Virtual Currencies: the birth of the blockchain

An overview of the blockchain technology vis-à-vis virtual currencies and its effect on Anti-Money Laundering law

What is a virtual currency?

- Non-tangible
- Cryptocurrency/Non-cryptocurrencies
- Centralised/Decentralised
- Open/Closed
- Convertible/Non-convertible

Some examples of Virtual Currencies before Bitcoin

- E-Gold
- Second Life
- Amazon Points
- Facebook Credits
- World of Warcraft gold

Centralised

The advent of Bitcoin

- In 2009, Satoshi Nakamoto issued a white paper regarding a **decentralised** virtual currency
- First virtual currency to solve the double-spend problem
- First completely decentralised virtual currency

What is Bitcoin?

- Common perception: A **Peer-to-Peer** (P2P) **decentralised** virtual currency deriving from an **open-source** software based on a **consensus** system
- Derived from **mining**
- Based on the **blockchain** system

Solve the following calculation:

- (8 x 2 x 2) ÷ 4 x 10 x (2 ÷ 2 x 1)
  - 32 ÷ 4 x 10 x 1
    - 8 x 10 x 1
      - **80**

The Blockchain

- Bitcoin is built upon the so-called "blockchain" system
- A block is essentially made up of all the transactions conducted in a 10-minute window on the Bitcoin network
- The transaction data is gathered into "blocks", and the solved mathematical calculation by the winning miner confirms the transactions that have taken place in that block and validates them

Characteristics

- No central authority
- No intermediaries
- Everyone is his own bank
- No exchange rates
- Low transaction fees
- Value relies purely on demand and supply
- Speedy transaction times

Bitcoin participants

- Miners
- Exchanges
- Retailers
- Service providers
- Users

How are Bitcoins created?

- Bitcoins are created through the **mining** process
- Use computing power to solve complex mathematical calculations and obtain the block reward
- Whoever solves the calculation first gets the block reward and the transaction fees for that particular block
- If 51% of the network agrees that the particular miner managed to solve the algorithm, they will move on to his blockchain, and gradually the whole network will move onto that same blockchain

Transparency

- A log of the transactions conducted is reserved and stamped onto each and every block mined
- The transactions can be seen on websites such as http://blockchain.info
- If the owners of the addresses used for the transaction are known, the sender and receiver can be easily tracked
- Public ledger

Transactions

- Transactions take place via wallets
- Wallets are software programmes which access the blockchain and allow the users to send/receive Bitcoin on their devices
- A wallet can either be local or hosted
- Local = on one's own PC, laptop, mobile phone, etc
- Hosted = on a website offering a wallet-hosting service. This includes exchanges

Addresses

- The senders and receivers are identifiable thanks to their public address, which is a string of letters and integers derived from the wallet's public key
- No private details of the users are required or shown in the transaction details
- The public ledger shows the sender's address, the receiver's address and the I.P. address of the node via which the transaction is transferred
- BTC is therefore "pseudonymous" not "anonymous"

Advantages of the blockchain

1. Public Ledger and oversight
2. Complete log of all the transactions
3. Decentralisation of consensus
4. Automation
5. Public blockchain = near impossible loss of data

Disadvantages of the blockchain

1. 51% attack
2. Blockchain size
3. Hard-forks
4. Confirmation times
5. Decentralisation (who acts in a crisis?)

Uses

1. Bitcoin / Virtual Currencies
2. Smart contracts
3. Smart appliances
4. Automatic reporting
5. The sky is the limit!

Legislation

- EU: VCs tend to have properties that are very similar to those provided by conventional payment service providers (EBA)
- VCs are not e-money
- Outside the scope of 4th AML Directive
- Anonymity and global reach 2 main risks of VCs
- Possible creation of VC solely for ML purposes

Skatteverket vs. David Hedqvist

- Hedqvist wanted to open a Bitcoin exchange
- Preliminary reference on whether Bitcoin is subject to VAT
- ECJ ruled that since the VAT Directive (2006/112/EC) exempts transactions relating to 'currency, bank notes, and coins used as legal tender', and Bitcoin qualifies as **alternative means of payment**, then it is simply an exchange of different means of payment and therefore exempt from VAT.

U.S. Legislation

- Internal Revenue Services (IRS) treats BTC as property and charges capital gains tax on it
- Financial Crimes Enforcement Network (FinCEN) treats Bitcoin as a **currency** and classifies BTC exchanges as money transmitters
- *Securities and Exchange Commission vs. T. Shavers et* – Texan court ruled Bitcoin as a **currency** and declared that Bitcoin investment funds and transactions fall under the Securities Exchange Act
- *New York BitLicense* – first ad hoc regulation

Isle of Man

- Proceeds of Crime Order: imposed AML requirements upon VC businesses, defining them as "the business of issuing, transmitting, transferring, providing safe custody or storage of, administering, managing, lending, buying, selling, exchanging or otherwise trading or intermediating convertible virtual currencies, including crypto-currencies or similar concepts where the concept is accepted by persons as a means of payment for goods or services, a unit of account, a store of value or commodity".

Canada

- In June, 2014, Bill C-31 was passed which amended Proceeds of Crime (Money Laundering) and Terrorist Financing Act (not yet in effect)
- Regulates VCs as Money Service Businesses (MSBs) and thus subject to AML procedures
- No definition of "dealing in VCs"
- VC MSBs required to register with FINTRAC
- Targets both Canadian businesses and entities aiming their business towards Canada
- Banks prohibited from dealing with unregistered VC MSBs
- No threshold for reporting obligation on STs

AML law in other countries

- Most countries treat VCs under the general auspices of AML law and no specific ad hoc legislation has yet been made on such VCs vis-à-vis AML.
- Most legitimate businesses still perform KYC and CDD even though they may not be obliged to do so

Malta

- Ranked as 131st country out of 177 most likely to adopt BTC
- One of the definitions of currency under the PMLA is "any currency, whether or not the same is legal tender in Malta"
- Therefore, BTC seems to classify as a non-legal tender currency and hence caught under the PMLA
- Even if this were not the case, it would be caught under the generic definition: "property of every kind, nature and description, whether movable or immovable, tangible or intangible"

Jurisprudence

- ***Silk Road*** case – Ross Ulbricht operated underground e-commerce marketplace for various illicit items, including drugs
- Bitcoin currency of choice
- Layers of anonymity – BTC Tumbler & Tor
- Ulbricht received a life sentence

Aftermath – Senate Committee

- Patrick Murck: traditional payment systems follow the "person known, transaction unknown" pattern while VCs follow the "person unknown, transaction known" pattern
- Jerry Brito: BTC was not designed from the get-go as an anonymous cryptocurrency; cash is more anonymous
- Mythili Raman: Proper regulation and global coordination key to control VCs properly from AML perspective

Liberty Reserve

- LR was a centralised VC setup primarily as a money laundering mechanism
- Several anonymity tools in place, such as users able to hide account numbers for a small fee, and no direct deposits/withdrawals on the LR website (external exchanges were used)
- Maliciously hid info from Costa-Rican authorities and even fed them false info by creating an alternative computer portal
- Investigative authorities issued the first-ever cloud-based warrant whereby they had the authority to investigate Amazon Web Services irrelevantly of where their servers were located

Chainanalysis Inc.

- A NY "blockchain forensics firm"
- Tracks transactions on the BTC network by flooding it with a lot of nodes
- Partnered up with Europol
- Criticised heavily by active members of the BTC network
- Not the right way to legitimise the system!

The future

- Regulate from an AML perspective only and incentivise VC businesses, including taxation
- Study the effects of VCs closely
- Education
- Recognise the uses of the blockchain
- Include private businesses in regulatory decisions
- Work towards global cooperation
- Regulate VCs, do not regulate the blockchain!
- Admit that the digital era has long since been ushered in and wake up!