SMART CONTRACTS: LAW IN THE AGE OF BLOCKCHAIN

Saurabh Bhalla, LL.B., Faculty of Law, Delhi University

ABSTRACT

Blockchain offers cryptographically secured transactions that are replicated across a network of computer nodes. The blockchain's reliance on public-private key cryptography, peer-to-peer networks and consensus mechanisms helps create a novel system of exchanges and transactions, which overcomes the issues of trust inherent in systems managed by intermediaries. A blockchain network enables not only transfer of digital currency without intermediaries, but also change of ownership status of an asset, smart contracts, transfer of land titles, and the like. Smart contracts, which are seen as agreements that can be executed automatically and may transform legal agreements into code, have generated particular interest in recent times. Proponents believe that smart contracts will replace traditional legal agreements (today's contracts written in standard legal prose) and by enabling code-based execution will obviate the need of lawyers, escrow agents etc. However, this scenario seems to be highly unlikely, at least in the foreseeable future. While smart contracts may be given legal sanction, they are likely to be only a part of traditional legal agreements, and not replace them as not all rights and obligations that are otherwise covered in a traditional legal agreement can find their way into the code of a smart contract. In this context, the paper gives an introduction to blockchain and thereafter moves on to one of its most innovative aspects: smart contracts. The next part seeks to answer whether smart contracts can replace traditional legal agreements. Subsequently, an attempt has been made to provide possible answers to questions about the legal enforceability of agreements, which include smart contracts, particularly in the context of India.

Smart Contracts: Law in the Age of Blockchain

Introduction

There has been an increasing interest towards blockchain technology, in general, and what have come to be known as 'smart contracts', in particular, in recent times. Proponents believe that smart contracts have the potential to replace traditional legal agreements written in standard legal language, and by enabling code-based execution of agreements they will not only lead to the "rule of code", but also obviate the need of lawyers, escrow agents etc.

Given this curiosity around smart contracts, their potential, limitations and related issues, the paper is structured around first providing a brief conceptual understanding of the blockchain including an explanation of its technological aspects. It then provides a description of the Ethereum blockchain and moves towards an explanation of smart contracts. The next part of the paper provides a review of the literature related to smart contracts, in brief. Thereafter, the paper seeks to answer whether smart contracts can replace traditional legal agreements. Here it is argued that a scenario wherein smart contracts will completely replace the agreements written in standard legal prose is highly unlikely in the foreseeable future. At most, smart contracts may become a part of traditional legal agreements, in some specific instances. Subsequently, an attempt has been made to provide possible answers to questions about the legal enforceability of agreements, which include smart contracts, particularly in the context of India.

Blockchain: Concept and Fundamentals

A blockchain can be understood as a ledger, which is continuously updated across all the participating computer nodes without there being a centralized master copy (distributed); information can be added to the ledger but cannot be removed (append-only); public-private key encryption technology is used for sharing and controlling information (provably signed); entries in the ledger are linked forming a chronological series of blocks and they are protected using cryptography (sequentially-linked and cryptographically secured); and the ledger is copied across all the nodes in the blockchain (replicated).[1]

[1] PAUL VIGNA & MICHAEL J. CASEY, THE TRUTH MACHINE: THE BLOCKCHAIN AND THE FUTURE OF EVERYTHING 64-65 (HarperCollinsPublishers 2018).

Essentially, blockchains are highly resilient and tamper-resistant decentralized databases, blending together peer-to-peer (P2P) networks, public-private key cryptography and consensus mechanisms.[2]

Blockchains address the limitations of client-server models, including problems of trust between individuals and businesses transacting via centralized intermediaries, and one-sided flow of information, among others. For example, a decentralized payment system implemented on a blockchain does away with the need of a central clearinghouse and enables transactions between individuals (nodes) who may not necessarily trust each other; though such a system needs to solve the double-spending problem, which requires that the total amount of currency in circulation be fixed.

Blockchain: Technology

This section provides a brief understanding of the blockchain technology. It uses the Bitcoin blockchain as a point of reference and its technology as an underlying link to understand smart contracts.

It is to be noted that transactions between nodes on the blockchain are grouped together into separate 'blocks'. A block not only records the details of a particular number of transactions in its 'header' but also the timestamp and a link to the previous block, which is known as a hash. It is by way of the hash that all the blocks are linked together. Also, all the transactions are broadcast across the entire blockchain and all the participating nodes are updated. The nodes store these transactions when a block is appended in the blockchain.

However, for the blockchain to store information it takes work and this can be achieved only collectively. The underlying protocol requires that a block's hash begin with a specified number of zeros. This is called as 'proof of work' and requires solving a mathematical puzzle, which is more in the nature of a guessing game but consumes a lot of computing power. Once the puzzle is solved, a valid hash is generated for the block and it is broadcast to all the participating nodes to make sure that it meets the protocol's standards. Only when it is ensured by all the participating nodes that the block is valid, is it appended to the blockchain.

[2] PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 13 (Harvard University Press 2018).

The nodes that are engaged in the task of solving this puzzle by offering their computing resources are called 'miners' and the process of updating the blockchain is called as 'mining'. Mining ensures orderly storage of information in the blockchain without a central clearinghouse having to go through the task of clearing every transaction between two nodes.

Ethereum

Since the Bitcoin blockchain was updated only once every ten minutes and it could be used mainly for transaction of the digital currency, there were attempts to create more efficient blockchain based systems. One such system was Ethereum. The Ethereum blockchain allows not just storing information related to transactions of its digital currency, but also 'a medium to host decentralized applications (or "dapps") that rely on a blockchain, at least partially, for their underlying functionality'.[3]

The Ethereum implements transactions using its own digital currency called as 'ether' and also allows the participating nodes to deploy smart contracts. The blockchain is updated every twelve seconds. All nodes can write and deploy smart contracts using a Turing-complete programming language, known as 'Solidity'.

The Ethereum network consists of an "externally owned account", for everyday users of the network as well as a "contract account", for smart contract applications. The contract account 'stores the compiled bitcode of a particular smart contract and can collect and distribute ether, record data to the Ethereum blockchain, process information, and possibly also trigger the execution of other smart contracts'.[4]

It is the Ethereum Virtual Machine (EVM) – a part of the Ethereum protocol - that is responsible for processing smart contracts. Also, it should be noted that the execution of a smart contract can be triggered by any participating node by means of transacting ether.[5]

'Contracts interact by either "receiving" or "sending" messages. A "message" is an object containing a particular quantity of ether, an array of data, the address of the sender, and a destination address (which can be either another contract account or an externally owned

[3] PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 27-29 (Harvard University Press 2018).
[4] ibid.
[5] ibid.

account). When a contract receives a message, it has the option of returning a message to the original sender – acting, to a large extent, like a standard computer function'.[6]

Since the code of smart contracts is executed by all the participating nodes in the Ethereum blockchain, they are neither controlled by any single node nor can be halted by one, making them different from traditional legal agreements.

Smart Contracts

It was with Nick Szabo's paper titled "Formalizing and Securing Relationships on Public Networks" that the idea of Smart Contracts came about. In this paper, Szabo explained that it was possible to develop computer programs that resembled "contractual clauses", which would be binding on the contracting parties. Since they were bound by a computer code, it would narrow the opportunities for either party to terminate its performance obligations.[7]

Smart contract has been defined as a program that runs on the blockchain and has its correct execution enforced by the consensus protocol. A contract can encode any set of rules represented in its programming language – for instance, a contract can execute transfers when certain events, like payment of security deposits in an escrow system, take place.[8]

Since smart contracts are represented in code and executed by computers, their performance is enabled and guaranteed by the underlying blockchain mechanism.[9] While it is by way of instructions written in their computer code that they execute transactions, this is usually according to contractual conditions, which are pre-agreed between the contracting parties.[10]

It is due to these features that a new opportunity regarding smart contracts is being sensed. Proponents have been arguing that it is possible to turn traditional legal agreements into the rule of code and with the subjectivity of human intervention being laid to rest, there would be much more certainty in executing contractual obligations.

---

[6] ibid.
[7] PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 73-74 (Harvard University Press 2018).
[8] Loi Luu & Duc-Hiep Chu et al., *Making Smart Contracts Smarter*, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 254-269, ACM.
[9] Eliza Mik, *Smart Contracts: terminology, technical limitations and real world complexity*, 9 (2), LAW, INNOVATION AND TECHNOLOGY, 269, 269 (2017).
[10] PAUL VIGNA & MICHAEL J. CASEY, THE TRUTH MACHINE: THE BLOCKCHAIN AND THE FUTURE OF EVERYTHING 81 (HarperCollinsPublishers 2018).

Smart Contracts: Review of Literature

Some view smart contracts as pieces of autonomous code operating on a blockchain[11] or 'systems which automatically move digital assets according to arbitrary pre-specified rules'.[12] At the same time, others see smart contracts as automated execution of legal contracts with code being used to perform contractual agreements.[13]

Some others use the term 'contract' in an informal sense without attaching any legal significance to the term.[14] However, still others attach legal significance to the term and argue that smart contracts will automate and guarantee contractual performance, thus obviating the need of lawyers and judges for issues related to contracts generally.

According to Nick Szabo, 'Smart contracts combine protocols with user interfaces to formalize and secure relationships over computer networks. Objectives and principles for the design of these systems are derived from legal principles, economic theory, and theories of reliable and secure protocols'.[15] In his paper, Szabo elaborated that smart contracts 'utilize protocols and user interfaces to facilitate all steps of the contracting process, including negotiation, performance and adjudication'.[16]

Szabo and others perceived the pre-internet laws as inadequate and assumed that technology will help in solving all problems, including the ones inherent in the operation of the legal system itself. Szabo's paper 'portrays courts and legal principles as inconvenient legacies to be made redundant by suitable technologies. Other propositions made therein, such as the use of technology to secure contractual performance or to ensure adherence to the law, have evolved into the theory that 'code is law' and that technology has normative implications'.[17]

Subsequently too, there has been much confusion around the idea of smart contracts. Given the state of affairs there have been attempts to bring about a distinction between smart contracts as

[11] Eliza Mik, *Smart Contracts: terminology, technical limitations and real world complexity*, 9, LAW, INNOVATION AND TECHNOLOGY, 269, 272 (2017).
[12] ibid.
[13] ibid.
[14] ibid.
[15] Nick Szabo, Smart Contracts: *Formalizing and Securing Relationships on Public Networks*, 2(9), FIRST MONDAY (1997) (https://firstmonday.org/ojs/index.php/fm/article/view/548/469).
[16] ibid.
[17] Eliza Mik, *Smart Contracts: terminology, technical limitations and real world complexity*, 9, LAW, INNOVATION AND TECHNOLOGY, 269, 273 (2017).

pure computer programs or codes and smart contracts in the legal sense. However, it has been found that such a distinction may be difficult to maintain as even if smart contracts are seen in the legal sense, they may still contain an element of program or code incorporated into them. Technical writings, which do not go into the details of legal processes and see even vending machines as examples of a contract, thus not differentiating between a contract and offer made to the world at large, further complicate the picture.[18]

Can smart contracts replace traditional legal agreements?

Smart contracts are similar to traditional legal agreements in that the terms of the agreement would need to be negotiated by the contracting parties, even in a smart contract. Once the parties to the contract agree with the terms of the contract, they may decide to place the whole agreement or a certain part of the agreement in the code underlying the smart contract. This means that the extent to which the agreement will be executed through the smart contract, is for the contracting parties to decide. While the whole agreement may be placed in the smart contract, given the nature of legal agreements, it is highly unlikely and only a small part is likely to find its way in the code.

The code, which forms a part of the smart contract, may execute when it is triggered, for example, by way of a certain successful transaction or at a particular point in time. This may prevent a situation of one of the parties to the contract from reneging, once a contract has been established after successful negotiations. However, if both the parties may wish to terminate the contract later, such a provision may either be inserted in the code or provision for intervention of a third party, by way of an arbitrator or a court of law, may be provided.

But at the same time, it needs to be recognized that unlike traditional legal agreements, smart contracts are more autonomous, as they depend on the execution of the underlying code. In a blockchain, it will be much harder to terminate the execution of the code underlying the smart contract, particularly if it is only one of the parties that wishes to terminate the execution and such a provision has not been expressly provided within the code itself.

Moreover, it may be very difficult to ensure that all rights and obligations that are otherwise covered in a traditional legal agreement find their way into the code of the program i.e. the

[18] ibid.

smart contract. While it may be easy to translate some part of the traditional legal agreement into software code, particularly the part that relates to exchange of digital currency or change in ownership status of an asset, it might not be possible to cover everything under the code. This is because traditional legal agreements offer such subjectivity and open-endedness as is necessary for human transactions and exchange. For example, while a blockchain is capable of validating transactions, there is no need to validate, at least initially, a traditional legal agreement between two parties, wherein parties have promised to act in good faith. If a dispute were to arise at any stage of the contract, it is only during the process of adjudication that an intermediary or a court of law decides whether there was indeed a valid contract or not.

Additionally, in situations where the transactions forming a contract are successfully recorded in the blockchain, but the contract itself is not legally tenable owing to one of the parties being a minor, lacking mental capacity or acting under duress, it is the law of the land that may provide reprieve and the role of code in such situations may be limited.

There may also be instances when one of the parties is interested in terminating the contract and compensating the other party for the losses that they may have incurred. In such a situation, if it were a smart contract instead of a traditional legal agreement, and some transaction were to be implemented irrespective of the wishes of one or more of the contracting parties, only because it was hard coded into the logic of the smart contract, it may lead to economic inefficiency. This is why, at times, contracts are intentionally kept open-ended, with a measure of flexibility introduced in them, as it may lead to increased efficiency.

Given these, it is highly unlikely that we will soon be entering a world where smart contract replace traditional legal agreements and make all intermediaries, as well as lawyers, judges and courts of law redundant.

We may however, see increasing use of smart contracts by way of contracting parties memorializing some part of a complex agreement into smart contracts, particularly those related to transactions of a digital currency or transfer of land titles, change of ownership status of an asset, and the like. Other aspects of the contract, particularly those that are best left open-ended and flexible, are not likely to be inserted into the underlying code of a smart contract in the foreseeable future. Similarly, there does not seem to be a situation arising wherein the role of lawyers, judges and courts of law can be assumed by code-based rules. Similarly, replacing the ‘rule of law’ by the ‘rule of code’ seems to be more a case of fantasy advanced by

technocrats with inadequate understanding of the role of both law and technology in human societies.

Can agreements relying on smart contracts be enforced legally?

Given the fact that the role of smart contracts will be limited to enforcing only a part of traditional legal agreements, particularly transfer of digital currency, transfer of land titles and change of ownership status of an asset, it seems likely that they may well be covered under existing laws and will be legally enforceable.

This is because the formation of a smart contract is likely to follow the process that is followed in case of traditional legal agreements. The parties to the contract are likely to negotiate the terms of the agreements beforehand and then decide which part of the contract is to be encoded in a smart contract.

If a dispute arises with respect to any part of the smart contract, it is likely to be adjudicated upon by third parties, as is the case with traditional legal agreements. In cases of misrepresentation and non-disclosure, mistake, frustration, duress or unfairness, it is the law of the land, which is the Indian Contract Act 1872 in the case of India, which is likely to provide relief.

If a party breaches the terms of the agreements, which have been negotiated, the other party is likely to retain the ability to approach the appropriate legal authority to bring action in the case. It is the courts of law, which will enforce law in case of any dispute and award damages to the aggrieved party.

Moreover, even if the parties to the smart contract have already decided on who the adjudicator might be in case of a dispute, it is the court of law, which will have the final say as to the validity of the adjudicator.

Particularly in the case of India, just as an electronic contract (or e-contract) is governed by the provisions of the Indian Contract Act, 1872 (ICA) as well as provisions of the Information Technology (Amendment) Act, 2008, and cannot be executed with validity unless it satisfies all the essentials of a valid contract under the Indian Contract Act, 1872; similarly a smart contract, as discussed above, would need to be a valid contract as defined by Indian Contract Act, 1872.

Moreover, since the Indian Contract Act, 1872 does not lay down any particular way in which an offer is to be communicated and agreement negotiated and accepted, e-contracts are held to be valid if they otherwise are valid under the Indian Contract Act, 1872.

If the same analogy is extended to a smart contract, there is no reason why the smart contract should be held to be invalid, if it is otherwise valid under Indian Contract Act, 1872.

Conclusion

Smart contracts are advantageous to the extent that they can reduce the costs associated with intermediaries and introduce certainty in regards to transactions, which can be completed without human intervention. They can lead to more objectivity in contractual relations by expressly providing some elements of a complex traditional legal agreement in a programmable software code. This may reduce the need of monitoring to ensure that mutual obligations are being fulfilled. Moreover, since it is extremely difficult to tamper with data that has been verified by the participating nodes in a blockchain, smart contracts may help in dealing with issues of trust that are present in any exchange between strangers.

However, neither all exchanges between human beings can be objectified beyond a reasonable extent nor is it desirable to do so. In some situations, contracts are kept open-ended and a measure of flexibility is retained, as this leads to increased efficiency, given the uncertainties that exist in the real world. Thus, it is feasible that a part of a traditional legal agreement be put in software code making up a smart contract, instead of their blanket replacement. Also, such a traditional legal agreement, part of which is encoded in a smart contract, may hold legal validity, even in the present legal system.

But the argument of technological proponents, in general and purists, in particular, that traditional legal agreements will be replaced by smart contracts and in the process obviate lawyers, escrow agents and courts of law seems to be a stretch of imagination and in the realm of speculation, at least for the foreseeable future.