BLOCKCHAINS AND MONEY LAUNDERING

An overview of the importance of effective anti-money laundering techniques in the world of cryptocurrencies and blockchain, with specific focus on detection methods and regulatory requirements.

Joseph Mari, CAMS, CBP
Peter Warrack, CAMS, CBP, CFE
AML Risk Intelligence, Bank of Montreal
Disclaimer:

The views and opinions expressed in this article are those of the presenters and do not necessarily reflect the official policy or position of any agency of Bank of Montreal.

Examples of analysis performed within this article are only examples. Assumptions made within the analysis are not reflective of the position of the Bank of Montreal, its subsidiaries or affiliates.
Overview

- Introduction
- Money Laundering 101
- AML Compliance
- Transaction Environments
- Case Study – First Canadian Law Enforcement Cryptocurrency Seizure
- Peer2Peer Exchanges
- Cryptocurrency ATMs and Cash
- Synthetic Identities (SYIDS)
- Identifying Bad Actors
- Education and Collaboration
- Recap
- Closing Remarks
Introduction
Introduction

- Under Canadian law*, regulated entities, (incl. banks) are required to identify and report suspicious transactions (or attempts) suspected to be related to the commission of money laundering or terrorist financing offences.

- The law doesn’t differentiate between cash, wires, cheques or cryptocurrency transactions.

- Cryptocurrencies are relatively new to AML and Law Enforcement and require a new knowledge base to identify and investigate suspicious transactions.

- This presentation outlines some of the AML and Law Enforcement challenges that are faced.

* Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)
Money Laundering 101

In simple terms money laundering is taking ‘dirty money’, i.e. money derived from crime and making it *appear to be clean* (from a legitimate source). Money laundering typically occurs in three *linear* stages:

- **Placement** - Cash from drug dealing ‘placed’ into the traditional financial system, e.g. deposited into an account at the ATM.

- **Layering** - Once ‘placed’ funds are split or moved between other accounts or products, e.g. funds from ATM deposits are emailed transferred to another bank and used to purchase an investment product.

- **Integration** - Investment is cashed out and used to buy a house, which is then sold, funds now have more legitimacy and the audit trail is harder to follow.
4 Stages of Money Laundering

The 3 stage model is a simplistic one and events do not always flow in that order, e.g.:

A fraudulent loan generates funds within the financial system credited to the suspect’s bank account, i.e. the funds are already ‘placed’ within the financial system. (Similar scenarios could occur with cryptocurrencies).

By definition, all money laundering requires a predicate offence from which the illicit funds are generated.
Money Laundering in Bitcoin – Reverse Smurfing

Initial bitcoin address

The blockchain is a gift to law enforcement, (if they can identify the wallet holders) as every transaction is visible and traceable – *is it really?*

Reference: Journal of Theoretical and Applied Information Technology 20th Jan, 2016 Vol83 No.2
AML Compliance

- A component of AML Compliance is known as **Know Your Customer (KYC)** and requirements may differ jurisdictionally.

- Generally, the challenges of knowing a customer are the same for any financial product. This includes if the product is opened online, e.g. a Bitcoin Wallet.

- What makes bitcoin unique is the varying degrees of **visibility** of a bitcoin wallet holder’s identity versus traditional banking products. For example, a wire transaction includes the names of both the remitting and receiving parties.

- The identity of a bitcoin wallet holder is more difficult to decipher, e.g.: 19HGYSRWiSKrRCybsMbcWDqZpSRj5GQ5bm and associated IP addresses can be masked or ‘spoofed’, e.g. stealth addresses.
Transactional Environments

- Cryptocurrency presents a new dimension in the world of remittances.
- Blockchain allows for trustless and seamless value transfer between two parties.
- At this stage in the evolution of cryptocurrencies, traditional outlets are largely still required as onboard and offboard conduits between fiat and cryptocurrencies.
- Currently, AML professionals are presented with two transactional environments, Interactive and Contained.
- The main difference between the two environments is the involvement of identifiable institutional parties (i.e. banks, exchanges, etc.)
Transactional Environment - Interactive

Drug purchase by Suspect 1 paid in bitcoin to Wallet ‘A’

1. Wallet ‘A’

2. Wallet ‘B’ (Bitcoin Exchange)

Transfer to Bank 1

3. Bank 1

4. Wire Transfer to Bank 2 Account, owned by Wallet ‘A’ Owner

Digital Environment

Traditional Banking Environment

Legend
- Value Transfer
- Account Ownership
Case Study – First Cryptocurrency Seizure by Law Enforcement in Canada (Interactive)

2015 Toronto Police Case:

- Info received re: suspected ‘Dark Web’ firearms purchase.
- Controlled delivery of disabled firearm is arranged and suspect arrested.
- During search of his apartment suspect admits to selling firearms and drugs on the Dark Web and receiving payment in bitcoins.
- The suspect was found to be receiving deposits from well-known cryptocurrency exchanges, as well as cash deposits.
Case Study - Transactions

- Funds were depleted in cash and through payments to the suspect’s credit card.

- Computer is seized and searched by Toronto Police Cyber Crime Section and a bitcoin wallet is discovered containing 288 Bitcoins ($84,000 - at the time of arrest).

- Law enforcement challenge – How to seize and how to process the seized bitcoin.

*Note:* A second cryptocurrency seizure occurred in Calgary on 6th June, 2016.
Case Study - Challenges

- **How to ‘Seize’** (take control of) – Law Enforcement does not have a formal bitcoin wallet, nor does the Seized Property Management Directorate (SPMD).

- If not seized, can bitcoin be **restrained**? (Yet to be legally tested.)

- Questions around conversion to fiat currency and volatility in value (particularly if suspect is found to be not guilty and the funds have to be returned), or if court orders some of the funds to be used to pay legal fees.
Transactional Environment - Contained

- Peer2Peer exchanges / Cryptocurrency ATMs.
- Cryptocurrency miners.
- Wallet providers.

Digital Environment (Outside Traditional Financial System)

1. Gun purchased by Suspect 1 paid in bitcoin
2. Drugs purchased by Suspect 2 etc.
3. Value Transfer
4. Wallet ‘C’
5. Wallet ‘D’
6. Purchase at Online Retailer in bitcoin.

Legend
- Value Transfer
- Account Ownership
Peer2Peer Exchanges

Activity involving Peer to Peer (P2P) bitcoin exchanges represent significant risk for traditional financial institutions (FI).

Lack of transparency creates inability to enact proper KYC.

Many are using personal accounts at FIs for informal MSB services.

Banks need to differentiate between individual and commercial use of accounts.
Cryptocurrency ATMs and Cash

“Cryptocurrency is the most anonymous form of receiving and sending payment. Unlike a traditional credit card your name and info is NOT required. When you buy from our ATMs, we have no idea who you are or what you do with your money, ever.” (Source Cryptocurrency ATM Provider, Canada)

- **Note**: Not all Cryptocurrency ATM operators operate like this or do not require identification.

- Let’s look at an example of how this ATM could be used by criminal ‘A’ to purchase an illegal gun from Criminal ‘B’. They met in a forum on the Dark Web.
Example (‘A’ buying a gun from ‘B’)
Synthetic Identities (SYIDS)

A synthetic identity is one that doesn’t exist in real life, i.e. the person was never born and differs from stealing the identity of a real person (ID Theft).

According to Toronto Police, as many as 200,000 SYIDs exist in Ontario, many supported by real Ontario drivers licences obtained through corruption.

SYIDs are used to open bank accounts, obtain credit etc. – they can also be used to open Crypto Wallets.

Identifying Bad Actors

- Not everyone in the blockchain space is a criminal.

- Blockchain technology requires its own set of AML solutions.

- Identifying “bad actors” involves a mix of searching for traditional AML typologies, as well as employing analytics.

- Establishing a list of common indicators for suspicious activity is necessary.

- Newly emerging blockchain companies are offering AML/TF solutions.
Identifying Bad Actors - Technical Solutions

- Several companies in the blockchain space offer technical solutions to identify illicit activity.

- Blockchain analytics offer the following possibilities;
  - AML Visualization
  - Bitcoin Tracing
  - Dark Wallet Tracing

- Approximately 10 to 20 cryptocurrency AML related analytics companies in the market.
  - Chainalysis
  - Elliptic
  - Blockseer
Identifying Bad Actors - Indicators

- Funds deposited into an account with **rapid depletion** via cash, email, or wire transfers.

- **Frequent deposits/withdrawals** from cryptocurrency exchanges.

- Unusual **3rd party** deposits, often structured in nature, from online wallets or payment processors.

- **Rounded** dollar amounts.

- Transactional values that total **5, 10** or **25** (soon to be **12.5** after halving) bitcoin.
Identifying Bad Actors - Indicators

- Frequent payments/debits involving credit cards.

- Search emails for any associated identification handles through open source investigation.

- Unusual unrelated business activity associated to a previously identified entity.

- Involvement of foreign jurisdictions deemed to be “high risk”.

- Transactions related to law firms.

- Vape companies.
Education and Collaboration

- Education and collaboration are paramount to the proliferation of blockchain and cryptocurrency amongst traditional institutions (banks, governments, etc.)

- Blockchain education is recommended for traditional institutions.

- Collaboration with law enforcement and regulators is encouraged for blockchain companies.

- Education and collaboration do intersect, however approaches vary.
Education and Collaboration

Legacy Financial Institutions – (Education)

- Increasing blockchain and cryptocurrency knowledge will allow for:
  - A more efficient approach to identify money laundering.
  - Increased revenue.
  - Providing a better customer experience.

Fintech Sector– (Collaboration)

- Collaborating with law enforcement provides many benefits;
  - Increasing awareness.
  - Dispelling common myths.
  - Influencing legislative outcomes.
  - Opening new relationships.
  - Enacting social good.
BITCRIME is a bilateral German-Austrian research project concerning the prevention and prosecution of organized financial crime committed with virtual currencies. The project is funded by the German Federal Ministry of Education and Research (BMBF) and the Austrian Federal Ministry for Transport, Innovation and Technology (BMVIT).

**Goals:**
- Develop innovative and workable approaches toward regulation of virtual currencies.
- Develop actionable, internationally applicable, and interoperable solutions for Europe and beyond.
Collaboration Example - Blockchain Alliance

The Blockchain Alliance is a public-private forum created by the several representatives from the blockchain community which consists of a broad coalition of companies and organizations.

Goals:
- Provide a forum for open dialogue between industry, law enforcement and regulatory agencies.
- Serve as a resource for law enforcement and regulatory agencies.
- Provide education, technical assistance, and periodic informational sessions regarding cryptocurrencies.
Recap

- Importance of AML & KYC.

- Transactional environments: Interactive vs. Contained.

- Success in identifying “bad actors” pays off.

- Leverage blockchain analytics.

- Establish indicators, cross reference with traditional AML typologies.

- Importance of Education and Collaboration.
Closing Remarks