a dividend accruing to existing stakeholders.

Finally, another cryptocurrency called the ripple, is a good example of how quickly e-money is developing and how fluid the concepts and definitions are. Ripple is based on technology similar to bitcoin, and thus is often referred to as a cryptocurrency. However, it is controlled by a third party, Ripple Labs, which issues the currency — in Bitcoin lingo, the ripple is pre-mined. Importantly, Ripple Labs refers to the ripple as a "payment system, currency exchange, and remittance network" rather than money as in a generally accepted means of payment. This payment system is meant to allow users to trade a range of currencies, including other cryptocurrencies, remit money, et cetera, making it more of an e-payment system than e-money, strictly speaking.

Beyond these few cryptocurrency examples, there are perhaps 200 others. Most of them have a relatively small consumer base, and a few are all but defunct after a brief spike of interest.

Je crois que nos collègues du ministère des Finances vous ont déjà parlé de certaines de ces questions.

[*Français*]

Comme je l'ai dit tantôt, le bitcoin est la cryptomonnaie dont on entend le plus parler, mais il en existe de nombreuses autres. Parfois celles-ci sont dotées de caractéristiques destinées à pallier certaines lacunes perçues de bitcoin. Parfois elles ne sont que des imitations de ce dernier auxquelles on a donné un nom différent.

Je vais vous en présenter quelques exemples. Le litecoin, créé en 2011, est une cryptomonnaie dont le fonctionnement s'inspire largement de celui du bitcoin. Des modifications ont toutefois été apportées au protocole original afin d'accélérer le processus de confirmation des transactions, le règlement. De plus, à terme, la masse monétaire totale du litecoin sera quatre fois plus élevée que celle du bitcoin. Pour l'heure, il s'agit de la deuxième cryptomonnaie en importance sur le marché.

Un autre exemple, peut-être plus intéressant encore, est celui du peercoin. Cette cryptomonnaie est beaucoup moins populaire que le bitcoin ou le litecoin, mais elle est dotée de caractéristiques uniques. D'abord, il n'y a pas de limite au nombre total de peercoins qui seront émis. Au contraire, l'offre de cette monnaie doit augmenter de 1 p. 100 chaque année. En outre, une partie des peercoins qui sont créés est remise aux participants qui accomplissent certaines tâches au sein du système, comme c'est le cas pour le bitcoin et le litecoin, mais aussi aux utilisateurs qui en possèdent déjà. En gros, si on détient, disons 1 p. 100 des peercoins existants, cela donne le droit de percevoir 1 p. 100 des peercoins nouvellement émis. On pourrait comparer cela aux dividendes versés à des actionnaires.

Finalement, mentionnons le cas du ripple, qui témoigne de la rapidité avec laquelle évoluent les monnaies électroniques et qui prouve à quel point les définitions et les concepts qui s'y rattachent sont fluides. Le ripple est fondé sur une technologie similaire à celle des bitcoins, ce qui fait qu'on le classe souvent parmi les cryptomonnaies. Toutefois, il est géré et émis par une entité centrale, Ripple Labs. Dans le jargon du bitcoin, on dirait donc que cette monnaie est pré-extraite. Il est intéressant de noter que le ripple est qualifié par son propre émetteur de système de paiement de plateforme de change et de réseaux destiné au virement de fonds plutôt que de monnaie au sens de moyen de paiement généralement accepté. Les utilisateurs peuvent s'en servir pour échanger diverses devises, y compris des cryptomonnaies, pour envoyer des fonds, et cetera. Cela le rapproche effectivement davantage d'un système de paiement que d'une monnaie électronique au sens strict du terme.

Ce ne sont là que quelques exemples. Il existerait environ 200 cryptomonnaies à l'heure actuelle. La plupart ne sont utilisées que par une poignée de consommateurs, et certains, après avoir jouit d'un engouement éphémère, les ont déjà abandonnées.

[*English*]

In closing, any discussion of e-money needs to take a balanced view of the weaknesses and potential risks of these innovations and economic benefits. These benefits arise from payment needs that e-money satisfies. As long as the needs are there, even if bitcoin or similar crypto-currencies ultimately fail, other payment innovations will rise to replace them.

One thing that history has shown us is that changing consumer needs, changing technology, will be reflected in innovations in payment systems. Such innovations may well be based on the technology that is similar to that underlying bitcoin. They may be implemented not only in a decentralized fashion like bitcoin but perhaps also incorporated into products or services offered by private companies or maybe even governments.

Now, the payment landscape is changing rapidly, both in Canada and around the world, with a number of innovations, participants and systems. At the Bank of Canada, we cannot predict the exact direction that this innovation will take. However, what we can do is assure the committee that we'll continue our efforts to monitor developments and assess implications. We will share our findings with Canadians through publications on our website.

Thank you very much.

The Chair: Thank you, Mr. Johnson and Mr. Pomorski, for your opening presentations. They were very helpful.

We have just over 35 minutes left for questions. I have a long list of questioners, so I will ask that you keep your questions sharp and to the point.

[*Translation*]

Senator Bellemare: Thank you for your presentation. As you know we began studying the bitcoin because we are interested in cryptocurrency. We understood that there were some differences, as you explained, between e-payment methods and cryptocurrency.

My question relates to conversion. As compared to other methods of payment, the innovation of the bitcoin and similar currencies is very much linked to the possibility of conversion, but at the same time that is what causes it to fluctuate, and that is what makes this currency very volatile.

We also see that this payment method is used quite a bit, with the globalization of e-commerce and Tesla, and we wonder why Tesla. Would a country that exports a lot of goods and would like to encourage global transactions have an interest in starting production and promoting digital money like bitcoins? It could be called something else and in a way offer a certain guarantee to

[*Traduction*]

Je dirai, pour conclure, que tout examen de la monnaie électronique doit faire la part tant des lacunes et des risques qui lui associés que des avantages économiques qu'elle peut apporter. Ces avantages deviennent manifestes lorsqu'une monnaie électronique contribue à satisfaire à des besoins en matière de paiement. Même si le bitcoin et les cryptomonnaies qui s'en inspirent finissent par disparaître, tant que ces besoins existent, d'autres moyens de paiement novateurs seront mis au point pour y répondre.

L'histoire a démontré que les besoins changeants des consommateurs et l'évolution de la technologie favorisent l'innovation dans le domaine des systèmes de paiement. Les prochaines nouveautés reposeront peut-être sur des technologies semblables à celles qui permettent au réseau Bitcoin de fonctionner. D'autres pourraient, en plus de jouer sur la décentralisation, s'intégrer aux produits et services offerts par des entreprises du secteur privé, voire du secteur public.

L'arrivée de nouveaux instruments, participants et systèmes transforme très rapidement l'univers des moyens de paiement au Canada et dans le monde entier. Même si la Banque du Canada n'est pas en mesure de prévoir l'orientation précise que prendront ces changements à l'avenir, nous pouvons vous assurer que son personnel continuera à surveiller attentivement leur évolution et à en évaluer les conséquences. La banque tiendra la population informée en publiant les résultats de ses recherches sur son site web.

Je vous remercie de votre attention.

Le président : Je vous remercie, monsieur Johnson et monsieur Pomorski, de vos exposés que nous avons trouvés très utiles.

Il nous reste un tout petit peu plus de 35 minutes pour les questions. Comme j'ai une longue liste de membres qui souhaitent intervenir, je vous prie d'être aussi concis que possible.

[*Français*]

La sénatrice Bellemare : Merci de votre présentation. Nous avons commencé, comme vous le savez, l'étude du bitcoin parce que nous sommes davantage intéressés à la cryptomonnaie. On a compris qu'il y avait des différences, comme vous l'avez expliqué, entre les modes de paiement électronique et la cryptomonnaie.

Ma question a trait à la convertibilité. Par rapport à d'autres modes de paiement, l'innovation du bitcoin et des monnaies semblables est beaucoup liée à la possibilité de conversion, mais en même temps c'est ce qui la fait fluctuer, et c'est ce qui rend la monnaie très volatile.

On voit aussi que ce mode de paiement est beaucoup utilisé, avec la mondialisation du commerce électronique et Tesla, et on se demande pourquoi Tesla. Un pays qui exporte beaucoup et qui voudrait encourager les transactions mondiales aurait-il intérêt à se lancer en affaires et à promouvoir la monnaie numérique comme les bitcoins? Cela pourrait porter un autre nom, et en

allow its convertibility and prevent the volatility of the currency. Is that something we could think about? And what do you think about it, as a representative of the Bank of Canada?

[*English*]

Mr. Johnson: I will make a couple of points. Generally, those countries that are active in global trade would support advances that make cross-border international payments faster, more secure and cheaper. That would tend to facilitate this.

I should stress that at this stage these methods of payment are largely person to person. Obviously, a lot of exporting is business to business with a reseller buying from a supplier — one business buying from another business to resell. There has been relatively little in the way of crypto-currency activity in that. Letters of credit are quite important for global trade. There's no credit in crypto-currencies, making trade difficult. A very good question about the price volatility, as Lukasz pointed out, is that at this stage it's one of the key things that stands to make bitcoin and other crypto-currencies not fully meet the definition of "money."

In order to mask the volatility, you would need to control the supply of the money. If you have a given supply of goods or a given level of economic activity that fluctuates and you want to keep the price level constant, the amount of money needs to fluctuate. I would say that the Bank of Canada and most other central banks have set an inflation target as a way to achieve that. We will manage the money supply, as such, and the interest rate to keep the value of the Canadian dollar relatively stable in terms of goods.

That is contrary to the very foundation of a crypto-currency with a fixed supply. As in bitcoin, that's impossible. By definition, if the level of economic activity in trade fluctuates but the supply of crypto-currency does not, you will have volatility. That's certain and significant.

[*Translation*]

Senator Bellemare: Do you not think that the speed of circulation of that currency could increase? Could we not see a situation where the speed of bitcoins might differ from the circulation rate of ordinary currency?

[*English*]

Mr. Johnson: Yes, it certainly could be, but not a monetary thirst. The velocity of money is extremely volatile and difficult to predict. It can move around rapidly and lead to large fluctuations in the relative price of goods in a certain currency. The price of

quelque sorte offrir une certaine garantie pour permettre sa convertibilité et empêcher la volatilité de la monnaie. Est-ce une chose à laquelle on pourrait penser? Et qu'en pensez-vous, en tant que personne associée à la Banque du Canada?

[*Traduction*]

M. Johnson : J'ai quelques observations à faire à ce sujet. D'une façon générale, les pays qui participent au commerce international sont en faveur des innovations qui peuvent accélérer les paiements transfrontaliers et en réduire le coût. Ce facteur tendrait à favoriser l'utilisation de telles monnaies.

J'insisterai cependant sur le fait que ces modes de paiement se limitent essentiellement aux transactions de personne à personne. Bien entendu, beaucoup d'exportations se font entre entreprises, un revendeur achetant des biens à un fournisseur. Autrement dit, une entreprise achète des biens à une autre pour les revendre. Toutefois, le recours aux cryptomonnaies est relativement rare dans ce domaine. En effet, les lettres de crédit jouent un rôle important dans le commerce international. Or la notion de crédit est absente dans le contexte des cryptomonnaies, ce qui rend leur utilisation difficile dans les échanges commerciaux. La volatilité des prix, comme l'a signalé Lukasz, constitue à ce stade l'un des principaux facteurs qui font que le bitcoin et les autres cryptomonnaies ne répondent pas pleinement à la définition d'une monnaie.

Pour atténuer la volatilité, il faudrait réguler l'offre. Pour une offre de biens et un niveau d'activité économique qui fluctuent, il est nécessaire de faire fluctuer l'offre de monnaie si on veut maintenir le prix constant. Ainsi, la Banque du Canada et la plupart des autres banques centrales se fixent un taux d'inflation cible comme moyen d'assurer la stabilité des prix. Nous gérons la masse monétaire et le taux d'intérêt pour que le pouvoir d'achat du dollar canadien reste relativement stable.

Cette façon d'agir est contraire au principe même des cryptomonnaies dotées d'une offre fixe. Dans le cas du bitcoin, la gestion de l'offre est impossible. Par définition, si le niveau d'activité commerciale fluctue, mais que l'offre de cryptomonnaies reste fixe, les prix seront nécessairement instables. Cela est certain, et c'est un facteur important.

[*Français*]

La sénatrice Bellemare : Vous ne pensez pas que la vitesse de circulation de la monnaie pourrait augmenter? La vitesse des bitcoins ne pourrait-elle pas différer de la vitesse de circulation de la monnaie régulière?

[*Traduction*]

M. Johnson : Oui, cela peut certainement arriver sans pour autant entraîner une soif monétaire. La vitesse de l'argent est très instable et très difficile à prédire. L'argent peut circuler rapidement et provoquer de fortes fluctuations du prix relatif

goods denominated in bitcoin is extremely volatile, and part of that would be rapid changes in the velocity.

Mr. Pomorski: I would add to that. I would always try to look at the underlying economic needs that the currency might serve. I agree with you that perhaps the greatest needs are actually at the level of remittances or sending money abroad. To the extent that people are not satisfied with the current offering of economic services, they might gravitate to services such as crypto-currencies. To the extent that crypto-currencies can provide lower fees for these services, they might be adopted eventually.

I want to make two points that I think are important. First, if you develop a system to cater to this need for remittances, then this is more a payment system than a currency. You're not issuing a currency; you're providing a service for this particular need. In fact, one of the examples that I mentioned was ripple. The designers of that system were specifically identifying the area of international remittances as one of the key features of their business model. At the same time, they were very clear that what they have is not currency; it is not money. They provide a way to send money abroad cheaply, maybe more cheaply than other methods. In this sense, I think similar innovations may have a role, but it wouldn't be a role of currency.

[*Translation*]

Senator Hervieux-Payette: You spoke earlier about M-Pesa in Africa, and about Octopus, in Japan. You say that this method is used by countries that have a less developed system. Can you tell us more about that? What do you mean by a less developed system?

Mr. Johnson: Could you repeat that question?

Senator Hervieux-Payette: In your presentation you talked about a system in Africa that is called M-Pesa and about a system in Japan that is called Octopus. You say that this method of payment or transaction is more useful for less developed systems. Less developed as compared to what? We have a developed system and so we would not need it, whereas other systems could benefit? Could you explain to us where we are located in that system, developed or not.

[*English*]

Mr. Johnson: We referred to systems. Canada is a very good example in this regard of a country with a very well-developed payment system with technology that is provided by major institutions. It is very good. I don't know the number exactly but a huge percentage of Canadians are what we call "banked," i.e. they have bank accounts with large institutions. When you're banked, you have things like debit cards, credit cards and this method of payment.

des biens dans une devise donnée. Exprimé en bitcoins, le prix des biens peut être extrêmement volatile, cela étant attribuable en partie à des fluctuations rapides de la vitesse.

M. Pomorski : J'ajouterai une chose. Je pense toujours aux besoins économiques sous-jacents auxquels une monnaie peut satisfaire. Je conviens avec vous que le plus grand besoin se situe dans le domaine des envois de fonds et des virements à l'étranger. Si les gens ne sont pas satisfaits des services actuellement offerts, ils peuvent s'orienter vers des services tels que les cryptomonnaies. Et, dans la mesure où celles-ci permettent d'obtenir les services voulus à un prix moindre, elles sont susceptibles d'être adoptées un jour.

Je voudrais insister sur deux points que je crois importants. Premièrement, si on met en place un système permettant de satisfaire à ce besoin de virements, il s'agit alors davantage d'un système de paiement que d'une monnaie. On n'émet pas une monnaie, on dispense plutôt un service répondant à un besoin particulier. J'ai en fait mentionné à cet égard l'exemple de ripple. Les concepteurs de ce système ont clairement fait des virements internationaux un aspect essentiel de leur modèle commercial. En même temps, ils ont explicitement dit que ripple n'est pas une devise ou de l'argent. Ils offrent un moyen peu coûteux d'envoyer de l'argent à l'étranger, un moyen moins cher que les autres. Dans ce sens, je crois que les innovations semblables peuvent jouer un rôle, mais ce n'est pas celui d'une monnaie.

[*Français*]

La sénatrice Hervieux-Payette : Vous avez parlé plus tôt de M-Pesa, en Afrique, et d'Octopus, au Japon. Vous dites que ce moyen serait utilisé par des pays qui ont un système moins développé. Pouvez-vous nous en dire davantage là-dessus? Qu'entendez-vous par système moins développé?

M. Johnson : Est-ce que vous pourriez répéter?

La sénatrice Hervieux-Payette : Dans votre présentation vous parlez d'un système en Afrique qui s'appelle M-Pesa et d'un système au Japon qui s'appelle Octopus. Vous dites que ce mode de paiement ou de transaction serait plus utile pour les systèmes moins développés. Par rapport à qui et par rapport à quoi? Nous, qui avons un système développé, nous n'en aurions pas besoin, alors que d'autres systèmes en bénéficieraient? Expliquez-moi où vous vous situez dans ce système, développé ou pas.

[*Traduction*]

M. Johnson : Vous avez parlé de systèmes. À cet égard, le Canada est un excellent exemple de pays ayant un système de paiement très développé grâce à la technologie fournie par les grandes institutions. C'est un très bon système. Je ne connais pas le nombre exact, mais un énorme pourcentage de Canadiens ont un compte dans une grande institution financière. Ils disposent donc de choses telles que des cartes de débit et de crédit ainsi que des méthodes de paiement correspondantes.

In Africa, for example, a very small percentage of the population has a bank account. A payment system such as M-pesa helps to accommodate in that you don't need a bank account. You can load monetary value on M-pesa and use that as a means of exchange.

I mentioned the tools that give access to your demand deposit to exchange. If you do not have a demand deposit, if you're in a country that's not well banked, an access tool does you no good; so you need a store of monetary value.

As for the Octopus card, I'll turn to Lukasz.

Mr. Pomorski: The point I was making is that the Octopus card was designed specifically for the mass transit system. Within a few years, it gained widespread adoption across a variety of retail establishments, not only transit. Since then, there were two similar innovations, one in the U.K. with the Oyster card, and one in Canada with the PRESTO card. Technologically, they are very similar. You can store value on them and potentially use the value not only for rides on a transit system but also for purchases.

Somehow in Hong Kong these cards became used for a variety of purposes, but in both the U.K. and Canada they haven't and are used almost exclusively for transport. I would interpret it this way: As Grahame said, we already have a payment system that caters to the needs that such cards might satisfy. For example, debit and credit cards allow you to pay for coffee or a newspaper in the blink of an eye. Perhaps in Hong Kong those new devices were competing for people looking for this convenience, whereas in Canada that niche was already filled.

Senator Hervieux-Payette: People pay for the transportation card in Canada. This is what we use for a monthly transit pass. Money is involved in that.

Mr. Pomorski: I agree. The key difference is that we're using a PRESTO card only for this one use. I would go back to the defining feature of money as being "generally accepted." If you're using this card for only one service, I wouldn't call it money. In Hong Kong, it's actually used for a broad range of services.

As other examples, we could talk about stored value cards issued by Bridgehead or Starbucks. These cards are used exclusively to buy coffee or whatever else you buy at Bridgehead or Starbucks. They're not used outside the chain.

En Afrique, par exemple, le pourcentage de la population qui a un compte en banque est très faible. Un système de paiement comme M-Pesa est très commode parce que ses utilisateurs n'ont pas besoin d'un compte bancaire. Il leur suffit de charger un certain montant dans leur carte pour pouvoir l'utiliser comme moyen d'échange.

J'ai parlé des moyens qui donnent accès à un dépôt à vue à des fins d'échange. Si on n'a pas un dépôt à vue, si on se trouve dans un pays où peu de gens ont un compte bancaire, un moyen d'accès n'est pas très utile. Il est alors préférable d'avoir une réserve de valeur.

Pour ce qui est de la carte Octopus, je vais laisser Lukasz vous répondre.

M. Pomorski : Comme je l'ai mentionné, la carte Octopus a été spécialement conçue pour les transports en commun. En quelques années, elle a été adoptée par un grand nombre de commerces de détail de toutes sortes. Depuis, deux innovations du même genre sont apparues, d'une part, au Royaume-Uni, avec la carte Oyster et, de l'autre, au Canada avec la carte PRESTO. Sur le plan technique, elles sont très semblables. Elles servent de réserve de valeur : on y stocke de l'argent dont on se sert ensuite non seulement pour utiliser les transports en commun, mais aussi pour faire des achats dans différents commerces.

D'une façon ou d'une autre, la carte Octopus s'est étendue à beaucoup de domaines autres que le transport, tandis que les cartes équivalentes du Royaume-Uni et du Canada ne l'ont pas fait, de sorte qu'elles sont presque exclusivement limitées aux transports. Mon interprétation est la suivante : comme Grahame l'a dit, nous avons déjà un système de paiement qui répond aux besoins que pourraient satisfaire de telles cartes. Par exemple, nos cartes de débit et de crédit nous permettent d'acheter du café ou un journal en un clin d'œil. Il est possible qu'à Hong Kong, ces nouveaux dispositifs aient répondu aux besoins de gens qui étaient à la recherche d'un moyen de paiement commode tandis qu'au Canada, ce créneau était déjà occupé.

La sénatrice Hervieux-Payette : Les gens paient au Canada pour avoir une carte de transport, c'est-à-dire pour l'abonnement mensuel aux transports en commun. L'argent entre en jeu dans ce cas.

M. Pomorski : Je suis bien d'accord. La grande différence, c'est que nous utilisons la carte PRESTO exclusivement à cette fin. Je reviens à la définition de l'argent selon laquelle il est « généralement accepté ». Si on n'utilise cette carte que pour un service unique, elle n'aurait pas, pour moi, les caractéristiques de l'argent. À Hong Kong, la carte Octopus permet d'obtenir toute une gamme de services.

Il y a d'autres exemples : les cartes Bridgehead et Starbucks à valeur stockée. Ces cartes servent exclusivement à l'achat de café ou de tout autre produit vendu par Bridgehead ou Starbucks. Chacune n'est utilisable que dans sa propre chaîne.

Air Miles can be used for a variety of services, in particular for airplanes but also for goods specifically from one provider. You cannot take your Air Miles card and go to Walmart to buy goods. Because of this, the Air Miles card would not qualify as money. These cards are not generally accepted means of payment.

Senator Black: You've been very helpful in advancing our study. My line of questioning this afternoon will focus on opportunities that might flow from this innovation. I would start by asking if you would agree with me that bitcoin is an innovation, not the endgame.

Mr. Johnson: Yes, I would agree with that. I think we would agree with that.

Senator Black: And you would agree as well?

Mr. Pomorski: Yes.

Senator Black: From that point of view, then, how might we in Canada — and we will get specifically to your role in my next question — be able to harness the positive aspects of these currencies while mitigating downfalls? Can you offer your views on that, please?

Mr. Johnson: Again, coming back to a distinction we made in the opening remarks and one Lukasz made, to use bitcoin as an example, there's a difference between the big "B" Bitcoin which is the network. That is, this underlying technology that allows verifiable payments without a trusted third party to go very cheaply, which really was quite a material breakthrough in computer science, in my understanding at least. Then there is small "b" bitcoin, which is the currency that it uses right now.

I think there's no doubt that the payment system technology underlying this was a material advance, as you said, senator. It is an advance; it is not the endgame. It showed that what seemed to be unsolvable isn't, so there will be more work done on this. In terms of payment system efficiency, absolutely these are good advancements.

The question of how you harness it, while at the same time protecting people, is one that, quite frankly, we will spend a lot of time on. We have not really formed solid opinions on that. To date, it is largely a consumer protection education aspect — even the education of the volatility of the underlying currency. The price is volatile and it is not broadly accepted. As I said, that seems to be the biggest issue right now. Quite frankly, it is something that falls outside of the Bank of Canada's mandate. Again, we will advance our research on this.

Senator Black: A work-in-progress?

Mr. Johnson: A work-in-progress, much like the system itself.

La carte Air Miles permet d'accéder à une gamme de services, notamment le transport aérien, mais aussi à des produits vendus par un seul fournisseur. Elle ne pourrait pas servir à faire des achats chez Walmart, par exemple. Pour cette raison, la carte Air Miles ne répond pas à la définition de l'argent. Ce n'est pas un moyen de paiement généralement accepté.

Le sénateur Black : Vous nous avez beaucoup aidés à avancer dans notre étude. Cet après-midi, mes questions porteront sur les perspectives que peut ouvrir cette innovation. Je vais commencer par vous demander si vous êtes d'accord avec moi que le bitcoin est une innovation et non un produit fini.

M. Johnson : Oui, je suis d'accord avec vous.

Le sénateur Black : Est-ce que vous êtes d'accord vous aussi?

M. Pomorski : Oui.

Le sénateur Black : Cela étant, comment pouvons-nous au Canada — j'en viendrai plus précisément à votre rôle dans ma prochaine question — tirer parti des aspects positifs de ces monnaies tout en en atténuant les inconvénients? Pouvez-vous me donner votre point de vue à ce sujet?

M. Johnson : Je reviendrai encore une fois à une distinction que nous avons faite dans les exposés préliminaires, Lukasz et moi. Dans le cas du bitcoin, par exemple, il y a une différence entre Bitcoin avec un grand « B », qui désigne le réseau, et bitcoin avec un petit « b », qui désigne la monnaie. Le réseau Bitcoin comprend une technologie sous-jacente qui permet de faire des paiements vérifiables à très bas prix sans l'intervention d'une tierce partie fiable. Cela représente une importante percée technologique en informatique, du moins à mon sens. Le bitcoin avec un petit « b » est la devise actuellement utilisée sur ce réseau.

Il n'y a pas de doute que la technologie de paiement mise en œuvre sur le réseau Bitcoin constitue un important progrès, comme vous l'avez dit, sénateur. C'est un progrès et non un produit fini. Cette technologie nous a montré que ce qui semblait impossible ne l'était pas. Par conséquent, d'autres travaux seront réalisés dans ce domaine. Pour ce qui est de l'efficacité du système de paiement, il est indubitable que cette technologie représente un progrès considérable.

En toute franchise, la question de savoir comment en tirer parti tout en protégeant les gens nous occupera longtemps encore. Nous n'avons pas d'opinion arrêtée à ce sujet. Jusqu'ici, il s'agit essentiellement d'éduquer les consommateurs quant à la volatilité de la monnaie, dont le prix est instable et qui n'est pas largement acceptée. Comme je l'ai dit, c'est probablement la plus importante question qui se pose actuellement. Et, pour être franc, je dirai que cela ne fait pas partie du mandat de la Banque du Canada. Nous continuerons cependant à faire des recherches dans ce domaine.

Le sénateur Black : C'est donc un travail en cours?

M. Johnson : Oui, un travail en cours, comme c'est le cas du système lui-même.

Senator Black: Absolutely, and that's appropriate.

Can you see a circumstance where the Bank of Canada would issue e-money?

Mr. Johnson: There is a question. The Bank of Canada issues Canadian dollars under the Currency Act. That is the legal tender of the Government of Canada and the Bank of Canada is the sole issuer of that, so we issue Canadian dollars.

Under the current legal act, we couldn't issue another currency. In terms of a digital currency, it is not under the current legal framework.

The e-money or e-payment system is different. We currently do not. We could have made the decision to offer demand accounts to Canadians, which we did not. We could have made the decision to offer debit cards for those demand accounts to Canadians, which we did not. The decision, well before either of our times, was clearly that this level of innovation and scale and customer service was best left to the private sector in an appropriate regulatory framework. I think that has served Canadians very well, going back to the fact that we have not seen a lot of this sort of Octopus card or M-pesa. Canadians are well-served by their payment system technologies now.

Senator Black: Are you shutting the door to the question?

Mr. Johnson: No. Again, as I said in my opening statement, one of the key questions we're looking at is this: What is the role of the central bank?

Senator Black: I'm advised that there is something called MintChip.

Mr. Johnson: A great name; mint cookie.

Senator Black: I'm told the MintChip is being developed by the Royal Canadian Mint as a digital currency backed by the government. Can you comment?

Mr. Johnson: I would actually defer that to the Mint.

Senator Black: You would as well?

Mr. Pomorski: I also would defer that comment. I can tell you that we are in communication with our colleagues at the Mint who are working on this, or working on this innovation, but I would be out of line if I were to comment on this on behalf of the government.

Senator Black: Are my researchers close to right? Do you understand that that might be the case?

Mr. Pomorski: In terms of the product that was being developed, it was essentially a centralized e-money development similar to the ones that I was talking about in my presentation; so you're right. This is one of the examples of where an institution might go in issuing e-money.

Le sénateur Black : Absolument. C'est préférable ainsi.

Y a-t-il une circonstance quelconque qui pourrait amener la Banque du Canada à émettre de l'argent électronique?

M. Johnson : C'est une bonne question. La Banque du Canada émet des dollars canadiens en vertu de la Loi sur la monnaie. Le dollar est la monnaie légale du gouvernement du Canada, et la Banque du Canada en est l'émetteur exclusif.

En vertu de la loi actuelle, nous ne pourrions pas émettre une autre monnaie. Une monnaie électronique ne s'inscrirait pas dans le cadre législatif actuel.

Le système de paiement électronique constitue un cas différent. À l'heure actuelle, nous ne nous en occupons pas. Nous aurions pu prendre la décision d'offrir aux Canadiens des comptes de dépôt à vue, mais nous ne l'avons pas fait. Nous aurions pu décider d'offrir des cartes de débit associées à de tels comptes. Encore une fois, nous ne l'avons pas fait. La décision, qui a été prise bien avant notre temps à tous les deux, visait clairement à laisser au secteur privé ce niveau d'innovation et de service à la clientèle, dans le cadre d'un ensemble de règles appropriées. Je crois que cette façon de faire a permis de très bien servir les Canadiens, comme en témoigne l'absence chez nous de cartes du genre Octopus et M-Pesa. Les Canadiens sont bien servis par les technologies de leur système de paiement actuel.

Le sénateur Black : Fermez-vous la porte à cette possibilité?

M. Johnson : Non. Encore une fois, comme je l'ai dit dans mon exposé préliminaire, l'une des grandes questions que nous nous posons concerne le rôle de la Banque du Canada.

Le sénateur Black : On me parle de quelque chose qui porte le nom de Cybermonnaie ou MintChip.

M. Johnson : Excellent nom. Cela fait penser aux biscuits à la menthe.

Le sénateur Black : On me dit que la Cybermonnaie est mise au point par la Monnaie royale canadienne à titre de monnaie électronique soutenue par le gouvernement. Qu'avez-vous à dire à ce sujet?

M. Johnson : Je crois que je laisserai la Monnaie royale répondre à cette question.

Le sénateur Black : C'est la même chose pour vous?

M. Pomorski : Oui. Je peux vous dire que nous sommes en contact avec nos collègues de la Monnaie royale qui travaillent sur ce projet ou cette innovation, mais je n'aurais sûrement pas assez de temps pour parler de cette question au nom du gouvernement.

Le sénateur Black : Nos analystes auraient-ils raison? Croyez-vous que cela pourrait se faire?

M. Pomorski : Le produit mis au point consiste essentiellement en une monnaie électronique centralisée semblable à celles dont j'ai parlé dans mon exposé. Vous avez donc raison. C'est un exemple d'organisme gouvernemental qui pourrait s'occuper de l'émission d'une monnaie électronique.

Senator Black: Where Canada might go?

Mr. Pomorski: Yes, where Canada might go. It's certainly a possibility. It has been evaluated by the Mint, but again I will stop short.

Senator Black: I understand.

The Chair: That's a very good try, senator.

Senator Massicotte: Senator Black, in the last statement you sounded like a journalist trying to pry something out of somebody.

[*Translation*]

We are not experts, and several of our discussions are aimed at allowing us to learn a bit more about the nature of bitcoins and that type of currency. According to what I have read, I am convinced that this can never become the national currency. If only in terms of monetary policy, why would the government lose control over one monetary policy?

As a currency, as a means of exchange, does it have any usefulness? There are a lot of them in circulation. We are told that it costs very little from the point of view of issuing the technological message, but it has to be purchased from an exchange and that currency has to be used to purchase a product; it costs something. If you buy the currency from someone, it is relatively expensive; I checked that out this afternoon. And when you add that fee to the product, there are so many variations in its value that you may think you are saving money, but on the contrary, you have paid 5 per cent or 10 per cent more because it is not recognized, and you do not know that. And, there is something else, regarding the high degree of privacy; we were advised that that is not the case. As with Internet, you can check. So what is its future utility? It is popular currently, there is a way of marketing it to suppliers, but what is our role? Do the government and the Bank of Canada have a moral obligation to protect those who own some? What are your comments on that?

[*English*]

Mr. Johnson: I think we both said that, in any area, looking into the future is extremely difficult, especially one this rapidly changing.

You make a good point about the importance that governments place on maintaining control over money. It's a very valuable tool. Obviously, for the Bank of Canada it is a very valuable tool for economic management.

In terms of the utility that bitcoin brings, I would again distinguish between the big "B" Bitcoin payment system and the small "b" currency. As we have seen, payment systems evolve over time. They generally allow for transactions to take place simpler, faster and cheaper and there continues to be a progression along that. This is clearly a step along this road. The transactions are quite quick, reversible and can be done much more cheaply than in a lot of other areas that use trusted third party providers. That may well be the most fertile ground for

Le sénateur Black : Le Canada s'y prêterait?

M. Pomorski : Oui. C'est certainement une possibilité. La Monnaie royale a procédé à une évaluation, mais, encore une fois, je préfère ne pas en dire davantage.

Le sénateur Black : Je comprends.

Le président : Très bonne tentative, sénateur.

Le sénateur Massicotte : Sénateur Black, dans votre dernière intervention, vous aviez l'air d'un journaliste à l'affût d'une nouvelle.

[*Français*]

Nous ne sommes pas des experts et plusieurs de nos discussions visent à nous permettre d'apprendre un peu ce que sont les bitcoins et ces devises-là. D'après ma lecture, je suis convaincu que cela ne peut jamais devenir la devise nationale. Juste en termes de politiques monétaires, pourquoi le gouvernement perdrait le contrôle sur une politique monétaire?

Comme devise, comme moyen d'échange, y a-t-il une utilité? C'est quand même desservi par un tirage important. On dit que cela coûte très peu au point de vue de l'émission du message technologique, mais il faut l'acheter d'un échangeur et il faut se servir de cette devise pour acheter un produit, cela coûte quelque chose : quelqu'un qui vous vend la devise, cela coûte relativement cher, je l'ai vérifié cet après-midi. Et quand on l'ajoute au produit, il y a tellement de variations du prix que l'on pense sauver de l'argent, mais au contraire, on a payé 5 ou 10 p. 100 plus cher parce que ce n'est pas reconnu, et on ne le sait pas. Et autre chose, quand on parle de *high degree of privacy*, on nous a avisés que ce n'est pas le cas. Comme on l'a fait avec Internet, on peut vérifier. Quelle est l'utilité future? En ce moment, c'est populaire, il y a un moyen de marketing auprès des fournisseurs. Mais quel est notre rôle? Le gouvernement et la Banque du Canada ont-ils une obligation morale de protéger ceux qui en possèdent? Quels sont vos commentaires?

[*Traduction*]

M. Johnson : Nous avons dit tous les deux que, dans n'importe quel domaine, il est extrêmement difficile de prévoir l'avenir, surtout en présence d'une évolution aussi rapide.

Vous avez noté avec raison l'importance que les gouvernements accordent au contrôle de la masse monétaire. C'est un outil précieux. De toute évidence, c'est un outil inappréciable de gestion économique pour la Banque du Canada.

Pour ce qui est de l'utilité du bitcoin, je rappellerai une fois de plus la distinction à faire entre le système de paiement Bitcoin avec un grand « B » et le bitcoin avec un petit « b ». Comme nous l'avons vu, les systèmes de paiement évoluent avec le temps : les transactions deviennent plus simples, plus rapides et moins coûteuses et des progrès sont réalisés à cet égard. C'est certainement un pas franchi sur cette voie. Les transactions sont assez rapides, sont réversibles et peuvent être beaucoup moins coûteuses que dans beaucoup d'autres domaines régis par des

future work here. What you said about the price volatility making it difficult as a means of exchange is very true. Lukasz's example of the $6 million pizza is a good one.

I'll turn to Lukasz in a second, but one reads and hears about these 15,000 merchants, or however many, that accept bitcoins. But they don't really. They accept it and then instantly turn it into a national currency, such as a U.S. dollar, a euro or a Canadian dollar, for exactly the reason that you said, sir: There's zero interest in holding this for even a day because of it.

In effect, people can use the Bitcoin payment network by waiting until the very last minute. You go online, you wish to purchase something, you wait until the very last minute to buy your bitcoin, immediately pay with it, and the vendor immediately turns it back into Canadian or U.S. dollars. You've used the big "B" Bitcoin network and minimized your exposure to the small "b" bitcoin currency, which again is a possibility.

We don't have a crystal ball, but these are some of the potential advantages the system offers.

Senator Massicotte: I'm not optimistic on the small "b" bitcoin. It's probably because I don't understand it. I agree the technology is phenomenal. It probably could be used for registration of other assets or even real estate. But in a small "b" sense, I don't see much of a future. Also, my reading is that 80 per cent of the holders are speculators. It's more of a commodity than a currency. As you know, income tax wise —

Mr. Johnson: And some have used it that way.

Senator Massicotte: The U.S. and Canada are saying that exactly: It's a prop.

Having said that, do we have a responsibility as a government to deflate this balloon, like China? What do we do? I think Senator Tkachuk said last week that if 80 per cent are speculators, they have a right to. Why should we care? Why should we try to protect anybody? It's "buyer beware." People know it's a highly variable currency, so maybe there is no role for the government other than to say, "Be very cautious; be careful."

Mr. Johnson: Financial consumer education is an important role. Much of the interest in bitcoin in the early adoption was — and I know this was covered in previous sessions — a sort of libertarian view of "get away from state currencies." Once it started to move, much of the interest did become speculative.

tierces parties fiables. C'est là que réside le terrain le plus fertile pour l'avenir. Vous avez dit que l'instabilité du prix fait qu'il est difficile de s'en servir comme moyen d'échange. Vous avez bien raison. L'exemple de la pizza à 6 millions de dollars donné par Lukasz le prouve bien.

Je céderai la parole à Lukasz dans un instant, mais je voudrais dire d'abord qu'on entend parler des quelque 15 000 commerces qui acceptent le bitcoin. En réalité, ce n'est pas vrai. Ils l'acceptent, puis l'échangent immédiatement contre une devise nationale telle que le dollar américain, l'euro ou le dollar canadien, exactement pour la raison que vous venez de mentionner, monsieur : ils n'ont absolument aucun intérêt à le garder, ne serait-ce qu'un seul jour.

En effet, les gens peuvent utiliser le réseau de paiement Bitcoin en attendant jusqu'à la dernière minute. S'ils doivent acheter quelque chose, ils vont sur Internet, attendent jusqu'à la dernière minute pour acheter des bitcoins, s'en servent immédiatement pour payer leur achat, après quoi le vendeur convertit immédiatement sa recette en dollars canadiens ou américains. Ainsi, les gens utilisent le réseau Bitcoin avec un grand « B », mais minimisent leur exposition au bitcoin avec un petit « b ». C'est encore une possibilité.

Nous n'avons pas une boule de cristal, mais ce sont là quelques-uns des avantages possibles du système.

Le sénateur Massicotte : Je ne suis pas très optimiste au sujet du bitcoin avec un petit « b ». C'est probablement parce que je ne le comprends pas. Je suis bien d'accord que la technologie est phénoménale. On pourrait sans doute s'en servir pour l'enregistrement d'autres éléments d'actif ou même de biens immobiliers. Toutefois, je ne vois vraiment pas d'avenir pour le bitcoin avec un petit « b ». De plus, d'après mes lectures, 80 p. 100 de ceux qui en détiennent seraient des spéculateurs. C'est donc plus un bien qu'une devise. Comme vous le savez, dans une optique d'impôt sur le revenu...

M. Johnson : Il y en a effectivement qui s'en sont servis de cette façon.

Le sénateur Massicotte : Les États-Unis et le Canada disent exactement cela : ce n'est qu'un accessoire.

Cela dit, le gouvernement a-t-il la responsabilité de faire éclater ce ballon comme la Chine? Que devons-nous faire? Le sénateur Tkachuk a dit la semaine dernière, je crois, que même si 80 p. 100 des détenteurs sont des spéculateurs, ils ont le droit de spéculer. Pourquoi faudrait-il s'en soucier? Pourquoi nous chargerions-nous de protéger quiconque? C'est un marché pour acheteurs avertis. Les gens savent que c'est une monnaie hautement instable. Peut-être le gouvernement n'a-t-il aucun rôle à jouer, à part dire aux gens : « Faites attention et prenez vos précautions. »

M. Johnson : L'éducation financière des consommateurs est un rôle important. Initialement, l'intérêt suscité par le bitcoin — je sais que vous en avez entendu parler au cours de séance précédente — était pour une grande part attribuable à une vision libertaire tendant à s'écarter des devises nationales. Une

There is nothing wrong with speculation, and I don't think it's the role of the government to protect anyone from known speculation.

There is an important role of consumer protection at this stage. It is at least portrayed as a currency, so perhaps it needs to be made clear that this is not Canadian currency and the Canadian Deposit Insurance Corporation does not stand behind this; you're not in a bank. Consumer education has a role.

From the Bank of Canada's view in terms of economic and systemic risks, it's far too small. The amount of bitcoins in Canada is far too small to be economically or systemically important at this stage. That doesn't mean it won't become that way. Again, my point is that this is a work-in-progress; this will evolve. If it gets several orders of magnitude bigger, would the story change? Potentially, yes, and it again speaks to the fact that we're following this closely, and it's an activity research agenda item.

The Chair: Are there further questions?

Senator Campbell: Do you think we would be even looking at this if there hadn't been Silk Road? It sort of captured our attention. It has all the makings of a great spy movie, but do you really think we would be here if it wasn't for that?

Mr. Johnson: That's a very good question. Certainly the backstory behind bitcoin is fascinating, with the "Dread Pirate Roberts," the guy who ran Silk Road. Even with Mt. Gox and the subsequent collapse there, the backstory is interesting and certainly makes for good journalistic coverage. It has accelerated.

Would we be looking at it? We certainly would. The Bank of Canada held a conference on e-money two years ago, before bitcoin was really in the common lexicon. This is a material advance in money and payment systems, and it's something we need to understand. The Bank of Canada has a currency department. We have been studying alternative means of payment for 30 years, probably even longer.

I had comments about the risks to the bank of demand for cash falling off precipitously and that this would have impacts on the Bank of Canada's balance sheet, which would have knock-on effects. These worries existed when credit cards came out and then when debit cards came out. You could look at it and wonder if everyone has a credit card and debit card, wouldn't the demand

fois que le mouvement du bitcoin a pris de l'ampleur, ce sont surtout les spéculateurs qui s'y sont intéressés. Il n'y a rien de mal à spéculer, et je ne crois pas que le gouvernement ait un rôle à jouer pour protéger quiconque se livre ouvertement à la spéculation.

À ce stade cependant, il y a un important rôle à jouer pour protéger les consommateurs. Le bitcoin est une devise, du moins en apparence. Par conséquent, il importe de dire clairement aux gens que le bitcoin n'est pas une devise canadienne, qu'il n'est pas protégé par la Société d'assurance-dépôts du Canada et que ceux qui en achètent n'ont pas affaire à une banque. La sensibilisation des consommateurs est importante.

Quant aux risques économiques et systémiques, le volume des transactions est beaucoup trop petit pour que la Banque du Canada s'en inquiète. À l'heure actuelle, il y a bien trop peu de bitcoins au Canada pour qu'ils puissent influer sur l'économie et les systèmes. Cela ne veut pas dire que les risques ne sont pas susceptibles de s'intensifier à l'avenir. Je répète encore une fois que c'est une affaire en cours qui évoluera avec le temps. Si le volume devait augmenter de plusieurs ordres de grandeur, y aurait-il lieu de s'inquiéter? Peut-être bien. Cela explique nos efforts pour suivre de très près cette évolution. C'est un sujet actif dans notre programme de recherche.

Le président : Y a-t-il d'autres questions?

Le sénateur Campbell : Croyez-vous que nous aurions quand même entrepris cette étude si Silk Road n'avait pas existé? Cette affaire a retenu notre attention. Elle présente toutes les caractéristiques d'un excellent film d'espionnage, mais croyez-vous vraiment que nous serions ici indépendamment de Silk Road?

M. Johnson : C'est une très bonne question. Il n'y a pas de doute que les dessous du bitcoin sont fascinants, de même que cet homme, Dread Pirate Roberts, qui dirigeait le Silk Road. Même si on se limite à Mt. Gox et à l'effondrement qui s'est produit là-bas, le contexte est intéressant, suffisamment pour susciter l'intérêt des journalistes. Et cet intérêt ne fait qu'augmenter.

Aurions-nous étudié ce phénomène autrement? Sans le moindre doute. La Banque du Canada a organisé une conférence sur la monnaie électronique, il y a deux ans, avant que le bitcoin ne soit vraiment entré dans le vocabulaire courant. Le phénomène se fonde sur des progrès considérables des systèmes monétaires et de paiement que nous devons bien comprendre. La Banque du Canada a un service responsable de la monnaie. Nous étudions les différents moyens de paiement depuis 30 ans ou plus.

J'ai parlé tout à l'heure du risque que présenterait pour la banque une diminution brusque et sensible de la demande de monnaie et des effets négatifs qu'elle pourrait avoir sur notre bilan. Ces mêmes inquiétudes ont été ressenties lors de l'arrivée sur le marché des cartes de crédit, puis des cartes de débit. On pouvait se demander à l'époque si la demande de monnaie ne

for cash collapse? It never did. Banknotes outstanding goes up 5 per cent per year and does so every year, in line with nominal GDP growth. It has for the past three decades.

We pay a lot of attention to this; we have paid close attention to every advancement in the payment system — credit cards, debit cards and automatic cheque clearing — and we will continue to do so with this.

Mr. Pomorski: I would add that I wouldn't necessarily trivialize bitcoin or other similar currencies. It's easy to do so —

Senator Campbell: All of a sudden, it went from being off the radar to reading about it every day.

Mr. Pomorski: I do take your point. Unfortunately, perhaps a lot of attention is driven by things like Silk Road or colourful names. But at the same time, I would bring this back to a question. You mentioned regulation and should we be regulating that innovation. It's always a question of a trade-off. What is it about bitcoin that we want to regulate? Is there a systemic issue? We don't see any. So at present, the only dimension is consumer protection. There is also the other side of the trade-off, which is the gain to our economy and our consumers who may be using these tools for particular needs and goals.

Let me offer one example on this point. One of the features of crypto-currencies that are often considered nefarious is anonymity. They are nefarious for very good reasons. But at the same time, suppose you want to transact with a merchant based in Poland. I will use this example because I am of Polish origin. How comfortable would you be to send your credit number and address to a merchant based in that country? You might not be very comfortable. It doesn't have to be bitcoin; it could be whatever else. But these developments have a role in providing a way to transact with a merchant in Poland, say, without revealing who you are, where you live and what your credit card number is. Even things like anonymity have a role. Some consumers are looking for that.

Senator Campbell: My second question relates to Octopus. I had an opportunity to meet with the board of Hong Kong Transit. In Vancouver, we were looking at this type of card. I brought this up with them about the transit card. The reason it branched from transit into other areas for them is because such a high level of the population uses public transit that it is natural to have this card, whereas in Canada it's not that large.

So transit actually looked forward on this and started with this, but realized they captured this huge part of the population. Octopus would like to come to Canada. When we looked at it, we

s'effondrerait pas au cas où chacun aurait sa propre carte de crédit et de débit. Cela ne s'est jamais produit. Le volume des billets de banque en circulation augmente régulièrement de 5 p. 100 par an, parallèlement à la croissance nominale du PIB. Il en est ainsi depuis 30 ans.

Nous suivons cela de très près. Nous surveillons étroitement tous les progrès réalisés dans le domaine du système de paiement — carte de crédit, cartes de débit, compensation automatique des chèques — et nous continuerons à le faire.

M. Pomorski : J'ajouterai qu'il ne faut pas nécessairement considérer que le bitcoin et d'autres monnaies semblables sont insignifiants. Il est facile de le faire...

Le sénateur Campbell : Le bitcoin était inconnu puis, du jour au lendemain, les médias en parlent constamment.

M. Pomorski : Vous avez parfaitement raison. Malheureusement, l'intérêt du public est dû pour une grande part à des choses telles que Silk Road et autres noms pittoresques. En même temps, je ramènerais tout cela à une question. Vous avez parlé de réglementation. Vous vous êtes demandé s'il fallait réglementer cette innovation. Il y a toujours un compromis à faire. Quel aspect du bitcoin voudrions-nous réglementer? L'aspect systémique? Nous n'en voyons aucun. Bref, pour le moment, le seul aspect pertinent est celui de la protection des consommateurs. Il y a aussi l'autre terme du compromis, c'est-à-dire l'avantage qu'il y a, pour notre économie et nos consommateurs, à utiliser ces moyens pour répondre à des besoins et des objectifs particuliers.

Permettez-moi de vous donner un exemple. L'anonymat est une des caractéristiques des cryptomonnaies qu'on juge souvent nuisible pour de très bonnes raisons. Supposons cependant que vous voulez acheter quelque chose à un marchand établi en Pologne. J'ai choisi ce pays parce que je suis d'origine polonaise. Dans quelle mesure voudriez-vous donner votre adresse et votre numéro de carte de crédit à un vendeur de ce pays? Je suppose que vous hésiteriez. Vous pourriez cependant régler la transaction en bitcoins ou dans toute autre monnaie. Ces moyens de paiement ont donc un rôle à jouer s'ils vous permettent de traiter avec un marchand établi en Pologne sans avoir à dévoiler votre identité, votre adresse et votre numéro de carte de crédit. Par conséquent, même l'anonymat a un rôle à jouer. Certains consommateurs le croient en tout cas.

Le sénateur Campbell : Ma seconde question porte sur la carte Octopus. J'ai eu l'occasion d'avoir un entretien avec le conseil d'administration des transports en commun de Hong Kong. Nous pensions à une carte de ce genre à Vancouver. J'avais donc évoqué la possibilité de créer une carte de transport. La raison pour laquelle l'utilisation de la carte Octopus s'est étendue à des domaines autres que le transport, c'est qu'un pourcentage élevé de la population a recours aux transports en commun et qu'il était naturel d'avoir cette carte. Ce n'est pas le cas au Canada.

Par conséquent, les responsables des transports en commun de Hong Kong, ayant lancé cette carte, se sont aperçus qu'elle avait été adoptée par une énorme proportion de la population. Octopus

thought it wasn't going to get the lift. They were clear on that; they had a captive audience, and they were going to push this card. And it's hugely successful.

The Chair: We will conclude with a very brief question from Senator Bellemare.

[*Translation*]

Senator Bellemare: I wanted to know, in terms of figures, what the Canadian money supply is, in billions, as compared to the bitcoin supply.

Senator Hervieux-Payette: Sixty-three, they said that at the beginning.

[*English*]

Mr. Johnson: I'm not an expert in money supply, and there are a lot of definitions of it. I would have to come back to you.

In terms of currency outstanding, it's 63 or 64 billion right now in terms of banknotes outstanding. In terms of M1 —

Mr. Pomorski: I wouldn't go to M1. I would try to compare apples to apples if you talk about a specific currency.

Talking about the money supply of bitcoin in terms of U.S. or Canadian dollars is tricky because those numbers are changing rapidly. As of today, the money supply of bitcoin is of the order of $7 billion globally, which is 100 times smaller, roughly, than the money supply of cash. So not money supply, but supply of banknotes in Canada, Canada alone. You may want to add to this the supply of — if I am correct — $1.2 trillion worth of banknotes that the U.S. emits.

In terms of the importance of bitcoins at the moment in the global system, it's relatively unimportant, which perhaps explains why we haven't seen, in terms of a systemic impact, any evidence that it might have an impact at the moment. It does have an impact for consumers, for individuals who transacted, often with high risk to their wealth, but not systemically. Not in Canada, and certainly not worldwide.

Senator Massicotte: Having said that, right now there is a delay of around 10 minutes for every transaction. It's growing a little bit. Is the technology even available to do international currency?

Mr. Johnson: There is a delay. Bitcoin is not instantaneous, obviously. The miners have to verify it, and the ledger has to be updated, and it can take an hour to do a full chain.

aimerait bien s'établir au Canada. Lorsque nous avons examiné la chose, nous avons pensé que la carte n'aurait pas le succès escompté. Les responsables de Hong Kong ont été très clairs là-dessus : ils avaient une clientèle captive, ce qui leur permettait d'aller plus loin. Cela explique l'énorme succès de cette carte.

Le président : Nous allons terminer avec une très brève intervention de la sénatrice Bellemare.

[français]

La sénatrice Bellemare : Je voudrais savoir, en termes de chiffres, à combien se monte l'offre de monnaie, au Canada, en termes de milliards, comparativement à l'offre de bitcoins.

La sénatrice Hervieux-Payette : Soixante-trois, ils l'ont dit au début.

[*Traduction*]

M. Johnson : Je ne suis pas expert en matière de masse monétaire, qui a de nombreuses définitions. Je vais devoir me renseigner et vous répondre plus tard.

Pour ce qui est des billets de banque en circulation, leur valeur s'élève actuellement à 63 ou 64 milliards de dollars. Pour ce qui est du M1...

M. Pomorski : Je n'aborderais pas la question du M1. Je préférerais limiter les comparaisons aux choses comparables dans le cas d'une devise particulière.

Essayer d'attribuer une valeur en dollars américains ou canadiens à l'agrégat monétaire de bitcoins est assez difficile parce que les nombres fluctuent très rapidement. Sur la base du cours d'aujourd'hui, cet agrégat monétaire est de l'ordre de 7 milliards de dollars à l'échelle mondiale, ce qui représente en gros un centième de la circulation fiduciaire. Je parle non de la masse monétaire, mais des billets de banque en circulation uniquement au Canada. Vous voudrez peut-être ajouter à cela — si ma mémoire est bonne — les 1 200 milliards de dollars en billets de banque que les États-Unis émettent.

Pour ce qui est de l'importance actuelle du bitcoin dans le système mondial, elle est relativement insignifiante. Cela explique peut-être que nous n'ayons constaté jusqu'ici aucun indice d'effets systémiques. Le bitcoin a sans doute des effets sur les consommateurs ou plutôt sur les particuliers qui l'utilisent dans leurs transactions, en prenant souvent le risque de perdre tout ce qu'ils possèdent, mais il n'a pas d'effets systémiques. Pas au Canada, et certainement pas à l'échelle mondiale.

Le sénateur Massicotte : Cela dit, il y a actuellement, pour chaque transaction, un retard d'environ 10 minutes, qui semble augmenter quelque peu. La technologie est-elle en fait suffisante pour traiter des devises internationales?

M. Johnson : Il y a un délai. De toute évidence, le réseau Bitcoin n'est pas instantané. Les « mineurs », ou nœuds du réseau, doivent vérifier chaque transaction et mettre à jour le registre. Dans l'ensemble, il faut peut-être une heure pour couvrir toute la chaîne.

Senator Massicotte: Because you've got to do it all again —

Mr. Johnson: The other thing that advances as quickly is the amount of computing power devoted to this. I don't think we have it with us, but you can see graphs that show essentially the hash rate or what is referred to essentially as the network computing power. This is a peer-to-peer network. Gone are the days when you could hook your laptop up and mine bitcoins. These are now special-purpose, dedicated machines that are extremely powerful. More and more get on the network every day. The amount of computing power devoted to this has gone asymptotic as well.

I think it has been a bit of a draw so far.

Mr. Pomorski: I would finish off by offering one statistic. At present, there are about 40 transactions in bitcoin per minute as compared to maybe 200,000 transactions on Visa alone. I'm not an expert to answer the question as to whether bitcoin could be, in principle, able to handle that volume of transactions.

One thing that I would be very careful about is that bitcoin is not the only innovation. In fact, at least one of the examples that I gave you — I think it was the litecoin — actually is designed in a way to cut the settlement time to a quarter.

The Chair: Most interesting, but our time is coming to an end. On behalf of all of the members of our committee, I would like to express great appreciation for your presentations today.

You have talked about the work-in-progress for the Bank of Canada. You can see it's also very much a work-in-progress for the committee, and I suspect we will look forward to having you back.

Members of the committee, if I could have you stay for five minutes for an in camera meeting.

(The committee continued in camera.)

OTTAWA, Thursday, April 3, 2014

The Standing Senate Committee on Banking, Trade and Commerce met this day, at 10:31 a.m., to study the use of digital currency.

Senator Céline Hervieux-Payette (*Deputy Chair*) in the chair.

[*Translation*]

The Deputy Chair: Good morning; I call this meeting of the Standing Senate Committee on Banking, Trade and Commerce to order.

Le sénateur Massicotte : Parce qu'on doit tout refaire...

M. Johnson : Il y a un autre aspect qui évolue aussi rapidement : c'est la puissance de calcul consacrée au réseau. Je ne crois pas que nous les ayons sous la main, mais vous pouvez voir des graphiques montrant le « hashrate », ou puissance de calcul du réseau. Il s'agit ici d'un réseau de pairs. Il n'est plus question aujourd'hui de brancher votre ordinateur portable pour essayer de faire du « minage » de bitcoins. Cette opération se fait maintenant avec des ordinateurs spécialisés extrêmement puissants. Le nombre de ces ordinateurs branchés sur le réseau augmente tous les jours, et la puissance de calcul qui y est consacrée grimpe à une allure vertigineuse.

Jusqu'ici, cela semble avoir attiré les amateurs.

M. Pomorski : Je terminerai par une statistique intéressante. À l'heure actuelle, il y a une quarantaine de transactions en bitcoins par minute, par rapport à quelque 200 000 transactions sur la carte Visa seulement. Je ne m'y connais pas suffisamment pour dire si, en principe, le réseau Bitcoin est en mesure de traiter un tel volume de transactions.

J'ajouterai qu'il est très important de se rendre compte que le bitcoin n'est pas la seule innovation. En fait, un autre des exemples que je vous ai donnés — il s'agissait du litecoin, je crois — est conçu pour réduire des trois quarts le délai de compensation.

Le président : C'est extrêmement intéressant, mais le temps prévu est écoulé. Au nom de tous les membres du comité, je voudrais vous exprimer notre reconnaissance pour l'information que vous nous avez présentée aujourd'hui.

Vous avez parlé d'un travail en cours dans le cas de la Banque du Canada. Vous pouvez constater que c'est particulièrement vrai pour le comité. Il est donc très possible que nous vous demandions plus tard de revenir nous voir.

Membres du comité, je vous saurais gré de rester cinq minutes de plus pour une petite réunion à huis clos.

(La séance se poursuit à huis clos.)

OTTAWA, le jeudi 3 avril 2014

Le Comité sénatorial permanent des banques et du commerce se réunit aujourd'hui, à 10 h 31, pour pour étudier l'utilisation de la monnaie numérique.

La sénatrice Céline Hervieux-Payette (*vice-présidente*) occupe le fauteuil.

[*Français*]

La vice-présidente : Bonjour, je déclare la séance du Comité sénatorial permanent des banques et du commerce ouverte.

Today, the committee is holding its fourth meeting as part of its study on the use of digital currency. The committee has heard so far from the Department of Finance Canada, an economic historian, a professor at the Rotman School of Management at the University of Toronto, and the Bank of Canada.

During the first hour of this meeting, we will receive a presentation from Mr. Jeremy Clark, assistant professor at the Institute for Information Systems Engineering at Concordia University. Mr. Clark's research interests include applied cryptography, Bitcoin, and security in network communications. He has contributed to many projects and publications in these fields.

Mr. Clark, on behalf of the committee, welcome. My particular thanks for accepting this invitation to appear before us. I am sure that you have all the skills you need to help us better understand the subject we are studying.

[*English*]

Jeremy Clark, Assistant Professor, Concordia Institute for Information Systems Engineering, Concordia University, as an individual: Thank you. I have some prepared remarks to make, and then I will move to questions and answers.

Honourable senators, it's my pleasure to present to you today on the subject of virtual currencies. My background was mentioned, but I will just remind you that I am an assistant professor in Information Systems Engineering at Concordia University. I received my PhD in 2011 from the University of Waterloo. My research is in the areas of cryptography and cybersecurity.

Given my expertise, I feel I can best assist you by providing the technical details of how bitcoin and other virtual currencies work, with a particular emphasis on the math-based currencies like bitcoin. Bitcoin has been a research area of mine for several years. I am not an economist, nor do I have extensive public policy experience; however, it is my belief that successful regulation in these other areas requires an accurate understanding of the technology.

If we broadly define digital currencies, we may include things like online credit card transactions, Interac by email, online bill payments, cashing cheques with a camera phone, et cetera. It is important to note that each of these consists actually of two transactions. There is the digital transaction that we see as users, and this merely authorizes the payment. Then, behind the scenes, a second transaction occurs that actually moves the money around. It actually settles the account. This second transaction is not necessarily a digital transaction. Therefore, I would consider these digital authorizations, not necessarily digital currencies.

Aujourd'hui, le comité tient sa quatrième réunion dans le cadre de son étude sur l'utilisation de la monnaie numérique. Le comité a entendu jusqu'à présent des représentants du ministère des Finances, un économiste spécialisé en histoire de la monnaie, un professeur de la Rothman School of Management de l'Université de Toronto et des représentants de la Banque du Canada.

Lors de la première heure de cette réunion, nous recevrons M. Jeremy Clark, professeur adjoint à l'Institut d'ingénierie des systèmes d'information de l'Université Concordia. M. Clark s'intéresse à la cryptographie appliquée, à la monnaie numérique — plus précisément à Bitcoin — et à la sécurité dans les télécommunications en réseau. Il a participé à de nombreux projets et publications dans ces domaines.

Monsieur Clark, au nom du comité, je vous souhaite la bienvenue, mais je vous remercie surtout d'avoir accepté de comparaître devant nous. Je pense que vous avez toutes les compétences nécessaires pour nous aider à mieux comprendre le sujet que nous étudions.

[*Traduction*]

Jeremy Clark, professeur adjoint, Institut d'ingénierie des systèmes d'information de Concordia, Université Concordia, à titre personnel : Merci. J'ai préparé un exposé, puis nous pourrons passer aux questions.

Honorables sénateurs, je suis ravi de venir discuter avec vous aujourd'hui des monnaies numériques. La vice-présidente vient de me présenter, mais j'aimerais vous rappeler que je suis professeur adjoint en ingénierie des systèmes d'information à l'Université Concordia. J'ai obtenu mon doctorat en 2011 de l'Université de Waterloo. Mes recherches portent sur la cryptographie et la cybersécurité.

Compte tenu de mon expertise, je crois être en mesure de vous aider dans votre étude en vous expliquant en détail le fonctionnement de Bitcoin et d'autres monnaies numériques, en particulier les cryptomonnaies comme Bitcoin. J'étudie le système de paiement Bitcoin depuis quelques années. Je ne suis pas économiste, et je n'ai pas une grande expérience en matière de politiques publiques; par contre, je suis d'avis qu'une réglementation efficace dans ces domaines exige une compréhension exhaustive de la technologie.

Une définition élargie des monnaies numériques pourrait notamment inclure les transactions par carte de crédit en ligne, les virements Interac par courriel, les paiements de factures en ligne et le dépôt de chèques au moyen de l'appareil-photo d'un téléphone intelligent. Il importe de souligner que ces méthodes de paiements comprennent deux transactions. Il y a la transaction numérique que voient les utilisateurs et qui sert seulement à autoriser le paiement. Ensuite, en coulisse, il faut une deuxième transaction pour que l'argent soit en fait transféré d'un compte à l'autre. Cela sert tout simplement à régler le paiement. La deuxième transaction n'est pas nécessairement une transaction

In contrast with the class of what I will call math-based currencies, in a digital transaction the user initiates, authorizes, clears and settles the transaction. The currency actually moves from the sender's account to the receiver's account.

The pre-eminent math-based currency is bitcoin. However, it's a large umbrella that covers other established currencies like ripple, litecoin and peercoin, as well as new experimental currencies like mastercoin and ethereum.

I will go through a couple of the major properties that bitcoin has. Many of these are shared with other math-based currencies. In certain cases, you will need more context to judge whether these are good or bad properties. I will neutrally say what the properties are and you can interpret them however you like.

The primary property that bitcoin has is a decentralized ledger. To understand this property, it's important to understand that bitcoins aren't bearer instruments in the sense that you cannot possess a bitcoin, digitally or otherwise. What you possess is a cryptographic key that gives you signing authority over an account. You can think of accounts as having a unique number. I'll refer to them as bitcoin addresses. Technically, they correspond to a public key in a digital signature scheme. The ledger keeps track of every inflow and outflow associated with every bitcoin address, and every outflow has to be signed for by the person who has signing authority over that account. The ledger is updated and maintained by a decentralized network of computers, and there is no entity in charge of this process. That's why I called it a decentralized ledger.

The second property is that bitcoin uses secure cryptography. From my work in cryptography and reading the literature, what I have seen is that cryptographic algorithms, when they break, tend to do so slowly over many years, with theoretic attacks eventually leading to practical attacks. In terms of the specific cryptographic primitives that bitcoin uses, we haven't seen any indication even of theoretic attacks against those primitives. That said, it is unlikely to remain secure forever, so if we think long term, maybe five decades or something like that, it may be time to transition the encryption algorithms that underlie the currency, but that is completely possible with the way the currency is set up.

The third property is short transaction delays. Transactions first require an Internet connection. As an aside, this is the reason why I don't think bitcoin will ever replace standard currency or ever become the national currency of any country. Given that you have an Internet connection, you send your transaction to the network of computers that are maintaining this decentralized ledger. Just like email, you can do a bitcoin transaction any time of day or any day of the year. After you hit send, the network learns of the transaction nearly instantly. The transaction will be grouped together with other active transactions, and the

numérique. Par conséquent, je ne les considérerais pas nécessairement comme des monnaies numériques, mais plutôt comme des autorisations numériques.

À l'opposé, dans le cas des cryptomonnaies, l'utilisateur fait une transaction numérique qui enclenche, qui autorise, qui efface et qui règle le paiement. Les fonds sont en fait transférés du compte de l'expéditeur au compte du bénéficiaire.

La principale cryptomonnaie est Bitcoin. Toutefois, cela comprend diverses autres monnaies bien établies, comme ripple, litecoin et peercoin, ainsi que de nouvelles monnaies au stade expérimental, comme Mastercoin et Ethereum.

Je passerai en revue les principales propriétés de Bitcoin. La plupart des propriétés sont communes aux autres cryptomonnaies. Dans certains cas, vous aurez besoin de plus de contexte pour être à même de juger s'il s'agit de propriétés positives ou négatives. Je m'abstiendrai de commenter les propriétés pour vous laisser le soin de les interpréter à votre guise.

La principale propriété de Bitcoin est la présence d'un registre décentralisé. Pour bien saisir ce concept, il faut comprendre qu'il ne s'agit pas d'effets payables au porteur et qu'on ne peut pas posséder un bitcoin, au sens numérique ou autre. On possède plutôt une clé cryptographique qui vous autorise à utiliser un compte. Les comptes ont des numéros uniques que j'appelle des adresses Bitcoin. Techniquement, ces adresses correspondent à une clé publique dans un mécanisme à signature numérique. Le registre recense toutes les entrées et les sorties de fonds associées à chaque adresse Bitcoin, et chaque sortie de fonds doit être autorisée par la personne qui a la clé pour le compte. Le registre est mis à jour et est maintenu par un réseau d'ordinateurs décentralisé, et aucune entité n'en est responsable. Voilà pourquoi j'appelle cela un registre décentralisé.

Ensuite, Bitcoin utilise une cryptographie sécuritaire. Selon mes travaux et la littérature dans le domaine, j'ai constaté que les algorithmes cryptographiques ont tendance, le cas échéant, à prendre plus de temps à être décryptés; cela prend la forme d'attaques théoriques qui mènent un jour à des attaques réelles. En ce qui a trait aux primitives cryptographiques qu'utilise Bitcoin, nous n'avons même pas encore vu d'indications d'attaques théoriques contre ces primitives. Cela étant dit, il est peu probable que cela demeure sécuritaire indéfiniment. Donc, à long terme, dans une cinquantaine d'années peut-être, nous devrons modifier les algorithmes de chiffrement de la devise, mais la manière dont Bitcoin est fait rend cela tout à fait possible.

La troisième propriété est la rapidité des transactions. Premièrement, il faut une connexion Internet. Soit dit en passant, voilà pourquoi je ne pense pas que les bitcoins remplaceront un jour les devises traditionnelles ou qu'un État adoptera le bitcoin comme devise nationale. Étant donné que vous avez une connexion Internet, votre transaction est envoyée au réseau d'ordinateurs qui maintient le registre décentralisé. À l'instar d'un courriel, vous pouvez échanger des bitcoins en tout temps. Lorsque vous envoyez votre transaction, le réseau en est informé quasi instantanément. La transaction est regroupée avec

transactions set, which is referred to technically as a block, will be added to the ledger of all transactions, which technically is called a block chain. This process typically takes 10 minutes. It takes about 10 minutes to bundle together all the transactions and add them to the ledger. Within an hour after sending the transaction and having it added to the ledger, the transaction will be deep enough in the ledger that it is highly unlikely that it will be subject to a reorganization of transactions. Reorganizations do tend to happen, but they happen right at the tail-end of the ledger.

The bottom line is that transactions can be recognized instantly and finalized with high certainty within an hour. As a party to a transaction, you can choose to wait only for the transaction to reach the network, or, if you want, you can wait the full hour for full confirmation, or you can wait any time in between. The decision basically comes down to how much trust you have in your counter-party. As I mentioned, the transaction actually moves the money. Even at an hour at the longest, that's a very short transaction for something that actually moves and settles accounts.

The next property is low transaction fees. Fees for bitcoin are technically voluntary; however, popular bitcoin software, by default, will include fees. The way that you calculate fees is a very nuanced calculation, but you can think of something like five cents for a standard transaction. The fees do not depend on how much bitcoin is being sent. They only depend on how big the digital representation of the transaction is — how much work the computers have to do to process and verify the transaction.

Low transaction fees enable everything from remittance and overseas workers sending money home to things like micro-transactions. You can imagine paying 10 cents to read a newspaper article online.

The next property is that transactions are irreversible. Once the transaction is in the ledger, it can't be reversed even if it's widely known to be, for example, stolen money. However, because there is a ledger-based system, transactions are traceable. There are cases, for example, where money traced to a theft was deposited with a web service and the web service promptly returned it to the original owner.

The next property has to do with anonymity, and this is one of the most misunderstood parts of bitcoin. The term we use is "pseunonymous." We say that transactions are pseunonymous or pseudononymous. As we've established, transactions are associated with an account number or a bitcoin address. The link between the address and the account holder is not known by default, however it can be established. Many users or companies will say what their bitcoin address is so they can receive payments. Other people might purchase things with bitcoin and have them shipped to a physical address. Now you know the link between the physical address and the bitcoin address. There are also more indirect methods of linking addresses to identities. As mentioned,

d'autres transactions actives, et ce groupe de transactions, qu'on appelle techniquement un bloc, sera ajouté au registre de toutes les transactions, qui lui s'appelle techniquement la chaîne de blocs. Cela prend normalement 10 minutes. Il faut une dizaine de minutes pour regrouper toutes les transactions et les ajouter au registre. Moins d'une heure après l'envoi de la transaction et son ajout au registre, la transaction aura suffisamment été traitée par le réseau que le risque qu'elle fasse l'objet d'une réorganisation sera presque inexistant. Les réorganisations sont une réalité, mais elles surviennent à la toute fin.

Bref, les transactions peuvent être reconnues instantanément et confirmées avec un degré de certitude élevé en moins d'une heure. En tant que participant à la transaction, vous pouvez attendre l'accusé de réception de la transaction par le réseau ou attendre une heure pour recevoir la confirmation officielle ou vous pouvez attendre le temps qui vous plaît entre les deux options. La décision dépend en gros de la confiance que vous avez à l'égard de l'autre partie. Comme je l'ai mentionné, la transaction transfère réellement des fonds. Si l'on considère que cela prend au pire une heure, c'est très rapide pour une transaction qui transfère des fonds et qui règle les paiements.

La prochaine propriété vise les frais de transaction modiques. Les frais pour le système de paiement Bitcoin sont en fait des contributions volontaires; par contre, les logiciels populaires pour le système de paiement exigeront, par défaut, des frais. Le calcul des frais est très variable, mais c'est d'environ 5 cents pour une transaction normale. Les frais ne varient pas en fonction de la quantité de bitcoins échangés. Ils dépendent seulement du poids numérique de la transaction, soit l'ampleur de la tâche pour les ordinateurs en vue de traiter et de vérifier la transaction.

Les frais de transaction modiques permettent une vaste gamme de possibilités, dont des remises, l'envoi par des travailleurs à l'étranger de fonds à leur famille et des microtransactions. Nous n'avons qu'à penser aux gens qui paient 10 cents pour lire un article de journal en ligne.

Les transactions sont également irréversibles. Lorsque la transaction se trouve dans le registre, elle ne peut être annulée, même dans le cas de fonds volés, par exemple. Cependant, étant donné que le système est fondé sur un registre, on peut retrouver toutes les transactions. On a des cas où des fonds volés ont été déposés au moyen d'un service Web, et le service Web a rapidement retourné le tout au propriétaire.

La prochaine propriété du système de paiement Bitcoin est l'anonymat, et c'est l'un des aspects les moins bien compris du système. Nous parlons de « pseudoanonymat ». Nous disons que les transactions sont pseudoanonymes. Comme je l'ai déjà expliqué, les transactions sont liées à un numéro de compte ou à une adresse Bitcoin. L'utilisateur de l'adresse n'est pas connu par défaut, mais on peut le dévoiler. Bon nombre de particuliers ou d'entreprises divulgueront leur adresse Bitcoin pour recevoir des paiements. Certains peuvent acheter des biens avec des bitcoins et faire livrer leurs achats à une adresse physique, ce qui permet de faire le lien entre une adresse physique et une adresse Bitcoin. Il y a aussi des méthodes plus indirectes pour mettre un

bitcoin transactions are sent from a computer and computers, when online, have a pseudonym, which is an IP address. Internet service providers maintain a link between which customers have IP addresses and at what time.

There is interest in both strengthening and weakening bitcoin's anonymity, depending on your perspective. Arguments in favour of strengthening it would be to provide better consumer privacy and protect businesses from corporate espionage or the fact they are basically opening up their books to all their competitors to look at their inflows and outflows. The arguments in favour of weakening it basically come down to allowing law enforcement to do their job more effectively. The way I think of it is this: Bitcoin is more anonymous than the banking system but less anonymous than cash.

The next property has to do with mining. "Mining" technically has different definitions, but I mean "the minting of new currency." This is also a misunderstood property of bitcoin, I think. Mining is not at all a central component to bitcoin. In fact, bitcoin is designed to work without mining at all. Mining simply solves the problem of whom you give the initial set of bitcoins to in a fair and equitable manner. The decision of the designer was that they would give it to the computers that were doing the work and maintaining the ledger. However, when you look at how this is actually used, these miners tend to subsidize the transaction fees that they're charging; so really it's the end users who are sending transactions that benefit the most from mining.

The inflation rate is programmed into the currency, so bitcoin mining is capped. This is a design decision of bitcoin specifically and is not inherent to math-based currency. If you didn't want a cap on the amount of currency and wanted it to inflate forever, that's something you could totally do. With bitcoin, the cap is 21 million bitcoins. This is sometimes misinterpreted as 21 million units of currency. You should remember that bitcoins are divisible to eight decimal points, so what you really have is 2.1 quadrillion units of the smallest transactional amount.

The final property is one we are still coming to grips with as researchers: The fact that bitcoin gives us what we call "programmable money." A cheque has a "To" line. You have two choices for it: You can leave it blank, which says that anyone can cash it; or you can specify a single person and that single entity can cash it. With bitcoin, in the "To" line you can write a little computer program that describes sets of or the properties of the entities that could redeem the transaction or the exact set of conditions under which this redemption would be possible. This

nom sur une adresse Bitcoin. Comme je l'ai déjà mentionné, les transactions au moyen du système de paiement Bitcoin sont faites à partir d'un ordinateur, et les ordinateurs, lorsqu'ils sont en ligne, ont un pseudonyme, soit leur adresse IP. Les fournisseurs de services Internet peuvent déterminer le client qui utilisait une certaine adresse IP à un moment précis.

Il y a des raisons de vouloir tant renforcer que réduire l'anonymat des utilisateurs du système de paiement Bitcoin, selon votre perspective. Ceux qui militent pour le renforcement de l'anonymat avancent que cela protégerait davantage les renseignements personnels des consommateurs et protégerait les entreprises qui pourraient être victimes d'espionnage, d'autant plus que les entreprises concurrentes peuvent consulter à leur guise le compte des entreprises et voir les entrées et les sorties de fonds. D'autres prônent la réduction de l'anonymat, en gros, en vue de permettre aux forces de l'ordre d'accomplir plus efficacement leur travail. Voici comment je vois le tout : Bitcoin est plus anonyme que le système bancaire, mais moins anonyme que les paiements en espèces.

La propriété suivante de Bitcoin est le minage. Le « minage » a différentes définitions, mais je le vois comme « la création de pièces ». D'après moi, c'est aussi une propriété mal comprise de Bitcoin. Le minage n'en est aucunement une composante centrale. En fait, le système de paiement Bitcoin est conçu pour fonctionnement sans cet aspect. Le minage résout tout simplement le problème de déterminer de manière juste et équitable les personnes auxquelles on remet les bitcoins initiaux. Le concepteur a décidé de les donner aux propriétaires d'ordinateurs qui faisaient le travail et qui maintenaient le registre. Cependant, lorsqu'on s'attarde à la manière dont le tout se déroule en réalité, les mineurs ont tendance à éliminer les frais de transaction qu'ils imposent; bref, ce sont vraiment les utilisateurs finaux qui font des transactions qui profitent le plus du minage.

Le taux d'inflation est programmé dans la monnaie. Le minage de bitcoins a donc un plafond. Cette décision a été prise à la conception de Bitcoin, mais ce n'est pas propre aux cryptomonnaies. Si vous ne voulez pas plafonner le nombre de pièces en circulation et que vous voulez laisser la monnaie croître à l'infini, c'est possible de le faire. Dans le cas de Bitcoin, le plafond est fixé à 21 millions de bitcoins. On pense souvent à tort qu'il s'agit de 21 millions d'unités. Il ne faut pas oublier que les bitcoins sont divisibles jusqu'à la 8^{e} décimale. Donc, il y a vraiment 2 100 billions d'unités de la plus petite forme de cette cryptomonnaie.

Les chercheurs sont encore en train de se pencher sur la dernière propriété, à savoir que Bitcoin nous donne ce que nous appelons de « l'argent programmable ». Un chèque a une ligne pour inscrire le bénéficiaire. Nous avons le choix de ne rien y écrire, ce qui permet à quiconque de l'encaisser, ou de préciser qui peut le faire. En ce qui concerne la ligne du bénéficiaire pour les transactions de bitcoins, on peut rédiger un petit programme informatique qui décrit les propriétés des entités qui peuvent encaisser la transaction ou l'ensemble exact des conditions

leads to all sorts of novel applications — escrow transactions, two out of three signatures, bonds, payments for computation and other things that sometimes are called "smart contracts."

This is currently a very active area of development with math-based currencies. I don't think we understand the full potential of what this will allow at this time; it really is a new paradigm for currencies.

That concludes the properties I wanted to mention. I know that the interest in this room is mainly on points of regulation, so I will say where I think regulation may be appropriate. This isn't my opinion as I'm not encouraging anything. These are areas that people have identified as potential points of regulation. In terms of consumer protection, the signing keys that give you signing authority are frequently stolen. They are typically on your computer and if you get malware or someone hacks your computer they can be stolen. Consumers will go to the local police in the case of theft but local police probably don't want to deal with these types of things. It may be interesting to think of better options for people who have their keys stolen. There are exchanges with currencies, like fiat currency and Canadian dollars, into bitcoin. They go bankrupt more often than we'd like, so we could think of bankruptcy insurance or some security auditing of these firms.

There are no guarantees that the exchanges are providing the best execution of orders, so we may want to look at establishing market rules for exchanges. Exchanges sometimes operate in a data centre, so that means the exchange is basically a website that is hosted by a third party.

There was a case recently in Ottawa where the data centre gave unauthorized access to the exchange computer resulting in a theft of $100,000. We have to think about what kind of liability we want data centres to have for hosting exchanges as well.

In terms of money laundering, I can use bitcoin to move large amounts of money overseas. There are no limits on the countries as bitcoin doesn't have any concept of countries or borders. In order to get bitcoins out of Canada, typically it would be in cash. I would have to go through an exchange in order to turn them into bitcoins. You can consider exchanges to be money service businesses and then make them subject to the standard laws, like know your customer, and report certain types of transactions, et cetera.

requises pour l'encaisser. Cela engendre diverses applications novatrices : des dépôts fiduciaires, la présentation de deux signatures sur trois, des obligations, des paiements pour les calculs et d'autres éléments que nous appelons parfois des « contrats intelligents ».

C'est actuellement un domaine de recherche en pleine ébullition en ce qui concerne les cryptomonnaies. Je ne crois pas que nous comprenons actuellement tout ce que cela nous permettra un jour de faire. C'est vraiment un nouveau paradigme dans le domaine des monnaies.

Voilà pour ce qui est des propriétés que je tenais à mentionner. Je sais que vous vous intéressez principalement à la réglementation. Je vous mentionnerai donc des aspects qui pourraient mériter d'être réglementés. Je n'exprimerai pas mon opinion; je ne vous encourage à rien en ce sens. Il s'agit d'aspects que des gens considèrent comme des points à réglementer. En ce qui a trait à la protection des consommateurs, les clés qui donnent accès aux comptes sont souvent volées. Elles sont normalement stockées sur l'ordinateur et elles peuvent être volées, si votre ordinateur est infecté par un logiciel malveillant ou qu'il est piraté. Les consommateurs feront appel aux policiers lorsqu'ils se font voler, mais les services de police locaux ne veulent probablement pas s'occuper de ce genre de vols. Il serait intéressant de trouver des recours plus adéquats pour les gens qui se font voler leur clé. Des devises, comme une monnaie fiduciaire et des dollars canadiens, sont converties en bitcoins, et des consommateurs peuvent se retrouver sans le sou plus souvent qu'on le pense; on pourrait mettre en place une assurance contre la faillite ou vérifier la sécurité des entreprises.

Rien ne garantit que les plates-formes d'échanges fonctionnent de manière optimale. On pourrait envisager l'adoption de règles du marché en la matière. Les plates-formes d'échanges se trouvent parfois dans des centres de données, ce qui signifie que les plates-formes d'échanges sont en gros un site web qu'héberge un tiers.

Il y a récemment eu un cas à Ottawa où le centre de données à accorder un accès non autorisé au système informatique qui gère les transactions, ce qui a permis un vol d'une valeur de 100 000 $. Nous devons examiner les responsabilités que nous aimerions qu'aient les centres de données en ce qui concerne l'hébergement de plates-formes d'échanges.

En ce qui a trait au blanchiment d'argent, je peux me servir des bitcoins pour transférer de grandes sommes d'argent à l'étranger. Il n'y a pas de limite quant au pays, étant donné que Bitcoin ne tient pas compte de la notion des pays ou des frontières. Pour transférer des bitcoins à l'extérieur du Canada, je devrais normalement le faire en espèces. Je devrais ensuite convertir le tout en bitcoins en passant par une plate-forme d'échanges. Vous pourriez considérer les plates-formes d'échange comme des entreprises de transfert de fonds et les assujettir aux lois actuelles, comme celles de connaître leurs clients et de rapporter certains types de transactions.

In terms of illicit transactions, it's important to remember that bitcoin transactions are packets on the Internet. They are no different than other types of illicit packets that law enforcement is interested in tracking. They are already involved in lots of cat and mouse games tracking illicit information on line. The most notable case for illicit transactions is called Silk Road, where you can purchase illegal things like drugs and weapons. It is important to know that in the case of Silk Road, bitcoin was a component of a larger system. If you just had bitcoin, you couldn't do Silk Road because you also need ways of anonymizing users in terms of their Internet traffic.

Basically, you have to put a server up and have it so that no one knows where it is located. Somehow you can visit the server over the Internet and not know where it is located. That uses a highly sophisticated piece of technology called Tor:Hidden Service. If you want illicit things shipped, you probably want them shipped to an anonymous address like a post office box. Silk Road is an example of a combination of technologies that came together in order to make that possible. Of course, law enforcement was able to get to the bottom of it and make arrests in that case.

The final category is taxation, about which I know the least. I guess I see it mainly as a classification issue: What does bitcoin fall under? I'm not sure what the answer is. Economists would probably have a better opinion than I would have on that.

In conclusion, we are in the early adopter phase of math-based currencies. It's hard to assess their true potential at this time; however, a low-fee, international pipeline for financial transactions that is akin to sending an email is an important innovation in and of itself without getting to the more futuristic possibilities of a programmable currency. Small businesses in the sector are growing with significant innovation happening right here in Canada. We have to be careful not to stifle innovation, while addressing the legitimate concerns banks and law enforcement have with math-based currencies.

The Deputy Chair: Thank you. In trying to follow you, I hope my colleagues have picked up all the points that you raised. We may have a few questions to clarify these points.

Senator Tkachuk: That was quite remarkable, actually.

When you talked about the payment and the fact that it takes 10 minutes to finally move the key that I have or a portion of the key that I have or the asset that I have to somebody else, can you make multiple payments? Can I pay three things at one time or do I have to make every transaction separate? How does that operate?

Pour ce qui est des transactions illicites, il ne faut pas perdre de vue que les transactions de bitcoins sont des paquets de données sur Internet. Ces paquets ne sont pas différents des autres paquets illicites que les forces de l'ordre ont à l'oeil. On joue déjà beaucoup au chat et à la souris en vue de suivre à la trace les renseignements illicites en ligne. Le cas le plus médiatisé de transactions illicites concerne le site web Silk Road, où on pouvait acheter des biens illicites, comme des stupéfiants et des armes. Il importe de rappeler que, dans le cas de Silk Road, les bitcoins étaient une composante d'un plus grand système. Si vous aviez seulement des bitcoins, vous ne pouviez pas profiter de ce marché noir, parce que vous aviez aussi besoin de trouver des moyens de garantir l'anonymat des utilisateurs en ce qui a trait à leur trace sur Internet.

En gros, vous devez installer un serveur et faire en sorte que personne ne sache où il se trouve. Les utilisateurs arrivent à visiter le serveur sur Internet sans savoir où il est situé. Cela nécessite une technologie hautement sophistiquée appelée les services cachés de Tor. Si vous voulez vous faire livrer des biens illicites, vous voudrez probablement qu'ils soient livrés à une adresse anonyme comme une case postale. Le site web Silk Road est un exemple de technologies qui sont combinées pour rendre le tout possible. Bien entendu, les forces de l'ordre ont été en mesure d'aller au fond des choses et de réaliser des arrestations à cet égard.

La dernière catégorie concerne l'imposition, soit ce que je connais le moins. Je vois cela principalement comme un problème de classification. Sous quelle catégorie devrions-nous classer les bitcoins? Je ne suis pas certain de la réponse. Des économistes seraient mieux placés que moi pour vous donner une réponse éclairée en la matière.

En conclusion, nous sommes à l'étape des premiers utilisateurs des cryptomonnaies. Il est difficile d'évaluer leur véritable potentiel pour l'instant; par contre, on peut considérer un système de paiement international qui impose des frais modiques pour les transactions financières et qui s'apparente à l'envoi de courriels comme une innovation importante en soi, sans nous lancer dans les possibilités futuristes d'une devise programmable. De petites entreprises du secteur connaissent un essor, et des innovations importantes sont actuellement réalisées au Canada. Il faut faire attention de ne pas gêner l'innovation, lorsque nous aborderons les questions légitimes des banques et des forces de l'ordre quant aux cryptomonnaies.

La vice-présidente : Merci. J'espère qu'en essayant de suivre votre exposé mes collègues ont saisi tout ce que vous avez mentionné. Nous vous poserons probablement des questions en vue de préciser certains aspects.

Le sénateur Tkachuk : C'était en fait remarquable.

Vous avez parlé des paiements et du fait qu'il faut 10 minutes pour que la clé que je détiens, une partie de la clé que je détiens ou le bien que je détiens soit transféré à quelqu'un d'autre. Est-il possible d'effectuer des paiements multiples? Puis-je acheter trois choses en un seul paiement, ou dois-je faire des transactions distinctes? Comment cela fonctionne-t-il?

Mr. Clark: The basic rule is you can do multiple payments and bundle them together. The way it works is with inflows and outflows. In a transaction there will be a bunch of money that comes into the transaction and there will be a bunch of money that comes out, so you can think of it as input addresses and then output addresses. If you're paying five people from five different accounts you can put that together in one transaction. You will probably get lower fees by bundling together so it's an advantage to do that.

The only rule is that if you have an input you can't send it to two places at once. That would be called a double spend, and it's obvious why you shouldn't be able to double spend. When the computers update the ledger they are ensuring that when an input comes into a transaction it hasn't been spent in any other transaction.

Senator Tkachuk: The bitcoin itself has such big valuations and it moves up and down. Why does it do that? It seems to me, if I'm paying for a piece of digital currency, let's say I pay $100 for a bitcoin and so I put in that much cash. I need cash to get a bitcoin, otherwise there is no bitcoin, so I pay $100 for it. My view is that $100 is now stored in that bitcoin so it can be released to someone else who I'm buying something from. Why does it increase or decrease in value?

Mr. Clark: I don't necessarily view it as being stored. That's one way of thinking about it. Let's go back to where the bitcoin that you buy for $100 comes from. In the very beginning it will be mined by a computer, which means it just comes out of thin air, essentially. This bitcoin comes out of thin air and then if there is a demand for bitcoin someone will pay $100 for it and so the miner will sell that for $100. Then you'll spend that bitcoin, someone else will have it and maybe they will sell it later for $150 or the price will change. The price is closer to about $500 for a bitcoin.

It's like a commodity, I suppose, from that standpoint. As to why the exchange rate is so volatile, I'm not sure we know. First off, you have to figure out who is holding bitcoins and why. It doesn't pay any interest, for example, so why would you hold bitcoins instead of holding cash if you're not going to earn interest? Some people might argue it's deflationary, so that you might expect a rate of return. A lot of people are just speculators; they think that the price may increase and so that may be why they hold onto it. We don't know the answers, but the answer to that question may lead us to being able to model the volatility better.

Senator Tkachuk: I find it difficult. Commodities are something. There has to be some input into commodities such as corn and oil, there has to be some cash or something to create something real so people eat or whatever. With this thing there is

M. Clark : La règle de base, c'est que des transactions multiples sont possibles, pourvu qu'elles soient regroupées. Le fonctionnement est fondé sur des entrées et sorties. La transaction comporte deux éléments : l'entrée de fonds et la sortie de fonds. Ces deux éléments peuvent être comparés à des adresses d'entrée et des adresses de sortie. Si vous payez cinq personnes à partir de comptes distincts, vous pouvez regrouper ces paiements en une transaction unique. Le regroupement vous permettra probablement d'avoir des frais moins élevés; il y a donc un avantage à le faire.

La seule règle, c'est que si vous avez une entrée, vous ne pouvez la dépenser à deux endroits en même temps. C'est ce que l'on appellerait une « double dépense », ce qu'il convient de ne pas faire, pour des raisons évidentes. Pendant la mise à jour du registre, les ordinateurs s'assurent qu'une entrée utilisée dans une transaction n'a pas été utilisée dans une autre transaction.

Le sénateur Tkachuk : Le bitcoin lui-même connaît d'importantes fluctuations, à la hausse ou à la baisse. Pourquoi? Il me semble que si j'achète de la monnaie numérique... Disons que je dépense 100 $ pour un bitcoin; je verse ce montant d'argent. Il me faut de l'argent pour acheter un bitcoin, sans quoi le bitcoin n'existe pas. Je paie donc 100 $ pour l'obtenir. D'après ce que je comprends, ce 100 $ est maintenant stocké dans le bitcoin. Il peut donc être transféré à quelqu'un d'autre, soit la personne de laquelle j'achète un bien quelconque. Pourquoi sa valeur fluctue-t-elle, que ce soit à la hausse ou à la baisse?

M. Clark : Je ne considère pas nécessairement qu'il y ait stockage. C'est une façon d'aborder la question. Retraçons l'origine de ce bitcoin que vous vous procurez pour 100 $. Au début, il sera créé par minage à l'aide d'un ordinateur. Essentiellement, il est créé à partir de rien. Le bitcoin est créé et s'il y a une demande, quelqu'un l'achètera au prix de 100 $ et le mineur le vendra donc pour 100 $. Lorsque vous dépenserez ce bitcoin, il appartiendra à quelqu'un d'autre qui, ultérieurement, le vendra peut-être 150 $ ou un autre prix. Le prix d'un bitcoin se rapproche davantage de 500 $.

D'une certaine façon, cela ressemble à une marchandise. Quant à savoir d'où vient cette volatilité du taux de change, je ne suis pas certain qu'on le sait vraiment. Premièrement, il faut savoir qui détient des bitcoins, et pourquoi. Par exemple, aucun intérêt n'est versé. Donc, pourquoi conserver des bitcoins plutôt que de l'argent réel si vous n'obtenez pas d'intérêts? Certains diront que c'est déflationniste, de sorte que l'on pourrait s'attendre à un taux de rendement. Beaucoup de gens ne sont que des spéculateurs qui considèrent que le prix pourrait augmenter, ce qui expliquerait pourquoi ils veulent les conserver. Nous ne connaissons pas les réponses, mais ce sont elles qui pourraient nous permettre d'établir un modèle plus précis pour cette volatilité.

Le sénateur Tkachuk : Je trouve cela difficile. Les marchandises, c'est une chose. Pour des marchandises comme le maïs et le pétrole, il doit y avoir des intrants, il doit y avoir des liquidités ou quelque chose visant la création de quelque chose de

no input except it's produced. As you say, there's nothing there except what I'm willing to pay for it.

Mr. Clark: Right. I think maybe what it derives its value from is scarcity, so you can't just go out and make a string of bits that is equivalent to something that would be a bitcoin. Because it's scarce, that may be where it derives its value from.

Senator Tkachuk: Can you deposit bitcoins anywhere else outside of the ledger? Are there any banks that actually take bitcoins?

Mr. Clark: There are no banks that I'm aware of that take bitcoins. It's possible that they exist in other countries.

There are exchanges online. Bitcoins and fiat currency are deposited with the exchange. They hold it in street name and then the transaction moves the money from within their own company, from one customer's account to the other person's account.

There are other services that will hold your bitcoin. This is more of a convenience for users so you have easy access to your bitcoins if you sit down at a new computer and your bitcoins are on one computer. If the signing authority over the bitcoins are on one computer and you want to use it from a second computer, that's a substantial problem. It's more addressed at solving that problem as opposed to them actually wanting to hold your bitcoins, for example, to loan them back out or whatever a bank might do.

Senator Massicotte: I think I heard you say that there is no question that the small "b" bitcoins could never be our national currency and I think I share your pain. I know it has become very popular, but why is it so popular? For instance, I hear people say that it's very cost efficient and less expensive. I'm not sure that's the case because obviously the retail price has to change immensely. The retailer doesn't deal with bitcoins and he's probably charging 5 per cent or 10 per cent more. Even when you set off the account and you go to an iCloud or you want to fix the currency that's going to cost you something.

Is it a false argument to say it's cost efficient? That first step is very efficient but there are all the other steps you need to cause a transaction. I'm not sure it's cheaper than a debit card.

Mr. Clark: There are companies and their business model is to basically provide a bitcoin pipeline for companies so that users just pay in Canadian dollars, it gets converted to bitcoin on the back end, sent through bitcoin and then the company immediately converts it back to fiat. There are fees associated with moving Canadian dollars into bitcoin and then back the other way.

réel pour que les gens puissent manger, et cetera. Dans ce cas-ci, il n'y a aucun intrant à l'exception du fait qu'il est produit. Comme vous l'indiquez, il n'y a rien de concret, sauf le montant que je suis prêt à payer pour me le procurer.

M. Clark : Exactement. Je pense que sa valeur découle de sa rareté. On ne peut donc pas simplement créer une chaîne de bits qui serait l'équivalent d'un bitcoin. Ce serait sa rareté qui ferait augmenter sa valeur.

Le sénateur Tkachuk : Est-il possible de déposer des bitcoins ailleurs que dans le registre? Existe-t-il des banques qui acceptent les bitcoins?

M. Clark : À ma connaissance, aucune banque n'accepte les bitcoins. Il pourrait y en avoir dans d'autres pays.

Il existe des plates-formes d'échange en ligne, où sont déposés les bitcoins et la monnaie fiduciaire. Les monnaies y sont conservées au nom de la plate-forme d'échange, puis la transaction a lieu; les fonds sont transférés du compte du client au compte de l'autre personne.

D'autres services offrent le stockage des bitcoins. Pour les utilisateurs, c'est plus pratique. Cela leur permet d'avoir accès aux bitcoins à partir d'un ordinateur autre que celui où ils sont stockés. Si la clé d'autorisation se trouve dans un ordinateur et que vous voulez utiliser un autre ordinateur, c'est un problème important. Donc, cela vise davantage à résoudre un problème qu'à stocker les bitcoins aux fins de prêts ou de toute autre activité qu'une banque pourrait mettre en place.

Le sénateur Massicotte : Si je ne me trompe pas, vous avez indiqué que les bitcoins, avec la minuscule, ne deviendraient jamais notre monnaie nationale; je pense la même chose. Je sais qu'ils sont devenus très populaires, mais pourquoi le sont-ils autant? Par exemple, certains disent que le bitcoin est très rentable et moins coûteux. Je ne suis pas certain que ce soit le cas, parce que le prix au détail doit être très différent. Le détaillant n'a pas l'habitude de faire des transactions en bitcoin et il augmente probablement ses prix de 5 p. 100 ou 10 p. 100. Que l'on ouvre un compte, que l'on ait recours au stockage virtuel ou que l'on établisse une monnaie, il y a des coûts associés à cela.

Dire que c'est rentable est-il un faux argument? La première étape est très rentable, mais elle est suivie de toutes sortes d'étapes pour que la transaction ait lieu. Je ne suis pas certain que ce soit moins coûteux qu'une transaction par carte de débit.

M. Clark : Il existe des entreprises dans ce secteur et leur modèle d'affaires consiste essentiellement à offrir aux entreprises une plate-forme d'échange de bitcoins qui permet aux utilisateurs de payer en dollars canadiens. Les fonds sont convertis en bitcoins, en aval, puis sont renvoyés par l'intermédiaire de Bitcoin jusqu'à l'entreprise qui les reconvertit alors en monnaie fiduciaire. Des frais sont exigés pour la conversion des dollars canadiens en bitcoins et pour la transaction inverse.

Those fees tend to range from 0.5 per cent to 1.5 per cent, and so I think it's still lower than credit card payments and maybe debit payments. I'm not an expert. I don't know all the numbers.

Senator Massicotte: Debit cards are very cheap. It's a fixed cost per transaction of 10 cents to 18 cents.

When you go to a convenience store to buy a pack of gum you're not going to wait 10 minutes — so you can't use it there.

On the issue of being anonymous, that's also, as you confess, somewhat false. There is actually a tracker. If it's extremely important they can find out. Maybe the drug dealer or whatever has been using it under a false pretense that he thought was totally anonymous and he's finding out, oh, oh, look at the FBI recently, they shut down.

What is the eventual life of this stuff? I know it's very popular now and I suspect the retailer who is using this, including the car dealer, because it's more marketing oriented. It's not oriented at all to fundamentals. Do you share that opinion?

Mr. Clark: Maybe to a certain extent. If you look at the demographic of people who are willing to use bitcoins that is an interesting demographic, and so it's totally possible that companies are using bitcoins just to appeal to that specific demographic.

In terms of going to a store and waiting 10 minutes to buy a pack of gum, that is a drawback. The 10 minutes is a design decision by bitcoin so that doesn't necessarily apply to other math-based currencies. The reason that you have to wait 10 minutes is — it's a very technical discussion — essentially you're worried that the consumer is going to do this elaborate theft where they try and double spend, so they give you the bitcoins for the pack of gum and then they also send it back to themselves at the same time and you don't know which of those two transactions is going to make it into the ledger. They compete, they contradict each other and they both can't go in.

In the case of things like packs of gum, you probably trust your consumers enough that they're not going to do this elaborate hoax, and they could simply walk out with a pack of gum. There are easier ways of stealing a pack of gum probably than launching this bitcoin-based theft.

Generally there are small businesses that do accept bitcoins for things like cupcakes and that type of thing. They essentially trust the consumer that they're not going to double spend and so they wouldn't wait the full 10 minutes. They will just see that it was broadcast to the network.

Ces frais ont tendance à se situer entre 0,5 p. 100 et 1,5 p. 100. À mon avis, c'est toujours plus faible que les frais pour les transactions par carte de crédit ou de débit. Je ne suis pas un spécialiste; je ne connais pas tous les chiffres.

Le sénateur Massicotte : Les transactions par carte de débit sont peu coûteuses. On parle de frais fixes de 10 à 18 cents par transaction.

Si vous allez au dépanneur pour acheter un paquet de gomme, vous n'attendrez pas 10 minutes. Donc, on ne peut pas l'utiliser là.

Pour ce qui est de l'anonymat, c'est aussi faux, comme vous l'avez indiqué. En fait, il y a un mécanisme de suivi. Donc, si c'est extrêmement important, il y a moyen d'effectuer un suivi de la transaction. Un narcotrafiquant, par exemple, y a peut-être eu recours de façon frauduleuse en pensant que cela se faisait de façon tout à fait anonyme, pour ensuite constater, à son grand désarroi, que le FBI avait fermé le réseau.

Quelle est sa vie utile? Je sais que c'est très populaire actuellement et je suppose que le détaillant qui l'utilise, dont le concessionnaire automobile, le fait parce que c'est davantage axé sur le marketing. Ce n'est aucunement axé sur les notions fondamentales. Êtes-vous de cet avis?

M. Clark : Peut-être, dans une certaine mesure. Si vous regardez le profil démographique des gens qui sont prêts à utiliser les bitcoins, c'est un groupe intéressant. Il est donc tout à fait possible que des sociétés utilisent les bitcoins simplement pour plaire à ce groupe.

Quant au fait d'aller dans un magasin et d'attendre 10 minutes pour acheter un paquet de gomme, c'est un inconvénient. L'attente de 10 minutes relève d'une décision prise par Bitcoin à la conception. Elle ne s'applique pas nécessairement aux autres monnaies fondées sur la cryptographie. La raison pour laquelle il faut attendre 10 minutes — c'est un aspect très technique — est essentiellement liée à une préoccupation selon laquelle le consommateur tentera de mettre sur pied un stratagème dans le but de faire une double dépense en vous donnant des bitcoins pour le paquet de gomme et en se les retournant au même moment, de façon à ce que l'on ne sache pas quelle transaction sera inscrite au registre en premier. Elles sont en concurrence; elles sont contradictoires et ne peuvent pas être inscrites toutes les deux.

Dans le cas de choses comme un paquet de gomme, vous ferez probablement assez confiance à vos clients pour qu'ils ne se lancent pas dans un tel stratagème complexe. Ils pourraient tout aussi bien dérober un paquet de gomme, tout simplement. Il y a d'autres façons de voler un paquet de gomme que de se lancer dans ce genre de vol à l'aide de bitcoins.

Il existe de petites entreprises qui acceptent les bitcoins pour des choses comme les petits gâteaux, et cetera. En général, ils ont confiance que le consommateur ne tentera pas de faire une double dépense et ne demandent pas que le consommateur reste sur place pendant 10 minutes. Ils veulent seulement voir que la transaction a été publiée sur le réseau.

Senator Massicotte: National currency is out of the question, so it's a convenient form of bartering; it's a commodity oriented form of bartering. Maybe there is a cost advantage, which is not clear to me because the variability of price is scary. Those motivated by anonymity maybe should be concerned, as the Senate should be concerned. What's the next step? What's the national interest? Why would we as a body recommend any form of regulations? It's buyer beware.

That guy is buying silver or gold or whatever. The government doesn't guarantee that they won't lose money. You mentioned five or six places where we could legislate, but why get into this? Where's the national interest?

Mr. Clark: I think it does go with the cost advantage, but it's not for the types of transactions that you're thinking of, the mainstream transactions. There are other transactions that are much more difficult to do. For example, if I want to send money overseas, my brother lives in Kiev, Ukraine. If I want to send him some money, that's really hard to do with the banking system. There will be large delays and large fees. I can send him bitcoin. Even if it takes 10 minutes or an hour for it to fully clear, that's still a very fast transaction, and there are low fees. For things like the remittance market, it's interesting in those cases.

Generally, if you think about the Internet, it's purely digital, and it doesn't know international boundaries. This is a currency that I think is perfectly designed for, basically, transacting online.

Senator Massicotte: Especially in countries in which there's a significant inflation in currency, you can't trust the local currency or you think the fees are a disadvantage. As you know, the more you regulate and try to achieve the same form of comfort that you get from national currency, there go your fees again. Even then, if you send it to your brother-in-law in Bulgaria, I'm not sure it will convert the bitcoins into real currency to buy a pack of gum or whatever.

Mr. Clark: That's correct. You do need to find an exchange on the other end to convert it for it to be useful, or you have to transact directly.

Senator Black: Dr. Clark, thanks for being here. That was very helpful. It was helpful in terms of the technical discussion, but I want to take you, if you're comfortable, to a discussion about what the future might look like.

From the very end of your comments, I take that you believe that bitcoin is likely a step on the innovation road for digital currencies. Do you agree with that?

Mr. Clark: Yes, I would agree.

Le sénateur Massicotte : La monnaie fiduciaire est exclue. Il s'agit donc d'une forme pratique de troc, un troc axé sur les marchandises. Il y a peut-être un avantage lié aux coûts. Or, cela ne m'apparaît pas évident, parce que la variation du prix est inquiétante. Les personnes motivées par l'anonymat devraient être préoccupées, et le Sénat devrait être préoccupé aussi. Quelle est la prochaine étape? Qu'est-ce qui est dans l'intérêt du pays? Pourquoi le Sénat devrait-il recommander une réglementation quelconque? Il revient à l'acheteur de prendre ses précautions.

Quelqu'un achète de l'argent, de l'or, peu importe. Le gouvernement garantit qu'il ne perdra pas d'argent. Vous avez mentionné cinq ou six aspects qui pourraient faire l'objet d'une loi, mais pourquoi le ferait-on? En quoi est-ce dans l'intérêt national?

M. Clark : Je pense que c'est lié à l'avantage relatif aux coûts, mais pas pour le genre de transactions courantes auxquelles vous pensez. Il y a d'autres transactions bien plus complexes. Par exemple : je veux envoyer de l'argent à l'étranger, à mon frère qui habite à Kiev, en Ukraine. Il est très difficile de lui envoyer de l'argent par le système bancaire. C'est long et coûteux. Je peux lui envoyer des bitcoins. Même s'il fallait 10 minutes, voire une heure, pour que la transaction soit approuvée, ce serait tout de même une transaction très rapide, et les frais sont bas. Pour des choses comme le marché des envois de fonds, c'est une solution intéressante.

En général, Internet est purement numérique; les frontières internationales n'existent pas. À mon avis, cette monnaie est la monnaie parfaite pour les transactions en ligne, et c'est à cette fin qu'elle a été conçue.

Le sénateur Massicotte : On pense particulièrement aux pays où la devise est soumise à une forte inflation, où elle inspire peu confiance et où l'on estime que les frais sont un désavantage. Comme vous le savez, plus on augmente la réglementation et plus l'on cherche à atteindre une certitude aussi grande que pour la monnaie fiduciaire, plus les frais augmentent. Encore là, si vous envoyez cet argent à votre beau-frère, en Bulgarie, je ne suis pas certain qu'il convertira les bitcoins en devise réelle pour acheter un paquet de gomme, et cetera.

M. Clark : C'est exact. Il faut trouver une plate-forme d'échange à l'autre bout afin de les convertir en devise utilisable; autrement, il faut effectuer la transaction directement.

Le sénateur Black : Merci d'être ici, monsieur Clark. C'était très utile. C'était utile sur le plan technique, mais si cela vous convient, j'aimerais vous amener sur une autre tangente; j'aimerais que vous nous parliez de ce que l'avenir pourrait nous réserver.

D'après vos derniers commentaires, j'en déduis que vous pensez que Bitcoin représente une étape de l'évolution de la monnaie numérique. Êtes-vous d'accord avec cette affirmation?

M. Clark : Oui.

Senator Black: Let's go down that road a little bit. What role do you see digital currencies playing in the Canadian economy three to five years from now?

Mr. Clark: I think they'll have a more prominent role to play, especially for online transactions. We have seen some major retailers start to accept bitcoin. TigerDirect is one that has a Canadian presence. I think you'll be able to go online and buy things with bitcoin on more sites than you can today.

I mentioned the programmability of money. That's maybe more than three to five years out, but I think we'll see other currencies that really enhance that feature of the currency. Whether that's added to bitcoin itself or there's another currency that comes along and replaces it, I think there are exciting opportunities in that space as well.

Senator Black: I take from that that you don't see digital currencies going away?

Mr. Clark: That's correct. I would be very surprised, at this point, if they would go away, unless there were draconian measures taken by governments to shut them down.

Senator Black: Right. In terms of Canada's position, is there an opportunity for Canada to play, globally, some kind of role? Is there a first-mover advantage to Canada, in your view?

Mr. Clark: It's sort of a double-edged sword because, if you regulate and get it wrong and don't have the opportunity to learn from what other countries did in terms of regulation, it's dangerous. On the other hand, once you get regulations in place, I think it gives a lot of confidence to entrepreneurs who want to innovate in the space. Right now, there are a lot of question marks around it. They have trouble dealing with traditional banks just because it's sort of up in the air. So I would say that there is a first-mover advantage in terms of instilling confidence, which will lead to entrepreneurship, which will lead to innovation for the Canadian economy. As I said, there's also a risk to moving first.

Senator Black: Dr. Clark, are you aware of something called the mint chip, a digital currency developed by the Canadian Mint, apparently?

Mr. Clark: Yes.

Senator Black: Can you share what you know about that?

Mr. Clark: I don't know all of the technical details of it. My understanding is that it's still based on Canadian currency. It's not a digital currency; it's just a digital representation. Earlier, I mentioned what I consider digital authorizations. I consider it a

Le sénateur Black : Explorons cette avenue quelque peu. À votre avis, quel rôle les monnaies numériques joueront-elles dans l'économie canadienne dans trois à cinq ans?

M. Clark : Je pense qu'elles joueront un rôle plus important, en particulier dans le cas des transactions en ligne. D'importants détaillants ont commencé à accepter Bitcoin. TigerDirect est un joueur présent sur le marché canadien. Je pense qu'il sera possible d'aller sur Internet et d'acheter des marchandises avec Bitcoin sur plus de sites qu'aujourd'hui.

J'ai parlé de la programmabilité de la monnaie. Il faudra peut-être plus de trois à cinq ans, mais je pense que nous verrons d'autres monnaies pour lesquelles on exploitera pleinement cette caractéristique de la monnaie. Que ce soit ajouté à Bitcoin ou à une autre monnaie qui la remplacera, je pense qu'il y aura là des possibilités intéressantes.

Le sénateur Black : J'en déduis que vous croyez que les monnaies numériques sont là pour rester?

M. Clark : C'est exact. À ce moment-ci, je serais très surpris qu'elles disparaissent, à moins que les gouvernements ne prennent des mesures draconiennes pour les éliminer.

Le sénateur Black : Exactement. Le Canada est-il placé de façon à pouvoir jouer un rôle quelconque sur la scène internationale? À votre avis, le Canada pourrait-il bénéficier de l'avantage du premier venu dans ce marché?

M. Clark : C'est un couteau à double tranchant, si l'on veut, parce que si vous adoptez une réglementation, que vous vous trompez et que vous n'avez pas la possibilité de tirer des leçons de la réglementation adoptée par d'autres pays, c'est dangereux. D'un autre côté, lorsque la réglementation est en place, je pense que cela inspire grandement confiance aux entrepreneurs qui souhaitent innover dans ce domaine. Il y a actuellement beaucoup d'incertitude à cet égard. Ces sociétés ont de la difficulté à faire des affaires avec les banques traditionnelles en raison du flou sur cette question. Je dirais donc qu'il y a un avantage à être le premier venu : cela favorise la confiance et, par conséquent, l'entrepreneuriat, qui mène à son tour à l'innovation, au profit de l'économie canadienne. Comme je l'ai indiqué, être le premier à bouger comporte aussi des risques.

Le sénateur Black : Monsieur Clark, avez-vous entendu parler de ce quelque chose que l'on appelle la cybermonnaie, une monnaie numérique que la Monnaie royale canadienne tenterait actuellement de mettre au point?

M. Clark : Oui.

Le sénateur Black : Pouvez-vous nous dire ce que vous savez à ce sujet?

M. Clark : Je ne connais pas tous les détails techniques qui s'y rapportent. Je crois comprendre qu'elle est fondée sur le dollar canadien. Ce n'est pas une monnaie numérique, mais une représentation numérique. J'ai parlé plus tôt de ce que je

system that's based on authorizing payments digitally and how that money actually moves around. I haven't looked at the details, though.

Senator Black: You understand that it would be a process as opposed to a currency?

Mr. Clark: Yes.

[*Translation*]

Senator Bellemare: I have two questions for you; here is the first. Yesterday, we had people here from the Bank of Canada; they talked to us about bitcoin as a store of value. We all know that bitcoin is highly volatile. They also told us that, in some countries, there are private organizations like BitPay, which are in the business of quickly converting bitcoin to the local currency. Are you at all familiar with organizations of that kind?

The Bank of Canada people told us that bitcoin is used a lot as a payment method and that people who use it internationally convert bitcoin quickly so that it does not lose value.

Are you at all familiar with organizations like BitPay? How do they make their money? Are they taking a risk when they convert the currency into local currency?

[*English*]

Mr. Clark: If I understand your question, you're concerned about what the business model is for exchanges, particularly when bitcoin is extremely volatile.

They provide a matching service between people who have bitcoins and want local currency and people who have local currency and want bitcoins. They do tend, at certain times, to hold a lot of bitcoins, so there is a bit of risk due to the exchange rate fluctuations. But their general business model is that they will take a transaction fee for arranging the swap between the two currencies. It's sort of independent of what the exchange rate does. They can still make money as long as there's demand on both sides.

[*Translation*]

Senator Bellemare: Are there other companies like BitPay in the market, or does that company have a monopoly on this kind of transaction at the moment?

[*English*]

Mr. Clark: There are a lot of exchanges. BitPay is just one of many. Right now, I think we are seeing a consolidation. There are major exchanges at the top. I didn't run the numbers, but my intuition is that it's sort of an 80/20 type of thing, where 80 per cent of the exchange goes through 20 per cent of the exchanges. It's probably more extreme than that. I think the vast majority of exchanges probably go through three exchanges.

considère comme des autorisations numériques. Il s'agit d'un système fondé sur l'autorisation numérique des paiements et sur le déplacement des fonds. Cependant, je n'ai pas examiné cela en détail.

Le sénateur Black : Vous considérez que ce serait un mécanisme plutôt qu'une monnaie?

M. Clark : Oui.

[*Français*]

La sénatrice Bellemare : J'ai deux questions pour vous et voici la première : Hier, nous avons reçu des gens de la Banque du Canada qui nous ont parlé des bitcoins comme d'une réserve de valeur. Nous savons tous que le bitcoin a une grande volatilité. On nous a dit également qu'il existait, dans certains pays, des organisations privées comme BitPay qui s'occupaient de convertir rapidement les bitcoins en monnaie locale. Connaissez-vous un peu ces institutions?

Les gens de la Banque du Canada nous disaient que le bitcoin était beaucoup utilisé comme mode de paiement et que les gens, lorsqu'ils l'utilisaient à l'international, faisaient rapidement la conversion avant que le bitcoin ne perde de la valeur.

Connaissez-vous un peu ces organisations comme BitPay? Comment font-ils leur argent? Prennent-ils le risque de convertir cette monnaie en monnaie locale?

[*Traduction*]

M. Clark : Si j'ai bien compris votre question, vous voulez savoir en quoi consiste le modèle utilisé pour les échanges, surtout étant donné l'extrême volatilité du bitcoin.

Les plates-formes offrent un service de jumelage entre les personnes qui ont des bitcoins et qui souhaitent obtenir la devise locale, et celles qui ont la devise locale et souhaitent obtenir des bitcoins. Elles tendent parfois à garder beaucoup de bitcoins, ce qui entraîne un léger risque en raison des fluctuations des taux de change. Toutefois, selon leur modèle d'entreprise général, elles perçoivent des frais de transaction pour l'échange de devises, indépendamment du taux de change. Elles font de l'argent tant qu'il y a de la demande des deux côtés.

[*Français*]

La sénatrice Bellemare : Y a-t-il d'autres entreprises comme BitPay sur le marché ou est-ce que cette entreprise a le monopole de ce genre de transaction présentement?

[*Traduction*]

M. Clark : Les plates-formes sont nombreuses. BitPay n'est qu'une parmi tant d'autres. À l'heure actuelle, je crois qu'on assiste à un regroupement. Il y a certaines grandes plates-formes. Je n'ai pas fait le calcul, mais à mon avis, c'est un rapport de 80 à 20, c'est-à-dire que 80 p. 100 des échanges passent par 20 p. 100 des plates-formes. C'est probablement encore plus que cela. Je crois que la grande majorité des échanges se font par l'entremise de trois grandes plates-formes.

[*Translation*]

Senator Bellemare: What you are telling me is that, basically, BitPay operates like a stock exchange: it provides the users with a service and also establishes the exchange rate.

[*English*]

Mr. Clark: The exchange rate is not established by any exchange. It's just established by supply and demand on both sides.

In terms of BitPay, if I recall correctly — there are so many of these exchanges, and they all have similar names — they do operate as an exchange, but they're one of the companies that provides more of the bitcoin pipe so that companies can use them in order to exchange fiat currency into bitcoin, send it through the pipe and have it come out the other end. I forget exactly if that's BitPay's business model. In that case, they do operate an exchange; plus, they have additional services on top of that.

[*Translation*]

Senator Bellemare: My next question deals with the network and the people behind the system. As I understand it, during a Bitcoin transaction, the network is alerted and the miners behind the scenes solve the mathematical problem. We have learned that those miners are paid in bitcoin. Do you have an idea of the amount of bitcoin going into the pockets of these invisible people working behind the scenes?

[*English*]

Mr. Clark: First, I'll give you a little more detail of how the network works, and then I'll try to answer your question, which is: How many people behind the scenes have these bitcoins? The way it works is if I send you money, for example, I'll broadcast it to the network, and the network is going to add it to the ledger. The problem is that what you want is everyone on the network to verify that that update was correct, that I didn't spend more money than I have, that I actually have signing authority over the account.

What you want to avoid is a scenario where the ledger updates too quickly. If it updates really fast, then the other computers won't be able to keep up. If you want to start from the beginning of bitcoin time and go through the ledger from the beginning all the way through, you need to be able to do that in a reasonable amount of time as well. For that reason, the protocol puts in an artificial delay which slows things down, so it makes sure that the ledger updates on the order of about every 10 minutes.

You've referred to a computational problem. The way they do it is they give this computational problem that's hard to do, and it's not inherent to the currency at all; it's basically an artificial delay to slow things down, to make sure lots of verification happens. That's why it takes about 10 minutes. Because there are mining rewards and fees, the miner gets both the fees and the mining reward.

Senator Bellemare: There are fees, too?

[*Français*]

La sénatrice Bellemare : Ce que vous me dites, c'est que BitPay, au fond, fonctionne plutôt comme une bourse : elle donne le service à l'utilisateur et établit également le taux de change.

[*Traduction*]

M. Clark : Le taux de change n'est pas établi par les plates-formes d'échange, seulement en fonction de l'offre et de la demande des deux côtés.

En ce qui a trait à BitPay, si je me souviens bien — il y a tellement de plates-formes, et leurs noms se ressemblent tous —, l'entreprise agit à titre de plate-forme d'échange, mais elle fait partie des entreprises qui agissent à titre de conducteurs, qui permettent aux entreprises d'échanger la monnaie fiduciaire contre des bitcoins. Je ne sais plus si c'est le modèle d'entreprise de BitPay. Si c'est le cas, c'est une plate-forme d'échange qui offre en plus d'autres services.

[*Français*]

La sénatrice Bellemare : Ma prochaine question a trait au réseautage et aux gens derrière ce système. Si je comprends bien, lors d'une transaction en bitcoins, le réseautage est alerté et les mineurs résolvent le problème mathématique. On a appris que ces mineurs étaient payés en bitcoins; avez-vous une idée de la quantité de bitcoins qui se retrouve dans les poches des gens qui travaillent derrière le rideau et qui sont invisibles?

[*Traduction*]

M. Clark : Je vais d'abord vous expliquer plus en détail le fonctionnement du réseau, puis je tenterai de répondre à votre question, c'est-à-dire : combien y a-t-il de gens derrière les bitcoins? Si je vous envoie de l'argent, par exemple, je l'envoie sur le réseau, et il est ajouté au registre. Le problème, c'est qu'on veut que tous les intervenants du réseau vérifient l'exactitude de cette mise à jour, que je n'ai pas dépensé plus d'argent que je n'en possède, et que j'ai le pouvoir de signature pour le compte.

Il faut éviter de mettre à jour le registre trop rapidement. Si c'est le cas, les autres ordinateurs ne pourront pas suivre le rythme. Il faut pouvoir consulter toutes les transactions du registre selon un délai raisonnable. Par conséquent, le protocole ajoute un délai artificiel qui ralentit le processus, de sorte que le registre soit mis à jour toutes les 10 minutes environ.

Vous avez parlé de résoudre des problèmes mathématiques. Ils n'ont rien à voir à la monnaie, mais visent à créer un délai artificiel qui ralentit les choses, pour qu'on puisse faire de nombreuses vérifications. C'est pour cela qu'il faut compter environ 10 minutes pour une transaction. Il y a des frais et récompenses; le mineur obtient les droits et les récompenses.

La sénatrice Bellemare : Il y a des frais, aussi?

Mr. Clark: Yes. They are very small, but there are fees. The miner is the one who gets that fee. What you get is a competitive environment where all the miners are trying to compete to be the one that sells the block, because they're the ones who will get the fees and the mining reward. Because it's competitive, it leads to these roughly incentive-compatible things that make sure all the verification works. The design of it is intricate.

The question is: How much of the currency is held by the miners themselves? We know that a large amount was held by the first miner, the first person who started mining it, which was likely the person who created the currency. He or she or they hold a lot of the currency in reserves. It's safe to say that the miners hold a significant amount, but we don't have numbers for that.

Senator Bellemare: Do we know how many miners there are?

Mr. Clark: We know in terms of computational power, how much power they have. You can see how long it takes them to solve the puzzle, and then you can determine how many computers you would need to solve it, and then you have a sense of how much computation they have.

Senator Bellemare: Are those people at home waiting for an alert? Is that how they work?

Mr. Clark: In terms of the alert, that happens automatically. There's no human in the loop; it's just a computer that's set up. The computer receives it digitally and processes it. Originally, it was people at home, but now that the mining reward is substantially high, people have taken more of a commercial approach to mining. People buy specialized hardware. They hold it in typical server rooms. You're not going to make any money mining from home on a computer anymore.

Senator Greene: Thank you very much. As you're aware from your work in the area, we live today in a rapidly changing digital environment in which new products happen all the time. In fact, the rate of change is speeding up. That's certainly my perception.

Could we not be in a position five or ten years from now where you could have 30 or 40 or maybe 50 digital currencies competing for space in the international environment?

Mr. Clark: Yes. That's certainly one outcome that people consider. Even now, we've seen the emergence of something that's generally called altcoins. They're alternatives to bitcoins. There are a lot of them out there. They are competing to a certain extent, but bitcoin is far and away the most prominent one.

Senator Greene: It is now, but there could come a time — and I suspect there will come a time — when somebody will create a currency that is perceived to be better, maybe more anonymous or less anonymous, or with lower transaction costs, et cetera, that would challenge bitcoin. Currencies might come and go rather

M. Clark : Oui. Ils sont minimes, mais il y en a. Cet argent va aux mineurs. C'est un environnement concurrentiel où tous les mineurs se font concurrence pour vendre les blocs, parce qu'ils récolteront les droits et les récompenses. Puisqu'il s'agit d'un environnement concurrentiel, il donne lieu à des mesures compatibles avec les incitatifs, qui permettent de veiller à ce que toutes vérifications fonctionnent. C'est une structure complexe.

Vous voulez savoir quelle part de la monnaie appartient aux mineurs. Nous savons que le premier mineur — et probablement la personne qui a créé la monnaie — en détenait une grande quantité. Cette personne ou ces personnes ont une grande quantité de monnaie dans des réserves. On peut affirmer que les mineurs en possèdent une grande quantité, mais nous n'avons pas les chiffres exacts.

La sénatrice Bellemare : Est-ce qu'on sait combien il y a de mineurs?

M. Clark : On peut le déduire en fonction de leur puissance de calcul. En calculant le temps nécessaire pour résoudre une énigme on peut déterminer le nombre d'ordinateurs utilisés, et donc la capacité des mineurs.

La sénatrice Bellemare : Est-ce que ces personnes sont chez elles et attendent une alerte? Est-ce que c'est comme cela qu'ils travaillent?

M. Clark : L'alerte se fait automatiquement. Il n'y a pas d'intervention humaine; l'ordinateur reçoit la demande de façon numérique et la traite. Au départ, les demandent étaient traitées par des gens à la maison, mais comme les récompenses sont aujourd'hui assez importantes, les gens ont adopté une approche plus commerciale. Ils achètent de l'équipement spécialisé, qu'ils installent dans des salles de serveurs. On ne peut plus faire d'argent avec un ordinateur personnel.

Le sénateur Greene : Merci beaucoup. Comme vous le savez, nous vivons dans un environnement numérique en constante évolution, et de nouveaux produits sont créés tous les jours. En fait, les changements se font de plus en plus rapides. C'est ma perception.

Est-ce qu'on pourrait se retrouver dans 5 ou 10 ans avec 30, 40 ou même 50 monnaies numériques qui se feraient concurrence sur le marché international?

M. Clark : Oui. C'est ce qu'on pense. Déjà, on a vu apparaître ce qu'on appelle les atlcoins. Il y en a beaucoup en circulation. Ils font concurrence aux bitcoins, dans une certaine mesure, mais les bitcoins demeurent de loin les plus utilisés.

Le sénateur Greene : C'est la situation actuelle, mais il se peut — et je crois que cela va arriver — qu'on crée une monnaie que l'on jugera meilleure que les bitcoins, qui sera peut-être plus ou moins anonyme ou dont les coûts de transaction seront moins élevés, et cetera, et qui remettra en cause les bitcoins. Les

quickly. How convertible are these digital currencies with each other?

Mr. Clark: To address your first point, even today with these altcoins I referred to, they are trying to improve on the design of bitcoin in some aspect. Generally, they shorten the delay from 10 minutes down to a shorter time. Some of them are looking at making it more anonymous. Some of them change this computational puzzle so it consumes less electricity. Those are some of the changes that people are interested in. Yes, I do think you will see competition. There will be different currencies. As a consumer or a company, depending on the properties you want, you'll choose the currency that gives you the properties that are as close as possible to the ones you want.

In terms of exchanging between digital currencies, exchanges also offer this service. Once again, it's just a demand-based thing. If I have bitcoin and I want to change them into peercoin, and someone else wants to change peercoin into bitcoin, then the exchanges that exist today will facilitate those transactions.

A lot of them, though, do go through bitcoin as a common currency. Bitcoin is exchangeable with everything else, but the other ones aren't necessarily exchangeable with each other yet. But that's something that could change.

Senator Greene: With regard to regulation, it seems to me that national regulation is a bit problematic. Do you think that international regulation is required at some level, at some point, in order to be effective?

Mr. Clark: I'm not an expert on regulatory issues, so I can't really comment. I know that in other spheres that involve things on the Internet, new technologies and things that people are concerned with, such as piracy and that type of thing, there are international organizations that try to step in and at least suggest what regulation should look like, and then it's up to countries to sign on. It wouldn't surprise me to see that, but I have no opinion about whether that's better or worse.

Senator Greene: Do you have any bitcoin?

Mr. Clark: I do, yes.

Senator Greene: How long have you had it?

Mr. Clark: I've had them for several years.

Senator Greene: And you've watched them go up and down?

Mr. Clark: That's right, yes.

Senator Greene: Have you purchased anything with bitcoin?

Mr. Clark: No, I haven't. I've held on to them. Because I do research in this area, they're useful for me to have for research purposes. Because I bought them — or I obtained them. They

monnaies risquent d'apparaître et de disparaître assez rapidement. Est-ce que ces monnaies numériques sont facilement convertibles?

M. Clark : Je vais d'abord répondre à la première partie de votre question; déjà aujourd'hui, on tente d'améliorer le concept des bitcoins, avec les altcoins dont j'ai parlé, par exemple. En gros, on a réduit le délai, qui est inférieur à 10 minutes. Certaines entreprises tentent d'offrir un processus plus anonyme. D'autres modifient le casse-tête informatique afin de réduire la consommation d'électricité. Ce sont certains des changements qui intéressent les gens. Oui, je crois que la concurrence va s'accroître. Diverses monnaies seront offertes. Les consommateurs et les entreprises pourront choisir la monnaie dont les propriétés correspondent le mieux à leurs besoins.

Les plates-formes d'échange offrent des services de conversion des devises numériques. Encore une fois, c'est un système fondé sur la demande. Si j'ai des bitcoins et que je veux les échanger contre des peercoins, et qu'une autre personne veut échanger ses peercoins contre des bitcoins, alors les plates-formes d'échange permettront ces transactions.

La plupart de ces plates-formes utilisent toutefois le bitcoin à titre de monnaie commune. On peut échanger le bitcoin contre toute autre monnaie, mais les autres monnaies ne sont pas toutes aussi facilement interchangeables pour le moment. Cela pourrait toutefois changer.

Le sénateur Greene : Il me semble que la réglementation est problématique. Croyez-vous qu'il faudra éventuellement mettre en œuvre un règlement international pour veiller à l'efficacité du système?

M. Clark : Je ne suis pas un expert des questions réglementaires; je ne peux donc pas vraiment me prononcer. Je sais que dans certains autres domaines, qui sont associés à l'utilisation d'Internet et des nouvelles technologies, et à des questions de préoccupation comme la protection des renseignements personnels, entre autres, il y a des organisations internationales qui tentent à tout le moins de proposer un modèle de réglementation; la décision revient ensuite à chaque pays. Je ne serais pas surpris de voir cela, mais je ne sais pas si ce serait mieux ou pire.

Le sénateur Greene : Avez-vous des bitcoins?

M. Clark : Oui, j'en ai.

Le sénateur Greene : Depuis combien de temps?

M. Clark : Je les ai depuis plusieurs années.

Le sénateur Greene : Et vous avez vu leur valeur fluctuer?

M. Clark : C'est cela, oui.

Le sénateur Greene : Avez-vous fait des achats avec vos bitcoins?

M. Clark : Non. Je les garde. Ils me sont utiles dans ma recherche. Je les ai achetés — ou je les ai obtenus; ils m'ont été offerts en cadeau. Je m'en suis procuré de diverses façons, mais je

were actually a gift. I've acquired them through different means, but I mean the original set. They were worth a lot less. Psychologically, I don't maybe attribute the full value to them, even though they're worth a lot. If I had put out that much money to obtain them, I would treat them with more security than I actually do.

Senator Greene: Thank you.

[*Translation*]

Senator Rivard: Yesterday, we had a presentation from officials from the Bank of Canada. I will not go over everything that was said. But one part made an impression on me, a slide called "The Potential Role," which I would describe as synonymous with "Advantages." They talked to us about the reduced costs of financial intermediation, the irreversibility of payments, and something they called the "high degree of privacy"; not the "degree of privacy," but the "high degree."

When I hear things like that, I think about money laundering. You mentioned it a little earlier. It was your impression that money launderers will always stay faithful to the exchange rate and that Bitcoin are not of interest because you said that they could be traced back almost as easily as someone using an exchange. Is that what you said, actually?

It is your impression that money launderers are not interested in Bitcoin, but will just carry on. I would love to hear from officials at the Canada Revenue Agency to see if they are as optimistic as you have been. My impression is that they will focus on the exchanges and that they will not be interested in Bitcoin as such.

[*English*]

Mr. Clark: The question, I guess, is on money laundering and whether launderers are interested in bitcoin, and in terms of exchanges as well. As I mentioned, in order to obtain bitcoins, you do have to go through exchanges. Right now there are no regulations on exchanges, I believe, that apply. I believe most exchanges based in Canada voluntarily subscribe to the regulations that would be imposed, under their best estimate of what would happen. That does make it less attractive.

The fact that it is traceable presents new technical challenges because, as I mentioned, law enforcement have pretty decent mechanisms for tracing Internet packets, so you have to worry about the traceability on that front as well. Yes, it's completely possible that money launderers would not prefer to use bitcoin. I'm not exactly sure.

[*Translation*]

Senator Bellemare: I was under the impression that the countries using bitcoin the most are the United States, Canada, Australia, and perhaps England, the United Kingdom, because there has been no mention of countries that use the euro. Would

parle des premiers bitcoins que j'ai eus. Ils valaient beaucoup moins qu'aujourd'hui. Sur le plan psychologique, je ne leur attribue peut-être pas leur pleine valeur, même s'ils valent beaucoup. S'ils m'avaient coûté le prix qu'ils valent aujourd'hui, je leur ferais sûrement beaucoup plus attention.

Le sénateur Greene : Merci.

[*Français*]

Le sénateur Rivard : Hier, nous avons eu une présentation des représentants de la Banque du Canada. Je ne reprendrai pas tout ce qui a été dit. Mais un élément m'a impressionné, une fiche intitulée « Le rôle potentiel », que je qualifierait de synonyme d'avantages. Ils nous parlaient de la réduction des coûts associés à l'échange, des paiements irréversibles et d'une chose qu'ils ont appelée « caractère hautement confidentiel »; pas « caractère confidentiel », mais « hautement confidentiel ».

Quand on parle de cela, on pense au blanchiment d'argent. Vous en avez parlé un peu plus tôt. Vous aviez l'impression que les blanchisseurs d'argent vont toujours rester fidèles au bureau de change et que les bitcoins ne sont pas intéressants parce que vous avez dit qu'on pouvait les retracer presque aussi facilement que quelqu'un qui utilise un bureau de change. C'est bien ce que vous avez dit?

Vous avez l'impression que les blanchisseurs d'argent ne sont pas intéressés aux bitcoins, mais vont plutôt continuer. J'ai hâte d'entendre les représentants de l'Agence du revenu du Canada pour voir s'ils sont aussi optimistes que vous l'avez été. J'ai l'impression qu'ils vont se concentrer sur les bureaux de change et que les bitcoins ne seront pas intéressants pour eux.

[*Traduction*]

M. Clark : Si je comprends bien, votre question porte sur le blanchiment d'argent et sur l'intérêt des blanchisseurs pour les bitcoins, et aussi sur les plates-formes d'échange. Comme je l'ai dit, pour obtenir des bitcoins, il faut passer par les plates-formes d'échange. À l'heure actuelle, ces plates-formes ne sont pas réglementées. Je crois que la plupart des plates-formes du Canada se conforment volontairement aux règlements qui s'imposeraient, selon leur meilleure estimation. Elles sont donc moins attrayantes.

Comme les transactions sont traçables, elles représentent un nouveau défi technique puisque, comme je l'ai dit, les organismes d'application de la loi sont dotés de mécanismes assez efficaces pour retracer les paquets Internet; il faut donc penser à la traçabilité. Oui, il est tout à fait possible que les blanchisseurs d'argent préfèrent ne pas utiliser de bitcoins. Je n'en suis pas certain.

[*Français*]

La sénatrice Bellemare : J'avais l'impression que les pays qui utilisaient le plus les bitcoins étaient les États-Unis, le Canada, l'Australie et peut-être l'Angleterre et le Royaume-Uni, car on n'a pas mentionné de pays qui utilisent l'euro. Est-ce que l'utilisation

the use of bitcoin be less attractive in the euro zone because people can already do business with a common currency and because there is perhaps a link with the fact that a large number of people using the euro makes it easier to use in transactions?

Do you see a link between the use of a single currency in European countries and the use of individual currency in other countries?

[*English*]

Mr. Clark: Your question is if there's any connection between the use of euros, which is already international currency, and bitcoin.

First off, I don't know for sure, I haven't seen numbers, but I've heard that Germany is one of the most accepting of bitcoin.

[*Translation*]

Senator Bellemare: So my premise is not correct because you are saying that Germany is a major user of bitcoin.

[*English*]

You're saying Germany, even though they're using the euro.

Mr. Clark: That's right.

Senator Bellemare: Perhaps my hypothesis wasn't correct.

Mr. Clark: That's true. It's an interesting question to think about, whether that type of currency that you can take across borders, whether bitcoin competes with that property of currency. I'm not sure we've seen evidence that it does. When I think about bitcoin, I'm primarily thinking about online transactions as the main potential. I'm not sure it competes necessarily.

The Deputy Chair: As I have no other names, I have a few questions.

Your second point was the secure cryptography, that there were some algorithms that were probably very difficult. If Mr. Snowden would like to enter into the business, do you think he would have much problem? He seems to be good at it. The NSA in the United States probably has good algorithms and he went into their computer and got the information. We know that year after year — it's not published — our banks are also victims of people going into their computers. Could you clarify that question of security?

Mr. Clark: Sure, that's a very good question. We don't obviously know what intelligence agencies know in terms of cryptographic breaks on cryptographic elements. Is there the potential that the NSA, or CSEC in Canada, has the ability to break things like bitcoin?

des bitcoins serait moins encouragée dans la zone euro, parce que les gens sont déjà capables de transiger avec une monnaie unique et qu'il y aurait peut-être un lien à faire avec le fait qu'il y a beaucoup d'habitants qui utilisent l'euro et que ce serait donc plus facile de faire les transactions?

Voyez-vous un lien entre l'utilisation d'une monnaie unique dans les pays européens et l'utilisation des monnaies individuelles des pays en général?

[*Traduction*]

M. Clark : Vous me demandez s'il existe un lien entre l'utilisation de l'euro — qui est déjà une monnaie internationale — et les bitcoins.

D'abord, je ne pourrais vous répondre avec certitude; je n'ai pas vu les chiffres, mais j'ai entendu dire que les Allemands étaient les plus grands utilisateurs du bitcoin.

[*Français*]

La sénatrice Bellemare : Ma prémisse n'était donc pas correcte puisque vous dites que l'Allemagne est un grand utilisateur de bitcoins.

[*Traduction*]

Vous parlez de l'Allemagne, même si elle utilise l'euro.

M. Clark : C'est cela.

La sénatrice Bellemare : Mon hypothèse n'était peut-être pas fondée.

M. Clark : C'est vrai. C'est une question intéressante, à laquelle il faudrait réfléchir. Il faut se demander si le bitcoin peut faire concurrence à ce type de devise, qui traverse les frontières. Je ne sais pas si on peut le prouver. Les bitcoins sont surtout utilisés pour les transactions électroniques. Je ne sais pas si ces devises se font concurrence.

La vice-présidente : Comme il n'y a plus de nom sur ma liste, j'aimerais vous poser quelques questions.

Vous avez parlé de cryptographie sécurisée, et de certains algorithmes très complexes. Si M. Snowden souhaitait pénétrer le système, croyez-vous qu'il y arriverait? Il semble s'y connaître. La NSA des États-Unis est probablement dotée de bons algorithmes, et il a réussi à entrer dans son système informatique pour obtenir des renseignements. Nous savons qu'année après année — ce n'est pas publié —, nos banques sont également victimes de piratage. Pourriez-vous expliquer la question de la sécurité?

M. Clark : Bien sûr, c'est une très bonne question. Nous ne savons pas ce que savent les organismes de renseignements au sujet des bris associés aux éléments cryptographiques. Est-ce que la NSA ou le CSTC au Canada sont capables de déchiffrer des systèmes comme le bitcoin?

I watched the Snowden revelations closely, and the feeling I and most of the cryptographic community got from them is they're interested in attacking what's called the end point. If you think of cryptography as a tunnel, the message has to go in somewhere and come out somewhere. That's where they're attacking. They're not actually attacking the tunnel itself. None of the revelations suggested they have any potential to break new things that we didn't know about. I can't say, it's unknowable, but there's no indication in any way they have special abilities to break it.

The second point I would make is that a lot of the cryptography that underlies bitcoin also underlies standard transactions online. If you send your credit card online it goes over SSL which is the cryptographic tunnel that protects those credit card numbers. Depending exactly on what algorithms they have, my sense is any major break they have against bitcoin could apply to those algorithms as well. I don't think you go after bitcoin if you have that ability.

The Deputy Chair: Yes, but you have many others that are creating other electronic currency. I guess each one has a different algorithm?

Mr. Clark: I can get into the details. There are basically two algorithms. One gives you signing authority over the account, and that tends to be the same across all currencies. The other is what's called a hash function, which is used in maintaining the ledger, making sure the ledger is correct and kept orderly.

Specific points where the hash function is used do tend to differ from currency to currency. It's maybe not as security-critical as the signature scheme. If you can break the signature scheme you can basically steal everyone's money. That's the most substantial reliance on cryptographic algorithms, and that one, we're fairly confident, is secure.

The Deputy Chair: Going back to what Senator Tkachuk said before, it's a commodity. You were talking about those who were mining the system. I had the impression that it would be like when we buy shares, when a new mine is developed and there is no production. It's just a piece of paper and we buy the possibility that one day there will be gold or silver.

The bitcoin itself is a market. If I buy U.S. dollars and intend to make money just in dealing with money, I can do it. I can be in the business of making money with bitcoin and I can use it to buy other goods.

Where do you see the development? Is it on bitcoins themselves or as a tool to buy? As a tool to buy, we have to do all these transactions with money already to get the bitcoin, so why bother doing all of this? Would it be better to say this would be more of a business itself in dealing with bitcoin?

Mr. Clark: To your first question, there are definitely people who hold bitcoin for both purposes: one is to transact in bitcoin and the other is to hold it more like a commodity, like a

J'ai écouté avec attention les révélations de M. Snowden, et la plupart des membres de la communauté cryptographique en ont conclu qu'on voulait surtout s'attaquer au point final. On peut comparer la cryptographie à un tunnel; il faut que le message entre et sorte quelque part. C'est à ce message qu'on s'attaquait, et non au tunnel en soi. Les révélations n'ont pas permis de déterminer si on pouvait pirater de nouvelles composantes. Je ne dis pas que ce n'est pas possible, mais je ne crois pas qu'on ait de capacités particulières pour le faire.

Ensuite, la cryptographie qui sous-tend le bitcoin est en grande partie identique à celle associée aux transactions habituelles en ligne. Si vous transmettez les renseignements de votre carte de crédit en ligne, ils passent par le protocole SSL, qui constitue le tunnel cryptographique qui protège les numéros des cartes de crédit. À mon avis, tout bris des algorithmes des bitcoins peut s'appliquer à ces algorithmes également. Je ne crois pas qu'on s'attaquerait aux bitcoins si on avait cette capacité.

La vice-présidente : Oui, mais on crée de nombreuses monnaies électroniques; je suppose que chacune d'entre elles a un algorithme différent?

M. Clark : Je peux entrer dans les détails. Il existe essentiellement deux algorithmes. L'un vous donne le pouvoir de signature pour un compte, et il semble être le même pour toutes les monnaies. L'autre, qu'on appelle la fonction de hachage, sert à tenir le registre, à veiller à ce qu'il soit en bon ordre.

L'utilisation de la fonction de hachage semble varier d'une monnaie à l'autre. Elle n'est peut-être pas aussi critique sur le plan de la sécurité que le schéma de signature. Si l'on peut pénétrer le schéma de signature, on peut essentiellement voler l'argent de tout le monde. C'est là où l'on se fie le plus aux algorithmes cryptographiques, et nous croyons qu'ils sont assez sécuritaires.

La vice-présidente : J'aimerais revenir sur les propos du sénateur Tkachuk, sur l'utilisation des bitcoins à titre de marchandise. Vous parliez des mineurs du système. J'ai l'impression qu'on peut comparer cela à l'achat d'actions, lorsqu'on aménage une nouvelle mine et qu'il n'y a pas encore de production. Ce n'est qu'un bout de papier, et on l'achète en espérant que la mine produira de l'or ou de l'argent.

Le Bitcoin est un marché en soi. Je suis libre d'acheter des dollars américains dans le seul but de m'enrichir en faisant des transactions, et je peux donc en faire autant avec des bitcoins, et m'en servir pour acheter d'autres biens.

En quoi les choses ont-elles changé? Parlons-nous des bitcoins proprement dits ou de la possibilité de s'en servir comme mode de paiement? S'il s'agit du mode de paiement, il faut déjà faire de nombreuses transactions monétaires pour en obtenir. Pourquoi se donner tout ce mal? Ne serait-il pas préférable de dire qu'effectuer des transactions avec des bitcoins serait plutôt une activité en soi?

M. Clark : Pour répondre à votre première question, il y a sans aucun doute des gens qui se procurent des bitcoins pour ces deux activités : faire des transactions et s'en servir davantage comme

speculative instrument. They compete, I would argue, because if I buy shares in companies, it's not because I want to spend those shares in order to actually transact with them.

I think the main people, the developers of the software, their intention is to try to encourage bitcoin to move more towards being a currency and not a speculative instrument or a commodity. A lot of the businesses are set up around trying to use it as a currency, and that's essentially their business model. People are willing to spend these bitcoins. They don't want to hold onto them. They're willing to actually spend them in order to complete transactions.

The Deputy Chair: I am tempted to say it would be mostly people less than 30 years of age who would do business like that rather than people over 50 years of age. I think people have to really be part of the computer culture rather than senior citizens trying to do this. I look at this and, even after a few weeks of meeting with experts like you, I would have a problem explaining that to somebody not familiar with this, even though I have received a lot of good information.

I'd like to thank you for providing your part. I'm sure my colleagues appreciate your knowledge.

I look forward to seeing what our researchers produce as a report, because they put all the pieces together. We will have to look at this and see where we go with that. Thank you very much.

Mr. Clark: Thank you.

Senator Irving Gerstein (*Chair*) in the chair.

The Chair: During this second hour of the meeting, we have the opportunity to receive a presentation from Mr. David Descôteaux, Associate Researcher at the Montreal Economic Institute.

In January of 2014, Mr. Descôteaux published an economic note entitled *Bitcoin: More Than a Currency, a Potential for Innovation*. This note offers an overview of the bitcoin phenomenon and issues that it raises.

Mr. Descôteaux, thank you for accepting this invitation to appear before us. You have the floor, and we will follow with questions after your presentation.

[*Translation*]

David Descôteaux, Associate Researcher, Montreal Economic Institute, as an individual: Hello and thank you very much for this opportunity. I am honoured to be here.

I am currently an associate researcher at the Montreal Economic Institute and I have reported on economic issues for radio and for magazines. In recent years, I have worked mainly in journalism and writing for the general public, so I will offer a kind

marchandise, comme instrument de spéculation. Je dirais que les deux se font concurrence, car si j'achète des actions de sociétés, ce n'est pas dans le but de faire des transactions.

Je pense que l'intention des principaux concernés, les créateurs du logiciel, est plutôt de faire en sorte que les bitcoins deviennent une monnaie, pas un instrument de spéculation ou une marchandise. Beaucoup d'entreprises sont créées dans le but de s'en servir comme monnaie, et c'est essentiellement leur modèle d'affaires. Les gens sont disposés à dépenser des bitcoins. Ils ne veulent pas les conserver. Ils sont prêts à les dépenser pour faire des transactions.

La vice-présidente : J'ai envie de dire que ce serait surtout des personnes âgées de moins de 30 ans plutôt que du monde âgé de plus de 50 ans qui mèneraient des activités de cette façon. Je pense qu'il faut vraiment faire partie de la culture de l'informatique et que cela ne concerne pas les personnes âgées. J'étudie la question, et même après quelques semaines de rencontres avec des experts comme vous, j'aurais quand même de la difficulté à expliquer ce qu'il en est à quelqu'un qui ne connaît pas bien le sujet, malgré toute l'excellente information que j'ai entendue.

J'aimerais vous remercier d'avoir apporté votre contribution. Je suis certaine que mes collègues vous sont reconnaissants de nous avoir fait part de vos connaissances.

Je suis impatiente de voir le rapport qui sera préparé par nos chercheurs, car ils réunissent les divers éléments. Nous devrons y jeter un coup d'œil pour déterminer ce que nous ferons dans ce dossier. Merci beaucoup.

M. Clark : Merci.

Le sénateur Irving Gerstein (*président*) occupe le fauteuil.

Le président : Durant la deuxième heure de la séance, nous aurons l'occasion d'entendre l'exposé de M. David Descôteaux, chercheur associé à l'Institut économique de Montréal.

En janvier 2014, M. Descôteaux a publié une note économique intitulée *Bitcoin : plus qu'une monnaie, un potentiel d'innovation*. On y donne une vue d'ensemble de l'avènement des bitcoins et des questions que cela soulève.

Monsieur Descôteaux, merci d'avoir accepté notre invitation. Vous avez la parole, et nous allons poser des questions après votre exposé.

[*Français*]

David Descôteaux, chercheur associé, Institut économique de Montréal, à titre personnel : Bonjour à tous et merci beaucoup de cette opportunité, vous m'en voyez honoré.

Je suis actuellement chercheur associé à l'Institut économique de Montréal et aussi chroniqueur économique à la radio et dans certains magazines. Mon expérience des dernières années en est surtout une de journalisme et de vulgarisation, donc je vais

of "Bitcoin 101." In other words, I will present it from the perspective of the average person since I am not an expert in computer science or monetary issues.

That said, in January, I published an economic note on Bitcoin, which is intended as an introduction to the subject for the general public. Without going into too many technical details, the document explained how the virtual currency works. It also touched on the benefits Bitcoin offers retailers and consumers, such as lower transaction fees. These benefits are derived from Bitcoin's main features — a decentralized network of cryptographic security — which do not require users to fill out forms with their personal information or pay transaction fees to third parties to process their payments, as is the case with Visa or PayPal, for example.

I also pointed out that Bitcoin has the potential to improve the way financial services are delivered. You may have heard this from other people as well. For example, Bitcoin could eventually be used for international money transfers like those handled by companies such as Western Union, given the relatively high transaction fees these companies charge.

However, the use of Bitcoin for this type of transaction depends on one element in particular: transaction fees must return remain low because that is Bitcoin's main advantage. And there are several reasons why there is no guarantee that fees will remain low. We can talk more about that when we move on to questions.

In my economic note, I also explained the challenges that Bitcoin must overcome in order to be more widely used. These challenges include a reputation for use in illegal activities, its high volatility, and security and fraud issues.

Bitcoin is two things: it is a digital currency and, in particular, it is a payment system. This is demonstrated by the many start-ups that are constantly inventing new products and services related to Bitcoin.

Several companies offer what is probably the best-known and most useful Bitcoin service: they allow merchants to convert Bitcoin to dollars or other currency almost instantly in return for a small fee. Just about a year ago, these merchants were still reluctant to accept Bitcoin as payment for fear that their value would plummet within a few hours or days of the transaction. Now that risk is borne by the company offering this service.

One subject that has caught my attention is the financial industry's interest, or lack of interest, in Bitcoin. A few months ago, Wells Fargo invited government officials and other participants to a meeting on Bitcoin. According to a report in the *Financial Times*, the purpose of the meeting was to explore

présenter ici ma vision plutôt pratico-pratique de Bitcoin, c'est-à-dire du point de vue de monsieur et madame Tout-le-monde, n'étant pas moi-même un expert en informatique ni un spécialiste des questions monétaires.

Ceci dit, j'ai publié en janvier dernier une note économique sur Bitcoin qui se voulait surtout une introduction pour le public en général. La note expliquait la mécanique derrière cette monnaie virtuelle sans aller trop dans les détails techniques. Je parlais entre autres des avantages de Bitcoin pour les commerçants et consommateurs, par exemple les coûts de transaction moins élevés. Ces avantages viennent du fait que les principales caractéristiques de Bitcoin — c'est un réseau décentralisé, doté d'une sécurité cryptographique — font que dans la plupart des transactions, l'utilisateur n'a pas à remplir des formulaires contenant des informations personnelles ou à payer des frais de transaction à une tierce partie, un peu comme c'est le cas avec le paiement des cartes de crédit par exemple.

Je soulignais également que Bitcoin avait un certain potentiel de bonifier l'offre actuelle de services financiers. Par exemple, et d'autres avant moi vous en ont peut-être déjà parlé, le transfert d'argent international, un peu comme le fait une entreprise comme la Western Union, pourrait être une niche d'avenir pour Bitcoin en raison des frais de transaction relativement élevés qu'on y trouve.

Par contre, l'intérêt de Bitcoin pour ce genre de transaction dépend d'une chose en particulier, c'est que les frais de transaction demeurent bas, puisque c'est son principal avantage et, pour toutes sortes de raisons, il n'est pas dit que ces frais vont demeurer bas. Nous pourrons en parler plus en détail au cours de la période de questions.

Ma note économique expliquait aussi les défis que Bitcoin doit surmonter s'il veut être utilisé à plus grande échelle. Parmi ces défis, il y a le risque que sa réputation puisse être utilisée surtout à des fins illicites, la grande volatilité du bitcoin et les questions de sécurité et de fraude.

Bitcoin représente deux choses : c'est une monnaie numérique, mais c'est aussi et surtout un système de paiement. C'est une technologie qui contient un grand potentiel d'innovation, tel que le démontrent de nombreuses jeunes entreprises qui inventent chaque jour ou presque des services liés à Bitcoin.

Le plus connu — et utile — de ces services est probablement le service de conversion instantanée de bitcoins en dollars ou autres devises que certaines entreprises offrent aujourd'hui à des commerçants en échange d'un frais minime. Il y a à peine un an, ces commerçants hésitaient encore à accepter cela de peur de voir leur valeur chuter dramatiquement quelques heures ou quelques jours après la transaction. Maintenant, le risque est soutenu par ces services.

Un sujet qui m'intéresse aussi est l'intérêt — ou l'absence d'intérêt — de l'industrie financière envers Bitcoin. Il y a quelques mois, la banque Wells Fargo aux États-Unis a démontré un certain intérêt pour Bitcoin, en organisant une rencontre qui incluait, entre autres, des représentants du gouvernement. Selon le

what kind of Bitcoin services banks could offer — without going into detail about the services — and to try to grasp the possible regulatory implications.

You have to understand that the banks, and this is particularly true in Canada, are still waiting for more specific regulations on Bitcoin. Many are not offering banking services to Bitcoin companies out of fear of breaking existing laws, particularly on money laundering. However, without access to basic services like a simple commercial bank account, many of these companies may prefer to set up shop elsewhere, which could mean economic losses for Canada. Clearer rules could make it easier for banks and Bitcoin companies to do business with each other.

Generally speaking, I believe that for Bitcoin to continue growing, it needs an appropriate legal and regulatory framework in order to strengthen the confidence of consumers, merchants and investors, and encourage the system's wider use. Greater confidence could, in turn, lead to a greater demand for and greater interest in Bitcoin, which would mitigate the currency's volatility. With more participants buying and selling Bitcoin, the market would become more liquid and price volatility would decrease.

By eliminating investor uncertainty — and by investors, I mainly mean venture capitalists, for example, with money to invest in start-up companies — clearer rules would also encourage investment in Bitcoin initiatives and businesses. So the jurisdictions moving most quickly to clarify their regulations would likely be those benefiting the most from Bitcoin's potential for job creation and economic impact.

Before concluding, I would like to go back to something I said earlier. I said to that Bitcoin was two things: a currency and, in particular, a system. Things move very quickly in the Bitcoin world and there are several projects underway that would use the Bitcoin network to offer expanded financial services. One of these innovations is called "coloured coins". I am still trying to figure out what this is all about, and someone more qualified than I could perhaps give you more details. But, in general, by "colouring" a Bitcoin, users could trade shares, issue bonds or even transfer property in the same way that they can now send Bitcoin. So, while I am not a computer expert, I think we should approach Bitcoin as an idea whose potential goes beyond that of simply a digital currency.

Financial Times, qui rapportait la nouvelle, ces rencontres avaient pour but de susciter la réflexion sur le genre de « services Bitcoin » qu'une banque pourrait offrir — on ne précisait pas quel genre de service — et d'essayer de comprendre quelles seraient les implications en matière de réglementation.

Il faut comprendre que les banques, et vous le savez probablement mieux que moi — et c'est vrai ici au Canada — sont toujours dans l'attente de règlements plus spécifiques à l'égard de Bitcoin. Par crainte de ne pas respecter les lois actuelles sur le blanchiment d'argent, notamment, plusieurs évitent d'offrir les services bancaires à des entreprises Bitcoin. Or, sans service bancaire de base comme un simple compte bancaire d'entreprise, plusieurs de ces entreprises préféreront peut-être s'établir ailleurs, ce qui pourrait occasionner des pertes économiques pour le Canada. Donc, des règles plus claires à ce sujet pourraient faciliter l'interaction entre les banques et les entreprises Bitcoin.

De façon générale, j'émettais l'opinion que pour que son développement se poursuive, Bitcoin a besoin d'un cadre juridique réglementaire approprié afin de renforcer la confiance des consommateurs surtout, des commerçants et même des investisseurs dans Bitcoin, et ainsi favoriser son usage à plus grande échelle. Une plus grande confiance pourrait à son tour susciter une plus grande demande et un plus grand intérêt pour les bitcoins, ce qui aurait comme effet de mitiger sa volatilité, puisqu'avec davantage d'acheteurs et de vendeurs de bitcoins, le marché deviendrait plus liquide, ce qui réduirait la volatilité du prix d'un bitcoin.

Donc des règles plus claires, en éliminant l'incertitude pour les investisseurs — et quand je parle d'investisseurs, je parle surtout de gens du domaine du capital de risque, par exemple, qui voudraient peut-être investir dans les jeunes compagnies —, ce qui aurait pour effet d'encourager l'investissement dans les projets de bitcoins. Et donc les juridictions qui vont peut-être clarifier leurs règles plus rapidement seront peut-être celles qui profiteront le plus des emplois liés au bitcoin et des retombées économiques.

Avant de terminer, j'aimerais faire un lien avec une chose que j'ai dite plus tôt. Je disais que bitcoin se résumait à deux choses : une monnaie et surtout un réseau. Les choses bougent très rapidement dans le monde Bitcoin. En ce moment, il y a plusieurs projets en cours qui feraient en sorte d'utiliser le réseau Bitcoin pour offrir des services financiers élargis. Une de ces innovations s'appelle les *coloured coins* — j'essaie encore moi-même de comprendre ce que c'est exactement, quelqu'un de plus qualifié pourrait sûrement mieux vous l'expliquer en détail. Mais en gros, en colorant un bitcoin, un utilisateur pourrait non seulement faire des transactions actuelles avec des bitcoins, mais aussi traiter peut-être des actions, des obligations, des titres de propriété, même des contrats à l'aide du même réseau. Alors tout cela pour dire que, même sans être un expert en informatique, ces développements font en sorte qu'il faut aborder Bitcoin comme quelque chose dont le potentiel va au-delà d'une simple monnaie numérique.

To sum up, while I cannot predict the future or even say how Bitcoin might revolutionize the way we use money, it seems to me that, until now, the public and the media have focused on Bitcoin as a currency or investment, while its true potential probably lies elsewhere in a form that has yet to be discovered.

[*English*]

The Chair: Thank you very much for your opening remarks.

You include in your remarks a reference to the fact that banks are waiting for more specific regulations. It was with interest that I noted that at the shareholders' meeting of the Bank of Montreal several days ago, the President of the Bank of Montreal indicated they were going to be open to perhaps dealing in bitcoin if there were regulations brought forward.

Could you comment on the significance of the fact that there has been a reaction from one of the chartered banks?

[*Translation*]

Mr. Descôteaux: The CEO of the Bank of Montreal made that statement in the *Financial Post* yesterday. I am not a banker, I cannot speak for them, but I imagine that, at this stage, as we have seen in the United States, there are banks that might simply like to be able to finance some Bitcoin businesses, with venture capital perhaps, or just to offer basic bank accounts to those businesses.

As for using the Bitcoin network and providing services in Bitcoin, it is not yet possible to be precise about that. I think that the banks are still thinking about it themselves.

Senator Maltais: Thank you for your presentation, Mr. Descôteaux. There are certainly a lot of question marks about Bitcoin.

You talked about regulation in a legal framework. Could the legal framework that regulates Canadian banks apply to Bitcoin?

Mr. Descôteaux: I am not a legal expert, of course, but I feel that the current need, the first step, would be to clarify Bitcoin's place in current legislation. I am not sure that we need to invent new legislation. But for a bank, for example, the uncertainty is in not knowing exactly whether any given regulations on money laundering apply to Bitcoin. I think that clarifying Bitcoin's status would probably situate it within current regulations automatically.

The devil is in the detail, of course. There are all kinds of regulations for all kinds of Bitcoin businesses. So it is very complex. But, at this stage, I feel that a simple clarification of

Pour résumer, bien que je ne puisse pas moi-même prédire l'avenir ou simplement préciser comment Bitcoin pourrait ou non révolutionner la façon dont nous transigeons l'argent, il me semble que jusqu'ici, l'attention des gens et des médias s'est surtout posée sur Bitcoin en tant que monnaie ou investissement, alors que le vrai potentiel de Bitcoin est probablement ailleurs, sous une forme qui n'est pas encore précisée.

[*Traduction*]

Le président : Merci beaucoup de votre déclaration liminaire.

Dans vos observations, vous avez fait allusion au fait que les banques attendent une réglementation plus précise. C'est avec intérêt que j'ai remarqué que, à l'assemblée des actionnaires de la Banque de Montréal il y a quelques jours, le président de la banque a indiqué qu'ils seraient peut-être disposés à faire des transactions en bitcoins si des règles étaient adoptées.

Pourriez-vous nous parler de l'importance que revêt cette réaction d'une des banques à charte?

[*Français*]

M. Descôteaux : Hier, dans le *Financial Post*, le président-directeur général de la Banque de Montréal faisait cette affirmation. Je ne suis pas banquier, je ne peux pas parler à leur place, mais j'imagine qu'à ce stade-ci, et on l'a vu aux États-Unis, il y a des banques qui aimeraient peut-être simplement pouvoir financer certaines entreprises Bitcoin, avec du capital de risque ou autre, ou simplement offrir des services de comptes bancaires de base à des entreprises.

Pour ce qui est d'utiliser le réseau Bitcoin et d'offrir des services en bitcoins, ce n'est pas encore quelque chose que l'on peut préciser. Je pense que les banques elles-mêmes sont encore en réflexion à ce sujet.

Le sénateur Maltais : Merci, monsieur Descôteaux, pour votre présentation. C'est certain qu'il y a beaucoup de points d'interrogation sur le bitcoin.

Vous avez parlé d'une réglementation dans un cadre juridique. Est-ce que le cadre juridique qui régit les banques canadiennes pourrait s'appliquer au bitcoin?

M. Descôteaux : Je ne suis pas un juriste, évidemment, mais je pense que le besoin actuel, la première étape, serait de clarifier où se situe Bitcoin dans la loi actuelle. Je ne suis pas certain que l'on ait besoin d'inventer de nouvelles lois. Mais pour une banque, par exemple, l'incertitude est de ne pas savoir exactement si Bitcoin s'applique à telle ou telle réglementation pas rapport au blanchiment d'argent. Je pense que clarifier le statut de Bitcoin le placerait probablement automatiquement dans les règles actuelles.

Évidemment, le diable est dans les détails, et il y a toutes sortes de règlements pour toutes sortes d'entreprises Bitcoin, donc c'est très complexe. Mais je pense qu'à ce stade-ci, une simple

what a Bitcoin business is and what kind of box it has to fit into, would be a good place to start.

Senator Maltais: What tack would our committee take to make sure that it fits into the legal framework for banking?

Mr. Descôteaux: Once again, it is a question of clarifying Bitcoin's status. For example, in the United States a few days ago, the Internal Revenue Service issued a statement that Bitcoin is a commodity, not a currency, so it is taxable. If you make capital gains in Bitcoin, for example, you have to declare them. I think it applies to consumers as well as to merchants. Everyone wants to know where Bitcoin fits. Some merchants, for example, are still a little hesitant to do business with, to accept, Bitcoin because they do not know where to declare those earnings in their tax returns. Clearly, from the consumers' point of view, there is almost no protection. If people want Bitcoin to continue its popularity, it is critical to establish a legal framework for it.

Senator Maltais: Last year, the Standing Senate Committee on Banking Trade and Commerce conducted a study on money laundering. Despite Canada's very strict legal framework, despite the oversight bodies, the RCMP estimates that about $15 billion, perhaps more, are laundered in Canada.

Does Bitcoin's arrival open the door for unregulated money laundering?

Mr. Descôteaux: Possibly. Money laundering is clearly very, very big, though, and Bitcoin is still very, very small.

I was reading statistics saying that the black market in the United States is calculated to be about $2,000 billion. While it is true that Bitcoin can be used for illicit purposes, at the same time, it is still very small in the big picture.

The other interesting point is that regulations, depending on the way in which they are made, could help authorities to better control Bitcoin use, depending on the details, of course.

Senator Maltais: If you had a recommendation for the committee, what would it be?

Mr. Descôteaux: As I said at the beginning, we have at least to try to find out where Bitcoin stands in the current situation. Is it a currency? A commodity? What kind of legislation applies to Bitcoin, so that everyone, businesses and consumers, knows what the rules of the game are?

Senator Massicotte: Thank you for being here and for providing your clarifications, Mr. Descôteaux.

clarification de ce qu'est une entreprise Bitcoin et dans quelle espèce de case elle doit se placer serait peut-être un point de départ.

Le sénateur Maltais : Sur quelle voie notre comité pourrait-il s'aligner pour s'assurer que cela corresponde au cadre juridique bancaire?

M. Descôteaux : Encore une fois, la question est de préciser le statut de Bitcoin. Par exemple, aux États-Unis, il y a quelques jours, l'Internal Revenue Service a émis une déclaration selon laquelle Bitcoin était un bien, que ce n'était pas une monnaie, donc que cela devenait taxable. Par exemple, si vous faites des gains en capitaux avec Bitcoin, vous devrez les déclarer. Je pense que c'est autant du point de vue des consommateurs que des commerçants. Tout le monde veut savoir où se situe Bitcoin. Certains commerçants, par exemple, hésitent peut-être encore à faire des affaires, à accepter des bitcoins parce qu'ils ne savent pas où placer ces gains dans leur déclaration d'impôt. Et évidemment, du point de vue du consommateur, il n'y a à peu près aucune protection du consommateur. Si certaines personnes veulent que Bitcoin continue d'être populaire, il devient incontournable de créer un cadre légal juridique.

Le sénateur Maltais : L'an passé, au Comité sénatorial permanent des banques et du commerce, on a fait une étude sur le blanchiment d'argent. Malgré le cadre juridique très strict au Canada, malgré les agences de surveillance, la GRC estime qu'il se blanchit environ 15 milliards de dollars et peut-être plus au Canada.

Est-ce que l'arrivée de Bitcoin n'est pas une porte ouverte pour le blanchiment d'argent sans réglementation juridique?

M. Descôteaux : C'est possible. Évidemment, le blanchiment d'argent, c'est beaucoup, beaucoup d'argent. Bitcoin, c'est encore très, très petit.

Je lisais une statistique selon laquelle le marché noir aux États-Unis se chiffrait à environ 2 000 milliards de dollars. Alors c'est sûr que Bitcoin peut être utilisé à des fins illicites, mais en même temps, cela demeure très petit dans l'ensemble.

L'autre point qui est intéressant, c'est qu'une réglementation, dépendamment de la manière dont elle est faite, pourrait aider les autorités à mieux contrôler les usages de bitcoins, tout dépendant des détails, évidemment.

Le sénateur Maltais : Si vous aviez une recommandation à faire au comité, quelle serait-elle?

M. Descôteaux : Comme je le disais au début, il faudrait au moins essayer de savoir où se situe Bitcoin dans le cadre actuel. Est-ce que c'est une monnaie? Un bien? Quelle loi s'applique à Bitcoin afin que tous, entreprises comme consommateurs, sachent quelles sont les règles du jeu.

Le sénateur Massicotte : Merci, monsieur Descôteaux, pour votre présence et vos clarifications.

I am going to follow along the same lines as my colleague. You were looking for clarification, but I believe that Revenue Canada, as well as the IRS in the United States, has declared bitcoin to be a commodity, something people own. In tax terms, you are taxed for any profit or loss when you hold the commodity.

What else do we need? Why would the government recommend coming up with other regulations? Because, as has been said very clearly, the important thing is that the cost must remain very low for it to remain competitive and useful.

The more regulations you have, the more guarantees you require, the more it going to cost someone and the more the costs will go up. What kind of regulations could we need? Why would they be necessary?

Mr. Descôteaux: That is a very good question because, in fact, most people agree that Bitcoin needs a regulatory framework, but very few people can say exactly which legislation has to be amended or introduced. Not being a legal expert myself, I have difficulty in venturing an opinion along those lines.

You mentioned the costs of the regulations, of course. That is quite a delicate balance because, at the moment, one of the advantages of Bitcoin, as you said, is that the fees are very low.

Now, if we go about creating substantial regulations that would result in costs for Bitcoin companies, those costs would likely have to be passed on to the consumer in one way or another, and the competitive advantage would be lost. This is quite a delicate balance, but there have actually been communications with the Canada Revenue Agency. I do not think that the general public really knows what to do about Bitcoin in terms of taxes. If regulations have already been issued, perhaps it is just a question of informing the public what they are.

Senator Massicotte: Do we agree that Bitcoin will never become the official currency of the country?

Mr. Descôteaux: I would not go there. As I was saying in the introduction, I am much more optimistic about the technology behind it all and about the network that continues to develop daily and that may result in an innovation. But as a currency per se, I doubt it. I do not know if we need new currencies, but we always need innovations in order to reduce costs for consumers and business.

Senator Massicotte: I agree with you. I do not think that it could become our currency. The government will not allow it because Canadians would lose all the flexibility of a monetary policy. That said, you are a member of the Montreal Economic Institute, after all, which is a firm believer in free trade, the free market and the capitalist system.

Je poursuivrai dans le même ordre d'idée que mon collègue. Vous cherchez une clarification, mais je pense qu'autant Revenu Canada que l'IRS aux États-Unis ont déclaré que le bitcoin est une commodité, une propriété. Du point de vue fiscal, on est imposé sur tout gain ou perte pour détenir cette commodité.

Qu'avons-nous besoin d'autre? Et pourquoi le gouvernement recommanderait d'établir d'autres règlements? Parce que comme on l'a dit très clairement, l'important c'est qu'il faut que le coût demeure très bas afin que ce soit concurrentiel, utile.

Plus on réglemente, plus il y a d'assurance sur la garantie, plus cela va coûter cher à quelqu'un, plus on augmentera les coûts. De quelle réglementation pouvons-nous avoir besoin? Et pourquoi serait-ce nécessaire?

M. Descôteaux : C'est une très bonne question parce qu'en fait, la plupart des gens s'entendent pour dire que Bitcoin a besoin d'un cadre réglementaire, mais il y a très peu de personnes qui peuvent dire exactement quelle loi il faut modifier ou qu'est-ce qu'il faut amener. Et n'étant pas juriste moi-même, j'ai de la difficulté à m'aventurer précisément dans cette voie.

Vous mentionnez les coûts de cette réglementation évidemment. C'est un équilibre assez délicat parce qu'en ce moment, un des avantages de Bitcoin, comme vous le disiez, c'est d'avoir des frais très minimes.

Maintenant, si on s'engage dans la création d'une réglementation lourde qui engendrerait des coûts pour les entreprises Bitcoin, ces coûts devront probablement être pris en charge par le consommateur d'une façon ou d'une autre et on perdrait cet avantage concurrentiel. C'est un équilibre assez délicat, mais effectivement, il y a eu des communications avec l'Agence du revenu du Canada. Je crois que le public en général ne sait pas vraiment quoi faire avec les bitcoins sur le plan fiscal. Si on a déjà émis des règles, il s'agirait peut-être simplement de faire en sorte que le public en soit informé.

Le sénateur Massicotte : Sommes-nous d'accord pour dire que le bitcoin ne pourra jamais devenir la monnaie officielle du pays?

M. Descôteaux : Je n'irais pas dans ce sens. Comme je le disais en introduction, je suis beaucoup plus optimiste par rapport à la technologie derrière tout cela ou au réseau qui continue de se développer chaque jour et qui peut déboucher en tant qu'innovation, mais la monnaie en tant que telle, je suis assez méfiant. Je ne sais pas si nous avons besoin de nouvelles monnaies, mais nous avons toujours besoin d'innovations pour réduire les coûts pour les consommateurs et les entreprises.

Le sénateur Massicotte : Je suis d'accord avec vous. Je ne pense pas que cela puisse devenir notre monnaie. Le gouvernement ne le permettra pas parce que les Canadiens perdraient toute la flexibilité d'une politique monétaire. Cela étant dit, vous êtes quand même membre de l'Institut économique de Montréal qui croit beaucoup au libre-échange, au libre marché et au système capitaliste.

Why the regulations? The government does not regulate other commodities like gold and silver. There are a bunch of other commodities, and the government has no role to play in making sure that people will not lose money. Why not let the market determine how things turn out? Yes, there is quite a high risk, as is the case for many commodities. Why would we want to act differently in this case?

Mr. Descôteaux: From a regulatory point of view, as I mentioned earlier, Canada comes in second after the United States among the countries that receive the most venture capital for bitcoin enterprises. I think it is 15 per cent in Canada. A lot of investors could be ready to invest more, but when you do not know if from one day to the next a country will decide that the bitcoin is illegal — as has happened in some countries — there is a risk and one hesitates to invest. As for economic advantages, some clear rules could facilitate things and would attract more investment here.

Senator Massicotte: If I understand your last comment correctly, you are asking the Government of Canada to say that in the years to come no legislation will be brought in that will hinder the bitcoin? I do not understand.

Mr. Descôteaux: And I am not sure I understand your question.

Senator Massicotte: To give assurances, comfort to those who want to invest in this commodity, you are asking the Government of Canada to create regulation which will not be binding? I do not understand your request.

Mr. Descôteaux: I am not asking for anything, but if the Bitcoin is to continue to grow, there have to be clear rules — for instance, how does the bitcoin fit into the financial system — from the government which would specify that it is a virtual currency that is tolerated and accepted — this would facilitate things. And afterwards, the market should be allowed to do what the market does.

Senator Rivard: Thank you, Mr. Descôteaux, for your presentation. Before asking you a question, I would like to go back to a few words at the end of the French version of your presentation. It says: "The devil is in the details."

In the penultimate paragraph of the French version of your presentation, you say: "As we speak, there are several projects that are ongoing."

"Ongoing," means that this is before a court and not in process. So, it is true that the devil is in the details.

We discussed the danger of money laundering, but several witnesses have drawn our attention to the fact that the Bitcoin is currently accepted by certain establishments as payment. You are from Montreal and probably own a few bitcoins. Can you tell us

Pourquoi des règlements? Le gouvernement ne réglemente pas d'autres commodités comme l'or et l'argent. Il y a une tonne d'autres commodités et le gouvernement n'a pas de rôle à jouer pour nous assurer que les gens ne perdront pas d'argent. Pourquoi ne pas laisser le marché dicter la suite des choses? Oui, il y a un risque assez élevé, comme dans le cas de bien des commodités. Pourquoi s'impliquer autrement?

M. Descôteaux : D'un point de vue réglementaire, je le mentionnais tantôt, le Canada est le deuxième pays qui reçoit le plus de financement en capital de risque pour les entreprises Bitcoin, après les États-Unis. Je crois que c'est 15 p. 100 au Canada. Beaucoup d'investisseurs pourraient être prêts à en mettre davantage, mais quand on ne sait pas si, du jour au lendemain, un pays va décider que le bitcoin est illégal — comme cela se fait dans certains pays — il y a un risque et on hésite à investir. Du point de vue des bénéfices économiques, des règles claires pourraient faciliter les choses et feraient en sorte d'attirer davantage d'investissements ici.

Le sénateur Massicotte : Si je comprends bien votre dernier commentaire, vous demandez au gouvernement du Canada de dire que, dans les années futures, aucune législation mise en oeuvre ne va préjuger le bitcoin? Je ne comprends pas.

M. Descôteaux : Je ne suis pas certain de comprendre votre question.

Le sénateur Massicotte : Pour donner une assurance, un confort à ceux vont investir dans cette commodité, vous demandez au gouvernement du Canada de créer une réglementation qui ne légiférera pas? Je ne comprends pas votre requête.

M. Descôteaux : Je ne demande rien, mais si pour que le bitcoin continue de croître, il faut des règles claires — par exemple, comment s'inscrit le bitcoin dans le régime fiscal —, de la part du gouvernement qui préciseraient que c'est une monnaie virtuelle qui est tolérée et acceptée, cela faciliterait les choses. Et ensuite, on laisserait le marché faire ce qu'il a à faire.

Le sénateur Rivard : Merci, monsieur Descôteaux, pour votre présentation. Avant de vous poser une question, je voudrais reprendre quelques mots inscrits à la fin de la version française de votre présentation. Il est inscrit : « le diable est dans les détails. »

À l'avant-dernier paragraphe de la version française de votre présentation, vous dites : « En ce moment même, il y a plusieurs projets en cour. »

« En cour », écrit de cette façon, veut dire que c'est devant un tribunal et non en processus. Alors, c'est vrai que le diable est dans les détails.

On a parlé du danger du blanchiment d'argent, mais plusieurs témoins ont attiré notre attention sur le fait que le bitcoin est présentement accepté par certains établissements en contrepartie du paiement. Vous qui êtes de Montréal, vous possédez

what type of businesses accept the bitcoin for products or services?

Mr. Descôteaux: In Canada there are about 100 businesses. There are not many in Montreal. I believe there are only two. They are mostly retail businesses. In Montreal I think they are clothing shops. In Europe and in the United States, a lot of cafés and bars accept the bitcoin.

For this type of business, the advantage is that they do a lot of small transactions where clients use credit cards, and I expect that at the end of the month this makes a difference in their costs. A lot of boutiques decided to join the Bitcoin adventure for marketing purposes. A few months ago if you had a small business and decided to accept the bitcoins, you would get publicity in papers all over the country. That is a good way of getting a little publicity. Retail merchants see concrete advantages in using them.

Senator Rivard: Do you think that in the near future a lot of businesses will accept the bitcoin in exchange for goods or services? For the moment, it is practically a speculative currency.

Mr. Descôteaux: As an investment, indeed, it is pure speculation. If there are tangible and concrete advantages for a business — those are two different things. I am not saying that an incredible number of businesses will start using it. I am waiting to see how all of this is going to develop. As long as the transaction fees remain low, which is the main advantage for a business, this could be popular if people open up to it a bit.

You have to understand also that one of the problems of the bitcoin, one of the barriers to its popularity, is the fact that it remains relatively complicated for the common person. If it is not understood quickly enough, people hesitate to invest in it. The future will tell if it will become more popular. At this time, over a one-year period, the number of businesses who see advantages to the bitcoin is growing.

Senator Bellemare: First, I want to congratulate you for your economic statement. I found it very clear and very interesting to read. We were saying earlier that the devil is in the details, and that may have drawn your attention. In your economic statement, there is a note, note No. 9. You refer to the BitPay enterprise which plays a role in the convertibility of the bitcoin into fiduciary currency, and it says that the BitPay website claims that it offers this service to 12,000 businesses and charity organizations. It is the charity organization that got my attention.

We know that the bitcoin is often used in international transactions. Did you look further into this matter of charity organizations using this? If it is written there, it is because they must deal with those organizations on a regular basis. This is not an anomaly or an exception.

probablement quelques bitcoins. Pouvez-vous nous dire quel genre d'établissements accepte le bitcoin en échange de produits ou de services?

M. Descôteaux : Au Canada, il y a peut-être une centaine de commerces. Il n'y en a pas beaucoup à Montréal. Je crois qu'il n'y en a que deux. C'est surtout des commerces de détail. À Montréal, je crois qu'il s'agit de boutiques de vêtements. En Europe et aux États-Unis, beaucoup de cafés et de bars acceptent le bitcoin.

L'intérêt pour ce type de commerces est que ce sont des commerces qui réalisent peut-être beaucoup de petites transactions par carte de crédit, et j'imagine qu'à la fin du mois, cela peut faire une différence dans les frais. Plusieurs boutiques se sont lancées dans l'aventure Bitcoin à des fins de marketing. Il y a à peine quelques mois, si vous aviez une boutique et que vous décidiez d'accepter les bitcoins, vous faisiez les manchettes dans les journaux partout au pays. C'est une bonne façon de se faire un peu de publicité. Jusqu'à présent, les commerçants de détail y voient des avantages concrets.

Le sénateur Rivard : Croyez-vous que d'ici une période de temps prévisible, beaucoup de commerces vont accepter le bitcoin en échange de services ou de marchandises? Pour l'instant, c'est pratiquement une monnaie de spéculation.

M. Descôteaux : En tant qu'investissement, effectivement, c'est de la pure spéculation. Si cela a des avantages tangibles et concrets pour un commerce — ce sont deux choses différentes. Je ne dis pas qu'un nombre incroyable de commerces vont utiliser cela. J'attends de voir comment tout cela va se développer. Tant que les frais de transaction resteront bas, ce qui est le principal avantage pour un commerce, cela pourrait être populaire si les gens s'ouvrent un peu au phénomène.

Il faut comprendre aussi qu'un des problèmes du bitcoin, un des obstacles à sa popularité est le fait que cela demeure quelque chose de relativement compliqué pour le commun des mortels. Si ce n'est pas compris assez rapidement, les gens hésitent à y faire des investissements. L'avenir nous dira si cela va devenir plus populaire. En ce moment, sur une période d'un an, le nombre de commerces qui voit des avantages à Bitcoin augmente.

La sénatrice Bellemare : D'abord, je voudrais vous féliciter pour votre note économique. Je l'ai trouvée très claire et intéressante à lire. On disait tout à l'heure que le diable est dans les détails et c'est ce qui a peut-être attiré votre attention. Dans votre note économique, il y a une note et c'est la note 9. Vous parlez de l'entreprise BitPay qui joue un rôle dans la convertibilité du bitcoin en monnaie fiduciaire, et on peut y lire que le site web de BitPay affirme offrir ce service auprès de 12 000 commerçants et organismes de charité. C'est l'organisme de charité qui m'a fait réagir.

On sait que le bitcoin est utilisé souvent dans le cas de transactions internationales. Êtes-vous allé fouiller cette question des organismes de charité? Si c'est inscrit là, c'est parce qu'ils doivent transiger avec ces organismes régulièrement. Ce n'est pas une anomalie ou une exception.

Mr. Descôteaux: That is a very interesting observation. Unfortunately, I did not look into the charity organizations. In my reading, I read — and I have often heard that this was a fairly popular use — that a lot of gifts are made to charity organizations using bitcoins. I am not certain of the advantages there, but indeed that is something it would be interesting to look into further.

Senator Bellemare: I don't know if you can answer my second question. We often hear that these transactions are managed in a decentralized way using algorithms and that those algorithms become increasingly complex. Is the complexity of the algorithms proportional to the scope of the transaction?

In other words, when you purchase a coffee, you do not pay a large amount with the bitcoin, but will the algorithm be the same if you negotiate a Tesla, for instance? Or are there less onerous mechanisms with regard to the flexibility and complexity of the mathematical algorithm according to the size of the transaction?

Mr. Descôteaux: I am going to try to answer you as best as I can, even though I am not a computer geek. I think the algorithm you are talking about is the type of puzzle you must solve to obtain the bitcoins, when you confirm transactions. That algorithm is indeed designed so that it becomes harder and harder to resolve. Because of course there are very powerful computers that work on this, whereas a year or two, you could from your home, with your laptop, mine bitcoins. Today that is impossible.

Of course, the algorithm adjusts to the speed it takes to solve the last puzzle. If it does not take enough time, the next puzzle will be more complicated so that there is always a challenge, in order to respect the production rate for bitcoins, because I think they expect that bitcoins will be minted until 2025 or 2030. Of course, it has to be very, very complicated because it has to reflect the technological innovations that allow things to be resolved more quickly.

But in a transaction, I think the issue is to know whether the transaction costs will be higher according to whether it is a small or large transaction. To my knowledge, no. I would have to check, but I would even say that the costs are sometimes lower when it is a big transaction, perhaps because the reward in bitcoins is proportionally higher for a bigger transaction. But, that said, it remains minimal, it remains under 1 per cent in the vast majority of cases.

M. Descôteaux : C'est une observation très intéressante. Malheureusement, je n'ai pas fouillé le côté des œuvres de charité. Dans le cadre de mes lectures, j'ai lu — et j'ai souvent entendu que c'était une utilisation assez populaire —, beaucoup de dons sont faits à des œuvres de charité par bitcoins. Je ne suis pas certain des avantages à en tirer, mais c'est effectivement quelque chose qu'il serait intéressant d'approfondir.

La sénatrice Bellemare : Je ne sais pas si vous serez en mesure de répondre à ma deuxième question. On dit souvent que ces transactions sont gérées de manière décentralisée à l'aide d'algorithmes et que ces algorithmes deviennent de plus en plus compliqués. La complexité des algorithmes est-elle proportionnelle à l'ampleur d'une transaction?

En d'autres mots, quand vous achetez un café, ce n'est pas un gros montant qu'on paie avec le bitcoin. Mais est-ce que l'algorithme va être aussi important que si on négociait une Tesla, par exemple? Ou y a-t-il des mécanismes moins onéreux pour ce qui est de l'électricité et de la complexité de l'algorithme mathématique à régler selon l'ampleur de la transaction?

M. Descôteaux : Je vais essayer de vous répondre de mon mieux, je ne suis pas un *geek* en informatique. Je pense que l'algorithme dont vous parlez c'est surtout l'espèce de casse-tête à résoudre pour obtenir les bitcoins, lorsqu'on confirme les transactions. Cet algorithme est effectivement préconçu de façon à ce qu'il devienne de plus en plus compliqué à résoudre. Parce qu'évidemment, vous avez des ordinateurs super puissants qui s'affairent à cette tâche, alors qu'il y a un an ou deux, vous pouviez de votre maison, avec votre ordinateur portable, miner des bitcoins. C'est impossible aujourd'hui.

Évidemment, l'algorithme s'ajuste à la vitesse que cela prend pour régler le dernier casse-tête. Si cela ne prend pas assez de temps, le prochain casse-tête sera plus compliqué pour qu'il y ait toujours un défi, de façon à respecter le rythme de production prévu des bitcoins. Parce que je pense qu'on s'attend à ce qu'il y ait des bitcoins qui soient minés jusqu'en 2025 ou 2030. Évidemment, il faut que ce soit très, très compliqué parce qu'il faut que cela reflète les innovations technologiques qui permettent de résoudre plus rapidement ces choses.

Mais dans le cadre d'une transaction, je pense que la question est de savoir si les frais de transaction pourraient être plus élevés pour une grosse ou une petite transaction. À ma connaissance, non. Il faudrait vérifier, mais je dirais même que les frais sont parfois plus bas lorsque qu'il s'agit d'une grosse transaction. Peut-être parce que la récompense en bitcoins est proportionnellement plus élevée pour une grande transaction. Mais ceci étant dit, cela demeure quand même minime, cela demeure en bas de 1 p. 100 dans la très grande majorité des cas.

[*English*]

The Chair: Thank you very much. Mr. Descôteaux, that concludes our questions today. On behalf of the members of the Banking Committee, I would like to express our great appreciation for your appearance before us today and helping us with our deliberations. This meeting is concluded.

(The committee adjourned.)

[*Traduction*]

Le président : Merci beaucoup. Monsieur Descôteaux, c'était la dernière question aujourd'hui. Au nom de tous les membres du Comité des banques, j'aimerais sincèrement vous remercier d'être venu témoigner aujourd'hui et de nous aider dans le cadre de nos délibérations. La séance est levée.

(La séance est levée.)

WITNESSES

Wednesday, April 2, 2014

Bank of Canada:

Grahame Johnson, Chief, Funds Management and Banking;

Lukasz Pomorski, Assistant Director, Funds Management and Banking.

Thursday, April 3, 2014

As individuals:

Jeremy Clark, Assistant Professor, Concordia Institute for Information Systems Engineering, Concordia University;

David Descôteaux, Associate Researcher, Montreal Economic Institute (by video conference).

TÉMOINS

Le mercredi 2 avril 2014

Banque du Canada :

Grahame Johnson, chef, Gestion financière et Opérations bancaires;

Lukasz Pomorski, directeur adjoint, Gestion financière et Opérations bancaires.

Le jeudi 3 avril 2014

À titre personnel :

Jeremy Clark, professeur adjoint, Institut d'ingénierie des systèmes d'information de Concordia, Université Concordia;

David Descôteaux, chercheur associé, Institut économique de Montréal (par vidéoconférence).