

# Unravelling Smart Contracts: Smart Contracts and the Law of Rescission in Canada

---

A N D R E W L U E S L E Y \*

## ABSTRACT

Cryptocurrencies and blockchain technology underpin a rapidly expanding industry and smart contracts are a key area of this blockchain innovation.<sup>1</sup> A smart contract is an agreement in digital form that is self-executing and thus self-enforcing.<sup>2</sup> Max Raskin puts it succinctly when he says

---

\* Ph.D Candidate and research fellow at the Peter A. Allard School of Law, the University of British Columbia. I would like to thank Professor Bruce MacDougall, Professor Gregory Hagen, and Professor Janis Sarra, for this piece would not have been possible without their guidance, advice and support. I am also deeply grateful to my wife, Chen Chen - for her unwavering support and encouragement to persevere in completing this article, while tolerating my sometimes-single-minded focus on it. Many thanks to the editors of the *Asper Review of International Business and Trade Law*, especially Meghan Payment and Danelle Rougeau-Suchy, who were understanding and patient in getting this paper published with my submitting it the day Chen Chen and I welcomed Anna-Marie, our first child, into the world.

<sup>1</sup> For a great explanation of how Bitcoin and Blockchain work see Brianna Bogucki, "Buying Votes in the 21st Century: The Potential Use of Bitcoins and Blockchain Technology in Electronic Voting Reform" (2017) 17 *Asper Rev Int Bus Trade Law* 59 at 62.

<sup>2</sup> Alexander Savelyev, "Contract law 2.0: 'Smart' Contracts as the Beginning of the End of Classic Contract Law" (2017) 26:2 *Inf Commun Technol Law* 116, online: <<https://doi.org/10.1080/13600834.2017.1301036>> [perma.cc/2VSK-XVLK]; ISDA Linklaters, "Whitepaper: Smart Contracts and Distributed Ledger-A Legal Perspective" (2017) online (pdf) : <<https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf>> [https://perma.cc/L2TF-YMAE] K Werbach & N Cornell, "Contracts ex machina" (2017) 67:2 *Duke Law J* 313, online: <<https://www.scopus.com/inward/record.uri?eid=2-s2.0-85034790368&partnerID=40&md5=e696f8d48267cfbd95df24d0003a23ab>>; Alex B Levi, Stuart D;Lipton, "An Introduction to Smart Contracts and Their Potential and Inherent Limitations", (2018), online: *Harvard Law Sch Forum Corp Gov Financ Regul*

“a smart contract is an agreement whose execution is automated” and that “alternative and broader definitions of smart contracts exist and these may be better for computer science purposes, but for legal purposes, what is relevant is the excision of human control.”<sup>3</sup> A major difference between a traditional contract and a so-called smart contract, is that contracts create enforceable obligations, whereas smart contract automatically enforce obligations. Compare signing a contract to purchase an item versus purchasing an item from a vending machine. Like the smart contract, the vending machine will automatically complete the transaction by dispensing the item, whereas a paper contract for the sale of an item does not actually force the sale, and thus can be reneged by breaching the contract.

Smart contracts have the potential to transform supply chain management, contracting, payment and banking services, and perform real estate transactions.<sup>4</sup> It is noted that smart contract technology is still in its nascent stage and that there are few examples of practicable use cases. For the purposes of this paper, we will assume that they will function as purported in the literature.<sup>5</sup>

The focus of this paper is not on showing which smart contracts create legally enforceable contracts. They are self-enforcing meaning the court will not need to enforce them by ordering damages or specific performance. The greater need will be for the courts to determine whether the smart contract is unenforceable, meaning void or voidable. In this case, the courts will have to undo the transaction after it has been executed using the tools of rescission and restitution, perhaps via money substitutes. The Canadian law of rescission can be liberally applied in order to combat the mischief of legally

---

<<https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/>> [perma.cc/9NUR-6F7E].

<sup>3</sup> Max Raskin, “The Law and Legality of Smart Contracts” (2017) 305:1 *Georg Law Technol Rev*, online: <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2959166](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166)> [perma.cc/N242-6LES] at 309.

<sup>4</sup> Jason J Brooks, “Decoding the Legal Grey Zones Around Cryptocurrencies”, (1 February 2019) online: <<http://www.mondaq.com/canada/x/776908/fin+tech/Decoding+The+Legal+Grey+Zones+Around+Cryptocurrencies>> [perma.cc/D72N-JRNN].

<sup>5</sup> There is a broad consensus that smart contracts can create enforceable contracts. See Aaron De Filippi, Primavera; Wright, *Blockchain and the Law* (Cambridge: Harvard University Press, 2018); Don Tapscott & Alex Tapscott, *Blockchain Revolution: How the Technology Behind BITCOIN and Other CRYPTOCURRENCIES is Changing the World* (Toronto: Penguin, 2018).

unenforceable smart contracts which nonetheless auto-enforce or execute. While legislation can be used to prevent unenforceable smart contracts from being entered into or smart contract and blockchain architecture can be designed to prevent unenforceable smart contracts from being executed;<sup>6</sup> currently however, unenforceable smart contracts can be entered into and it will fall to courts to undo them. Part 1 gives a brief introduction to smart contracts and blockchain, Part 2 identifies the types of smart contracts that would be considered unenforceable at law, and Part 3 examines the legal tools Canadian courts have for undoing unenforceable smart contracts.

## I. SMART CONTRACTS

A smart contract is an agreement in digital form that is self-executing and thus self-enforcing.<sup>7</sup> In simpler terms smart contracts are “decentralized agreements built in computer code and stored on a blockchain.”<sup>8</sup> Smart contracts could take the form of a simple bet between friends which cannot be reneged,<sup>9</sup> for example, or a securities trade that settles and transfers ownership instantly.<sup>10</sup> Some other suggested applications for smart contracts include wills, mortgage transactions, insurance and financial services and crowdfunding systems.<sup>11</sup>

---

<sup>6</sup> Bill Marino & Ari Juels, *Setting Standards for Altering and Undoing Smart Contracts* (Rule Technologies. Research, Tools, and Applications, 2016).

<sup>7</sup> Saveliev, *supra* note 2; ISDA Linklaters, *supra* note 2; Werbach & Cornell, *supra* note 2; Levi, Stuart D., Lipton, *supra* note 2.

<sup>8</sup> Jeremy M Sklaroff, "Smart Contracts and the Cost of Inflexibility" (2017) 166:1 Penn L Rev at 263

online: < [https://scholarship.law.upenn.edu/penn\\_law\\_review/vol166/iss1/5/](https://scholarship.law.upenn.edu/penn_law_review/vol166/iss1/5/)> [<https://perma.cc/B97W-T4N5>].

<sup>9</sup> A hypothetical sports betting example: Bruce and Greg are hockey fans who support their local teams. Bruce says to Greg, "I'll bet the Vancouver Canucks will finish higher in the standings than the Calgary Flames" and Greg responds "you're on." They find a simple open sourced sports betting smart contract that has been audited and both transfer to it X Bitcoins (or more likely some other cryptocurrency like Ether). The smart contract is programmed to fetch data from [www.nhl.com](http://www.nhl.com) at the conclusion of the regular season and to disperse 2X Bitcoins to Greg if Calgary finished higher in the standings, and 2X Bitcoins to Bruce if Vancouver finished higher in the standings.

<sup>10</sup> Tapscott & Tapscott, *supra* note 5 at 102.

<sup>11</sup> Jack Choros, "5 Real-Life Applications of Smart Contracts and Blockchain Technology", (2018), online: *Coinsquare* <<https://news.coinsquare.com/blockchain/5-real-life>

Smart contracts and blockchains are not the same. A blockchain is a type of decentralized ledger technology (“DLT”): a shared public ledger of transactions maintained by consensus among the nodes on its network.<sup>12</sup> The following description provides a more in-depth explanation of what DLT is:

It is a digital record that is shared instantaneously across a network of participants. It is distributed because the record is held by each of the users (or nodes) on the network and each copy is updated with new information simultaneously. DLT uses a consensus technique to ensure that every node agrees on the record, with different distributed ledger technologies using different consensus methods. A key advantage of DLT is that there are not multiple competing sets of records that need to be reconciled but just one, albeit maintained on multiple nodes. This one record represents a golden source of data.<sup>13</sup>

Transactions can be automated using smart contracts “hosted and executed” on a DLT such as a blockchain.<sup>14</sup> Once these transactions are stored immutably on a blockchain, they cannot be changed or avoided by either party – the transaction will execute by the network according to its scripted code. Ethereum is perhaps the best example of a blockchain suitable for hosting and executing smart contracts:

Ethereum blockchain stores both transaction data (concerning its native cryptocurrency, Ether) and the code of computer programs called, for better or for worse [26], “contracts.” The code for these contracts is injected onto the blockchain when a personal account sends contract code in the data field of an unaddressed transaction. After this, the contract is added to a block and assigned an address, at which point its code becomes immutable [27]. . . Contracts on Ethereum can hold balances of Ether. Like objects in object oriented programming, they can also have variables and functions

---

applications-of-smart-contracts/> [perma.cc/LEM7-J98A].

<sup>12</sup> Dirk A Zetzsche, Ross P Buckley & Douglas W Arner, “The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain” (2017) 2018 Univ Ill Law Rev 1361 (online: <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3018214](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018214)> [https://perma.cc/7NSL-HYKQ]); Jeremy Narayanan, Arvind; Clark, “Bitcoin’s Academic Pedigree” (2017) 15:4 acmqueue, online: <<https://queue.acm.org/detail.cfm?id=3136559>> [https://perma.cc/2H4Z-CYVA].

<sup>13</sup> ISDA Linklaters, *supra* note 2 at 7.

<sup>14</sup> *Ibid* at 8.

that, if called, adjust those variables or do other nifty things, like send Ether to other contracts or accounts on Ethereum.<sup>15</sup>

One very simple example of a smart contract would be: “parties place Bitcoins or other digital currency (like Ether) into a suspended state on the blockchain, and once certain terms are met, those Bitcoins (or Ether) are transferred to the appropriate account.”<sup>16</sup> In so far as they can be used to suspend digital currency pending the satisfaction of certain conditions, smart contracts resemble escrow-like mechanisms. Escrow mechanisms are used to “suspend execution of a valid contract, and empowers a trusted third party to complete the process.”<sup>17</sup> In a typical escrow transaction, “performance of conditions is in the volitional control of the grantee” while “once the escrow is formed, the grantor still has legal title, but the grantee has an irrevocable power to divest that title by performance of certain conditions and concomitantly to vest title in himself.”<sup>18</sup> It is a trusted third party intermediary which ensures that conditions are met before completing the transaction. With a smart contract however, trust in the blockchain protocol replaces trust in a third-party intermediary, meaning there is no escrow agent to sign off or waive conditions that are only partially (though satisfactorily) met, in order to facilitate the closing of a deal.

For another way to conceptualize smart contracts, consider Szabo’s analogy of the concept involving a vending machine.<sup>19</sup> Like the vending machine smart contracts automate performance by taking in money and dispensing products. In this case, we see that it is the provision of the good is being automated while the payment obligation is only just verified. In fact, there really is no payment obligation. Acceptance of the contractual obligation begins with the inserting of the payment. Similarly, the smart contract does not create a payment obligation, and is only formed once payment has been made. The vending

---

<sup>15</sup> Marino & Juels, *supra* note 6 at 158.

<sup>16</sup> Werbach & Cornell, *supra* note 2 at 17.

<sup>17</sup> *Ibid* at 344.

<sup>18</sup> Wesley Newcomb Hohfeld, *Fundamental Legal Conceptions* (New Haven: Yale University Press, 1919) at 54.

<sup>19</sup> Nick Szabo, “Formalizing and Securing Relationships on Public Networks” (1997) 2:9 First Monday, online: <<https://ojphi.org/ojs/index.php/fm/article/view/548/469>> [perma.cc/8TCN-C2QV]. “The vending machine is a contract with bearer: anybody with coins can participate in an exchange with the vendor. The lockbox and other security mechanisms protect the stored coins and contents from attackers, sufficiently to allow profitable deployment of vending machines in a wide variety of areas”.

machine is secure enough relative to the amount of money it stores in order to make the cost of breach or breaking into the machine exceed the potential rewards. Blockchains offer smart contracts this level of security as well, as breach is theoretically possible but would be prohibitively expensive.<sup>20</sup> Finally, the offer being made by the vending machine “is the entirety of the contractual environment for its transactions – its performance of the contract is effectively final.”<sup>21</sup> Smart contracts have also been characterized as “entire agreement[s]”,<sup>22</sup> because when using smart contracts the code of the contract constitutes its terms, with written memorialization serving as “just an explanation.”<sup>23</sup> Some have gone as far as to say: “if a court concludes that some writing better reflects the parties’ meeting of the minds, it would be powerless to invalidate the smart contract; it would have to find some way to reverse the transfer of value *ex post*.”<sup>24</sup> Entire agreement (or entire obligations) clauses are a type of exclusion clause that have the effect of eliminating claims for relief for misrepresentation by creating the legal reality that no representations were made other than those “set out as agreed in the contract.”<sup>25</sup> Entire agreement clauses are vulnerable to operative misrepresentations that may make *the contract itself* rescindable, however. Situations such as these are the focus of this paper.

It is important to note that smart contracts are not necessarily actual legal contracts, and that calling them smart contracts is actually misleading and leads to confusion. To form a contract, there must be: a) an offer and acceptance of said offer; b) consideration for the offer, or some value exchange; c) an intention to form legal relations; and, d) a certainty of the terms of the contract.<sup>26</sup> For the purposes of this paper, I will assume, as many other authors have, that some smart contracts will create enforceable contractual obligations. My focus, however, is not on smart contracts that create enforceable contractual obligations, but rather smart contracts that would be void or voidable, meaning they do not create enforceable contractual obligations. The literature, which includes both technical computer science as well as legal

---

<sup>20</sup> Marino & Juels, *supra* note 6.

<sup>21</sup> Werbach & Cornell, *supra* note 2.

<sup>22</sup> *Ibid* at 348.

<sup>23</sup> *Ibid* at 351.

<sup>24</sup> *Ibid* at 350.

<sup>25</sup> Bruce MacDougall, *Misrepresentation* (Toronto: LexisNexis, 2016) at 35.

<sup>26</sup> ISDA Linklaters, *supra* note 2 at 6.

scholarship, speaks of both strong and weak smart contracts.<sup>27</sup> This paper focuses on auto-executing agreements and is thus premised on the “strong” type of smart contracts, which are auto-executing and auto-enforcing, and which cannot be modified by human parties.<sup>28</sup> Alexander Savelyev asserts that these *true* smart contracts can be regarded as legally binding agreements with the impossibility of breach.<sup>29</sup>

## SUMMARY

A full discussion of smart contracts is beyond the scope of this short essay, and much has already been written. What is important is that smart contracts innovate by automating the execution of transactions, guaranteeing performance of payment obligations without the need for a trusted intermediary.

## II. UNDOING OBLIGATIONS

When it comes to contracts, the law operates in two different time periods, pre and post contract formation. Once the contract has been formed, its obligations may be enforced by court ordered specific performance or damage awards. Smart contracts purport to supplant this with automated enforcement. Ideally then, smart contracts can minimize transactions costs associated with fraud, theft and enforceability. Nevertheless, courts still have a role in regulating the formation of smart contracts. The contract that is (or is not) formed cannot be the sole regulator of its own process of formation. Code may execute as programmed, but if an agreement that is executed should never have been, then rescission should be available to reverse the process that formed the agreement.

The issue of void or voidable smart contracts is important because the prototypical smart contract compels performance through automation. This is a problem where a party has a legal right to be relieved from any supposed contractual obligations. With fully automated self-enforcing smart contracts, it

---

<sup>27</sup> Savelyev, *supra* note 2.

<sup>28</sup> *Ibid*, This narrower definition of smart contracts is embraced by Savelyev who defines smart contracts as: “a piece of code, implemented on a blockchain platform, which ensures self-performance and the autonomous nature of its terms, triggered by conditions in advance and applied to blockchain-titled assets”.

<sup>29</sup> *Ibid* at 130.

is impossible to breach the contract. Even if one has a legal right to relief of contractual obligations, performance is compelled. Thus, if there are issues with the smart contract formation that make the smart contract voidable by one of the parties, that party must engage the legal system to try and undue the contract after it has been performed.<sup>30</sup> This means the burden of litigation surrounding issues of formation rendering a smart contract void or voidable will shift to the aggrieved party, while theoretically reducing to nil the litigation burden of the party trying to compel performance of a void or voidable smart contract. The end result is the court's decreased role in interpreting agreements and ordering performance or payment, and its increased equitable role in providing contract relief, namely through the rescission of smart contracts.

Rescission, or the "lawful setting aside of the contract", may come as a right when a contract has flaws with its formation such as having been induced into by fraud.<sup>31</sup> Rescission undoes damage done as it "retrospectively removes the contract and restores any transferred property back to the transferor" while also "eliminat[ing] the ability of the other party to the contract to seek any form of contract relief, be it damages, debt or an equitable remedy."<sup>32</sup> The core aim of this remedy is restitution and compensation, not punishment.<sup>33</sup> Each party should be returned to their respective positions had there been no contract. Next some of the flaws in the context of contract formation that create cause for rescission will be examined.

### A. Insufficient Capacity

Smart contracts may be void or voidable using rescission where one of the parties lacks sufficient legal capacity to contract. This may be as a result of mental incapacity, intoxication, or being underage.<sup>34</sup> For example, a smart contract may be voidable if a contracting party lacks capacity as a result of intoxication due to either drunkenness or the effect of drugs.<sup>35</sup> A smart

---

<sup>30</sup> This can also occur with partially performed contracts as well, it's just that the possibility of merely not performing is not an option as it would in a larger subset of traditional contracts.

<sup>31</sup> MacDougall, *supra* note 25 at 292.

<sup>32</sup> *Ibid* at 287,292.

<sup>33</sup> *Ibid* at 327.

<sup>34</sup> Bruce MacDougall, *Introduction to Contracts*, 1st ed (Markham: LexisNexis, 2007) at 169.

<sup>35</sup> *Ibid* at 168 *Bawlf Grain Co. v Ross* (1917), 55 SCR 232 (SCC).



contract with a minor is void unless it is for the individual's benefit, and if not void, the smart contract may still be voidable until they affirm it after reaching adulthood.<sup>36</sup>

There are problems regarding ensuring the capacity of parties to smart contracts.<sup>37</sup> Parties to a smart contract are assumed to be represented by their "secret private key", similar to how automated bank machines require the inputting of a personal identification number ("PIN") in order to withdraw money. PINs can be stolen, intercepted, or used without permission, however, just as a secret private key could be stolen or discovered. When it comes to minors, there are "no legal limitation[s] on minors having private encryption keys or owning Bitcoins" therefore they would be able to enter into smart contracts that may in the end be voidable, even perhaps without the knowledge of the other contracting party.<sup>38</sup>

## B. Misrepresentation

An operative misrepresentation is an untrue statement of a material fact that is relied on by a contracting party as a reason to enter into a contract.<sup>39</sup> A fraudulent misrepresentation is a misrepresentation knowingly made, in which case "the court will exercise its jurisdiction to the full order . . . to prevent the defendant from enjoying the benefit of his fraud at the expense of the innocent plaintiff."<sup>40</sup> Conduct such as "deliberately concealing or disguising problems

---

<sup>36</sup> *Ibid* at 169. In British Columbia "The Infants Act, RSBC 1996, c 223, Part 3. Makes contracts made by infants unenforceable by the other party, unless, among other things, the infant affirms the contract or does not repudiate it within a year of attaining the age of majority." Rest of Canada: contracts with infants are voidable unless: 1) it is for necessities, 2) it is a labour or service contract for the child's benefit; or 3) the child affirms the contract on attaining adulthood. See *Altobelli v Wilson*, [1957] OJ No 87, [1957] OWN 207 (Ont CA).

<sup>37</sup> Werbach & Cornell, *supra* note 2 at 48.

<sup>38</sup> *Ibid*.

<sup>39</sup> A misrepresentation is material when it is "substantial" and "to the root of" a contract: *Guarantee Co of North America v Gordon Capital Corp*, [1999] SCJ No 60, [1993] 3 SCR. 423 (SCC) at para 47. A misrepresentation can be said to have been relied on where it formed at least part of the reasons for entering into the contract: *Edgington v Fitzmaurice* (1885), 29 Ch D 459 (CA). MacDougall, *supra* note 2.

<sup>40</sup> MacDougall, *supra* note 25 at 327 quoting from *Spence v Crawford* [1939] 3 All ER 271 (Eng H.L.).

or flaws” have been characterized as fraudulent misrepresentations.<sup>41</sup> In the context of smart contracts, were one of the contracting parties to program a smart contract protocol in such a way as to “conceal” or “disguise” the true nature of the program, this could be considered a fraudulent misrepresentation, even where the plaintiff had the opportunity to inspect the code, as there is no duty for the receiver of the statement to investigate whether or not the representation is true.<sup>42</sup> An innocent misrepresentation made unknowingly may even lead to a right of rescission.<sup>43</sup> The overarching doctrine of misrepresentation itself will therefore be useful where representations or warranties have been made as enticements to smart contracting but have not been replicated in the underlying code protocol.

### C. Mistake

Mistakes can be unilateral,<sup>44</sup> mutual,<sup>45</sup> or common.<sup>46</sup> If only one party is mistaken, the mistake is unilateral, and may lead to relief if the mistake was in an offer that the offeree snaps up.<sup>47</sup> This could be the case, for example, where an offeree discovers that the smart contract they have been offered contains an exploit that is to their advantage and quickly accepts it to prevent the mistaken party from revoking it. As Bill Marino and Ari Juels write:

Of the grounds for rescission, unilateral mistake (when one party *thinks* the smart contract does one thing, while the other party *knows* it does another) is of particular interest to smart contracts. Due to the introduction of code to the agreement-making process, unilateral mistake may be a greater danger than ever before. Few feel confident reading “legalese”; even fewer feel confident reading code.<sup>48</sup>

---

<sup>41</sup> MacDougall, *supra* note 34 at 178.

<sup>42</sup> *Ibid* at 182.

<sup>43</sup> *Ibid* at 180; *Redgrave v Hurd* (1881), 20 Ch D 1 (CA).

<sup>44</sup> *Ibid* at 189, Unilateral mistake is where one party is mistaken about some aspect of a contract, and this mistake is not attributable to the other contracting party.

<sup>45</sup> *Ibid*, Mutual mistake, is where both parties have differing though reasonable views as to their agreement.

<sup>46</sup> *Ibid*, Common mistake is where both parties have the same mistaken belief about their agreement.

<sup>47</sup> John D McCamus, “Mistaken Bids and Unilateral Mistaken Assumptions, a New Solution for an Old Problem” (2008) 87:1 Can Bar Rev.

<sup>48</sup> Marino & Juels, *supra* note 6 at 155.

To constitute “snapping up”, the offeree is not required to actually know of the offerors mistake, only that it was unreasonable for him not to have realized it.<sup>49</sup> Whether a mistake in the programming of an offered smart contract is obvious enough to make its acceptance a snapping up, may be a question of normal coding practices.

Glanville Williams explains that upon certain premises, conclusions can be logically implied. These conclusions are not always known in advance, which leads to “psychological surprises.”<sup>50</sup> In contract law, these psychological surprises can also fall under the category of unilateral mistakes. These types of psychological surprises will be prevalent in the use of smart contracts code – programmers and illiterate users alike. It is very difficult to foresee all the logical implications of lines of coded commands executed literally and unforgivingly. Williams submits that where a party has knowledge of the other party's mistake as to the logical implications of a bargain, their contract should be void.<sup>51</sup> This will be true in the context of smart contracts in which programming errors or shrewd programming may lead to unilateral psychological surprise.

A mutual mistake is often better seen as a lack of *consensus ad idem*, leading to a contract being void.<sup>52</sup> Perhaps an error in the code which contradicts writings leading up to the formation of a smart contract can be considered a mutual mistake, as the meeting of the minds was not replicated in the code. If both parties had different interpretations of the implications of the code, then it may be that the contract is legally void. In the event of a unilateral contract, the mistake may not even need to be mutual.<sup>53</sup> Smart contracts “are by default unilateral; only one party places them on the blockchain” so there might be issues as to whether there was a true “meeting of the minds” or “overt acts of assent” rendering the contract void.<sup>54</sup>

A type of common mistake could occur in smart contracts where both parties believe the code to function a certain way, or blockchain title to be a certain way, and it is not. Common mistake requires that there be no warranty

---

<sup>49</sup> MacDougall, *supra* note 34 at 202.

<sup>50</sup> Glanville L Williams, “Language and the Law” (1945) 61:1 LQR 179 at 399.

<sup>51</sup> *Ibid* at 400.

<sup>52</sup> MacDougall, *supra* note 34 at 199.

<sup>53</sup> Werbach & Cornell, *supra* note 2 at 46.

<sup>54</sup> *Ibid* at 23.

by either party regarding the state of affairs of which there has been a mistake, not the fault of one of the parties, the mistake must lead to the impossibility of the contract.<sup>55</sup>

#### D. Equitable Rescission

A broad equitable approach to rescission for common mistake was put forward by Denning L.J. in *Solle v Butcher* where he suggests that a contract “can be set aside on such terms as the court thinks fit” for mistakes “as to facts or as to their relative and respective rights” if the mistake is “fundamental and . . . the party seeking to set it aside was not himself at fault”, if “it was unconscientious for the other party to avail himself of the legal advantage which he had obtained” and that “it could be done without injustice to third parties.”<sup>56</sup> A mistake in a smart contract could lead to a windfall to one party at the expense of the other. It may be such a situation where it would be “unconscientious” for that party to “avail himself” of the benefits resulting from common mistake, and ought to lead to a right of rescission. While a distinct equitable rescission for mistake for contracts not rendered void by the common law doctrine of mistake as described in *Solle v Butcher* has been overruled in England by *Great Peace Shipping Ltd. v Tsavlis Salvage (International) Ltd.*,<sup>57</sup> it appears Denning L.J.’s broad approach to mistake in equity is good law in Canada.<sup>58</sup> As a result, equitable rescission may be the perfect tool to inject equitable control over smart contracts.

---

<sup>55</sup> *Great Peace Shipping Ltd. v Tsavlis Salvage (International) Ltd.*, “The Great Peace”, [2002] 4 All ER 689 at 708-709 (CA).

<sup>56</sup> *Ibid* at paras 1119-1121

<sup>57</sup> *Ibid* at 708-709 (C.A.)

<sup>58</sup> At least in both Alberta and Ontario. For example, In *Stone’s Jewellery Ltd. v Arora*, 2009 ABQB 656 at para 30 the Queen’s Bench found that the decision in *Great Peace* had not “changed the law in Canada that recognized a wider availability of equitable rescission for mistake than exists at common law.” The Alberta Court of Appeal affirmed this equitable doctrine of mistake in *Beazer v Tollestrup Estate*, 2017 ABCA 429 at para 27: “The equitable doctrine of mistake arises when a mistake renders the enforcement of a contract unconscionable: *Solle v Butcher*, [1950] 1 KB 671 at 692, [1949] 2 All ER 1107 (Eng CA). Because of the mistake, the contract is voidable and rescission can be granted. Rescission is a discretionary remedy and available even where the mistake is insufficient to render the contract void *ab initio* at common law.” In *Miller Paving Limited v. B. Gottardo Construction Ltd.*, 2007 ONCA 422 (CanLII) The Ontario Supreme Court endorses the *Solle* approach to equitable rescission notwithstanding *Great Peace*: “*Great Peace* appears not yet to have been adopted in Canada and, in my view, there is good reason for not doing so. The loss

## SUMMARY

Smart contracts are formed when computer protocols containing instruction for the transactions are recorded onto a blockchain containing the private keys of the contracting parties authorizing it. The smart contract protocol is unilaterally submitted for recording on the blockchain by just one of the parties. Some of these smart contracts may create enforceable contractual obligations, however the focus of this section in particular, and this paper more generally, are those smart contracts that do not form enforceable contractual obligations due to the way they were formed. Contracting parties may have a right to rescission if at the time their smart contract was created they lacked capacity, they relied on misrepresentations, were mistaken as to the agreement, or for some other equitable reason.<sup>59</sup>

## III. CODE IS LAW OR RULE OF LAW?

Blockchains are immutable, therefore smart contracts for transactions considered illegal or invalid at law will remain valid on the blockchain creating two realities: one depicted digitally on the blockchain, and one depicted by law in the physical world. The unlawful owner can still validly transfer the asset in the blockchain digital world.<sup>60</sup> Marino and Juels suggests that this fact eliminates the usefulness of the courts and that the only solution is coding rescission into smart contracts themselves:

contract law has a well-honed set of tools for undoing and altering contracts, including . . . rescission. Unfortunately, these traditional tools often fail when applied to smart contracts. True, they successfully undo the legal agreement that a smart contract manifests. If these tools are exercised, no

---

of the flexibility needed to correct unjust results in widely diverse circumstances that would come from eliminating the equitable doctrine of common mistake would, I think, be a step backward.”

<sup>59</sup> MacDougall, *supra* note 34 at 161; GHL Fridman, *The Law of Contract in Canada*, 6th ed (Toronto: Carswell, 2011) at 461-463.

<sup>60</sup> Savelyev suggests two solutions to this, both of which he views as sub-optimal: 1) creating government super-users who can override the blockchain and 2) giving courts and states the power to pursue specific users and force them to make the changes in the blockchain themselves in combination with using traditional tort, unjust enrichment, and specific performance claims. Savelyev, *supra* note 2 at 133.

court will enforce the agreement. The problem, of course, is that technology still might.<sup>61</sup>

While they say this in the course of making valuable contributions to the development of smarter more useful smart contracts with the ability to undo or alter built on, there will still be situations where smart contracts are created without such mechanisms and thus the courts must be relied upon to provide relief. Using money substitutes for the restitution of digital assets is one solution to the issue of unlawful property transfers immutably stored on a blockchain. There has been a trend in Canadian law towards a broad approach to using money substitutes where restitution of the unlawfully transferred assets themselves is impossible. This was discussed in *Kupchak v Dayson Holdings Co. Ltd. et al.*, where the defendant used fraudulent misrepresentations to sell shares in a motel company to the plaintiff in exchange for some real estate. These properties were sold or redeveloped before the plaintiffs learned of the fraud and sought rescission. Overturning the trial judge's decision that the impossibility of restitution prevented the rescinding of the contract on appeal, Davey J.A for the British Columbia Court of Appeal said:

. . . equity as an incident of its peculiar remedy of rescission, or under its power to award compensation, may adjust the rights of the parties by ordering either one to pay compensation to the other to make good some deficiency in perfect restitution.<sup>62</sup>

The broad approach to money substitutes is still looked upon quite dubiously in the context of negligent or innocent misrepresentations.<sup>63</sup> Therefore, if a party is unable to prove that a misrepresentation that induced them into a smart contract reached the level of fraud, rescission may be unavailable as a remedy.

Smart contracts are rule-governed, challenging the role of law as a system regulating our activity, especially contract law. Because they are self-executing, smart contracts eliminate the role of specific performance (used to compel execution of obligations) and damages (used to compensate for non-performance). This automatic enforcement leads to an added emphasis on the court's role in relieving parties from performance using rescission. Rescission is relevant where there is a problem with the contract formation due to

---

<sup>61</sup> Marino & Juels, *supra* note 6 at 152.

<sup>62</sup> *Kupchak v Dayson Holdings Co Ltd. et al.*, 1965, 53 DLR (2d) 482 (BCCA). at para 488.

<sup>63</sup> MacDougall, *supra* note 25 at 341.

misrepresentation or mistake for example, and where (unaltered) performance should not be allowed. Some courts view the execution of a contract as a bar to rescission for innocent misrepresentations,<sup>64</sup> though in *Solle v Butcher*, Denning L.J. points out this limitation “would mean that innocent people would be deprived of their right of rescission before they had any opportunity of knowing they had it.”<sup>65</sup> This is particularly true in the context of self-executing smart contracts, where rescission even for innocent misrepresentations ought to be considered. The court has an equitable jurisdiction to do so, under the court’s equitable jurisdiction as described by Friedman:

Wherever a court considers, on general equitable grounds, that a contract should not be allowed to stand, and that the request by one party that it be annulled and avoided should be granted, the court has the power to do so. A court of equity can do what is “practically just”.

...

Rescission may be granted even where the contract is not susceptible of attack at common law. When it is, the purpose of the court is to produce *restitution in integrum* . . . there may have to be, and the court has the power to order, adjustments, perhaps involving monetary payments by way of compensation for use of property, or reimbursement of expenses, so as to ensure that, so far as is within the capability of the court, the parties are restored to their original situations, before the contract was ever concluded between them.<sup>66</sup>

The remedy will be unavailable where restitution (or the return of property) is impossible. The return of tangible property can be impossible where the property has been: permanently altered or changed, destroyed, or transferred to a third party. Equity can step in, however, and award money substitutes instead of “the restitution of the actual property transferred.”<sup>67</sup> Assets that are fungible, money or bitcoins for example, can almost always be restituted because the property returned does not have to be exact but rather of the same kind.<sup>68</sup> The return of shares exchanged under contract can present an impossibility of restitution where the shares have been exchanged for different

---

<sup>64</sup> MacDougall, *supra* note 34 at 185 *Shortt v MacLennan*, [1958] SCJ No 61, [1959] SCR 3 (SCC).

<sup>65</sup> *Solle v Butcher*, [1949] 2 All ER 1107 at 1121 (CA).

<sup>66</sup> Friedman, *supra* note 59 at 761–763.

<sup>67</sup> MacDougall, *supra* note 25 at 325.

<sup>68</sup> *Ibid* at 328 “It may be that moneys received by a representor cannot, however, be returned if it would have an adverse impact on other creditors of the representor”.

shares, or where the share issuing company no longer exists. In both these cases, the property no longer exists or has been destroyed. This may be relevant for smart contracts connected with initial coin offerings (“ICO”) in subsequently folded-up companies. However, blockchain by definition consist of a record of all transactions, so if funds raised in an ICO are embezzled by a corrupt party, equitable tracing<sup>69</sup> may be a tool to help effect restitution.

Rescission will not be granted where it would cause hardship to a contracting or third party. This bar to rescission is particularly relevant where a misrepresentation was innocent or made by a third party. A court may also decide that hardship operates as a bar to rescission for practical reasons, such as if a rescission order will be hard to frame or if monitoring compliance with the order will be difficult.<sup>70</sup> Thus, hardship may have a negative impact on the availability of rescission in the context of smart contracts, where restitution may require the use of tracing, complex money substitutes, novel technologically complex crypto assets, or extra jurisdictional transfers.

Smart contract code will always be regulated in a *code is law* architectural sense.<sup>71</sup> The question is whether courts will have a hand in the regulating. If courts do not get involved, “code is law” will replace the rule of law in the future as the use of smart contract code proliferates.<sup>72</sup> While smart contracts may be able to oust certain aspects of the common law and certain remedies, courts have an underlying equitable jurisdiction rooted in unconscionability and principles of equity to regulate smart contracts. In the context of auto-executing smart contracts, invoking the common law will likely be for remedial purposes. Therefore, contract law leaves freedom to innovate with smart contracts, while providing underlying security of potential recourse when things go wrong. Over time and with the development of case law, best practices for smart contracting will emerge, nurturing continued technological innovation and economic growth.

## SUMMARY

While there are technological complexities and practicalities that make restitution and thus rescission difficult, the common law is resilient and can

---

<sup>69</sup> *Ibid* at 357, “the process of locating or identifying a new fund or asset that is acquired through a dealing with the original fund or asset”.

<sup>70</sup> *Ibid* at 357.

<sup>71</sup> Larry Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 2000).

<sup>72</sup> De Filippi, Primavera; Wright, *supra* note 5 at 193.



adapt. There have been other novel contracts where restitution was difficult or impossible where (money) substitutes were used. In the case of smart contracts Bitcoin would be amenable to money substitutes. Money substitutes can also be used to replace digital assets or the loss of digital title to physical assets. The law always adapts to overcome obstacles. Smart contracts can be undone using rescission, because fraud unravels everything. Otherwise, code is law.

#### IV. CONCLUSION

The rapid adoption of blockchain, Bitcoin and other cryptocurrencies have left democratic and legal institutions struggling to keep up.<sup>73</sup> Rapid technological progress brings with it new risks and courts must adapt to keep up. The right dose of regulation will help develop a technology rather than stifling its growth.<sup>74</sup> Regulatory uncertainty leads to capital flight, while regulatory certainty and rule of law provides confidence to innovators and investors.<sup>75</sup> Canadian governments and regulators have been slow to regulate the cryptocurrency and blockchain space, this leaves it to the courts to deal with issues retroactively as they come up.<sup>76</sup> As courts begin filling gaps in the regulatory framework, governments will look to these to inform their regulatory decisions. Overall, this development of a regulatory framework will stop the flow of developers considering moving their operations elsewhere.<sup>77</sup>

The prototypical smart contract will be on an immutable blockchain or decentralized ledger, exchanging cryptocurrencies, digital assets or other blockchain titled property. In addition to shifting the role of the legal system from enforcement to contract relief, and the burden of seeking legal system

---

<sup>73</sup> Yuval Noah Harari, *21 Lessons for the 21st Century* (New York: Penguin Random House, 2018).

<sup>74</sup> Kevin D Werbach, "Trust, But Verify: Why the Blockchain Needs the Law" (2016) forthcoming Ssrn at 58.

<sup>75</sup> Barbara Shecter, "Lawyers see plenty of work ahead as innovation economy takes hold | Financial Post", online: <<https://business.financialpost.com/technology/lawyers-see-plenty-of-work-ahead-as-innovation-economy-takes-hold>> [perma.cc/L5P2-4RHT].

<sup>76</sup> "[I]n the absence of strong regulatory Framework, litigation in Canadian courts . . . [will] shape the guidance and rules needed to protect individuals and Businesses." Kevina A McGivney, "Smart Cities: Are there Privacy Potholes Ahead?", online: <[https://blg.com/en/News-And-Publications/Top-Innovative-Industries\\_-\\_Smart-Cities](https://blg.com/en/News-And-Publications/Top-Innovative-Industries_-_Smart-Cities)> [perma.cc/RGM4-FSZ9].

<sup>77</sup> Shecter, *supra* note 74.

intervention to those with rights of contractual relief rather than those claiming rights to contractual performance, smart contracts also create significant doctrinal and practical issues to contract relief, perhaps making it impossible or impractical due to the cost of litigation exceeding the expected restitution. On the whole, one consequence of smart contracts (intended or otherwise) will be an increase in the performance of legally void or voidable obligations.

Smart contracts pose unique risks to unsophisticated users, calling into question some of the key justifications and rationales of contract law. Due to their technological complexity, there will likely be a power imbalance between those who create these contracts and consumers who may be enticed to use them. The unsophisticated user may be misled as to the contents of the smart contract code.<sup>78</sup> This fact can be used to defraud people. Another risk includes the presence of an unintended mistake which may benefit one party at the expense of the other. Historically, equity has provided mechanisms to protect unsophisticated parties from unconscionable, deceitful or barely-honest practices.<sup>79</sup> For example, misrepresentations are often dealt with using the largely equitable remedy of rescission to unravel a contract and relieve the representee of his or her obligations.<sup>80</sup> However, the use of the discretionary, interventionist, conscience-based principles and doctrines of equity – including the retroactive approach of relief through rescission – is challenged by smart contracts.<sup>81</sup>

Smart contracts use automation and blockchain to compel the performance of obligations. Once a smart contract is entered into, payment obligations are automated and there is no reversing payment. When smart contracts are used to commit fraud, their automation shifts the litigation burden to the innocent party and limits the court to *ex-post facto* interventions after the execution of the transaction and transfer of funds. Further, seeking

---

<sup>78</sup> Marino & Juels, *supra* note 6 at 157. “Fraud and unconscionability are high risks for the same reason: code-savvy parties are in a position to defraud or force unconscionable terms on code-naive parties. For these reasons, Reformation of smart contracts is likely to occur.”

<sup>79</sup> Henry Mather, *Contract Law and Morality* (Westport: Greenwood Press, 1999); Rick Bigwood, “Exploitative Contracts” in (Oxford: Oxford University Press, 2003); MacDougall, *supra* note 25; Bruce MacDougall, *Mistake in Contracting* (Toronto: LexisNexis, 2018); McCamus, *supra* note 48.

<sup>80</sup> MacDougall, *supra* note 25.

<sup>81</sup> Savelyev, *supra* note 2.

restitution is complicated by the architecture of the blockchain, specifically its immutability and pseudo-anonymity. Thus, in addition to compelling the performance of even void or voidable obligations, smart contracts make lumping it (or taking the loss) more economically efficient than seeking relief from the legal system. Regulators must find ways to make unravelling smart contracts more efficient. The *ex-post facto* unravelling of an auto-executing smart contract induced to by fraud will require rescission and restitution using money substitutes and equitable tracing. Identifying how barriers to the rescission of smart contracts can be over-come, including using legislation and regulation, is an area ripe for further research.

Programming rescission and reformation into smart contracts has been studied<sup>82</sup>, however implementation has been slow, and this is only helpful where parties are using trusted smart contracts or are programming them themselves. This paper seeks to address the mischief of smart contracts used maliciously, and ways the ways in which Canadian regulators, particularly courts, can go about rescinding them. The preservation of contracting parties' legal and equitable rights to rescission and restitution in cases where automated smart contracts compel the performance of void or voidable contracts warrants a broad approach to the court's use of equitable remedies. This paper examines smart contracts and discusses void or voidable obligations, identifying how automated smart contracts may compel their performance. Finally, it concludes that the remedy of rescission can be used in Canada as a check against code as law to protect innocent parties.

---

<sup>82</sup> Marino & Juels, *supra* note 6 at 158. "There are at least two ways to *undo* contracts (i.e., implement Termination by Right, Rescission by Agreement, or Rescission by Court) on Ethereum. The first, the global selfdestruct function, is easy to implement and effective. That said, it is also a blunt instrument, lacking the nuance of the second way, which is to turn the entire contract "off" at the function level using a combination of Solidity's modifiers and enums."

