SENATE | SÉNAT
CANADA

DIGITAL CURRENCY: YOU CAN'T FLIP THIS COIN!

REPORT OF THE STANDING SENATE COMMITTEE ON BANKING, TRADE AND COMMERCE




The Honourable Irving R. Gerstein
C.M., O.Ont., Chair

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

June 2015

Ce rapport est aussi disponible en français

****

This report and the committee's proceedings are available online at:
www.senate-senat.ca/banc.asp

TABLE OF CONTENTS

MEMBERS 4

ORDER OF REFERENCE 5

EXECUTIVE SUMMARY 6

LIST OF RECOMMENDATIONS 9

CHAPTER 1: INTRODUCTION 10

CHAPTER 2: THE COMMITTEE'S THOUGHTS 12

A. Digital Currency Types and Uses 12

B. Digital Currency-Related Opportunities 13

C. Digital Currency-Related Risks 14
1. Use of Digital Currencies to Launder Money and Finance Terrorist Activities 14
2. Protecting the Users of Digital Currencies 15
3. Taxation Challenges in Relation to Digital Currencies 16

D. Focusing on the Future 17

CHAPTER 3: WITNESSES' TESTIMONY 18

A. Digital Currency Types and Uses 18
1. Definitions for "Digital Currency" 18
2. Common Types of Digital Currency 18
3. Potential Uses for Digital Currencies 19
4. Bitcoin as an Example 27

B. Digital Currency-Related Opportunities 32
1. Innovation 32
2. Transaction Costs 34
3. Payment Options 36
4. Identity Protection and Recording of Transactions 39

C. Digital Currency-Related Risks 40
1. Potential Criminality and its Effects 40
2. Losses 47
3. Taxation 52
4. Access to Information and Protection for Users 54
5. Other Challenges in Using Digital Currencies 56

CHAPTER 4: CONCLUSION 58

APPENDIX A: WITNESSES 59

APPENDIX B: FACT-FINDING MISSION TO NEW YORK – FEBRUARY 2-4, 2015 62

APPENDIX C: GLOSSARY OF DIGITAL CURRENCY-RELATED TERMS 64

MEMBERS

The Honourable Irving R. Gerstein, C.M., O.Ont., Chair
The Honourable Céline Hervieux-Payette, P.C., Deputy Chair

and

The Honourable Diane Bellemare
The Honourable Douglas Black, Q.C.
The Honourable Larry W. Campbell
The Honourable Stephen Greene
The Honourable Ghislain Maltais
The Honourable Paul J. Massicotte
The Honourable Pierrette Ringuette
The Honourable Scott Tannas
The Honourable David Tkachuk

Ex-officio members of the Committee:
The Honourable Senators Claude Carignan, P.C., (or Yonah Martin) and James S. Cowan (or Joan Fraser).

Other Senators who have participated from time to time in the study:
The Honourable Senators Marjory LeBreton, P.C., Michael L. MacDonald, Fabian Manning, Don Meredith, Percy Mockler, Thanh Hai Ngo, Dennis Glen Patterson, Rose-May Poirier, Nancy Greene Raine, Michel Rivard, Betty E. Unger and David M. Wells.

Parliamentary Information and Research Service, Library of Parliament:
Michaël Lambert-Racine, Brett Stuckey and Adriane Yong, Analysts.

Senate Committees Directorate:
Keli Hogan, Danielle Labonté and Barbara Reynolds, Committee Clerks; and Brigitte Martineau, Administrative Assistant.

ORDER OF REFERENCE

Extract from the *Journals of the Senate* of Tuesday, March 25, 2014:

> The Honourable Senator Gerstein moved, seconded by the Honourable Senator Lang:
>
> That the Standing Senate Committee on Banking, Trade and Commerce be authorized to examine and report on the use of digital currency including the potential risks, threats and advantages of these electronic forms of exchange; and
>
> That the Committee submits its final report no later than June 30, 2015, and that the Committee retains all powers necessary to publicize its findings until 180 days after the tabling of the final report.
>
> After debate,
>
> The question being put on the motion, it was adopted.

Gary W. O'Brien

Clerk of the Senate

EXECUTIVE SUMMARY

The Minister of Finance often asks the Standing Senate Committee on Banking, Trade and Commerce to undertake studies that might be helpful for government policy-making. This was the case when the late Jim Flaherty asked us to study cryptocurrency. Committee members had only a vague idea of what the Minister was talking about. We had no choice but to start at the beginning, with the essential question:

What is cryptocurrency?

The answer is complicated. The passionate and optimistic witnesses we heard from described a genuinely new technology. One that may well usher in a world where money flows as freely as data flows over the Internet; where there are no intermediaries (such as a bank) between you and your transaction, and where the 2.5 billion unbanked people in the world can potentially enjoy access to financial services.

While the Committee gave itself a broad mandate to study "digital currencies" in general, most witnesses discussed the subcategory of cryptocurrencies.

Cryptocurrencies belong to a nascent industry that has brought with it an entirely new vocabulary. In this report we provide a glossary of terms and technical descriptions of what cryptocurrencies are and how they work.

For this executive summary, the Committee will keep it simple:

Cryptocurrencies are a new medium of exchange. In their most basic form, they are a communications technology that offers peer-to-peer (P2P) transactions, eliminating the need for a third-party (ie. a bank) to carry out and authorize the transaction.

Of the hundreds of cryptocurrencies that have been created since 2009, Bitcoin is by far the most popular and has become synonymous with cryptocurrency itself. For these reasons, the Committee thinks a description of Bitcoin is useful to illustrate cryptocurrencies in general.

What is Bitcoin?

Bitcoin is a computer-coded, P2P cash system. Value is measured in units of bitcoin (lower case b) divisible (into satoshis[1]) like a dollar into cents. It relies on its own, unique and novel architecture. Bitcoin (upper case B) is a payment system, a decentralized (controlled by users) P2P network that allows for transactions with built-in security, eliminating the need for a central bank. This is Bitcoin's most distinctive feature – it is not associated with any physical commodity, central banking authority, or government.

Bitcoin transactions are made on the public ledger. The public ledger is exactly what it sounds like – a large bulletin board (written in a cryptic computer database called the blockchain). The public ledger logs and broadcasts transactions to the entire network.

Everyday transactions – using, for example, a debit or credit card to buy a cup of coffee – are tied to a bank. If you have enough money in your account, or credit on the card, the bank authorizes the

[1] Named after the alleged and mysterious inventor of Bitcoin, Satoshi Nakamoto. While an inventor published *Bitcoin: A P2P Electronic Cash System* in 2008 under the name of Satoshi Nakamoto, this inventor has never been identified. So, the true identity of the inventor of Bitcoin is a mystery. The idea of Satoshi Nakamoto is a big part of Bitcoin culture, and when weighing in with their opinion, Bitcoiners are known to say "that's just my two satoshis".

transaction and you get your coffee. If you bought that same cup of coffee with bitcoin, you would simply announce it on the public ledger without the bank or any other financial institution (and all their transaction fees) being involved. The merchant gets their money and you get your coffee.

The public ledger is always accessible through computers literate in the blockchain. It cannot be forged or changed. It provides a permanent record of all bitcoin transactions that have ever happened, a history that within an hour is unalterable.

The *'if a tree falls in the forest'* thought experiment is useful here. In the case of Bitcoin if a tree falls in the forest, and millions of independent computers with cameras record its fall, we can trust that it fell. That is the value of Bitcoin – the mathematical verification by millions of computers reaching a consensus that they witnessed the same thing at the same time. Trust in Bitcoin is a product of that security – which brings us to Bitcoin mining operations.

Bitcoin mining is a kind of lottery, except that your computer has to work in order to have a chance at winning. Of the millions of computers working to verify the public ledger, one will receive bitcoin as a reward. And presto, more bitcoin enters the money supply. Thousands of people are acquiring bitcoin this way, and an incredible amount of computing power has gathered to mine and verify the public ledger.

That's Bitcoin and cryptocurrency in a nutshell. But, our inquiry did not end there. Several times in our study, the Committee heard that bitcoin, the currency, is not the most significant innovation - but rather, the real innovation is blockchain technology.

What is blockchain technology?

Blockchain technology is an ingenious computer code, stored entirely by computers, that forms the underlying architecture for hundreds (if not thousands) of cryptocurrencies and also shows great promise in extending beyond the realm of just currency.

Opportunities

We took a close look at blockchain technology and considered its opportunities. Bringing financial services to the unbanked in the developing world is one of the exciting things we heard about. The Committee developed a vivid sense of how this is possible and already happening.

Another opportunity offered by blockchain technology is its ability to put a person's security and online identity into their own hands. Cyber-attacks for the purpose of identity theft are becoming one of the defining security threats of the 21st Century. Databases filled with our personal information are under attack from nation-states and organized crime. Hackers who target governments, data breaches at large department stores, even celebrity nude photo leaks are the result of the same problem; criminal elements breaking through cybersecurity to their prize; databases filled with valuable personal information.

FBI Director James Comey recently told CBS's 60 Minutes, "*Cybercrime is becoming everything in crime because people have connected their entire lives to the Internet. That's where those who want to steal money or hurt kids or defraud go. And so it's an epidemic."*

A Canadian chartered bank explained that their cybersecurity faces thousands of attacks a day from hackers. Fortunately, they have the resources to fight this onslaught. But the same information consumers are sharing with banks, they are also sharing with online retail outlets. These retail outlets cannot deploy the financial resources a major bank puts into cybersecurity and are left vulnerable to cyber-attacks.

Blockchain technology offers a secure alternative to consumers who do not wish to see their personal information fall prey to the Internet. It offers the ability to transact on the Internet without sharing their personal information with third parties whose databases make juicy targets for hackers. Instead, blockchain technology gives consumers the power to provide their own hack-proof online security.

Risks

The security offered by blockchain technology on the Internet has a flip side, however. The anonymity it provides presents an opportunity for criminals and terrorists. Our study takes a look at the criminality around digital currencies, most infamously represented by Silk Road transactions on the so-called Deep Web – an untraceable part of the Internet that allows users to avoid being found by search engines like Google.

U.S. Senator Tom Carper (Democrat, Delaware), the lawmaker who exposed online drug and criminal elements using Bitcoin, stated, "*The ability to send and receive money over the internet, nearly anonymously, without a third party, has a lot of wide-ranging implications. The government needs to pay attention to this technology and to understand, and where appropriate, address these implications.*"

The 'wide-ranging implications' that Senator Carper refers to are money laundering, terrorist financing, and tax evasion. These are the risks inherent in the technology and they mean that, like all industries, a certain amount of regulation is prudent. But to what extent?

The Committee traveled to New York – specifically to meet with the New York State Department of Financial Services – to hear firsthand about proposed regulations being debated, including BitLicenses. These licenses, currently being developed in consultation with stakeholders, seek to regulate the so-called "on and off ramps" for exchanges that buy and sell cryptocurrencies. In short, licensing means that cryptocurrency exchanges would have to know their customers. The Committee believes this is reasonable.

Conclusion

New technologies attendant to cryptocurrency have unimagined applications. We've heard, and we agree, that blockchain technology is at a delicate stage in its development and use. This is why we urge the Government to explore the vast potential of this technology, while treading carefully when contemplating regulations that may restrict and stifle its use and development.

We believe that the best strategy for dealing with cryptocurrencies is to monitor the situation as the technology evolves; that Canada Revenue Agency and Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) must prepare to navigate and use blockchain technology; that this technology offers new ways to protect the personal information of Canadians; and, finally, that this technology requires a light regulatory touch – almost a *hands off* approach. In other words, not necessarily regulation, but regulation as necessary.

LIST OF RECOMMENDATIONS

The Committee recommends that:

Recommendation 1 (page 13)
The federal government, in considering any legislation, regulation and policies, create an environment that fosters innovation for digital currencies and their associated technologies. As such, the government should exercise a regulatory "light touch" that minimizes actions that might stifle the development of these new technologies.

Recommendation 2 (page 14)
The federal government consider the use of blockchain technology when advantageous to deliver government services and to enhance the security of private information.

Recommendation 3 (page 14)
Digital currency exchanges, the "on and off ramps" of the digital currency system, be defined as any business that allows customers to convert state-issued currency to digital currency and digital currencies to state-issued currency or other digital currencies. To minimize the risks of illegal activity in relation to Canada's anti–money laundering and anti–terrorist financing laws, the federal government should require digital currency exchanges, with the exclusion of businesses that solely provide wallet services, to meet the same requirements as money services businesses.

Recommendation 4 (page 15)
The federal government, on an active and ongoing basis, work with other countries to formulate global guidelines for digital currencies while respecting the "light touch" premise outlined in Recommendation 1 above.

Recommendation 5 (page 15)
The Minister of Finance convene a roundtable with stakeholders, including banks, to look for solutions to the lack of access to banking services for digital currency related businesses, while recognizing the requirements of Canada's anti–money laundering and anti–terrorist financing regime.

Recommendation 6 (page 16)
The federal government, through appropriate federal entities, provide concise information to the public about the risks of digital currencies and alternative payment systems.

Recommendation 7 (page 17)
The federal government, through the Canada Revenue Agency, provide concise information to Canadians about the tax obligations of digital currencies when received as income, held as an investment, or used to purchase goods or services.

Recommendation 8 (page 17)
Due to the evolving nature of digital currencies, the Standing Senate Committee on Banking, Trade and Commerce review this study of digital currencies and their associated technologies to assess the appropriateness of the regulatory environment in the next three years.

CHAPTER 1: INTRODUCTION

On 25 March 2014, the Senate authorized the Standing Senate Committee on Banking, Trade and Commerce (the Committee) to study digital currencies, with a particular focus on the potential risks, threats and advantages of these electronic forms of exchange. The Committee's interest in the topic was partially motivated by media reports about bitcoin being used to make and receive payments over the Internet, and comments by witnesses during our recent statutory review of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* about trends in the use of the Internet to launder money.

Throughout the study, the Committee was reminded that identifying the types of technology that will succeed or fail is difficult – if not impossible – to predict with any accuracy. It seems that, for every television and Internet, there is a Betamax and Segway. In thinking about technology and financial services, the Committee recognized that – over the past decade – the Canadian payments system has changed in substantial ways, including the introduction of Internet-based and mobile-based payment methods. Along with cash, cheques, credit cards and debit cards, Canadians and Canadian businesses now have more ways to make and receive payments, and undertake their banking activities.

While the focus of the Committee's study was "digital currencies" in general, many of our witnesses spoke specifically about cryptocurrencies, which are digital currencies that rely on encryption; in particular, their focus was often Bitcoin. This emphasis is probably not surprising, as Bitcoin is currently the most widely used cryptocurrency. Created in 2009, this decentralized convertible cryptocurrency enables funds to be transferred over the Internet without the need for an intermediary, such as a bank or money services business. Witnesses said that Bitcoin consists of a combination of four technologies that the Committee feels are quite innovative and provide opportunities in both the financial services sector and possibly other areas:

- a decentralized peer-to-peer network;
- a currency-issuing system;
- a transaction verification system; and
- a public ledger relying on the "blockchain."

During the study, 55 witnesses appeared before the Committee in Ottawa. Witnesses included representatives from federal departments and agencies, the Bank of Canada, law enforcement entities, provincial securities regulators, the financial services sector, money services businesses, payment card operators, academics, lawyers, digital currency-related businesses, trade associations, a charity and individuals who participate in the digital currency sector.

The Committee's witnesses spoke about potential definitions for the term "digital currency," common types of digital currencies and potential uses for these currencies. As well, they identified a range of opportunities resulting from the use of digital currencies and their technologies, such as Bitcoin's blockchain technology. Of particular note was the innovation associated with these technologies, the implications for transaction costs, the availability of another payment option, and the impact on the protection of users' identities and the recording of transactions. Finally, the Committee's witnesses highlighted a variety of challenges with digital currencies, technologies and businesses. In this context, such issues as potential criminality and its effects, losses, taxation, and access to

information and protection for users were discussed. Their testimony is summarized in Chapter 3, and their names and organizations are listed in Appendix A.

The witnesses' comments were invaluable in helping the Committee to understand the issues relating to the digital currency sector, and informed our thoughts and recommendations, which appear in Chapter 2. The Committee's conclusions are contained in Chapter 4.

The Committee also took a fact-finding trip to New York City in February 2015 to learn about New York State's proposed regulations for digital currency-related businesses and the potential effects on that state's digital currency sector. The groups and individuals with whom the Committee met in New York City are indicated in Appendix B.

A glossary of digital currency-related terms is provided in Appendix C.

As final points of context for this report, the Committee provides one definition and one data-related caution. For the purposes of this report, the term "digital currency" describes electronic forms of exchange and their associated technologies that operate on the Internet and/or on mobile devices, and that are not issued or governed by a government or central bank. Finally, as the study commenced more than a year ago, the data in Chapter 3 are now somewhat dated, as the digital currency sector has evolved in the last year. For this reason, dates for particular amounts and percentages are indicated, as the data may not reflect the sector's current state.

CHAPTER 2: THE COMMITTEE'S THOUGHTS

A. Digital Currency Types and Uses

When the Committee began its study on digital currencies, a priority was understanding the meaning that should be given to the term "digital currency." One key conclusion that the Committee reached is that elements of the "digital currency sector" – the currencies, the technologies and the businesses – are constantly evolving, and the terms used when discussing the sector are often unclear. On balance, the Committee supports the Department of Finance view that a digital currency is defined by four key characteristics:

- Its value can be held and exchanged without the use of banknotes or coins.
- It is not the official currency of a country.
- It has the intended purpose of being exchanged for real or virtual goods and services.
- Its units can be transferred between individuals, between businesses, and between individuals and businesses.

During the study, the Committee learned about various classification systems for digital currencies, including whether they can be converted to state-issued currencies, and whether they are "centralized," and thus managed by a central authority, or "decentralized," and thereby controlled by the users of the digital currency. The Committee determined that decentralized convertible digital currencies, which are known as cryptocurrencies and of which Bitcoin is the most popular example, should be the focus for any potential regulations.

Cryptocurrencies protect their technology from cyber-attacks and counterfeiting attempts through both encryption and a decentralized network called the public ledger.

In the Committee's view, Bitcoin's blockchain – or public ledger – technology is extremely innovative and has the potential to be used in a growing number of applications, including as a registry to record such events as marriages and real estate purchases, and in the context of "smart contracts" that can be executed by a computer. The Committee firmly believes that additional applications for this technology are on the horizon, that may result in reduced costs, increased choices and convenience, for individuals and businesses.

As well, the Committee agrees with witnesses that – at present – digital currencies have three main roles in Canada:

- a form of money;
- a commodity; and
- a payments system.

In our opinion, the role that digital currencies play as a payments system is perhaps the most significant of the three functions. The Committee holds this view largely because of the blockchain technology that records bitcoin transactions and – as noted above – may hold the promise of many more applications.

The Committee believes that digital currencies, technologies and businesses give rise to a number of opportunities, but like almost all new and emerging technology, there are also challenges and

risks. In our view, the federal government should consider actions in four main areas in order to maximize the opportunities associated with digital currencies, and to manage their associated challenges. These areas are:

- the effect of regulation on innovation in the digital currency sector;
- the use of digital currencies to launder money and finance terrorist activities;
- protecting the users of digital currencies; and
- taxation challenges in relation to digital currencies.

B. Digital Currency-Related Opportunities

During the study, the Committee learned that the emergence of digital currencies has led to a range of opportunities, and that Canada could become a global hub for the digital currency sector if the legislative and regulatory environment is conducive to innovation. In our view, to foster this type of environment in Canada, it is critically important that regulations for the digital currency sector be appropriate.

In particular, the Committee is aware of the potentially negative impacts that future regulations imposed on the digital currency sector could have on innovation. In the Committee's view, digital currencies, especially their associated technology, is among the most notable developments in recent history, and was even compared to the invention of the Internet itself by several witnesses. Blockchain technology is particularly promising as a means to transact without a third party and as a permanent public database. The Committee believes that, in time, even incumbent financial institutions will recognize the benefits of this technology and may adapt it to meet their needs. Many witnesses stated that this technology is at a risk of failure because of poor judgement on the part of regulators and lawmakers. Therefore the Committee understands that familiar, centralized solutions built from a centralized financial system are unsuitable for this decentralized payments technology. Believing that conscious efforts are required to support digital currency-related innovation, the Committee recommends that:

Recommendation 1:

The federal government, in considering any legislation, regulation and policies, create an environment that fosters innovation for digital currencies and their associated technologies. As such, the government should exercise a regulatory "light touch" that minimizes actions that might stifle the development of these new technologies.

The Committee heard of the many opportunities resulting from the emergence of digital currencies and their technologies. Lowering transaction costs may be the first opportunity realized by the marketplace, as increased choices for payment systems may put pressure on the current high cost for international remittances. In our opinion, lower costs are relevant for the many Canadians making international transfers.

As well, it seems to the Committee that there is also an opportunity for the government. Blockchain technologies that facilitate identity protection can benefit Canadians, as governments seek to protect the information they hold on behalf of its citizens. The Committee recognizes that, in recent years,

hackers have targeted government databases, including those at the Canada Revenue Agency, in an attempt to steal identities and other personal information. In our view, compared to centralized databases, blockchain technology may provide a more secure way to manage information, as it does not rely on security software developed by third parties. From this perspective, the Committee recommends:

Recommendation 2:

The federal government consider the use of blockchain technology when advantageous to deliver government services and to enhance the security of private information.

C. Digital Currency-Related Risks

1. Use of Digital Currencies to Launder Money and Finance Terrorist Activities

In the Committee's view, potential criminality is perhaps the greatest challenge to be managed. The Committee has a long and ongoing interest in issues of criminality, having conducted two statutory reviews of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, and having held hearings on various proposed amendments to the Act.

The Committee understands that digital currencies can be attractive to criminals who want to launder money, finance terrorism or perpetrate other crimes. As well, the Committee recognizes that it is the anonymity of digital currencies, and the ease they can be used to make domestic and – particularly – international transfers, that may make them conducive to criminal activity.

In the Committee's opinion, illicit users of digital currencies are most readily identified at the "on and off ramps," or digital currency exchanges, where digital currencies are converted to and from state-issued currencies. Furthermore, in recognizing the Committee's past and likely future examinations of Canada's anti–money laundering and anti–terrorist financing regime, we also believe that the similarities in the operations of digital currency exchanges and money services businesses give rise to a need for identical obligations for these two groups in relation to that regime. Therefore, the Committee recommends that:

Recommendation 3:

Digital currency exchanges, the "on and off ramps" of the digital currency system, be defined as any business that allows customers to convert state-issued currency to digital currency and digital currencies to state-issued currency or other digital currencies. To minimize the risks of illegal activity in relation to Canada's anti–money laundering and anti–terrorist financing laws, the federal government should require digital currency exchanges, with the exclusion of businesses that solely provide wallet services, to meet the same requirements as money services businesses.

Partially because of the Committee's previous studies on Canada's anti–money laundering and anti–terrorist financing regime, the Committee is aware of the global nature of the real and potential

criminality that is facilitated by digital currencies and – thereby – the need for global solutions. In today's globalized world, improvements in technology have made it easier for legitimate and illegitimate businesses to transact internationally.

A recurring theme with cryptocurrencies is the idea of *consensus*. It is consensus which provides transaction verification, and it is consensus which gives value to a cryptocurrency. As it is a theme of cryptocurrency, so it must be a theme in laws and regulations. The Committee believes that, where cryptocurrencies are shaped by network consensus, laws and regulations ought to be shaped by jurisdictional consensus.

In the Committee's view, coordinated international efforts are a particular priority to effectively counter the international nature of criminal activities and to prevent "jurisdiction shopping" by digital currency-related businesses. Consequently, the Committee recommends that:

Recommendation 4:

The federal government, on an active and ongoing basis, work with other countries to formulate global guidelines for digital currencies while respecting the "light touch" premise outlined in Recommendation 1 above.

During the study, the Committee was told that the association of certain digital currencies with criminal activity has had a negative effect on industry-wide growth. One obstacle is regulatory uncertainty. Regulators – such as Quebec's Autorité des marches financiers and New York State's Department of Financial Services – have started to implement licensing requirements for certain digital currency-related businesses in their jurisdictions.

Another obstacle faced by some cryptocurrency businesses is the inability to establish banking relationships.

The Committee listened to witnesses describing their difficulty in accessing financial services. The Committee does not believe that banks are prejudiced against cryptocurrency businesses, and think this is perhaps a result of banks being concerned about inadvertently violating the obligations of Canada's anti–money laundering and anti–terrorist financing regime. The Committee is mindful that, before money services businesses were regulated, banks were reluctant to accept these businesses as customers. In that context, the Committee recommends that:

Recommendation 5:

The Minister of Finance convene a roundtable with stakeholders, including banks, to look for solutions to the lack of access to banking services for digital currency related businesses, while recognizing the requirements of Canada's anti–money laundering and anti–terrorist financing regime.

2. Protecting the Users of Digital Currencies

During the study, the Committee learned that digital currency losses can occur in a variety of situations, and the Committee believes that any loss of funds – whether through cyber-theft,

bankruptcy or price volatility – is regrettable for financial services providers and their customers. The Committee recognizes that such losses are not limited to digital currencies in their role as a form of money or a commodity; in that regard, the periodic volatility in the relative value of the Canadian dollar and the current decline in oil prices should be remembered. In the same way individuals presumably consider the risk-return trade-off when purchasing or holding state-issued currencies or commodities, the Committee urges this type of analysis when considering the purchase of digital currencies.

The Committee has come to appreciate the importance of the digital currency sector being aware of any weaknesses in their technologies and systems, and of taking appropriate efforts to protect against cyber-attacks. Equally, the Committee believes that individuals must consider the risks that may result when holding funds in digital wallets, which are also being used for digital representations of state-issued currencies, or when placing their digital currency with digital currency exchanges, which are not regulated prudentially. While the Committee does not believe that these issues warrant regulation, the Committee encourages digital currency-related businesses and individuals to be mindful of these potential risks.

While securities regulation is not within the federal jurisdiction, the Committee is confident that Canada's securities regulators have expertise in assessing risk, and encourages them to continue to release relevant and timely information about digital currency-related risks. As well, notwithstanding our earlier comments about the need for digital currency-related businesses and individuals to be aware of weaknesses and risks, the Committee believes that the federal government has an important role to play in developing policies and providing information that will help consumers and merchants assess the benefits and risks of various financial products, and make the choices that are most appropriate for their situations. For these reasons, the Committee recommends:

Recommendation 6:

The federal government, through appropriate federal entities, provide concise information to the public about the risks of digital currencies and alternative payment systems.

3. Taxation Challenges in Relation to Digital Currencies

During the study, the Committee learned that there is some question about the taxation of digital currencies, such as bitcoin, which are used as a form of money by some and as a commodity by others. The Committee is also mindful that, due to the difficulties associated with tracing digital currency transactions, the government may have difficulty combating tax evasion that is committed using digital currencies. Nevertheless, the Committee urges the government to work with other countries and in appropriate venues to address, in particular, this taxation issue.

The Committee believes that providing the public with specific and comprehensive guidance about the taxation rules for digital currencies – whether received as business or employment income, held as an investment, or used to buy goods and services – would assist individuals and businesses in understanding the rationale for these rules and in complying with them. As well, further examination of the use of digital currencies as a form of money would assist the government, particularly the Canada Revenue Agency, in determining whether other taxation rules – such as those that apply to

foreign currencies – should apply to digital currencies. In that context, the Committee recommends that:

Recommendation 7:

The federal government, through the Canada Revenue Agency, provide concise information to Canadians about the tax obligations of digital currencies when received as income, held as an investment, or used to purchase goods or services.

D. Focusing on the Future

In the Committee's view, there is currently not a need for the government to take actions to regulate digital currencies beyond those that are specifically mentioned in our recommendations. The Committee believes that additional actions could have unintended consequences, such as hampering the innovative aspects of digital currencies that may hold great future promise in finance and other areas. With traditional methods of payment and institutions, individuals are expected to undertake due diligence, and – in our view – the same situation should exist regarding digital currencies, their technologies and businesses.

The Committee understands that, as can be seen with other new technologies in the payments sector, the technology associated with digital currencies is dynamic and evolving rapidly; thus, the opportunities and challenges identified in this report may no longer be applicable in just a few years. The Committee intends to revisit the issue of digital currencies, and, at that time, the Committee hopes to learn about the evolution of the digital currency sector, and to make recommendations for further federal action to maximize the opportunities and manage the risks that have arisen since this study. In this light, the Committee recommends that:

Recommendation 8:

Due to the evolving nature of digital currencies, the Standing Senate Committee on Banking, Trade and Commerce review this study of digital currencies and their associated technologies to assess the appropriateness of the regulatory environment in the next three years.

CHAPTER 3: WITNESSES' TESTIMONY

A. Digital Currency Types and Uses

1. Definitions for "Digital Currency"

Some of the Committee's witnesses spoke about the term "digital currency." According to the Department of Finance, there is no universally agreed upon definition for the term; it may include electronic forms of a state-issued currency, such as prepaid access cards and wire transfers. Similarly, the Bank of Canada stated that the term may include online credit card transactions, Interac transactions sent by email, online bill payments and the cashing of cheques with a smart phone's camera. The Bank also indicated that individuals often use terms such as "e-money," "e-cash," "digital money," "digital currency" and "virtual currency" interchangeably, erroneously believing that they have the same meaning.

The Bitcoin Alliance of Canada suggested that a "virtual currency" is based on a ledger, a "digital currency" only exists digitally, and a "cryptocurrency" is based on cryptography. It identified cryptocurrencies as a subset of digital currencies, which are a subset of virtual currencies.

The Department of Finance said that it considers a digital currency to have four characteristics:

- its value can be held and exchanged without the use of banknotes or coins;
- it is not the official currency of a country;
- it has the intended purpose of being exchanged for real or virtual goods and services; and
- its units can be transferred between individuals, between businesses, and between individuals and businesses.

2. Common Types of Digital Currency

Witnesses noted that digital currencies can be classified in several ways. The Department of Finance indicated that a digital currency can be classified in relation to its convertibility: a "convertible" digital currency can be converted to a state-issued currency, while a "non-convertible" digital currency can be used only to purchase real or virtual goods and services from particular retailers. It suggested that convertible digital currencies should be the primary focus for possible regulation.

As well, the Bank of Canada and the Department of Finance identified a classification method that focuses on whether a particular digital currency is "centralized" or "decentralized." According to the Bank, a centralized digital currency can be used to purchase a variety of goods and services, and is issued – and often managed – by a central authority that typically has a corresponding debt for the amount of digital currency that it has issued. The Department described these central authorities as entities that – in relation to a particular digital currency – verify the transactions, determine the supply, and create rules regarding exchange or use.

According to the Bank of Canada, prepaid payment cards are a good example of a centralized digital currency; in this case, such entities as Visa and MasterCard are the central authorities. The Bank also provided another example of a centralized digital currency: the pre-paid Octopus card in Hong

Kong; originally intended as a prepaid transit card, the card has become generally accepted by retailers. The Royal Canadian Mounted Police mentioned Liberty Reserve, which had a central authority that issued Liberty Reserve dollars and was used as part of a global money laundering scheme.

The Bill and Melinda Gates Foundation discussed the mobile phone-based centralized digital currencies that are used in a number of developing countries. For example, it mentioned M-PESA, which is owned by Vodafone – a mobile telecommunications company – and is used in Kenya and other countries. It said that M-PESA allows individuals to exchange an electronic form of the local currency through their mobile phones.

The Bank of Canada characterized decentralized digital currencies, which are sometimes referred to as cryptocurrencies, as digital currencies that operate over peer-to-peer networks where no single entity manages the currency or assumes a debt for the currency that has been issued. Samir Saadi, of the University of Ottawa, stated that digital currencies and online payments have existed for decades, but that cryptocurrencies are unique because decentralized peer-to-peer networks allow the ownership of digital currencies to be transferred without the need for an intermediary.

In providing examples of decentralized digital currencies, the Department of Finance noted that bitcoin is a decentralized, convertible digital currency. The Canadian Virtual Exchange and the Bank of Canada commented on litecoin, which is the second most popular decentralized, convertible digital currency. The Bank also mentioned peercoin and Ripple.

Ripple Labs described Ripple as an open-source payment protocol designed to provide interoperability among the payments systems of financial institutions, clearing houses and central banks. It indicated that the Ripple network relies on a decentralized public ledger and cryptographic technology that are similar to those used by Bitcoin; however, its "consensus" verification process differs from that used by Bitcoin. It also mentioned that all currencies – state-issued or digital – can be traded over the Ripple network, and that the system has its own digital currency – the XRP – that is used as a security mechanism and to convert currencies. TD Bank Financial Group commented that some banks are experimenting with the Ripple network to exchange funds between them.

The Bitcoin Strategy Group stated that, as of 9 April 2014, there were more than 100 different decentralized, convertible digital currencies worldwide. According to Bitcoin Foundation Canada, as of 2 October 2014, between 500 and 1,000 cryptocurrencies were being used, and between 50 and 100 digital currency exchanges were converting bitcoin to other digital currencies. Andreas Antonopoulos, author of *Mastering Bitcoin*, highlighted that anyone can – at minimal cost – create a new digital currency that is secure and globally accessible.

3. Potential Uses for Digital Currencies

A number of the Committee's witnesses identified the various ways that digital currencies are being used in Canada, and generally commented on three roles: a form of money; a commodity; and a payments system. They also discussed other potential uses for digital currencies.

(i) A Form of Money

The Bank of Canada discussed the definition for the term "money," indicating that three characteristics must exist:

- in being a medium of exchange, it must be generally accepted among individuals and businesses;
- in being a unit of account, it must allow the value of various goods and services to be compared; and
- in being a store of value, it must enable individuals and businesses to assume – with confidence – that its value will be stable over time.

According to the Department of Finance, if digital currencies become both a stable store of value and generally accepted as a means of payment for goods and services, they could become more widely used as money. That said, it noted that long-term use of digital currencies as a form of money would be unlikely, partially due to volatility in the price of digital currencies, as has occurred with bitcoin.

The Canadian Payments Association suggested that confusion exists about the role that digital currencies play in the Canadian economy. In its view, digital currencies – particularly bitcoin – do not constitute money, as they are not a medium of exchange, a unit of account and a store of value.

Similarly, the Bank of Canada highlighted that bitcoin and other cryptocurrencies currently are not a popular medium of exchange. As of 2 April 2014, less than 200 Canadian retailers accepted bitcoin. Regarding bitcoin as a unit of account, the Bank noted that the value of a transaction where bitcoin is the method of payment is often considered in terms of a state-issued currency. It also suggested that, as of 2 April 2014, the price of bitcoin was forty times more volatile than the relative value of the U.S. dollar; thus, bitcoin is not a stable store of value.

The Department of Finance stated that the *Currency Act* governs legal tender and currency, lists the characteristics of coinage and banknotes, and identifies the dollar as Canada's monetary unit. It highlighted that the Act does not limit the use of digital currencies for transactions in Canada, and that merchants can accept a variety of methods of payment in exchange for goods and services, including U.S. dollars and Canadian Tire "money." Joshua Gans, of the University of Toronto, indicated that – in Canada – taxes must be paid with legal tender; therefore, as long as bitcoin is not considered to be legal tender, the Canadian dollar will be required for that function.

The Bitcoin Alliance commented on the meaning that Canadian law gives to the term "money"; "legal money" likely does not include bitcoin, which is not state-issued and is not universally accepted. It also noted that the Canada Revenue Agency and the Bank of Canada do not view bitcoin as "legal money," and observed that bitcoin cannot denominate a negotiable instrument under the *Bills of Exchange Act* if it is not "legal money."

HISTORY *of* MONEY IN CANADA

1600 - 1850 Wampum (strings and belts with beads and shells) and copper shields

1600 - 1770 Beaver pelts, wheat, moose skins, and French and Spanish coins

1685 - 1759 Card money (playing cards) and paper money

1700 - 1870 UK and US coins

1817 - 1934 Bank notes issued by commercial banks

1854 Introduction of *Currency Act* and Canadian dollar (UK coins and US coins declared legal tender)

1867 - 1935 Dominion notes issued by the provinces

1870 Canada's first coins issued

1935 First bank notes issued by the Bank of Canada

1970s Credit cards

1990s Debit cards

2009 Cryptocurrencies?

Source: Bank of Canada, A History of the Canadian Dollar, December 2005, figure prepared by the Library of Parliament.

According to John Jason, of Norton Rose Fulbright Canada, the *Currency Act* states that any contract in Canada that references "money" is referring to Canadian dollars; thus, if contracts refer to payment in bitcoin, they will have to describe the way to make that type of payment. He also said that the government became the issuer of currency to support economic activity and so that people had confidence in using paper notes as a medium of exchange. In his view, people may not have confidence in bitcoin, as its price fluctuates significantly; that said, those who advocate using bitcoin believe that its price will stabilize as its supply rises.

Jeremy Clark, of Concordia University, highlighted the Royal Canadian Mint's "Mint Chip" project, stating that Mint Chip is a "digital representation" of Canadian currency.

(ii) A Commodity

The Department of Finance pointed out that many people have invested in digital currencies, and – on 26 March 2014 – noted that an exchange-traded fund based on bitcoin would soon be available in the United States. Similarly, Joshua Gans indicated that a number of holders of bitcoin are not exchanging their bitcoin for goods and services; instead, they are retaining their bitcoin, which will be beneficial if the price of bitcoin rises. According to the Department of Finance, it is too early to determine whether digital currencies will be successful as a commodity, as any value they might have in this regard is linked to their use as a currency. Bitcoin Foundation Canada suggested that, although bitcoin is likely not a security, it can be used as the unit of account for a securities transaction, such as an investment fund denominated in bitcoin.

Samir Saadi stated that New York's Wall Street has recently shown an interest in digital currency trading. He highlighted that hedge funds are being created that involve strategic trading based on volatility in the price of digital currencies. He also mentioned that Nasdaq Group is providing Noble Markets – a company that facilitates institutional trading in bitcoin – with software used by major securities exchanges, and that the New York Stock Exchange is providing Coinbase – a digital wallet provider and the first U.S.-based digital currency exchange – with capital. In his view, Coinbase appears to be a reliable and secure platform for trading in bitcoin.

The Ontario Securities Commission indicated that platforms for trading bitcoin-based derivatives are being developed in the United States, and that the U.S. Securities and Exchange Commission has received applications to create exchange-traded funds using bitcoin.

The Department of Finance suggested that digital currencies, as a commodity, could be subject to securities regulation in Canada. According to Quebec's l'Autorité des marchés financiers and the Ontario Securities Commission, because of their current form, digital currencies do not qualify as "securities" or "derivatives" under their provinces' securities and derivatives legislation; consequently, they are not regulated as such. In their view, if digital currencies are packaged as an investment product or a derivative, that legislation would apply. The Ontario Securities Commission also stated that any publicly traded digital currency-related business is subject to the same regulatory requirements as other publicly traded companies, including disclosure to investors about material risks.

Elliot Greenstone, of Davies Ward Phillips & Vineberg LLP, noted that no Canadian securities regulator has indicated whether digital currencies should be treated as a security or derivative for the

purposes of securities law. He highlighted l'Autorité des marchés financiers' recent decision to monitor digital currencies pursuant to Quebec's *Securities Act*, *Derivatives Act* and *Money-Services Businesses Act*. He also mentioned that the *Securities Act* does not define the term "security," although it does define the term "investment contract."

Regarding Ontario's securities legislation, Elliot Greenstone and John Jason suggested that bitcoin may not fall within the definition for the term "security," as there is no person or entity that "issues" bitcoin. Elliot Greenstone said that the Ontario Securities Commission plans to monitor investment activities that are related to digital currencies and to take action when Ontario's *Securities Act* is violated.

(iii) A Payments System

The Department of Finance and the Canadian Payments Association stated that because of Bitcoin's framework, it is like a payments system. The Canadian Payments Association commented that a digital currency may not be appropriate for Canada's clearing and settlement system, as the system facilitates transactions in Canadian dollars; in 2012, $16.7 trillion in payments – excluding cash transactions – were made in Canada. It indicated that, of these payments, 80% was cleared through the Canadian Payments Association's systems, including the Automatic Clearance Settlement System – which is used by private payment networks, such as Interac, for clearing and settlement – and the Large Value Transfer System; the remaining 20% was cleared by credit card companies, within financial institutions or through closed-loop mechanisms, such as prepaid payment cards and digital currencies.

According to the Interac Association, as of 12 June 2014, its network was used an average of 12 million times daily through Automated Teller Machine (ATMs), e-commerce purchases and person-to-person e-transfers; these transactions represented approximately 55% of all payment card-based transactions. As well, the Canadian Payments Association mentioned that the unregulated payments sector, which includes PayPal and Google, has not yet identified a need to access the Canadian clearing and settlement system. The Interac Association and PayPal stated that they do not process digital currency payments.

Using global data, the Canadian Payments Association estimated that – as of 10 April 2014 – there were between 1,000 and 2,000 daily transactions in Canada involving bitcoin, which represented 1/100 of 1% of the total volume of daily Canadian payments transactions. It noted that developers of digital currencies are not eligible for membership in the Canadian Payments Association, as they are not regulated financial institutions. Bitcoin Foundation Canada said that, as of 2 October 2014, approximately 80,000 Bitcoin transactions occurred daily around the world.

SELECTED POINT-OF-SALE PAYMENT METHODS USED IN CANADA

Cash

According to the Bank of Canada, while the use of cash for retail payments is declining due to advancements in payment method technologies, cash is Canada's most commonly used and accepted form of retail payment, as it is perceived to be less costly, easier to use, more secure and more widely accepted than debit cards and/or credit cards. In 2013, cash accounted for 43.9% of the volume and 23.0% of the value of point-of-sale transactions.

Debit Cards and Credit Cards

According to the Bank of Canada, debit card use increased significantly over the period from 1994, when the Interac system was introduced, to the early 2000s; credit card use has grown consistently since 2000, partly due to an increasing number of rewards programs. Bank of Canada data show that, in 2013, debit cards and credit cards accounted for 21.1% and 30.8% respectively of the volume of point-of-sale transactions, and 25.1% and 45.9% respectively of the value of such transactions. Contactless payments represented 2.9% of debit card and 19.3% of credit card point-of-sale transactions in that year.

Cryptocurrencies

According to the Canadian Payments Association, as of 10 April 2014, there were between 1,000 and 2,000 daily transactions in Canada involving bitcoin. These transactions represented 1/100 of 1% of the total volume of Canada's daily payments transactions.

Visa Canada Corporation and MasterCard suggested that an important indicator of whether Bitcoin has a role to play in the Canadian payments system is the number of merchants that accept bitcoin as a method of payment. The Department of Finance said that, as of 26 March 2014, approximately 1,500 businesses around the world accepted – or were willing to accept – bitcoin; of these, about 200 were located in Canada. It also noted that many of these businesses are online retailers, particularly in the technology sector, or offer online gambling; examples of businesses that accept bitcoin include Overstock.com, WordPress, Zynga, Tesla and Virgin Galactic. The Department suggested that Canadian merchants that accept bitcoin as a method of payment, and the extent to which they are treating bitcoin as a currency and paying suppliers with it, should be identified.

According to the Canadian Virtual Exchange, as of 9 April 2014, there were 22 Canadian merchants accepting bitcoin as a method of payment for online purchases; it stated that another 150 Canadian merchants would be doing so by 9 May 2014, and an additional 1,000 by October 2014. Andreas Antonopoulos identified Bitcoin as being most commonly used for charitable donations and tipping.

MasterCard indicated that digital currency payments could be incorporated into its network or processed through a separate network if digital currencies become regulated. In its view, digital currencies can be useful for person-to-person payments and business payments. It also noted that it has U.S. patents for digital currencies.

TD Bank Financial Group said that banks incur costs in settling transactions; thus, they would welcome less expensive forms of settlement, including through the use of digital currencies if appropriate regulation and security exist. As well, TD Bank Financial Group noted that it does not compete with digital currencies.

PayPal mentioned that it does not accept deposits in PayPal wallets in the form of cash or digital currencies. MoneyGram International commented that, while it does not currently transfer digital currencies, it would consider doing so if these currencies are regulated.

Selected Payments Systems Used in Canada

CRYPTOCURRENCIES

Some cryptocurrencies function as both a currency and a decentralized payments system, such as bitcoin and Bitcoin respectively. Users of cryptocurrency-based payments systems perform all steps in a transaction, interacting with each other directly through an Internet-based peer-to-peer network without the need for a central computer server. Transactions are recorded on a public ledger, which is shared across the network, and their validity is verified through cryptographic techniques. Merchants accepting cryptocurrencies may use payment processors, such as BitPay, Coinbase and BitNet, to help with clearing and settling cryptocurrency payments. As well, payment processors may convert such payments into a state-issued currency for deposit into a merchant's bank account.

PAYPAL

PayPal is a third-party intermediary that verifies and settles online transactions between a purchaser and a merchant. It allows a merchant to accept a credit card or debit card as a method of payment without having a direct relationship with the credit card or debit card company, or with a payment processor that clears and settles transactions. Verification is conducted on the PayPal website when the purchaser opens an account and registers his/her financial information with PayPal. Settlement occurs when a payment is transferred by PayPal from the purchaser's account to the merchant's account.

CREDIT CARDS

In Canada, Visa and MasterCard are structured in accordance with the four-party model: the cardholder; the merchant; the card issuer; and the payment processor. A fifth participant is the credit card company itself. Visa and MasterCard have proprietary clearing systems that are not subject to the Canadian Payment Association's rules or standards.

DEBIT CARDS

Like credit cards, point-of-sale debit card transactions in Canada are structured in accordance with the four-party model; with these transactions, a fifth participant is the Interac Association. The Interac Association's Direct Payment network is decentralized, with clearing and settling occurring at the financial institution where the funds are located. The Interac Association's members clear and settle their transactions through the Canadian Payments Association's Automated Clearing Settlement System.

The Canadian Bankers Association indicated that Canada's banks support the creation of new ways for consumers and merchants to engage in e-commerce, and noted that banks are involved in promoting new payments technologies, such as near field communication (NFC) for contactless payment cards and mobile wallets on cell phones. It also mentioned that Canadian banks and credit unions have been collaborating on a set of principles, entitled the Canadian NFC Mobile Payments Reference Model, for mobile payments. Similarly, MasterCard said that, as cash is used less often as a method of payment, payments system developments have included contactless payment cards, mobile payments and direct deposit to prepaid cards.

The Royal Bank of Canada commented on its "RBC Secure Cloud," which allows its clients to choose among debit, credit or gift cards when making a mobile payment; sensitive information is stored on its servers in Stratford, Ontario and Guelph, Ontario, and not on a cell phone. It also noted that it offers free person-to-person transactions that can be accessed through bank accounts or Facebook.

The Interac Association mentioned Interac Flash, which allows contactless use of a debit card and can be used with other technologies, such as RBC Secure Cloud. The Canadian Payments Association commented that it has participated in the implementation of products that enable consumers to make deposits with photographs of cheques and to use contactless debit cards.

PayPal said that it allows users to transfer money or make payments online without having to disclose banking or financial information. It noted that – as of 12 June 2014 – $1 of every $6 spent globally on e-commerce was processed through PayPal, and it had 148 million active registered accounts; 5.5 million of these accounts were held in Canada. It also stated that it processed $27 billion in mobile payments in 2013, an increase from $600 million in 2010.

According to the Bill and Melinda Gates Foundation, mobile phone-based digital currencies – such as M-PESA – are used as digital payments systems for making low-cost transfers and payments. It said that there are more than 250 mobile phone-based payments systems worldwide, which together have more than 200 million users. It explained that an individual can use M-PESA to exchange cash for an electronic form of the local currency through an agent, generally without a fee, and then – at a cost of $0.02 or less in some countries – transfer this electronic money to another individual using his/her mobile phone; the recipient can then exchange the electronic money for cash at an agent, with the fee for this service ranging from $0.25 to $0.35.

MasterCard highlighted the use of mobile phones in some countries – such as the Democratic Republic of the Congo – to receive government benefits and as a means of identification, as few individuals have access to a bank account. Visa Canada Corporation mentioned Fundamo, a South African company that it owns; the company enables individuals to send money to others using mobile phones and text messages, with the mobile phones linked to a mobile network operator account or a bank account.

(iv) Other Potential Uses

According to the Bitcoin Embassy, digital currencies are not simply another payments system to be studied within the traditional framework for financial services, and nor are they a new form of money that can be examined like a foreign currency or a commodity; rather, they could be viewed as a new technology that is replacing their obsolete predecessors. Elliot Greenstone said that many research

papers refer to cryptocurrencies as "pseudo-fiat currencies." In his view, this term suggests that cryptocurrencies have the characteristics of a commodity, such as having a limited supply, and of a currency, such as being used to make payments.

The Bitcoin Embassy stated that new products involving digital currencies are currently being developed, such as smart contracts, decentralized autonomous corporations, and decentralized markets that enable peer-to-peer sales of goods and services. Similarly, Ripple Labs commented on smart contracts, which it described as contracts having a set of automatic rules that are entirely readable and operable by computers. L'Autorité des marchés financiers noted that, in the United States, there have been attempts to use Bitcoin's technology to develop decentralized securities exchanges.

Andreas Antonopoulos said that Bitcoin's technology in relation to its public ledger is being used to record events, such as the purchase of automobiles, company shares and real estate, as well as marriages. The Bill and Melinda Gates Foundation suggested that this technology could be used to develop title registries for land and other types of assets, from which low-income people would benefit; Ripple Labs and Elliot Greenstone also mentioned title registries. Moreover, Elliot Greenstone indicated that the blockchain technology could potentially be used to rent cars with digital keys.

Andreas Antonopoulos noted that some individuals and organizations are providing "digital tokens" when a transaction is submitted on the blockchain; these tokens allow an individual or organization to access a service, such as Internet bandwidth or an AirBnB property.

As well, Andreas Antonopoulos noted that a business operating internationally could use a digital currency to pay employees who live in various countries, and suggested that a computer programmer could easily incorporate a digital currency into payroll software.

4. Bitcoin as an Example

In commenting on digital currencies, the Committee's witnesses often focused on bitcoin and Bitcoin, the currency and the payments system respectively. In particular, they spoke about the creation of the underlying technology and the functioning of the payments system, and the currency that is used with that system.

(i) The Technology and Payments System

According to the Department of Finance and the Bank of Canada, the term "Bitcoin" generally describes the decentralized, cryptographic network that functions as the payments system for "bitcoin," which is the digital currency used by Bitcoin.

The Bitcoin Embassy and Andreas Antonopoulos described Bitcoin as a combination of four new mathematical and cryptographic technologies: a decentralized peer-to-peer network; a decentralized currency-issuing system; a decentralized transaction verification system; and a public ledger, called the blockchain, that records transactions. The Bitcoin Embassy noted that Bitcoin's most distinctive features are its decentralized and interdependent payments system and digital currency, which cannot function without each other.

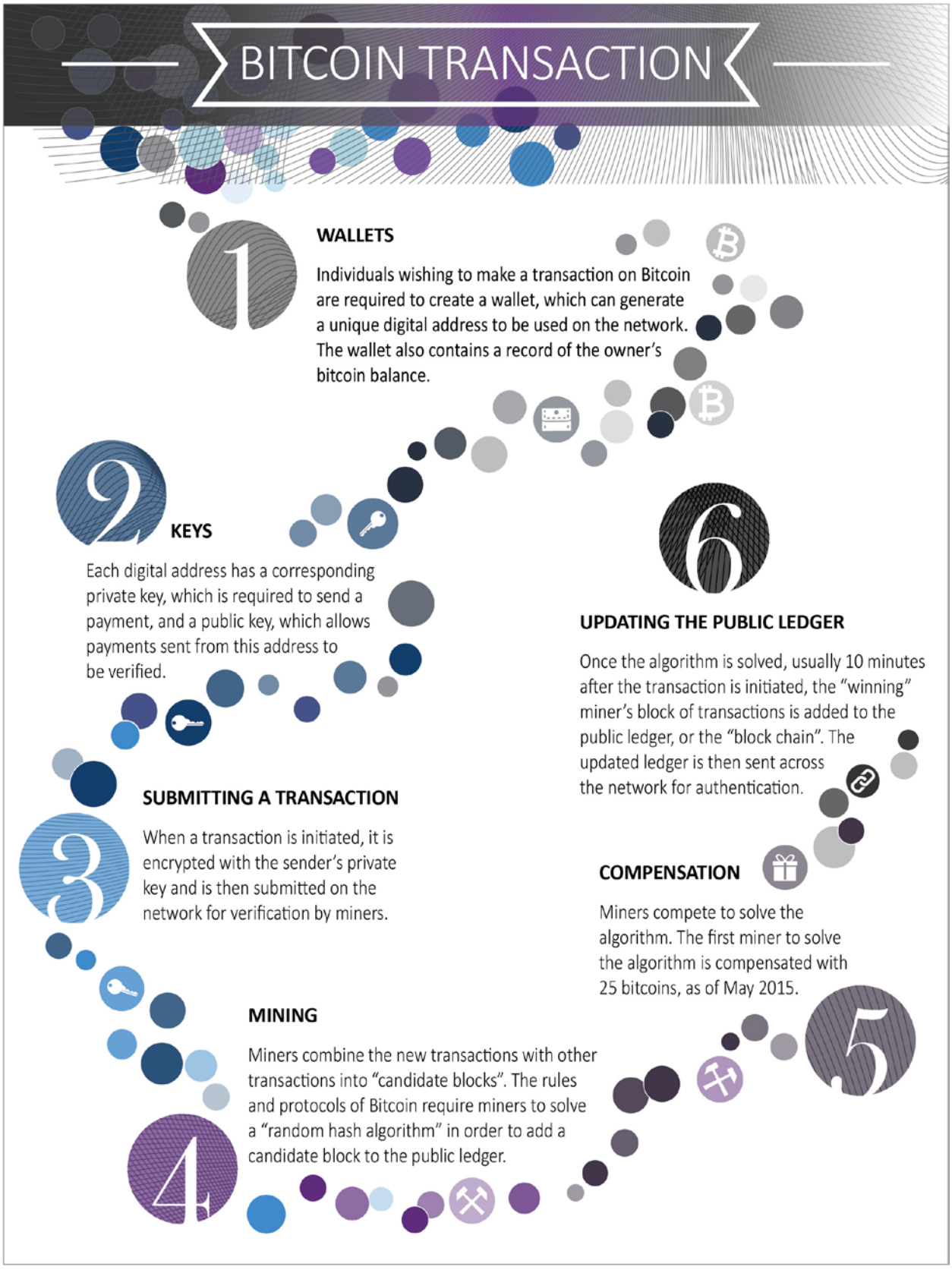
BitPay indicated that Bitcoin was created in 2009 as an open-standard, open-protocol and open-source payments system; it is designed for the Internet and is owned collectively by all of its users. The Department of Finance mentioned that the demand for digital currencies, particularly bitcoin, originated with people who had a libertarian philosophy, and who wished to transfer money without government interference and at low cost. It also commented that Bitcoin was developed by a group of people who were interested in mathematics, and was not created in order to generate a profit. Samir Saadi highlighted that Bitcoin was created after the 2008 global financial crisis, when some people lost faith in the traditional financial system.

Andreas Antonopoulos said that Bitcoin is at the same stage of development as the Internet was in the early 1990s. He suggested that, within eight years, more applications relating to Bitcoin will be available to consumers.

According to the Bank of Canada, before the creation of Bitcoin, decentralized digital currencies were not considered to be feasible, as it was not possible to verify whether "double spending" – an amount sent to one individual is also sent to another person – had occurred. The Bank stated that Bitcoin's verification of transactions through the blockchain ensures an absence of "double spending."

The Department of Finance noted that Bitcoin transactions are recorded on a public ledger that can be accessed on a website, and that "miners" undertake a "mining" process to verify the availability of funds for a transaction. According to it, the miners' computers solve mathematical problems to ensure that each bitcoin's private key, which is like a personal identification number, is authentic; once the mathematical problem is solved, the transaction is verified and recorded on the public ledger. Andreas Antonopoulos emphasized that the main purpose of mining is to secure and verify transactions, and that receiving bitcoin as compensation for mining activities is meant to provide Bitcoin users with an incentive to verify the transactions.

BitPay and Andreas Antonopoulos described Bitcoin transactions as being more similar to cash, than to credit card, transactions; for example, a payment made using bitcoin involves the purchaser sending a precise amount directly to the seller, while a payment made using a credit card involves the purchaser providing his/her credit card number to a merchant, which – through the authorization associated with its receipt of that number – receives payment after involving intermediaries. Andreas Antonopoulos also commented that a single Bitcoin transaction does not authorize any future payments or reveal the sender's identity to the entity receiving the payment.



Source: Figure prepared by the Library of Parliament.

Bitcoin Foundation Canada indicated that, as of 2 October 2014, the cost of mining and the price of acquiring one bitcoin were approximately US$310 and US$385 respectively. It noted that this gap is narrowing, and that mining costs are falling as miners consolidate and offer "cloud mining services," rather than using individual computers to mine bitcoin. Samir Saadi suggested that increased computing power and the development of new technologies could offset the increased costs of verifying Bitcoin transactions.

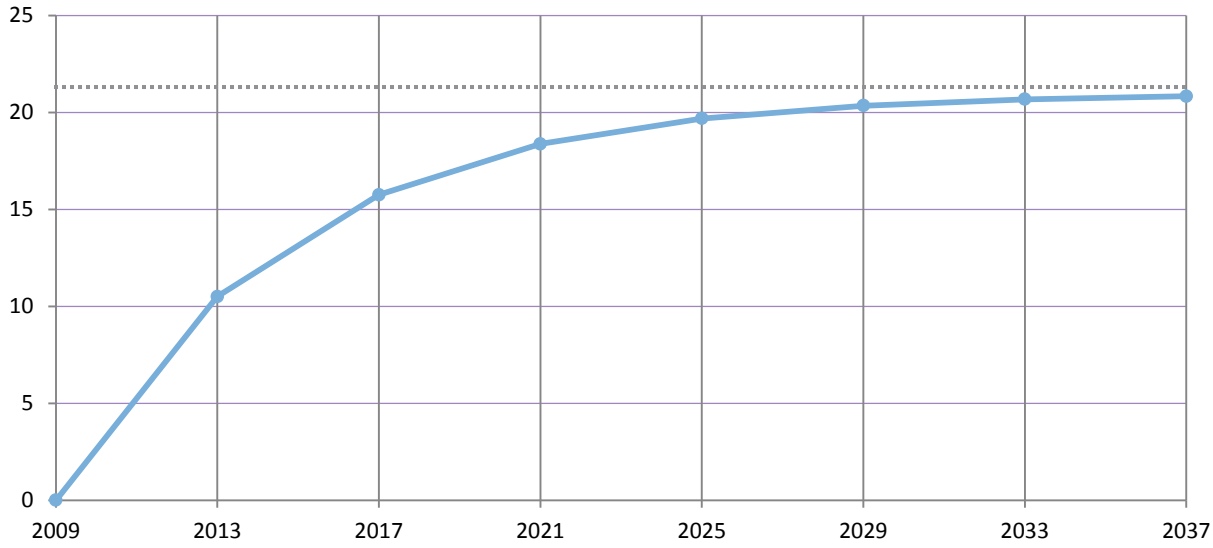
Andreas Antonopoulos commented on a group of independent miners – called GHash.IO – that, in 2014, was undertaking nearly 51% of Bitcoin's mining activities. He said that some miners voluntarily left GHash.IO and joined other mining groups due to the "reputational risk" to Bitcoin of one mining group potentially being able to disrupt the verification of transactions. In his view, if a mining group controls more than 50% of Bitcoin's mining activities, it could delay the processing of transactions; however, it would not be able to steal bitcoin or invalidate transactions.

(ii) The Currency

The Department of Finance stated that a bitcoin is not a file, but rather a number associated with a Bitcoin address, which functions like a bank account. According to Jeremy Clark, bitcoin is not a bearer instrument and cannot be held physically; rather, an individual obtains a cryptographic – or private – key that gives him/her "signing authority" for the Bitcoin address. Bitcoin Foundation Canada noted that the loss of the only copy of a private key results in a permanent loss of the associated bitcoin. Andreas Antonopoulos highlighted that private keys, which are essentially numbers, can be stored digitally or physically; physical storage involves printing the keys out on paper, which is relatively more secure and not subject to hacking.

As well, the Department of Finance said that the supply of bitcoin – which was 15 million as of 26 March 2014 – is limited to 21 million; the supply is determined not by a central authority, but rather by a mathematical formula in the mining process, with miners receiving new bitcoin when they verify transactions. It suggested that miners may charge a fee to verify transactions once this limit is reached and bitcoin is no longer received as compensation.

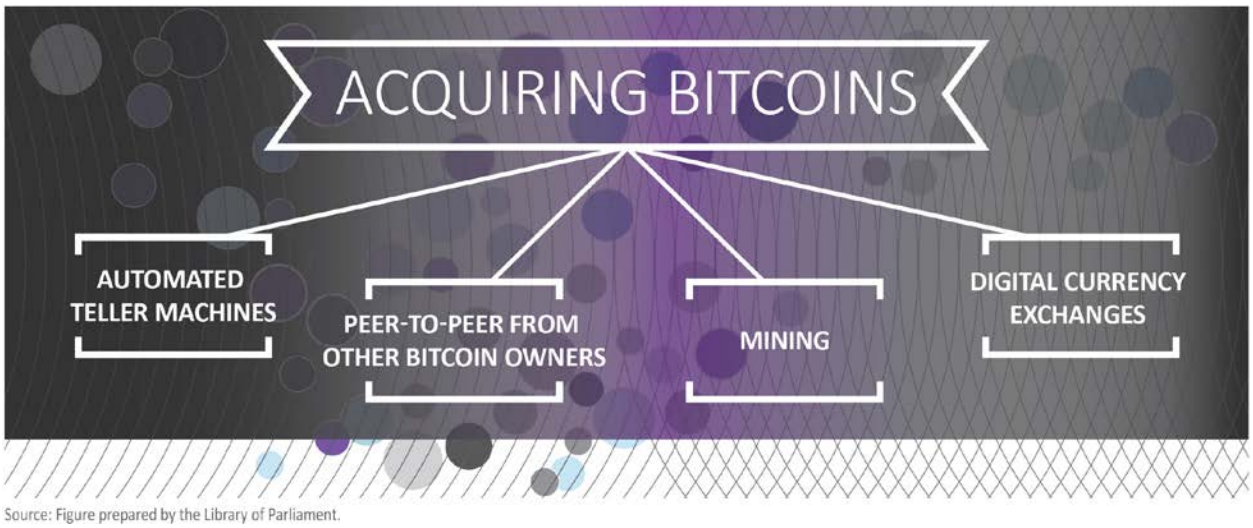
Projected Supply of Bitcoin, 2009–2037 (millions)



Source: Figure prepared using information obtained from: Coin wiki, "Controlled Supply."

Andreas Antonopoulos noted that the mathematical algorithm that regulates the supply – and determines the maximum supply – of bitcoin is based on the supply curve of a precious metal, such as gold, which is just one option when considering the supply of a digital currency. Bitcoin Foundation Canada mentioned that, although the supply of bitcoin is limited to 21 million, the ability to divide one bitcoin will allow Bitcoin to expand.

The Bitcoin Strategy Group said that, in addition to mining, bitcoin can be obtained in three ways, with the price of a bitcoin perhaps being different in each case: directly from a holder of bitcoin; through a bitcoin exchange; or from a bitcoin ATM.



Source: Figure prepared by the Library of Parliament.

Bitcoin Foundation Canada highlighted that making a payment with bitcoin is separate from having the transaction recorded on the blockchain, and noted that a bitcoin payment occurs instantaneously, while the recording of the transaction can take between 30 seconds and 60 minutes. The Department of Finance stated that the average time taken to verify a transaction – about 10 minutes – is a result of the computing power required for the verification process.

B. Digital Currency-Related Opportunities

1. Innovation

In speaking to the Committee about the innovation arising from digital currencies and their technologies, witnesses discussed the possible impacts of regulation, Canada's role as a digital currency hub, and state-supported digital currencies and associated technologies.

(i) Possible Impacts of Regulation

Witnesses commented that regulations for digital currencies could negatively affect innovation in relation to them and their technologies. The Department of Finance noted that digital currencies may not be extensively regulated in Canada in the future, as doing so could constrain these currencies' innovative aspects, while Jeremy Clark and Joshua Gans indicated that any federal regulations for these currencies should be implemented in a way that would encourage innovation. Similarly, the Royal Canadian Mounted Police said that laws and regulations for digital currencies should not negatively affect the innovative benefits that legitimate users derive from these currencies.

In focusing on a particular digital currency, Andreas Antonopoulos and the Digital Finance Institute suggested that regulations for digital currencies should not be implemented until Bitcoin's technology, and its potential applications, are better understood. The Bitcoin Alliance supported regulations that would be technologically neutral and respect Bitcoin's innovative aspects, while Ripple Labs said that any regulations should consider digital currencies' reliance on decentralized public ledger technology and its potential use in ways that would benefit payments systems.

Andreas Antonopoulos also said that imposing a centralized model of regulations for all digital currencies would not be suitable or efficient for decentralized networks, as this approach would weaken Bitcoin's security and hamper innovation; it would be more appropriate to secure decentralized digital currency networks through innovative decentralized technologies, including smart contracts, multi-signature escrow to release funds and "hardware wallets." The Bitcoin Embassy stated that Bitcoin should not be regulated, as doing so would discourage innovations designed to address potential cybersecurity risks, but noted that some digital currency-related businesses have indicated that they want to be regulated. The Digital Finance Institute mentioned the importance of dialogue among digital currency stakeholders regarding potential regulations.

John Jason noted that there are two perspectives to consider when deciding whether to regulate digital currencies: the need to protect consumers against harm, and the development of Canada's digital currency sector. He also said that legal issues may arise over the next few years, as Canada's legal framework may not currently address certain aspects of digital currencies' technologies.

According to the Canadian Payments Association, any potential regulations for digital currencies should consider past market failures – and their impacts – in the areas where these currencies could play a role in the Canadian economy, including as a form of money, an investment or a payments system.

(ii) Canada as a Global Digital Currency Hub

Witnesses said that Canada could become a global hub for digital currencies. For example, Samir Saadi noted that digital currency-related businesses seeking to expand are looking for countries where regulations are not onerous. The Bitcoin Embassy stated that Canada has the potential to become a global hub for these businesses, as it has a high rate of Internet usage, a skilled workforce that is knowledgeable about technology, competitive electricity rates, and "organized" Bitcoin meetings and groups in almost every major Canadian city. Similarly, Bitcoin Foundation Canada suggested that Canada could play a lead role in digital currency mining if it maintains a fiscal and regulatory framework that is technologically neutral in relation to digital currencies. Elliot Greenstone mentioned that Canada should not implement regulations for digital currencies that are more stringent than those in other countries, as doing so could hamper the expansion of Canada's digital currency sector.

Warren Weber, who appeared as an individual, indicated that Canada could have a larger share of global digital currency-related businesses and investment if the country were to be a "first mover" in establishing a stable legislative and regulatory environment for digital currencies. That said, he also commented that Canada could avoid expensive mistakes if it first considers the impacts of digital currency-related regulations in other countries. According to Jeremy Clark, if Canada were to be among the first countries in the world to regulate Bitcoin, entrepreneurship and innovation could result, both generally and regarding Bitcoin.

David Descôteaux, of the Montreal Economic Institute, noted that – from a global perspective and as of April 2014 – Canadian Bitcoin-related businesses had received the second-largest amount of venture capital, after the United States. He highlighted the importance of ensuring that individuals, investors and businesses understand the types of legislation that apply to Bitcoin in order to strengthen their confidence in the technology, and of creating a regulatory environment that promotes Bitcoin and encourages venture capital investments in Canada's Bitcoin-related businesses. In his opinion, regulations for digital currencies would reduce investors' perceived risk that Bitcoin will be determined to be illegal in Canada and would increase investment in Bitcoin-related businesses.

(iii) State-supported Digital Currencies and Their Technologies

Witnesses discussed specific federal support for digital currencies and their technologies. For example, Joshua Gans said that a state-issued digital currency in Canada should be considered, while Andreas Antonopoulos indicated that central banks may use Bitcoin's blockchain technology to develop a state-issued digital currency. Regarding its development of a digital currency, the Bank of Canada stated that innovation with respect to digital currencies and payments system technologies is best provided by the private sector, which should be guided by an appropriate legal framework.

Warren Weber suggested that promoting a government-sponsored, centralized digital currency – and restricting decentralized digital currencies – could stifle innovation. According to Samir Saadi,

the federal government should not develop a digital currency, as the failure of a government-sponsored digital currency could affect the entire economy; a digital version of the Canadian dollar would likely be a better option. He also commented that digital currencies should not be viewed as technologies that should either become the dominant type of currency or fail; rather, they could be used alongside state-issued currencies.

The Dominion Bitcoin Mining Company supported the government "sanctioning" or "endorsing" a regime of bitcoin wallets; these wallets would be protected by strong encryption protocols and would be subject to a small fee per transaction, similar to a Tobin tax. It stated that the revenue generated from this proposed fee could be used to establish an insurance scheme, similar to deposit insurance, and that the proposed fee could become a source of revenue for the government if bitcoin becomes widely used. According to it, the existence of "sanctioned" digital wallets could accelerate the use of bitcoin throughout Canada and serve as a model for other countries.

The Digital Finance Institute said that governments should make investments and create policies that would support the development of digital finance technologies. In particular, it and the Bitcoin Embassy said that the government should make positive public statements about digital currency technologies. Similarly, Samir Saadi highlighted that the development and expansion of Canada's digital currency sector could be supported by encouraging the innovative use of bitcoin, as well as the associated technology.

2. Transaction Costs

The Committee's witnesses commented that the use of digital currencies and their technologies affects transaction costs for both individuals and businesses.

(i) Individuals

Witnesses highlighted that digital currencies reduce the need for intermediaries in the payments system, which enables lower costs. According to the Department of Finance, Bitcoin's true technological innovation is the reduced need for intermediaries. Similarly, the Bitcoin Embassy noted that Bitcoin avoids the inefficiencies that result from using financial intermediaries to transfer or store assets; any individual is able to transfer bitcoin to others at low cost, instantaneously and without the need for documentation. Joshua Gans mentioned that digital currencies – such as bitcoin – reduce the need for governments, banks and other financial institutions to be involved in transactions. In his opinion, the lack of such intermediaries results in lower costs for certain types of transactions, especially those that are international.

The Department of Finance suggested that peer-to-peer transfers of digital currencies may be an attractive and cost-effective mechanism for individuals to send international remittances; these transfers can be less costly than those that involve banks or money services businesses, and do not require a currency exchange. Similarly, Jeremy Clark said that Bitcoin's low transaction fees could enable international remittances and micro-transactions, which usually have a value that is less than $1. According to Joshua Gans, international transactions are an area where innovation in digital currencies would provide the largest benefit. As well, the Digital Finance Institute commented that the development of new technologies in the financial sector, such as purely digital financial products and their delivery through international digital platforms, reduces the cost of financial services and their delivery.

BitPay indicated that, in its role as a payments system, Bitcoin could compete with existing financial services, such as money transfers. MoneyGram International stated that it provides money transfer services in more than 200 countries, and that the average transaction amount is $300 to $400; moreover, it can facilitate person-to-person money transfers and transfers of money directly to bank accounts in countries that receive large volumes of international remittances, such as China, Mexico, India and the Philippines. It explained that, with its money transfer services, the sender pays all of the transaction fees, the transfer to the recipient can take only minutes, and the amount of the fees depends on both the country to which the transfer is being sent and the size of the transfer, with relatively higher fees charged when lower amounts are transferred. It also said that, for a transfer of $100, the transaction fee could range from $5.00 to $10.00 and the currency exchange fee could be equivalent to a couple of percentage points of the value of the transaction; for a transfer of $1,000, the transaction fee would be at least $9.99.

Jeremy Clark noted that, as of 3 April 2014, the cost of a standard Bitcoin transaction was approximately $0.05; the fee did not depend on the value of the transaction. He and the Department of Finance indicated that – as of 3 April 2014 – the transaction fee to convert one bitcoin into a Canadian dollar ranged from 0.5% to 1.5%, depending on the bitcoin exchange. According to the Canadian Bankers Association, as of 10 April 2014, the charges that applied when buying bitcoin through a particular exchange included a fee of about $5 per $100 to deposit Canadian dollars into an account with the exchange, and a fee of 1.5% of the amount of the transaction to exchange those dollars for bitcoin; similar fees applied when selling bitcoin and withdrawing the dollars from an account at a particular exchange. The Royal Bank of Canada mentioned that the use of digital wallets involves costs; on 10 April 2014, these costs were a minimum fee of 1% to transfer bitcoin person-to-person.

(ii) Businesses

Witnesses said that digital currencies and their technologies may reduce transaction costs for businesses. For example, the Department of Finance and the Bank of Canada indicated that digital currencies' transaction fees are low in comparison to credit card acceptance fees. The Interac Association highlighted that, as of 12 June 2014, its average fee for retailers was $0.03 to $0.05 per transaction, which included the mark-up by the payment processor. PayPal stated that businesses benefit from its system because they can receive payments without any start-up fees; as of 12 June 2014, the standard processing fee was 2.9% of the value of the transaction plus $0.30. Samir Saadi mentioned that, because of low transaction costs, businesses that export may benefit from using digital currencies. Bitcoin Foundation Canada suggested that, due to China's control over the transfer of yuans outside of the country, Bitcoin has become popular in China as individuals and businesses have sought other options to trade internationally.

Cost of Selected Payment Methods for Merchants, 2014

DEBIT CARD	CREDIT CARD	PAYPAL	BITPAY
$0.03 to $0.05 per transaction	1.5% to 4.0% of the value of the transaction	2.9% of the value of the transaction plus $0.30	No fee per transaction; the cost of monthly plans varies from $0 to $300 or more

Sources: Prepared using data obtained from: Department of Finance, *The Road to Balance: Creating Jobs and Opportunities*, 11 February 2014; and BitPay, BitPay pricing, accessed 2 April 2015. Costs for the debit card and PayPal payment methods are based on testimony by the Interac Association and PayPal in their appearances before the Standing Senate Committee on Banking, Trade and Commerce on 12 June 2014.

BitPay noted that, since its creation in 2011, more than 30,000 merchants have become clients; its competitors include Coinbase and BitNet, and additional competitors are emerging on an ongoing basis. It explained that its role is similar to that of a credit card payment processor: it acts as the merchant's agent to help clear and settle payments made with bitcoin. BitPay also mentioned that merchants can receive the proceeds of their sales in the form of a state-issued currency or as a mix of bitcoin and a state-issued currency.

Andreas Antonopoulos stated that banks could benefit from the blockchain technology; for example, they could adapt it for their own purposes, and eliminate the need for intermediaries in clearing international fund transfers or in purchasing stocks and equities. Similarly, BitPay commented that financial institutions could implement Bitcoin's technological advancements, thereby enabling them to provide interbank settlements, international transfers, foreign exchange transactions and other products at lower cost.

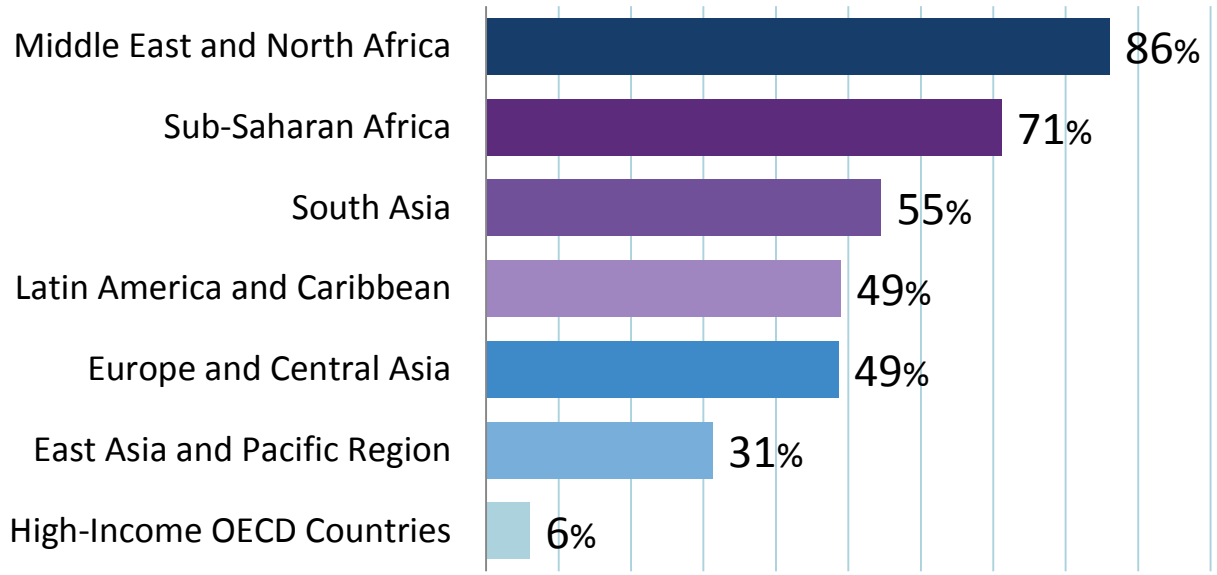
3. Payment Options

According to the Committee's witnesses, the emergence of digital currencies as another payment option in some situations provides an opportunity to increase individuals' access to financial services in developing countries. Witnesses also commented that businesses may benefit from new payment options.

(i) Individuals in Developing Countries

Witnesses highlighted that digital currencies can lead some individuals to have access, or enhanced access, to financial services. Andreas Antonopoulos indicated that individuals who lack access to financial services or international credit have the greatest need for Bitcoin; some of these individuals – many of whom live in Kenya, Lagos, Nigeria and other African countries – use their mobile phone extensively. He stated that, as of 8 October 2014, there were 2.5 billion people worldwide who were "unbanked" and lived in cash-based societies; up to 6 billion individuals could not access international markets or credit with their domestic banking system. According to him, with digital currencies and mobile phones, those who lack access to financial services can connect to the world on an equal basis to those in Western countries.

Adults without an Account at a Formal Financial Institution, Various Regions, 2014 (%)



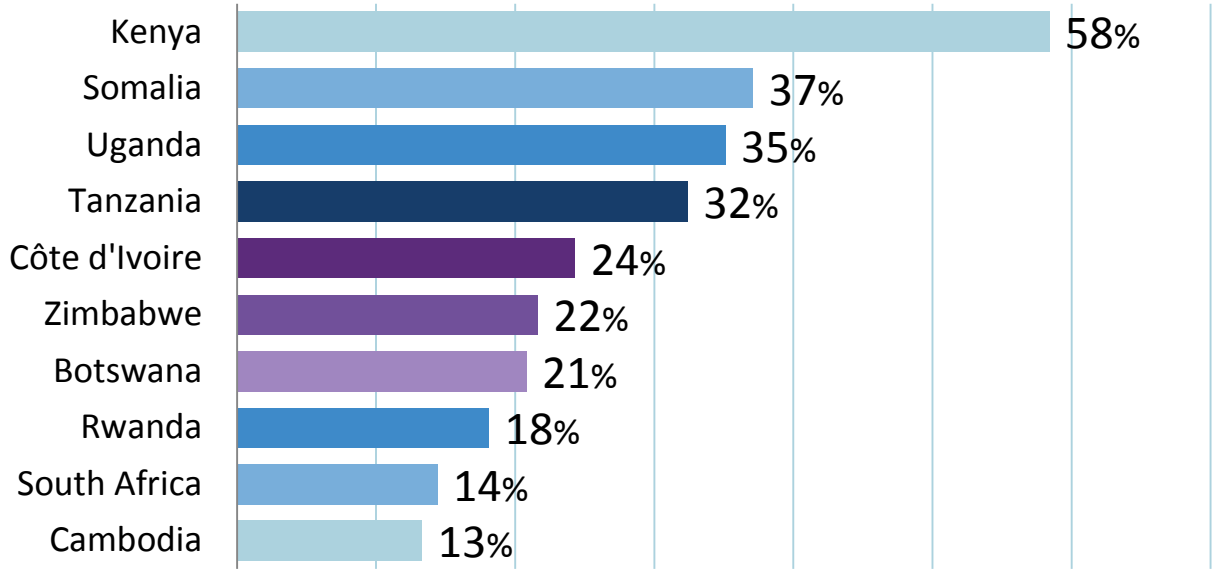
Source: Figure prepared using information obtained from: The World Bank, Global Findex Database, accessed 27 May 2015.

The Bill and Melinda Gates Foundation mentioned that the least expensive way to improve financial inclusion in developing countries is through digital products, including mobile phone-based payments systems. It said that, in many developing countries, a significant portion of the population has a mobile phone, including individuals with lower incomes; consequently, there is great potential to increase financial inclusion through mobile phone-based financial services. It highlighted that a large portion of the population in Tanzania is accessing financial services through a mobile phone.

According to the Bill and Melinda Gates Foundation, mobile phone-based payments systems, such as M-PESA, have a number of advantages in developing countries: they are significantly less expensive than the alternatives currently available to low-income people; the number of access points for these systems is far greater than the number of bank branches; and people who are part of a large mobile payments network are better protected against income shocks, such as a medical emergency, a marriage or having a baby, as it is easier for friends and relatives to send money through the network than through regular channels. It also said that mobile phone-based payments systems can increase access to credit for low-income individuals in developing countries; new banking services offered through M-PESA, such as M-Shwari in Kenya and M-Pawa in Tanzania, make short-term emergency loans based on a user's history of M-PESA transactions.

The Digital Finance Institute suggested that M-PESA's success in Kenya shows that new technologies in digital finance, including cryptocurrencies, have the potential to increase access to financial services for those who are "unbanked" or excluded from financial markets. It noted that, according to a World Bank report, these individuals are mostly women.

Adults Who Reported Using a Mobile Phone for Monetary Transactions, Various Countries, 2014 (%)



Source: Figure prepared using information obtained from: The World Bank, *Global Findex Database*, accessed 27 May 2015.

The Bill and Melinda Gates Foundation explained that some digital currencies, particularly those that offer anonymity, would not meet the needs of low-income individuals in developing countries. It said that being unknown to financial institutions and governments is generally a problem for them, and they may be charged a higher interest rate and not receive government services as a result; using digital currencies to make anonymous transactions would not address the issue of not being known to financial institutions and governments. As well, according to it, bitcoin's price volatility limits its usefulness for low-income people in developing countries, as these individuals need their limited assets to have a stable value.

MoneyGram International said that it can transfer money to mobile phones when countries have appropriate technology; these countries include Kenya. In its view, the ability to make money transfers online and through mobile phones provides individuals with enhanced access to financial services.

Andreas Antonopoulos noted that Bitcoin is not yet adapted for use on Nokia 1000, which is the most widely used cell phone platform in the world. That said, he highlighted that Bitcoin is gradually being used with simpler technologies, such as text messaging, and that the cost of manufacturing smart phones is falling; one smart phone could provide thousands of individuals with access digital wallets and other financial services. According to him, parts of Canada could benefit from Bitcoin, as some regions may have limited access to the traditional banking system.

(ii) Businesses

Witnesses identified a number of unique characteristics of digital currencies and their payments systems from which businesses could benefit. For example, BitPay and MasterCard highlighted the ability to transfer an asset – such as bitcoin – and immediately settle a transaction with no

counterparty risk. According to the Bill and Melinda Gates Foundation, the instantaneous clearing and settlement of small-value payments that is a feature of the mobile-phone based payments systems used in developing countries could benefit developed countries.

The Department of Finance, BitPay, the Bank of Canada and Jeremy Clark commented that payments are irreversible when digital currencies are the method of payment, which is beneficial for merchants; credit card transactions can be reversed when fraud occurs. BitPay also noted that this irreversibility is useful for businesses that wish to sell to customers in jurisdictions where it is difficult to collect payment for goods and services.

The Canadian Virtual Exchange stated that Bitcoin is not affected by banking hours or holidays, as it operates all day, every day.

4. Identity Protection and Recording of Transactions

The Committee's witnesses indicated that digital currencies and their technologies may protect the identity of the parties involved in transactions and provide a payments system that is recorded because of the public ledger.

(i) Identity Protection

Witnesses stated that individuals can protect their personal information when using digital currencies. In the opinion of the Bank of Canada, the anonymity associated with digital currencies may be useful to individuals who wish to conduct specific types of transactions; for example, someone may want to undertake a transaction with an individual who is unknown to him/her without divulging personal information, such as a bank account or credit card number. The Royal Canadian Mounted Police noted that legitimate users of digital currencies can benefit from increased privacy.

According to BitPay, the risk of identity theft can be reduced if bitcoin is the method of payment for online transactions, as – unlike credit card payments – a customer's identity and account number are not provided with Bitcoin transactions; thus, there is no identity information that can be stolen. It stated that, as of 12 June 2014, using bitcoin as the method of payment could have prevented 12 million people annually from becoming a victim of identity theft and $20 billion per year globally in payment fraud. It also noted that one of the major differences between credit card payments and bitcoin payments is that, with the former, merchants can retain and reuse the cardholder's account information to process multiple, perhaps illegitimate, charges; conversely, as each bitcoin transaction is unique, merchants cannot reuse the information. Similarly, the Bill and Melinda Gates Foundation noted that mobile payments systems in developing countries do not require a customer's identity and account number to be provided when a transaction is made, which reduces the risk of fraud; developed countries would benefit from such systems.

The Bitcoin Embassy said that both bitcoin and a credit card can be a method of payment for an average user; however, the former has lower fees and a reduced risk of fraud or identity theft. In comparing transactions with credit cards to those with bitcoin, Andreas Antonopoulos suggested that Bitcoin users have direct control over the privacy of their financial transactions, are not required to disclose their identities to undertake a transaction, and do not have to trust that financial intermediaries will safeguard their financial accounts. He stated that requiring identification for Bitcoin transactions would compromise users' privacy and weaken the payments system.

(ii) Recording of Transactions

Witnesses in Ottawa and groups the Committee met during its fact-finding trip to New York City commented on the record of transactions that is a part of the public ledger. The Department of Finance stated that Bitcoin is one of the most transparent payments systems because transactions are recorded on the public ledger and any emails associated with Bitcoin addresses are traceable. That said, it explained that a Bitcoin address is a series of letters and numbers; consequently, the entity associated with a particular address may be unknown, which gives rise to the notion that Bitcoin is pseudo-anonymous.

Jeremy Clark mentioned that Bitcoin addresses can be identified, as – for example – companies may publish their addresses so that they can receive payments from clients using Bitcoin, individuals may make purchases with bitcoin and have goods shipped to a physical address, or an individual's Internet Protocol address may be discovered.

The Department of Finance suggested that Bitcoin's public ledger generally makes transactions using bitcoin more transparent than those with most other methods of payment, while Jeremy Clark indicated that an individual using bitcoin is more anonymous than someone using a debit or credit card; both said that Bitcoin transactions are more transparent than transactions with cash. Andreas Antonopoulos noted that cash is more useful than digital currencies for illicit activities, as Bitcoin transactions can be traced with the public ledger. Joshua Gans stated that those who engage in illicit activities are dissuaded from using bitcoin because of the public ledger. That said, the Royal Bank of Canada commented that Bitcoin is not more transparent than other payments systems.

According to the Bitcoin Alliance, Bitcoin's public ledger could greatly assist law enforcement agencies that are investigating the flow of money in an allegedly fraudulent transaction; for example, there is little to no delay in retrieving records about a particular Bitcoin transaction, as all transactions are recorded on the public ledger. It mentioned that techniques that are similar to those used in traditional digital forensic investigations, such as linking an Internet Protocol address to a home or business, allow the "owner" of a Bitcoin address to be identified. Similarly, Ripple Labs indicated that a decentralized public ledger may enable suspicious financial flows to be traced, reported and analyzed more easily, as the information on the ledger would be more comprehensive than financial institutions' individual databases if digital currencies become more widely used.

C. Digital Currency-Related Risks

1. Potential Criminality and its Effects

Witnesses told the Committee that certain digital currencies have been linked to criminal activities, particularly money laundering and terrorist financing, and that some regulators have implemented – or are considering the implementation of – licensing requirements as a way to deter criminals from operating digital currency-related businesses and using digital currencies for criminal purposes. They also suggested that the association of digital currencies with criminal activities has negatively affected digital currency related-businesses that are trying to access banking services.

(i) Money Laundering and Terrorist Financing

Witnesses appearing before the Committee in Ottawa and law enforcement agencies the Committee met during a fact-finding trip to New York City commented on specific criminal investigations involving digital currencies that were linked to money laundering activities. The Royal Canadian Mounted Police discussed the Silk Road website, which was an online illegal market that used bitcoin as the method of payment and was shut down by the U.S. Federal Bureau of Investigation in 2013, and the Silk Road 2.0 website, which was shut down by international law enforcement agencies in November 2014. According to the Department of Finance, Canadians were making purchases on the Silk Road website and Canada was the fourth most common country of origin for illicit items listed on the website, after the United States, the United Kingdom and the Netherlands.

The Royal Canadian Mounted Police also mentioned the Liberty Reserve website, where criminal activity was conducted through the Liberty Reserve centralized digital currency exchange. It indicated that the exchange's operators were charged with laundering $6 billion through 55 million illegal transactions, and said that the Liberty Reserve investigation involved 17 countries, including Canada.

CRIMINAL ACTIVITY AND DIGITAL CURRENCIES

Liberty Reserve

Created in Costa Rica in 2006, Liberty Reserve was an international online payment processor whose website operated using anonymous accounts that accepted funds for transfer to other individuals; the funds were converted into Liberty Reserve Dollars that were tied to the value of the U.S. dollar, the euro or ounces of gold. In May 2013, U.S. law enforcement agencies and prosecutors shut down the Liberty Reserve website, arrested five people and seized bank accounts located in eight countries in relation to a money laundering scheme perpetrated by Liberty Reserve's owners. An estimated $6 billion was laundered through Liberty Reserve, which operated in 17 different countries.

Silk Road

Silk Road was an Internet-based black market for illegal goods and services that operated from January 2011 to 2 October 2013. It was used to distribute illegal drugs, as well as other illicit goods and services, to more than 100,000 buyers, with vendors accepting payments in bitcoin. According to estimates, Silk Road generated sales revenue of more than 9.5 million bitcoins and the website's operators collected more than 600,000 bitcoins in commissions from these sales. The U.S. Federal Bureau of Investigation made its first arrests in relation to Silk Road in October 2013. In February 2015, the creator of Silk Road was found guilty on seven charges, including money laundering, narcotics trafficking and computer hacking.

David Descôteaux noted that the amount of state-issued currencies that is laundered annually is several magnitudes larger than the amount of bitcoin in circulation, making this digital currency relatively insignificant in terms of money laundering. That said, the Department of Finance, the

Financial Transactions and Reports Analysis Centre of Canada, l'Autorité des marchés financiers and the Ontario Securities Commission stated that the anonymity provided by digital currencies and the ease they can be used to make transfers make them vulnerable to being used for money laundering and terrorist financing activities. According to MasterCard, regulations that would remove anonymity from Bitcoin transactions, and that would regulate digital currency exchanges in a similar manner to commodity exchanges or banks, would reduce the risk of Bitcoin being used for illicit activities.

The Royal Bank of Canada said that difficulties arise when attempting to trace the source of funds when payments are made using bitcoin; bitcoin exchanges cannot be properly monitored to ensure the absence of money laundering and terrorist financing. Elliot Greenstone highlighted that an individual carrying bitcoin across a border in a digital wallet on a cell phone would not have to report the amount of the bitcoin to border officials, even if it exceeds the $10,000 reporting threshold for the movement of monetary instruments across borders.

According to the Royal Canadian Mounted Police, a major challenge for law enforcement agencies is the time required to identify criminals who are using digital currencies. It stated that digital currency-related businesses could assist law enforcement agencies by being able to identify a client quickly, and in a manner that is similar to banks.

In mentioning the reported use of digital currencies to finance terrorism, the Canadian Security Intelligence Service indicated that it has not seen any evidence to substantiate media reports suggesting that terrorist groups are using bitcoin. It noted that it actively investigates the travel-related financial activities of foreign fighter terrorists; currently, it can identify situations in which state-issued currencies have financed travel, which might indicate that bitcoin is not being used for this purpose. The Digital Finance Institute stated that the U.S. Department of the Treasury has said that bitcoin is not being used to finance terrorism to any significant extent.

The Canadian Security Intelligence Service said that it is not overly concerned about digital currencies or online payments systems being threats to national security, perhaps because of high volatility in the price of digital currencies and relative difficulty in using such currencies to make payments, particularly when travelling. It stated digital currencies have not been found to fund or facilitate threats to Canada or other countries in any substantial way, but they could be used by terrorists in the future.

In commenting on the terrorist financing risks relating to digital currencies, the Digital Finance Institute explained that an individual can set up a bitcoin wallet that is completely anonymous, and can use that wallet to transfer significant sums to the anonymous wallet of a terrorist organization; it is unclear whether such a transaction would be detected under Canada's anti–money laundering and anti–terrorist financing regime's proposed regulations.

In the first budget bill introduced following the 2014 federal budget, the* Proceeds of Crime (Money Laundering) and Terrorist Financing Act *was amended to classify digital currency exchanges as money services businesses for purposes of Canada's anti–money laundering and anti–terrorist financing regime.

In relation to recent amendments to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, the Department of Finance said that it is currently developing regulations that will define the types of digital currency businesses that will be classified as money services businesses for purposes of Canada's anti–money laundering and anti–terrorist financing regime, and the obligations that will be imposed on these businesses. According to the Department, its regulatory approach will target the most vulnerable areas, including digital currency exchanges that facilitate the conversion of digital currencies to state-issued currencies, and will impose similar obligations on digital currency exchanges and money services businesses. It said that this approach, whereby regulations are not imposed on the technology and infrastructure underlying digital currencies or on digital currency users, should not stifle innovation.

According to MoneyGram International, for purposes of money laundering and safety and soundness requirements, digital currency exchanges and money services businesses should be regulated in a similar manner; consequently, exchanges should be required to have a program to ensure compliance with the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. It explained that the Act requires money services businesses to collect information on the identity of clients when transactions have a value of $1,000 or more; additional information must be collected if there is a business relationship with a customer. It also noted that reports are sent to the Financial Transactions and Reports Analysis Centre of Canada in two situations: suspicious transactions and international electronic funds transfers of $10,000 or more. John Jason said that regulating digital currency exchanges will target situations where a criminal is likely to convert funds resulting from criminal activities to a digital currency.

The Royal Canadian Mounted Police suggested that the Department of Finance's regulatory approach is consistent with actions being taken by the United States, the United Kingdom, Australia and New Zealand regarding digital currency exchanges. MasterCard and the Department of Finance commented that, in March 2013, the United States classified entities that facilitate Bitcoin transactions as money services businesses; they are subject to reporting requirements and know-your-customer rules under that country's anti–money laundering and anti–terrorist financing regime.

John Jason highlighted that the recently enacted provisions in the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* regarding digital currencies will attempt to regulate entities that operate outside of Canada. He explained that Canadian banking law does not regulate foreign banks unless they operate in Canada.

The Digital Finance Institute noted that no national risk assessment in relation to digital currencies occurred prior to the development of the 2014 amendments to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*; in its opinion, such an assessment should take place

before these amendments and the related regulations are implemented. It supported consultations with relevant stakeholders to determine the extent to which digital currencies represent a risk of being used in illicit activities, and commented that the government should consider regulations only if the risk of illicit activities rises.

Despite the difficulties with attempting to trace Bitcoin transactions, the Bitcoin Alliance indicated that Bitcoin-related businesses will be able to comply with the requirements of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* once they are in force; for example, they will be able to identify the source of funds in a Bitcoin transaction. The Canadian Virtual Exchange, which has ceased operations, said that it complied with the Act's regulations for money services businesses. BitPay highlighted that it screens potential clients and their businesses to ensure that they are not engaging in money laundering or terrorist financing activities.

The Canadian Virtual Exchange suggested that Bitcoin and foreign currency transactions should be regulated in the same manner, and that bitcoin should be considered a foreign currency under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. In its view, while such regulation could be inconsistent with the original intent of Bitcoin and could increase the administrative costs for digital currency-related businesses, it would maximize Bitcoin's potential. The Canada Revenue Agency noted that the *Income Tax Act*'s provisions relating to foreign exchange gains and losses would probably apply to digital currencies if they were to be considered a foreign currency.

According to the Royal Canadian Mounted Police, regulations for digital currencies should be designed with a view to deterring crimes that involve these currencies and reducing the use of these currencies by organized crime groups, particularly to transfer funds internationally and to launder money. In its opinion, regulations that allow the tracking and detection of international digital currency transactions, and that require certain digital currency-related businesses to be registered with a government entity, would assist law enforcement agencies in combating money laundering and terrorist financing activities. It noted that it is developing tools to assist in tracking digital currency transactions.

The Canadian Security Intelligence Service suggested that, in the future, law enforcement agencies will likely require the authority to obtain information on individuals who are participating in digital currency transactions. It also supported the introduction of regulations that would ensure that documentation on these individuals' identity is retained.

The Department of Finance said that money laundering and terrorist financing risks with digital currencies are a global issue, and international coordination – including through the Financial Action Task Force – is required to mitigate "jurisdiction shopping." The Financial Transactions and Reports Analysis Centre of Canada stated that it is working with financial intelligence units in other countries to develop a better understanding of digital currencies, as well as guidelines to respond better to money laundering and terrorist financing risks.

(ii) Other Types of Crimes

Witnesses highlighted that, in addition to laundering money and financing terrorist activities, criminals use digital currencies to commit other types of crimes. According to the Royal Canadian Mounted Police, digital currencies are a real and evolving threat to Canada's economic integrity, as

criminals exploit any new technology that provides anonymity and unregulated movement of funds. It explained that digital currencies are a challenge for law enforcement agencies for a variety of reasons: they are not subject to the same laws or regulatory regimes as legal tender; they can be used globally; and digital currency-related businesses can operate in the jurisdictions having the least onerous regulations. It also noted that conducting transactions using digital currencies is not an offence, but financing illegal activities with digital currencies is a crime.

The Digital Finance Institute suggested that the use of bitcoin could facilitate corruption. It provided the example of China, where bitcoin is a preferred method of payment when accepting a bribe, as the digital currency can be moved out of the country easily and anonymously.

The Royal Canadian Mounted Police indicated that, since 2013, the Canadian Anti–Fraud Centre has received more than 3,000 complaints about "ransomware scams." According to it, a criminal hacks into an individual's computer, uploads malware, and then asks for a ransom – typically in bitcoin – in exchange for removing the malware from the computer. It also commented that online websites that sell illegal goods are always emerging, and that international cooperation among law enforcement agencies is required to combat these websites.

(iii) Licensing of Digital Currency Exchanges and Automated Teller Machines

Witnesses mentioned that regulators in Canada and elsewhere – such as Quebec's l'Autorité des marchés, which appeared in Ottawa, and New York State's Department of Financial Services, which the Committee met during a fact-finding trip to New York City – have started to implement licensing requirements for certain businesses in order to provide a mechanism for properly assessing the risks associated with digital currencies and related businesses. Quebec's l'Autorité des marchés financiers said that digital currency exchanges offering person-to-person fund transfers are subject to the province's *Money-Services Businesses Act*. Moreover, New York State's proposed regulations would require digital currency exchanges, digital wallet providers and entities that administer digital currencies to obtain a licence from the New York State Department of Finance Services if they wish to operate in New York State.

Pursuant to Quebec's* Money-Services Businesses Act*, certain digital currency exchanges and operators of automated teller machines must apply for – and obtain – a fund transfer licence issued by l'Autorité des marchés, and comply with a number of obligations. Some of the obligations pertain to keeping records and verifying the identity of their customers.

L'Autorité des marchés financiers also explained that Quebec's *Money-Services Businesses Act* applies to businesses operating digital currency ATMs, and that these businesses are required to obtain a licence from it. It pointed out that, to obtain a licence, a digital currency ATM operator must provide specific information about its business; this information is submitted to the Sureté du Québec and local police forces, which undertake certain investigations and make a recommendation about the granting of a licence. In its view, this process is designed to ensure the integrity of businesses operating digital currency ATMs and to prevent money laundering. John Jason noted that similar

types of investigations are done in relation to banks, and suggested that Quebec's model should be considered by other jurisdictions. Andreas Antonopolous commented that the use of bitcoin on a small scale and for personal use should not be subject to regulation; for example, individuals who hold or transfer bitcoin in these circumstances should not require a licence.

In highlighting that bitcoin ATMs are located in a number of Canadian cities, the Department of Finance stated that the world's first bitcoin ATM was launched in Vancouver, British Columbia in November 2013 and processed about $1 million in transactions in its first month of operation. It also said that some bitcoin ATM owners partner with a bitcoin exchange. Bit Access stated that – as of 9 April 2014 – its ATMs were operating in Slovenia, the United Arab Emirates, Hong Kong, the United States, Mexico, Belgium, Australia, Germany, Switzerland and Canada. It commented that, as of 9 April 2014, it had 15 operational ATMs worldwide; they accounted for approximately 70% of all bitcoin ATM transactions. L'Autorité des marchés financiers mentioned that, as of 12 March 2015, there were about 20 ATMs operating in Quebec.

Elliot Greenstone suggested that Quebec's regulations for bitcoin ATMs should achieve two goals: minimize the extent to which the public associates these ATMs with money laundering and terrorist financing activities; and encourage people to obtain bitcoin from legitimate sources, rather than anonymously from strangers in exchange for cash. The Canadian Virtual Exchange supported regulations for bitcoin exchanges and ATMs, but suggested that these entities should be regulated to a lesser extent than Canadian financial institutions.

(iv) Access to Banking Services for Digital Currency-related Businesses

Some witnesses highlighted that the lack of regulations for digital currencies, particularly in relation to domestic and international anti–money laundering and anti–terrorist financing, has led some businesses to have difficulties in accessing banking services; in certain cases, existing banking relationships have been ended. For example, the Canadian Virtual Exchange stated that two of its chief executive officer's personal accounts with Canadian financial institutions were closed as a result of transfers of bitcoin.

The Department of Finance noted that some banks perceive that providing financial services to digital currency-related businesses could create a risk of non-compliance with Canada's anti–money laundering and anti–terrorist financing obligations, particularly concerning the identification of clients. The Canadian Payments Association explained that the know-your-customer regulations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* have prompted banks to develop mechanisms to identify their clients. It stated that transactions that use a digital currency would likely require a bank to use different mechanisms for this purpose; a digital currency exchange would be required to identify the counterparty in a transaction, which may be more difficult than identifying a client.

The Bitcoin Embassy commented that individuals and businesses are currently unable to make all necessary payments using Bitcoin; consequently, banks accounts and credit cards are still required. According to Bitcoin Foundation Canada, the inability to open a bank account is a barrier for some Bitcoin-related businesses, as they are unable to pay their employees in Canadian dollars without a bank account.

In mentioning that banking regulators could be concerned about banks being associated with digital currencies, John Jason said that the Office of the Superintendent of Financial Institutions has told Canadian banks not to be a vehicle for money laundering; thus, some banks are hesitant about opening accounts for digital currency-related businesses. He also noted that banks were once reluctant to open accounts for money services businesses; this situation changed when these businesses began to be regulated and to put anti–money laundering compliance programs in place.

According to David Descôteaux, Canada's financial institutions are awaiting regulations that are specific to digital currencies, and are not offering banking services to Bitcoin-related businesses due to a fear of inadvertently violating anti–money laundering and anti–terrorist financing requirements. In his view, clearer legislation could make it easier for banks and Bitcoin-related businesses to work together, and could prevent the movement of Canadian Bitcoin-related businesses to foreign jurisdictions. As an alternative to regulations, Bitcoin Foundation Canada and Andreas Antonopoulos supported clarification of Bitcoin's legal status to assist Bitcoin-related businesses in opening accounts at Canadian banks.

The Department of Finance said that a more risk-based approach to anti–money laundering and anti–terrorist financing legislation could address banks' concerns regarding digital currency-related businesses. It stated that banks make the decision about whether to provide banking services to particular customers, including digital currency-related businesses; with a risk-based approach, banks could provide services if these businesses are determined to present a low risk of money laundering and terrorist financing activities.

TD Bank Financial Group noted that it has no policy against – or formal procedure in relation to – Bitcoin, and indicated that fair banking practices would likely require it to open accounts for applicants unless there is a reason not to do so. It also suggested that unregulated financial entities should be subject to anti–money laundering and anti–terrorist financing obligations that are similar to those imposed on financial institutions, such as verifying client identification and holding clients' funds in segregated accounts. The Royal Bank of Canada highlighted that it does not have concerns about money laundering and terrorist financing by businesses that accept bitcoin as a method of payment.

The Digital Finance Institute said that there is a risk that over-regulation could lead Bitcoin-related businesses to leave the regulated banking system, either voluntarily or because financial institutions do not provide services to them because of concerns about contravening anti–money laundering and anti–terrorist financing laws; these businesses could turn to the "underground banking system," where transactions are not monitored or reported. It supported an approach to regulating Bitcoin that would ensure that banking services are provided to Bitcoin-related businesses, and that transactions by these businesses are monitored and reported pursuant to Canada's anti–money laundering and anti–terrorist financing regime.

2. Losses

According to the Committee's witnesses, digital currencies – and their value – can be lost in a variety of ways. In particular, they commented on cyber-theft and bankruptcy of a digital currency exchange, and volatility in the price of digital currencies.

(i) Cyber-theft and Digital Currency Exchange Bankruptcies

Witnesses mentioned that cybersecurity is a major concern for all entities that offer financial services. For example, TD Bank Financial Group identified cybersecurity as a significant risk for banks, noting that it is attacked by hackers thousands of time daily, employs about 250 people in its cybersecurity program, and spends between $175 million and $200 million annually to address cybersecurity and privacy risks. It also indicated that banks can usually block attempts to hack their databases, but are frequent targets for malware attacks by hackers who try to encrypt the banks' databases and demand a ransom for decryption.

TD Bank Financial Group also highlighted that hackers who have stolen credit card information in recent years did not target banks, but rather merchants or other businesses engaged in bank-like activities; as banks are often involved in resolving problems arising from the theft of credit card information, they are working with merchants to improve cybersecurity programs. It stated that the computers of consumers and small businesses typically do not have adequate protections, and are frequently targeted multiple times by cybersecurity threats after the initial security breach.

Moreover, TD Bank Financial Group commented that, because of quantum computing and human error, digital currency technologies will eventually be hacked. Jeremy Clark explained that it takes a number of years for cryptographic algorithms, such as those used with Bitcoin, to be hacked. According to him, while Bitcoin's cryptography has not yet been hacked, its algorithms will need to be changed within five decades to avoid this situation.

Andreas Antonopoulos said that decentralized digital currencies are less likely than centralized digital currencies and payments systems to be hacked, as hackers would have to target each digital wallet. He stated that decentralized digital currencies are more secure than traditional payments systems, as authority is not concentrated in a single entity. He also noted that, as a single "bad actor" would not be able to compromise Bitcoin, the payments system can be accessed by anyone and with any software application; Bitcoin's prior authorization is not required. In his opinion, while individual digital wallets may be hacked if not secured properly, Bitcoin's technology cannot be hacked. Moreover, he said that modern computer systems and mobile phones are not designed to store digital currency safely; however, new devices are being developed that will be able to store private keys and digital wallets.

Similarly, the Bitcoin Embassy indicated that Bitcoin remains operational because the risks are assumed by individual Bitcoin participants; the failure of one participant, such as a digital currency exchange, does not affect the viability of Bitcoin as a whole. It also mentioned that such failures have resulted in new security innovations that address risks, thereby making regulation unnecessary.

The Department of Finance and the Canadian Bankers Association said that those who hold digital currencies do not have adequate protection if cyber-theft occurs, and nor do they have sufficient recourse when a digital currency exchange goes bankrupt. According to MasterCard, users of digital currencies lack safeguards – including government insurance – if digital currencies are stolen or lost, such as through the insolvency of a digital currency-related business. TD Bank Financial Group indicated, when bitcoin is stolen, the victim has no way to prove that the stolen currency belonged to him/her, a situation that is unlike the theft of information – such as credit card numbers – from a

centralized database; in the latter case, the information that has been stolen is known and it is clear to whom protection should be provided.

CYBERSECURITY RISKS AND DIGITAL CURRENCY EXCHANGES

Mt. Gox

In July 2010, the Tokyo-based Mt. Gox bitcoin exchange was launched; by 2013, it was handling up to 70% of all Bitcoin transactions. On 7 February 2014, Mt. Gox suspended bitcoin withdrawals by customers due to security concerns and, on 28 February 2014, it filed for bankruptcy in Japan, stating that it had lost up to 750,000 of its customers' bitcoins and 100,000 of its own bitcoins; 200,000 of the lost bitcoins were later found by Mt. Gox in a digital wallet. Some have attributed the loss to hackers, while others suspect theft by someone working for Mt. Gox.

CAVirtex

CAVirtEx was a Calgary-based digital currency exchange that provided digital wallets for individuals trading in bitcoin and litecoin. On 17 February 2015, CAVirtex announced that it would cease operations because an older version of its database had been compromised. It indicated that no digital currencies had been stolen and that it would be able to fulfil customers' withdrawals of their digital currencies. It also noted that its closure was influenced by difficulties in obtaining banking services.

Flexcoin

Flexcoin, an Alberta-based company that referred to itself as a "bitcoin bank," announced in March 2014 that it was ceasing operations after 896 bitcoins were stolen from customers' online accounts by hackers. Flexcoin indicated that customers who held bitcoins in Flexcoin's offline accounts would be able to access their bitcoins.

TD Bank Financial Group highlighted ways to enhance the security of payments, including those that occur with digital currencies. It explained that multi-factor authentication requires three pieces of information from an individual: something the individual knows, such as a password; something the individual has, such as a cell phone; and something that is part of the individual, such as a thumbprint. It suggested that, in 10 years, banking activities will be conducted primarily through cell phones' microchips, rather than through payment cards. It also mentioned that digital financial products are not entirely safe, and that some amount of fraudulent activity will always exist; that said, banks and the federal government are working together to develop best practices to address cybersecurity threats. Bitcoin Foundation Canada said that certain types of digital wallets require multiple signatures before funds are transmitted, which enhances security, and that some companies offer digital wallets that have deposit insurance.

The Bitcoin Strategy Group indicated that "hot" digital wallets are susceptible to theft because they are connected to the Internet. It noted that most bitcoin is held in "cold" or offline storage, such as on a Universal Serial Bus (USB) stick or a hard drive, with "deep cold" storage involving additional security, such as a hard drive in a safety deposit box.

John Jason commented on the potential need for mandatory safeguards against cyber-attacks, including in relation to digital wallets; the safeguards could include insurance or third-party testing of an entity's cybersecurity programs. Jeremy Clark supported federal legislation for bitcoin exchanges and the data centres that host their websites, and mentioned that the parties who would be held liable in cases of cyber-theft of digital currencies should be identified in legislation.

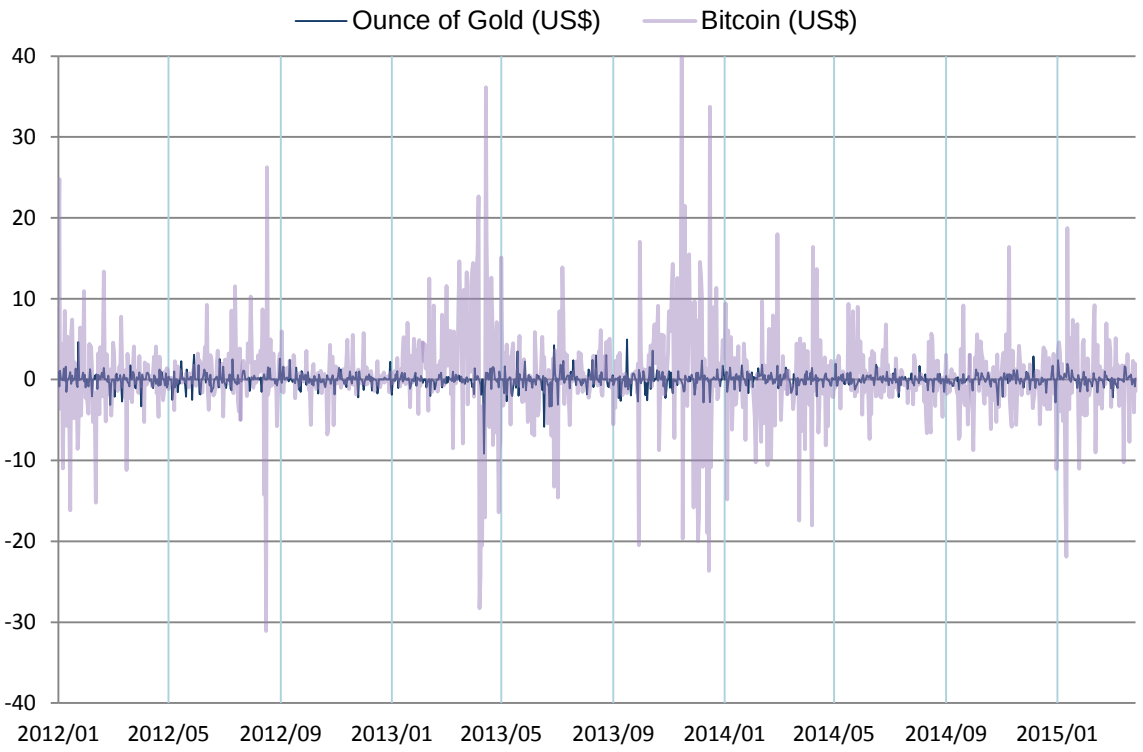
According to Andreas Antonopolous, if a holder of bitcoin gives control of that bitcoin to a "custodian," such as a digital currency exchange, the bitcoin is considered to be outside of the Bitcoin network; as digital currency exchanges are not subject to prudential regulation, there is a risk that bitcoin could be lost due to the bankruptcy of an exchange. In his opinion, when bitcoin is held outside of Bitcoin and authority to access the digital currency has been given to a "custodian," the "custodian" should be subject to regulation, as it would be acting like a bank; however, if the bitcoin holder controls his/her bitcoin, the funds are safeguarded by Bitcoin and regulation is not necessary.

Warren Weber suggested that government-backed insurance may be needed to ensure the stability of Canada's financial system if a particular centralized digital currency begins to be used extensively. In his view, the government may be required to provide financial assistance to Canadians if an entity that issues a widely used digital currency "fails." That said, John Jason noted that the number of people using bitcoin is so low that safeguards, such as deposit insurance, are not warranted.

(ii) Price Volatility

Witnesses discussed a variety of factors that could contribute to volatility in the price of digital currencies, and highlighted the limited supply of bitcoin. For example, the Bank of Canada stated that bitcoin's limited supply contributes to volatility in its price, with price adjustments occurring when supply and demand are not balanced. Andreas Antonopoulos mentioned that – as evidenced by bitcoin – the price of a digital currency is highly volatile when the currency is introduced but, as the number of units in circulation and liquidity rise, volatility declines; he suggested that, as the value of bitcoin in circulation as of 8 October 2014 totalled only $5 billion, the price of bitcoin will remain volatile for many years. Samir Saadi highlighted that bitcoin's price was quite volatile in 2013 and 2014, but is becoming more stable; the volatility is now similar to that of the price of gold. In his opinion, bitcoin was only created in 2009 and people should not be surprised that its price is volatile. John Jason said that, as bitcoin is limited in supply, its price should become more stable as the demand for it rises.

Daily Volatility in the Price of Bitcoin and Gold, 1 April 2012-4 March 2015 (%)



Sources: Figure prepared using information obtained from: World Gold Council, "Gold Price," and CoinDesk, "CoinDesk Bitcoin Price Index," accessed 8 April 2015.

Samir Saadi mentioned that the volatility in bitcoin's price may be the result of such factors as negative media coverage about the illicit activities associated with Bitcoin, the novelty of the technology, trades involving large amounts of bitcoin and "noise trading," which is based on trends and media reports and not on actual data.

TD Bank Financial Group suggested that the prices of decentralized digital currencies fluctuate because these currencies are not usually tied to a state-issued currency.

Bitcoin Foundation Canada commented that China has a major influence on exchange rates between bitcoin and state-issued currencies. It noted that about 70% of the trading volume in bitcoin occurs on Chinese digital currency exchanges, and that volatility in the price of bitcoin and in bitcoin exchange rates is decreasing rapidly.

The Department of Finance and the Canadian Bankers Association suggested that those who hold digital currencies do not have adequate protection against large fluctuations in the price of their digital currency and potential losses in value. MasterCard mentioned that the high volatility in the price of bitcoin may result in consumers and merchants not receiving "fair value" for their bitcoin transactions, as the price of bitcoin may fall before the digital currency is converted to a state-issued currency. That said, Elliot Greenstone indicated that the prices of many state-issued currencies are also highly volatile, which does not appear to impede speculative investment in them. Samir Saadi noted that regulations for digital currencies could lead to greater consumer, investor and business

confidence in these currencies, resulting in increased use of bitcoin and – perhaps – more stability in the digital currency's price.

Regarding other potential effects of the limited supply of bitcoin, BitPay said that – when compared to state-issued currencies – the use of bitcoin may be restricted; as of 12 June 2014, there was 8,000 times more units of state-issued currencies in circulation worldwide than units of bitcoin. According to the Dominion Bitcoin Mining Company, the limited supply of bitcoin is not problematic, as each bitcoin can be divided.

Joshua Gans stated that the limited supply of bitcoin is likely to result in deflation and – potentially – a recession or depression, while the Dominion Bitcoin Mining Company suggested that the deflationary nature of bitcoin could be beneficial.

3. Taxation

Witnesses spoke to the Committee about Canadian taxation of digital currencies when they are received as business or employment income and/or are purchased and sold as an investment, and highlighted some potential taxation challenges.

(i) Taxation as Business or Employment Income

Witnesses discussed the taxation rules that apply when businesses or employees receive digital currencies as income in Canada. According to the Department of Finance, like the U.S. Internal Revenue Service, the Canada Revenue Agency considers digital currencies to be property or a commodity for purposes of taxation; consequently, the taxation rules for barter transactions apply. The Canada Revenue Agency explained that when digital currencies are accepted as a method of payment in exchange for goods or services, they are taxable if earned through a "business." It also indicated that when a business is registered for purposes of the Goods and Services Tax, that tax should be applied on a transaction if a digital currency is the method of payment. The Canada Revenue Agency also said that, because it is treating digital currencies as commodities, no new rules should be required in the *Income Tax Act* to address the use of such currencies when they are earned as income or used as an investment.

For income tax purposes, the Canada Revenue Agency treats digital currencies as a commodity or property, and therefore the taxation rules that are applied to barter transactions are thereby relevant: if digital currencies are accepted as a method of payment, they are taxable if earned through a "business."

According to the Canada Revenue Agency, an employer is required to provide reasonable evidence demonstrating the manner in which bitcoin is valued for purposes of employment income, the Canada Pension Plan and the Employment Insurance program. It also highlighted that fluctuations in the prices of digital currencies make valuations more challenging, but digital currency prices are publicly available. As well, it stated that any profit an employee makes on the sale of bitcoin received from his/her employer is considered to be a capital gain.

The Canada Revenue Agency commented that bitcoin "mining" is currently treated as "the production of inventory" and tax is not paid until the bitcoin is sold; that said, it is examining this policy.

(ii) Taxation as an Investment

The taxation rules that apply when digital currencies are purchased and sold as an investment were mentioned. According to the Canada Revenue Agency, the purchase and sale of digital currencies are treated in the same manner as the purchase and sale of such commodities as copper: 50% of the capital gains resulting from the sale is included as income and, in the case of capital losses, 50% of the losses is deductible against any capital gains. As well, it explained that the capital gains taxation rules apply when bitcoin is considered to be personal property. It also noted that, for taxpayers who are in the business of trading digital currencies, the full value of the transaction is included as income and any losses are deductible against any income earned.

(iii) Potential Taxation Challenges

Witnesses discussed the use of digital currencies to avoid paying taxes, and the potential challenges that arise when digital currencies are treated as a commodity. Joshua Gans said that there is a risk that individuals will use bitcoin to avoid taxation, as some believe that the digital currency cannot be traced to them. Similarly, MasterCard commented that increased use of digital currencies could be a significant challenge for tax authorities. It said that, even if the record of a digital currency transaction is obtained, it could be difficult to identify the parties involved in the transaction and to collect taxes that are owed. As well, the Digital Finance Institute suggested that bitcoin wallets, which are anonymous, could potentially be used for offshore tax evasion. Regarding taxpayers who do not report digital currency income, the Canada Revenue Agency explained that digital currencies can be traced, and that cash transactions are much more difficult to "track."

Bitcoin Foundation Canada mentioned that double taxation of bitcoin could occur if the digital currency is treated as a commodity and thus subject to capital gains taxes, and is then treated as a currency for purposes of the Goods and Services Tax. Andreas Antonopoulos said that taxation of bitcoin should be based on the digital currency's use; it would be subject to capital gains tax if held as an investment and to sales tax when used as a currency. In his opinion, it would be beneficial to clarify tax issues in relation to digital currencies and the rights of those who use digital currencies in commercial arrangements.

The Dominion Bitcoin Mining Company spoke about the appropriateness of making bitcoin subject to capital gains taxation. In its view, it would be relatively easy for an individual to transfer bitcoin to himself/herself anonymously when bitcoin's price falls below the price at which the digital currency was purchased, and then to claim a deduction for the capital loss. It said that, rather than adapting the current taxation system to address digital currency issues, taxation policies that effectively and specifically address bitcoin should be implemented.

4. Access to Information and Protection for Users

Witnesses commented on the amount of information available to, and the nature and extent of protection for, those who use digital currencies.

(i) Access to Information

Witnesses suggested that, perhaps due to a lack of information, users of digital currencies are not well informed about the challenges with these currencies or their associated technologies and businesses. For example, according to the Bank of Canada, consumers may not have sufficient information about a new digital currency or digital currency-related business, especially about the terms and conditions of any contracts, service fees or dispute-settlement procedures that can be used when a contract is violated. It also suggested that users of digital currencies may not be fully aware of potential privacy issues; some business models involve sharing information about digital currency users to earn advertising revenue.

The Bank of Canada identified a need for consumer education, as the media give the impression that bitcoin is a coin. In its opinion, people should know that bitcoin is not a Canadian currency, and that the Canada Deposit Insurance Corporation does not protect bitcoin holdings. Similarly, David Descôteaux said that there is a general lack of public awareness about Bitcoin. The Department of Finance indicated that the Financial Consumer Agency of Canada has provided information about digital currency-related risks, as well as tips about the use and storage of digital currencies.

In commenting on information that Canada's securities regulators have provided about digital currencies, l'Autorité des marchés financiers noted that it has issued a warning about fraud risks and the lack of protection for users of digital currencies under Quebec's financial services compensation fund or its deposit insurance fund. Elliot Greenstone mentioned that the Ontario Securities Commission's initial publication on digital currencies focused on fraud, digital currency exchanges ceasing operations, and the potential connection between digital currencies and money laundering and terrorist financing.

John Jason said that provinces regulate risk through securities laws, such as the requirement to provide a prospectus, and that the government should consider whether digital currencies need to be subject to securities regulation. He suggested that digital currencies should be regulated on the basis of their use – such as an investment or as a currency – and the extent to which, in that use, regulation is required to mitigate any risks. According to Elliot Greenstone, the government has an obligation to provide information about the risks with digital currencies and their technologies, as not everyone has the financial knowledge needed to make informed decisions. He stated that the recent instances of fraud and the Mt. Gox bankruptcy are not representative of all digital currencies and their related businesses.

Although the Department of Finance suggested that Canada's securities regulators could play a role in overseeing digital currencies, l'Autorité des marchés financiers and the Ontario Securities Commission stated that – in their current form – digital currencies do not qualify as "securities" or "derivatives" under their provinces' securities and derivatives legislation and, consequently, are not regulated as such; that said, digital currencies could be packaged as an investment product or a derivative, in which case relevant legislation would apply. L'Autorité des marchés financiers mentioned that a business that markets investments in digital currencies is subject to Quebec's

securities legislation. The Ontario Securities Commission said that any publicly traded digital currency-related business would be subject to the same regulatory requirements as other publicly traded companies, including disclosure to investors about material risks.

(ii) Protection for Users

Witnesses indicated that users of digital currencies and users of traditional banking services do not have the same types of protections. The Royal Bank of Canada suggested that protection when using digital currencies and other types of unregulated payments systems is lacking. The TD Bank Financial Group commented that unregulated digital currencies and payments systems should have consumer protection requirements, as the entities that promote these systems are currently not obliged to disclose the risks with their products, establish procedures to address disputes, or develop processes to enable consumers to monitor their transactions.

According to MasterCard, procedures to resolve unauthorized transactions that occur with digital currencies are inadequate. Visa Canada Corporation said that digital currencies do not provide consumers and merchants with the same types of protection as those with credit cards; the latter offer zero liability for cardholders in the case of unauthorized use of the card and guaranteed payment for merchants.

The Canadian Bankers Association indicated that Canadian banks have not supported any forms of digital currency. It suggested that oversight should be considered for all unregulated payment methods; this oversight would ensure that consumers are properly informed about methods of payment at a merchant or other business, the extent to which payment providers are complying with regulations associated with payments clearing and settlement, and the recourse available if regulatory requirements are not met or there is failure to make the payment in question. It also highlighted the lack of protection if an inadequate number of entities wish to purchase a particular digital currency and illiquidity results.

As well, the Canadian Bankers Association said that there are no advantages to using digital currencies, as financial institutions' digital products provide a better client experience, increased security, a higher level of confidence and clear disclosure of the terms of use. The Royal Bank of Canada stated that Canadians are well served by Canada's current payments system and by the innovations in payments technologies that the country's banks are offering. The Bank of Canada stated that Canadians are well served by the current payments system technologies.

According to the Canadian Payments Association, innovative products and services have enhanced the efficiency of Canada's payments system; however, they have also increased the complexity of – and risks to – that system, and an appropriate level of oversight and regulation must exist. TD Bank Financial Group suggested that there is some systemic risk with unregulated payment method providers, as the standards applied to regulated companies for the protection of Canada's payment system are not applied to these entities.

The Canadian Payments Association explained that not every emerging payment method is subject to oversight in relation to the Canadian payments system. It said that emerging payment methods must be considered in the context of their risks, the ways that these risks can be mitigated, the extent to which these payment methods require access to the clearing and settlement system, and the ability of

regulators to address issues relating to consumer protection and the stability of Canada's payments system.

Regarding regulation of Canada's payments system, the Department of Finance noted that the federal government has broad oversight responsibilities. It mentioned the 2014 federal budget announcement about the development of a comprehensive, risk-based approach to oversight of the Canadian payments system, which will include digital currencies; the Canadian Payments Association supported this announcement. TD Bank Financial Group indicated that Canada's public policy framework for the safety and soundness of the Canadian payments system is operating well because it is based on regulatory oversight of the country's traditional financial institutions. John Jason mentioned that Canada has regulations to ensure the integrity of the payments system, and suggested that some of these safeguards might be applicable to digital currencies.

Bitcoin Foundation Canada commented on Bitcoin, noting that this payments system is largely regulated at present, as consumer protection legislation and the *Civil Code of Quebec* – including provisions regarding implied and legal warranties, as well as disclosure of fees – apply to both digital currency exchanges and consumer contracts where bitcoin is the method of payment.

Similarly, the Bitcoin Alliance of Canada suggested that Bitcoin transactions are currently regulated under consumer protection laws, and that Bitcoin-related businesses will be regulated under anti–money laundering and anti–terrorist financing legislation. In its view, Bitcoin-related regulatory changes may be unnecessary at this time, and Bitcoin should be allowed to find short- and medium-term solutions to consumer-related risks.

Samir Saadi said that regulations for digital currencies should perhaps not be introduced, as the digital currency sector is developing technologies to protect customers against fraud; rather, voluntary standards for best practices, such as for "refundability" of payments, could be less onerous than regulation of digital currency-related businesses. He suggested that, like sellers on eBay, digital currencies and digital currency-related businesses could be rated by their customers. He also indicated that any federal consumer protection legislation in relation to digital currencies should minimize the risk of fraud, and address the ability to reverse transactions and identify the parties involved in a transaction.

The Department of Finance said that it will determine the types of consumer protection measures needed in relation to digital currencies by examining the products and services provided by federally regulated financial institutions.

5. Other Challenges in Using Digital Currencies

In addition to potential criminality, losses, taxation issues, and access to information and protection for users, the Committee's witnesses mentioned other challenges in using digital currencies: the Bitcoin verification process; seignorage revenue for the Bank of Canada and the federal government; and the ability of businesses to access letters of credit for digital currencies.

(i) The Bitcoin Verification Process

Witnesses noted that Bitcoin transactions are not verified immediately. The Department of Finance, BitPay and the Bank of Canada mentioned that the somewhat lengthy verification process for Bitcoin

transactions, which could take an average of 10 minutes, may be a concern for merchants that choose to accept bitcoin directly from customers. In the opinion of Jeremy Clark, these delays are the reason that bitcoin will never replace traditional currencies or become a state-issued currency. According to BitPay, as of 12 June 2014, Bitcoin processed an average of 60 transactions per minute. Visa Canada Corporation said that transactions that occur on Visa's network generally take less than one second to verify and that merchants know instantaneously if the customer has the funds needed to complete the transaction. Ripple Labs highlighted that Ripple's "consensus" verification process takes only a few seconds to complete.

Elliot Greenstone suggested that there is a risk that one entity could acquire 50% of the computing power associated with Bitcoin's blockchain and, thus, potentially control the verification process; for example, if a country acquires 50% of the blockchain's computing power, it could reverse transactions or allow users to "double-spend" their bitcoin.

(ii) Seignorage Revenue

The possibility of lower revenue for the Bank of Canada and the federal government if digital currencies were to replace cash as a means of payment was mentioned. The Bank of Canada highlighted potentially lower revenue for it, and for the federal government, if the demand for digital currencies increases significantly. It explained that the proceeds from issuing banknotes are invested in Government of Canada bonds; the investment generates "seignorage revenue" that is used to pay the Bank's expenses, with the federal government receiving any excess revenue. The Bank said that, in 2013, seignorage revenue was $1.6 billion, and approximately $1.0 billion was remitted to the government. According to the Bank of Canada, a lower demand for cash resulting from increased use of digital currencies would reduce the amount of seignorage revenue available to it and remitted to the government; possibly, the Bank would be unable to finance its expenses, which would impair its ability to fulfil its mandate.

(iii) Access to Letters of Credit

Witnesses discussed the difficulties that some users of digital currencies may face when trying to obtain letters of credit that are based on these currencies. As no central authority exists with decentralized digital currencies and – thereby – letters of credit cannot be given, the Bank of Canada stated that the extent to which digital currencies can be used for business-to-business transactions may be limited.

That said, Andreas Antonopoulos suggested that organizations are going to provide global peer-to-peer lending with digital currencies; this model of lending could provide low-cost credit to individuals in the developing world.

CHAPTER 4: CONCLUSION

In the Committee's view, it is the case that legislators, governments, central banks, private-sector entities in a range of sectors, customers, merchants, investors and others are considering the opportunities and challenges that digital currencies present.

After hearing from a broad range of witnesses in Ottawa, and traveling to New York City for a fact-finding trip, the Committee has concluded that digital currencies and their technologies present a variety of opportunities. In the Committee's view, it is likely that the innovation underlying these currencies and technologies has applications that have not yet been imagined. There is evidence that they reduce transaction costs, increase the choices available to customers and merchants, protect users' identities and record all transactions. A key focus, then, is the actions that the federal government and other entities could take to maximize those opportunities.

Equally, the Committee acknowledges that digital currencies and their technologies present a range of challenges. Money laundering, terrorist financing, losses due to cyber-theft, bankruptcy of digital currency exchanges, price volatility, and a range of taxation issues are serious obstacles for a government whose primary duty is to protect its citizens.

Therefore, the Committee strongly believes that a balanced regulatory approach is needed in the digital currency sector. On one hand, the Committee is mindful that the government has the responsibility to protect consumers and root out illegal activity. On the other hand, it is critical that government action does not stifle innovation in digital currencies and its associated technologies that are in an early and delicate stage of development.

Having completed the study, the Committee is of the opinion that the opportunities presented by digital currencies, technologies and businesses outweigh the challenges. The Committee is confident that the implementation of our recommendations will have positive outcomes for consumers, merchants, digital currency-related businesses, Canada's financial services sector and others. The Committee looks forward to timely government action designed to maximize the opportunities and manage the challenges facing the digital currency sector.

APPENDIX A: WITNESSES

March 26, 2014	Department of Finance Canada	Rachel Grasham, Chief, Financial Crimes - Domestic, Financial Sector Division
March 26, 2014	Department of Finance Canada	David Karp, Economist, Financial Crimes - Domestic, Financial Sector Division
March 26, 2014	Department of Finance Canada	David Murchison, Director, Financial Sector Division
March 27, 2014	As an Individual	Joshua S. Gans, Professor and Area Coordinator of Strategic Management at Rotman School of Management, University of Toronto
March 27, 2014	As an Individual	Warren E. Weber, Economist
April 2, 2014	Bank of Canada	Grahame Johnson, Chief, Funds Management and Banking
April 2, 2014	Bank of Canada	Lukasz Pomorski, Assistant Director, Funds Management and Banking
April 3, 2014	As an Individual	Jeremy Clark, Assistant Professor, Concordia Institute for Information Systems Engineering, Concordia University
April 3, 2014	As an Individual	David Descôteaux, Associate Researcher, Montreal Economic Institute
April 9, 2014	Bit Access	Haseeb Awan, Co-founder
April 9, 2014	Canadian Virtual Exchange (CAVirtEx)	Joseph David, Chief Executive Officer
April 9, 2014	Bitcoin Strategy Group	Kyle Kemper, Partner
April 9, 2014	Canadian Virtual Exchange (CAVirtEx)	Larry O'Brien, Advisor
April 9, 2014	Bitcoin Strategy Group	Victoria van Eyk, Partner
April 10, 2014	Royal Bank of Canada	Jeremy Bornstein, Head, Emerging Payments
April 10, 2014	Royal Bank of Canada	Carolyn Burke, Vice-President, International Cards and Canadian Regulatory Payments
April 10, 2014	Canadian Bankers Association	Darren Hannah, Acting Vice-President, Policy and Operations
April 10, 2014	Canadian Payments Association	Doug Kreviazuk, Vice-President, Policy and Public Affairs
April 10, 2014	Canadian Payments Association	Carol Ann Northcott, Vice-President and Chief Risk Officer
June 5, 2014	Canada Revenue Agency	Michael Cooke, Manager, Income Tax Rulings Directorate

June 5, 2014	Canada Revenue Agency	Eliza Erskine, Director, Income Tax Rulings Directorate
June 12, 2014	BitPay	Tim Byun, Chief Compliance Officer
June 12, 2014	Interac Association	Caroline Hubberstey, Head, External Affairs, Enterprise Strategy
June 12, 2014	PayPal	Barry Murphy, Director, Government Relations, Canada and Latin America
October 1, 2014	Visa Canada Corporation	Derek Colfer, Head of Technology and Innovation
October 1, 2014	MasterCard	Jason Davies, Head of Emerging Payments, Canada
October 1, 2014	MasterCard	Sherri Haymond, Senior Vice President, Digital Channel Engagement, Emerging Payments
October 2, 2014	Bitcoin Foundation Canada	Guillaume Babin-Tremblay, Treasurer
October 2, 2014	Bitcoin Foundation Canada	Jillian Friedman, Legal Officer
October 2, 2014	Bitcoin Alliance of Canada	Stuart Hoegner, General Counsel
October 2, 2014	Bitcoin Alliance of Canada	Michael Perklin, Director
October 2, 2014	Bitcoin Embassy	Francis Pouliot, Director of Public Affairs
October 8, 2014	As an Individual	Andreas M. Antonopoulos, Author of *Mastering Bitcoin*
December 10, 2014	Dominion Bitcoin Mining Company	Jason Dearborn, Chair
December 10, 2014	Digital Finance Institute	Christine Duhaime, Co-founder and Executive Director
December 10, 2014	Digital Finance Institute	Manie Eagar, Co-founder and Chairman
January 28, 2015	Royal Canadian Mounted Police	Jean Cormier, Superintendent, Director, Federal Coordination Centres
January 28, 2015	Royal Canadian Mounted Police	Drew Kyle, Sergeant, Acting Officer in Charge, Financial Crime, Federal Policing Criminal Operations

January 28, 2015	Canadian Security Intelligence Service	Michael Peirce, Assistant Director, Intelligence
February 19, 2015	Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)	Bernard Gagné, Deputy Chief Compliance Officer, Compliance Relations and Support
February 19, 2015	Department of Finance Canada	Lisa Pezzack, Director, Financial Sector, Financial Sector Policy Branch
February 19, 2015	Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)	Martin Tabi, Manager, Research and Strategic Intelligence and International Relationships
February 19, 2015	Department of Finance Canada	Ian Wright, Chief, Financial Crimes - Domestic, Financial Sector Policy Branch
February 26, 2015	As an Individual	Elliot A. Greenstone, Lawyer, Davies Ward Phillips & Vineberg LLP
February 26, 2015	As an Individual	John Jason, Of Counsel, Norton Rose Fulbright Canada
February 26, 2015	Ripple Labs	Greg Kidd, Chief Risk Officer
March 11, 2015	TD Bank Financial Group	Paul Milkman, Senior Vice President and Head, Technology Risk Management and Information Security
March 12, 2015	Autorité des marchés financiers	Christian Desjardins, Manager, Market Surveillance, Enforcement Branch
March 12, 2015	Autorité des marchés financiers	Moad Fahmi, Financial Markets Specialist, Specialized Investigation Support Unit, Enforcement Branch
March 12, 2015	Autorité des marchés financiers	Jean-François Fortin, Executive Director, Enforcement Branch
March 12, 2015	Ontario Securities Commission	Paul Redman, Principal Economist, Strategy and Operations
March 12, 2015	Ontario Securities Commission	James Sinclair, General Counsel, General Counsel's Office
March 25, 2015	Bill & Melinda Gates Foundation	Rodger Voorhies, Director, Global Development, Financial Services for the Poor
March 26, 2015	MoneyGram International	Derek McMillan, Senior Director, Regional Compliance
March 26, 2015	As an Individual	Samir Saadi, Assistant Professor, Telfer School of Management, University of Ottawa

APPENDIX B: FACT-FINDING MISSION IN NEW YORK – FEBRUARY 2-4, 2015

February 2, 2015	Consulate General of Canada in New York	John F. Prato, Consul General
	As an Individual	Jeffrey Robinson, Financial Crime Journalist
	Circle Internet Financial Ltd.	John A. Beccia, General Counsel and Chief Compliance Officer
February 3, 2015	U.S. Department of the Treasury and the Financial Crimes Enforcement Network (FinCEN)	Sarah Runge, Director, Office of Strategic Policy for Terrorist Financing and Financial Crimes, U.S. Department of the Treasury
		Scott Rembrandt, Assistant Director, Office of Strategic Policy for Terrorist Financing and Financial Crimes, U.S. Department of the Treasury
		Jamal El-Hindi, Associate Director, Regulatory Policy and Programs Division, FinCEN
	U.S. Department of Homeland Security	Tate Jarrow, Special Agent, U.S. Secret Service
	Federal Reserve Bank of New York	Rodney Garratt, Vice President, Money and Payments Studies Function
		Vanessa Kagenian, Supervisory Associate
		Alex Entz, Policy and Markets Senior Analyst
		David A. Duttenhofer, Jr., Senior Vice President, Legal & Compliance Risk Function, Financial Institution Supervision Group
	New York State Department of Financial Services	Maria Filipakis, Executive Deputy Superintendent
		Dana Syracuse, Assistant General Counsel
		Colleen O'Brien, Senior Counsel
		Alexander Sand, Counsel
		Tom Eckmier, Snior Attorney

	New York Police Department	Lieutenant Kevin Yorke, Lieutenant Detective Commander Intelligence Division – Cyber intelligence & Analytical Programs
	Financial Crimes Enforcement Network (FinCEN)	Gary Novis, Director, Office of Strategic Policy
		Horacio Madinaveitia, Senior Regulatory Policy Officer
		Kevin Bleckley, Section Chief, Illicit Finance Methodologies
	U.S. Department of the Treasury (IRS)	Anne Wallmork, Senior Counselor, Strategic Policy, Office of Strategic Policy for Terrorist Financing and Financial Crimes
	Perkins Coie	Keith W. Miller, Partner and Firm-wide Chair
	As Individuals	Cameron Winklevoss Tyler Winklevoss
February 4, 2015	U.S. Internal Revenue Service	Gary L. Alford, Special Agent, Criminal Investigation, U.S. Internal Revenue Service
	Coin Comply	Brian Stoeckert, Managing Director and Chief Strategy Officer
	Bitcoin Centre NYC	Nick Spanos, CEO and Founder

APPENDIX C: GLOSSARY OF DIGITAL CURRENCY-RELATED TERMS

Bitcoin Blockchain (or Public Ledger): The public registry for all Bitcoin transactions, which are successively added in blocks once they have been validated through the mining process.

Centralized Digital Currency: A digital currency that has a single central authority that manages the supply, creates the rules for exchange and use, verifies transactions and maintains a central ledger of transactions.

Convertible Digital Currency: A digital currency that can be converted to a state-issued currency, and vice versa.

Cryptocurrency: A decentralized digital currency that is convertible and functions as both a currency and a decentralized payments system. Transactions are recorded on a public ledger, which is shared across a peer-to-peer network, and the validity of transactions is verified through cryptographic techniques. Bitcoin is an example.

Decentralized Digital Currency: A digital currency that is open-source, lacks a central authority and operates over an Internet-based peer-to-peer network; transactions using that currency are validated through that network.

Digital Currency: Electronic forms of exchange and their associated technologies that operate on the Internet and/or on mobile devices, and that are not issued or controlled by a government or central bank.

Digital Currency Exchange: A business that allows customers to convert fiat currency to digital currency and digital currencies to fiat currency or other digital currencies.

Mining: The process through which “miners” on the Bitcoin network compete to solve a “random hash algorithm” to validate and add a block of transactions to the public ledger, and for which they receive bitcoin as compensation.

Money Services Business: As defined by the Financial Transactions and Reports Analysis Centre of Canada, any Canadian business that offers foreign exchange dealing or money transferring services, or that cash or sell money orders, traveller's cheques or similar monetary instruments.

Non-Convertible Digital Currency: A digital currency that can only be used in relation to a particular retailer or virtual marketplace to purchase real or virtual goods and services; it cannot be converted to state-issued currency.

State-Issued Currency: A currency that is designated by a country as its legal tender, and that is customarily used and accepted as a medium of exchange in the issuing country.