Smart Contracts: Legal Considerations

Jack Gilcrest
College of Engineering and Computing
Miami University
Oxford, Ohio, USA
gilcrejp@miamioh.edu

Arthur Carvalho
Farmer School of Business
Miami University
Oxford, Ohio, USA
arthur.carvalho@miamioh.edu

***Abstract*—In this paper, we analyze the value of smart contracts and blockchains as an alternative to traditional contractual obligations. In particular, we start by exploring some of the advantages of these technologies, specifically the immutability of blockchains and automated contract remittance. We also discuss two critical shortcomings of decentralized smart contracts, namely regulatory uncertainty and a lack of confidential execution. With these issues in mind, we next explore how American legislators have begun to address smart contracts and blockchains. Though quite limited, there have been a few provisions clarifying the status of these technologies. We break down some of the language expressed in these bills so as to understand the current legal status of smart contracts and blockchains. Given this foundation, we consider the next steps that should be taken as smart contracts mature. This pertains to both the continued improvement of the underlying technology as well as the progress taken by regulators. Finally, assuming a futuristic scenario where there are no technological or regulatory barriers to smart contract adoption, we discuss how the process of contract remittance can be expedited in a world fully committed to the use of smart contracts.**

***Index Terms*—Smart Contracts, Blockchain, Contract Law, Remittance, Contract Dispute Resolution**

I. Introduction

The *Bitcoin* cryptocurrency [1] has experienced a meteoric rise since its conception in 2009. As an online payment system, the transactions involving bitcoins are stored in a public, distributed, decentralized, and shared ledger that requires no intermediaries such as a central bank. That distributed ledger, now called *Blockchain*, is immutable and auditable due to the use of cryptographic techniques, thus providing an uncensored source of truth. Given this definition, blockchains can be seen as special types of distributed database systems, *i.e.*, a data-analytics technology. Blockchains are special because they have distributed control, meaning that no single entity has the power to roll back or alter history, whereas traditional distributed databases are centrally controlled by an organization that can change access rules or modify records.

Blockchains have made possible event-driven, self-executing code statements called *smart contracts*. They allow for the encoding of rules and situations that are agreed upon by the various trading parties. These contracts autonomously execute pre-specified tasks, such as settling a contract, by examining changing environmental conditions in conjunction with the contract's embedded rules. Currently, there is immense regulatory uncertainty over the status of smart contracts and blockchains. Moreover, there are shortcomings in the technology that must be addressed before smart contracts can be fully embraced and adopted.

In this paper, we explore how smart contracts can disrupt and replace traditional contractual agreements. We start by providing a basic understanding of what smart contracts and blockchains are and how they achieve decentralization. Next, we evaluate the advantages and disadvantages of smart contracts as an alternative to traditional contracts. Thereafter, we analyze the language and precedents set by multiple state congressional provisions in the United States of America. This analysis is used to further propose potential developments required to see smart contracts become a standard aspect of contract law. Finally, assuming regulatory and technological issues are addressed, we theorize examples of a future that has moved from current contractual practices to smart contracts.

II. Smart Contracts

The idea of smart contracts was first proposed by Nick Szabo [2]. In short, a smart contract can be seen as a self-executable computer program that is able to carry out the terms of a contract or a business agreement between two or more parties. As automated algorithms, smart contracts execute when certain conditions are met. Suppose a smart contract C has the input conditions x, y, z, and produces an output operation Q. The underlying parties can trust that, for example, the smart contract follows the logic in Figure 1 every time contract C is executed.

Depending on the complexity of the input and output conditions, verifying x, y, and z may itself require calling a separate smart contract. Likewise, operation Q can be as simple as returning a Boolean value (TRUE or FALSE) or as complex as starting the execution of a logic tree in a separate smart contract. A smart contract might have an arbitrary amount of operational conditions, or may not even require any further condition besides its own initialization.

From a theoretical computer science perspective, modern smart contracts, such as implemented by the public blockchain platform *Ethereum* [3], are Turing complete, meaning that they can simulate any possible Turing machine. In practical terms, this means that modern smart contracts are able to successfully execute any arbitrary algorithm, from the simplistic procedure in Figure 1 to much more complex operations.

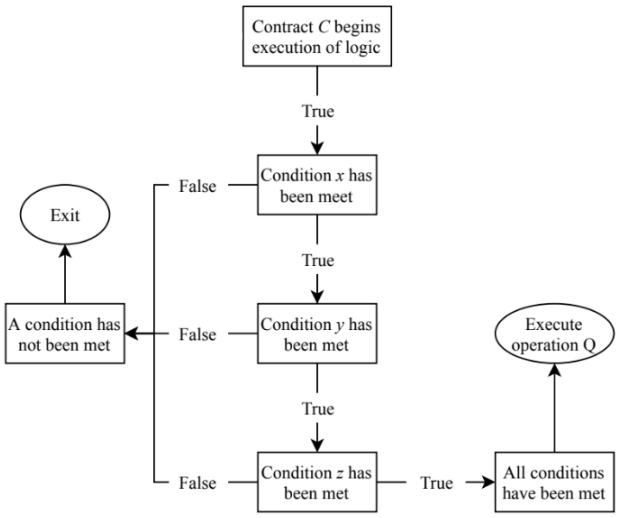

Fig. 1. Execution logic of a smart contract *C*.

It is interesting to note how smart contracts depart from traditional contracts when it comes to responses to contract violations. Specifically, traditional contracts rely upon: 1) a judicial system that decides upon the punishment a party deserves for breaching a contract; and 2) enforcement agencies to ensure that a punishment is followed. This reactive process can be fully automated using smart contracts since, as soon as a breach is automatically detected, actions can then be automatically taken. Consider for example the case when a bank and a company agree upon a loan covenant, where the conditional term is encoded into a smart contract. The smart contract can then monitor the conditions and activities of the company against the requirements previously agreed upon by the parties. Once a violation of the covenant is detected, the smart contract can then immediately trigger actions, *e.g.*, it can increase the underlying interest rate or issue a warning.

In the 1990s, without the recent advances in information and communication technologies, smart contracts were little more than a novel, but impractical idea. This has drastically changed after the rise of blockchains. The first blockchain was proposed by Satoshi Nakamoto as part of the Bitcoin cryptocurrency [1]. Citing an inability to transact with other parties over the internet without help from intermediaries, Nakamoto proposed the concept of a distributed and immutable ledger, which is now broadly referred to as blockchain. Among other features, Bitcoin relies on cryptographic signatures to provide control of ownership, and it financially motivates the members of a peer-to-peer network to validate new transactions. Since its conception, Bitcoin has experienced a tremendous success in terms of market capitalization[1], and it has also attracted considerable research interest (*e.g.*, see [4]).

Bitcoin is now considered the first version of blockchain [5], which is purely focused on the trading of cryptocurrencies. More recently, the term "Blockchain 2.0" has been used to define a much broader scope of financial applications [5], *e.g.*, transactions involving derivatives, digital asset ownership, *etc*. This is where smart contracts come into action, namely to expand the trading from digital currencies to a large variety of digitized products. As previously mentioned, Ethereum [3] is now the most popular smart-contract-enabled blockchain platform, and the second cryptocurrency in market cap[2], immediately after Bitcoin. Ethereum's release effectively sees Szabo's vision of self-executing, legally enforceable contracts becoming reality.

A. Smart Contracts and Blockchains

A smart contract executed in a centralized environment places too much power in the hands of the infrastructure owner, who in turn may, for example, try to change or even delete a smart contract. Blockchain, on the other hand, can provide sufficient decentralization. A block is a data structure that stores transactions executed on a network. Starting with the genesis block, a new block is expected to be added to the chain following a predetermined interval. Each block includes a reference to the block added before it, thus creating a chain of blocks. This append-only structure functions as a distributed ledger. To see why, consider the process of executing a transaction in Bitcoin's blockchain:

1) A computer (node) broadcasts its transactions to as many peers as possible.
2) The peers collect new transactions into blocks.
3) Each peer tries to solve a "computational puzzle" for its block.
4) The first peer who solves the puzzle broadcasts its block with the "solution" to all other network members.
5) Nodes accept the reported block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of a block by linking that block to previously reported blocks.

For such a decentralized environment to work, nodes must have incentives to behave appropriately, *e.g.*, to solve the computational puzzle and validate new blocks. Bitcoin achieves this by rewarding the first node that solves the computational puzzle. This means that nodes are essentially exchanging computational power and electricity for bitcoins. If a node tries to submit a block containing invalid transactions, each other node will likely invalidate the reported block and, consequently, the reporting node gets no reward. Thus, if a malicious attacker wishes to act against the interest of the Bitcoin network, it must commit enough resources to the validation process to control at least 51% of all validating power.

Once nodes add a suggested block to their local copies of the chain, the longer chain becomes the true state of the network, and the process of adding another block begins. Thus, consensus is achieved in a distributed fashion. Assuming that a single node is not able to consolidate validation power, the

[1]At the time of writing, Bitcoin's market cap is over $110,000,000,000 according to CoinMarketCap (http://coinmarketcap.com).

[2]At the time of writing, Ethereum's market cap is over $20,000,000,000 according to CoinMarketCap (http://coinmarketcap.com).

ledger then becomes decentralized and secure, thus satisfying the necessary conditions for a smart contract to function well. Blockchains can also store smart contracts. Once a contract has been published to the network, it will then perform exactly as specified without any maintenance or auxiliary input. This means that there is no possibility that a smart contract's operation produces unexpected results or that it can be violated.

B. The Case For Smart Contracts on Blockchains

The fact that a blockchain is a distributed, immutable ledger means that it allows for an easy auditing of all the transactions taking place on a (business) network. We next illustrate why the decentralization brought by blockchains provides the ideal infrastructure for smart contracts. For the sake of illustration, consider a hypothetical contract where Alice agrees to pay Bob $10 to wash her car. After signing the contract, Bob washes Alice's car and later claims that he has never received the amount of money agreed upon for the rendered service. Alice could then claim one of the following: 1) that she did pay in cash, but Bob did not issue a receipt; or 2) that she has already mailed a check to Bob, but Bob has never cashed the check. Dispute resolution can end up as "he said, she said", with potentially no way to prove whether or not Alice actually paid Bob or that Bob ever received the payment.

Now, consider the case where Alice and Bob use a smart contract on a blockchain network to record and process their car-washing transaction. In particular, both Alice and Bob digitally sign a contract stating that Alice will pay $10 after her car is washed, and that contract is safely stored on a blockchain. Moreover, both parties agree on using a device that detects the status of the car, *e.g.*, dirty or clean, and the smart contract periodically requests data from that device. Recall how a smart contract is an event-driven execution of an action. Alice and Bob have entered into a contract that will automatically move $10 from Alice's account to Bob's account when the status of Alice's car changes from dirty to washed. Once that condition is met, Alice automatically pays Bob $10 without either having to do any extra manual work. If the contract is not fulfilled because, say, Alice did not have enough funds to cover her costs, then Bob can take Alice to court and prove in a definitive manner that at no time did he ever receive a payment from Alice. Thereafter, it is rather straightforward to perform auditing procedures aiming at showing whether or not Alice ever sent $10 to Bob by checking the blockchain's transaction history. This shows how smart contracts have the potential to prevent and/or quickly resolve contractual disputes.

The above hypothetical scenario relies on the existence of an IoT device that measures the cleanliness status of a car, which might not exist today. However, there are some groundbreaking business ideas that rely on smart contracts and are already in use. For example, the company Etherisc[3] provides parametric insurance based on smart contracts. Specifically, an insurance policy, represented as a smart contract, can automatically trigger insurance payouts based on predetermined parameters, *e.g.*, a flight delay or the proximity of a Category 5 hurricane to the policy owner's house. The bottom line here is that the immutability of the environment smart contracts are executed in can revolutionize the way parties settle legal agreements. Nonetheless, as we discuss throughout this paper, while the technology is quickly maturing, there are numerous regulatory uncertainties to be addressed before one can realize the full potential of smart contracts on blockchains.

[3]https://etherisc.com/

C. The Case Against Smart Contracts on Blockchains

Governments around the world and, in particular, in the United States of America, have begun considering and legislating smart contracts. However, as a new and continually evolving technology that poses serious implications on current legal systems, there are many legal issues related to decentralized smart contracts that merit both improvement and clarity.

For example, consider the statement "*good faith effort*", an implied contractual term. During the hearing of *Troutt v. City of Lawrence* in 2008, that statement was defined as "*what a reasonable person would determine is a diligent and honest effort under the same set of facts or circumstances*." Even still, "*what a reasonable person would determine*" is a subjective statement, leaving the door open for a dispute on whether or not a person is or was reasonable. The point of the above example is that virtually no action is completely objective. Evaluating the context by which an action was taken is, arguably, a core principle of the existence of a judicial system. For example, civil judges and a jury of peers exist because many laws and rules do not account for every possible situation. That said, if a smart contract is just a preprogrammed set of rules, how can we expect it to capture all possible situations so as be able to universally remove the need for lawyers, legal hearings, or formal dispute resolution? We argue that while smart contracts might generally be more effective and efficient than traditional contracts, they are not omnipotent, and are unlikely to ever be able to automatically resolve every dispute or conflict.

Further, in their current state, most smart contracts are not entirely confidential, *i.e.*, the trait that empowers blockchains is also one of its biggest detriments when it comes to regulation. For example, there is already uncertainty as to whether or not blockchains violate the Global Data Protections Requirement (GDPR) of the European Union. This happens because an immutable ledger is incompatible with the right to be forgotten. This is unacceptable both for EU regulation and for the purposes of many commercial contracts in the United States of America. By tracking the input and output of a smart contract, one can also argue that patterns can be identified and information can be inferred. If any party in an agreement is uncomfortable with the lack of confidentiality, then public smart contracts are insufficient to replace traditional contracts.

III. Current Regulatory Landscape

After briefly introducing smart contracts and blockchains in the previous section, we now shift our focus to current legislative endeavors, focusing primarily on the United States of America. Recent years have seen a number of state bills providing definitions for smart contracts and blockchain, as well as some loose rules on the government role and interactions within these mediums. We next illustrate some of the proposed bills in order to understand the ramifications on current and future adoption of smart contracts.

Arizona HB 2417[4] introduces basic provisions that declare the authenticity of fundamental aspects of blockchains and smart contracts. First, cryptographic signatures are considered sufficient to act as binding electronic signatures: "*a signature that is secured through blockchain technology is considered to be in an electronic form and to be an electronic signature*". The scope of electronic records is then amended to include blockchains: "*a record or contract that is secured through blockchain technology is considered to be in an electronic form and to be an electronic record.*" Finally, the use of smart contracts to enforce an agreement between parties is expressly permitted: "*smart contracts may exist in commerce. a contract relating to a transaction may not be denied legal effect, validity or enforceability solely because that contract contains a smart contract term.*" This latter point effectively endorses the use of smart contracts from a legal standpoint.

Nevada SB 398[5] provides many of the same definitions provided in Arizona's HB 2417. It starts by describing itself as "*an act relating to electronic transactions; recognizing and authorizing the use of blockchain technology; prohibiting a local government from taxing or imposing restrictions upon the use of a blockchain; and providing other matters properly relating thereto*." It is particularly interesting that this bill explicitly prohibits a local government from taxing or imposing any certificate, license, or permit on any person or entity using a blockchain or a smart contract. Furthermore, electronic contract and record definitions are amended to include smart contracts and blockchains. Generally speaking, the bill states that electronic records cannot be invalidated because they are stored on a blockchain, and that smart contracts can be sufficient for many contractual agreements: "*a smart contract, record or signature may not be denied legal effect or enforceability solely because a blockchain was used to create, store or verify the smart contract, record or signature.*" This last point, together with the following one, legally validates the use of smart contracts on blockchains: "*in a proceeding, evidence of a smart contract, record or signature must not be excluded solely because a blockchain was used to create, store or verify the smart contract, record or signature.*" The bill also outlines numerous instances where blockchains are not sufficient methods for transmitting a notice, such as *"the recall of a product, or material failure of a product, that risks endangering the health or safety of a person."*

Vermont H.868 12 V.S.A. 1913[6] declares important provisions for the legal authenticity of blockchains, *e.g.*, "*a fact or record verified through a valid application of blockchain technology is authentic*." It further states that if a record on a blockchain is disputed, the disputer has the burden of producing evidence to disprove the blockchain. More progressive than the other mentioned bills, Vermont's bill expresses that the identity and ownership of assets recorded on a blockchain are legally valid. The bill, unfortunately, does not explicitly deal with smart contracts.

Generally speaking, the above bills seem to suggest that a smart contract is a valid legal contract when it includes an agreement between multiple parties, consideration of value exchange, valid consent by all parties, and does not seek to accomplish an illegal goal. While these bills provide an essential foundation for the regulatory landscape to grow from, the current legislation concerning decentralized smart contracts is still far from ideal. The same is true regarding some features of that technology, as we discuss next.

IV. Necessary Smart Contract Developments

Let's return to the Alice-Bob car washing scenario. We now know that Alice and Bob can enter a legally binding smart contract. By doing so, their contract becomes entirely public (assuming the underlying blockchain is public). Moreover, Alice and Bob need to make sure that the blockchain network hosting their contract is authentic, and that electronically transferring assets is legally valid in their jurisdictions. Thus, each of these issues must be resolved before Alice and Bob see smart contracts as an advantageous alternative to traditional contractual agreements. Focusing on data confidentiality, we now explore two different solutions to solve this issue.

Private blockchains, often referred to as *permissioned blockchains*, are the first solution to the data confidentiality issue. They are distributed ledgers where users need permission not only to join the network, but also to access different transactions stored in the blockchain. Permissioned blockchains sacrifice anonymity in favor of being able to restrict the involved parties to only those strictly necessary. By restricting who can validate transactions in the network, it is far easier for either a single entity or a group of validators to gain majority validating power to force consensus and, thus, effectively decide which transactions are valid or not. Thus, in this endeavor, it is paramount that the blockchain is able to achieve a safe distribution of validating power between parties with unaligned interests. But at the same, members of a permissioned blockchain are known to each other, which might help preventing malicious behavior.

The second solution to the confidentiality issue is the use of the concept from cryptography called *zero-knowledge proofs* [6]. Researched far before blockchains, zero-knowledge proofs allow for a party to prove a mathematical statement without revealing any extraneous information that leads to that statement being true. In terms of smart contracts and

[4]https://www.azleg.gov/legtext/53leg/1r/bills/hb2417p.pdf

[5]https://www.leg.state.nv.us/Session/79th2017/Bills/SB/SB398.pdf

[6]https://legislature.vermont.gov/statutes/section/12/081/01913

blockchains, zero-knowledge proofs can ensure, among other things, that a certain contract or transaction is valid despite the fact that information about the parties and other transaction details remain hidden. Some ideas related to zero-knowledge proofs are now implemented by cryptocurrencies such as *Zerocoin* [7]. One of the major issues with Zerocoin is the sizable overhead resulting from the proofs when compared to, for example, Bitcoin. Another cryptocurrency, called *Zerocash* [8], fixes the overhead issue by making zero-knowledge proofs more compact and efficient to verify. However, both Zerocoin and Zerocash rely on public parameters to set up the cryptocurrency system. If one is able to figure out the random numbers used to define these parameters, then the security of the whole system is compromised, *e.g.*, one can no longer detect double spending of coins. This means that one must trust the entity behind the development and deployment of zero-knowledge-proof systems. Zero-knowledge proofs have a long way to go when it comes to reliable implementations, but they present a compelling method to create the confidentiality needed for further adoption of blockchains and smart contracts.

V. Implications of Fully Developed and Regulated Smart Contracts

Thus far, we have discussed the current regulatory landscape and technological developments required to mainstream smart contracts and blockchains. We now shift focus to the future, when the lack of transaction confidentiality and regulatory uncertainty are no longer barriers to the adoption of smart contracts. How would such a future impact some of the current legal and financial services?

In this futuristic scenario, smart contracts and blockchains can be used to "tokenize" virtually any valuable asset since blockchain is now sufficient to establish ownership. Moreover, it is likely that tokens will indisputably represent online identities, meaning that the ownership of assets and medical records, for example, can be referenced from an identity token. Now, when Alice wants to pay for a service or purchase a widget from Bob, they can then rely on a smart contract that tracks when Bob ships the widget, records each stop as the widget makes its way to Alice, and finally establishes that the widget has been delivered to Alice. Once the smart contract determines that the widget has been delivered, the previously locked up payment is then released to Bob. Finally, the smart contract deducts all applicable taxes, sends the money to an IRS wallet, and provides tax references for each involved party.

The point of the above example is to show that, as contractual conditions, monitoring, and remittance become largely automated, many legal services and financial institutions become mostly obsolete. Banks, for example, might no longer need to provide debit services as blockchains can store and indisputably prove that a certain amount of unspent money belongs to a certain individual (this is essentially what cryptocurrencies currently do). Further, the costly process of ACH and wire transfers is, for the most part, avoided because the underlying blockchain provides a fully auditable record of the funds. From a legal perspective, the ease with which standard contracts between businesses can be both created and resolved vastly reduces the need for arbitration and tailored contract design. In other words, the contract needs of many can be addressed by publicly accessible smart contract templates. Contract lawyers, now smart contract architects, might specialize themselves in creating contracts that cannot be easily defined through templates. Although speculative in nature, the above scenario highlights the potential of smart contracts and blockchains to greatly disrupt many traditional services.

VI. Conclusion

Blockchain and smart contracts have the potential to disrupt several business domains, ranging from supply chain and healthcare to finance and accounting. Similar to the status of the internet about two to three decades ago, there is currently tremendous excitement over the potential of blockchains and smart contracts. At the same time, there is also some anxiety surrounding the legal and regulatory aspects of those technologies since poor regulation can strangle innovation, however strong regulation can boost the adoption of a disruptive technology. In this paper, we highlighted some of the pros and cons associated with blockchain and smart contracts, how they can disrupt some well-established services, and reviewed some of the legislation proposed in the United States of America.

Generally speaking, we are currently witnessing, at least in the United States of America, the rise of regulatory systems that see value in blockchains and smart contracts and that understand that the right regulations lay the groundwork for innovation. Still, there is much work to be done to unleash the potential of those technologies. This is rather expected since, for example, after nearly three decades, societies around the globe are still struggling with legislating the internet (*e.g.*, the Federal Communications Commission in the United States has recently dismantled net neutrality rules). We nonetheless expect more meaningful legislation following groundbreaking applications of blockchain and smart contracts.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Available at: https://bitcoin.org/bitcoin.pdf, 2008.

[2] N. Szabo, "Smart Contracts: Building Blocks for Digital Markets," *EXTROPY: The Journal of Transhumanist Thought*, vol. 16, 1996.

[3] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Available at: https://github.com/ethereum/wiki/wiki/White-Paper, 2014.

[4] N. Jerdack, A. Dauletbek, M. Divine, M. Hult, and A. Carvalho, "Understanding What Drives Bitcoin Trading Activities," in *Proceedings of the 2018 Annual Meeting of the Decision Sciences Institute*, 2018.

[5] Swan, M., *Blockchain: Blueprint for a New Economy*. O'Reilly Media, Inc., 2015.

[6] O. Goldreich, S. Micali, and A. Wigderson, "Proofs that Yield Nothing but Their Validity or all Languages in NP Have Zero-Knowledge Proof Systems," *Journal of the ACM*, vol. 38, no. 3, pp. 690–728, 1991.

[7] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous Distributed E-Cash from Bitcoin," in *Proceedings of the 2013 IEEE Symposium onSecurity and Privacy*, 2013, pp. 397–411.

[8] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized Anonymous Payments from Bitcoin," in *Proceedings of the 2014 IEEE Symposium on Security and Privacy*, 2014, pp. 459–474.