ABUAD Law Journal (ALJ)
Vol. 8, No. 1, 2020, Pages 74-93 https://doi.org/10.53982/alj.2020.0801.05-j
Published by College of Law, Afe Babalola University Law Journal,
College of Law, Afe Babalola University, Km 8.5, Afe Babalola Way,
P.M.B. 5454, Ado Ekiti, Ekiti State, Nigeria ISSN: *2971-7027*
www.abuad.edu.ng, abuadlawjournal@abuad.edu.ng

Contract Law in an Era of Technology: Examining Liability in Smart Contract Transactions

Tega Edema*

Abstract

The growing use of smart contracts in a wide range of transactions has raised a deluge of legal issues, including allocation of liability in such transactions. In many circumstances, using smart contracts involves a range of legal risks that might be distributed beyond the contractual parties to other parties, such as the developers of the smart contract code. While smart contracts have the potential to disrupt the current legal and transactional status quo, notorious occurrences such as attacks on Ethereum or Bitcoin platforms highlight the need to properly dissect the issue of liability and rightly apportion liability where it falls. This also includes working on any lapses in the existing legal and transactional framework to cater for these issues. This article sets out to examine the validity of smart contracts in the light of existing contract law principles. It examined the legal regime and development of smart contracts in Nigeria. It further discussed the problem of allocation of liability associated with smart contracts. It made certain propositions on how these issues could be tackled including the amendment of existing legal framework to aptly provide for and regulate the smart contracts era particularly in Nigeria. The doctrinal method of research was employed to dissect the issues raised and discussed in the article. Relevant texts were scrutinized and analyzed to arrive at the findings and recommendations contained in the article.

Keywords: Smart Contracts, Blockchain Technology, Liability, Validity, Contracts

1.0 INTRODUCTION

The growth of smart contract transactions, notably in Nigeria, has been phenomenal. Though smart contracts have various applications, they are the bedrock of cryptocurrency transactions. Nigeria has recorded a high volume of transactions in cryptocurrency trading.[1]In October 2020, about $32.3 million worth of bitcoin was traded in Nigeria.[2]With several Nigerian startups floating businesses such as 'Xend Finance' and 'Afen Blockchain'[3] powered by blockchain technology, thousands of smart contract codes are being executed daily. Given the peculiar nature of smart contracts namely, their automaticity and autonomous characteristics, several legal issues arise in the execution of these contracts and applications. One of such critical issue is the question of liability. For instance, who bears liability in the event that the smart contract fails to execute as expected? Or who is liable if a smart contract violates regulatory compliance?This paper makes an attempt at considering these issues with particular reference to Nigerian laws and cases and the contractual framework in Nigeria.

1.1. Meaning and Nature of Smart Contracts

A look into the meaning of Contracts is instrumental to any discussion on smart contracts. In simple terms, a contract is an agreement which the law will enforce or recognize as affecting the legal rights and duties of the parties.[4] It can be viewed as an agreement involving promises, obligations, liabilities, and remedies

*LL.B, B.L, LL.M, DRS. Assistant Lecturer, Admiralty University of Nigeria, Ogwashi-Uku/Ibusa, Delta
State, Email: edema-law@adun.edu.ng. Phone Number: +2348133518440

[1] Olumide Adeshina, 'Nigeria's Bitcoin P2P Trading surge by 16% since CBN enforced Crypto Ban' <https://nairametrics.com/2022/02/06/nigerias-bitcoin-p2p-trading-surge-by-16-since-cbn-enforced-crypto-ban/> accessed 14 March 2022

[2] Tage Kene-Okafor, 'In 2020, Nigerians traded more than $400m worth of crypto on local crypto exchange platforms' *Techpoint*<https://techpoint.africa/2021/01/06/nigerians-traded-more-than-400m-worth-crypto-2020/> accessed 14 March 2022

[3] Ahamdi Abarikwu, 'Blockchain/DeFi Year in Review: Nigeria in Focus'*Bscnews*<https://www.bsc.news/post/blockchain-defi-year-in-review-nigeria-in-focus> accessed 14 March 2022

[4] Itse .E Sagay, *Nigerian Law of Contract* (3rd ed, Sweet & Maxwell, 2018), 1

in the event of a breach or a failure to deliver on an expected term of the contract. The scope of contract law governs such questions as which agreements the law will enforce, what obligations are imposed by the agreement in question and what remedies are available if the obligations are not performed. Thus contract law is the law based on liability for breach of promise.[5]

A smart contract in the same fashion is an agreement albeit, designed as a computer code to be executed on an IF-THEN basis. Smart contracts are computer codes which represent the agreements of parties. A smart contract is an automatable and enforceable agreement. Automatable by computer, although some parts may require human input and control. It is enforceable either by legal enforcement of rights and obligations or via tamper-proof execution of computer code.[6]A smart contract code is designed to operate in such a way that obviates the need for intermediaries. This means the contract is self-executing based on some pre-existing conditions.[7] Smart contracts differ from regular contracts in that they can be provided in program code and performed by computers, as opposed to traditional contracts that are normally established by negotiations, written documents, and decisive actions. Smart contracts are computer programs that self-implement and self-execute based on a program algorithm.[8]

Since its invention, the ability to store immutable code and data in a transparent manner on a blockchain as well as the desire to eliminate human involvement has

[5] H. G Beagle and W.D Bishop and M. P Furmston, *Contract Cases and Materials*, (3rd ed, Butterworths, 1995)

[6] Christopher D. Clack and Vikram A. Bakshi and Lee Braine, ‘Smart Contract Templates: Foundations, Design Landscape and Research Directions’ <https://arxiv.org/pdf/1608.00771.pdf> accessed 14 March 2022

[7] Alexandros A. Papantoniou, 'Smart Contracts in the New Era of Contract Law' *Digital Law Journal*(2020) (1) 4 <https://www.digitallawjournal.org/jour/article/view/30?locale=en_US> accessed 9 March 2022

[8] KristianLauslahti and JuriMattila and TimoSeppälä, ‘Smart Contracts – How will Blockchain Technology Affect Contractual Practices?’ *ETLA Reports* (2017) 68 <https://www.etla.fi/wp-content/uploads/ETLA-Raportit-Reports-68.pdf> accessed 14 March 2022

sparked considerable interest in smart contract development.[9]Nick Szabo, a computer scientist and cryptographer, first proposed the concept of smart contracts, which predates even the invention of blockchain technology. According to Nick, a smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises.[10] Notably, Smart contracts are not a passive list of instructions enumerating the contracting parties obligations; rather, they are perceived as “autonomous agents” who execute a certain part of the program code (“smart contract”) when they receive certain information defined as a “code trigger”, which is the condition for the execution of the “smart contract” norm.[11]

1.1.2 Nature of Smart Contracts

Smart contracts usually operate on a decentralized and distributed ledger technology (DLTs). Decentralized computing is a trademark of the twenty-first century. They provide a democratized, distributed, and networked system in which no single body is in charge. As aresult, each level has a certain level of autonomy and is accountable for the system's flawless operation.[12] An example of such decentralized systems is Blockchain technology.

1.1.3. Blockchain Operation and Smart Contracts

Blockchain technology is an emerging technology which possesses the core features of decentralization, distribution, immutability, transparency, and

[9] Stuart Levi and Alex Lipton and Cristina Vasile, ‘Legal Issues Surrounding the use of Smart Contracts’ in Josias N. Dewey (ed) ‘Blockchain and Cryptocurrency Regulation’ *Global Legal Insights*(2020),< https://www.skadden.com/-/media/files/publications/2019/11/legalissuessurroundingtheuseofsmartcontracts.pdf>

[10] Nick Szabo, ‘Smart Contracts: Building Blocks for Digital Markets’ <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html> accessed 14 March 2022

[11] Vitalik Buterin,‘Ethereum Whitepaper’*Ethereum* <https://ethereum.org/en/whitepaper/> accessed 15 March 2022

[12] Afolabi Ijaoba, 'How Smart Contracts can Promote E-Commerce in Nigeria', <https://www.google.com/amp/s/www.benjamindada.com/smart-contracts-ecommerce-nigeria/amp/> accessed 11 March 2022

automation. Blockchain technology is backed by cryptography. Blockchain technology becomes relevant in economic exchange as it lowers costs and contributes to cost-efficiency and effectiveness of economic transactions. Decentralized governance shifts trust away from banks, multinational corporations, and governments, allowing peers to maintain control over their own data and transactions. Blockchain delivers a faster, safer, and less expensive cross-border transactional technique, as well as increased efficiency advantages over existing systems, which are highly centralized and rely on the involvement of intermediaries.[13]

Predrag[14] provides a vivid explanation of how blockchain works viz;

> Blockchain is a compound of the words "block" and "chain". It is a concept based on the use of a cryptographically protected chain of transaction blocks. Transactions are packed into blocks, and blocks are tied into a chain. Blocks are bound cryptographically, through a hash function: the contents of a block cannot be changed without changing the contents of all other blocks preceding it. Namely, each block is bound to the next block using a cryptographic signature. This allows the Blockchains to be used as a digital ledger which can be shared and verified by anyone with the appropriate permission to do so. A block consists of a title and transaction data. A title contains;
>
> • references to the previous block in the chain, i.e a short combination of letters related to a certain set of data (hash).
>
> • a time stamp indicating the time the block was entered into the "chain" of blocks, and

[13] Dimitrios Roumpos, 'Liability of the Smart Contract Developer: A Comparative Analysis in the light of US and EU Law', (2020) being a Masters Thesis submitted to the University of Tilburg, http://arno.uvt.nl/show.cgi?fid=152251, accessed 15 March 2022

[14] Predrag Cvetković, 'Liability in the Context of Blockchain-Smart Contract Nexus: Introductory Considerations' *Researchgate*<https://www.researchgate.net/publication/350474342_Liability_in_the_context_of_blockchain-smart_contract_nexus_Introductory_considerations> accessed 14 March 2022

- a hash tree or “Merkle tree” which lays out all transactions included in the block.[15]

Smart contract code, like other data on a blockchain (such as the amount of cryptocurrency held by an address), is duplicated across several nodes and executed using the same consensus mechanism. Furthermore, smart contracts allow parties to authenticate each other. With smart contracts, there exists a level of security not seen in many other automated transactions since they employ the same asymmetric cryptography as other blockchain-based transactions. In such transactions, users rely on private keys and public keys as a security measure for the contracts.[16]

The necessity of smart contracts is demonstrated in their potential to boost commercial efficiency, reduce transaction and legal costs, and promote transparency. They offer a wide range of possible uses, including automatic dividend payments, property transfers, and the automation of insurance claims, as well as the streamlining of clinical studies and more efficient data exchange.[17]

1.2.0. Characteristics of Smart Contracts

For clarity, the characteristics of smart contracts are outlined below:

1) Smart contracts are generated (programmed) using open source code; their standardization and execution are essentially free, lowering contract transaction costs;
2) Smart contracts possibly restrict the room for ambiguous or hazy interpretations, boosting the efficiency of contract execution. When the parties agree on the content of the terms, the smart contract program code executes those provisions without the possibility of violation of contract.
3) Smart contracts are intended to operate in a decentralized manner without the use of middlemen.
4) A smart contract is self-executing software, particularly in Blockchain technology, that strives to ensure that the parties perform and execute automated transactions.The execution can be based on data from the program or on data collected from the environment in which the transaction occurs.

[15] ibid
[16] supra, n.13
[17] supra, n.16

5) A smart contract benefits from the underlying Blockchain infrastructure's security (that is, multiple Blockchain nodes). Individuals or groups, for example, cannot halt its execution unless this option is explicitly built into the code.[18]

[18] supra, n.16 at 90.

1.3.0. Validity of Smart Contracts vis-a-vis Traditional Contracts

Before delving into the issue of liability of smart contracts, it is relevant to consider the validity of smart contracts vis-à-vis traditional contract. To be legally binding, contracts generally must possess these features. There must have been a valid offer, an acceptance, a consideration and an intention to create legal relations.[19] In application to smart contracts, it is apropos to consider whether these elements fit in and whether smart contracts pass these validity tests. These elements shall be considered anon.

1.3.1. Offer and Acceptance

An offer is an indication of one party's agreement to particular specific terms, with the expectation that the other party in the bargaining transaction will likely agree to the same terms.' When smart contract code is utilized on a distributed ledger, it is likely to be considered an offer if other ledger participants have the ability to interact with and execute the code.

Acceptance requires both an agreement by the counterparty to the substantive terms of the contract and an action by the counterparty to accept these terms within the time period and by the procedure required by the offer. By inputtinghis terms in the smart contract code, it is taken that a party has accepted the conditions of the offer.

1.3.2. Consideration

The general principles of Contract law with regards to consideration are also applicable to smart contracts.Consideration need not be adequate so long as it is something of value in the eyes of the law. In smart contracts, transaction fees paid by participants to the contract could well be taken as the consideration for the smart contract.

1.3.3. Intention to Create Legal Relations

Generally, in contract law, the parties' intentions are discernible from the written contract or from their words or conduct. The parties' intentions are assessed by reference to objective criteria: the status of their communication with each other is analysed by reference to what was communicated between the parties by words or conduct, and whether that leads objectively to a conclusion that they intended

[19] Orient Bank (Nig) Ltd. v. Bilante International Ltd (1997) NWLR (Pt.515) 37.

to create legal relations. Therefore, if the other requirements for a legally binding contract are satisfied in the case of a smart contract, it may be difficult for a party to assert, as against the other party who acted in reliance on it, that there was no intention to create legal relations with respect to the smart contract.[20]

Using the Ethereum blockchain as an example to illustrate how the above elements apply to smart contracts, participants and the group of core developers are taken to be the parties to the distributed ledger contract. The offer, acceptance, and meeting of minds (a*d idem*) are also satisfied when individuals who desire to join the blockchain network, download the Ethereum software and enable their devices to run Ethereum decentralized ledgers. The consideration may be in different ways, for instance, the payment of transactional fees such as gas fees or additional virtual assets.[21]

Other criteria with regards to the formal validity of contracts and by extension, smart contracts are proof of authenticity of the contract and identity of the parties to the contract. The question of proving the authenticity of the parties to a smart contract is easily dispensed by the immutability feature of smart contracts.[22] Similarly, the determination of the time of creation of smart contracts can be established on the assumption that indisputable, automatic date/time stamps are used in smart contracts.[23]With respect to the identity of the parties, the question remains as to whether, under the relevant laws, the cryptographic signature of a party qualifies as a proof of identity. To this it is suggested that the electronic signatures of the parties should be sufficient to identify the parties.[24] In many jurisdictions electronic signatures are already considered as equivalent to handwritten signatures.

[20]JelenaMaldvir, 'Smart Contracts-Self-Executing Contracts of the Future? *International In-house Counsel Journal*(2020) 13 (51), 1

[21] Dirk A. Zetzsche, Ross P. Buckley and Douglas W. Arne, ‘The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain’ *University of Illinois Law Review*(2018) 4 <https://www.illinoislawreview.org/wp-content/uploads/2018/10/BuckleyEtAl.pdf> accessed 14 March 2022

[22]Ibid

[23]Ibid

[24]Ibid

In Nigeria, recognition is accorded electronic signature by virtue ofSection 17 of the Cybercrime Prohibition Act, 2015 as follows;

> (a) Electronic signature in respect of purchases of goods, and any other transactions shall be binding.
> (b)Whenever the geniuses or otherwise of such signatures is in question, the burdenof proof, that the signature does not belong to the purported originator of such electronic signatures shall be on the contender.

Similarly, Section 93 (2) & (3) of the Evidence Act, 2011stipulates that;

> (2)Where a rule of evidence requires a signature or provides for certain consequences "if" document is not signed, an electronic signature satisfies that rule of law or avoids those consequences.
> (3) All electronic signatures may be proved in any manner, including by showing that a procedure existed by which it is necessary for a person, in order to proceed further with a transaction to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of the person.

It is therefore argued that the issue of validity of smart contracts is quite settled with already extablished principles of contract law. Smart contracts are just as valid as every other contract once they meet the basic criteria outlined above.

2.0. Brief overview of the Legal Regime of Smart Contracts in Nigeria

Suffice to note that the use of smart contracts in transactions is quite novel in Nigeria. There is no Legislation specifically provided to cover the subject matter of blockchain or smart contracts transaction. Rather than legislate on blockchain and smart contracts transactions, the Nigerian governments have issued a couple of Rules and Regulations[25] to regulate the era of cryptocurrency trading and

[25] The Cable, 'SEC issues new regulations on issuance, exchange of cryptocurrencies in Nigeria' <https://www.thecable.ng/sec-issues-new-regulations-on-issuance-exchange-

virtual Assets service operations in Nigeria. It must be stated that while these Regulations are not without their merits and demerits,[26] they mostly serve to regulate the relationship between the government and actors in the smart contract/blockchain field. They do not fully address the pertinent questions such as liability and dispute resolution in smart contract transactions.

From current data available, no smart contract transaction or case is being litigated in any Nigerian Court. More shocking is the fact that the few incidences or disputes which have arisen from cryptocurrency trading in Nigeria has been resolved by the parties involved without recourse to alternative dispute mechanisms such as institutional mediation centres or court assisted mediation. This demonstrates the lacuna existing in the area of legislation and judicial activism on blockchain and smart contract law. While it is hoped that laws would be passed to cover this field, parties involved in smart contract transactions may have to guide and govern their relations with the existing laws applicable to traditional contracts.

2.1. Legal Status of Smart Contracts

One nagging question which smart contracts and blockchain technology poses is, given their unique characteristics, do smart contracts command the force of law as traditional contracts? Furthermore, are the existing contract laws including case laws in Nigeria adequate to address the issues that arise from the writing and execution of smart contracts? What is the state of the laws in Nigeria concerning electronic contracts and do they adequately cover the peculiarities which smart contracts possess? These questions touch on the legal status of smart contracts which this section shall address forthwith.

of-cryptocurrencies-in-nigeria#:~:text=In%202020%2C%20the%20Central%20Bank,tokens%20that%20are%20considered%20securities%E2%80%9D> accessed 15 June 2022

[26] Ajibola Akamo, ‘Nigeria’s Crypto Heavyweights react to new SEC regulation on digital currencies'<https://nairametrics.com/2022/05/18/nigerian-crypto-community-react-to-secs-new-digital-asset-regulation/> accessed 15 June 2022

It has been argued that smart contracts are the beginning of the end of traditional contracts.[27] However, the general consensus from academics, practitioners and technology developers, seem to be that smart contracts should be viewed or regarded as contracts under the eyes of the law like other traditional contracts.[28]Just as in regular contracts, in civil matters, parties are bound by their agreement. The Courts generally do not interfere in the manner that parties choose to do business with each other as long as it is not criminal. When contracts are voluntarily entered into by parties, they become binding on them based on the terms they have set out for themselves. It is trite that where there is a valid contract agreement, parties must be held to be bound by the agreement and its terms and conditions.[29]

The above is also true and applicable to smart contracts. This means that there is no need to change the existing contract formation rules, such as the rules on offer and acceptance, consideration, purpose to create legal relations, and capacity. This observation is absolutely true when the algorithms are used solely as tools, as is most often the case in reality, rather than as true artificial agents.[30]

The rider is that smart contracts should carry with it the ability to alter the rights and obligations of the parties with regards to the terms of the contract. A smart contract should as much as possible reflect the desires of the parties to it and also make provisions for remedies or options available in the event of a breach or failure to perform. Once these functions are captured by the code written, then, such a smart contract should be enforceable in Court as a regular or traditional

[27] Alexander Savelyev, ‘Contract law 2.0: Smart Contracts as the Beginning of the end of Classic Contract Law’ *Information and Communications TechnologyLaw*, (2017) 26(2), 116–134. <https://doi.org/10.1080> accessed 6 March 2022

[28] Alexandros A. Papantoniou, 'Smart Contracts in the New Era of Contract Law' *Digital Law Journal*(2020) (1) 4 <https://www.digitallawjournal.org/jour/article/view/30?locale=en_US>accessed 6 March 2022

[29] Enemchukwu v Okoye&Anor (2016) LPELR – 40027 (CA)

[30] Mateja Durovic and Andre Janssen,‘The Formation of Smart Contracts and Beyond: Shaking theFundamentals ofContractLaw?’,<https://www.researchgate.net/publication/327732779_The_Formation_of_Smart_Contracts_ad_Beyond_Shaking_the_Fundamentals_of_Contract_Law> accessed 14 March 2022

contract.To this end, the existing case law decisions on contracts should be sufficient as authority to cover the status of smart contracts in Nigeria.

However, it must be noted that the existing case law do not adequately touch on the peculiarities of smart contracts considering the fact that smart contracts are rather new in our jurisprudence. There is thus need for judicial activism and ingenuity to be employed when deciding smart contract cases. As noted earlier, smart contracts can aptly fit into the requirements for validity of contracts and they carry the force of law which Courts should not shy away from enforcing.

3.0.Liability in Smart Contracts

Liability is a topical matter in law and it is necessary to set out a working definition of this subject for the purpose of the discourse of this paper. The Osborn's Concise Law Dictionary defines Liability as, 'subjection to a legal obligation; or the obligation itself. The person who commits a wrong or breaks a contract is said to be liable or responsible for it'.[31] A fuller description is offered by Ukeje as follows;

> legally bound as to make good any loss or damage; almost every character or hazard or responsibility, absolute, contingent or likely - all character of debts and obligations either absolute or contingent, express or implied condition which creates a duty to perform an act immediately or in the future duty bound to pay money i.e perform some other service.[32]

Thus, liability is based on the assumption that there are multiple participants in an action and that if one or more of them are harmed, one is held liable by law.[33]

3.1.0. Hacks/Errors in Smart Contract Codes

Determining liability in smart contracts is not an easy task. This is one of the biggest challenges with the smart contracts regime. Once a smart contract is

[31] Mick Woodley,*Osborn's Concise Dictionary* (12th ed, Sweet &Maxwell) 251

[32] R.N Ukeje, *Nigerian Judicial Lexicon* (Ecowatch Publications Limited, 2006) 267

[33]Elisabeth Frommelt, 'Liability Challenges in the Blockchain Ecosystem', *UC Davis Business Law Journal*<https://blj.ucdavis.edu/archives/vol-21-no-2/frommelt.html>accessed 14 March 2022

launched, it works autonomously in the sense that the developer does not need to actively manage, monitor, or even be in contact with it. Who bears liability in the event of a hack, error, bug in the code designed or a malfunction, malware or corrupted files detected in the system?[34] It should be noted that the immutability feature of blockchain technologies do not shield them from hacks or some form of software manipulations or cyber-attacks. Indeed, there have been two of such notable instances in the record of blockchain technology.

In the Mt. Gox case, which occurred in 2014, the victim, Mt. Gox, a Japanese Bitcoin exchange, lost about 740,000 bitcoins (6% of all bitcoin in existence at the time), valued at the equivalent of €460 million at the time and over $3 billion at October 2017 prices. An additional $27 million was missing from the company's bank accounts. Although 200,000 bitcoins were eventually recovered, the remaining 650,000 have never been recovered. The Exchange filed for bankruptcy while the Founder of the exchange is currently undergoing investigation and trial for fraud. Despite these measures, the customers whose Bitcoin investments were lost are in a fix as to how to recover them.[35] One wonders whether there are any hopes for recovery or whether these customers can sue under contract law for breach of contract and remedies such as damages or specific performance.

The DAO hack presented a more serious case for the blockchain community to consider. The DAO was a decentralized autonomous organization (DAO) that launched on the Ethereum network in 2016. The DAO was hacked after generating $150 million USD in ether (ETH) through a token sale due to flaws in its code base. The Ethereumblockchain was finally hard forked in order to recover the stolen cash, but not all stakeholders agreed, resulting in the network splitting into two independent blockchains: Ethereum and Ethereum

[34] Carla L. Reyes,'Conceptualizing Cryptolaw'*NEB. L. REV*(2017) (96). 384, 398 in Ryan Hasting, 'SmartContracts: Implications on Liability and Competence'(2020) 28(2),*University of Miami Business Law Review* <https://repository.law.miami.edu/cgi/viewcontent.cgi?article=1361&context=umblr> accessed 15 March 2022

[35] Andrew Norry, 'The History of the Mt Gox Hack: Bitcoin's Biggest Heist' <https://blockonomi.com/mt-gox-hack> accessed 9 March 2022

Classic.[36]Though, there are speculations on who the possible hacker of the DAO could be,[37]The DAO experience pose questions on whether the smart code developers could be held liable for the errors or bugs which were present in the code and made it vulnerable.

These two cases are illustrative of the fact that the question of liability in smart contracts is a central one and needs to be clarified at the outset of the contract. In determining liability, it is necessary to examine the parties to a regular smart contract or blockchain transaction.

3.1.1. Parties to Smart Contracts

Firstly, it is apposite to state there are several parties in relation to a blockchain transaction or smart contract.There are;

i. The core group that sets up the code design (software designers or developers). This also include the developers of the smart contract applications.

ii. The miners or owners of additional servers running the blockchain code for validation purposes (such as Bitcoin or Ripple validation nodes). These are also known as the node operators or validators.

iii. Users of the blockchain (such as banks and hospitals) and;

iv. Third parties affected by the system without directly relying on technology (such as bank customers and hospital patients or clients of brokers that hold cryptocurrency on behalf of clients).[38]

[36]Cryptopedia, 'What Was The DAO?' *Gemini* <https://www.gemini.com/cryptopedia/the-dao-hack-makerdao> accessed 14 March 2022

[37] Laura Shin points to Toby Hoenisch as the possible hacker. See, Laura Shin, 'Exclusive: Austrian Programmer and Ex Crypto CEO Likely Stole $11 Billion of Ether' *Forbes* <https://www.forbes.com/sites/laurashin/2022/02/22/exclusive-austrian-programmer-and-ex-crypto-ceo-likely-stole-11-billion-of-ether> accessed 14 March 2022

[38] Dirk Zetzsche et al, 'Liabilities Associated with Distributed Ledgers: A Comparative Analysis', in JelenaMadir (ed.) FinTech: Law and Regulation, *Edward Elgar* (2019)193 <https://www.elgaronline.com/view/edcoll/9781788979016/21_chapter9.xhtml> accessed 14 March 2022

Despite the different parties, it is to be noted that participants in a distributed ledger are highly likely to be potentially subject to liability, one way or another, for their conduct.[39] However, more than other categories of parties, the smart contract developers are in a more strategic position to have liability assigned to them as they play a critical role in smart contract transactions.This is because in many circumstances, the parties to a smart contract will lack the technical expertise to build a smart contract and will need to employ a third party to do so, or rely on a smart contract "template" given by a third party. In such circumstances, it is possible that the developer may make a mistake or that the parties did not adequately communicate their intentions to the developer.[40] Therefore, software developers could be liable for poorly written software code that results in a loss for the parties either through exploitation such as the DAO hack, or as a result of the code executing in a way not intended by the parties to the transaction.[41]

As regards Smart contract, it has been opined that it makes no difference whether the damage resulted from the misconduct of a human being or a machine’s malfunction. The owner or operator is liable for the machine’s malfunction.[42]

3.1.2.Allocating Liability in Smart Contracts

It has been suggested that to encourage parties to at least examine the allocation of liability, smart contract templates should ideally include a field specifying the contracting parties' preferred liability scheme in the event of a coding error. Parties would, however, retain the option of choosing no liability allocation scheme.

In such a case, an automatic warning message could appear, asking the parties to confirm thatthey do not want to specify what should happen if the code deviates f

[39] Dirk A. Zetzsche, Ross P. Buckley and Douglas W. Arne, ‘The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain’ *University of Illinois Law Review*(2018) (4)<https://www.illinoislawreview.org/wp-content/uploads/2018/10/BuckleyEtAl.pdf> accessed 14 March 2022

[40] supra, n.10 at 12

[41] John Salmon and Gordon Myers, 'Blockchain and Associated Legal Issues for Emerging Markets', <www.ifc.org/thoughtleadership>accessed 6/3/22

[42] Supra, n.36 at1394

rom the parties' expressed written wishes, and informing them that failure to designate a liability mechanism could result in losses being allocated wherever they fall.[43]

Another consideration on the issue of allocation of liability is where a smart contract offends the law or contains prohibitory provisions. Supposing a contract contains some elements of crime or substantially fails to comply with regulatory requirements, who bears liability in such instance? Node operators/validators may contend that they have no way of knowing to which use their fragmented network is put, which, for instance, could include money laundering or terrorist financing. Although,this argument seems quite plausible, yet, it is flawed. This is moreso as nodes could require AML/CFT ("Anti-Money Laundering/Combating the Financing of Terrorism") checks as a precondition for hard currency being exchanged into virtual assets. The Node operator could define this as a precondition for the overall use of the networks. In the event that the operators fail to put such mechanism in place, they would be bound to face whatever consequence result from their failure or negligence to so do. Ignorance of the law in such circumstances cannot be a valid defence to liability claims.[44] Therefore, where there is a case of fraud, money laundering or terrorism, the node operators/validators may be held liable jointly or severally with the smart contract developer. This is more so where it is extablished that the developer or node operator had fore knowledge of the purpose of the contract. In this regard, the admonition of the US Commissioner for Commodity Futures Trading Commission, Commissioner Brain D. Quintenz is apposite *to wit,*[45]

> While much of the assignment of liability depends on the facts and circumstances,…..looking at the spectrum of activity, on one

[43] JelenaMadir, 'Smart Contracts: (How) Do They Fit Under Existing Legal Frameworks?' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301463> accessed 14 March 2022

[44] supra, n.36 at 1396

[45] Brain D. Quintenz, 'How the CFTC can Take a Pro-Innovation Posture While Maintaining Orderly Markets' *CFTC,* <https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz19a> accessed 15 March 2022

> side there is the publication of code alone. Absent proof that developers intended that the code facilitate conduct that is illegal, the CFTC should not bring a case against them. On the opposite side of the spectrum, there are instances where developers knowingly design code that can be used for unlawful purposes, and intend that the code be used for such purposes. For example, take the case of a software developer who, at a broker's request, personally develops custom trading software that the developer knows can be used to "front run" or "trade ahead" of the broker's clients, and intends for the code to be used by the broker for that purpose. In that situation, the CFTC could pursue a case against the developer under an aiding and abetting theory.[46]

In assigning liability to specific parties, the Commissioner noted that,

> The key determination in every matter concerns the developers' intent. Questions that should be considered include whether the developers: 1) made modifications to the code that enhanced the unlawful activity; 2) promoted the unlawful activity through a website or marketing materials; or 3) had a financial stake in the unlawful activity. Another factor to consider is whether the code is narrowly designed to enable an unlawful purpose rather than broadly designed for legal activities. The more a code is narrowly tailored to achieve a particular end, the more it appears as if it was intentionally designed to achieve that end. Take for example, a computer code that is specifically programmed only to trade heavily on one side of the market during a future's contract settlement period to purposefully distort the final settlement price either higher or lower, otherwise known as "banging the close." If developers were aware that traders would use the program in this manner, the developers' conduct begins to look a lot like classic aiding and abetting.

[46] ibid

> Let me be clear. I do not view any of these factors as being independent, dispositive tests for liability. Nor do I view the list above to be exhaustive. But, when taken as a whole, these factors will help provide regulators with insight into an individual's responsibility for a software code's unlawful use. I am hopeful that this more holistic and detailed explanation of potential liability eases the minds of the vast majority of developers designing code for broad purposes intended to be put to legal uses.[47]

It is the opinion of this writer that the above reproduced passage should be the approach in fixing liability not only where there are elements of crime or failure to comply with regulatory provisions, but, generally, for smart contracts malfunction etc. Notably, dispute resolution in smart contract transactions should be adequately addressed by the parties to the transaction. There should be provisions on how the smart contract can resolve certain disputes and supplemental documentations on those areas of the transactions that cannot be resolved by the smart contract itself. These documents should cater for the procedure for resolving any dispute not covered by the smart contract code.

4.0.Recommendations

Granted that smart contracts are still contracts which are primarily governed by the agreement of the parties, however, from the above discussion, the issue of ascription of liability is one which could be thorny. The following points can be noted and incorporated into the existing legal and contractual framework for smart contract transactions in Nigeria:

1. Establishment/recognition of online courts or dispute resolution mechanisms with specialized jurisdiction or powers in blockchain technology/smart contracts interpretation.
2. Smart contracts are best suited for simple contracts. That is, contracts which do not involve complexity. The blockchain technology isa rather complex technology and would best fit complex transactions and applications. Smart contracts should therefore be deployed more to cater for less complex transactions.

[47]ibid

3. Given the immutability of smart contracts, it is safe to suggest that a combination of smart contracts codes and traditional contracts be employed by parties who want to take advantage of the blockchain technology but who do not at the same time desire to shoot themselves in the foot or be shoved in a corner by the complexities and the difficulty in attribution of liability in smart contract transactions.
4. Amendment of the existing laws on electronic signature to include a more expansive description of electronic signature to include cryptographic signatures or symbols. This would make proof of contractual agreements quite easy and straightforward.
5. Considering the proliferation of smart contract transactions, having a robust legislation to regulate on blockchain transactions with clear definitions on key concepts such as smart contracts and provisions for liability assignment is indispensable.

5.0.Conclusion

Blockchain technology and Smart contracts are revolutionary to the commercial space. Over and above traditional contracts, smart contracts hold great benefits to parties who employ them. As such, as much as parties are desirous of enjoying these advantages, they must be wary of the complexities in smart contracts and make adequate provisions to cater for thorny issues such as the question of liability.Perhaps it is safe to adopt the approach surmised by Sir Geofrey Vos of the United Kingdom when he stated as follows, '*There is no point in introducing regulations until you properly understand the legal status of the asset class that you are regulating. Likewise, one cannot consider what remedies ought or ought not to be available until one has that same underlying understanding.*[48]In the same vein, parties, regulators and lawmakers alike must seek an active and clear understanding of the nature of smart contracts and their interplay with other forces to adequately address the issue of liability in smart contracts.

[48] Sir GeofreyVos, 'The Launch of the Legal Statement on the Status of Cryptoassets and Smart Contracts'<https://www.judiciary.uk/wpcontent/uploads/2019/11/LegalStatementLaunch.GV_.2-1.pdf> accessed 9 March 2022