International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Smart Contracts: Need of the Hour

Dr. Suman Nasa[1], Ms. Shubhangi Nasa[2]

[1]Associate Professor, GVM Girls College Sonipat
[2]Advocate

ABSTRACT
Smart contracts are essentially programs that are kept on a block chain and implemented when certain pre-determined conditions are satisfied. Generally, they are utilized to automate the execution of a contract so that the involved parties can understand the outcome instantly, without the requirement for an intermediary or time loss. Moreover, they can even automate a work - flow by initiating the subsequent action when certain criteria's are met.

Keywords: automate; block chain, contract, intermediary, work- flow

INTRODUCTION

Smart contracts are pieces of computer code that are saved on a block chain-based platform and execute all or part of an agreement automatically. The code may serve as the only expression of the parties' agreement, or it could supplement a conventional text-based contract by carrying out specific provisions, for instance the funds being transferred from Party A to Party B. As the code is replicated along all multiple nodes of a block chain, it benefits from the security, stability, and data integrity that a block chain provides. This duplication also indicates that when a new block is placed on the block chain, the code is executed. If the parties have suggested that certain criteria have been satisfied by initiating a transaction, the code will implement the action stimulated by those parameters. If there is no such transaction, the code will do nothing. Almost all smart contracts are written in a programming language such as Solidity that is designed specifically for such programs.

Currently, input parameters and execution steps should be objective and specific for a smart contract. Alternatively, if "x" occurs, "y" must be executed. The precise tasks executed by smart contracts are therefore relatively simple, for instance the fully automated transfer of crypto currency through one party's wallet to the other when specific conditions are met. As block chain adoption increases and far more assets are tokenized or placed "on chain," smart contracts will get more sophisticated and able to handle more complex transactions. Already, developers are stringing together various transaction steps to generate smart contracts with a higher level of complexity. Nevertheless, we are at least several decades away from code evaluating more subjective legal requirements, such as whether if a party fulfilled a commercially reasonable effort standard or if an indemnification clause must be triggered and indemnity paid.

In a few block chains, a transaction fee has to be paid before such a compiled smart contract can really be executed in order for the contract to be included in the chain and executed. This ether-based payment is termed to as "gas" in the Ethereum block chain, where smart contracts are implemented on the Ethereum

Virtual Machine (EVM).[1] The quantity of gas required to carry out a smart contract is directly proportionate to the complexity of the contract. Subsequently, gas presently acts as a critical barrier to prevent the EVM from being overwhelmed by overly complicated or numerous smart contracts.[2]

At the moment, smart contracts are ideal to spontaneously carry out two types of transactions that are common in various contracts:

*Making sure that money is paid when certain events happen

*Imposing penalties, financially if specific criterions are not met.

Once the smart contract has been deployed and is working, there is no need for a person to step in, even if it is through a trusted escrow holder or the legal system. This lowers the costs of executing and enforcing contracts.

Smart contracts, for example, could completely eradicate so-called procure-to-pay gaps. When a product is scanned on arrival at a storage facility, a smart contract could instantaneously initiate queries for the necessary approvals and, once those approvals are obtained, transfer funds instantaneously from the buyer to the seller. Sellers would be paid more quickly and would no longer be obligated to engage in dunning, while buyers' account payable costs would decrease. This could affect the need for working capital and optimise the financial operations of both parties. A smart contract can be configured to disable communication to an internet-connected asset if payment is not received. For example, if payment isn't received, access to specific information could be denied automatically.

Smart contracts, which should be initiated on a block chain, have the potential to drastically reduce transaction fees, eliminate the need for middlemen, and automate contracting operations to a significant degree.

Smart contracts are often cited as one of the defining characteristics of the crypto currency movement, but their implementation in real-world scenarios can be challenging. Typically, they are utilized to manage on-chain events and provide decentralized financial services.

Due to technological limitations, widespread adoption has not occurred. These technological limitations are exemplified by smart contract platforms, which are block chain-based initiatives.

Smart contracts offer significant benefits over contracts that are drafted conventionally and may be the answer to problems as serious as fraud. Irrespective, smart contracts have significant drawbacks. They have been hailed as the future of contracting by the legal and technology press and have spawned companies that have raised millions of dollars in venture capital. However, they may not be the remedy anticipated by some. Indeed, smart contracts have considerable restrictions.

CONTRACT AUTOMATION

The potential to execute transactions instantaneously and without the intervention of humans is one of the most key traits of smart contracts. Nevertheless, this automation and the reality that smart contracts cannot be modified easily or revoked unless the parties include these functionalities during the formation of the smart contract are some of the most important impediments to the pervasive adoption of smart contracts. A party can easily excuse a breach in conventional text contracts by not enforcing the accessible penalties.

[1]'What Is The "Gas" In Ethereum?' (*CryptoCompare*, 2022) <https://www.cryptocompare.com/coins/guides/what-is-the-gas-in-ethereum/> accessed 23 August 2022.
[2]Ibid.

If a valued customer is a month late on payment, the vendor may decide in real time that maintaining long-term business relationships is far more crucial than any cancellation right or late fee. If such a relationship was reduced to a smart contract, the alternative choice to not enact the agreement on adhoc basis will most likely be lost. Unless otherwise specified in the smart contract, a missed payment will result in the completely automated deduction of a cancellation fee from the customer's account or the cessation of access to a software program or internet-connected device. As a result, the automated execution provided by smart contracts may not even correspond to how businesses are actually run.

In the same way, a party might be willing to accept, on a temporary basis, that partial performance is the same as full performance in a text-based contract. This could be because one party wants to keep the relationship going or because one party thinks that partial performance is better than none at all. Again, the need for objectivity in smart contract code might not match up with how contracting parties actually work together. With all these subjectivities, there lies so many limitations to this theory which generate many apprehensions in the minds of users.

The block chain is an intriguing technology because it can establish the facts of a situation independently, without the intervention of a reliable third party. In a world in which no one can be relied upon, this is an important consideration.[3]The term "distributed consensus" refers to the process by which the vast majority of nodes in a decentralised system come to the conclusion that a particular block has successfully completed the proof-of-work. The veracity of an event, such as the genesis of new tokens or their subsequent exchange, can be ascertained in this manner.

The block chain eliminates the requirement to place trust in third parties by allowing users to place their faith in the technology itself. A fundamental lack of trust underpins each and every one of the theories that link block chain technology to radical disintermediation. Since the beginning of its existence, online business has been hampered by the inherent unreliability and lack of security of the Internet.[4] The latter was never meant to be used as a platform for conducting business, and the open nature of the platform makes it particularly unsuitable for business dealings between strangers who are unable to trust one another due to the limited means available to authenticate identities or guarantee payment.

There are many different interpretations that people have regarding the idea of "validation." The mining process must first verify a transaction before it can be added to the block chain for it to be technically recorded there. This merely indicates that the majority of nodes have reached the conclusion that a particular node has fully performed the proof-of-work, that the transaction input is greater than the transaction output, and the conditions of the locking scripts have been satisfied.

However, in many different contexts, "transaction validation" is perceived to imply that (a) smart contracts, a premise that is typically broader than transactions, can be validated by the block chain, and (b) this validation is legally required or at the very least highly desirable. However, in legal systems based on common law, contracts are not obligated to be validated, and the concept of "contract validation" does not even exist. During the adjudication process, the questions about whether or not a contract has been created and whether or not it clearly represents the agreement of the parties are examined and decided based on the evidence presented.

[3]Leslie Lampert,'Byzantine Generals Problem 'Acmtransactionon progmminglanguages and systems.

[4] Marjory Blumenthal, David D Clark, 'Rethinking the Design Of The Internet: The End-To-End Arguments Vs. The Brave New World.

FINDINGS

The block chain shows proof that a transaction took place, which indicates that one or more tokens have been transferred from one account to another as the technical specifications for the transfer were satisfied. However, its validity cannot be established in a legal sense. Neither can it establish the legality of the contract comprising the transaction. The legal validity of a payment or a contractual relationship is always based on real-world events that cannot be seen by the block chain and cannot be validated by the mining process.

In the context of block chain technology and smart contracts, the term "self-enforcement" refers to the automatic performance of contractual obligations by the parties to the contract. Since they automatically transfer tokens on such occurrence of predetermined events or restrict access to cars or apartments in the case of non-payment of a loan or rent, respectively, smart contracts are referred to as "self-enforcing," which is a synonym for "self-executing."[5] The idea that people are usually biased and unreliable serves as the basis for this theory.

The code, on the other hand, is impartial and objective. It is not able to "change its mind," deny performance, or withhold payment. These options are all out of the company's control. Because neither party can sway or interfere with the operation of the smart contract after it has been placed "on" the block chain, the fulfilment of the contractual obligations is guaranteed to take place without any deviations. The actuality that performance is technologically guaranteed provides a level of certainty that is both legally and commercially beneficial. In technical writings, self-enforcement is associated not just with the automated processes of transactions and the removal of human discretion on the aspect of the contracting parties, but also, more typically, with the elimination of the requirement for judicial intervention.

As mentioned, the use of smart contracts based on block chain technology would do away with the requirement for legal regulations and institutions. These theories could have originated from a misinterpretation of the practical consequences posed by the decentralised nature of the block chain, in particular with regard to the consensus mechanism that it utilises for the validation of transactions. After all, decentralisation is frequently associated with the elimination of conventional judicial and administrative institutions. Similar assertions were common in the early years of cyberspace academia, which campaigned radical disintermediation as a logical outcome of the distributed nature of the Internet and affirmed cyberspace's autonomy from the legal system.[6]

It seems probable that there must be a document that clarifies what the agreement is about because the people who compose the code for the smart contract cannot decide on its business and legal aspects. This is because the individuals who publish the code for the smart contract are responsible for its security. As a result, the majority of smart contracts will initially take the form of written documents in basic language that will subsequently need to be translated into code. The majority of people are under the impression that this procedure is not very difficult.

It is occasionally recommended that smart contracts be published in code from the very beginning. This is done so that the difficulties associated with translating legal jargon into code can be avoided. This so-called "direct coding" will not only make it simpler for a computer to carry out the terms of a smart contract, but will also lessen or do away with the ambiguity that naturally occurs in spoken and written

[5]Kwesi D. Atta-Krah, 'Preventing A Boom from Turning Bust: Regulators Should Turn Their Attention to Starter Interrupt Devices Before the Subprime Auto Lending Bubble Bursts'

[6] David R Johnson and David Post, 'Law and Borders – The Raise of Law in Cyberspace' (1996) 48 Stanford Law Review 1367

language.[7] The contract would have been reasonable right from the beginning. For lawyers to be able to circumvent the stage of drawing up legal prose, they would need to gain skills in programming. Programmers will be required to acquire a basic understanding of contract law as an alternative. According to various technical writings, direct coding of smart contracts will indeed necessitate increased precision and organisation on the part of lawyers when describing the rights and responsibilities of the parties involved.

Any significant conversation of smart contracts should start with a comprehensive understanding of what can be lawfully and technically viable. Astonishingly, few legal obstacles exist for the use of smart contracts in commercial operations. Technical obstacles appear to be more significant than legal ones. The advantages of putting smart contracts in block chain systems could be questioned on a broader scale. The authentic Bitcoin block chain is secure, but it has extremely limited processing capacity and permits only the most elementary transactions. In essence, smart contracts are now comparable to the automated execution of simple payment instructions. Complex transactions necessitate more refined block chains or protocols built on top of them.

It is possible that these block chains are not decentralized, reliable, or secure. In practice, smart contracts should be regarded as computer programmes that run in distributed computing environments, and not as a quasi-magical technology which liberates parties to a contract from conventional legal and financial institutions. Consequently, the original block chain's ground-breaking claims regarding decentralization and self-enforcement are no longer valid.

Moreover, once smart contracts involve the fulfilment of real-world requirements, their effective implementation is dependent on various external, centralised and insecure entities. Since smart contracts are only as reliable as the oracle and data source that provides them with information about off-chain events, the reliability and security of the block chain become largely irrelevant. When smart contracts involve more complicated transactions, including exchanges that extend beyond the progression of tokens in response to the presentation of one or more private keys, the benefits of simply putting them on the block chain appear to be lost.

Smart contracts pose a distinctive set of problems unrelated to block chain technology. Aside from the rhetorical question as to whether complete automation or self-enforcement of certain obligations is desirable, it must be acknowledged that only a subset of contractual obligations can be expressed in code and that only a select group of commitments can be considered computationally ascertainable.

Smart contracts may therefore be only relevant to a subcategory of transactions. Contracts containing obligations based on ideas such as "reasonableness" or "best efforts" or requiring an overall evaluation of contractual performance are difficult to envision. Smart contracts may have restricted practical applications due to their inability to accurately reflect and report for the complexities of the real world. Simultaneously, they provide fertile surface for research in the field of computational law and necessarily require that practitioners become more aware of recent developments in coding.

CONCLUSION

Since there are often calls for the creation of a language which would functions a commonality for lawyers, developers or even allow the immediate coding of contractual obligations, it is also important to look into whether or not it would be better to reduce (or even get rid of) uncertainty in contracts and the trade-offs

[7] Stephen Wolfram, Computational Law, Symbolic Discourse and the AI Constitution—Stephen Wolfram Blog (2016) <*http://blog.stephenwolfram.com/2016/10/computational-law-symbolic-discourse-and-the-ai-constitution*>

among precision and certainty and ambiguity and flexibility. In technical writings, reducing ambiguity is acclaimed as one of the major benefits of smart contracts. However, it may not be as helpful as was first thought.

Smart contracts that enforce their terms are inflexible, deterministic, and divorced from the business environment in which they are used. The removal of human judgement and the mechanisation of choice both have the potential to quickly bring about a circumstance in which the parties to a contract lose the capacity to exercise their rights in accordance with their individual inclinations. Furthermore, smart contracts' code must be flawless in order to ensure perfectly smooth performance while also lowering transaction costs because of the elimination of intermediaries and conventional enforcement mechanisms. This implies that it clearly represents the parties' commercial agreement and is free of coding errors or security holes. Obviously, such a presumption cannot be used to proceed.

Intriguingly, the technical inadequacies of smart contracts appear to increase the necessity for a formal consent or complex regimes assigning liability for coding errors or irregularities in the operation of oracles and data sources. This notion raises the possibility of a potential ethical dilemma. Smart contracts might eliminate human bias and the possibility of non-performance, but they also present new risks, including the risk of programming errors, the risk of security breaches, and the risk of deviations from the contracts' original intension and actual implementation. It is unlikely that the use of smart contracts will eliminate the requirement for lawyers and courts or weaken the relevance of the legal profession in any other way. This is due to the fact that the events that have been mentioned above may result in complex disputes. To the best of our knowledge, we should anticipate the opposite until further notice.

BIBLIOGRAPHY

1. David R Johnson and David Post, ‘Law and Borders – The Raise of Law in Cyberspace’ (1996) 48 Stanford Law Review 1367
2. Leslie Lampert,'Byzantine Generals Problem 'Acm transaction on progmming languages and systems.
3. Marjory Blumenthal, David D Clark, ‘Rethinking the Design Of The Internet: The End-To-End Arguments Vs. The Brave New World.
4. Kwesi D. Atta-Krah, ‘Preventing A Boom from Turning Bust: Regulators Should Turn Their Attention to Starter Interrupt Devices Before the Subprime Auto Lending Bubble Bursts
5. Stephen Wolfram, Computational Law, Symbolic Discourse and the AI Constitution—Stephen Wolfram Blog (2016) *http://blog.stephenwolfram.com/2016/10/computational-law-symbolic-discourse-and-the-ai-constitution*
6. 'What Is The “Gas” In Ethereum?' (*CryptoCompare*, 2022) <https://www.cryptocompare.com/coins/guides/what-is-the-gas-in-ethereum/> accessed 23 August 2022