Freedom to (Smart) Contract:
The Myth of Code and Blockchain Governance Law

Tiffany M. Sillanpää

Introduction

Courts in common law jurisdictions like the UK, Canada and the USA have had the difficult job of balancing the overarching principle of "freedom to contract", which mandates they uphold contracts in their original form as much as possible, while protecting weaker parties from fraud, unjust treatment, and unconscionable outcomes. Historically, courts' success in walking this line has been mixed. In the US specifically, contract scholars like Friedrich Kessler have been known to condemn narrow adherence to the principle of "freedom to contract" while large-scale enterprises have attempted to circumvent any legal uncertainty stemming from judicial intervention by using imposing standard-form contracts onto their weaker counterparts.[1]

Of late, this struggle has acquired new life in the debate surrounding Smart Contracts. Much like the enterprises who used standard-form contracts as a tool for "excluding or controlling the 'irrational factor' in litigation",[2] Smart Contract advocates contend that removing the judiciary as the governing body over contract law and imposing contractual performance via decentralized blockchain governance will improve efficiency, legal certainty, and ultimately achieve true "freedom to contract" without judicial intervention. However, one's ability to write a contract that completely circumvents the potential for legal intervention or judicial enforcement, and achieve the complete separation between private and public law that "freedom to contract" advocates originally claimed, seem dubious at best. This paper will demonstrate, that as long as smart contracts meet the traditional requirements of a contract, they cannot fall outside the established legal system's purview. The common law legal system's deep-rooted belief in the rule of law and due process prevents the judiciary from being excluded from contract enforcement regardless the medium. The only thing a smart contract truly adds to traditional contracts is automated execution that is enforced by the blockchain's consensus mechanism; this may provide some efficiency to the legal system by streamlining basic performance but it cannot be the only form of governance over smart contracts. While there may be procedural challenges to undoing or enforcing specific performance under smart contracts because of their decentralized features, any substantive problems that could occur within a smart contract are imminently addressable with and must be subjected to the principles and remedies found in traditional contract law.

In order to explore these questions further, Part I of this paper will first outline the basic concepts of smart contracts and establish that they can and should be considered to meet the formation requirements of a traditional contract. It will also explore how courts can overcome any interpretation issues presented by the computer-code elements of a smart contract with plain-language supplements and expert witnesses. Part II will outline the respective anti-establishment nature of the blockchain community and highlight why their insistence on blockchain-only governance is incompatible with the common law legal system's requirements for rule of law and due process.[3] Part III will provide more context for the assertion that blockchain governance alone is not sufficient by outlining more complex situations where smart contracts can go wrong and applying potential solutions from traditional contract law. Having established that smart contracts are like traditional contracts and therefore must theoretically fall within the existing legal governance structures, Part IV will explore the practical challenges of litigating smart contracts and propose some solutions to common procedural issues surrounding anonymous parties. Finally, I will conclude with current developments in smart contracts which point to a potential for them to become an integral part of our legal system going forward. Overall,

[1] See generally, Kessler, *supra* n. 1.
[2] Kessler, *supra* n. 1, 632 & 638.
[3] While this paper will largely reference USA academics and perspectives on the matter, the general principles of contract law discussed and relied on are applicable to the general body of contract law found in common law jurisdictions like the USA, Canada, and the UK.

I will argue that smart contracts, if carefully drafted to consider potential pitfalls and the future needs of contracting parties to amend or enforce, can hold the potential to provide efficiencies and greater legal certainty to contracting parties, not through circumventing the legal system, but by working with it to automate simple performance enforcement and deferring more complex contractual breakdowns to the judiciary.

Overview: Smart Contracts vs. The Legal System

Smart contracts are agreements governed by "the blockchain—a digital ledger, distributed across a network, that securely records transactions between parties—to automatically and securely execute obligations when certain conditions are met."[4] In other words, once parties agree to a coded-version of the transaction they desire to execute, the smart contract will unequivocally execute the transaction when defined conditions are met. This generally requires an Oracle—some trigger that sits outside the contract—to inform the smart contract of when the specified conditions have been met. Because the contract and its results are stored on the blockchain, they cannot be unilaterally undone by any party to the contract without first achieving a 51% consensus of the blockchain members. Smart contract advocates claim these features offer a "way to make the application of legal rules and agreements more consistent and efficient." [5] But such claims are coloured by the highly political, anti-establishment nature of the blockchain community and arguably fail to appreciate that contracts are more than "bare financial transactions" and have been used as a "social resource" to organize relationships.[6]

Are Smart Contracts Actually Contracts?

While some question whether these code-based agreements have all the required elements to be legal contracts, the Chamber of Digital Commerce (CoDC) argues that most smart contracts demonstrate as having the three key legal elements required of a traditional contract (offer, acceptance, consideration).[7] An offer is made when a "smart contract code [is] deployed on a distributed ledger" for anyone on that ledger to interact with. [8] Acceptance is achieved when a participant on the ledger signs the transaction with a private key and thus binds both sides of the contract with the consideration of promising to perform in the future[9] or by putting funds into a wallet. Furthermore, the CoDC argues that even when a smart contract is executed between a human and the code, both the Electronic Signatures in Global and National Commerce Act (ESIGN) and Uniform Electronic Transaction Act (UETA) equate the code or computer's actions to those of a person or legal entity being bound, thus creating a contract.[10] Furthermore, even in such contracts, the code itself still requires a human author just like a written contract or a smart contract, where both parties know each other.

Can Courts Interpret Smart Contracts?

Not all smart contracts are equally reliant on code to define their terms. The CoDC identifies two main models of smart contracts: external and internal.[11] External smart contracts are those that are governed by traditional, natural language contracts with the smart, code-driven part of the contract merely automating the performance of terms as appropriate (e.g. payment, shipment, etc.). If there is any disagreement between the parties, the traditional, non-code version of the contract prevails, making it much easier for parties and courts to determine what was intended and the terms actually agreed to. CoDC equates this smart contract configuration to that of traditional contracts written in different languages, where one language is set to rule the other(s) in cases of discrepancy; therefore parties

[4] Karen E.C. Levy, "Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law" [2017] 3 Engaging Science, Technology, and Society 1, 1-2.
[5] *Ibid.*
[6] *Ibid.*
[7] Miren Aparicio Bijuesca *et al.,* "Smart Contracts: Is the Law Ready", (*Chamber of Digital Commerce: Smart Contracts Alliance*, Sep 2018) 15 - 16.
[8] *Ibid.* at 15.
[9] *Ibid.* at 16.
[10] *Ibid.* at 17.
[11] See, Bijuesca et al. *supra* n. 10, 25 - 26.

wishing to create an external smart contract must be clear about which version of the contract prevails in order to successfully put the natural-language terms first and foremost.[12] However, when such clarity is lacking in multi-language contracts, the UNIDROIT Principles stipulate that preference should be given to the contract that was originally drawn up.[13] Presumably, the same can apply to smart contracts; if the code was written first and the natural-language contract second, the code prevails. Inversely, one may say that code is not "language" in the way that French or Spanish is and therefore should not be interpreted as a substitute for the natural language contract at all; perhaps it can be treated like a schedule or appendix, but not the main, binding part of any agreement as code is not a "human" language of any kind. This approach may work in certain contexts, however, given that the code creates an outcome automatically, its interpretive value seems more relevant to the main body of most external smart contract.

Contrastingly, internal smart contracts surrender far more to the code-based part of the contract than their external counterparts. The CoDC identifies two types of internal smart contracts: 1) those where the code encompasses the entire agreement and any natural-language portion of the contract merely explains the terms of the code, and 2) those where the code forms the integral or operational portion of the legally binding contract and natural-language is reserved for non-operational clauses. [14] In both versions, however, the code is supreme and any natural-language portion of the agreement is secondary. Therefore, while the natural-language portion of the contract may help courts understand the parties' intent, they will still have to interpret code to definitively understand what consensus was reached. While this has been raised as a problem for courts wishing to exert power over smart contracts, the use of expert witnesses who can read and inform the court what the code "says", can quickly and easily remedy this issue (e.g. bringing a programmer to the stand to testify what the outcome of the code, as written, would be).

Indeed, interpreting code is generally less challenging than interpreting natural language. Since it is written to be performative, in that it is meant to be executed by a computer that is following directions without independent thought or outside context, the code itself is unambiguous and determinative to a much greater degree than natural language. Still, this does not mean that code will do what the human signing it thinks it will— it is possible for complex code to be misunderstood or generate undesired results in the presence of unexpected inputs. Such outcomes may, as this paper will later discuss, raise common law issues of "mistake" in contract formation.

Whether one chooses an external or internal smart contract, however, the inflexibility of the code-based executions present potential challenges when circumstances change or errors in the code create undesirable results for one party. While the CoDC suggests several internal mechanisms to help solve these problems which mirror those in current commercial agreements (e.g. escrows, arbitral clauses, claw-back mechanisms, etc.), they acknowledge that many of these "break" or undermine the advantages of smart contracts and do not completely eliminate the potential need for judicial intervention.[15] A contracting party's tolerance for such compromises on the ideology of "unstoppable" contracts depends on how strictly they adhere to the original social and political goals contained in blockchain and smart contract's anti-establishment roots.

[12] Bijuesca et al. *supra* n. 10, 26.
[13] International Institute for the Unification of Private Law, UNIDROIT Principles of International Commercial Contracts, 4.7 (2016).
[14] Bijuesca et al. *supra* n. 10, 26.
[15] Bijuesca et al. *supra* n. 10, 31-2.

Theoretical Grounds for Judicial Authority Over Smart Contracts

Satoshi Nakamoto clearly defined the goal of his blockchain in his 2008 Bitcoin Whitepaper: to circumvent financial institutions and enable "two willing parties to transact directly with each other without the need for a trusted third party."[16] This antiestablishment tone carried through into smart contract applications built atop blockchain and cryptocurrency systems, only here the establishment to circumvent is the legal system and, particularly, judicial intervention.

Ardent smart contract advocates dislike traditional, natural-language contracts because they see them as ambiguous; because natural language can be interpreted subjectively by both the parties and the judiciary, they provide no certainty or predictability of outcome. Much like standard form contracts, smart contracts attempt to pre-empt incalculable or undesirable risks presented by performance or litigation uncertainty by using code executed by infallible computers; advocates claim that because anyone reading a smart contract can predict what the code will do in any given situation, smart contracts are not ambiguous like natural-language agreements. [17]

For this reason, advocates argue that smart contract should "replace large swaths of the traditional contract system" and that such circumvention of the legal system is desirable.[18] The increased certainty of code-based contracts will result in lower transaction costs, higher consumer protection and improved liberty as individual preferences will be protected from subjective and unpredictable judicial interpretation; they boldly argue that it will also prevent corruption because, unlike human judges, the blockchain cannot be threatened or bribed.[19] Notably, such concerns of judicial manipulation may be more prevalent in some jurisdictions than others but advocates do not appear to make such distinctions when discussing the general global need for smart contract adoption.

In short, smart contract advocates are deeply committed to the "freedom to contract" ideals and a strict division between public and private law; [20] they acknowledge the need for governance but see this governance as being conducted via the blockchain amongst the private users of the smart contract platform itself and not by the judiciary. The benefits of judicial discretion in upholding principles of "justice" and "equity" in cases where fraud, frustration, or misrepresentation block or warp at least one party's contractual goals, are, from the smart contract advocate's perspective, outweighed by the uncertainty that judicial discretion introduces into an area of law critically dependent on legal certainty. While courts are already weary of altering private contracts unnecessarily and take every effort to uphold contracts whenever possible, ardent smart contract advocates wish to eliminate all centralized judicial involvement in favour of decentralized blockchain governance. This anti-establishment ideology, however, has severe practical limitations that necessitate the a centralized judicial function to ensure justice and equality remain present in contractual agreements.

[16] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", (Bitcoin.Org, Oct 2008) 1, <http://satoshinakamoto.me/bitcoin.pdf> last accessed 30 Nov 2019.
[17] James Grimmelmann, "All Smart Contracts are Ambiguous", [2019] 2 Journal of Law & Innovation 1, 3; See also, Kessler, supra n. 1, 631-2 (Provides examples of standard form clauses writing-out judicial risk in insurance contracts, the use of warranty classes in the machine industry that limit buyer's remedies or exclude his right to claim damages, and arbitration clauses in international trade agreements as means to exclude litigation risks).
[18] Verstraete, *supra* n. 2, 746.
[19] Verstraete, *supra* n. 2, 747; Grimmelmann, *supra* n. 20, 5.
[20] Verstraete, *supra* n. 2, 743.

Failings of the Anti-Establishment Ideology

While smart contract advocates claim to create decentralized systems of law, independent of any jurisdictional legal system, the plausibility of a completely anti-establishment contracting system is suspect. As James Grimmelmann says, "[t]here is no escape from politics, because blockchains are made out of people."[21] He goes on to posit that blockchain governance is as much a social institution as the legal system, only the contract "depends indirectly on what people think about the computer system on which it runs" rather than what the judiciary think it means when they read it as with a natural-language contract.[22] In this sense, smart contracts are more institutionalized than natural-language contracts as they require parties to put trust in the blockchain system and code rather than their contractual counterparts. As long as the code does what it is supposed to and blockchain nodes achieve consensus, the intent and actions of one's counterpart do not matter; once triggered, the contract moves forward as defined at the time of its writing, regardless of either party's change in circumstances, misunderstandings, or otherwise.

Therefore, while smart contract governance is decentralized, it is still capable of bureaucratic behaviour that smart contract advocates accuse legal institutions of.[23] Indeed, "code is law" ideology and "come hell or high water" enforcement models make smart contracts and blockchain governance stricter and more bureaucratic than the common law system's more flexible nature found in judicial interpretation's ability to look at matters on a case-by-case, fact-focused basis. Once put in motion, smart contracts grant the trusted blockchain all the power to keep both parties to the terms regardless of exigent circumstances or mistake. While such draconian enforcement measures are the very features of smart contracts that advocates tout as creating certainty within the system and complete freedom to contract, when code malfunctions or the contract outcome is different from what one or more parties thought they were agreeing to, important due process issues are raised.

Rule of Law, Due Process, and Smart Contracts

Because, "the law cannot possibly anticipate the content of an infinite number of atypical transactions into which members of the community may need to enter", the government has delegated some of its law-making power to individuals via the right or freedom to contract.[24] While this empowers individuals to be private legislators as to who can make and execute binding "law," it does not grant them a right to act arbitrarily.[25] Therefore, as long as "self-government by contract should be subject to the limitations inherent in the notion of the rule of law," meaning the freedom to contract is not an exercise of "individual autonomy but an entitlement to the use of governmental resources and authority." [26] In short, while we enjoy the freedom to set terms and agree to whatever commitments we see fit under private contract law, contracts must adhere to the democratic principles of public law and can be governed by judicial oversight when circumstance necessitate.

Smart contract advocates would find this logic a direct violation of the very meaning of private law and an undue limit on autonomy. Yet, even smart contracts do not eliminate the need for enforcement and governance over contract-made law; they simply attempt to automate execution with decentralize governances via the blockchain's consensus. "Freedom to contract" means nothing unless there is a means to enforce the contracts stemming from it. While the blockchain achieves basic enforcement through automation and the blockchain's consensus mechanism, this cannot replace judicial means of contract governance since, as we will see, blockchain governance lacks the ability to rectify complex contractual breakdowns in a way that respects the rule of law. While smart contracts may provide

[21] Grimmelmann, *supra* n. 20, 22.
[22] Grimmelmann, *supra* n. 20, 22 & 3.
[23] Same Mire, Blockchain In The Legal Industry: 10 Possible Use Cases, (Disruptor Daily, 26 Oct 2018) https://www.disruptordaily.com/blockchain-use-cases-legal/ last accesses 22 Nov 2019.
[24] Kessler, *supra* n. 1, 629.
[25] F. Eric Fryar, Common-Law Due Process Rights in the Law of Contracts, [1988] 66 Tex. L. Rev. 1021, 1023; see also, Douglas v. United States Fidelity & Guar. Co., 81 N.H. 371, 375, 127 A. 708, 710 (1924) as cited by Fryar.
[26] *Ibid.*

streamlined efficiency, judicial oversight is better positioned to analyze substantive issues in light of broader legal principles like justice and equality which include concepts of fairness and unconscionability.

Due process is one such essential part of the rule of law. It establishes boundaries within which the law makers must operate when subjecting individuals to its coercive power. Here, the judiciary has several tools to ensure due process in contract enforcement in addition to the basic concepts of offer, acceptance and consideration. These include concepts like mistake, misrepresentation, duress, and fraud as well as the potential for efficient breaches when performing a contract becomes less efficient than paying damages. Courts also, of course, look at contract performance against contact terms to resolve situations where one party has not upheld their end of the bargain or is taking advantage of the other party.

The blockchain, however, has no means to evaluate a contract's efficacy or fairness and once they are set in motion, there is no way for the blockchain governance to stop performance that is creating harm to one or more parties. If there were to be no judicial oversight or the ability for a governing body to impose remedy, then the irreversible nature of the blockchain would also allow one party to take advantage of mistakes or misunderstandings to his counterpart's detriment. To illustrate the limits of blockchain governance and the need for additional judicial support, let us take some hypothetical situations in which a smart contract could be abused or breached without remedy.

Situations Requiring Traditional Enforcement and Remedy

Example Agreement: A distributor and re-seller decide to make a smart contract for the purchase and sale of goods. The parties agree that the distributor will ship the re-seller a defined amount of product each month for 12 months; the smart contract is coded to release 50% of the monthly payment when the product is shipped and another 50% when the product is received. The "oracle" informing the smart contract when to execute parts of the code is a combination of the distributor's inventory system and the shipping company's parcel tracking system. When the shipping company confirms a shipment containing the correct amount of inventory (per the inventory system) has been picked-up from the distributor's facilities, the first half of the payment is automatically sent by the smart contract to the distributor; once the shipping company confirms the shipment has been delivered, the second half of the payment is automatically sent. The smart contract re-executes this process each month for one year, until the contract is complete.

This arrangement removes any risk of late or non-payment for the distributor and streamlines the re-seller's payment process so that it avoids any accidental late-payment penalties. However, there could be several opportunities for contractual disputes to arise in such a smart contract configuration despite its automated nature. While some of them could have been pre-empted by better coding, once the smart contract is agreed to and in motion any ability to correct drafting mistakes with addendums or a mutual understanding outside the contract becomes technically unavailable. Granted, if the parties know and trust each other well, they may certainly self-correct outside of the smart contract itself. However, should the relationship become contentious or one party decides to be uncooperative, smart contract advocates would say they must depend on the blockchain to force performance as it has been coded. Thus, if the code malfunctions and enriches one party to the other's detriment or one party decides to take advantage of places where human performance is still required to undermine the agreement, blockchain governance will not provide a remedy.

However, if this were a traditional contract, not only could drafting errors be fixed by mutually agreed addendums, but the judiciary could also use established legal principles to uphold due process and correct injustices. The following subparts will explain possible conflicts in smart contracts and compare the potential for remedy (or lack thereof) in blockchain governance against judicial intervention using traditional contract principles.

Code-Based Errors

Occasionally, smart contract code malfunctions or are miswritten and yield undesired results. However, blockchain governances would uphold the unexpected result because it is what the code dictated and the parties agreed to the code. This "code is law" ideology is driven by the blockchain community's political aversion to any kind of intervention—judicial or otherwise—on "code-legal" executions that could strip the code of its "certainty." From a contract law perspective, this is an extreme interpretation of the "freedom to contract" principle. While individuals are free to make and enter into agreements, contract law requires that there be *consensus ad idem* for the contract to be enforceable. Through one party making an offer and the other party accepting it, the two minds come together and a contract is formed.[27] A smart contract "merely executes the commands that a programmer integrated into it, which are intended to reflect the pre-existing common intent of the parties"[28]; however when the code's result and the parties' intent are at odds, has *consensus ad idem* really been achieved? Very likely not.

For instance, supposed the example smart contract above is accidentally coded to send 60% of the payment upon shipment, and another 50% upon delivery, amounting to an overpayment of 10% for that month. Blockchain governance would approve this outcome since it is what the code dictates should happen even if it is not necessarily what the parties thought the code would do or intended the code to do when it was written. Courts, however, have more dynamic ways of handling and correcting such mistakes in traditional contracts which could also be applied to smart contracts.

Mistranscription

First, let us suppose that the parties negotiated the terms of the agreement outside the code and one party was charged with creating a smart contract based on what they discussed. A court would likely deem the smart contract unenforceable under the concept of mistranscription. In a traditional contract, mistranscription occurs when two parties agree terms orally and one party is tasked with transcribing the oral agreement into writing but makes a mistake when doing so.[29] While both parties sign the written agreement, mistranscriptions are considered a mechanical error that occurs after the contract has been made as the "only contract the parties have made is the oral contract." [30] Generally, the appropriate relief in such cases is to amend the written version to correctly embody the oral contract; such a remedy will only be granted if the petitioner provides clear and convincing evidence that mistranscription has occurred. [31]

In a smart contract context, if the parties agreed their terms before inscribing them in code, the coded version of the contract should act as a transcription of their original agreement. If parties have a natural-language explanation of terms to accompany the smart contract, or even emails or other business documents demonstrating the original intent, the evidentiary burden on the party claiming harm becomes easily satisfied and reformation should be ordered. Despite the blockchain's immutable qualities, contract reformation on platforms like Ethereum is not an impossible task depending on how the smart contracts are coded—as long as the parties agree to it, or are otherwise ordered by a court to change it. [32] At the very least parties can mutually decide to "undo" a contract using the "self-destruct", "delegate call" or "call code" functions[33] and recreate a new, corrected contract.[34]

---

[27] See Generally, Carlill v Carbolic Smoke Ball Company [1893] 1 QB 256.
[28] Blaise Carron and Valentin Botteron, How Smart can a contract be*?, in* Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law 8 (Daniel Krause *et al* 2019).
[29] Melvin A. Eisenberg, Foundational Principles of Contract Law, 577 (2018).
[30] *Ibid.*
[31] *Ibid.* at 577-8.
[32] See Bill Marino and Ari Jules, Setting Standards for Altering and Undoing Smart Contracts, [2016] https://www.semanticscholar.org/paper/Setting-Standards-for-Altering-and-Undoing-Smart-Marino-Juels/91af4fd1a2de62ada8d8be2ad671b31479dea3d9 last accessed 7 Dec 2019. This article looks at the various coding options that can be implemented and against smart contracts to uphold classic legal principles of mistake.
[33] Solidity, Introduction to Smart Contracts, https://solidity.readthedocs.io/en/v0.5.13/introduction-to-smart-contracts.html last accessed 7 Dec 2019.
[34] See, Bill Marino and Ari Jules, *supra* n. 35; (positing various coding options that can be implemented and against smart contracts to uphold class legal principles of mistake).

However, courts may need to order more than simply reformation as the smart contract's automatic-execution will have already put the re-seller at a financial disadvantage. In the example provided, the re-seller has over-paid by 10% and a court order demanding the return of funds will also be required. While this goes beyond the normal remedy for mistranscription, as an equitable remedy in contract law, there is nothing stopping a judge from also incorporating the return of financial damages suffered as a result of the mistranscription.[35]

Notably, mistranscription is available even if one party "intentionally, rather than negligently, mistranscribes the parties' contract" thus, removing any ability for one party to fraudulently misrepresent the terms of the agreement to the other party's detriment. So, if the distributor was responsible for coding the contract, they cannot benefit from this power under traditional contract law. In the blockchain governance system alone, however, there is nothing stopping a code-writer from committing such *fraud in the factum*.

Mutual Mistake

Now, if the negotiations were done in code, with each party making changes to the code respectively to come to an agreement, and that code somehow executes an action or result that neither party intended, traditional courts may find a mutual mistake. Both parties thought the code would perform the act of releasing 50% of the payment at each stage; they have a tacit assumption[36] that the code will perform what they intended and thought they coded it to. Such an error in the code would be akin to a typographical error in a traditional contract which, so long as the courts can infer the parties' intent from the rest of the contract (e.g. total purchase price from which the percentages are drawn in this case) the contract will not be found ambiguous and unenforceable.[37]

Unilateral Mistake

From a traditional contract law perspective, the code itself in the example provided has also created a unilateral mistake. By sending too much money, which the distributor should know is a mistake, the code has caused the re-seller to make a mistake according to the originally agreed price. Once again, while the blockchain's "code is law" persuasion offers no remedy, contract law would find such a mistake required correction and the distributor would be ordered to re-pay the amount owing. Going forward, the automated-contract would either need to be reformed to correct this coding error or a court order would demand that re-payment occur each month— an easier but less efficient solution.

Fraudulent Misrepresentation

There are also opportunities for fraudulent misrepresentation in smart contracts which blockchain governance alone cannot correct. Suppose, perhaps, the distributor made some claims about the product that they knew were not true but critical to the re-seller's decision whether to contract or not.[38] Provided the re-seller relied on these claims and suffered harm as a result of the untruth, this is a fraudulent misrepresentation and renders a traditional contract voidable and may make the harmed re-seller eligible for compensatory damages.[39] However, once again, blockchain governance alone has no system for dealing with such situations. So, if the distributor knows that representing their product as better than it is, will get them a higher purchase price and influence the re-seller to sign the contract, they could take such action without fear of ever having to be held accountable.

[35] Notably, the court would also likely find a unilateral mistake resulting from the payment already made which is discussed later.
[36] Melvin A. Eisenberg, *supra* n. 29, 582.
[37] See, Corbin on Contracts §§ 25.19, 28.45 (describing various typographical errors as mutual mistake); *Starr v. Union Pac. R.R. Corp.*, 31 Kan. App.2d 906, 909-10, 75 P.3d 266 (Kan. Ct. App. 2001) ("errors in contracts, which do not create such inconsistency that the overall intent of the parties cannot be determined from the four corners of the instrument, do not result in an ambiguous contract but merely create an inconsistency subject to interpretation by the court considering the contract as a whole.").
[38] LII, Fraudulent Misrepresentation, Cornell Law https://www.law.cornell.edu/wex/fraudulent_misrepresentation# last accessed 7 Dec 2019.
[39] *Ibid.*

Breach of Contract

The risk for fraud in smart contracts seems to run quite high. In the specific example given, the ability for the distributor to profit off a fraudulent misrepresentation about the product could be rectified by changing the code so that the contract does not release the final payment until after the re-seller has inspected the shipment. However, replacing the (presumably) neutral shipping company with a party to the contract creates new opportunities for fraud. Should the re-seller decide to keep the product but not fulfill its role as the Oracle and prompt the smart contract to release final installment, the power to commit fraud merely shifted from one party to the other. The only thing that may stop the re-seller from committing such an act, is, of course the fact that his/her funds are tied to a wallet (presumably interest free) until the contract term has lapsed.

Suppose, however, there was an additional term that automatically charges the distributor a significant late-fee if they have not shipped by a certain day of each month. Without a remedy for breach of contract in the blockchain governance, the distributor would be trapped in an agreement where they would continue to lose money whether they shipped or not. Meanwhile, the re-seller may be happy to remain tied to the idle contract and collect the late fee until the contract has run its term.

The lack of remedy for breach of contract in blockchain governance necessitates judicial intervention. While smart contract advocates stipulate that breaches are not possible in automated code-based agreements, the examples above have proven that as long as any human action is required or any nexus with the “real world” occurs, the opportunity for fraud and breach are a reality.

Furthermore, smart contracts do not allow purposeful breaches when situations change and one parties becomes unable to perform his/her role in the contract. This can occur in extreme situations where situations outside of the breaching party’s control make performance impossible (e.g. the product is simply no longer available or attainable). Alternatively, there may be situations where the subject matter or performance of the contract itself suddenly becomes illegal. In a standard contract, this would automatically make the contract void and permit a party to breach it by refusing to supply illegal products or perform illegal acts.

While there are many further examples we could explore, the common contractual issues raised above demonstrate a clear need for dynamic and case-by-case judicial governance of smart contracts despite their automated natures. Smart contract advocates who propose that blockchain governance could unseat the traditional legal system or that the traditional legal system has no role in interpreting smart contracts disregard the very legal foundations upon which freedom to contract is founded. Furthermore, without a respect for the rule of law and due process, contracts become meaningless as the ability to enforce them in the dynamic way required is severely weakened. As it stands now, the blockchain is unable to govern the myriad of conflicts to which even the best written (or best coded) contracts may give rise.

In the interest of efficiency, smart contracts themselves should be carefully constructed to minimize the potential for complex conflicts that cannot be addressed by blockchain governance. However, unless blockchain governance becomes dynamic and capable of equitable and fact-based remedies, the potential need for judicial intervention can only ever be minimized rather than eliminated.

Procedural Challenges

Having discussed the theoretical need for judicial intervention, interpretation, and contract law remedies in smart contracts, we must now turn to the practical implications. The decentralized nature of the blockchain's governance system, capacity for parties to remain anonymous, and the ability to easily (or unknowingly) contract with anyone around the globe presents practical challenges to civil procedure that the current American legal system has yet to address. The CoDC identifies multiple specific procedural challenges that those wishing to exercise traditional legal enforcement against smart contract parties face, [40] though anonymity is the root of all the problems they identify. If parties can be identified, then smart contracts do not differ that much from ordinary international or cross-jurisdictional contracts and civil procedure has established methods for determining personal jurisdiction, applicable law, and enforcement procedures. While in a traditional cross-jurisdictional contract the parties would know the risks of contracting with an out-of-state/country party, such risks should be assumed by those in smart contracts as well given the blockchain's decentralized nature.

While the fictional contract we explored above was quite traditional in the sense that the parties presumably knew each other, many smart contracts take place between anonymous parties. For instance, should I want to trade Bitcoin for Ether when the exchange reaches a desirable rate, I may simply publish a contract to the blockchain thus, allowing anyone, anywhere to contract with me using their private but, anonymous key. Furthermore, while actors within Distributed Autonomous Organizations (DAOs) hold different powers within a coded-venture—Creators, Investors, Contractors, and Curators—and potentially different levels of liability depending on the cause of breach, they remain anonymous to the other parties in the venture. In the event of a fraud or an attack like the one that happened against The DAO, how can one take legal action if they do not know the offeror or offeree?

Identifying and Serving Parties

In one-to-one contracts, bringing an action requires an ability to identify who you contracted with. Similarly, while DAOs sit outside the realm of traditional corporate law, they may be considered general partnerships or unincorporated associations.[41] In such cases action can be brought against individuals as long as they can be identified.

In a traditional contract, an inability to find your co-contractor will necessarily bar one from taking further legal action. However, the statute of limitations can be paused and subpoena rights created by filing a case against a fictious defendant (i.e. "John Doe lawsuits") and using the time between filing and trial to locate the missing party. Presumably a court would allow the same to be done in smart contract situations, but the success rate of identifying an otherwise anonymous contracting party on a smart contract platform or DAO is highly circumstantial.

There are several ways to attempt to identify someone using their blockchain wallet address. For instance, people may post such an address elsewhere on the web which may have trace connections to their actual identities linked to email addresses, social media profiles, and IP addresses (though these are maskable using a VPN), etc.[42] One may also look at other transactions within the wallet to determine things like location and trace their initial entry into the blockchain using traditional banking systems. While more complex computer forensics, like those conducted by companies like Chainalysis, may not be feasible or attainable for individuals wishing to bring action, the potential to subpoena information on transactions processed through official exchanges may shed light on a wallet's owner.

[40] Bijuesca et al. *supra* n. 10, 31; (a) potential lack of personal jurisdiction over parties (assuming they can be identified) and the smart contract platform itself; b) difficulties in determining applicable law given no clear place of contracting or performance or subject matter; c) difficulties in enforcing monetary damages against anonymous and potentially distant parties; d) inability to stop automated-code without cooperation of parties or platform; e) inabilities to determine the location of the distributed ledger and who to serve if the platform is at fault.).

[41] Steven Palley, How to Sue a Decentralized Autonomous Organization, (Coindesk, 20 Mar 2016) https://www.coindesk.com/how-to-sue-a-decentralized-autonomous-organization, last accessed 7 Dec 2019.

[42] Ajay Chandhok, BLOCKCHAINS AREN'T ANONYMOUS. BUT THEY CAN BE, (LedgerOps) https://ledgerops.com/blog/blockchains-arent-anonymous-but-they-can-be/05/01/2019, last accessed 22 Nov 2019.

However, the success of such actions can vary by situation and provide limited comfort to those considering smart contracts. Those hoping to avoid such ambiguity going forward, may consider identifying parties or providing contact information for them within the smart contract code or an authoritative plain-language version of the coded contract. Much like a traditional contract, writing in these more standard pieces of information will take the guess work out of a court's ability to enforce a smart contract, should the code malfunction or parties' relationship otherwise breakdown.

Interestingly, there is potential for service of process to be conducted via the blockchain, thus removing the need to actually know the parties' identity or physical address at the initial states of a litigation. According to *Federal Rule 4(c)* procedural requirements, service of process is fulfilled provided it is accompanied by a copy of the complaint and issued by any person over the age of 18 years and not a party to the complaint.[43] Thus, in order to serve on the blockchain, a complainant would need to open a new smart contract offering to pay someone else on the blockchain to send the notice to someone else. If the recipient is outside the USA, however service must be given "by any means of internationally agreed means of service."[44] Whether the blockchain is considered such an appropriate channel under The Hauge Convention which governs this matter[45] is unclear, however according to Article 11 signatories are permitted to agree to their own appropriate communication channels[46]—for ease, the blockchain should be designated along with the choice of law clause within the smart contract.

However, if parties do not reply to this summons or comply with court orders, the value in knowing their identity and the other physical assets that a court can seize still stands. Again, though perhaps more common in smart contracts, the implications of an unknown contracting party are not unique to smart contracts—and unknown party in a traditional contract will present the same challenges.

Serving the Platform

In cases where parties cannot be identified one may also be able to bring action against the smart contract platform itself and its creators or controllers if such a structure exists. The Ethereum Foundation, for instance, set a precedent in 2016 when it intervened to unwind unwanted transactions resulting from a hacker exploiting faulty code in The DAO. In this instance, the Ethereum Foundation took action independently and created a hard-fork to undo the unwanted results of the hack. While a soft-fork was proposed,[47] the contentious nature of "fixing" a mistake that many though was fair under a "code is law" ideology – including the hacker himself[48] – meant that any hope of all nodes adhering to a new version of Ethereum and completely abandoning the original blockchain were far flung. So, Ethereum decided to take sole responsibility for correcting the "mistake" with a god-like action to override blockchain governance.[49] The hard-fork created a new version of Ethereum and while contentious and hotly debated, it was supported by 97% of Ethereum holders; still, today, we have two versions of Ethereum as a result: Ethereum Classic, and Ethereum 2.0 which continues to be developed.

Notably, the Ethereum Foundation, besides being the creators of the Ethereum blockchain upon which The DAO ran, held no direct responsibility for smart contracts that were exploited or creating the malfunctioning code. The inserted themselves into the situation because The DAO contained roughly 15% of all Ether and its failure would have negatively impacted the Ethereum network and value as a whole.[50] Very likely, the Ethereum Foundation also realized that despite the blockchain community's

[43] See, Federal Rule 4(c) (1-2) https://www.law.cornell.edu/rules/frcp/rule_4.
[44] Federal Rule 4 (f)(1) https://www.law.cornell.edu/rules/frcp/rule_4.
[45] See, *Volkswagenwerk Aktiengesellschaft v. Schlunk*, 486 U.S. 694 (1988) ("The [Hauge] Convention provides simple and certain means by which to serve process on a foreign national.").
[46] Hague Service Convention and Signatories, Art. 11 https://www.courts.ca.gov/partners/documents/ea_HagueService.pdf
[47] Michael del Castillo, The DAO: An Analysis of the Fallout, (Coindesk 18 Jun 2016) https://www.coindesk.com/the-dao-an-analysis-of-the-fallout last accessed 10 Dec 2019.
[48] Gautham, DAO Hack, Attacker Sends Open Letter to Ethereum Community, (NewsBTC, 2015), https://www.newsbtc.com/2016/06/18/dao-hack-attacker-sends-open-letter-to-ethereum-community/ last accessed 10 Dec 10 2019.
[49] Michael del Castillo, *supra* n. 50.
[50] David Siegel, Understanding The DAO Attack, (Coindesk, 27 Jun 2016) https://www.coindesk.com/understanding-dao-hack-journalists last accessed 10 Dec 2019.

insistence on being outside the traditional legal system, people had invested real money in The DAO which meant there were implications in the "real world" where national laws exist; any potential for the Foundation to be held legally liable would have been something that Vitalik and the other foundation members wanted to get ahead of. As David Siegel posited in an article preceding the foundation's hard-fork solution:

All parties here may have legitimate claims that could take years to settle out in courts around the world. […] It's also very likely that there will be lawsuits. We could see a total mess, with lawsuits extending for many years. […] Even though the letter and the spirit of smart contracts is that "smart contracts rule," and the rule of law doesn't apply – in this case, most people would like to see a do-over. I'm guessing we will see various rules of law apply.[51]

Unfortunately for blockchain advocates, the Ethereum Foundation has now proven its ability to override the "immutable" blockchain which, should it happen again soon or too often, may undermine the Ethereum blockchain's credibility altogether and prompt a mass exodus from the platform. For traditional-law advocates, however, the Ethereum Foundation's new-found power, so to speak, presents it as a viable party who can be subpoenaed to carry out court-orders resulting from legal action even when individuals cannot be found. An injured party may be able to bring action against the Foundation for any harm they suffered as a result of a contract made on the Ethereum blockchain and the Foundation may be compelled to correct it.

Now, this solution will only work in situations where the contractual intent was clear and the execution clearly contrary (e.g. fraud, some mistranscription, coding errors) and courts do not require the other anonymous party's presence in order for it to establish what both parties intended. Furthermore, the practicality of forcing Ethereum to conduct a hard fork for every minor contract dispute is incredibly limited. The Ethereum 2.0 fork received 97% consensus because the hack had, arguably, put all the claims about smart contracts being safer and more certain than traditional contracts into question; allowing one hacker to drain huge sums of money out of The DAO and claim that he had the right to do so because of a flaw in the code offended blockchain political (and perhaps group morality?) of the blockchain community. But, for less political or offensive contract breaches, the blockchain may not be as willing to consent to a fork given the amount of effort it takes.[52] Therefore, while a court could theoretically order the Ethereum Foundation to release a new version of the blockchain that unravels the smart contract in question, it will have very little control over whether that version is accepted by the nodes governing the blockchain itself.

[51] *Ibid.*

[52] See generally, Jordan Heal, Hard forks: Contentious or not?, (Coin Rivet, 16 Jan 2019) https://coinrivet.com/hard-forks-contentious-or-not/ last accessed 10 Dec 2019; Furthermore, there are security risks associated with hard forks like "replay attacks" that allow a transaction on one fork to be recreated on another thus allowing dishonest users to get free coins on the secondary blockchain. See for instance, SFOX, Life after Hard Forks: What You Need to Know About Replay Protection, (Medium, 1 Feb 2019) https://blog.sfox.com/life-after-hard-forks-what-you-need-to-know-about-replay-protection-ab8adaf6ddf6 last accessed 10 Nov 2019.

Conclusion

In conclusion, while Smart Contracts themselves are not substantively different from traditional contracts, the decentralized nature of the blockchain does present some procedural challenges for those seeking traditional remedies. This does not mean that all is lost for smart contracts, however. Their value in streamlining simple enforcement and potentially removing frivolous contractual disputes from the court system should not be discounted. However, serious contractors will need to put a significant amount of effort into their smart contract formations to ensure the valuable flexibility that traditional contracts offer, which necessitates fundamental operations of rule of law and due process, is incorporated. For instance, parties can remedy many of the enforcement and flexibility issues discussed in this paper by writing plain-language terms to accompany smart contracts that designate forum of law, formally identify both parties, and agree service of process methods. The code itself can also be written with built in "outs" that parties can decide to execute together should they need to breach or change the contract in some manner; Bill Marino has proposed a valuable set of coding standards for those hoping to have useful and valuable smart contracts to adopt. [53]

Unlike traditional contracts, the smart contract requires two types of expertise to ensure proper drafting: technical and legal. For those who are daunted by the marriage of computer languages and legalese, start-ups and technology companies are forming legal-tech partnerships to pave the way. From RocketLawyer announcing its partnershmeip with OpenLaw and ConsenSys to bring smart contracts to everyday consumers, to LegalZoom announcing a partnership with Clause to provide blockchain based smart contracts to their customers as well, Smart Contracts are starting to enter the mainstream.[54] Guidance from these fusions of legal and blockchain experts will only do good things for the viability of smart contracts going forward. The future of smart contracts will be neither a new eutopia of litigation-free contract law, nor a futuristic dystopia of cold code-based law. Rather, if done properly, smart contracts are an opportunity to bring current contract law into the 21st century and improve the efficacy of our legal system overall.

Tiffany M. Sillanpää

Tiffany M. Sillanpää holds an LL.B from The City Law School (City, University of London) and an LL.M in U.S. Law from The New York University School of Law. She is currently in the process of qualifying as a solicitor in Canada and New York, and plans to cross-qualify in the UK as well. Her primary legal interests revolve around Commercial Law and legal challenges facing technology companies and market disruptors. In her spare time, she writes a blog titled The Transition which is dedicated to helping UK Law graduates navigate North American legal qualification and develop commercial awareness in Canada, the United States, and the United Kingdom by discussing notable legal developments across all three jurisdictions.

[53] See Bill Marino and Ari Jules, *supra* n. 35; (looking at the various coding options that can be implemented and against smart contracts to uphold classic legal principles of mistake).
[54] Amy J. Schmitz and Colin Rule, Online Dispute Resolution for Smart Contracts, [2019] University of Missouri, 110.