Bitcoin Regulation

***Andreas Antonopoulos**, Canadian Committee on Banking, Trade and Commerce, October 8th 2014*

Today I welcome the opportunity to talk to you about bitcoin security, the decentralized architecture that underpins bitcoin's security, and the implications that architecture has for privacy, individual empowerment, innovation and regulation.

Until the invention of bitcoin in 2008, security and decentralization seemed like contrary concepts. Traditional models for financial payment networks and banking rely on centralized control in order to provide security. The architecture of a traditional financial network is built around a central authority, such as a clearing house. As a result security and authority have to be vested in that central actor. The resulting security model looks like a series of concentric circles, with very limited access to the centre and increasing access as we move further away from the centre. However, even the outer most circles cannot afford open access. In such a security model, the system is carefully protected by controlling access and ensuring that only vetted individuals and organizations can connect to it.

The entities near the centre of a traditional financial network are vested with enormous power, act with full authority, and therefore must be carefully investigated, regulated and subject to oversight. Centralized financial networks can never be fully open to innovation because their security depends on access control. Incumbents in such networks effectively utilize access control to stifle innovation and competition, presenting it as consumer protection.

Centralized financial networks are fragile and require multiple layers of oversight and regulation to ensure that the central actors do not abuse their authority and power for their own profit. Unfortunately, the centralized architecture of traditional financial systems concentrate power, creating cozy relationships between industry insiders and regulators and often lead to regulatory capture, lax oversight, corruption, and, in the end, financial crises. Bitcoin and other digital currencies based on the block chain architecture are fundamentally different.

The security model of block chain currencies is decentralized. There is no centre to the network, no central authority, no concentration of power and no actor in whom complete trust must be vested. Instead, the core security functions are put in the hands of the end users of the system. In this architecture, security is an emergent property of the collaboration of thousands of participants in the network and not the function of a single authority.

In addition to the differences in architecture, there are also fundamental differences in the nature of the payments themselves. Digital currencies, like bitcoin, are much more like cash

than bank accounts or credit cards. The transfer of value in bitcoin is a "push" mechanism, not a "pull" mechanism as is the case with credit cards, debit cards and most other digital payments. A bitcoin payment is not an authorization to pull from your account. Instead, it pushes the precise payment amount itself as a value token directly to the named recipient. A single transaction does not authorize any future transaction or expose the user's identity. The transaction itself is unforgeable and not exchangeable. As a result, bitcoin payments can be transmitted in the clear without encryption, over any network, and can be stored on unsecured systems without fear of compromise.

Bitcoin's unique architecture and payments mechanism has important implications for network access, innovation, privacy, individual empowerment, consumer protection and regulation. If a bad actor has access to the bitcoin network, they have no power over the network itself and do not compromise trust in the network. This means that the bitcoin network can be open to any participant without vetting, without authentication or identification, and without prior authorization. Not only can the network be open to anyone, but it can also be open to any software application -- again, without prior vetting or authorization. The ability to innovate without permission at the edge of the bitcoin network is the same fundamental force that has driven Internet innovation for 20 years at a frenetic pace, creating enormous value for consumers, economic growth opportunities and jobs.

Bitcoin's decentralized nature affords consumer protection in the most powerful and direct way, namely by allowing bitcoin users direct control over the privacy of their financial transactions. Bitcoin does not force users to surrender their identity with every transaction and put their trust in a chain of supposedly vetted intermediaries who must be trusted to control access to, securely store, and protect transaction data and vulnerable account identifiers. Bitcoin transactions never expose vulnerable account identifiers and bitcoin users can protect the privacy of their transactions without relying on or trusting any intermediaries. Because in bitcoin trust is not vested in central actors, there is no need for centralized regulation and oversight. When properly architected, bitcoin financial services are not vulnerable to central pointing of failure which would necessitate heavy handed oversight and regulation. Instead, the power lies with the end user whose interests are most aligned with the protection of their own funds. While individual bitcoin wallets can be targeted and compromised if not properly secured, the bitcoin network does not suffer from centralized systemic risks.

Contrary to popular misconception, bitcoin is not unregulated. Rather, several aspects of the bitcoin network and financial system are regulated by mathematical algorithm. The algorithmic regulation in bitcoin offers user predictable, objective, measurable outcomes such as a predictable rate of currency issuance. These outcomes are not subject to the whims of

centralized institutions or committees, which are both corruptible and often placed outside of democratic oversight. A bitcoin user can predict the monetary supply 30 years from now instead of hanging on the nuanced intonation of a single adjective by some high official of central banking who can dramatically change an entire country's monetary velocity a week hence.

Bitcoin's decentralized architecture does not easily conform to the expectations and experiences of consumers or regulators because there has never been a large-scale, secure decentralized network before. The combination of decentralization and security is the novelty at the heart of bitcoin. In trying to understand consumer protection, oversight, audits and regulation of bitcoin, there is a risk that many will try to apply familiar models of the past in to this new digital currency system. These models are all centralized and designed to provide regulation and oversight of centralized financial networks. Centralized solutions will be easier to understand and seem familiar. However, they are both inefficient and unsuitable for this new form of decentralized financial network.

I urge you to resist the temptation to apply centralized solutions to this decentralized network. Centralizing bitcoin will weaken its security, dull its innovative potential, remove its most disruptive yet also most promising features, and disempower its users while empowering incumbents. Consumer protection will not be achieved by removing bitcoin's built-in privacy characteristics. Demanding user identifiers and adding access control mechanisms on top of the bitcoin network and then trusting those identifiers to a chain of intermediaries will only replicate the failures of past by introducing single points of failure into a network that has none. We cannot protect consumers by removing their ability to control their own privacy and then asking them to entrust it in the same intermediaries who have failed them so many times before. Most failures in bitcoin security are the result of misguided attempts at centralization and removing control from the users. In the new decentralized financial network, we have the opportunity to invent new decentralized security mechanisms based upon innovations such as multi-signature escrow, smart contracts, hardware wallets, decentralized audit and algorithm mechanic proof of reserves. These are the new decentralized regulatory and security tools that are most appropriate for a decentralized digital currency.

Thank you for the opportunity to address this committee.

The Chair: Thank you, **AA**, for your opening remarks. They have clearly resonated and stimulated a number of questions.

Before I turn it over to senators for questions, I just might make an observation. In your remarks, you have told the committee that the decentralized security model of block chain

currencies is indeed secure, and the bitcoin financial services are not vulnerable to central pointing of failure, which would necessary date oversight and regulation.
As a result, as I hear you, you've come to the conclusion that this currency should be left "hands-off" by the government and other regulatory bodies. I quote, "centralizing bitcoin will weaken its security."
While listening closely to your comments I couldn't help but observe that you make absolutely no mention of illegal activity supporting a crypto-currency like bitcoin. I was surprised that you make no mention of money laundering, terrorist financing or other possible misuses because of the anonymous and open nature of bitcoin.
I think you stated in your presentation that the bitcoin network can be open to any participant without vetting, without authentication or identification, and without prior authorization.
I suspect that the misuse or potential misuse of bitcoin for nefarious purposes is very much a concern to Canadians as well as to this committee. Would you have any comments on that? Perhaps it may want to be picked up by some of the senators in their questions as well.
AA: Absolutely. I believe that there is a great misconception in the idea that bitcoin use is anonymous or that the network itself is anonymous. On the contrary, the central public ledger allows any participant to observe all transactions that occur on the network. Those transactions are not always tied to a specific identity, but with the use of traditional law enforcement mechanisms, when an identity is attached to a specific transaction that transaction can be followed throughout the network, and therefore the network does not afford more anonymity.
In fact, it is easier to implement strong transparency and accountability features on the network than it is to achieve strong anonymity on the bitcoin network.
Furthermore, I think bitcoin is not a very convenient network for such uses. The vast majority of such activities really occur with cash, in fact with the U.S. dollar. I don't see bitcoin as the primary vehicle for illicit activities of that type. I see the tremendous potential for the use of bitcoin among the more than 6 billion people in the world who have very limited access to international currencies, international credit markets and international trade. I think that use far outweighs the tiny minority that might put some currencies to illicit use.
The Chair: Thank you for those comments. With that, I'm going to start with my list.
Senator Massicotte: I think Senator Tkachuk has the same question. Try to explain how it all works. Can we try that?
The Chair: When it's his turn, we will turn it over to him.
Senator Black: Thank you very much, **AA**, for being here. I'm finding very real interest in what you have to say.

Let me outline first of all what I'm hoping to come to understand from you. I'm interested in coming to learn what is needed to ensure that this innovation can continue to develop. That's my premise, right or wrong. Building on the chairman's initial comments, I have a question or two for you.

When CAVirtex testified before this committee they stated they would like to see bitcoin regulations put in place as soon as possible to give clarity on how bitcoin is classified. They believe, and they told this committee, that this would allow bitcoin to thrive in Canada. In your remarks you've stated that bitcoin should not be regulated centrally because it will stifle innovation. Considering that other groups have echoed the statements of CAVirtex, help me with the disconnect that I'm hearing between the evidence of CAVirtex and what you have said today.

AA: Absolutely. I believe that the best way to help bitcoin is to ensure that there is clarity in the treatment of bitcoin and that bitcoin is not essentially forced into contorting itself into regulatory structures that are designed by banks for banks or with traditional models of finance in mind, which are primarily centralized, and recognizing bitcoin as programmable money with capabilities such as digital multi-signature escrow and has many more flexible ways of responding to the needs for consumer protection.

For example, in the traditional banking environment, unless you hold cash every account that you have as a consumer is a custodial account. That means that the account funds are held in trust by a bank and what you have in return is essentially a promise note that that money will still be there tomorrow morning. The bank controls the funds entirely.

Bitcoin allows a much more varied range of control between a consumer and the financial services institution that they may use, from completely decentralized control, where the consumer or end user is the only one with full control over the money, to complete custodial accounts where a financial services institution has full access to the keys and the consumer has none.

In between, there are also models that are hybrid where the bank may have a signatory role but not be able to change the direction of the funds, simply to approve transactions. Within this very broad range of possibilities obviously some aspects of that need to be regulated. What I mean by that is if you simulate a traditional financial environment with a custodial account where you take full control over users' funds, then those funds are now outside of the bitcoin security model. They are no longer protected by the user's control of the keys. They're no longer protected by the block chain. They are now in a grey area where they're not covered by regulatory requirements for capital adequacy audits, security requirements and control, et cetera, but they're also not covered by a bitcoin security model.

We've seen that whenever that has happened it results in disaster. Almost all of the exchanges that have been attacked in bitcoin had a full custodial model like that. However, that is not the only model that exists. There are digital bitcoin wallets where the user has complete control. There are wallets where the user has complete control, but transactions cannot happen unless an additional signature is placed by an institution that acts essentially as a risk manager to ensure that even if the user's systems are compromised the money can't be stolen: a hybrid model.

If you lump all of those together under a single, unifying regulation, assuming it's all just like a bank, then you miss out on opportunities to create better solutions for this new programmable money.

I believe that certain models of bitcoin use must be regulated. If control over the user's funds has been centralized, then that institution puts consumers at risk. But to lump a decentralized model where a user still has full control over their funds and an institution can't steal their money under that same regulation is not only misguided but doesn't leave any room for that technology to develop further.

Senator Black: Thank you very much for that. So what would you suggest to this committee in terms of regulation, if any?

AA: I believe we're still at the very early stages of this technology. Not only is bitcoin new, but bitcoin is already evolving.

For example, the capability to do multi-signature transactions, where there can be up to 20 different signatories on a single transaction and a transaction can be controlled by any mixture of signatures, that technology was introduced in 2012, four years after the introduction of bitcoin. It came into full fruition or full availability in 2013. So already bitcoin is developing new and exciting programmable capabilities for user security.

I think this technology needs time to breathe. It needs time to show the full potential of what is possible with decentralized, programmable money. Until that time, I think opening up those possibilities by making clear distinctions, where the technology allows it, between centralized and decentralized modes of operation, for example, understanding those nuances, can create niches where new players can come into the financial services market and introduce innovation, competition and, quite honestly, disruption into the banking industry by trying out new models for consumer protection. They are, in my opinion, superior to the ones we have today.

Senator Black: So your answer is what, in terms of what this committee should do, if anything?

AA: Wait until the technology is better understood by all of us. Also, understand that there are nuances in this technology that require very careful treatment, because a blanket

treatment as if this is just a currency, which it is not -- it is a network for money -- as if there is only one application of the bitcoin currency, which it is not -- there are many applications based on this model -- would stifle this technology in its early days.

Senator Campbell: Thank you so much for coming today.

I remember when I got an IBM Selectric that had the x-backspace so I could correct letters, and I thought, "Nothing will ever be cooler than this; it's impossible." I'm 67. That's my generation.

You say it needs some breathing space. Would it be fair to say that the younger generation gets this more so than my generation?

AA: That's the case with any new technology.

Senator Campbell: Do you think it's fair to say, for instance -- I would doubt very much that I will get into bitcoin. I don't really understand it even still, and we're on our 11th meeting. Senator Massicotte does.

But when I talk to younger people about this committee, they totally get it. They don't have any questions at all. They are like, "This is where we're going, and this is how we're going to get there." I've been told to keep my old nose out of it. I think you explained it: How much time does it take to breathe for this? How long do you think that would be? How rapidly will this come upon us?

AA: I would estimate that bitcoin today is approximately in the same position that the Internet was in 1992. In 1992, email required command line UNIX skills typed into a mainframe, and it was very difficult. Approximately 10 years after that, it had already reached mainstream adoption among especially younger people. Almost exactly 20 years after that, my mother got her first iPad and was able to send her first email.

It took a while before the technology went from something extremely esoteric that was only the purview of someone working in a computer-science department until my mother could do it with a swipe of her finger, and she's a self-acknowledged technophobe.

So it may take some time. But I can tell you for sure that this one will be about three times faster, and that's because we're not deploying physical infrastructure and we already have the Internet as a medium on which we can spread this technology.

I believe that within eight years we will see mainstream applications that will be much easier to use and secure that will allow consumers to use bitcoin in a way that feels very comfortable. At the moment, we are not there.

Senator Campbell: Okay. One more question.

The question I have is that if you don't need any centralized oversight, who provides -- you say, "Well, the front-end user and the end user control the whole thing." If there is nobody

finding out who is the front-end user, how can we be so sure that we won't see ISIS or one of those other whack-job crews use this as a method of transferring money around the world?
AA: I firmly believe that the possibility for positive use of this technology far outweighs the very small possibility for negative use of this technology. The truth is that ISIS is probably using pallets of money they stole from allies during their reign of terror and not bitcoin.
It's really a matter of understanding that to limit a technology that has the possibility of bringing economic inclusion to billions of people who do not have it today -- in the same way that cell phone technology allowed entire nations to leapfrog the landline and land in a technology realm and achieve communications that would be unthinkable -- bitcoin can do the same for banking and finance. It can empower billions of people around the world in areas such as remittances, international finance and credit, accessing liquidity and loans, and things like that.
As with any technology, this technology will reflect society, and there will be a tiny minority that will try to use it for evil. But I have full faith that law enforcement capabilities properly exercised can follow funds on bitcoin just as they can in the normal financial networks -- probably more so than they can in traditional financial networks.
Furthermore, I think bitcoin is the most open and transparent of crypto-currencies. There are already 500 others, and I believe that if bitcoin is not given the opportunity to work in a way that empowers people, eventually criminals will move to far stealthier and far less open currencies and use those instead.
Senator Campbell: Thank you for coming today. I appreciate it very much.
Senator Greene: Thank you very much for coming. This is without question the most interesting topic we've looked at since I've been a member of the committee. I'm just amazed.
Last night as I was reading your paper, the idea that occurred to me -- and I want you to comment on it -- is that bitcoin and related currencies are not hackable, because there is nothing to hack; is that a true statement? If it is, could you explain that in very simple terms, because I imagine there are a lot of people watching this.
AA: Individual bitcoin wallets -- my wallet -- can be hacked, and we see examples of that. The system as a whole cannot be hacked. I say that with confidence because, over the last five years, especially recently in the last year and a half with value transferred over that network exceeding $5 billion U.S. dollars, there has been no shortage of people trying to hack bitcoin. If anything, we have seen that bitcoin has changed the very dynamics of cybercrime and hacking; it has escalated the attacks and created a target for hackers that is extremely fluid that resides on people's computers, and they have tried to take advantage of that.

I know that bitcoin can't be hacked simply because many people have been trying nonstop for the past five years and can't hack it.
So there is a big difference between the system as a whole, which is a dynamic system that responds to hacking attacks, and individual wallets.
I think you see a very similar development timeline as with the Internet. I remember a time when groups of hackers could take down Yahoo for a day, as well as Microsoft and Google, and they don't do that anymore, and it's not because they stopped trying. It's because a dynamic system that is constantly exposed to threatening stimuli will develop resistance and will become more resistant to these types of attacks. That's a concept often called "anti-fragile;" it becomes dynamically stable and resistant to attack.
Bitcoin is not static; it continuously evolves and continuously deals with attacks better and better over time.
Senator Greene: You mentioned in answer to the previous questioner that there are roughly 500 other crypto-currencies. What is the size of bitcoin in relation to those? Are they major competitors or are they copycats?
AA: I would say they are copycats, for the most part. My personal opinion is that the allocation of crypto-currencies in terms of market size, adoption, users, et cetera, follows a long-tail or power-law curve, where the vast majority is concentrated in maybe a handful of currencies and then you have a tail that stretches out to encompass thousands of smaller currencies.
The dynamic of being able to create currencies at whim creates an environment where there will be thousands -- possibly tens of thousands -- of currencies in the future. Only a handful will have economic viability and market value, but that does not change the nature of it. In my opinion, people will create currencies the way they create Internet means. In many cases, they will be Internet means. We have seen that happen in currencies.
What is happening here is a laboratory of evolution and innovation, where new ideas are tested and some of the best results of that are often catastrophic failure on a small scale that informs future designs for bitcoin.
Senator Greene: It's amazing.
Do you foresee a time when, in the interests of economic development, or what have you, a nation state decides to forego its own currency and adopts bitcoin?
AA: That's a difficult question because I think the very nature of currency is changing. I think the economy, if you like, or organization that is adopting the currency is the Internet and that's a transnational entity. I think that has even more important implications for the future than national currencies. Bitcoin is already bigger than some national currencies and in

the future may end up being more important for economic activity than dozens of smaller international currencies.
I do foresee that in the future national central banks may utilize block chain technology to underpin national digital currency.
Senator Greene: Thank you.
Senator Massicotte: Thank you for being with us. It's very interesting and very useful. Let me follow up on the question from our chair.
Your presentation makes a reference that you discourage us from even recommending some form of identification. Your argument is that it's always visible. You are right; the chain is visible. However, what you do not see in the chain is who is behind the chain. That is why, I presume, people of illegal objectives and means are prepared to use it, as they are apparently using this mechanism to transfer money and launder money.
I gather your argument is I recognize that that is a negative, but please don't hesitate with that issue; don't put measures in place to restrict that flow because the usefulness of those measures to identify who is behind the transfers is lesser than the use to our society for letting this thing develop. Is that accurate? That is, the chain is visible, but not the identity of the person, which is what the chairman was asking.
AA: I am recognizing two aspects. One that attempts to impose identity on bitcoin will, in my opinion, be ineffective because there will always be channels upon which non-identifiable transactions can be introduced, either in bitcoin or in other currencies, while simultaneously removing one of the main advantages.
Senator, today I received three automated phone calls from Visa fraud prevention because I have used my card in Canada. They have been calling me all day. This is something that happens to me every time I travel. It's a symptom of the fact that, by releasing an identifier that allows others to pull from my account and that ties every transaction I do to every activity I do, I'm not only giving up my privacy but also endangering my personal security every time I use a credit card. This system is nonviable. I watch every few weeks on the news that yet another group has had 50 million consumer credit cards and identities lost. For the average consumer, that means months of identity protection and risk. These are the intermediaries who handle our identities. Over the last two decades we have seen that protecting information security systems in such a way that we can prevent these types of thefts is not possible. The mistake is tying identity to every transaction and creating systems that can continuously draw from our accounts. Bitcoin is fundamentally different. To break that in order to tie an identity that anyone can easily bypass if they have ill intent would not result in protecting us more but it would result in harming consumers.

Senator Massicotte: The conclusion is that while you acknowledge that this form of system could encourage money laundering, you are also arguing please don't do anything about it because the benefits to society from this form of transfer are more important. Is that your argument in principle? I gather that is what you are saying.

AA: My argument is that the invention of block chain technologies allows any of these systems to be used for ill intent without identity and nothing can be done to stop someone from abusing it.

Senator Massicotte: Or even try to stop it.

AA: I think that would harm the vast majority of people who do well with it.

Senator Massicotte: We are older than you are. I look at central banks because we are a Banking Committee, and they come across with new theories every 20 or 30 years about money supply, or money growth, or controlling inflation or controlling currency. We always learn 30 or 40 years later -- sorry; we got it wrong. Shit happens, in other words.

I look at your algorithm. You say, "We are going to predict the necessary growth of this currency" -- it's a form of transfer – "and we have it right." However, I highly suspect 20 or 30 years from now we will say that you did not get it right. When you predict the future, what are the one or two things you can get wrong? That is, where are the two weaknesses where you say, "I could have gotten it wrong and here is where I may have gotten it wrong?"

AA: It is useful to understand that bitcoin's monetary policy is just one recipe that is possible. Bitcoin and other currencies allow us to implement monetary recipes at will and then fix them in place for each currency. If bitcoin's monetary recipe is wrong, people will move to another currency that has the same characteristics of decentralized organization, but with a different monetary recipe. It is simply one of the possible choices.

I don't know if it is right or wrong, but I do know what it will be in 30 years exactly for bitcoin. I can tell you to the millionth decimal point exactly how many currency units will exist 140 years from now in bitcoin. What it provides, whether or not you like the recipe and whether or not you agree with it, is certainty and predictability, and it allows people to adjust their expectations for that. Whether that's the right monetary policy or not, with this new model you can build your own currency which has a different monetary policy. If it is better, it gets to win. It's an open competition.

Senator Massicotte: The supply is defined, given the algorithm formula. People like our chairman have bought this unit, so maybe the supply is limited. Will it be equal to the demand growth? Who knows?

AA: Nobody knows.

Senator Massicotte: Therefore, the price of that currency may fluctuate immensely if you have it wrong because obviously the purpose of the algorithm is to project that future growth

as reasonably as they can. Maybe the supply is defined but not the price. If you have high fluctuation of value, that will discourage its use.

AA: Absolutely. At the moment, I think volatility is a reflection of low liquidity in bitcoin. Bitcoin has a very specific recipe, namely to simulate the supply curve of a precious metal like gold. That is a specific monetary theory.

If there is a different monetary theory, you can build a different currency using block chain technology. You can even build a block chain technology currency where monetary supply is defined by a committee of 12 central bankers and then invite users to adopt that. It would still be more transparent than our current system of money.

Senator Wells: I am pleased to be here today filling in for someone. We ran into each other earlier today, chair, and you said it was going to be an exciting committee meeting, and it is. **AA**, thank you for coming here and thank you for your answers so far.

Who are bitcoin's biggest detractors and why are they enemies of bitcoin?

AA: I'm not sure who bitcoin's biggest detractors are. I can tell you that I, along with every other passionate advocate that I know, started off as a detractor. My initial response to first identifying bitcoin was this is nerd money; it can't possibly work. In fact, when Satoshi Nakamoto invented bitcoin and announced it on the crypto mailing list, everyone around him responded in pretty much the same way.

The circle of advocates, which is now numbering in the millions, consists entirely of people who started out as very strong skeptics. The difference is the first time I saw it that was my reaction. The second time I read the paper and understood this was not a currency, it was a decentralized network model for financial security and trust, which allows currency but also allows many other things. That literally blew my mind. Then I understood this was much bigger. We all started out as skeptics.

I don't know if all skeptics become advocates over time, but I see that most people who look at bitcoin carefully very quickly understand that there's a lot more than meets the eye to this.

Senator Wells: What would be bitcoin's biggest threat to growth? Would it be having people overcome fear of their unknowns? Would it be the security aspect, the level of technology available or the individual nodes that might not have the security that the whole system has?

AA: There are some significant security problems related to the ownership and control of bitcoin keys and bitcoin wallets for the end user.

The simple truth is we've been doing information security for a handful of decades. As an industry, that industry is not effective at doing it, whether that's trying to protect credit numbers or bitcoin for the end user. The nice thing about bitcoin is that risk is compartmentalized so there is no systemic risk.

Over time I think we're going to see the development of more secure mechanisms like hardware wallets, such as the ones beginning to appear in the market today. For every problem I see in bitcoin, as an entrepreneur I simultaneously see a tremendous opportunity. If you go back and look at the history of disruptive technologies like this, in 1994 there were dozens and dozens of articles about how the Internet would fail because no one would ever be able to find anything on the Internet. Sergey Brin and Larry Page decided that was an opportunity, not a problem. With bitcoin, each one of these problems also is possibly a very innovative new financial industry that can offer solutions.

Senator Wells: Of the millions of users of bitcoin currently, who would constitute the biggest user group? Are they international financial transactions? Who is the biggest user now, the one with the highest plurality?

AA: Honestly, I think there are a few statistical surveys that provide insight into that. I'm not sure about the exact numbers. The most common use for bitcoin is charitable giving, donations and tipping.

I would say probably the demographic at the moment is very similar to the early Internet, which is a very narrow demographic of technology professionals. There are a lot of nerds in this space. I can say that for sure. It just follows the same path as any other technology. It's becoming more and more broadly appealing to a broader demographic over time.

For me, the most interesting thing is not what bitcoin can do for western developed countries, because we have fairly sophisticated banking systems. I am fascinated by the idea of being able to deploy bitcoin on a Nokia feature phone in Kenya and Lagos, Nigeria, and bringing online to the global economy people who have never had access to financial services with international credit, and who could now be connected to everyone else in the world on an equal footing. That is exciting to me, and that's where the greatest need lies that bitcoin can fulfill.

Senator Ringuette: This is most impressive. You started out by saying you'd spent 20 years working on networks and data centres for financial services companies. I think they must be in dire need to hire you back.

With all the knowledge that you have gathered about crypto-currency, what would be your guesstimate to develop and create a similar crypto-currency?

AA: I'm not sure I understand the question.

Senator Ringuette: As you said, there are 500 different currencies on the networks. What would be the cost to develop and create a similar crypto-currency like bitcoin?

AA: Every day somebody decides that bitcoin isn't the correct answer and they have a better one. They go ahead and choose to try to build a better crypto-currency. The thing that block

chain technology has done is it has taken the very natural inclination of people to create currency as a form of language, as a form of expression of value. This exists in every society, whether it's from prehistoric times with beads and feathers to modern times with company money, company scrip and all the forms of currency that have existed before, federal, nationalized monopoly money.

That possibility of not only creating a currency but that currency being instantly, from its creation, global, secure, fast, predictable and transparent, that capability means that now a 10-year-old can create a currency and that currency can be as secure as the currency created by a monarch a few centuries ago.

Just like the Internet brought desktop publishing and communications into the hands of individuals and enabled the capability that previously was the purview only of those who had football-field-sized printing presses, the block chain technology has democratized access to currency creation. As a result, anyone with the impulse to create currency, for serious reasons to reasons that are completely trivial, can now do so. That currency is instantly global, secure and unforgeable.

Senator Ringuette: And without cost.

AA: And without cost. In fact, you can go on to a website and create the Ringuette coin today for a fifth of a tenth of a bitcoin, for small amounts in any case, and very soon that will be free.

I anticipate that you will see coins created by children, performers, entertainers, football teams, and most of these will only have entertainment effect or entertainment value. Some of them will surprise us and cross into the realm of economic value. It changes the fundamental relationship between individuals and the use of currency as a form of expression.

Senator Ringuette: You said individual bitcoin wallets can be targeted and compromised if not properly secured. How can one properly secure a bitcoin wallet?

AA: With great difficulty right now, and great technical skill. This is one of the issues that need to be addressed over the next many years in order to make bitcoin more accessible to mainstream users. Right now it's difficult to do so because our computer systems are not designed to secure money that has taken pure digital form and resides on, say, your iPhone or your desktop computer.

For experts and specialists there are new devices that come out, for example wallets that are completely embedded in hardware, small devices that you plug into your computer where all of the bitcoin keys are held only on that device. I actually print out my bitcoin keys on paper and I put them in a fireproof safe and store a second copy in a bank safe deposit box, which is ironic because I'm securing the bitcoin by putting it in the vault of a bank. But making it

physical actually allows me to impart the greatest form of security that I know how to use, because physical security is something that we're familiar with.
Information security is actually being accelerated because of bitcoin and a lot of innovation is happening in that space, which is very exciting.
Senator Ringuette: You indicated that a person could acquire a loan in bitcoin. How would one go about that?
AA: There are already organizations that are implementing a concept called peer-to-peer lending, which exists in the traditional currencies. For example, in the traditional currencies there are companies like lendingclub.com where I can go out and make a loan to a fellow American and they will end up paying a lower interest rate than a credit card, and I'll get an interest rate that's higher than I would get with a certificate of deposit. If I diversify my loans enough and only invest a small amount in each loan, I can suffer a pretty low default rate.
That model can now be taken global, and I could lend money with bitcoin -- there are companies already doing this -- to someone anywhere in the world, and, in fact, in that case, I would invest perhaps in two or three thousand different loans, so that default on one loan wouldn't affect my entire amount, and diversify my risk that way.
This has tremendous implications for worldwide credit, because it not only allows people in the developing world to source credit, but it also allows people in the developed world to invest their money directly with the borrowers, without intermediaries, at much lower cost, and it's already happening.
Senator Ringuette: But you have an interim intermediary. You have this organization that kind of directs what you are prepared to loan and the people that want to acquire a loan.
AA: Today we do, yes, indeed, but with bitcoin, this is one of the tremendous things that's happening, which is that many of the traditional financial services can now be redesigned and re-envisioned in a completely decentralized fashion without intermediaries. This concept of disintermediation, or removing intermediaries and connecting directly buyers to sellers, lenders to creditors and consumers to merchants, without intermediaries, is the magical power of bitcoin. That's what this invention has allowed us to do, without having to establish trust first.
So with bitcoin we can have a completely decentralized market for credit and lending that is simultaneously global, near instantaneous and allows access to a vast pool of credit, and that's a very exciting prospect.
Senator Ringuette: If Canada would move forward and do some regulation, as some witnesses have asked of us, and the G7 countries did not follow with similar regulation, what would be the pros and cons of such a move?

AA: That would be interesting because already we see tremendous regulatory fragmentation. We have a regulator in New York State that has taken initiative to do regulation based on New York state law, regulation that looks very similar to traditional banking regulation and is not very well-suited for bitcoin.

Simultaneously, there will be other forms of regulation. So in the United States, we're likely to end up with a patchwork of state, local and federal regulation, and I think you're going to see similar attempts in many countries.

Bitcoin technology is such that it can operate across borders very effectively, and, therefore, bitcoin companies can migrate to the area of least friction and can create the jobs, innovation and growth in the places where regulation is best informed about the nuances and particular needs of bitcoin companies.

So I think Canada and other countries that are looking at this regulation very carefully, rather than rushing into it, have an opportunity to create an environment that is friendly to those companies and attract one of the industries that, quite frankly, is creating thousands of jobs today, which is not to be said for too many other industries.

Senator Meredith: Thank you so much for your presentation. I read your notes last night, and this is a segue into what my colleague just raised with respect to regulations. Our committees here in the Senate are looking to put forward recommendations in a report to government that hopefully will become law to protect Canadians.

You talked about individuals being hacked and companies that you cited earlier that have spent millions of dollars on their security architecture to protect the data that has been provided by their consumers. We see how vulnerable they are, and this data has been lost. Major banks have come and indicated that they have been hacked months later, to the surprise of their consumers whose credit cards and data are out there.

Now you're advocating a decentralized system, when the traditional banking system is predicated on all the security measures put in place to protect consumers. We're about protecting Canadians.

To bring it back as to how we would do that, going forward with bitcoin and what you're proposing, I understand the rationale of access, especially when it comes to, for example, Africa and the outlying areas. We see the revolution of cellphones and how that has changed the dynamics of communication as well as transactions.

Talk to us about the security aspect of how we would go forth with respect to protecting Canadians who are engaged and who will become engaged in more transactions.

AA: One of the big failures of regulation in the traditional environment is that with centralized identifiers and centralized regulation comes centralization of risk. So when an organization such as Home Depot as a target is hacked, and they lose 60 million consumer

identities, the reason that represents such an enormous impact is because they were storing 60 million user identities in the first place. Instead, if each one of those 60 million consumers had to be individually attacked, targeted and hacked successfully, the possibility of that happening is much, much lower. So the advantage of a decentralized environment is that there is no central repository -- mother loads, cash, vault -- where everyone's identity is stored, and, therefore, everyone's identity can be attacked at the same time.

Bitcoin proposes a different model where the risk and the control are pushed out and put in the hands of the users, and the result of that is that it makes a system that is much more resilient to systemic risk. However, that means that the users themselves have enormous power, and with that, they have enormous responsibility. That control exposes them to individualized risk.

Senator Meredith: How do we mitigate that risk, though?

AA: That risk is already being mitigated by innovations. On the one hand, you have this increased exposure of the individual one by one, but on the other hand, we have programmable money. So the fact that it is programmable money allows us to invent completely new models for security, whether those are specialized devices that control keys and never expose them to an Internet environment, whether that is multisignature transactions where, in order to release funds, a number of signatures are required to release those funds. Those signatures could belong, perhaps, to two different devices that the user carries, so they simultaneously need to authorize a transaction from their laptop and their mobile phone, which gives them a greater degree of security.

You could have secondary or tertiary controls stored on paper or on a device that's kept off-line, in a vault, at home, in a fireproof safe, whatever. Those are the basic things we're doing right now.

But based on this technology, we're already seeing companies that are providing services to consumers where they will look at every transaction a consumer is making and provide a third signature to authorize that transaction based on a risk assessment.

In that case, that company has no custodial control over the funds. They can't take the users' funds. All they can do is sign or not sign that transaction. They're providing a risk check and just that.

These are very interesting models that we have never explored before because the user did not have enough control and the network was not open enough to allow this type of experimentation and access. The technology underlying it was not flexible enough.

So I have great faith. Already, just in the last two years, as this technology has gone mainstream, the amount of innovation around that exact problem has accelerated

tremendously, and we're gradually, I think, beginning to win in terms of protecting end-user wallets.

In this environment, specifically, requiring the users to attach identity to every transaction and then put all of those in a central repository, just like the regulations in New York have demanded, to me is folly, because it takes away the one opportunity we have to think of a different way of doing this and exposes us again to the same systemic risk of centralized points of failure and risk that we have with credit cards. So I'm hoping that the market is allowed to develop these solutions.

Senator Meredith: Going forward, my colleague Senator Black raised this with respect to breathing time and you indicated this as well, but what would be a suitable time frame for us to be able to look at? Obviously this is evolving, this is developing. However, we believe that there have to be some of sort of regulations put in place to govern, similar to what we've done now with the Internet in terms of privacy, requests for information and so forth.

With respect to the breathing time, if we were to enact some sort of legislation, give us your opinion as to what that would look like, to govern bitcoin and its transactions.

AA: I think that if we look at the experience with the Internet, the opportunity for the Internet to develop its own models for self-regulation was extremely effective, because it delivered a lot of good to a lot of people. In fact, ironically, when the U.S. Senate finally came around to regulating spam it was the same year that technology solved the problem. So in some cases waiting is the better option.

I don't think there's a major problem with consumer access to bitcoin at the moment in terms of the risk that it poses to consumers. However, there are particular areas where I believe your committee could offer clarity. The first one is making a clear distinction between centralized custodial accounts and decentralized models of bitcoin operation, and not lumping them together. Centralized custodial accounts are dangerous to consumers. They expose consumers to the exact same risk of a centralized financial institution only in this particular case there is zero oversight or control over these institutions because they operate outside of the banking environment.

For example, when CAVIRTEX came here and asked for a regulation in that environment, it is a very sensible idea because CAVIRTEX has complete control of the user's keys and operates in the traditional centralized custodial manner. However, I think leaving opportunities for the development of decentralized solutions, and recognizing that those are neither subject to the same risks for consumers nor do they need or can use effectively the same types of regulation as custodial accounts, would open up a lot of possibility for innovation in that space.

I think it's also important to carve out exceptions. There are exceptions already in existing law, in terms of personal use of small amounts of exchanges. For example, if I exchange a small amount of U.S. dollars for Canadian dollars on the street corner, I'm not going to be arrested for operating without a money transmitting licence.
I think it's important to recognize that on a small scale and for personal use, there should be clarity in the law that makes it clear that you don't require licences to operate and personal use as a consumer is not subject to banking level regulation, because that would be very useful in allowing for the development of this technology.
Senator Meredith: One final question, chair. You talked about the bad actors and the small percentage of them. What systems do you currently have in place to deal with those individual whose would abuse the system?
AA: Traditional law enforcement has been tremendously successful in being able to track and stop such activities on the network again and again. So far I haven't heard of any particular need for changing the way the network operates, and in fact such a request would be met with no change because this is a global network that isn't under the control of a single individual. I don't control bitcoin any more than anybody else controls bitcoin.
So the network itself provides a level of transparency that law enforcement can use.
(French follows -- Senator Hervieux-Payette: Si vous me permettez...)
(après anglais – **AA** -- law enforcement can use.)
La sénatrice Hervieux-Payette : Si vous me permettez, je vais vous poser des questions en français, compte tenu du fait qu'on n'a eu aucune intervention en français.
À l'heure actuelle, y a-t-il des pays qui reconnaissent et ont encadré le bitcoin?
(**AA**: I believe that there are several …)
(anglais suit)
(Following French -- Senator Hervieux-Payette -- encadré le bitcoin?)
AA: I believe that there are several countries in which bitcoin use has been recognized in many different ways at different levels of legislative or judicial process in terms of recognizing in fact that bitcoin is money and that it is subject to the same rules and regulations around taxation and operation. But with that it also carries certain liberties, such as freedom of association and freedom of expression. So in many countries, bitcoin fits comfortably within the existing system for currencies. However, I don't know that that has required specific legislation or that any country has legislated specifically for bitcoin.
(French follows -- Senator Hervieux-Payette: J'ai une très courte...)
(après anglais – **AA** -- specifically for bitcoin.)
La sénatrice Hervieux-Payette : J'ai une très courte question qui fait suite à une question posée plus tôt. Si la sénatrice Ringuette lançait un bitcoin Ringuette cette semaine et que

notre président avait son bitcoin depuis quelques mois, quelle serait la valeur de l'un par rapport à l'autre?
(**AA**: The various currencies that exist …)
(anglais suit)
(Following French -- Senator Hervieux-Payette -- par rapport à l'autre?)
AA: The various currencies that exist out there are related to each other based on a free-floating market rate, and that market rate is determined by trade between individuals on exchanges where those currencies can be sold and bought for each other. This is exactly the same mechanism with which the exchange rate between the Canadian dollar and the U.S. dollar is determined or between any currencies in the modern world, so all of these currencies have the free-floating market value.
I would argue that if there is very low liquidity in that market, it will be very difficult to establish a price that is representative of the value of that currency. Price discovery will be difficult and, in fact, will lead to very large volatility. As bitcoin and other currencies get larger, the volatility decreases. In fact, the volatility of bitcoin today is not at all dissimilar from the volatility of oil during the first decade of the discovery that oil could be used as a substitute fuel instead of whale oil that was used at the time. We see this with new technologies where, as the market develops, it starts off with tremendous volatility but over time as the amounts of volume and liquidity in the market increases, the volatility is reduced until these currencies become extremely stable.
For a global currency, a $5 billion valuation is tiny, and so I would expect that bitcoin will remain volatile for many years to come.
(French follows -- Senator Hervieux-Payette: La sénatrice Ringuette peut...)
(après anglais – **AA** -- for many years to come.)
La sénatrice Hervieux-Payette : La sénatrice Ringuette peut donc réfléchir aux cinq milliards qu'elle doit investir.
Vous parlez depuis tout à l'heure de la question de la sécurité qui entoure l'usage du bitcoin. Nous sommes des parlementaires et nous fonctionnons au sein d'un Parlement. Après ce comité, j'irai siéger au comité des finances.
Ma question concerne le contrôle du gouvernement. Si vous faites toutes vos transactions en bitcoins et que la valeur change continuellement, comment un gouvernement peut-il exercer son pouvoir fiscal?
(**AA**: The citizens of that government would …)
(anglais suit)
(Following French -- Senator Hervieux-Payette -- exercer son pouvoir fiscal?)

AA: The citizens of that government would exercise direct control over the currency through their own purchasing decisions, and through ownership control over their own units of currency. In many cases, as I mentioned before, bitcoin is not unregulated. It is regulated both by mathematics as well as dynamic markets that exist among its participants and users. Both the price of bitcoin, its value in commercial transactions and the use to which it is put is managed directly by the end user and those end users arguably are the same constituents. So if the constituents can apply direct control over the currency, they will do so.
(French follows -- Senator Hervieux-Payette: Si on parle de la valeur...)
(après anglais – **AA** -- over the currency, they will do so.)
La sénatrice Hervieux-Payette : Si on parle de la valeur au mois de janvier et que l'on prépare notre rapport-dépôt en avril, quelle valeur utilisera-t-on, aux fins de conversion, pour être capable de faire rapport aux autorités fiscales? Il faut quand même remplir un rapport d'impôt et établir une valeur. Les fluctuations peuvent être très grandes, alors que les quantités ne sont pas énormes. Peu nombreux sont ceux ou celles qui touchent des revenus annuels faramineux. Le Canadiens moyen touche environ 45 000 $ par année.
Quelle sera la valeur des revenus qui sera inscrite sur la déclaration de revenu d'un Canadien moyen qui gagne 45 000 $ par année pour les mois de janvier, février, mars? Comment cette personne pourra-t-elle faire le contrôle de ses revenus?
(M. Antonopoulos : That is a very interesting question …)
(anglais suit)
(Following French -- Senator Hervieux-Payette -- . . . le contrôle de ses revenus?)
AA: That is a very interesting question and one area where regulatory clarity would be extremely useful. I earn the vast majority of my income directly in bitcoin. Since October of last year, I have earned very little in terms of national currencies. I get paid in bitcoin and I pay many of my expenses directly in bitcoin.
For the purposes of taxation, I treat the bitcoin as earnings in a foreign currency, just as if I were doing contract work for a European company and being paid in euros. I will assess the market value of the transaction when I earn the income at that current market price, and then I will render taxes to the tax authority in the national currency. After, the primary power of the tax authority is to force the users to pay in the currency of their choice.
What becomes difficult is that, in the case of use of currency, the classification in the tax code depends on the use I have. For example, if I use my brokerage accounts to purchase euros for investment purposes and I sell those euros two months later and realize a gain, I will be subject to capital gains tax upon that gain. However, if I visit Paris and I use euros to pay for a ticket to the local Paris zoo, and the price of the value of euro changes between the moment I purchase that amount with my own currency and the moment I paid for the ticket,

I'm not assessed capital gains. It is considered a currency use, and therefore it is treated differently.

The tax code is flexible enough to allow me to declare the appropriate use for the appropriate tax classification, depending on how I've used it.

At the moment in the United States, at least, there has been a ruling that says that bitcoin operates as a commodity with capital gains taxation, which is, in my opinion, the wrong answer. However, if bitcoin had been classified purely as a currency, that would have been the wrong answer, too. In my opinion, the correct answer is that it depends on how it is used. If it is used for long-term investment, then it is subject to capital gains and losses, obviously. If it is used for consumer spending, then it operates as currency and means of exchange.

The tax system allows me to declare upon honour how I've used the currency and to then impose penalties if I have made that declaration incorrectly. That's how it works with every other currency.

So this is an area where clarity would be extremely useful, because it would allow us to use currency such as bitcoin in the same way as we use currencies from all over the world.

Senator Tkachuk: Thank you for your testimony here today. It has been an interesting afternoon.

Are the other virtual currencies based on an algorithm, as well, and is it the same one you used for bitcoin?

AA: There are several algorithms within bitcoin. There is a central invention, which is the block chain, and the security model that uses consensus through proof of work, which is a technology that allows a network to arrive at a secure picture of what the current ledger is, based on competition. That central technological innovation is used in the vast majority of currencies. I'll call that the block chain invention. However, there are other algorithms in bitcoin, such as the one that determines how often and how much of the currency is issued. Other currencies have taken different perspectives, so they use a different monetary policy recipe.

We've seen a very broad range of those choices, from currencies that are far more inflationary in nature with bigger supply of currency, even to ones that implement a demurrage interest rate -- meaning a negative interest rate -- that encourages consumption and discouraging savings. As a laboratory, these currencies can express a very broad range of monetary policies and even political perspectives.

The underlying invention, however, that secures the entire network is almost exactly the same across all of these currencies.

Senator Tkachuk: In previous testimony, we've heard about the miners, the people who actually issue or mine the currency. There were some stories in the paper in June of this year where a company had over 51 per cent of the mining market for bitcoin, so it was developing like a quasi- --

Does it have the ability to develop a total monopoly? Can one company develop a total monopoly in issuing bitcoins, and then does that jeopardize the whole currency itself? Are there controls on that, or how does that all work?

AA: It's important to emphasize the fact that the purpose of mining is to secure and verify all transactions. The reward for mining is currency issuance. We must not confuse the reward for the main purpose. Mining is rewarded with currency issuance for securing the network, and the reward acts as an incentive to ensure that the network remains secure.

The company in question, which is a mining organization, operates as a pool, similar to a lottery pool, which means they didn't control the hashing directly. They acted as a central location whereby many independent miners could pool their hashing power and put it behind this in order to achieve smoother returns on hardware investment. If you play the lottery by yourself, you may win but on a very irregular schedule. If you play as a part of a pool, you get lower payments more frequently.

In a similar way, because mining is a competitive function, individuals do not fare well -- they get very volatile payments -- so instead they pool their actions together. Interestingly, when GHash approached but did not reach 51 per cent -- but when they approached the high 40s -- this led to a market response, and the market response was such that individual miners, recognizing the potential risk to the reputation at least of the network -- although I don't think it was a serious technical risk -- withdrew their mining capacity from that pool operator and redirected it to other pool operators. Shortly thereafter, GHash.IO had their cumulative mining power dropped to what is at the moment slightly below 30 per cent of the total power of the network. That provides a very good level of protection against individualized attacks, because that's a very big amount but at the same time, it's not big enough to provide a monopoly.

On a technical note, a mining pool or an individual miner achieving the majority of the network can potentially disrupt the transaction processing function of the network for a short term. However, they cannot steal funds, redirect funds or invalidate transactions from the users; they can only delay them and delay the processing.

So it's not as big a risk as most people believe it is. Because of the marketing mechanisms behind it, we have seen again and again that it is a self-correcting system.

Senator Tkachuk: Just so I can understand whether it's just a method of exchange or a natural currency. If I have yen in Canada, I really can't buy anything. I have to go to a bank

and exchange it, because no one takes it. So I have to go to a bank and exchange it for Canadian dollars so I can buy something, and it's the same in each country. In each country, those dollars have certain value, so even though my Canadian dollar trades up and down as compared to the U.S. dollar, and so does everybody else, I still deal in Canadian dollars. It basically stays the same for Canadian products, unless it depends heavily on imports and all the rest of it.

Does the virtual sphere itself have its own stability? In other words, when something is priced in Europe for one bitcoin and I have one bitcoin, can I buy that for one bitcoin, even though the value of that bitcoin has changed in relation to the currency of my country or the American dollar?

AA: The exchange rate between bitcoin and individual currencies, such as the euro, the Canadian dollar and the U.S. dollar, et cetera, has sufficient liquidity that arbitrage is possible between the various exchanges, meaning that the purchasing power of one bitcoin is the same no matter what the national currency. The fluctuations are miniscule. If I could buy bitcoin for fewer Canadian dollars and sell it for more U.S. dollars, it would create an immediate opportunity arbitrage between the two markets; and that's exactly what is happening. In fact, arbitrage in bitcoin is, in many cases, even more effective because the bitcoin can be transferred but then it changes almost instantly across borders, whereas in traditional financial markets, moving money like that takes a bit longer.

The differences between national currencies even out quickly and there are no fluctuations. My bitcoin purchasing power, while volatile overall, is the same as across any national currency.

Senator Tkachuk: Is that where we're heading, where internationally things will be priced, bought and sold in bitcoins no matter what is happening underneath to national currencies only because you save so much money in exchange and all the rest of it? Is that where we're headed?

AA: I believe in the long term, bitcoin will be stable enough in terms of volatility that it will be possible to price things directly in bitcoin. At that moment, bitcoin becomes almost a universal currency in terms of its utility across the Internet. At least on the Internet, that would make it extremely competitive against national currencies in terms of ease of use and flexibility. I would expect that to happen; however, I think we're several years away before the volatility of the currency is such that things can be priced directly in bitcoin.

Senator Tkachuk: Bitcoin can be stored. Senator Gerstein, I don't know where you keep your bitcoin. Do you keep it in your wallet or is there a virtual wallet where you keep your bitcoins? Can you do that?

AA: This may be a tiny bit too technical, but I will provide some insight. The bitcoin is not stored by individuals but on the network on the public ledger; so the public ledger knows who has the bitcoin. Senator Gerstein has the keys that allow him to sign for transactions, essentially signatory control over those funds to unlock them. How you store the keys can depend as there are many ways to store the keys. Effectively, they are just numbers. For my protection, I print those out on pieces of paper and put them in a physical medium. I also have keys that control smaller amounts of bitcoin, spending change if you like, on my mobile phone. I have some on my desktop and some on hardware devices that I'm trying out. The vast majority I keep printed out on physical copies because it's more secure as they cannot be hacked you would actually need to break into my house.

Senator Tkachuk: Companies or businesses will do so many multiple transactions, thousands or millions in a day for all I know. Can bitcoins adapt to that? Can you do a payroll for 1,000 or 500 or 200 people easily with bitcoins? Can you do the deductions and all the rest of it or is it an issue?

AA: Not only can you do that but a medium-skilled programmer can do that in a few hundred lines of a programming language like Python accessing the entire financial network and instructing it to do that, which is fascinating. Not only that but they can do that with transactions to a thousand people living in 100 different countries, which is almost impossible to do with today's money. You can do payroll. There are many companies in the technology space. For example, Google pays tens of thousands affiliate companies for advertising revenue. The cost to them to pay these companies for that revenue across the world is enormous. The possibility of automating that and using a single currency for electronic payments can be done extremely fast, extremely efficiently, cheaply and globally.

Senator Tkachuk: I like it.

(French follows -- Le sénateur Maltais: Je suis d'accord avec mon collègue, .)

(après anglais)

Le sénateur Maltais : Je suis d'accord avec mon collègue, le sénateur Campbell, lorsqu'il a dit que les gens d'un certain âge pourraient avoir de la difficulté à utiliser cette monnaie. On a fait venir une machine à bitcoins, et le président a généreusement acheté des bitcoins pour une valeur de 100 $. Il ne nous en a jamais reparlé. On ne sait pas ce qui est arrivé, s'ils ont été perdus dans la brume, mais ce n'est pas votre problème.

Vous avez dit qu'un utilisateur de bitcoins peut prédire ce que seront leur valeur marchande dans 30 ans. Si un utilisateur de bitcoins, comme le président, pouvait prédire ce que sera leur valeur monétaire dans 30 ans, je ne comprends pas que le ministre des Finances ne soit pas déjà venu le chercher pour lui demander conseil sur ce qui pourrait arriver dans au moins cinq ans dans le secteur de l'économie et des finances. Trente ans, c'est loin. Vous êtes de

bons devins pour prédire ce que sera l'offre dans 30 ans. Je ne sais pas ce que vous pourriez me dire à ce sujet.
(**AA** : In the case of bitcoin…)
(anglais suit)
(Following French by Senator Maltais: . . . me dire à ce sujet.)
AA: In the case of bitcoin, specifically because it is designed to simulate the extraction of precious metals in its progression, it is entirely possible to predict with high accuracy how much currency will be available on the market at a specific period of time. That does not necessarily mean that supply will meet the demand or that it is the correct supply. It's just that we know what that supply will be. Today we can predict to a high degree of accuracy what the supply of gold will be over the next year because it has been extracted at a very predictable rate, similarly with bitcoin.
(French follows -- Le sénateur Maltais: Je vous arrête là dessus. . . .)
(après anglais)
Le sénateur Maltais : Je vous arrête là-dessus. N'importe quel actuaire de compagnie d'assurances, lorsqu'il établit une rente sur 30 ans, est quand même capable de projeter des sommes plus ou moins réalistes. Ils n'ont pas besoin du bitcoin pour établir l'offre monétaire d'ici 30 ans. Ils sont capables de faire de bonnes extrapolations par des formules très simples. Une chose me chicote cependant. Ne craignez-vous pas que le système bancaire soit en train de doubler le système bitcoin présentement? Les banques voient venir les coups. Elles sont capables de s'adapter à des technologies assez nouvelles. Il me semble que l'Association des banques mondiales, sur le plan du capital, est plus forte en ce qui concerne la recherche en technologie de monnaie numérique que Bitcoin peut l'être.
(**AA** : Yes, indeed, I think the invention behind bitcoin . . .)
(anglais suit)
(Following French by Senator Maltais: . . . que Bitcoin peut l'être.)
AA: Yes, indeed, I think the invention behind bitcoin, the block chain technology, will have a substantial influence over the future of banking. I have had several discussions with banks that are very interested in using similar systems to create more efficient networks within the banking system. For example today, a lot of clearing operations for worldwide fund transfer or clearing stock and equity purchases are handled by intermediaries. Bitcoin would allow banks to handle those in a decentralized network by simulating the same technology as bitcoin on their own. Furthermore, banks in the developing world are interested in using bitcoin to extend services to areas where they can't deploy
infrastructure. Telecommunications companies at first were threatened somewhat by the Internet but now run entire networks on top of the Internet. Similarly, banks will find ways to

utilize this technology. I would not be surprised if very big parts of financial services eventually run on top of technology very similar to bitcoin, perhaps bitcoin itself.
(1750 follows in French -- Senator Maltais: Ceci m'amène à vous demander: . .)
(après anglais 1740)
Le sénateur Maltais : Ceci m'amène à vous demander : n'avez-vous pas l'impression d'avoir été avalé avant que vous n'existiez? Les banques ne vous laisseront jamais un champ opérationnel. Je ne parle seulement des banques canadiennes ou américaines, mais de toutes les banques au monde. Je ne crois pas qu'elles se laissent avaler ainsi, sans dire un mot. Dans le moment, vous jouissez de la publicité dans les journaux et auprès des jeunes – et je n'ai rien contre la technologie. Toutefois, je ne crois pas que les banques se laisseront arracher la laine de sur le dos sans dire un mot et sans vous avaler. Soyons francs. Bitcoin n'a pas les reins solides. Tout n'est que virtuel.
(**AA**: Yes, indeed. In fact, I remember the exact …)
(anglais suit)
(Following French - Senator Maltais - Tout n'est que virtuel.)
AA: Yes, indeed. In fact, I remember the exact same discussion when the idea that the International Telecommunication Union would be thwarted or somehow threatened by this nascent technology called the Internet was ridiculous on its face. The idea that world leaders, states, would allow the Internet to give people freedom of expression was preposterous. The idea that the Internet would be allowed to subvert the will of despots around the world and would not be instantaneously shut down whenever they felt it was threatening their authority was preposterous, yet all of these have happened.
I believe that bitcoin, by empowering individuals -- and especially individuals who do not even have access to the banking facilities we're talking about -- will create a thriving economy of its own and an economy that will not threaten banks but will open new opportunities for banks. In the end, just like the telecommunications companies, many of their old models and old profit sources will be fundamentally disrupted.
Today AT&T's long distance network has been decimated and Skype has dominated that space. Yet AT&T did not give up. They became the world's largest Internet service provider. Eventually I believe bitcoin-like currencies will decimate certain industries, especially high-profit, low-service industries such as international remittances which are exploitative in their nature. However they will open new industries, products and services, and the economic activity enabled by bringing together billions of people on a fully connected global financial system is so much bigger than the potential risk this may pose to the profits of incumbents.
The Chair: In your comments, which have been fascinating, you made reference to the fact that one of the great motivators to you personally in getting involved in this is the technology

that it's going to bring to people who do not have it today, and I think you used the term "empower" billions around the world.

If I am correct, I believe Mr. Gates, in his charitable giving in Africa, is making use of digital currency called m-pesa.

AA: That's correct.

The Chair: Could you expand a little on what you see the impact of bitcoin, m-pesa or digital currency in general will have in terms of Africa?

AA: M-pesa is a fascinating study for those of us interested in digital currencies. It has shown what is possible when low-friction digital money is introduced into an environment without the need for massive infrastructure, an environment that doesn't have banking service well developed.

M-pesa was started as an experiment that allowed individuals to transfer cell phone minutes amongst themselves and their families by a telecom provider in Kenya. I imagine the moment this became a currency was a very mundane moment, such as for example a customer arriving at a store and realizing they didn't have sufficient money to buy a dozen eggs and saying, "Can I give you a couple of cell phone minutes instead?" With that simple concept a currency is born.

What is fascinating about m-pesa is we roll forward just 12 years, m-pesa is now responsible for 40 per cent of the GDP of Kenya. That is a staggering amount. It represents the adoption of what was largely an underground, cash-based economy, one that was illiquid, inflexible and slow to operate, and turbocharging that by providing enormous liquidity and fluidity into the economic system.

At the moment bitcoin is not ready to be adopted easily on the most deployed platform in the world, which is a Nokia feature phone, the Nokia 1000, of which there are billions. It requires a bit more infrastructure than that, but gradually we see two trends converging. One is bitcoin being applied on simpler and simpler technology, and we already see its use through SMS text messaging.

The other one is the collapse in the cost of producing smartphones, with the Android approaching $25. There are already applications of the bitcoin space that would allow a single Android phone to support thousands of simple SMS customers and give them bitcoin wallets. That would essentially allow a young kid in Lagos, Nigeria, to buy an Android smartphone and become a bank serving thousands of customers, simultaneously giving them access to the equivalent of a Western Union terminal, a credit facility for buying loans, as well as a trading facility for all of the world's markets, and this off a simple Android phone and SMS feature phones.

M-pesa shows us it is possible. Bitcoin now makes that phenomenon global. When we talk about the unbanked, the World Bank estimates that 2.5 billion people are completely unbanked, living in cash-based societies. However, that vastly underestimates the problem. If you look at the types of banking facilities we have in the western world, the ability that I have to access a brokerage account with access to any of the international markets to convert any currency I want without controls to transmit money to any country in the world I want, again with little controls, and use it as a simple consumer is very far removed from what most people have.

If you look at the unbanked as those who have a single currency only, close the account that does not have access to international markets, credit or trading capabilities, more than 6 billion people in the world live with that kind of banking, and 2.5 billion of them are completely unbanked. Bitcoin can change that environment dramatically in less than a decade.

Senator Black: I would like to again thank you for your contribution. It's extremely helpful. I want to move to a couple of final points that I want clear in my mind. I want to take from your comments, arising from what Senator Ringuette asked, that we've been exploring through this hearing the opportunity that may exist for Canada, for innovation, if we get this right. Can you succinctly tell us what you think that opportunity is?

AA: I think there are two aspects to this. One is the pure research and technology innovation capabilities that might exist in the bitcoin sphere. One of the things I'd like to emphasize is that bitcoin is not just money for the Internet. To look at it simply as money for the Internet is to miss the point.

Bitcoin is the Internet of money. Currency is just the verse, the app. Currency is an app running on a decentralized trust network based on block chain technology, which means that many other apps will exist.

The bitcoin currency is almost the same as email was in the 1990s. It enabled the growth of the Internet. It was the killer application that made it viable and worthwhile for people to get involved, but it couldn't possibly open our eyes to the endless possibilities that came afterwards. We couldn't envision the Web in the early 1990s, or even Facebook and Twitter and things like that today.

Bitcoin, the currency, is just the tip of the iceberg. It is the proto-technology that really brings that decentralized network of trust to consumers, but there will be other apps and it's already evolving at a tremendous rate. From a pure research and innovation perspective, it's incredible.

The other thing is to think about the possibilities of extending banking services. Even though Canada has a highly banked population, there are still pockets within this country. I know in

the U.S. close to 18 per cent of the population have very limited banking capabilities, and that is probably true of most developed nations. There are pockets within this country where people have very little access to banks.

I think the combination of doing primary research in innovation in these new technologies and opening banking to reach different corners of this country and disadvantaged parts of the population a very potent combination, especially if we take advantage of the international aspects of this currency.

Senator Black: How did New York State get it wrong?

AA: I think they got it wrong in many ways, first of all by rushing to regulate very soon, but more importantly, by regulating bitcoin in exactly the same way that the banking system currently operates and failing to see the distinctions between bitcoin and the current system. The only analogy I can think of is if in the proto-Internet, the Federal Communications Commission in the United States had decided that the Internet was simply a sophisticated form of CB radio and required a licence from every website operator. Such an outcome would have almost certainly destroyed the Internet industry in the U.S. However, because of the enormous need for such a tool, it would not have affected the Internet industry everywhere else; it would simply have pushed that innovation elsewhere.

I think treating bitcoin as a proto-bank account with some fancy features is to miss the point, and regulating it, then, as such completely stifles it. It puts it immediately into the playing field of incumbents. It ties them up in the same kinds of regulations, and it forces us to behave more like a bank when its unique characteristic is that it isn't a bank.

Senator Massicotte: Thank you again. I have one technical question and then a more important question.

On the technical side, many countries and provinces have sales tax coupled with income tax. For the merchants using your currency, is there software already in place? For my dollar cents (18:02:15), there are cash registers and it has gotten pretty sophisticated. Is it easy for them to do the accounting and collect the sales tax? Does that already exist for merchants?

AA: Absolutely. In fact, it's easier with bitcoin because the public ledger provides a complete record of all of the transactions. It's as if all of my bank statements from the first moment I use bitcoin are online. I render sales tax to the State of California for the business I ran selling products via bitcoin. I also pay my income taxes in U.S. dollars based on my income, which is entirely in bitcoin. And I do all of my accounting using traditional accounting software.

Senator Massicotte: You have software in place to do transfers and the calculations immediately?

AA: Yes, although it's rather cumbersome at the moment because the modalities are quite different. For example, in my normal banking -- traditional banking, if you like -- I have a handful, four or five, different accounts. In bitcoin, I have well over 2,000 accounts because with bitcoin, it makes sense to create a new account for every transaction. It's not really an account. Therefore, if you try to put it into the same model, it's difficult to work. However, the software is being developed.

Senator Massicotte: You basically answered the question, but the way I see it, this is a highly secure and anonymous form of transfer of property. You can call it currency; you're using it now as currency from a sense of bartering.

It seems this could be very useful in many things, including exchange of property. Today we have a bunch of lawyers or notaries who acknowledge the safe transfer of real estate property, but it seems this application could be used very often in many different facets. Let's fast-forward five years; how do you see this technology being used to the benefit of our society? Give me some examples.

AA: There are some very interesting applications. The decentralized ledger is used as a public record of sorts for all kinds of things, from registering bicycles to registering automobiles to registering company shares.

Two days ago, I was at a bitcoin conference where a couple was married, and their marriage was registered on the blockchain for the first time. They used the blockchain as a registrar of that contract.

You could use it to register titles and deeds for properties and transfer those titles and deeds for any form of property, including vehicles and real estate. With a simple electronic transaction, you can transfer the deeds to a car. Even better and more importantly, the car could look up its own title and render itself usable to the new owner automatically. This concept is called smart property, where the property recognizes its ownership through reference to the blockchain.

All forms of decentralized registration can be implemented with a blockchain. Furthermore, you can issue share certificates or any other form of token that can be traded, from sharing my bandwidth and receiving a token in return that I can spend to use somebody else's bandwidth to creating possibilities for sharing economy similar to how we do Airbnb or sharing cars today. We can do many of those things using digital tokens.

There is a company here in Toronto who developed an application that allows you, upon submitting a transaction on the blockchain, to unlock a door, for example, for an Airbnb apartment. So your smartphone would make the payment and also unlock the door to the apartment and allow you access to that property.

Senator Massicotte: It's amazing. I have a secondary question. I don't understand the blockchain for a couple getting married. Was he scared to get mixed up with the wife? What's the issue?

Senator Campbell: Let's not go there.

AA: It was largely symbolic and a proof of concept. This couple was already married under traditional state laws. However, what they wanted to do was to record their marriage on a record that was publicly accessible, unforgeable and completely unchangeable through time. It provides a permanent record of what has happened, an unalterable history that within an hour is completely unalterable by anyone and will be preserved through history because of the value of the transactions that occur.

Senator Greene: Thank you very much. I really take your point about the dangers of inappropriate or premature regulation because we don't know where this is heading, the pace of change is large and we don't want to influence, I don't think, the pace of change or what it might lead to.

We have to write a report, and the report will have recommendations. So my question is: What would your reaction be to just a report with one recommendation, and that recommendation would be that there be no regulations and that we revisit this in, say, five years?

AA: I think that would be a very good idea. I think there is some room for clarification, clarifying, for example, the tax status for individuals, or at least clarifying the rights of an individual to make a choice in the currency they use as a consumer and to affirm the legality of using digital currencies in all forms of commerce as entirely equivalent with any other national currency, recognizing this is a private form of barter and transaction, recognizing the corresponding principles, which I consider neutral principles, but they are principles of enlightenment, which are freedom of association, freedom of expression and freedom of conscience. So I think that removing ambiguity in that particular arena for personal use would be enormously useful.

Senator Greene: I agree. Thank you very much.

The Chair: **AA**, your reputation preceded you prior to your arrival. You may recall that in my introductory remarks, I did not introduce you as "a" bitcoin guru but as "the" bitcoin guru.

AA: You humble me, senator.

The Chair: I think I can speak on behalf of all of the members of the committee in saying that you have more than lived up to that reputation, and we greatly appreciate your appearance today.

Hon. Senators: Hear, hear! -- The Chair: Thank you very much.