Table of Contents

I. Introduction 1

II. Blockchain and Mining 4

III. Law, Blockchain-based Transactions, and Challenges 7

A. Complexity 7

B. Digital Contracts or Smart Contracts? 9

C. Offer, Acceptance, and Freedom of Contract 12

D. Unconscionability 15

E. Smart Contracts as Valid Legal Contracts in Equity 19

F. A Feature of Blockchains: Pseudonymity in Transactions 21

G. The Decentralized World and the Rule of Law 23

H. Ethereum and Attempts to Use Smart Contracts 29

I. Examples of Fraud 32

J. Regulating the Blockchain Technology 35

K. Environmental Concerns 40

IV. Conclusion 43

Appendix “A” 45

Bibliography 46

Crypto Meets Contracts: Navigating Legal Challenges in Blockchain and Cryptocurrency Transactions

I. Introduction

Using digital currencies to complete real-world transactions has been a matter of debates in the past decade. Think of digital currency as the equivalent of cash in the virtual world. Digital currency is frequently referred to as cryptocurrency ("crypto"). Cryptocurrencies reside on Blockchains. Blockchain is a fairly recent technological innovation. There are countless arguments and analysis about its future and how it can change the way we work and live in modern times. Some businesses have started to accept digital currencies as a method of payment. In 2021, Starbucks made headlines by announcing it would allow customers to pay for their coffee by Bitcoin[1] rather than traditional currencies. Bitcoin is the most widely recognized digital currency and became an accepted method of payment at Starbucks through partnership with *Bakkt*[2] - a crypto platform that enables its users to manage their crypto assets[3] and pay for their goods and services. In other words, if the person ordering coffee pays Starbucks Bitcoin, it does not matter if they have fiat money[4] in their pocket or not; they still leave the store with their coffee in their hands.

This paper takes the Starbucks example as a springboard for thinking about the legal and commercial concerns surrounding this fiat-blockchain convergence. If the crypto transactions work for

---

[1] Jeanette Settembre, "Starbucks drinkers can now pay for coffee with Bitcoin via Bakkt digital wallet app" (2 April 2021), online (news): <fox2detroit.com> [perma.cc/364P-XM4T].

[2] [Unknown author], Bakkt, "Custody, Trading & Onramps for Crypto" [undated], online: <bakkt.com> [perma.cc//GZS3-6KLZ].

[3] "The term 'crypto assets' is generally used to reference a broad range of digital assets with a variety of properties and/or use. The term 'cryptocurrencies' refers to a specific type of crypto asset, which is generally designed to be used as a medium of exchange, like the way we use fiat currencies (a.k.a. government-issued money) to purchase goods and services." See BC Securities Commission, "Test Your Crypto Asset Knowledge" (accessed November 2024), Quizzes, online: <investright.org> [perma.cc/UX58-SE2A].

[4] "Fiat money" refers to traditional forms of currency, such as the US or Canadian dollar.

Starbucks, then would they work for every other type of transaction? An exchange of currency for a cup of coffee is an example of the simplest form of a contract. This purchase has the essential elements of a contract which include offer, acceptance, and consideration. Starbucks stores are putting the offer to the world, at every corner of every major city. The acceptance occurs when customers place their order. The consideration is the money paid by customer and coffee delivered to them by the Starbucks employee. After April 2021, the consideration can be the Bitcoin on the blockchain. This means that blockchain is the crucial element in the execution of this simple contract. The question is whether similar and regular use of cryptocurrencies in *complex* transactions would be equally possible, efficient, and secure? This is the question that drives this paper.

Transactional contracts dominate today's complex commercial world. Other than for daily grocery shopping or buying a cup of coffee, people and entities rarely use simple form transactional contracts. The Starbucks example might remind us of early forms of contracts where people in small communities would exchange goods for services or for other goods. Today, multiple factors that may render such simple transactions impractical, including the lack of multi-faceted negotiations.

Blockchain has uncertain and evolving aspects in both law and technology. One area of technological development is focused on improving transactions on blockchain. Using Bitcoin for daily transactions without an intermediary platform such as *Bakkt* has delays that makes it impractical for retail purchases; it takes at least ten minutes for a transaction to complete on the Bitcoin blockchain. Transactional delays on the Bitcoin blockchain may be tolerable and inconsequential for international transfers,[5] but they are impractical for day-to-day dealings. An intermediary platform, such as *Bakkt,*

[5] Casey Watters, "When Criminals Abuse the Blockchain: Establishing Personal Jurisdiction in a Decentralised Environment" (2023) Laws, 12, 2, 33, online: <mdpi.com> [perma.cc/A6PH-3P37].

facilitates Bitcoin daily transactions through its trade execution features. Beyond emerging intermediary platforms, blockchain developers are continuously introducing new blockchains and cryptocurrencies that have configurations to address transactional challenges including inefficiencies, technological issues, and delays. For example, Ethereum blockchain processes transactions faster than Bitcoin.[6]

On the parallel grounds, there are constant legal challenges arising from uncertainties about how blockchain transactions uphold relevant legal principles, such as principles of contract law. In Canada, regulation of crypto markets and trades are not unified and have multiple layers. Additionally, some governments have recognized that mining crypto[7] raises environmental concerns.[8] Despite these challenges and controversies, blockchain technology is likely to persist alongside traditional forms of contracts and transactions. As with every other evolving technology in the past century, law and society will adapt to address the challenges arising from modern technologies while finding ways to benefit from them. To lay down the groundwork for exploring these challenges, this paper will first examine blockchain technology. It will then examine its features, challenges in law, regulatory considerations, and environmental impact.

---

[6] Wesley Esbertseet et al., "Replacing Paper Contracts With Ethereum Smart Contracts, Contract Innovation with Ethereum" (10 June 2016) at 6, online (PDF): <allquantor.at> [perma.cc/62NN-UCSH].

[7] Part II of this paper discusses "crypto mining".

[8] Such as heat and carbon dioxide emissions. Last section of this paper further discusses environmental concerns arising from this technology.

II. Blockchain and Mining

Understanding the basics of software architecture is crucial for grasping how blockchains work. The architecture of software is fundamental to its function.[9] It dictates how the system operates to achieve specific goals. There are two primary software architectures: centralized and decentralized.

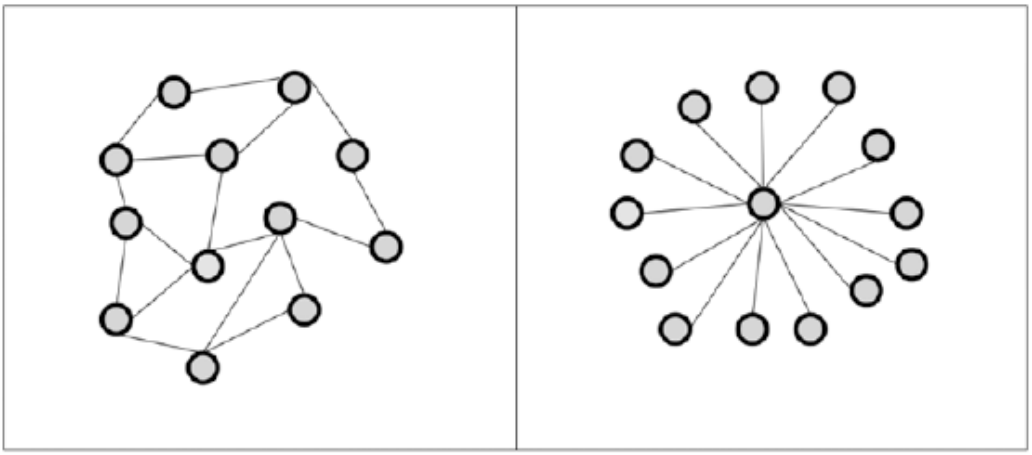

Figure 1. Distributed (left) vs. Centralized (right) system architecture. [10]

In "Figure 1" directly above, circles represent "nodes" in networks. Nodes are points where computers or devices connect to exchange and validate data. Nodes are crucial in both centralized and decentralized systems as they ensure the proper functioning of the network. In technology language, the terms "node" and "peer" are used interchangeably. "Peer" refers to participants in a decentralized network. In a decentralized network, participants are in equal positions and directly communicate with other peers.[11]

---

[9] Daniel Drescher, *Blockchain Basics, A non-Technical Introduction in 25 Steps*, Germany, Apress, 2017. Drescher in this book provides 25-step as a path to build up knowledge about the blockchain and one of the steps introduces software structures.

[10] *Ibid* at 11.

[11] *Ibid* at 15.

The blockchain technology attracted significant attention when an unidentified person, or persons, called "Satoshi Nakamoto" proposed Bitcoin blockchain in 2008 and launched it 2009.[12] Satoshi Nakamoto combined two earlier technologies of hashing mechanism[13] and public key infrastructures[14] and created a secure method of tracking money transfers and ownership on the blockchain. A blockchain is a software with decentralized architecture. As the name entails, it is a chain of blocks. Each block contains specific data (such as transaction details), a unique hash (think of hash as a digital fingerprint)[15], and the hash of the previous block.

The blocks connect in sequence through the hash on the previous block and the current block. The hash is always a unique length of fixed characters that represent data; it is always unique to a specific input but is always the same length, regardless of the size of the data being hashed. Hash means a process that converts input data to a fixed-length string of characters at random. Further, blockchain is a distributed ledger storing the record of every transaction that is open to anyone on the chain. One notable feature of the Bitcoin blockchain is its security and integrity. This integrity is due to the Blockchain's protocol[16]—a set of rules that governs how data is received or shared on the

---

[12] [Unknown] "Bitcoin P2P e-cash paper" (13 November 2008), Satoshi Nakamoto Institute, online: <satoshi.nakamotoinstitute.org> [perma.cc/WTK5-VUEM]. See also Florence G'sell & Florian Martin-Bariteau, *The Impact of Blockchains for Human Rights, Democracy, and the Rule of Law* (Council of Europe, 2022) at 8, online (PDF): <edoc.coe.int> [perma.cc/ZR2Z-ELSE].

[13] Drescher, *supra* note 9 at 72.

[14] Public key enables the encrypted data transfer. It is usually a long code. Public key is shared on the network and other users have access to it. See *ibid* at ch 11 "Hashing in the real world". See also Nick Szabo, "Formalizing and Securing Relationships on Public networks" (1 September 1997), online (HTML): <firstmonday.org> [perma.cc/5QAK-W2VX].

[15] Drescher, *supra* note 9 at 71.

[16] "A protocol in computer science is a sequence of messages between at least two computers" quoted from Szabo, *supra* note 14.

blockchain. Because of the integrated protocol on the blockchain, when some data is recorded on the block, it is very difficult (or even impossible) to change or delete it.[17]

An example of how a user could gain Bitcoins on blockchain is as follows. Imagine that "John" wants to gain Bitcoin. To do so, John needs to engage in a process called "mining". The first step for John is to download and install the Bitcoin software on their computer. The software is openly available on Bitcoin.org. The software allows John to connect to the Bitcoin network through creating a Bitcoin "wallet".[18] Upon creating an account on the Bitcoin wallet, John is given a public key and a private key. The public key is like a username and is visible to other users on the chain. John can send and receive Bitcoin via this public key (like an address). The private key is akin to a password through which John can authorize sending Bitcoin to other public key holders and access the Bitcoins they gain on the blockchain. At this point, John's computer is a node on the network. John can see other peers' public key and the record of transactions on their block. So far in the process, John has gained access to the blockchain and has obtained a public and private key.

The next step in the process is for John to engage in building blocks. This is done through the mining process, which includes solving the math problem or "proof of work",[19] verification by other peers, and finally receiving a reward. For mining, John needs another software product on their computer that works with Bitcoin blockchain. John then runs the Bitcoin blockchain code on their computer. The goal for the code is to find an answer to a mathematical problem integrated in the

---

[17] Drescher, *supra* note 9 at 60: "…the transaction history cannot be changed once written".

[18] Think of wallet as a tool on the blockchain software. Read more about digital wallets in Asmaa A. Mohmmed, Abdul M.S. Rahma & Hala B. AbdulWahab, "Digital Wallets Evolution: Navigating Challenges, Innovation and the Future Landscape" (2024) 29:1 Al-Qadisiya J Pure Science, online: <qjps.researchcommons.org> [perma.cc/H4YG-G3Z7].

[19] For more about "proof of work" see Arvind Narayanan & Jeremy Clark, "Bitcoin's Academic Pedigree" (2017) 15, 4, online:<dl.acm.org> [perma.cc/P5LY-A83L]. See also Drescher, *supra note* 9 at 156.

blockchain protocol. The code generates random guesses until one is the correct answer. Once the right answer is generated, other peers can see that a public key holder (John's identity is hidden) has determined the answer. Their computers then run the same code, and, if they get the same answer, they verify that the guess on John's end was the correct answer to the problem. Once more than 50% of the peers approve John's guess was correct, the block is formed and is secured and transferred to John's public key.

In the above example, John has mined one block on the chain which is called the Bitcoin. The Bitcoin is the crypto and is simply a record of transfer of data and ownership taped on the blockchain through the hashing mechanism and the public key technology. Of note, John and other peers are technically the codes on their computer. No human brain is involved in solving the math problem (the math problem is called cryptographic problem). The mining process for Bitcoin and for other types of cryptocurrencies is virtually the same.

The above complicated technological process is merely the beginning of a journey into the fascinating world of blockchain technology. The intersection of blockchain and the law links these technological complexities with established legal principles and adds another layer of sophistication to crypto transactions. The following section of this paper explores some of the challenges arising from the intersection of the law and blockchain.

III. Law, Blockchain-based Transactions, and Challenges

A. Complexity

Fully understanding crypto technicalities requires expertise as well as programming abilities and mathematical skills. One of the challenges for both the public and the courts in dealing with issues arising from digital transformations, is understanding the processes and mechanisms in creation and

use of cryptocurrencies. For many, the complexity, terminologies, and the abstract nature of the digital currency is barrier in understanding and using such technology. In *ABL*,[20] the Court attempts to explain how Bitcoin mining works. In *ABL*, at paragraph 11, the Court states that mining is a process through which the user produces countless guesses to solve a mathematical problem. Once one guess turns out to be the true answer, the user behind the blockchain triggering the codes, will receive a reward in form of a Bitcoin. The Court cites an earlier decision in which the judge elaborated on bitcoin mining:

> [6] Bitcoin mining is not like mining in the conventional sense. New Bitcoin is created by Bitcoin software as a reward for a process that involves creating new blocks and appending transactions in Bitcoin's blockchain. The creation of new blocks requires repeated trial and error computations conducted by specialised computers called "application-specific integrated circuit miners" also known informally as mining rigs. The goal of the process is to guess the inputs to a mathematical formula known as a hash algorithm. If successful, the process results in a so-called "valid hash". The speed at which the computers produce such solutions is called the "hashrate."
>
> [7] Mining rigs demand a great deal of computational power and the process is therefore energy-intensive. … .[21]

This Court's emphasis on elaborating and understanding the process of mining in this case reflects the struggle with understanding crypto transactions. When courts deal with issues arising from digital transactions, the courts need to not only understand what cryptocurrencies are, but also need to ensure the public audience reading the decision understands both how such transactions are created and how blockchain works.

The technicalities of cryptocurrencies do not end in the basic understanding of this technology. A more complicated issue arises when there are attempts to use these digital and crypto transactions as substitutes for contracts. In the crypto world, transactions are based on blockchain technology. The

---

[20] *NYDIG ABL v IE CA 3 Holdings Ltd*., 2023 BCSC 1383 [*ABL*].

[21] *Ibid* at para 11.

blockchain automatically runs the codes to execute transactions. Some argue that these transactions have elements of a contract and can be a substitute for them. These contracts are known as "smart contracts".[22] It is important to understand that so-called "smart contracts" and "digital contracts" are not the same, as discussed in the following section.

B. Digital Contracts or Smart Contracts?

The term "digital contracts" and "smart contracts" are often used interchangeably by mistake. They are two different concepts. Digital contracts are prevalent on websites and media platforms, for example on Facebook (online contracts).[23] By opening an account on Facebook, new members form a contract with Facebook simply by agreeing to Facebook's terms and conditions of use when opening an account. Once the user accepts the terms and conditions, they sign the digital contract with Facebook. Digital contracts are online expressions of traditional principles of contract law.

In comparison, a smart contract is an agreement residing on a blockchain that is self-executing and thus self-enforcing, without the need for a central authority.[24] In other words, smart contracts are "decentralized agreements built in computer code and stored on a blockchain".[25] When a computer code automatically executes all or parts of an agreement between the parties, we have a smart contract.

---

[22] Usha R. Rodrigues, "Law and the Blockchain" (2019) Iowa L Rev, 104, 679 at 680: "The blockchain is a distributed ledger that allows the cryptographic recording of transactions and permits 'smart' contracts that self-execute automatically if their conditions are met", online (PDF): <ilr.law.uiowa.edu> [perma.cc/484M-JP3J].

[23] Lisa A. Peters, Q.C. et al, "Contract Law Update: Developments of Note (2017)" (2017) Lawson Lundell LLP, online (PDF): <lawsonlundell.com> [perma.cc/KMG4-LX8G].

[24] Moin A. Yahya, "Book Review: *Cryptocurrencies and The Regulatory Challenge* (London, UK,: Routledge, 2022)" (2022) Alberta L Rev, 60, 1, at 311, online (PDF): <albertalawreview.com> [perma.cc/ZMP4-LALS].

[25] Andrew Luesley, "Unravelling Smart Contracts: Smart Contracts and the Law of Rescission in Canada" (2019) 19 Asper Rev Intl Bus& Trade L 155, at 157.

This automatic execution consists of a data set stored on the blockchain platform. Therefore, a blockchain is crucial to a self-executing smart contract.

The digital (or online) contracts we see today have their roots in what are called "Ricardian Contracts".[26] In 1996, prior to the emergence of blockchain technology, Ian Grigg invented a payment system called the "Ricardian Contract" based on the "Bowtie model".[27] Ricardian contracts use a set of parameters to connect the text of contracts to codes. It does so by setting parameters representing parts of a contract—including the issuer and the holder, the right of the holder, and the digital signature—to turn their text into secure identifiers ("hash").[28] Then, it converts the hash to understandable accounting units. The Ricardian model acknowledges the need for the courts to understand such forms of contract. To address this need, the bowtie model integrates parameters in the digital contract to account for the parties of a contract and their signatures, making it comparable to its paper form.

The original application of Ricardian contracts was in bond trading systems.[29] The purpose of Ricardian contracts is to facilitate honest, fair, and complete communication between parties in various forms of digital trade. Ian Grigg claims that clarity and trust are the main elements of a fair and open market; by using the Bowtie model, these elements are secured, allowing people to focus on their business rather than dealing with untrustworthy partners. Grigg further claims that Ricardian contracts are legible to both the court of law and to software.[30] Grigg claims that the "Ricardian Contract [is not]

---

[26] Ian Grigg, "The Ricardian Contract", online (HTML): <iang.org> [perma.cc/3HJG-QDH6].

[27] [Unknown author], "The Ricardian Contract" [undated], online: <iang.org> [perma.cc/5PG5-S2A7].

[28] To read more about hashing mechanism see Drescher, s*upra* note 9 at 72.

[29] *Supra* note 26.

[30] *Supra* note 27.

the contract but merely our best efforts at creating a single document that dominates the contract as found by the court".[31] This implies that, according to Grigg, Ricardian contracts have the necessary elements to be recognized as contracts under the law.

Ricardian contracts are not the same as smart contracts and are digital representations of paper form contracts.[32] Florence G'sell Florian and Martin-Bariteau argue that smart contract "are not necessarily contracts in the legal sense of the term".[33] They explain the benefits of the smart and self-executory features of such contracts, which involve a set of protocols triggered by "if-then" conditions. The self-executory nature of smart contracts brings certainty, which is an advantage of using blockchain technology to execute a contract. However, once the protocol is triggered, the parties cannot modify the contract's conditions.

Thus, smart contracts cannot replace contracts in the legal sense, "[e]xcept when such a possibility [of modifications] is provided in the initial code".[34] When parties negotiate a contract, and agree to terms and modifications in advance, the contract can be embedded in the blockchain protocol, thus allowing for later modification. In that sense, the smart contract or the blockchain, is not the contract itself, but rather a tool for executing the contract. A traditional form contract supports the terms encoded in the blockchain and the blockchain cannot be a substitution of traditional contracts. Therefore, "smart contract" is not a legal terminology and refers to the self-executory aspect of

---

[31] Ian Grigg, "On the Intersection of Ricardian and Smart Contracts" (February 2013), online (HTML): <iang.org> [perma.cc/P3AQ-RUGC].

[32] *Ibid.*

[33] G'sell, *supra* note 12 at 10.

[34] *Ibid.*

transactions on blockchains. In blockchain transactions, the concepts of contract law, including offer, acceptance, freedom of contract, and unconscionability remain unsettled as the next section will detail.

C. Offer, Acceptance, and Freedom of Contract

Formation of a contract requires an offer and an acceptance. Common law has established that until a party receiving the offer makes a clear declaration of acceptance of that offer, the parties may negotiate the terms of their agreement,[35] and a new offer ("counteroffer") can replace the original offer.[36] When a party gives a counteroffer the original offer is overtaken. Then, the person receiving the counteroffer must clearly declare their acceptance of the counteroffer. In the formation stage of a contract, the acceptance must reflect the terms and conditions of the offer as it was put forward.[37] To form a contract, parties of a contract use natural language in the offer and in declaring acceptance of the offer. Smart contracts exist as a set of if-then conditions in code that allow for automatic execution of the contract, as opposed to traditional contracts that are executed pursuant to natural language.

Those in favor of using computer code as the language of contract, argue that the code brings certainty to the terms.[38] They state that the performative nature of the code brings the advantage of certainty. Tiffany M. Sillanpää states that "the code itself is unambiguous and determinative to a much greater degree than natural language"[39] and that in comparison, natural language can be ambiguous

---

[35] For an illustration of "negotiation" and "change of the offer" see *Livingston v Evans*, [1925] 3 W.W.R. 453, [1925] 4 D.L.R. 769 (Alta. S.C.), citing *Cowan v Boyd* (1921), 61 D.L.R. 497.

[36] *Ibid.*

[37] *Butler Machine Tool Co. v Ex-Cell-O Corp*., [1979] 1 W.L.R. 401, [1979] 1 All E.R. 965 (C.A.). See also, *Felthouse v Bindley* (1862), 11 C.B. (N.S.) 869, 142 E.R. 1037 (Ex. Ch.).

[38] Tiffany M. Sillanpää, "Freedom to (Smart) Contract: The Myth of Code and Blockchain Governance Law" (Autum 2020), IALS Student L Rev, 7, 2, at 39.

[39] *Ibid* at 40.

and interpreted subjectively by parties and the judiciary.[40] However, one issue that arises is that the parties and the court may not understand the code. Sillanpää elaborates the role of interpretation of the code in two separate pieces: the intent and the consensus of the agreement. Sillanpää adds that understanding the true intent when the language of a contract is natural, is not a novel challenge for the courts. Sillanpää further states that the remedy for the courts to understand the code, is an expert witness who can testify as to what the code does.[41]

One issue with relying on the certainty of the code to execute the crypto transaction, is the assumption that the code would actually execute what the parties believe it to execute. Sillanpää explains that even though the code is performative and is certain, "it is possible for complex code to be misunderstood or generate undesired results in the presence of unexpected input".[42] This could lead to misrepresentation of the contract. Misrepresentation can occur because smart contracts are based on codes residing on a blockchain which cannot identify misrepresentation or other fraudulent techniques in the code. The code simply executes the parameters whenever it is triggered—meaning the if-then conditions are met.[43] Sillanpää proposes that the doctrine of "mistake"[44] can address such misrepresentation[45] if it occurs. However, the inflexibility of the code-based executions is potentially problematic. In fact, there are no mechanisms to prevent or reverse the execution of the code.[46] It can

---

[40] *Ibid* at 41. See also *Sattva Capital Corp. v Creston Moly Corp.*, 2014 SCC 53.

[41] *Supra* note 38 at 41.

[42] *Supra* note 38 at 40.

[43] To explain that the code does not identify mistakes, I compare the code on the blockchain and how emails are sent. If a user includes a confidential information in their email by mistake, the code of Gmail or Yahoo that delivers the message to the receiver, does not identify the mistake and still delivers the email with the confidential information. The if-then conditions are triggered when users click on the send button and the code executes the order which is sending the email.

[44] *Supra* note 38.

[45] See Luesley, *supra* note 25 at 157 to read more about mistake and misrepresentation.

[46] *Ibid* at 172: "Smart contracts use automation and blockchain to compel the performance obligations. Once a smart contract is entered into, payment obligations are automated and there is no reversing payment".

be inferred that the party who writes the code on the blockchain, who may remain unidentified due to the decentralized nature of such a contract, would have the opportunity to conduct fraud or misrepresentation without being held accountable. Moreover, another challenge is that the blockchain protocol, like any other computer or code-based system, may have glitches that cause the blockchain to operate improperly. These are some of the remaining challenges in implementing blockchain technology to substitute traditional form contracts.

Parties without expertise in crypto may also face problems in understanding such smart contracts. As stated above, understanding crypto transactions requires technical knowledge. It would mean that, as with the courts, for crypto-illiterate parties to understand the terms of the contract, they would need an expert to explain to them what the code means and how it operates. An expert who appears in court to testify as a witness would affirm or swear an oath to be impartial, competent, and truthful.[47] Unlike in court, challenges arise when parties to a crypto contract[48] need an expert to interpret the code—an individual who likely does not have the same duty of impartiality, competence, and honesty. When a contract is in natural language, parties to a contract can retain a contract lawyer to help them with understanding the terms and conditions of the contract and their legal implications. However, unlike lawyers who are in a fiduciary relationship with their clients,[49] the crypto expert is

---

[47] Hamish Stewart et al. *Evidence: A Canadian Casebook, 5th Ed. (*Toronto, Canada: emond, 2020), ch 2, at 22. See also, *Court Rules Act,* B.C. Reg. 168/2009, Supreme Court Civil Rules, Rule 11-2 — Duty of Expert Witnesses.

[48] The term "crypto contract" may not be technical, but I refer to it as a reference to a smart contract that resides on a blockchain. There are different types of smart contracts, see: Hedera, "Types of Smart Contracts"[undated], online: <https://hedera.com/learning/smart-contracts/types-of-smart-contracts>. See also Chiradeep BasuMallick, "What Are Smart Contracts? Types, Benefits, and Tools" (20 November 2023), online: <spiceworks.com> [perma.cc/W8UX-GX7W]. However, in the matter of *Bitvo Inc. (Re)*, 2022 BCSECCOM 223 (CanLII), the term Crypto Contract was defined specifically: "contracts involving crypto assets, because the user's contractual right to the crypto asset may itself constitute a security and/or a derivative (Crypto Contract)."

[49] The fiduciary duty of lawyer-client relationship was at issue in *Strother v 346920 Canada Inc*., [2007] 2 SCR 177, and the Court stated that "Fiduciary duties provide a framework within which the lawyer performs the work and may include obligations that go beyond what the parties expressly bargained for". For more information on fiduciary duty of lawyer-client relationship, see Alice Woolley, "The Lawyer as Fiduciary: Defining Private Law Duties in Public Law Relations"

not in such a relationship and there are no fiduciary duties imposed on the so-called "expert".[50] This is because the technology has not led to a regulated profession of crypto experts or blockchain experts, at least for now. This lack of trustworthy expert leaves the parties to a crypto contract to their own will. The lack of understanding the crypto contract may lead to unconscionability of contract.

D. Unconscionability

Forming a contract solely based on the language of the code highlights concerns about clarity of its terms. It is established in the Canadian law of contracts that parties to a contract should have a shared understanding of its terms and conditions at the time they enter the contract. This is referred to as "meeting of the minds" and means that both parties have the same understanding of their contractual obligations. This is a very important principle and requires parties to have clarity in the offer and acceptance.

Freedom of contract is another important and established principle in contract law. Parties are free to enter any contract provided that the contract is not contrary to statutory laws. For example, if a contract is in violation of the *Criminal Code of Canad*a, then it is void. Parties can freely enter a contract, only if they fully understand its terms and conditions. If they do not have full understanding of the contract, then their freedom is compromised. Freedom of contract is inter-related with unconscionability.

(2015) UTLJ (Forthcoming). See also Alice Woolley, Richard Devlin, & Brent Cotter, *Lawyers' Ethics and Professional Regulation*, 4th ed. (Canada, LexisNexis, 2021) at ch 2.

[50] Carla L. Reyes, "(Un)corporate Crypto-governance" (2020) 88 Fordham L Rev, at 1879. The paper states that there is "an emerging line of legal literature suggesting that the open-source software developers should be subject to fiduciary law for the mere act of contributing code to an open project.", online: <ir.lawnet.fordham.edu> [perma.cc/4RPX-NGGS].

In *Uber*[51] the Court stated that the unconscionability doctrine is the general law of contracts, and it applies when there are three elements. Two of the elements are "significant inequality of bargaining power stemming from a weakness or vulnerability",[52] and when "the stronger party knows of the weaker party's vulnerability".[53] The Court used this test in assessing whether there is unconscionability in the contract between Uber and Uber drivers. Full understanding of the contract is the key element in deciding whether the parties have equal power, or whether one is in a vulnerable position and is being taken advantage of because of their vulnerability.

In a smart and self-executory contract, where the language of the contract is based on codes, the risk for a contract to be unconscionable is higher. This is because, as stated above, such contracts are written in convoluted code language and not a natural language. A party may not even be aware of their vulnerability because they may, mistakenly, believe their bit of knowledge of codes is sufficient to fully understand the code. Further, because crypto contracts can be anonymous, the weaker party know that they are in a vulnerable position as compared to the other party.

Those in favor of smart contracts, may appeal to the principle of freedom of contracts and argue that people are free to take risks in engaging in any contract. This is akin to *Loychuk*[54] where the Court did not find an exclusion of liability clause to be unconscionable. The Court stated that the public is free to engage in such activities and there was no unfairness, or imbalance bargaining power, in forming the contract. Similarly, there can be an argument that the public is free to engage in crypto transactions, digital or smart contracts, because the public is aware of the risks involved in participating in such

---

[51] *Uber Technologies Inc. v Heller*, [2020] 2 S.C.R, 2020 SCC 16 [*Uber*].

[52] *Ibid* at 128.

[53] *Ibid.*

[54] *Loychuk v Cougar Mountain Adventures Ltd.* (2012, BCCA) [*Loychuk*].

dealings. The user knows better that without technical knowledge of crypto transactions or smart contracts, they are participating in a risky activity.[55]

While the contract in *Loychuk* was not a digital or smart contract, this case upholds the important principle of freedom of contract. *Uber* is another relevant case involving the question of unconscionability and freedom of contract in a digital contract. In this case, the Court also reiterated the importance of freedom of contract in the "Canadian commercial and legal system".[56] The Court cited *Tercon*[57] and stated that freedom of contract as an essential principle to "the Canadian commercial and legal system and, to promote the certainty and stability of contractual relations, often trumps other societal values".[58]

Another famous case dealing with digital contracts is *Douez*[59] where the Court discussed freedom of contract and unconscionability. The Court at paragraph 115 stated that the doctrine of unconscionability requires two elements: (1) inequality of bargaining power; and (2) unfairness. In both *Uber and Douez*, the issue surrounds clauses in digital contracts, and the Court in both cases found that the clauses were unconscionable, because users, in accessing the services of Uber and Facebook, had no choice other than to agree to the terms of conditions including those clauses. The Court in both cases found the clauses to be invalid because those clauses put the user in an unequal

---

[55] *Ibid* at para 33.

[56] *Supra* note 51 at para 107.

[57] *Ibid,* citing *Tercon Contractors Ltd. v British Columbia (Transportation and Highways)*, 2010 SCC 4 [2010] 1 SCR 69.

[58] *Ibid.*

[59] *Douez v Facebook Inc.,* 2017 SCC 33 [*Douez*].

bargaining power and the clauses were unfair. The crux of the reasoning was in relation to this unfairness, as well as public policy and public protection.[60]

While *Uber* and *Douez* properly elaborate on principles of contract law in digital contracts, referring to these cases as a comparison to crypto transactions to argue that crypto contracts may be unconscionable is inappropriate. Even though the contracts in *Uber* and *Douez* are digital, they are not a proper comparison to self-executory crypto transactions or smart contracts. The issue in these cases is that one party, Facebook, or Uber, is in the position of power that creates an unfair advantage, which leads to the clause in question being unconscionable. In these cases, the party has no other choice, or bargaining power, other than agreeing to the terms and conditions, which led to unconscionability of the terms. In crypto transactions, unconscionability may arise not only from a possible lack of bargaining power, but also from lack of understanding. In other words, the unconscionability goes back to the nature of the code. In crypto transactions, avoiding unconscionability requires a full understanding of the contract.[61] For an individual to freely enter a contract, they must have a complete understanding of its terms, which may not be possible when dealing with complex or automated systems like crypto contracts. In a crypto contract, to fully understand the contract, one must fully understand the code. One cannot expect the public to have an in-depth and complete knowledge of how codes execute themselves and how a blockchain rules the contract. In fact, many in the public and

[60] See *ibid* to read more about unfairness, public policy and public protection. The case provides that when an overriding public policy outweighs public interest in enforcement of a contract, the court can refuse to enforce a contractual provision. Refer to paras 144 – 175 for the relevant discussions.

[61] In *Butler v Butler*, 2015 ONCA 6796, the court found that the domestic contract was unconscionable due to Ms. Butler's lack of understanding of the consequences of what she was agreeing to. The Court notes that the in that case, Ms. Butler "demonstrated a remarkable lack of sophistication". Similarly, if one demonstrates a remarkable lack of sophistication when it comes to crypto contracts, the contract may lead to unconscionability. The Court in that case discussed the effect of Ms. Butler's lack of legal representation at the time she agreed to the domestic contract and that this lack of independent legal advise had a role in her lack of understanding of the consequences.

indeed the legal profession have only just began learning about blockchain. This is where the risk of unconscionability arises.[62]

In the last two sections, this paper discussed the principles of offer, acceptance, freedom of contract and possible unconscionability in forming crypto contracts. It was discussed that due to the challenges in implementing these contract law principles in crypto contracts, such smart contracts do not constitute contracts in the legal sense. The next section briefly presents a competing viewpoint where the author states that smart contracts are valid legal contracts, which is worth noting.

E. Smart Contracts as Valid Legal Contracts in Equity

While prevailing thought suggests that smart contracts are not valid in a purely legal sense, Conrad Flaczyk provides a contrary viewpoint. Flaczyk says that smart contracts and other blockchain technologies can form valid contracts under existing law.[63] However, it seems that Flaczyk is referring to digital contracts rather than self-executory smart contracts. In summary, the author advocates for equitable principles and argues that smart contracts could qualify as valid legal contracts if the blockchain protocol is based on statutory provisions, rather than common law principles. Flaczyk notes that Raymond Samuels[64] has identified six elements for a valid legal contract: "intention to create legal relations, offer, acceptance, value consideration, capacity to contract, and legality".[65] Samuels' argument builds on the fact that every province in Canada, in their respective Electronic Commerce

---

[62] *Supra* note 25 at 172.

[63] Conard Flaczyk, "Technology, the Changing Nature of Disputes, and the Future of Equitable Principles in Canadian Contract Law", 17, 2, 2, Canadian Jr L and Tech at 170.

[64] *Ibid* at 170. citing Raymond Samuels II, Contract Law Backgrounder to E-Commerce Affiliate Programs (Kanata, ON: Agora Business Foundation, 2002) at 7-8.

[65] *Ibid.*

Acts, set out provisions that speak to the validity of these elements, except for capacity and legality.[66] For example, s.19 of the *Ontario Electronic Commerce Act*[67] states that an offer, the acceptance of an offer, or any matter that is material to the formation or operation of a contract may be expressed by electronic means or in digital format. Further s.19(2), the act states that a contract is not invalid merely because it is in electronic form.[68]

Flaczyk also brings up the challenge of "mutual assent" in electronic form contracts[69] and questions how the parties to a contract can achieve mutual assent[70] in smart contracts, when they use the code to enter into agreements on their behalf. Flaczyk proposes that the answer to this question lies in the concept of an "electronic agent".[71] In that context, the technology that enables the parties to enter the contract is the agent or instruments of other entities "that have legal capacity" or "other legal persons that can be held accountable under the law".[72] With this approach, Flaczyk concluded that the blockchain is "merely a platform for contracting".[73] This claim aligns with this paper's earlier view that blockchain is a tool for execution of the contract, but not a contract itself.

After exploring some of the challenges of electronic form contracts, such as the possibility for hacking or the possible negative impact on average consumers, Flaczyk discusses the connection between "equitable principles and reasoning, emerging from technologies and contract law".[74] In

---

[66] *Supra* note 63.

[67] *Ontario Electronic Commerce Act*, 2000, S.O. 2000, c. 17.

[68] *Supra* note 63 at 171.

[69] *Ibid*, citing Reggie O'Shields.

[70] This concept was referred to as "meeting of the minds" in Part D of this paper.

[71] *Supra* note 63 at 172.

[72] *Ibid at* 171.

[73] *Ibid at* 172.

[74] *Supra* note 63 at 184.

summary, the argument is that by codifying principles of equity in statute, as opposed to reliance on common law, equity-based principles may be implemented in self-executory modern contracts.[75] In short, Flaczyk's article suggests that statutory law can be fairer than common law and that incorporating statutory regulation into the protocol can make smart contracts legally valid. In my view, excluding contractual common law principles from the formation and interpretation of smart contracts, or diminishing their value to promote smart contracts, may not necessarily justify declaring smart contracts as legally valid contracts in their entirety. Notwithstanding this argument that smart contracts can be legally valid, blockchains have other features—such as anonymity of the parties—that might create gaps resulting in additional legal issues, a topic explored in the next section.

F. A Feature of Blockchains: Pseudonymity[76] in Transactions

Primavera De Filippi and Aaron Wright in their book[77] name some features of blockchain, including pseudonymity. The idea of pseudonymity here is that the identity of the person who is active on the blockchain is covered behind the public key. One of the important challenges in dealing with crypto transactions, relates to the parties' pseudonymity. Narayanan and Clark, in "Bitcoin's Academic Pedigree",[78] explained how the parties' interaction in a crypto transaction can occur without revealing their true identity. Their identity is concealed behind their respective *public key* that represents them on the blockchain. This pseudonymity is a problem[79] in contracts because it creates room for malicious actors to pay for drugs or other unlawful goods or engage in money laundering[80]. In the Bitcoin world,

---

[75] *Supra* note 63.

[76] See G'Sell, *supra* note 12 at 18, where the author refers as "Pseudo-Anonymity".

[77] Primavera De Filippi & Aaron Wright, *Blockchain and the Law, The Rule of Code* (United States of America: Harvard University Press, 2018).

[78] *Supra* note 21. See also Drescher*, supra* note 9.

[79] See *Supra* note 12 at 7. The authors referred to "pseudonymity" as an advantage.

[80] *Supra* note 5.

public keys are the only kinds of identity[81] and the users' access to their crypto depends on the private key. The downside is that if they lose it, they lose access to all their cryptocurrencies. Some argue that this end-to-end unidentified transaction is a feature that keeps the blockchain secure.

The complexity of directly using blockchain has led to the development of digital wallets, which serve as an intermediary interface to access the blockchain. Learning to use digital wallets are complex. Digital wallets present a record of the transactions on the crypto blockchain, but they only "display" the users' crypto balance/status. All cryptocurrencies still reside on the decentralized blockchain and not the wallet. Mobile bank applications are the closest analog to digital wallets. For example, RBC mobile application shows the balance of the holder's account, but the actual ledger and the money is not stored on the mobile application. Similarly, with digital wallets, the crypto is stored on the blockchain, and the wallet is only a representation of the crypto. When we use RBC mobile application to transfer funds, we are changing the display on our account. By clicking on "transfer", the ledger and the banking system is triggered, and the new amount would show on the sender's and the receiver's display. There is no hard cash involved in such transaction.[82]

However, with the advance of technology and knowledge of the blockchain's structure, the source of the public key may be traceable, and the users' identity can be revealed.[83] However, identifying the owner of the public key requires expertise as well as enormous computational and

---

[81] *Supra* note 12 at 7. See also Drescher*, supra* note 9, at 18.

[82] I can also compare email accounts on Yahoo or Gmail, where unlike in crypto wallets, users' personal data is collected. In accessing e-mail domains, individuals need to identify themselves and enter personal details to create an account. Yahoo or Gmail as an organization or the central service provider can access users' personal data. In contrast, when accessing the blockchain, the blockchain software and the digital wallet do not require individuals to provide personal data. The wallet generates their public and private key without the need for personal information. Yahoo or Gmail are entities, whereas the blockchain is not. So, in the decentralized blockchain there is no access to users' personal data.

[83] G'Sell, s*upra* note 12 at 18.

electrical power. These resources are not available to the public. It would mean that revealing the identity of the public key holder, can be done by experts in the field with access to sufficient resources only. This complexity leads to the parties in a transaction remaining unidentified at the time of their dealings.

Pseudonymity challenges one of the most important, and oldest, principles in contract law. The relationship between the parties and trust between them is at the core of a contract. To have trust and relationship, one would need to know the identity of the other. Despite this core principle, the claim for the blockchain technology is that by using the code, there will be no need for trust in the parties. The trust is built into the code, which is based on mathematical principles at its core and, therefore, is even more reliable than an individual or a corporation.[84]

The idea of blockchain technology goes beyond trust in the parties and seeks to remove the need for a trustworthy centralized authority in transactions between the parties altogether. This is the "libertarian crypto-anarchist perspective".[85] Timothy C. May calls us to "[a]rise, you have nothing to lose but your barbed wire fence!".[86] This anarchist perspective may provoke debate about the rule of law, which is further examined in the next section.

G. The Decentralized World and the Rule of Law

The rule of law means that no one is above the law and the law is supreme. This concept gives power to the entity enforcing the law, usually the State. For a society to function at its optimum, the

---

[84] Szabo, *supra* note 14.

[85] G'Sell, *supra* note 12 at 31.

[86] Timothy C. May, "The Crypto Anarchist Manifesto" [undated], online (HTML): <groups.csail.mit.edu> [perma.cc/Z7C7-66TS].

rule of law is a necessity. In a society without the rule of law, chaos will reign, fraud will be prevalent, and victims will have limited or no recourse. To avoid such dystopian society, the State and its institutions uphold the rule of law.[87]

The idea of a decentralized method of communication between parties in a transaction at their will is to "replace established institutions such as states and banks",[88] and instead implement the blockchain technology as a trustworthy environment "outside of traditional institutions".[89] The State and traditional institutions uphold the rule of law to ensure freedom in the society. However, this freedom is not absolute. There are laws, rules, and regulations that constrain absolute freedom. Many believe that a decentralized platform, such as blockchains, with the possibility of anonymous transactions, "could support fundamental freedoms".[90] It reminds the early days of the Internet[91] where according to legal scholars,[92] the Internet would undermine laws.[93] The development of the Internet might serve as a good analogy to predict the trajectory of blockchain technology.

The Internet and the World Wide Web (the "Internet") have been the biggest decentralized communication platforms.[94] The Internet as a decentralized system, came to be as a fight against

---

[87] See more in Michael S. Boudreau, *City of order: crime and society in Halifax, 1918-35* (Vancouver, 2012 UBC Press). While the book is an analysis of changes in the criminal justice system in a specific era in Halifax, the concept of the rule of law is constantly brought up. The book unpacks and assesses challenges in maintaining order in Hallifax between 1918-1935.

[88] *Supra* note 12 at 4.

[89] *Ibid.*

[90] *Ibid* at 17.

[91] *Supra* note 77 at 50. See also João Pedro Quintais et al., "Blockchain and the Law: A Critical Evaluation", Stanford Journal of Blockchain Law & Policy, (2019), 2.1, at 88, online: <stanford-jblp.pubpub.org> [perma.cc/UM5M-GDQ4].

[92] *Supra* note 77 at 50, referring to legal scholars David Johnson and David Post.

[93] *Ibid*: "No longer would the world be governed by nation-states, and no longer would governments be able to enact laws to establish fundamental rights, shape markets, or manage social interactions".

[94] [Unknown author], "Who controls the Internet?" [undated], online: <internethealthreport.org> [perma.cc/46PR-NN2G].

censorship. It is a platform where networks can communicate and transfer data from one to another according to a set of rules.[95] The Internet enabled lots of new innovations and developments and revolutionized communications in the world in a way never seen before.[96] However, gradually regulations and the State had to intervene in response to problems arising from misuse of this decentralized innovative technology. Fraud, invasion of privacy,[97] and criminal activities were among the issues calling for this intervention.[98] Does this sound familiar?

Today, huge institutions, like Facebook, are centralized institutions on the decentralized Internet. The Internet remains decentralized, but what the public do on the Internet, is governed by these institutions, which are bound to abide by certain laws and regulations of the State.[99] Depending on the geographical location and the jurisdiction where individuals access the Internet, these centralized platforms may be dominant. For instance, Google is one platform that is the dominant search tool in North America. Some governments seek to restrict Internet access through platforms that ensure public access to the Internet remains within the boundaries of their legal system. For example,

---

[95] Pelle Braendgaard, "A personal look at the early days of Internet vs blockchain today, Pelle Braendgaard, January 21, 2018" (21 January 2018), online: <medium.com> [perma.cc/D7DT-DNXP].

[96] Barry M. Leiner et al., "A Brief History of the Internet" (1977), Internet Society, online: <internetsociety.org> [perma.cc/2UBZ-WAQT].

[97] Jonathan Shaw, "Exposed: The erosion of privacy in the Internet era" (September-October 2009), Harvard Magazine, online: <harvardmagazine.com> [perma.cc/P8Z5-E8RS].

[98] Arctic Wolf, "A Brief History of Cybercrime", [undated], online: <arcticwolf.com> [perma.cc/7P4G-ZH9S]. The first major cyber-attack on the internet came courtesy of Cornell grad student Robert Morris. The "Morris Worm" struck in the year before the World Wide Web debuted, back when the internet was primarily the domain of academic researchers. It infected computer systems at Stanford, Princeton, Johns Hopkins, NASA, Lawrence Livermore Labs, and UC Berkeley, among other institutions".

[99] Facebook is now one of many platforms of "Meta Platforms Inc." corporation, incorporated under General Corporation Law of the State of Delaware. See the corporation's amended certificate of incorporation, dated October 21, 2021, online: <https://investor.fb.com/leadership-and-governance/>.

this means that people in North America have access to Google, while people connecting to the Internet from China do not.[100]

Just like how the decentralized Internet became a tool to connect the world, it is reasonable to infer that blockchain technology becomes a tool to serve societies in transactions or data management.[101] Some benefits of blockchain technology are undeniable. Blockchains can be highly secured. Bitcoin, for example, has never been successfully hacked.[102] Blockchains can provide secure platforms to store health care records.[103] However, not all blockchains are secure. If a blockchain's structure changes, its security may be diminished.[104] Ethereum was hacked in 2017.[105] Blockchain developers are working to find ways to further secure blockchains. For instance, Ethereum Mist wallet implements multiple signature[106] wallet technology to increase Ethereum's security.[107]

In much the same way as the Internet, different jurisdictions may have different ways to use and regulate blockchain technology. For instance, effective July 2017, Japan recognized Bitcoin as a

---

[100] Charles Potter, "Baidu vs. Google: What's the Difference?" (31 December 2022), Investopedia, online: <investopedia.com> [perma.cc/2CJA-Q8T3]. See also Access to China, "Public internet structure in China" [undated], online:<accesstochina.com> [perma.cc/97D3-TX28].

[101] Saeed Banaeian Far et al., "Blockchain and its derived technologies shape the future generation of digital businesses: a focus on decentralized finance and the Metaverse" (September 2023), Elsevier ScientDirect, Data Science and Management, 6, 3, online: <https://sciencedirect.com/science/article/pii/S2666764923000280>.

[102] *Ibid* at 3.

[103] *Supra* note 5 at 4.

[104] *Ibid*.

[105] Ran Levi (the podcast host), "Malicious Life Podcast: The Ethereum DAO Hack" [undated], online: <cybereason.com> [perma.cc/YYE2-LD5L]. See quote: "On July 19th, 2017, a hacker was able to steal 32 million dollars from Ethereum cryptocurrency investors by exploiting a vulnerability in the Parity smart contract".

[106] Think of this multiple signature feature as a multiple authentication factor that is wildly used these days. Blockchain technology is constantly progressing so that different industries could commonly use this technology and benefit from the speed and security it can provide.

[107] *Supra* note 6 at 18.

"means of payment". [108] Use of such technology can reduce costs associated with transactions. If we picture a future where blockchain technology is the new Internet, then it is possible that, just as Internet regulation exists, a form of regulatory regime would come into play for blockchain technology. Yahya, in his paper[109] discusses different approaches to blockchain regulation, which are briefly discussed in the next section.

Douez or *Uber* are examples of cases dealing with centralized institutions on the decentralized Internet. In those cases, the Court had jurisdiction. The Court's ruling was upheld, and the relative clauses found to have been unconscionable. The rule of law governed the terms of contracts in both *Douez* and *Uber*. Analogously, the rule of law would remain paramount in dealing with issues arising out of using blockchain technology. The reason is that even though the blockchain has a pseudonymity feature where the user's identity is concealed behind a set of digits (the public and private keys), the organization or the individual behind the keys is still traceable.[110] There may be difficulties, risks, and challenges, but "it is still possible to re-identify the owner of an address since it is possible to trace all transactions, which may infer the identity of the user".[111] The individual or the corporation, once identified, is not above the law. They would still be accountable for their actions.

Additionally, blockchain technology is undermining the decentralized utopia it claims to promote. This is because, over time, the crypto mining process has become extremely complex[112] and

---

[108] Gabrielle Patrick & Anurag Bana, "Rule of Law Versus Rule of Code: A Blockchain-Driven Legal World" (November 2017), IBA Legal Policy & Research Unit Legal Paper, The Global Voice of the legal profession, online: <ibanet.org> [perma.cc/B6RT-FMP8].

[109] *Supra* note 24 at 309.

[110] G'Sell, *supra* note 12 at 18.

[111] *Ibid* at 8.

[112] *Supra* note 9 at 91. See also [unknown author], "Coin Wars, Bitcoin Difficulty" [undated], online: <coinwarz.com> [perma.cc/N2E7-ER5C].

the complexity of the validation process and the proof of work has resulted in normal computers to be inefficient for mining. Because the gain for miners comes from the mining process, miners have incentive to have computers with more powerful CPUs.[113] This has led to creation of mining pools.[114] While smaller, home-based mining rig setups are available, they lack the efficiency and processing power of large mining pools owned by corporations or governments. The larger the mining pool, the higher the chance of solving the validation problem and gaining the block. This implies that the substantial size and capacity of industrial mining rigs give organizations more computational power and speed in mining over other miners, creating an uneven playing field that favors certain entities. This would centralize the power to those larger entities, and, in my view, this is how the development of blockchains is going against the idea of a decentralized network.[115]

Going back to the Starbucks example, the digital wallet company, *Bakkt* is a centralized platform on the decentralized blockchain; much like Google on the Internet, *Bakkt* must comply with the acts and corporate laws of the jurisdiction it is established. If individuals take any legal actions to seek damages or recourse, like in *Douez,* the court's ruling would be paramount, and the rule of law prevails. The next section explores examples of self-executory contracts on the Ethereum blockchain and examines where the current use of smart contracts stands in commerce.

---

[113] CPU stands for Central Processing Unit. CPUs are the primary component of computers responsible for the processing and controlling functions. See also [author unknown], "CPU", Gigabyte, Glossary [undated] online: <gigabyte.com> [perma.cc/79A9-4BWU].

[114] See Appendix A.

[115] To read more about mining and stronger computers, see Elena G. Popkova & Bruno S. Sergi (editors), *Current Problems of the Global Environmental Economy Under the Conditions of Climate Change and the Perspectives of Sustainable Development*, (Switzerland: Springer, 2023) at 17, online: <link.springer.com> [perma.cc/T98D-53Z6].

H. Ethereum and Attempts to Use Smart Contracts

As mentioned earlier in the introduction, Esbertseet et al. discuss Ethereum uniqueness, its actual use, and how it works. “Ethereum emphasizes situations where rapid development time, security for small and rarely used applications, and the ability for different applications to very efficiently interact, are necessary”.[116] Even though the technology is the same, blockchains are distinct from one another depending on their features. While both Bitcoin and Ethereum are products of blockchain technology, the two blockchains have differences that make their use and applications distinct.

Some of the main differences between Bitcoin and Ethereum are notable. Bitcoin is a blockchain designed for the sole purpose of generating crypto, while Ethereum is a blockchain platform that supports not only generating crypto but also various other applications. Bitcoin blockchain does not support smart contracts, but Ethereum’s does. Bitcoin platform is used to store and exchange the Bitcoin, so it stores data and is a medium of exchange. Ethereum is a general-purpose blockchain used to store and exchange diverse types of digital transactions, including its crypto, called Ether. The other curious difference between Bitcoin and Ethereum is in the time it takes for the blocks to complete. Bitcoin blocks take ten minutes to be validated whereas in Ethereum, one Ether block is validated in twelve seconds.[117] Depending on the features a blockchain offers, various industries are gradually implementing smart contracts in their transactions and workflow. Namely, Ethereum can be used to complete transactions because of its self-executory feature. Two examples of businesses attempting to implement this technology in providing their services are noted in the following paragraphs.

---

[116] *Supra* note 6 at 3.

[117] Eye on Tech, “Ethereum vs. Bitcoin: What's the Difference?” (25 April 2022), online: <youtube.com> [perma.cc/F566-G3UM].

Slock.it is a platform in Germany owned by the company named "Blockchains", which claims "Slock.it brings the benefits of the blockchain - transparency, security and auditability - to real-world objects".[118] Slock.it[119] attempts to use Ethereum blockchain to be able to rent, sell, or share anything without the need for a middleman. It enables the user to rent the item without the need to connect with the team at Slock.it or the renter. Slock.it claims that a smart contract embedded on the Ethereum blockchain controls the transaction between the user and the entity renting the item. The idea is that the deposit is held on the blockchain and will be sent to the owner of the Slock automatically. Here, "Slock" refers to the rental item. Slock.it is currently working on electrical charging stations with a similar idea and is partnering with RWE, a large German power company. The goal is to change the way users charge their electric cars. They seek to link the car, which is associated with a digital wallet, to the charging station. Then, use the embedded smart contract on the Ethereum blockchain to allow users to rent the charging station spot, pay a deposit, charge their car and then get their deposit back. All without a third party involved.[120] The idea of Slock.it seems relatively attainable. However, my attempt in visiting their website to learn more about their service was unsuccessful, as the website did not load. This indicates that there is still work to be done until such technology could reliably, transparently, and regularly serve both businesses and the public.

Another example is Ujo Music.[121] Ujo's mission is "Making Musicians More Money".[122] Ujo is trying to reduce the cost of doing business for artists and create new economies for fans to support

---

[118] [Uknown author], "Slock.it" [undated], Crunchbase, online: <https://www.crunchbase.com/organization/slock-it>.

[119] *Supra* note 22 at 699.

[120] Ian Allison, "RWE and Slock.it – Electric cars using Ethereum wallets can recharge by induction at traffic lights" (22 February 2016) International Business Times[UK], online: <ibtimes.co.uk> [perma.cc/P39Y-9EJ5].

[121] Simon de la Rouviere, "Introducing Ujo Portal: Making Musicians More Money" (13 December 2018), online: <ujomusic.com> [perma.cc/BT3N-6TNT].

[122] *Ibid.*

musicians. This is done by removing the middleman and connecting the user with the artist directly. Ujo refers to a *new economy* in which the funds the musicians receive are in crypto. Ujo claims that 100% of the funds goes to musicians. On the "How to" page of Ujo's website, there are a few steps to take in order to pay for the music you like. First, install *MetaMask*. Second, buy Ether. Third, navigate to rac.ujomusic.com, click on the album they would like, and submit the payment on the MetaMask popup. And finally, to download and enjoy the music.

For all these steps, there are other "how to" pages, i.e., how to buy Ethereum using Coinbase, how to use MetaMask, and so on. This simplified step by step guide is very complex. In my research, I referred to the steps and specifically the third step—navigate to rac.ujomusic.com—then click on "Buy Album" in step four. The objective was to access the platform where the actual transaction occurs. However, due to security concerns, I decided not to proceed. An error message appeared, stating that "rac.ujomusic.com [does not] support a secure connection". This simple experiment indicates the need for further developments before blockchain technology gains public trust and would be considered secure. The idea of directly supporting artists is appealing and seems plausible, but it is not yet practicable. Referring to both Ujo and Slock.it suggests that the technology is still in development.

In addition to blockchains used for smart contracts, there is another category of blockchains known as smart contract-capable blockchain platforms.[123] These can be used for purposes other than as a medium of currency and exchange. For example, as mentioned earlier, they can be used in health care for securing patient records. In these types of blockchains, even though crypto transactions occur as a way to record data, there is no reward of crypto coin per se. Blocks are simply records of data

[123] See for example "Cardano": [unknown author] "Maling the World Work Better For All" [undated], online: <cardano.org> [perma.cc/56M3-LD7A].

transactions. This is one of the advantages of blockchain technology because it is secure, fast, and reduces the storage space required for records and documents. To benefit from blockchain technology more prevalently, developers and governments would need to address concerns such as fraud, jurisdiction, and its environmental impacts. The following section provides fraud examples.

I. Examples of Fraud

When we mention fraud in crypto transactions, what typically comes to mind are crimes related to money laundering. In 2022, US Department of Justice expressed concerns over the use of crypto in crimes including sanctions evasions.[124] The victim in most fraud cases is usually an unsophisticated user or an investor attempting to gain a profit from this new industry. This section provides a few examples of fraud in this area briefly.

One way these frauds may occur, is through Initial Coin Offerings ("ICO"). ICO is when a company sells shares to raise funds for a crypto project.[125] The shares sold are crypto coins. These crypto projects are based on crypto asset trading platforms, which are regulated under securities regulations.[126] If they are centralized, then they are more likely to be regulated depending on their jurisdiction.[127] Crypto projects that raise funds through ICO, are treated as selling securities and are regulated. Ethereum is an example of one of legitimate ICOs. Those who purchase tokens (think of tokens as the investor's share in the crypto coin) for a crypto project, do so in trust that the project

[124] *Supra* note 5.

[125] *Ibid* at 5.

[126] Canadian Securities Administrators, "Canadian securities regulators clarify interim approach to value-referenced crypto asset" (5 October 2023), online: <securities-administrators.ca> [perma.cc/X8GJ-V2BK].

[127] See s*upra* note 144 for examples of crypto platform listed in the Toronto Stock Exchange.

would continue, and the crypto's asset-value would increase in the future. This is where many fraudulent actors take advantage of investors.

One example of ICO fraud was the case of OneCoin.[128] Over $4 billion US dollars was raised for a crypto project that was never actually initiated. This was a serious crime case[129] and the Bulgarian founder of OneCoin, who disappeared with all the money in 2017, is on the FBI's wanted list.[130] One of the main issues in such cases, is jurisdiction. The advertising for the ICO in this case was happening all around the world. This means that no specific authority would be protecting the victims. To address the jurisdiction issue, once founders of untrue crypto projects are identified and it is revealed from which country or geography they committed the financial crime, they would be subject to the laws of the specific location where they were at the time of the fraud.[131] Since the beginning of Bitcoin craze, there have been several instances of large-scale fraud in the crypto industry.[132]

---

[128] *Donald Berdeaux et al. v OneCoin Ltd. et al,* 1:19-cv-04074-VEC, online (PDF): <https://www.skadden.com/-/media/Files/Publications/2021/11/Inside-the-Courts/Berdeaux-v-OneCoin-Ltd.pdf>.

[129] See the United States Attorney's Office, "Co-Founder Of Multibillion-Dollar Crypto Scheme 'OneCoin' Sentenced To 20 Years In Prison" (12 Sep 2023), Press Release, online:<justice.gov> [perma.cc/DDC4-LLPT].

[130] Department of Justice, Federal Bureau of Investigation, "FBI Ten Most Wanted Fugitive", online (PDF): <fbi.gov> [perma.cc/688M-96CK].

[131] António Madeira, "OneCoin: A deep dive into crypto's most notorious Ponzi scheme" (1 September 2020), online: <https://cointelegraph.com/news/onecoin-a-deep-dive-into-crypto-s-most-notorious-ponzi-scheme>.

[132] FTX is another example of fraud with the element of jurisdiction. FTX was a crypto trading platform. The company was managed from Bahamas but was advertising in the US. In this fraud, the company providing the platform where crypto trades would occur, secretly transferred user's funds on FTX, to another crypto trading company with headquarters in China. Then the founder had used the transferred funds for personal use, political purposes, and other investments. In November 2022, following a drop in crypto value, traders and investors tried to withdraw their funds from FTX. FTX failed to cover the amounts, and it collapsed. The collapse of FTX revealed the deception. The details of FTX fraud are so subtle that at first it was thought to have been an accounting discrepancy. However, the discrepancy of $8 billion dollars was nothing but stolen funds from investors.[132] This was not a novel way of defrauding others. A common example of such fraud occurs when professionals withdraw from trust accounts and later cannot cover the discrepancy – either intentionally or unintentionally. See *Securities and Exchange Commission v Samuel Bankman-Fried*, 1:22-cv-10501, online: <https://www.sec.gov/files/litigation/complaints/2022/comp-pr2022-219.pdf>.

Canadian crypto market has had its fair share of fraud in crypto as well. In *Patryn*,[133] known as the Quadriga CX, a Ponzi scheme led to a range between $190 million dollars to $250 million dollars of missing funds. In *Patryn,* two investors filed fraud complaints against Quadriga CX in 2019, claiming that they, along with other investors, could not access or withdraw their funds from Quadriga's trading platform. Following their claim, RCMP began investigating the founders. The investigations revealed that the one founder who had the passwords to the trading platform on Quadriga had mysteriously died in 2018 while on a trip in India, taking the keys to the crypto assets to his grave. RCMP's investigation concluded that the founder had never invested the funds he received in any crypto projects.

Above cases are examples of fraud surrounding cryptocurrencies. The cases that came up in my research[134] were not directly about legal issues arising from the blockchain, where the claimant seeks for damages because of the nature of the blockchain. In other words, in the cases involving crypto, the claimant was not seeking damages because the code did not function, or that the code did something wrong. The types of alleged fraud in cases involving cryptocurrencies are not novel fraudulent activities and are not direct results of the blockchain technology. However, the scale of fraud in these cases is likely due to the pseudonymity and decentralized nature of blockchains. One potential problem that is worth noting here is that if the blockchain is hacked, the investors (miners and those who purchase the crypto on the stock exchange) may not be notified. Bitcoin is the only known crypto that has never been successfully hacked.[135] There are 18,000 other cryptocurrencies in existence.[136]

---

[133] *British Columbia (Director of Civil Forfeiture) v Patryn,* 2023 BCSC 2445.

[134] See *Georgas v Ball,* 2024 BCSC 958, 2023 (CanLII) 124314 (ON LRB). See also *MiningSky Technology Ltd. v Zhang,* 2021 BCSC 198, *Jafari v Cord3 Innovation Inc.*, 2023 (CanLII) 5369 (ON LRB), & *Hobbs v Warner,* 2021 BCCA 290.

[135] *Supra* note 5.

[136] G'sell, *supra* note 12 at 9.

This would mean that there are opportunities for fraud or criminal activities through hacking those less secure blockchains. The risk may be higher if it is true that the blockchain and the distributed ledger do not record all crypto transactions.[137] Even though, there are agencies that can trace the individual behind transactions through a process called "blockchain analysis",[138] the risk for cyber-crimes is still present. Another issue is that crypto transactions are irreversible. So, if crypto is stolen, it is hard, or even impossible, to recover it.[139]

In response to opportunities for fraud, as seen in the above examples, governments have taken actions to prevent bad actors and protect the public. However, regulating such a complicated and multifaceted technology, which can be without jurisdiction, is challenging. The next section explores some of the challenges in regulating the blockchain industry.

J. Regulating the Blockchain Technology

With new developments, comes new and unknown problems. The law intervenes when new developments may cause unfair treatment of the public, or cause harm to the public - even when there is a perceived harm. Governments and authorities establish regulations to protect the public in their dealings with private and governmental organizations. Generally speaking, there are multiple approaches towards choosing a regulatory framework in response to issues in society, and choosing a regulatory framework for blockchains is not different. The writers in "Blockchain and the Law"[140] explore a range of regulatory modes. The most direct method of regulation by government is to pass

---

[137] Alison Jimenez, "Cryptocurrency Traceability: Unravelling Underlying Assumptions" (2 February 2024), online: <securities analytics.com> [perma.cc/FN4V-L4B5].

[138] Robert A. Schwinger, "Anonymous no more: Blockchain analytics in the courts" (24 May 2024), online: <nortonrosefulbright.com> [perma.cc/25QG-NN9Y].

[139] *Supra* note 77 at 175.

[140] *Supra* note 77.

laws and another more subtle way is through indirect pressure on individuals or organizations – for example, through taxation.[141] The following paragraphs, briefly notes two modes of regulating blockchain: 1) regulating blockchain industry, and 2) regulating the blockchain itself.

Regulating blockchain industry is a challenge due to its decentralized nature. Governments can regulate the use of blockchain by regulating the users.[142] This user-regulating approach is valid when, through mapping mechanisms,[143] users' identities are traceable.[144] Further, as the process of mining becomes more complicated and the techniques improve, preserving confidentiality of the transactions becomes a struggle.[145] However, this approach is not practical because it is burdensome[146] and time consuming.[147]

There are other approaches toward regulating blockchain. Among them is regulating the code and architecture of the blockchain itself. "Code has long been recognized as a powerful tool to enforce legal rules".[148] This approach would indirectly regulate blockchain developers to implement the laws in the underlying blockchain protocol. The idea is that the protocol includes parameters that ensure the

---

[141] *Ibid* at 173-174.

[142] *Ibid* at 175.

[143] *Ibid.* Mapping mechanisms refers to deanonymization techniques to reveal the users' identity.

[144] G'sell, *supra* note 12.

[145] *Supra* note 77 at 176.

[146] See *ibid* for more information about "Burdensome" which refers to the difficulty of locating and brining actions against the individual user.

[147] *Ibid* at 175-176.

[148] *Ibid* at 181.

smart contract comply with the relevant laws.[149] Regulating blockchain protocol allows governments to pass laws, to disable, or suspend blockchain-based applications that "fail to comply with the law."[150]

Other than the two regulatory modes mentioned above, another approach is to situate blockchain and crypto assets within existing laws. The difficulty with this approach lies in categorizing crypto and blockchain to fit current regulatory regimes. As summarized by Professor Moin Yahya,[151] the author Allan C. Hutchinson in his book, proposes a new category of property to include cryptocurrencies. He called the new category "chose-in-virtuality".[152] This would allow regulators to create causes of actions and remedies for such virtual properties.[153] Yahya further explains that crypto market has two sectors which resembles other securities traded on the market: the primary market and the secondary market.[154] Both crypto primary and secondary markets resemble other traditional securities being traded,[155] and securities commissions regulate trading such crypto assets. The following paragraphs will briefly discuss the securities commission's regulatory role.

The crypto secondary market is technically formed when the miners gain crypto through solving predefined computational challenges and then sell that crypto on the stock exchange, or when one who is not a miner themselves purchases a crypto asset through the stock exchange.[156] Regulating

---

[149] *Ibid.*

[150] *Ibid.*

[151] *Supra* note 24 at 309.

[152] *Ibid*.

[153] *Ibid.*

[154] The primary market refers to the market where securities are created, while the secondary market is one in which they are traded among investors. See Brian Beers, "Primary Market vs. Secondary Market: What's the Difference?" (last updated 17 June 2024), online: <investopedia.com> [perma.cc/6YMX-EF6L]."

[155] See examples of crypto listings on the Toronto Stock Exchange Listings at TMX, Stocklists tab, ETFs &Bitcoin, online: <money.tmx.com> (last updated December 12, 2024, at 11:22 PM ET) [perma.cc/9QU8-HQG3].

[156] I avoid saying through proof of work because proof of work is not the only computational process on a blockchain.

crypto primary market is complicated and relates back to the first proposed regulatory mode mentioned above – the blockchain regulation. Regulating here would mean regulating the protocols that run the code on the blockchain.[157] However, as Yahya explained, Hutchinson responded differently, which is closer to secondary market regulations. This is where Hutchinson introduced "chose-in-virtuality". Yahya further explains that Hutchinson introduced the concept after applying a test for a new form of property and concluded that crypto coins can be a form of property.[158] A trade in a property can be a security. Rose Lewis in her article,[159] discuses different regulatory approaches towards securities and crypto in Canada and the United States. In British Columbia, the BC Security Act[160] ("BCSA") mandates accurate and complete disclosure of financial information of a company that issues securities of any kind.[161] The entity that is selling the securities, is called the issuer,[162] and the document the issuer must periodically issue for the investors to consult prior to making an investment is called prospectus.[163] In the US, similar provisions are provided in the *Act of 1933* and *Act of 1934.*[164]

In crypto trading, "whitepapers" are much like the prospectus and provide information about the blockchain. "A whitepaper is a document released by the issuing company that explains the goals,

---

[157] Regulating the primary market in this sense equals the protocol blockchain mentioned in the earlier paragraphs.

[158] *Supra* note 24 at 308.

[159] Rose Lewis, "The View from the Border, A Comparative Analysis of Securities Regulations for Cryptocurrencies in the United States and Canada Student Articles and Notes" (20222) Canada-United States L J, 46, 1*,* 14, at 190.

[160] *BC Securities Act*, RSBC 1996, c 418, s. 61, online: <bclaws.gov.bc.ca> [perma.cc/845C-GPC3].

[161] For the definition of security, see Mark R. Gillen, *Securities Regulation in Canada*, 4th ed. Canada, Thomson Reuters Canada Limited, 2019, at 5. The *BC Security Act* provides a non-exhaustive list of different types of securities for the definition of the term "security", see *ibid* at s. 1.1 "security".

[162] Gillen, *supra* 161 at 1.

[163] *Ibid* at 7.

[164] US Securities and Exchange Commission, "Statutes and Regulations" [undated], *Securities Act of 1933,* and *Securities Exchange Act of 1934,* online: <https://www.sec.gov/rules-regulations/statutes-regulations#secact1933>.

financing, timelines, and feasibility for the project".[165] The regulatory bodies try protecting the investors through regulations and by educating them. For instance, in 2017, the US Securities and Exchange Commission ("SEC") posted an investor bulletin to educate investors about ICOs and warned investors about signs of investment fraud.[166]

The SEC in the US and the Securities Commission of each Canadian province have authority over transactions involving securities, which includes crypto trades. The individuals participating in ICOs enter investment contracts with companies raising funds. The question then becomes whether these "investment contracts" are securities. The definition section of the BCSA includes the term "investment contract"[167] but it does not define what is an investment contract for the purposes of BCSA. Whether investment contracts are securities is an old age issue, and the judiciary has been interpreting the term both in the US and in Canada through a legal test known as *Howey.* The *Howey* test developed over the years in the US and in 1978, Supreme Court of Canada adopted the test in the case of *Pacific Coast Coin*.[168] The most recent expression of the *Howey* test in Canada was in *Re Furtak* in 2018.[169] The SEC has determined that ICOs are subject to security regulations.[170] Similarly,

---

[165] Nathan Reiff, "How to Identify Cryptocurrency and ICO Scams" (updated 16 November 2024), online: <investopedia.com> [perma.cc/TH9F-BP8P].

[166] US Securities and Exchange Commission, "Investor Bulleting: Initial Coin Offerings" (25 July 2017), online: <investor.gov> [perma.cc/XS6N-TNWW].

[167] *Supra* note 160.

[168] *Pacific Coast Coin Exchange v Ontario Securities Commission,* [1978] 2 S.C.R. 112 [*Pacific*].

[169] Capital Markets Tribunal, Proceeding Documents, *Furtak (Re)*, online: <capitalmarketstribunal.ca> [perma.cc/3JHH-NCZU].

[170] *Supra* note 77 at 189.

in Canada, securities law frameworks regulate cryptocurrencies.[171] This general approach is not applicable if the crypto asset is a derivative.[172]

The above paragraphs illustrate the multiple layers of regulatory frameworks for blockchains and that when trade occurs through real-world transactions, securities commissions are engaged to regulate the trade and to protect the investors. The development of the blockchain technology over the past couple decades, has revealed its negative environmental impact. The next section briefly discusses the regulatory bodies that have set out regulations to minimize this industry's adverse effects.

K. Environmental Concerns

It is ironic that the customer in the Starbucks example orders their coffee in a non-plastic or reusable cup to have a less environment impact, while pay for their coffee through a process that leaves enormous carbon footprint. The amount of energy necessary for mining is so substantial that it raises concerns over the carbon footprint of crypto mining. In 2021, Elon Musk announced that Tesla has suspended accepting Bitcoin for purchases of its vehicles. Musk stated the reason to be the emissions harming the environment because of rapid increase in use of fossil fuels for mining and completing transactions.[173]

Mining pools burn fossil fuel to support the energy the Graphic Processing Units ("GPU") and the Central Processing Units ("CPU") require. Both GPU and CPU are essential for the computational problem solving. The more guesses a user makes, the higher the chances of a correct guess. The chance

---

[171] *Ibid* at 212.

[172] BC Securities Commission, *supra* note 3 at question 7/10. "Not all crypto assets are securities or are subject to securities laws. That said, the regulatory treatment of a particular crypto asset will depend on whether it is a security or derivative. Despite the fact that a crypto asset may not be classified as a security or derivative, the way they are bought, sold and/or traded can be subject to securities laws."

[173] *Supra* note 115 at 15, citing Elon Musk's posting on Twitter, online: <twitter.com> [perma.cc/VT55-T2AP].

of solving the problem by processing the guesses on a personal computer's GPU and CPU is extremely low. Mining on a personal computer makes the computer a mining rig. The user would have a higher chance when connecting and making guesses in a mining pool. Mining pool means a third party provides the equipment, or a group of computers are connected to solve the problem. This connection raises the chances of building a blockchain. Mining pools generate enormous amounts of heat.[174] Further, as mentioned earlier, the difficulty of the problem on the chain increases overtime. Therefore, to address the challenge of increasing mining difficulty as the network grows, miners invest in more powerful equipment and set up improved mining rigs. The incentive of having stronger computer network result in mining pool, which results in higher emissions.[175] Due to high emissions and energy concerns, some countries, like China, banned mining because of the amount of energy it requires. However, such bans would hinder the development of technology. One solution proposed to address the energy concern, was to replace the proof of work with proof of stake.[176] Ethereum attempts to adopt proof of stake of which does not seem to have many supports because it takes longer and the total energy consumption was roughly the same.[177] Unlike China, countries like Iran[178], Siberia, or El Salvador, have generally been supporting big scale mining.[179]

The law and the regulations surrounding mining pools' environmental impact are unsettled. Blockchains lack of jurisdiction further complicates implementing rules and policies. But the concern

---

[174] Nathan Reiff, "What's the Environmental Impact of Cryptocurrency?" (25 August 2024), online: <investopedia.com> [perma.cc/R6RR-GZ7V].

[175] *Supra* note 115.

[176] *Ibid* at 18. Proof of stake is an alternative algorithm to proof of work. For the proposed solution.

[177] *Ibid.*

[178] See: BBC, "Iran bans crypto mining for four months after blackouts" (26 May 2021, last retrieved 29 November 2024), online: <bbc.com> [perma.cc/7VS9-2TUZ].

[179] *Supra* note 77 at 233.

is nothing new. There have always been debates on how to balance the effect of technological developments on environment while supporting new inventions and progress. Possibly referring to how laws and regulations addressed similar environmental concerns in other industries could shed light on appropriate policies. Countries have different approaches towards blockchain technology and mining, which has resulted in inconsistent regulations and policies towards this technology around the world. Because blockchain technology has no one jurisdiction, a more unified approach towards its global environmental concerns is needed.[180] This is also true for other environmental concerns. As an illustration, there are efforts to reduce plastics production and waste in North America, however, that does not necessarily reduce the global production and waste of plastic. This is because another country may increase its plastic production. Global environmental causes require global actions. Similarly, addressing global environmental concerns arising from mining, require global unification. Yet, this does not mean that local rules and regulations are ineffective or unnecessary. This is specifically true in countries where energy supply is a struggle, costly, or where the government intends to move towards environmentally friendly policies.

For example, in Canada, the government of British Columbia introduced legislative amendments to enable electricity service for crypto mining.[181] The government has suspended electricity-connection requests from crypto mining operations for 18 months. Further, it has engaged with "B.C. First Nations, municipalities, utilities, industry associations, and the crypto mining industry to seek feedback on the development of a permanent policy regarding crypto mining connections to

[180] *Supra* note 159.

[181] Government of the Province British Columbia, "New legislation ensures B.C. benefits from clean, affordable electricity" (11 April 2024), online: <gov.bc.ca> [perma.cc/NR2K-KRND].

B.C.'s electricity system".[182] Manitoba had similar restrictions in 2022. Additionally, Hydro-Quebec implemented policies for crypto mining with higher rates and caps on the amount of electricity supply for crypto mining.[183] These actions taken by the governments indicates that they are investigating various aspects of energy concerns to adopt approaches and policies that balances between cost and benefit of crypto mining.

IV. Conclusion

This paper introduced blockchain technology and explored its various aspects, including its implications in contract law, some of its advantages and disadvantages, as well as the regulatory response to this technology. Blockchains are not the first decentralized technological innovation, and they will not be the last one. Perhaps one reason for such decentralized innovations is the human's desire for true liberty Liberations from shackles of law and the State. It is arguable whether a society with such freedom would be a desirable utopia or a dystopia. The freedom from the State and the ideology of crypto punk,[184] even though appealing, is not attainable through blockchain or crypto transactions. This technology may create opportunities for violations of the rule of law and may lead to lawlessness and chaos which would harm the society. As such, the law would respond to regulate and control blockchain aiming to uphold the rule of law. This research further explored issues arisen from the blockchain technology that are relevant to contract law principles. Since the emergence of blockchain, the law has been grappling with various issues from its complexity, opportunities for fraud, regulatory challenges, and to its adverse environmental impact. In response, the courts and regulatory

---

[182] Government of the Province British Columbia, "Engagement on Crypto Mining Policy" (1 August 2024), online: <https://www2.gov.bc.ca/gov/content/industry/electricity-alternative-energy/electricity/engagement-cryptocurrency-mining-policy>.

[183] Government of the Province of British Columbia, "Province hits pause on electrical connections for cryptocurrency mining" (21 December 2022), online: <news.gov.bc.ca> [perma.cc/F43L-TQ3S].

[184] G'sell, *supra* note 12.

bodies have set out rules to minimize the adverse effects of this technology. This technology, whether for transactions or for other purpose, will persist, develop, and grow—until the next innovation takes its place; one which would bring novel issues and challenges for the law and society. Legal institutions and regulations would adopt to respond to various problems arising from this technology to protect the public, benefit form the technology, and to allow further innovations.

Appendix “A”

“A picture of an industrial mining pool in Russia”.[185]

[185] Yuliya Fedorinova & Gem Atkinson, “Russia’s Largest Bitcoin Mine Turns Water Into Cash**.** Power-hungry crypto mining has found an ideal home in the city of Bratsk, where the weather is cold, and the electricity is cheap” (23 November 2019), online: <bloomberg.com> [perma.cc/5RYB-YTES].

Bibliography

Legislation

BC Securities Act, RSBC 1996, c 418.

Court Rules Act, B.C. Reg. 168/2009.

Ontario Electronic Commerce Act, 2000, S.O. 2000, c. 17.

U.S Securities Act of 1933, 15 USC § 77.

U.S Securities Exchange Act of 1934, Pub. L. No. 73-291, 48 Stat. 88.

Jurisprudence

Bitvo Inc. (Re), 2022 BCSECCOM 223 (CanLII).

British Columbia (Director of Civil Forfeiture) v Patryn, 2023 BCSC 2445.

Butler Machine Tool Co. v Ex-Cell-O Corp., [1979] 1 W.L.R. 401, [1979] 1 All E.R. 965 (C.A.).

Butler v Butler, 2015 ONCA 6796.

Douez v Facebook Inc., 2017 SCC 33.

Felthouse v Bindley (1862), 11 C.B. (N.S.) 869, 142 E.R. 1037 (Ex. Ch.).

Furtak (Re), proceeding documents, online: <capitalmarketstribunal.ca> [perma.cc/3JHH-NCZU].

Georgas v Ball, 2024 BCSC 958, 2023 (CanLII) 124314 (ON LRB).

Hobbs v Warner, 2021 BCCA 290.

Jafari v Cord3 Innovation Inc., 2023 (CanLII) 5369 (ON LRB).

Livingston v Evans, [1925] 3 W.W.R. 453, [1925] 4 D.L.R. 769 (Alta. S.C.), citing *Cowan v Boyd* (1921), 61 D.L.R. 497.

Loychuk v Cougar Mountain Adventures Ltd,, 2012 BCCA 122 (CanLII).

MiningSky Technology Ltd. v Zhang, 2021 BCSC 198.

NYDIG ABL v IE CA 3 Holdings Ltd., 2023 BCSC 1383.

Pacific Coast Coin Exchange v Ontario Securities Commission, [1978] 2 S.C.R. 112.

Sattva Capital Corp. v Creston Moly Corp., 2014 SCC 53 (CanLII), [2014] 2 SCR 633.

Securities and Exchange Commission v Samuel Bankman-Fried, 1:22-cv-10501, online: <https://www.sec.gov/files/litigation/complaints/2022/comp-pr2022-219.pdf>. [perma.cc/L2A5-CB4K].

Strother v 346920 Canada Inc., [2007] 2 SCR 177.

Tercon Contractors Ltd. v British Columbia (Transportation and Highways), 2010 SCC 4 (CanLII), [2010] 1 SCR 69.

Uber Technologies Inc. v Heller, [2020] 2 S.C.R, 2020 SCC 16 (CanLII), [2020] 2 SCR 118.

Secondary materials: Journals and Articles

Woolley, Alice, "The Lawyer as Fiduciary: Defining Private Law Duties in Public Law Relations" (2015) UTLJ (Forthcoming).

Banaeian Far, Saeed et al., "Blockchain and its derived technologies shape the future generation of digital businesses: a focus on decentralized finance and the Metaverse" (September 2023), Elsevier ScientDirect, Data Science and Management, 6, 3, online: <https://sciencedirect.com/science/article/pii/S2666764923000280>.

Esbertseet, Wesley et al., "Replacing Paper Contracts With Ethereum Smart Contracts, Contract Innovation with Ethereum" (10 June 2016), online (PDF): <allquantor.at> [perma.cc/62NN-UCSH].

Flaczyk, Conard, "Technology, the Changing Nature of Disputes, and the Future of Equitable Principles in Canadian Contract Law", 17, 2, 2, Canadian Jr L and Tech.

Lewis, Rose, "The View from the Border, A Comparative Analysis of Securities Regulations for Cryptocurrencies in the United States and Canada Student Articles and Notes" (20222) Canada-United States L J, 46, 1, 14.

Luesley, Andrew, "Unravelling Smart Contracts: Smart Contracts and the Law of Rescission in Canada" (2019) 19 Asper Rev Intl Bus& Trade L 155.

Reyes, Carla L., "(Un)corporate Crypto-governance" (2020) 88 Fordham L Rev.

Rodrigues, Usha R., "Law and the Blockchain" (2019) Iowa L Rev, 104, 679.

Sillanpää, Tiffany M., "Freedom to (Smart) Contract: The Myth of Code and Blockchain Governance Law" (Autum 2020), IALS Student L Rev.

Watters, Casey, "When Criminals Abuse the Blockchain: Establishing Personal Jurisdiction in a Decentralised Environment" (2023) Laws, 12, 2, 33, online: <mdpi.com> [perma.cc/A6PH-3P37].

Yahya, Moin A., "Book Review: Cryptocurrencies and The Regulatory Challenge (London, UK: Routledge, 2022)" (2022) Alberta L Rev, 60, 1, online (PDF): <albertalawreview.com> [perma.cc/ZMP4-LALS].

Secondary materials: Books

Boudreau, Michael S., *City of order: crime and society in Halifax*, *1918-35* (Vancouver, 2012 UBC Press).

Daniel Drescher, *Blockchain Basics, A non-Technical Introduction in 25 Steps*, Germany, Apress, 2017.

De Filippi, Primavera et al., *Blockchain and the Law, The Rule of Code* (United States of America: Harvard University Press, 2018).

G'sell, Florence et al., *The Impact of Blockchains for Human Rights, Democracy, and the Rule of Law* (Council of Europe, 2022), online (PDF): <edoc.coe.int> [perma.cc/ZR2Z-ELSE].

Gillen, Mark R., *Securities Regulation in Canada*, 4th ed. Canada, Thomson Reuters Canada Limited, 2019.

Hamish Stewart et al. *Evidence: A Canadian Casebook*, 5th ed. (Toronto, Canada: emond, 2020).

Popkova, Elena G. et al., *Current Problems of the Global Environmental Economy Under the Conditions of Climate Change and the Perspectives of Sustainable Development*, (Switzerland: Springer, 2023), online: <link.springer.com> [perma.cc/T98D-53Z6].

Woolley, Alice et al., *Lawyers' Ethics and Professional Regulation*, 4th ed. (Canada, LexisNexis, 2021).

Secondary Materials: Websites and other online sources

Access to China, "Public Internet structure in China" [undated], online:<accesstochina.com> [perma.cc/97D3-TX28].

Allison, Ian, "RWE and Slock.it – Electric cars using Ethereum wallets can recharge by induction at traffic lights" (22 February 2016) International Business Times^{UK}, online: <ibtimes.co.uk> [perma.cc/P39Y-9EJ5].

Amended certificate of incorporation of Meta Platforms Inc., dated October 21, 2021, online:<https://investor.fb.com/leadership-and-governance/>.

Arctic Wolf, "A Brief History of Cybercrime" [undated], online:<arcticwolf.com> [perma.cc/7P4G-ZH9S].

Bakkt, "Custody, Trading & Onramps for Crypto" [undated], online: <bakkt.com> [perma.cc//GZS3-6KLZ].

BasuMallick, Chiradeep, "What Are Smart Contracts? Types, Benefits, and Tools" (20 November 2023), online: <spiceworks.com > [perma.cc/W8UX-GX7W].

BBC, "Iran bans crypto mining for four months after blackouts" (26 May 2021, last retrieved 29 November 2024), online: <bbc.com> [perma.cc/7VS9-2TUZ].

BC Securities Commission, "Test Your Crypto Asset Knowledge" (accessed November 2024), Quizzes, online: <investright.org> [perma.cc/UX58-SE2A].

Beers, Brian, “Primary Market vs. Secondary Market: What's the Difference?” (last updated 17 June 2024), online: <investopedia.com> [perma.cc/6YMX-EF6L].

Bitcoin P2P e-cash paper (13 November 2008), Satoshi Nakamoto Institute, online: <satoshi.nakamotoinstitute.org> [perma.cc/WTK5-VUEM].

Braendgaard, Pelle, “A personal look at the early days of Internet vs blockchain today, Pelle Braendgaard, January 21, 2018” (21 January 2018), online: <medium.com> [perma.cc/D7DT-DNXP].

Canadian Securities Administrators, “Canadian securities regulators clarify interim approach to value-referenced crypto asset” (5 October 2023), online: <securities-administrators.ca> [perma.cc/X8GJ-V2BK].

Cardano, “Maling the World Work Better For All” [undated], online: <cardano.org> [perma.cc/56M3-LD7A].

Coin Wars, Bitcoin Difficulty, online: <coinwarz.com> [perma.cc/N2E7-ER5C].

De la Rouviere, Simon, “Introducing Ujo Portal: Making Musicians More Money” (13 December 2018), online: <ujomusic.com> [perma.cc/BT3N-6TNT].

Department of Justice, Federal Bureau of Investigation, “FBI Ten Most Wanted Fugitive”, online (PDF): <fbi.gov> [perma.cc/688M-96CK].

Eye on Tech, “Ethereum vs. Bitcoin: What's the Difference?” (25 April 2022), online: <youtube.com> [perma.cc/F566-G3UM].

Fedorinova, Yuliya et al., “Russia’s Largest Bitcoin Mine Turns Water Into Cash. Power-hungry crypto mining has found an ideal home in the city of Bratsk, where the weather is cold, and the electricity is cheap” (23 November2019), Online: <bloomberg.com> [perma.cc/5RYB-YTES].

Gigabyte, Glossary [undated] online: <gigabyte.com> [perma.cc/79A9-4BWU].

Government of the Province British Columbia, “Engagement on Crypto Mining Policy” (1 August 2024), online: <https://www2.gov.bc.ca/gov/content/industry/electricity-alternative-energy/electricity/engagement-cryptocurrency-mining-policy>.

Government of the Province British Columbia, “New legislation ensures B.C. benefits from clean, affordable electricity” (11 April 2024), online (NEWS): <gov.bc.ca> [perma.cc/NR2K-KRND].

Government of the Province of British Columbia, “Province hits pause on electrical connections for cryptocurrency mining” (21December 2022), online (NEWS): <news.gov.bc.ca> [perma.cc/F43L-TQ3S].

Grigg, Ian, “On the Intersection of Ricardian and Smart Contracts” (February 2013), online (HTML): <iang.org> [perma.cc/P3AQ-RUGC].

Grigg, Ian, “The Ricardian Contract”, online (HTML): <iang.org> [perma.cc/3HJG-QDH6].

Hedera, “Types of Smart Contracts” [undated], online: https://hedera.com/learning/smart-contracts/types-of-smart-contracts.

Jimenez, Alison, “Cryptocurrency Traceability: Unravelling Underlying Assumptions” (2 February 2024), online: <securities analytics.com> [perma.cc/FN4V-L4B5].

Leiner, Barry M. et al., “A Brief History of the Internet” (1977), Internet Society, online: <Internetsociety.org> [perma.cc/2UBZ-WAQT].

Levi, Ran, (the podcast host), “Malicious Life Podcast: The Ethereum DAO Hack” [undated], online: <cybereason.com> [perma.cc/YYE2-LD5L].

Madeira, António, “OneCoin: A deep dive into crypto’s most notorious Ponzi scheme” (1 September 2020), online: <https://cointelegraph.com/news/onecoin-a-deep-dive-into-crypto-s-most-notorious-ponzi-scheme>.

May, Timothy C., “The Crypto Anarchist Manifesto” [undated], online (HTML): <groups.csail.mit.edu> [perma.cc/Z7C7-66TS].

Mohmmed, Asmaa A. et al., “Digital Wallets Evolution: Navigating Challenges, Innovation and the Future Landscape” (2024) 29:1 Al-Qadisiya J Pure Science, online: <qjps.researchcommons.org> [perma.cc/H4YG-G3Z7].

Musk, Elon, Twitter, online: <twitter.com> [perma.cc/VT55-T2AP].

Narayanan, Arvind et al., “Bitcoin’s Academic Pedigree” (2017) 15, 4, online: <dl.acm.org> [perma.cc/P5LY-A83L].

Patrick, Gabrielle et al., “Rule of Law Versus Rule of Code: A Blockchain-Driven Legal World” (November 2017), IBA Legal Policy & Research Unit Legal Paper, The Global Voice of the legal profession, online:<ibanet.org> [perma.cc/B6RT-FMP8].

Peters (Q.C.), Lisa A. et al., “Contract Law Update: Developments of Note (2017)” (2017) Lawson Lundell LLP, online (PDF): <lawsonlundell.com> [perma.cc/KMG4-LX8G].

Potter, Charles, “Baidu vs. Google: What’s the Difference?” (31 December 2022), Investopedia, online: <investopedia.com> [perma.cc/2CJA-Q8T3].

Reiff, Nathan, “How to Identify Cryptocurrency and ICO Scams” (updated 16 November 2024), online: <investopedia.com> [perma.cc/TH9F-BP8P].

Reiff, Nathan, “What’s the Environmental Impact of Cryptocurrency?” (25 August 2024), Online: <investopedia.com> [perma.cc/R6RR-GZ7V].

Rodrigues, Usha R., “Law and the Blockchain” (2019) Iowa L Rev, 104, 679.

Schwinger, Robert A., “Anonymous no more: Blockchain analytics in the courts” (24 May 2024), online: <nortonrosefulbright.com> [perma.cc/25QG-NN9Y].

Settembre, Jeanette, “Starbucks drinkers can now pay for coffee with Bitcoin via Bakkt digital wallet app” (2 April 2021), online: <fox2detroit.com> [perma.cc/364P-XM4T].

Shaw, Jonathan, “Exposed: The erosion of privacy in the Internet era” (September-October 2009), Harvard Magazine, online: <harvardmagazine.com> [perma.cc/P8Z5-E8RS].

“Slock.it”, Crunchbase, online: <https://www.crunchbase.com/organization/slock-it>.

Szabo, Nick, “Formalizing and Securing Relationships on Public networks” (1 September 1997), online (HTML): <firstmonday.org> [perma.cc/5QAK-W2VX].

The Ricardian Contract, online: <iang.org> [perma.cc/5PG5-S2A7].

The United States Attorney’s Office, “Co-Founder Of Multibillion-Dollar Crypto Scheme ‘OneCoin’ Sentenced To 20 Years In Prison” (12 Sep 2023), Press Release, online:<justice.gov> [perma.cc/DDC4-LLPT].

Toronto Stock Exchange Listings at TMX, Stocklists tab, ETFs &Bitcoin, online: <money.tmx.com> (last updated December 12, 2024, at 11:22 PM ET) [perma.cc/9QU8-HQG3].

US Securities and Exchange Commission, “Investor Bulleting: Initial Coin Offerings” (25 July 2017), online: <investor.gov> [perma.cc/XS6N-TNWW].

US Securities and Exchange Commission, “Statutes and Regulations” [undated], *Securities Act of 1933*, and *Securities Exchange Act of 1934*, online: <https://www.sec.gov/rules-regulations/statutes-regulations#secact1933>.

“Who controls the Internet?”, online: <Internethealthreport.org> [perma.cc/46PR-NN2G].