# Bitcoin: Introducing the Future of Money

Canadian Bar Association
Banking Law Section

Ross McGowan Andrew Hodhod

October 7, 2015

# Agenda

- Bitcoin – Terminology and Fundamentals
- A short history of the modern ‘theory of money and banking’ from coinage to clicks
  - The role of ‘fiat currency’
  - Fractional Reserve Banking
  - Is virtual currency, including Bitcoin, money?
- Regulatory Implications / Policy Direction
- Lending on security of virtual currency
- Opportunities

Borden Ladner Gervais

# Terminology

- **Digital currency (a.k.a. “virtual currency”?)**
- **Centralized vs. decentralized digital currency**
- **Convertible vs. non-convertible digital currency**
- **Cryptocurrency – a decentralized digital currency that is convertible and functions as both a currency and a decentralized payments system.**
  - Bitcoin is an example.
  - October 2014 – between 500 and 1,000 cryptocurrencies.

Borden Ladner Gervais

# Bitcoin Fundamentals

- **What is Bitcoin?**
  - Invented in 2008 – “Satoshi Nakamoto”
  - Open source, peer-to-peer digital currency.
  - Completely decentralized. Bitcoin exists on the hard drives of users all over the internet, each updating one another about new transactions and checking each others work.

- **How does it work?**
  - Ownership of Bitcoins is tracked on a public ledger (the “block chain”) that is distributed to all users of the system. When a transfer takes place, the transfer is added to the ledger and distributed to all users.

Borden Ladner Gervais

# Bitcoin Fundamentals

- **Basic Elements**
  - Public Key (“Address”)
    - Points to an entry in the block chain “ledger”.
    - Think of this as a bank account number.
  - Private Key
    - Authenticates ownership of Bitcoins in an entry on the “ledger”.
    - Think of this as the password to the bank account.

Borden Ladner Gervais

# Bitcoin Fundamentals

- **Conceptually:**

| BLOCK CHAIN | | |
|---|---|---|
| Public Key | Bitcoins | Private Key |
| … | | |
| 111123759 | 100 Bitcoins | XXXXXXXXX |
| 111123760 | 50 Bitcoins | XXXXXXXXX |
| 111123761 | 300 Bitcoins | XXXXXXXXX |
| 111123762 | 8 Bitcoins | XXXXXXXXX |
| 111123763 | 0.78 Bitcoins | XXXXXXXXX |
| … | | |

Borden Ladner Gervais

# Bitcoin Fundamentals

- **What is a wallet?**
  - A list that keeps track of all of your public/private keys.
  - Password protected.  Easier than remembering 40+ character public/private keys.
  - Hides some of the ugly mechanics “under the hood” to make use of Bitcoin user-friendly.
  - There are also “paper wallets” which are hard copies of your public/private keys.

Borden Ladner Gervais

# Bitcoin Transaction

## 1) Wallets

- Generates a unique digital address to be used on the network and contains a record of the owner's Bitcoin balance.

## 2) Keys

- Each digital address has a corresponding private key (required to send a payment) and a public key (allows payments sent from this address to be verified).

## 3) Submitting a transaction

- Transaction is encrypted with sender's private key and submitted on the network for verification by miners.

Borden Ladner Gervais

# Bitcoin Transaction (cont'd)

## 4) Mining

- Confirmation of the transaction.
- "Candidate blocks"
- The rules and protocols of Bitcoin require miners to solve a "random hash algorithm" in order to add a candidate block to the public ledger (a.k.a. the "block chain).

## 5) Compensation

- Miners compete to solve the algorithm.
- The first miner to solve the algorithm is compensated with 25 Bitcoins (market value – approximately $7,624.74 CAD as of Sept. 13, 2015).
- This is how Bitcoins come into existence.

Borden Ladner Gervais

# Bitcoin Transaction (cont'd)

## 6) Updating the public ledger (a.k.a. the "block chain")

- Once the algorithm is solved (approx. 10 minutes after the transaction is initiated), the "winning" miner's block of transactions is added to the public ledger.
- The updated ledger is then sent across the network for authentication.

Source: adapted from a diagram prepared by the Library of Parliament.

Borden Ladner Gervais

# Bitcoin Transaction Sample


Temporary Bitcoin Wallet

SHARE

Public Key:
15rNB9BMPfPa8GQQS
mBVmAGboW8N6E6feg

bitcoin

SECRET

Private Key:
Ky8NX29RPqTZBVFCp91XFCXRMe
xmYPfwWMN2KgX8GhtyEkumVZBB

WARNING: Back up this wallet as soon as possible. WE CANNOT RECOVER LOST WALLETS!
http://decentral.ca/paperwallet/

BITACCESS
Transaction Receipt

22/08/2014 04:03 PM
Ref: YW50aG9ueTI2Mzk4
Mobile: +14165245006
Type: buy
Price: 602.02 CAD
Cash deposited: 5 CAD
BTC sent: 0.00810537 BTC
BTC address: 15rNB9BMPfP
a8GQQSmBVmAGboW8N6E6feg
TXNID: 914eade7eebc2e37
bda92143ad62e963934d6f8
799a326c4ebcf8af190c84925
---
bitaccess.ca
operator message

Borden Ladner Gervais

# Acquiring Bitcoins

- **ATMs**
  - 26 in Quebec, 83 in Canada (Sept. 13, 2015)
  - USA – 156, UK – 28
  - World – 459
  - http://coinatmradar.com/
- **Peer-to-peer**
- **Mining**
- **Digital currency exchanges**
  - A business that allows customers to convert fiat currency to digital currency and digital currencies to fiat currency or other digital currencies.

Borden Ladner Gervais

# Other Facts

- **Only 21 million Bitcoins can ever be created.**
- **In theory, the mining process slows down over time.**
  - But, computing power?
- **Bitcoins are divisible into smaller units (.00000001 Bitcoins – a “satoshi”).**
  - Smallest transaction possible on Bitcoin network is 5430 satoshis.
- **Transaction fees are minuscule.**
- **The “51% attack”**
  - Prevent transactions? Allow double spend?
  - Ghash.io

Borden Ladner Gervais

# A short history of money and banking:
## Definition

- **Money – definition:**

  **"Any generally accepted medium of exchange."**

- **The main functions of money are distinguished as:**

  **a) a medium of exchange;**
  **b) a unit of account;**
  **c) a store of value; and,**
  **d) occasionally in the past, a standard of deferred payment.**

Borden Ladner Gervais

# A short history of money and banking:
## Notable evolution of money and payments

- **Pre-money:** barter, commodity standards (chattel)
- **Metal Ingots:** copper, silver, gold
- **Coinage:** 7th century B.C. – stamped metal with stipulated weights and value
- **Goldsmith receipts and promissory notes:** early middle ages, mercantile fairs, the advent of fractional reserves
- **Bank notes and bills of exchange:** late middle ages – culminating in Bank of England 1694 as one of the first 'modern' central banks, the rise of 'bankers'

Borden Ladner Gervais

# A short history of money and banking:
## Notable evolution of money and payments (Cont'd)

- **Charge Cards:** 1920's and 30's – Western Union and oil company payment cards for affiliated customers
- **Multi-merchant Charge Cards:** 1958 – Amex
- **Multi-merchant Credit Cards:** 1966 – Visa ('chargex')
- **Multi-branch debit cards:** 1970's in Canada
- **Advent of 'Internet' banking:** 1983 with Bank of Scotland
- **Mobile Payments:** IPhone 1 launched in January 2007, leading to mobile apps
- **Bitcoin:** launched in January 2009

Borden Ladner Gervais

# A short history of money and banking:
## Observations

1) Evolution of money and payments from tangible to ethereal has been ongoing for thousands of years.
2) Each shift in paradigm maintains past advances, and borrows heavily from the concepts and nomenclature of past paradigms.
3) The concept of money and payments has evolved in sync with the globalization of the underlying economic needs of society and to fulfill the convenience and efficiency of coordinating payments.
4) These trends are inevitable.

Borden Ladner Gervais

# The status and role of ‘fiat currency’

- Invented in China in the 11th century
- By the 17th century was gaining widespread use throughout Europe (in conjunction with modern fractional reserve banks)
- Late 1800’s many governments issued and legislated use of ‘fiat currency’ – convertible to gold
- 1900’s – Central governments used the power of the printing press to pay war debts with the result of volatility in the value of currencies and hyperinflation

Borden Ladner Gervais

# The status and role of ‘fiat currency’
## (Cont’d)

- 1930’s – advent of Keynesian economics and the rise of governments in fiscal policy and the Central Bank in monetary policy to stabilize economies
- 1980’s – the rise of Monetarism and belief in the primacy of monetary policy as the fundamental stabilizer
- 2008 – the Great Recession – total collapse averted through massive injections into the world money supply and fiscal stimulus (with many economic casualties along the way)

Borden Ladner Gervais

# The status and role of ‘fiat currency’:
## Observations

1) Governments and Central Banks work in tandem to grow the money supply to create stable inflation.
2) Economies around the world thrive with modest stable inflation. Hyperinflation and deflation are to be avoided.
3) Fiat currencies have not always been a successful:
   a) medium of exchange;
   b) unit of account; or
   c) store of value.

Borden Ladner Gervais

# Fractional Reserve Banking:
## Purveyors of credit – the first digits …

- **"First, as to banking. A banker has been defined as "a dealer in credit." True, in ordinary speech, bank credit implies a credit which is convertible into money. But money as commonly understood is not necessarily legal tender. Any medium which by practice fulfils the function of money and which everybody will accept in payment of a debt is money in the ordinary sense of the words even although it may not be legal tender..."**
  per Lord Duff *Re: Alberta Legislation [1938] S.C.R. 100*

Borden Ladner Gervais

# Fractional Reserve Banking:
## The Psychology of Reputation

- Underlying all fractional reserve banking systems is the reality that:
  a) capital reserves are less than current liabilities;
  b) stability of the institution is founded on its reputation for integrity and the safety and soundness of its lending and investment practices.
- Traditionally banks fostered this by having imposing tangible bricks and mortar branches.
- More recently financial institutions foster reputations through marketing the sanctity of “The Brand”.

Borden Ladner Gervais

# Is Bitcoin money?

Or a payment process or something else...

- **There is a basis for reasonable debate that Bitcoin has many of the characteristics of being both money and a payment process, so, perhaps it is something new.**

- **The key elements of 'money' are:**
  **a) a medium of exchange;**
  **b) a unit of account; and**
  **c) a store of value.**

Borden Ladner Gervais

# Is Bitcoin money?

## Or a payment process or something else... (Cont'd)

- **Medium of Exchange: not yet universally accepted, but then neither was 'fiat currency' in its infancy.**
- **Unit of Account: prices and value are not generally recognized in "Bitcoins", but there is no fundamental impediment to doing so.**
- **Store of Value: highly volatile market at present due to lack of stable reputation and media attention to frauds (Mt. Gox). However, I will trade my 5 Trillion Zimbabwean dollars for 1 Bitcoin.**

Borden Ladner Gervais

# Evolution vs. Revolution:
## Policy implications and ‘digital’ finance

- **The concept of Bitcoin is revolutionary to money and payments in the same way Esperanto was to language, except Bitcoin is being adopted.**
- **Bitcoin presently creates an opportunity to:**
  - **a) transact some business for some goods through an anonymous exchange;**
  - **b) store some value outside of ready access or control of government intervention or monitor; and**
  - **c) perhaps speculate on a volatile market for Bitcoin through purchase and sale on an unregulated open market.**

Borden Ladner Gervais

# Evolution vs. Revolution:
## Policy implications and 'digital' finance (Cont'd)

- **Bitcoin or whatever digital world currency may overtake it represents an evolutionary supplement to the global demand for anonymous mobile payments.**
- **Current market cap of Bitcoin in circulation was estimated to be about $3.36 Billion USD equivalent on September 13, 2015.**
- **Relative to world 'fiat currency' money supply, Bitcoin is presently infinitesimal. The USD Federal Reserve July 2013 estimate of USD 'fiat currency' alone is $1.5 Trillion or $10.5 Trillion if we use broad definition of money supply.**

Borden Ladner Gervais

# Evolution vs. Revolution:
## Policy implications and 'digital' finance (Cont'd)

- **Bitcoin's attributes will continue to attract both unsavory 'participants', desperate localized global account holders, and early adopters seeking to explore a new payment medium.**
- **The short term challenge for governments are to:**
  - **a) develop anti-money laundering compliance guidelines and protocols;**
  - **b) identify processes for identifying and imposing taxation on transactions; and**
  - **c) develop policy on whether it poses a serious risk to monetary and fiscal policy.**

Borden Ladner Gervais

# Opportunities & Mining for Bitcoins:

Making money the old fashioned way, sell things to the miners

- **There are at least three ways to make money from Bitcoin:**
  - **a) mine it yourself, (but that requires computing power, which for most CPU's is uneconomic relative to the cost of electricity);**
  - **b) purchase and speculate in the ownership of Bitcoin, hoping that it is an appreciating asset; or**
  - **c) accept and exchange Bitcoin for transactions as one would with other digital payment processes, setting price, commissions and conversion rates favourable to the transaction.**

Borden Ladner Gervais

# Regulatory Implications

***Currency Act***

- Legal tender is coins or notes issued by the Bank of Canada for circulation in Canada.

***Bank of Canada Act***

- Does not recognize Bitcoins as “notes” for circulation in Canada.

***Proceeds of Crime (Money Laundering) and Terrorist Financing Act***

- Currently Bitcoin exchanges and Bitcoin ATMs are not considered “money services business”.

Borden Ladner Gervais

# Regulatory Implications
## (Cont'd)

### *Provincial Regulation*

- Subject to provincial laws of general application, including consumer protection laws.
- In some circumstances, may be subject to securities laws.
  - Currently, digital currencies do not qualify as "securities" or "derivatives" under their securities and derivatives legislation in Ontario and Quebec, and consequently, are not regulated as such.
  - However, digital currencies could be packaged as an investment product or a derivative, in which case relevant legislation would apply.

Borden Ladner Gervais

# Regulatory Implications
## (Cont'd)

### *Provincial Regulation*

- Quebec
  - Transactions involving virtual currency may be subject to *Securities Act*, the *Derivatives Act* and the *Money-Services Businesses Act.*
  - On February 12, 2015, the Autorité des marchés financiers ("**AMF**") announced that it had amended the Policy Statement to the *Money-Services Businesses Act* (the "**Act**") to bring virtual currency ATMs (such as Bitcoin ATMs) and virtual currency trading platforms within the purview of the Act.
  - As a result, businesses that operate a virtual currency ATM or a virtual currency trading platform are now required to obtain a licence from the AMF and comply with the provisions of the Act.

Borden Ladner Gervais

# Regulatory Implications
## (Cont'd)

### *Tax Treatment*

- CRA: Cryptocurrencies are a commodity for tax purposes
- Gains in connection with Bitcoins are taxable in Canada
- Subject to the same rules as barter transactions
  - i.e., valued in accordance to the goods or services for which they are exchanged.
- May be subject to income tax
- Goods and services purchased in Bitcoins are subject to GST

Borden Ladner Gervais

# Future of Bitcoin:
## Proposed Regulations

### Canada 2014 Federal Budget

*"The Government of Canada is committed to a strong and comprehensive regime that is at the forefront of the global fight against money laundering and terrorist financing and that safeguards the integrity of Canada's financial system and the safety and security of Canadians… It is important to continually improve Canada's regime to address emerging risks, including virtual currencies, such as Bitcoin, that threaten Canada's international leadership in the fight against money laundering and terrorist financing."*

Borden Ladner Gervais

# Future of Bitcoin:
## Proposed Regulation (Cont'd)

- **Amendments to *Proceeds of Crime (Money Laundering)Terrorist Financing Act***

  - Section 5 (h) provides, in relevant part, that persons and entities that have a place of business in Canada and that are engaged in the business of dealing in virtual currencies, as defined in the regulations, are subject to Part 1 of the Act.

  - Section 5 (h.1) provides, in relevant part, that persons and entities that do not have a place of business in Canada, that are engaged in the business of dealing in virtual currencies, as defined in the regulations, directed at persons or entities in Canada are subject to Part 1 of the Act.

Borden Ladner Gervais

# Future of Bitcoin:
## Proposed Regulation (Cont'd)

- **Amendments to *Proceeds of Crime (Money Laundering)Terrorist Financing Act* (cont'd)**
  - Subsection 9.31(1) states, in relevant part, that no bank, federal or provincial trust company or credit union shall open or maintain an account for, or have a correspondent banking relationship with, a person or entity that does not have a place of business in Canada and that is engaged in the business of dealing in virtual currencies, as defined in the regulations, directed at persons or entities in Canada, unless that person or entity is registered with FINTRAC.
  - Regulations pending.

Borden Ladner Gervais

# Future of Bitcoin:
## Policy Direction

- **Finance Canada Study of Retail Payments, including digital currencies**
  - Discussion paper or other consultation process still to be announced.

- **Standing Senate Committee on Banking, Trade and Commerce**
  - June 2015 – the Committee published a report on digital currencies which highlighted the potential risks, threats and advantages of these forms of exchange.

Borden Ladner Gervais

# Standing Senate Committee on Banking, Trade and Commerce

## “Digital Currency: You Can't Flip This Coin!” (June 2015)

- 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.”

- 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.”

Borden Ladner Gervais

# Standing Senate Committee on Banking, Trade and Commerce (Cont'd)

## "Digital Currency: You Can't Flip This Coin!" (June 2015)

- 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."

# Standing Senate Committee on Banking, Trade and Commerce (Cont'd)

## "Digital Currency: You Can't Flip This Coin!" (June 2015)

- **Opportunities**
  - Lower transaction costs for Canadian individuals and businesses (especially re: international transfers).
  - Bringing financial services to the unbanked in the developing world (in conjunction with mobile phones).
  - Using block chain technology to protect and manage information.
  - Canada as a global digital currency hub.

Borden Ladner Gervais

# Standing Senate Committee on Banking, Trade and Commerce (Cont'd)

## "Digital Currency: You Can't Flip This Coin!" (June 2015)

- **Risks/Challenges**
  - The use of digital currency to launder money and finance terrorist activities
    - E.g. Liberty Reserve, Silk Road
  - Licensing of digital currency exchanges and ATMs is currently lacking
    - Exceptions – Quebec, New York State
  - Digital currency-related businesses often have difficulty in accessing banking services
    - Banks fear risk of non-compliance with AML and KYC obligations

Borden Ladner Gervais

# Standing Senate Committee on Banking, Trade and Commerce (Cont'd)

## "Digital Currency: You Can't Flip This Coin!" (June 2015)

- **Risks/Challenges (Cont'd)**
  - Cyber-theft, loss and bankruptcy of digital exchanges
  - Volatility in the price of digital currencies
  - Taxation issues/challenges
    - Still easier to trace than cash, says CRA
  - Lack of information available to the public re: digital currencies
  - Protection for users (e.g. disclosure of risks, procedures to address disputes, monitoring of transactions, deposit insurance, etc.)
  - Lengthy verification process for Bitcoin transactions
    - Approximately 10 minutes

Borden Ladner Gervais

# U.S Regulatory Developments

- US FinCEN has stated that that any administrator or exchanger of bitcoins (or other convertible digital asset) must be a registered MSB under money transmitter regulations.
- Various U.S. state regulators have followed FinCEN's lead and required registration (e.g. the “BitLicense” in New York State).
- New York’s proposed regulations require digital currency companies to record the identity of their customers and all Bitcoin transactions and inform regulators if they observe any activity involving Bitcoins worth $10,000 or more.
- CFTC approved trading platform for Bitcoin derivatives trader, swap contract approvals to follow.

Borden Ladner Gervais

# Lending Implications – Bitcoins as Collateral

***Personal Property Security Act***

- "Goods" – tangible personal property.
- "Intangible" – personal property that is not goods, chattel paper, documents of title, instruments, money or investment property.
- Bitcoins are not "goods", "chattel paper", "documents of title", "instruments" or "money".

***Securities Transfer Act***

- Bitcoins are not "investment property"

**<u>Therefore, Bitcoins are "intangibles"</u>**

Borden Ladner Gervais

# Taking Security in an “Intangible”

## Enforceable security interest:

1. Attachment
2. Perfection

## Attachment:

1. Value given
2. Debtor has rights in the collateral
3. Signed security agreement

## Security Agreement

- Sufficiently describe collateral

Borden Ladner Gervais

# Taking Security in an "Intangible" (Cont'd)

## Issue of Adequate Information to Enable Enforcement

- To enforce a security interest where Bitcoin is the collateral, the secured party would need to know the holder's private key to access the holder's wallet.
- Anonymity of Bitcoin transactions
  - Blockchain will show the wallet address making or receiving the payment, but not the identity of persons behind a wallet address.
  - Holder of key can make anonymous transaction.
- Trust between debtor and lender will be a key factor.

## Possible Solution and Opportunity for Some?

- Escrow Arrangements
- Multi-key Addresses

Borden Ladner Gervais

# Taking Security in an "Intangible" (Cont'd)

## Major Risks Associated with Taking a Security Interest in Bitcoins

- Volatility – significant fluctuations in debtor's asset base.
    - Different than taking security interest in securities?
- Uncertainty – loss or theft.
- Control issues/prevention of loss.

Borden Ladner Gervais

# Revolution and Opportunity in Context

- **Revolutions are best recognized in hindsight. They are rarely instantaneous events.**
  - a) the invention of money occurred over millennia;
  - b) the adoption of fractional reserve banking over hundreds of years; and
  - c) the development of mobile payments in a decade.
- **Bitcoin will continue to capture imaginations and speculation, but it clearly has sufficient attention to be transformative for mainstream payment processing, business transactions and lending.**
- **Whether Bitcoin leads to social anarchy….TBD**

Borden Ladner Gervais

# THANK YOU

**Ross McGowan, Vancouver**
T: 604-640-4173 / E: rmcgowan@blg.com

**Andrew Hodhod, Montreal**
T: 514-954-3140 / E: ahodhod@blg.com

Borden Ladner Gervais