CARLTON FIELDS

Set It and Regret It?: Smart Contracts, Injunctions, and Fraudulent Transfers, Part I

October 24, 2019

Smart contracts built on top of blockchains may create recurring violations of injunctions and new ways to conceal fraudulent transfers. In the first half of this series, we will discuss the collision course set by smart contracts and court orders awarding injunctive relief.

Introduction:

Smart contracts, initially discussed by Nick Szabo, suggest that "contractual clauses (such as collateral, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive." The combination of computer hardware and software together, coupled with blockchains that allow computer code to direct transactions of value, creates opportunities to modify or supplant traditional contract-based relationships, and has spurred a burgeoning industry of smart contract developers testing and developing new products. Their value proposition is simple: smart contracts can be valuable to parties who want to apply code driven-logic to ensure that transactions occur in predictable ways, and to allow those parties to remove intermediaries who can stop their transaction ("censorship resistance") for reasons other than those of the parties to the transaction. Smart contracts make sense for transactions that are impractical to conduct via traditional contracts, or where an agreement cannot be practically enforced via the traditional justice system. Most smart contracts, based upon their design, will not comply with or act in accordance with court orders. This issue creates the significant tension that is explored below.

Max Raskin, among others, has argued that smart contracts should be viewed as a type of self -help; to Raskin, "[a]utomated execution of a contract is a preemptive form of self-help because no recourse to a court is needed for the machine to execute the agreement." However, as Kevin Werbach has noted, while self-help provides an extra-judicial means of dispute resolution, it is "traditionally judicially supervised;" self-help must be authorized by law, and rights to exercise self-

help are likewise limited by law. It is through the interpretive prism of smart contracts as a form of self-help that we will first examine whether smart contracts will lead to a plague of violations of injunctions and identify potential recourse for courts and creditors. In a follow-up blog, we will examine smart contracts' potential to create a rash of fraudulent transfers, and suggest strategies to avoid inadvertent fraudulent transfers.

Asset Freezes/Injunctions:

One potential limitation on self-help would be the entry of an injunction or asset freeze order ("injunction") that prevents both the party restrained and its creditors from taking any assets of value without Court approval.

To illustrate the potential issue, we discuss a hypothetical smart contract:

Person X and Person Y each transact 1 bitcoin to a smart contract on September 1, 2020 that is coded to pay 2 bitcoins to Person X if Candidate 1 is elected President of the United States, or pay 2 bitcoins to Person Y if Candidate 2 is elected President of the United States once the final result of the election is reported; if neither candidate wins the election, each party receives back their contributed value. (We will ignore transaction fees.)

An injunction freezing all assets of X is entered on October 1, 2020, but the smart contract executes on December 15, 2020 (after a lengthy recount and numerous lawsuits culminate in a decision by the US Supreme Court awarding the election to Candidate 2) and those two bitcoins are transacted by the Smart Contract to a wallet controlled by Y.

In that case, the execution of the smart contract may be viewed as a violation of the injunction, as some of the assets held by the smart contract may be considered to be property owned by X. In such a case, who should be liable for the violation of the injunction?

It is tempting to look to X, the transferor who sent value to that smart contract; however, if the transfer occurred prior to the entry of the injunction, it would be unlikely that the transfer of assets would be considered a violation of the injunction. (As a practical matter, we will ignore potential preference or fraudulent transfer issues until part 2 of this series).

Person Y, the recipient of the assets held by the smart contract, may be viewed as violating the injunction by taking the value contributed by X in the above hypothetical when the Candidate 2 is elected. However, X and Y may not know each other's real-world identity. In many cases, counterparties to smart contracts may be pseudo-anonymous and thus not be easily identifiable. In that case, that counterparty may not have any notice of the injunction, which suggests that enforcement by the court against that transferee for violation of the injunction may be practically

impossible, or inappropriate on due process grounds. Also, it may be inappropriate to punish the transferee (or the transferor) if neither party took an active role in triggering the smart contract; however, if the smart contract was to be executed at the whim of X, or based upon some other conduct of X, then X may be viewed as being in control of the transaction, which would suggest that X intentionally transferred the value to Y in violation of the injunction.

If the smart contract is being used in a way that subjects the operator or beneficiary of the smart contact code to laws requiring Anti-Money Laundering/ Customer Identification Program ("AML/CIP") compliance under the Bank Secrecy Act ("BSA") or other applicable law, and if that party actually complies with those obligations, the smart contract's operator or beneficiary may know the identity of the transferor of value into the smart contract, and may be viewed as an intermediary holding assets for the transferor, like an escrow. However, in the absence of this compliance, it is likely that participants in the smart contract are only identified by public key addresses, which complicates efforts to identify transferees. In short, it may be impossible or infeasible to identify the transferee or transferor, which would complicate efforts to hold them liable for receiving a transfer of assets in violation of an injunction.

What about the smart contract itself? Can a smart contract violate an injunction? Smart contracts are typically computer code operating on a decentralized network of computers. Generally, computer code does not have legal personality. However, a Court may look to the party who implemented the computer code or who otherwise benefits from the execution of that computer code ("code operator"), if they can be identified. The code operator may have written the smart contract code or may simply be deploying code previously written by others (which goes to the intent and knowledge of that code operator). In some cases, the smart contract code may be implemented without the code operator taking any action to solicit or induce the transferor to transfer value into the smart contract; in many cases, the code operator may not know who transferred value into that smart contract. In that case, it may be illogical and inconsistent with US regulatory policy to impose any obligation to comply with an injunction upon the code operator, and it would be difficult to ascribe liability upon that code operator.

Finally, a Court may attempt to compel performance by the oracle responsible to supply the information necessary to trigger the smart contract code. The effectiveness of this approach will depend on whether a Court or party can identify and control the oracle via court order. The oracle itself may be a person or entity amenable to process, or may itself be mere code, whose writer, implementer, or beneficiary may be difficult or impossible to identify. For example, the oracle may be a data feed from the national weather service that provides temperature readings for a given location. In the above hypothetical, the oracle may be a news reporter working in Washington DC, or a script that attempts to pull information from a news web site. Even assuming that a Court can identify and use its power to compel the oracle, the oracle generally cannot modify the smart

contract code; the oracle may only be able to cause the smart contract to execute, or prevent the smart contract from executing.

Thus, a smart contract may violate an injunction without a clear answer of who, if anyone, may prevent a violation, or properly be held responsible. The transferee of the value caused by the execution of the smart contract may be liable for improperly receiving value in violation of the injunction, but that transferee may have received no notice of the injunction, and may not be identifiable. The code operator may be liable for creating the structure used to transfer value in violation of the injunction, but also may not be identifiable, may not receive notice, or may have acted without knowledge and intent. Smart contract code itself has no legal personality and cannot be held legally liable for violations caused by other parties using that code. Acting against the oracle may prevent a transfer, but may not permit the value held in the smart contract to be returned to the transferor. A Court may be able to recover the value transferred if the transferee is identifiable and amenable to process; if not, the Court may lack recourse. The result may be that smart contract technology could be used or abused to violate injunctions (and as will be discussed in Part 2, to commit fraudulent transfers).

Automatic Stays

Another example of a legal limitation on self-help is the automatic stay created by 11 USC 362 upon the debtor filing a petition for relief under the US Bankruptcy Code. The automatic stay operates as an injunction against certain activities affecting the debtor and assets of the debtor's estate. The purpose of the automatic stay is to allow the debtor temporary relief from burdens created by mounting debt and creditors efforts to collect on that debt and to allow the debtor to reorganize, or to allow the court to determine the rights of various creditors to assets of the debtor's estate.

These limitations include actions by a creditor "to obtain possession of property of the estate or of property from the estate or to exercise control over property of the estate." *See* 11 USC 362(a)(3). The debtor's estate is defined to include all of the debtor's legal and equitable interests in property. Legal characterization of a debtor's interest in property is based upon state law; a Court may determine that a smart contract containing value transferred to it by the debtor prior to the automatic stay is subject to the injunction created thereby, and need to evaluate the legal status of the value held by that smart contract.

Depending on the Court's view, smart contracts that have yet to execute and that hold value contributed to them by a debtor may be viewed as violating a subsequently entered automatic stay if they later transact that value to anyone besides the debtor. For more discussion of this concept, *see* Raskin, and this blog by Alan Rosenberg, both of which frame the discussion by reviewing cases examining the use of automobile starter interrupters that affect debtor property rights after the entry of the automatic stay.

To illustrate the legal analysis, we will examine a different hypothetical smart contract structure.

Person X funds a smart contract on October 31, 2019 that is coded to pay that value to Person Z if Person A does not pay some value to Z on X's behalf by January 1, 2020; if Z confirms receipt of that other value from A, the smart contract would send the value held by the smart contract back to a wallet controlled by person X. (Again, we will ignore transaction fees.)

Under this hypothetical, if X subsequently files a petition for bankruptcy relief on November 15, 2019, creditors of X would receive a Notice of Automatic Stay which obligates that creditor to refrain from any collection activity. Although the arrangement in this hypothetical resembles that of a traditional escrow, there is one key difference- in the above hypothetical, there is no escrow agent to serve.

Most traditional escrows include a legally identifiable actor who agrees to provide escrow services for a fee; that actor typically will be identified in an escrow agreement and in most circumstances will be amenable to service of process, including of a Notice of Automatic Stay. However, in the above example, there may be no person or entity to receive the notice of automatic stay; the smart contract is mere code operating on a blockchain, which not amenable to process, as discussed above.

It is possible that a smart contract could be viewed by a bankruptcy court as a type of escrow agreement. Likewise, a court may view a smart contract as an executory contract, which is generally defined as a contract where both parties to the agreement still have pending obligations to perform under the contract. In that case, the debtor may have the right to abandon the contract and decide to not perform. However, given that the debtor contributing value prior to the filing of her petition in the above hypothetical owes no further performance, the contract may not be considered by a bankruptcy court to be executory.

Although there is considerable nuance as to the property rights issues at bar, including whether the specifics of the agreement create a tenancy in common, joint tenancy, a bailment or a custodial trust, we suggest that a bankruptcy court will likely construe the smart contract configuration to be a form of an escrow.

Assuming the Court considers the smart contract to be an escrow, certain states' laws would consider the funds in escrow to belong to the escrow agent, and the principals under that escrow agreement have a contractual (i.e. "contingent equitable") right to delivery upon satisfaction of conditions specified in the escrow agreement. In those states, that contingent equitable interest is the property of the bankruptcy estate, not the escrowed assets.

When evaluating an escrow, a court will generally look to the terms of the escrow agreement to determine if there is a real escrow arrangement. As discussed in this outstanding blog post, Courts will consider the arrangement to be an escrow if the event triggering the release of value from escrow is objective and beyond the discretion of the debtor who contributed value to the smart contract. If the claimed escrow allows the debtor to exercise discretion over the funds in the escrow, it is less likely to appear to be a real escrow. If the smart contract itself limits disbursement of value to objective criteria not under the debtor's control (in this case, the debtor contributing value does not control the oracle or the circumstances to be reported by the oracle to cause the smart contract to execute) and transfers by the smart contract do not reduce the debtor's debt, the value contributed to the smart contract may be viewed by a bankruptcy court as property outside of the bankruptcy estate and thus not subject to the injunction created by the automatic stay.

(There is some controversy as to the treatment of pending escrows at the time of the entry of the automatic stay under bankruptcy law; the prevailing view is that an escrow that results in the debtor losing their contingent right to some property held in escrow by circumstances that do not violate the automatic stay themselves does not violate the automatic stay, but if the actions that trigger the release of the escrowed property from the debtor to a third party themselves would violate the automatic stay, the release of escrowed property is also a violation of the automatic stay. However, most courts would agree that a smart contract structured to sweep funds away from a debtor upon the receipt from an oracle of notice that a bankruptcy action was filed, would be an improper *ipso facto* clause that would probably be reversed.)

There are some complications in applying this analysis to smart contracts. First, many smart contracts do not incorporate conventional legal agreements; others may include oral agreements, and others still may include formal agreements along with smart contract code. Thus, a Court will be forced to confront the question of what precisely the parties agreed to do when using the smart contract, and what sources should be considered dispositive of their agreements. A Court engaged in the above analysis may either conclude that (a) there is no escrow agreement at all, or (b) there is an escrow and the Court needs to understand the terms of the smart contract code to identify what the parties intended, or © there is an escrow and the Court needs to understand the terms of the smart contract code and of any other agreements related to the value at issue to identify what the parties intended.

Judicial interpretation of code is itself is a tremendously complicated issue, which may necessitate expert testimony to determine the meaning of the smart contract code, and potentially lead the Court to absurd or problematic strategies of interpretation, such as a Court's examination of the code writer's intent in the *B2C2 v. Quoine* opinion issued by a Singapore court. Assuming the court opts to evaluate the code, the court would next need to identify the potential recipients of transfers by the smart contract code and to determine whether the debtor has any influence over the oracle that is expected to supply the data to trigger the smart contract to execute. As discussed above,

identification of parties who may receive value from a smart contract may be difficult or impossible. However, a court will probably be able to determine if the debtor who contributed value into the smart contract has any ability to control the oracle, and may determine if they know the counterparty potential transferee.

Thus, in the above hypothetical, debtor X, at the time of filing his petition for relief under the Bankruptcy Code would probably be viewed as having a contingent right to the assets held by that smart contract, which right would be considered to be an asset of the debtor's estate in bankruptcy. Thereafter, if the smart contract executes by its terms and sends Z the value, there may be a violation of the automatic stay.

So…now what?

What are some potential solutions? Some, like OpenLaw, have suggested that smart contracts should be designed to allow for modification or termination after value has been deposited but prior to execution. Others, like ZeroLaw, suggest a model of code deference, wherein parties to smart contracts agree to resolve disputes without resort to the conventional justice system. (It is not clear that such provisions would be enforceable in bankruptcy or otherwise).

A smart contract with an "Escape hatch" that terminates the contract when the oracle or other empowered third party is served with a court order may be helpful, but the party who has the ability to cancel the smart contract must be identifiable and amenable to service. This inclusion of a third party breaks the immutable character of the smart contract and introduces new vulnerabilities into the smart contract. Introducing new intermediaries may undermine trust reduction or censorship resistance and thus defeat the purpose of using smart contracts in some instances.

Rosenberg, noted *supra*, suggests that smart contracts may use oracles that search PACER to look for Notices of Automatic Stay prior to executing, or that a contract require a party to sign the smart contract to confirm that there is no automatic stay pending upon execution, which Rosenberg acknowledges would eliminate the automatically-executing character of the smart contract.

Rosenberg's suggestions make sense when conventional transactions featuring full disclosure of the parties' identities are conducted via smart contract; in the more likely instance of a smart contract among pseudo-anonymous parties, these suggestions are inapplicable. Although parties are free to create smart contracts including oracles that check court dockets, this would ultimately require an oracle that can search for injunctions issued by any court in the US, or perhaps worldwide which may be unreasonable or technically infeasible.

These observations lead to a few inescapable conclusions. First, smart contracts that respond to court orders may be useful for parties who intend to use smart contracts as an "execution layer" in

conventional contractual undertakings, where they want traditional law to be enforced in their agreement. However, the complexity and uncertainty in the use and interpretation of agreements manifested only by the entry into bare smart contracts for traditional agreements may outweigh any efficiency achieved by opting to document their agreement using only code. For the parties and the subject matters for which traditional contracts (and traditional dispute resolution) are not available, smart contracts may be more efficient, effective and useful. In those situations, the lack of responsiveness to court orders may be an intended and desirable feature.

How should courts look at this second type of agreement? Most likely, they would refuse to enforce agreements that deal with parties lacking in capacity or regarding subject matter that is not enforceable. In such a case, courts may conclude that these agreements are void, and if they are able, seek to compel transferees to return the value obtained in violation of the Court's order awarding injunctive relief. Raskin argued that courts should police smart contracts *ex post*, and should allow smart contracts to be enforced unless they were unconscionable or violated public policy. Does every smart contract that cannot comply with an injunction violate public policy?

In part 2, we will discuss the implications of these agreements potentially creating a rash of fraudulent transfers. Stay tuned!

Reprinted with permission from Medium.

Related Practices

Blockchain and Digital Currency
Crypto Insolvency and Fiduciary Practice