CHAPTER 15

HARMONIZING THE LAW OF NEW TECHNOLOGY: DIGITAL CURRENCIES, THE BLOCKCHAIN, DISTRIBUTED LEDGER TECHNOLOGY AND THE LAW

Christine Duhaime*

I DIGITAL CURRENCIES OVERVIEW

Consumer payments and ways of transferring value in Canada and globally have shifted over the last several decades from paper-based media, such as cash and cheques, to card-based media such as credit and debit cards, electronic methods such as pre-authorized payments through ACH, and more recently, digital methods such as digital currencies.

A digital currency is an electronic, or digital, form of a monetary instrument. Such a currency is a product of coding. A digital currency is often mistakenly described as a virtual currency. They are not the same thing. A virtual currency is one that does not truly exist, such as currencies generated by a computer game. In contrast, a digital currency is not fictional but rather it exists as a real creation of computer coding.

There are several types of digital currencies. Bitcoin is a digital currency with a bidirectional flow. Digital currencies with bidirectional flow allow users to buy and sell digital currencies according to the exchange rates with their own national currency and to purchase goods and services using the digital currency. In contrast, digital currency with unidirectional flow allows users to buy digital currency but it cannot be exchanged back to original form.

II BITCOIN

The most prominent form of digital currency is Bitcoin. As a digital currency, Bitcoin operates peer-to-peer and machine-to-machine ("**M2M**"). M2M means that

---

* BA, JD, Executive Director, Digital Finance Institute.

the complete financial transaction is commenced and completed by virtue of computer transactions without human intervention. Bitcoin financial transactions are pure M2M.

Unlike traditional fiat currencies, such as the US dollar, that are issued by national governments and controlled by central banks, Bitcoin has no central monetary authority and is not backed by any central bank, authority or government. The supply of Bitcoin is likewise not controlled by any central governmental authority.

III DIGITAL CURRENCY WALLETS

To use a digital currency, a customer downloads and uses a digital currency wallet. Digital wallets serve a similar purpose as physical wallets or bank accounts – they hold or store value or monetary instruments. There are three methods of using wallets: a software wallet stored on a customer's computer, mobile wallets that run as an app on a smartphone, and web-based wallet services. Like any account, in order to complete a transaction, a user must fund their wallet by purchasing a digital currency such as Bitcoin with real, or fiat currency.

IV WALLET KEYS

There are two keys associated with wallets – a public key and a private key. A public key is a numeric address similar to the combination of a bank account number and a SWIFT code, which is the network address used to send or receive digital currencies. The transactions associated with public keys are on the Blockchain and can be viewed by anyone. Although the public keys do not have names of legal or natural persons publicly associated with them, a Bitcoin address does reveal the number of Bitcoin held in a wallet. This means that anyone can go online to the Blockchain and see the balance in anyone's digital currency wallet. In other words, anyone can see a person's digital currency value, or wealth, which raises privacy concerns and security concerns.

A private key is similar to a PIN code, which must be used to access digital currencies held by a person, either to spend or transfer digital currencies. If a person loses his or her private key, they have completely lost the digital currencies they hold forever. Thus, there are consumer protection and legal concerns that arise with the purchasing, use and storage of digital currencies by the general public who are not warned of, or familiar with, a financial transactional model in which funds may be irretrievable permanently, causing loss of wealth, perhaps economic hardship, and an economic windfall to a digital currency exchange that is not legally subject to account to customers whose funds are irretrievable.

Once a user has a wallet, he or she can buy digital currencies online with real monetary instruments. The purchase and selling price for digital currencies is determined by supply and demand in the digital currency market.

V NO CENTRAL AUTHORITY

The transactions for goods and services bought or sold using digital currencies are not processed through a centralized authority, or clearing house. A Bitcoin transaction is processed through the Blockchain, or by distributed ledger technology.

The Blockchain acts similar to a third party clearing house except that the clearing (or reconciliation and verification of transactions) component is entirely M2M on the Blockchain. The digital component of such transactions is a math-based transfer of one item of value to another, virtually instantaneously on the Blockchain.

Cryptographic software validates each transaction through a process called "mining." Mining is a process whereby computers held by the private sector are used to validate each financial transaction going through the Blockchain. Each financial transaction is verified several times by computer processing during a process called "mining." The verification transactions are sequentially recorded on the Blockchain. The private sector miners who are engaged in the mining process earn revenue by mining in the sense that their Bitcoin wallets are credited with digital currencies for financial transactions verified.

The validation process of transactions performed by mining prevents anyone from double spending, ergo using digital currencies they do not own. The inability, technically, to double spend on the Blockchain gives the Blockchain a measure of financial integrity that surpasses existing financial technology. That is one of the strengths of the Blockchain from a legal perspective.

By contrast, other online currencies or payment systems, such as bank credit cards, involve a central administrator or financial institution middleman. These intermediaries reconcile transactions to identify double spending by a person. But they cannot always prevent it from occurring as part of a real-time transaction like the Blockchain. Digital currency transactions on the Blockchain rely on computer software to perform verification functions, cutting out the institutional go-between in financial transactions and eliminating human intervention and the capacity for errors in [reconciliations].

The Blockchain is a type of distributed ledger because it is similar to an accounting ledger, only it is electronic and online and operates without human intervention during the transactional processing of financial transfers of value. All

of the transactions that are processed through the Blockchain are recorded, linked and dated. The Blockchain's innovation is the existence of a public transactional record without a central authority. If coded with integrity, ethics and pursuant to the rule of law, the Blockchain could be a perfect financial system with integrity built in. The Blockchain is decentralized by nature, i.e., shared by all who are connected to a network. The distributed ledger is similar to a public searchable database of all of a customer's financial transactions ever conducted through their account.

One of the obvious security risks and issues arising from privacy protection, is that if public keys had information identifying each account holder, anyone could look at the Blockchain to see the number of Bitcoin a wallet holder owns (which shows their wealth in that account) and what purchases they made and where, which would reveal their location. Merchants such as Microsoft, for example, provide its Bitcoin address as a merchant to the public and its transactions are accessible, as is its Bitcoin wealth.

The Blockchain also stores every transaction ever executed by any person using the Blockchain historically, allowing anyone to view their financial transactions over time. One benefit of such transparency is the traceability of funds for financial crime purposes; another is for traceability of goods of value in instances where the Blockchain is used for identifying and transacting with certain controlled goods such as controlled narcotics.

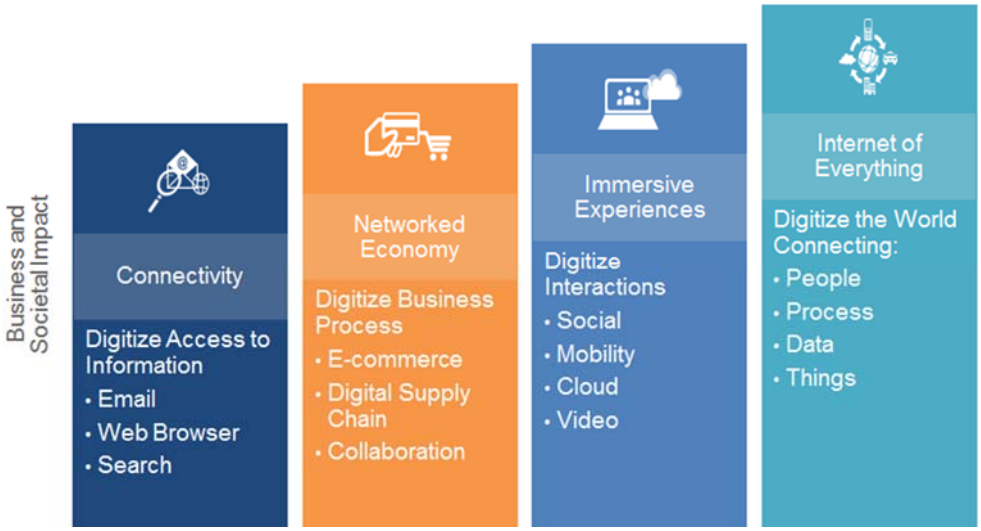
As a result of Bitcoin, for the first time in history, it is possible to buy currency, shop for goods or services and remit money overseas instantaneously, purely M2M without the need for institutional middlemen for almost no fees. For global consumers, Bitcoin eliminates the need for traditional banking services and eliminates banking fees, credit card fees and currency exchange fees, and because it can be anonymous, consumers can conduct financial transactions with privacy and without the risk of identity theft.

VI DISRUPTIVE OF FINANCIAL SERVICES

Bitcoin is incredibly disruptive to the financial services sector. There is no plastic, no paper currency, no intermediaries, no infrastructure, no employees, no management and no oversight or regulation involved. The entire process is via machine and self-generated as a matter of coding. Virtually entire banking infrastructure can be eliminated if financial transactions move to a distributed ledger system. As the world progresses to connectivity and towards the Internet of Everything, practically all services will be digital, including currency. Connecting the payment functions of a connected system like the Internet of Everything will

require a M2M component for payments. Figure A is a representation of the evolution of digitization.

Figure A: Evolution of Digitalization



VII NEGATIVE LEGAL ISSUES

Digital currencies, while promising, have certain legal risks, especially when used as a currency for international transfers of value.

VIII CONSUMER PROTECTION

The biggest legal risk for digital currencies is consumer protection. The private key attached to a digital currency wallet like Bitcoin, is a computer-generated string of letters and numbers that can be easily lost by a consumer. Users all over the world have lost tens of millions of dollars in Bitcoin because they didn't understand the importance of the private key when they set up a Bitcoin wallet. They have no way of ever recovering their money. Digital currency exchanges that accept money from the public, sell and exchange digital currencies, and accept deposits, are not regulated as financial institutions anywhere in the world. Anyone, including a person with a criminal record, can own or operate a digital currency exchange and be entrusted to hold customer funds on deposit.

Digital currency exchanges become unjustly enriched when a customer loses his or her private key and ergo, loses their funds. There are no legal remedies for customers against exchanges when they lose their money via a lost private key. Moreover, unlike a regulated financial institution that is required to hold unclaimed funds in trust or with a central bank, digital currency exchanges have no such legal requirements.

If criminal elements are involved in a digital currency exchange and embezzle customer's funds, there are likewise few remedies available that provide recourse for customers. A number of digital currency exchanges have folded in recent years, causing the loss of tens of millions of dollars to consumers.

There are also consumer protection risks with using digital currency exchanges that may not have sufficient liquidity to repay funds held by customers or sufficient resources to operate in a fiscally or technically secure manner to protect transactions or wallets.

Transactions on the Blockchain or with any digital currency are also irreversible, which means that once a wallet address is used to make a payment, if it's entered incorrectly, the purchaser can't reverse the transaction to recover their funds even if the wrong amount was sent or it was sent to the wrong party. The Blockchain was purposely designed with this feature coded into its programming in order to ensure financial transactions went one way only and could not be reversed. Legally speaking, the irreversibility of a digital currency transaction is incompatible with consumer protection laws in every country in the world, whether the laws are based on Islamic finance, the civil code or the common law. As a result, every financial transaction of digital currency used for the purchase of goods or services is completed in a manner that violates consumer protection laws.

IX FINANCIAL CRIME

Many digital currency exchanges accept purchases of digital currencies with large amounts of cash anonymously. The anonymity is a concern for law enforcement agencies because the financial transactions cannot be monitored, recorded or reported for money laundering or terrorist financing mitigation or to comply with sanctions lists. Purchasing digital currencies anonymously with cash means a person can send funds to anyone anywhere, including a terrorist organization, and can avoid economic and trade sanctions without detection. Digital currency transactions are immediate and irreversible and therefor even if financial crime is involved, the funds cannot be recovered with any facility.

Digital currencies are an ideal vehicle for tax evasion by natural and legal persons. A person could anonymously and instantaneously convert unreported income earned anywhere in the world into a digital currency, such as Bitcoin, and redeem it in a tax haven, such as the Cayman Islands, without reporting or paying taxes to national tax agencies. Such transactions cannot easily be detected by tax authorities. Merchants that accept digital currencies can earn income without reporting it since it does not go through the financial system.

X ACCESS TO JUSTICE

Underlying every society is the premise that the rule of law prevails and that the law exists to grant certain rights and to protect others. The rule of law exists in non-democratic states as much as in democratic states and can be seen as a thread that connects all countries internationally.

One of the legal concerns with digital currency transactions is that they represent the first instance in the world where the rule of law does not necessarily universally prevail. That is because digital currency financial transactions can be made to anyone anywhere anonymously and because such transactions don't touch the existing financial system in the normal course (until cashed out to fiat currency), there is no easily identifiable jurisdiction whose laws would prevail in such transactions.

That has implications for access to justice and operates to deprive users and customers of legal recourse by established court systems. With respect to countries governed by the principles of Islamic finance, financial products and services, such as digital currencies, that do not allow for the resolution of disputes by reference to the law (in this case Sharia law), are illegal.

The failures in respect of access to justice with digital currency transactions impacts the ability of digital currencies to scale into a useable, reliable and legally based system of financial transactions.

There is also no dispute resolution mechanism governing digital currencies or Blockchain financial transactions in the event of a dispute associated with its acquisition, disposition or storage.

XI CURRENCY RESTRICTIONS

Digital currencies are sometimes used to circumvent restrictions in countries like Argentina and China that control the exchange and removal of currency. Given the ability to transfer funds using digital currencies anywhere in the world, digital currencies have the potential to harm the economies of these jurisdictions if there is a sustained and large volume of transactions over time to another country.

This has implications for asset recovery because once assets of digital currency are removed from one jurisdiction, the recovery is practically impossible, in a M2M environment, particularly when the location of where the funds settled is not easy to determine.

XII POSITIVE LEGAL ISSUES

The Blockchain, distributed ledger technologies and digital currencies have important roles to play. As the world's first programmable financial instrument, the

financial applications are vast. The Internet of Everything, for example, will have to intersect with a distributed ledger to effect its M2M transactions. The same is true for future collaborative economies and collaborative cities. The shifting of traditional banking services digitally opens the door to the explosion of new FinTech to bridge the Blockchain technology with traditional financial institutions through digital currencies. The potential for distributed ledger technology and digital currencies in law provides for harmonization of law opportunities across a common landscape where there is, as of yet, no such law in the private law context. Such a harmonized law for digital currencies could be drafted and implemented quickly due to the legal vacuum that currently exists in this area. Such a harmonized model law would inform states on the most appropriate legal regime applicable and would provide worldwide consensus on the law of this emerging legal area, providing legal certainty, legal remedies and a dispute resolution process internationally, helping to provide consumer protection.

Interestingly, although digital currencies are a financial crime risk, the Blockchain can help reduce financial crime. Because every transaction is recorded on the Blockchain, it provides a permanent and public record of global transactions that are not anonymous, in other words a permanent bank of evidence which law enforcement can use for years to come in cases where they may suspect money laundering, tax evasion or other criminal conduct. This advantage in law becomes unavailable when these transactions, however, are anonymous.

The elimination of the double spend problem means that digital currencies can eliminate some forms of fraud, and prevents a person from spending digital value they do not own. These advantages combined mean that securities-related fraud or fraud that occurred in the carbon credit markets in the EU could be eliminated.

Non-anonymous digital currency transactions can eliminate systemic corruption by allowing people to opt out of using corrupt financial institutions where account holders routinely have to pay bank officials for the privilege of cashing a pay cheque or withdrawing funds from their bank account and provides financial freedom for women, especially, who are denied banking services because of social, political, economic or geographical circumstances, for example, because they live in repressive societies where women cannot receive banking services or are victims of human trafficking whose ID is confiscated by traffickers. These benefits assist in the advancement of the law because it brings people into the financial system who otherwise would not be in the system. Having financial services introduces citizens to financial inclusion.

Finally, the distributed ledger system has the potential for smart contracts, which are payments of digital currencies released automatically by the distributed

ledger upon the fulfilment of certain conditions precedent under a contract and can also be used for automated dispute resolution systems programmed to manage certain limited disputes in the future.