## Ethical Issues Regarding the Use of Blockchain

### Introduction

Blockchain technology or more technically distributed ledger technology was developed in 2008.[1] Its distinguishing feature is that, by means of operating through a peer-to-peer network without any central party coordinating the network, it permits the secure transfer of funds, information, and assets without requiring any third-party intermediary financial institutions or central recordkeeping. Blockchain can be used, for example, to create digital registries to record, transfer, and verify asset ownership and to monitor the integrity and authenticity of sensitive documents such as passports or birth certificates.[2] Using tamper-resistant and append-only databases, interactions between parties can be chronologically validated, executed and recorded, remaining available on the Internet for lookup and verification.[3] Blockchain's best known application is to Bitcoin, a crypto-currency that uses Blockchain to process its transactions. Increasingly, however, Blockchains are being used in commercial operations.

Two distinguishing features of blockchain, both having to do with decentralization, are: (1) its strong encryption permits parties and their transactions to remain anonymous and thus free of interference, and (2) its decentralization makes it possible to create organizational structures immune from destruction by an attack on a central institution. As is the case with most new technologies, blockchain creates new possibilities that can be put either to ethical or unethical use.

### Ethical Issues Arising from the Use of Blockchain

*Blockchain Anonymity and Privacy*

We have noted that one of the distinguishing features of blockchain is the anonymity and privacy it provides. Advocates point out how this feature could be put to good use. In countries dealing with widespread electoral fraud blockchain could possibly be used to make vote-rigging much more difficult and provide the safety of anonymity to voters. A worry, however, in advocating such a use of blockchain is what happens if Blockchain stops being anonymous. In such an instance voter records would be publicly exposed and could not be erased.[4]

Advocates also point out that the use of Blockchain could help ensure ethical business practices. For example, Blockchain might be used to discourage blood diamond trade[5] and to prevent synthetic diamonds being sold as natural diamonds. A problem, of course, is that the certainty provided by Blockchain only applies to events that occur inside the Blockchain. There inevitably exists at some point an interface between the Blockchain and the real world. The information put into a Blockchain cannot be altered once within the Blockchain, but this in no way guarantees the trustworthiness of the information it receives.

The fact that Blockchain is not regulated and lends itself to anonymity makes it very attractive to cyber-criminals and rogue nation states wishing to avoid traditional financial institutions by means of using crypto-currencies such as Bitcoin. Allegedly, North Korea has helped fund it nuclear and missile programs through hacking crypto-currency exchanges.

The development of cryptocurrencies depending on Blockchain can be directly correlated to the increase in cybercrime.[6] Although ransomware is not a product of Blockchain

technology, the fact that cryptocurrencies make it easier to be paid electronically allows ransomware to be employed more successfully.[7]

Companies such as Chainalysis[8] have begun to help victims of cybercrime on the Bitcoin Blockchain. These companies work to reveal the structure of cyber-criminal organizations and monitor when Bitcoin is transferred into government-issued currency. At this point of transfer there exists the possibility of revealing the true name of the criminal or an IP address that can be tracked. This has led cyber-criminals to avoid using the Bitcoin Blockchain and move to alternative Blockchain crypto-currencies such as Monero, which guarantee much greater anonymity.[9]

We have noted that one of distinguishing features of Blockchain is its anonymity. In light of its use by cyber-criminals it is fair to raise the question of whether the anonymity provided by Blockchain is ethically justified. Currently, Blockchain is largely unregulated. Societies and governments need to develop regulatory policies aimed at integrating Blockchain into legal and ethical frameworks. One of the crucial questions that needs to be addressed is to what degree anonymity should be permitted in Blockchain transactions.

*Blockchain and the Right to be Forgotten*

The *General Data Protection Regulation* (GDPR)[10] passed in Europe in 1995 affirms the right to be forgotten. Other countries have similar legislation. The right to be forgotten is distinct from the right to privacy. Whereas the right to privacy concerns not having information made public, the right to be forgotten concerns the right to have once public information become private, that is to say it is the right to have information once public, removed from internet searches and other directories.

The concern underlying the assertion of the right to be forgotten is that certain information about behavior can unfairly affect a person's reputation and interests indefinitely if not removed from the possibility of public scrutiny. Thus, for example, in Canada the *Youth Criminal Justice Act* (YCJA) protects the privacy of juveniles who are accused or found guilty of a crime by keeping their identity and other personal information confidential. The Act prohibits any publication of information that would identify a juvenile's involvement in the criminal justice system and restricts access to their youth records. After a length of time which depends on the severity of the offence and whether a sentence was imposed, and if no offence is committed in the meantime, the record is sealed and/or destroyed.[11] Similarly, depending on the offence, convicted adults can apply for record suspensions whereby a person's criminal record is sealed.[12]

The fact that information within a Blockchain can never be destroyed raises ethical issues regarding the use of Blockchain technology. Currently, Blockchain technology is mainly used as a vehicle for cryptocurrency, but its wider application as a means of record keeping could place it in conflict with the right to be forgotten. For example, law enforcement agencies might find Blockchain effective in sharing information and guaranteeing chains of evidence, but this would come at the cost of individuals never being able to have their criminal records expunged. Even more worrisome is that Bitcoin's Blockchain has been used to store links to images and lists of websites of child abuse.[13] The advantages of Blockchain technology that make keeping permanent records possible must be weighed against the fact that this same technology also enables destructive and highly illegal material to be made permanently available.

*The Environmental Impact of Blockchain Mining*

Blockchain miners earn cryptocurrency credits by verifying transactions that use that cryptocurrency. Without going into the details of how Blockchain mining is done, it is enough to note that Blockchain transactions rely on extremely complex algorithms that require enormous amounts of computing power. Blockchain mining accounts for roughly .25% of the world's energy consumption, which is more energy than the country of Switzerland uses in a year[14] and the carbon footprint of Blockchain mining is comparable to that of the country of Denmark.[15] China is the world leader in Blockchain mining, with most of the electricity it uses being generated by coal. Because of its immense use of electricity some regions in the U.S.A. have stopped allowing Blockchain mining in order to be able to supply enough electricity to meet the needs of ordinary consumers.[16]

*The Danger of a 51% Attack*

An additional danger attends the use of public Blockchain technology, namely the possibility of a 51% attack. A 51% attack is possible when a single actor possesses over 50% of a Blockchain's computing power. Possessing a majority of a Blockchain's computing power would effectively undermine its decentralized nature. Depending on how a Blockchain was being used, this could allow a controlling entity to manipulate events; for example, financial transactions or election results. 51% attacks have been successful against several cryptocurrency Blockchains, including Bitcoin Gold and Litecoin Cash.[17] If Blockchain technology is to be widely employed it is necessary that measures be put in place to protect Blockchains from such attacks.

**Blockchain and the Real-World Interface**

A great attraction of using Blockchain technology is that so long as a contract does not require accessing data outside the Blockchain it can self-execute within the Blockchain without any need for intermediaries or arbitrators. Software algorithms with a Blockchain can guarantee that transactions will occur once predefined conditions corresponding to the terms of the contract are met. Such a contract is 'smart' inasmuch as it can be entirely executed within a Blockchain without any need for trusted third-party involvement to guarantee that the requirements of the contract have been met. Business can thus be done in a trustless environment, since such contracts make non-compliance impossible.

This is true, however, only to the degree that transactions occur within a Blockchain. It is for this reason that most 'smart' contracts operate in terms of an automatic cryptocurrency payment triggered by another on-chain event. If the execution of a smart contract, say payment, needs to be set in motion by something taking place in the real world, say the delivery of material goods, then trustworthy data concerning off-chain facts must be entered into the Blockchain. Similarly, if a smart contract is to set in motion an event in the real world, say access to material goods upon a fee having been paid, then the Blockchain must interact with a real-world device or service. Blockchain technology does not, therefore, entirely do away with the need for trustworthy intermediaries.

Such intermediaries are known as oracles.[18] Their task is to furnish the real-world data that trigger Blockchain contracts in a secure and trusted manner. Once the required real-world conditions are met the oracle inputs the necessary information into the Blockchain. Three

different types of oracles can be distinguished: software oracles, hardware oracles and human oracles.

Software oracles are computer programs that extract the real-world data needed by Blockchain contracts from trusted online public sources and then input that data into the Blockchain. Such programs provide a public and verified declaration on the authenticity of the contents of secure web pages, thus providing a means of inputting reliable data into a Blockchain.

In many instances, the real-world data necessary for the execution of Blockchain contracts is not publicly available and cannot be automatically retrieved from online data sources. An example would be where the condition for payment is that certain goods have in fact been delivered. Such facts require local verification in real time. If this verification is to be done automatically this requires technological hardware, known as hardware oracles, that can input information to Blockchain contracts.

In still other instances, where types of contractual performance are not computationally verifiable human oracles are necessary. Humans are better able to parameters that are not computationally verifiable or where contractual performance must be evaluated holistically rather than by measuring a specific parameter. Thus, for example, Matija Damjan argues that "insurance companies . . . will probably continue to rely on human claims adjusters rather than establish complex sensor systems to do their task because humans can inspect a wide range of damage types and are at the same time better suited to assess the validity of a claim and suspect a case of insurance fraud."[19]

**Going Forward**

Forecasts concerning the effects of new technologies routinely waffle between exaggerated fears and exaggerated expectations. The consequences of new technologies are not yet known, making possible all sorts of predictions ranging from apocalyptic to utopian. What does seem clear is, as is the case with many other forms of technology, that Blockchain technology is basically ethically neutral, which is to say that it can be used by malicious agents, as well as morally virtuous agents. The same features of Blockchain which could help mitigate election fraud and ensure transparent trade tracing can equally be exploited by cyber criminals to launder dirty money. Given that Blockchain is a new technology, the regulatory frameworks needed to ensure it is not used unethically are still in the process of being developed. Clearly, national and international legal systems will need to be modified in order to deal with new issues and problems attending the use of Blockchain.

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

http://gazette.gc.ca/rp-pr/p2/2019/2019-07-10/html/sor-dors240-eng.html

On July 10, 2019, each of the regulations of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) were amended and will become effective June 1, 2021. The aim of these amendments is to modernize the Act, to take account of Fintech industries[20] and virtual, i.e. cryptocurrencies, the overall purpose being to enhance Canada's anti-money laundering and counter-terrorism financing regime.

Under an amendment, the definition of 'virtual currency' is now "a digital representation of value that can be used for payment or investment purposes that is not a fiat

currency [fiat currency is money whose value is backed by the government which issued it] and that can be readily exchanged for funds or for another virtual currency that can be readily exchanged for funds" or "a private key of a cryptographic system that enables a person or entity to have access to [such] digital representations of value."[21]

When the amendments become effective, those dealing in virtual currencies must register with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). FINTRAC's mandate is "to facilitate the detection, prevention and deterrence of money laundering and the financing of terrorist activities, while ensuring the protection of personal information under its control."[22] Dealers in virtual currencies must register with FINTRAC as money services businesses (MSBs) and meet PCMLTFA requirements which include having in place a compliance program.

---

[1] Damjan, Matija. "The Interface Between Blockchain and the Real World." *Ragion Pratica*. Vol 51, Dec 2018, 380.
[2] Melanie Swan/Primavera De FilippI. "Towards a Philosophy of Blockchain" *Metaphilosophy* Vol. 48, No. 5, October 2017, 604.
[3] Melanie Swan/Primavera De FilippI. "Towards a Philosophy of Blockchain" *Metaphilosophy* Vol. 48, No. 5, October 2017. 603.
[4] Wilkinson, Troy. "Blockchain Ethics" 115-126 in Stückelberger, Christof/Duggal, Pavan. *Cyber Ethics 4.0*. (Geneva Switzerland: Globethics, 2008) 121.
[5] The term 'blood diamonds' refers to diamonds which are mined in a war zone and illegally traded to fund conflict.
[6] "Blockchain Ethics," 117.
[7] Ibid.
[8] https://demo.chainalysis.com/
[9] "Blockchain Ethics," 117.
[10] https://gdpr-info.eu/
[11] https://www.justice.gc.ca/eng/cj-jp/yj-jj/tools-outils/sheets-feuillets/recor-dossi.html
[12] http://www.rcmp-grc.gc.ca/en/managing-criminal-records
[13] "Blockchain Ethics," 120.
[14] https://www.cbeci.org/, https://www.theverge.com/2019/7/4/20682109/bitcoin-energy-consumption-annual-calculation-cambridge-index-cbeci-country-comparison
[15] https://digiconomist.net/bitcoin-energy-consumption

[16] https://jsis.washington.edu/news/the-political-geography-and-environmental-impacts-of-cryptocurrency-mining/
[17] "Blockchain Ethics," 123.
[18] Damjan, Matija. "The Interface Between Blockchain and the real world" *Ragion Pratica* Vol 51, Dec 2018, 388.
[19] Ibid. 392.
[20] 'Fintech' (financial technology) is the term used to describe new technologies, e.g. AI, blockchain, and data science, which compete with traditional methods of delivering financial services.
[21] As quoted in https://www.mccarthy.ca/en/insights/articles/final-amending-regulations-issued-under-proceeds-crime-money-laundering-and-terrorist-financing-act
[22] https://www.fintrac-canafe.gc.ca/intro-eng