Plagiarism Declaration

"This thesis/dissertation has been submitted to the Turnitin module (or equivalent similarity and originality checking software) and I confirm that my supervisor has seen my report and any concerns revealed by such have been resolved with my supervisor."

Name: Oriana Esau

Student number: ESXORI001

Signature: Signed by candidate

Date: 30 JUNE 2022

SMART CONTRACTS: A SOUTH AFRICAN PERSPECTIVE

A legal analysis of the possibilities and challenges posed to the recognition and enforcement of smart contracts under the South African law of contract

By Oriana Esau
ESXORI001

TABLE OF CONTENTS

I. CHAPTER ONE – INTRODUCTION 3

1.1 Introduction 3

1.2 Contextual Background of Smart Contract Technology 4

(a) Why Smart Contracts? Smart Contracts versus Traditional Contracting Methods *5*

(b) Smart Contracts as Reflecting Fourth Industrial Revolution Modes of Interactions *9*

1.3 Research Question 9

1.4 Organization of Study 10

II. CHAPTER 2 – UNDERSTANDING SMART CONTRACTS 12

2.1 Defining Essential Terms 14

(a) Smart Contract *14*

(b) Decentralised Ledger *16*

(c) Blockchain *16*

2.2 Fundamentals of a Smart Contract 17

III. CHAPTER 3 – SMART CONTRACTS AND THE EXISTING LEGAL FRAMEWORK 22

3.1 Contracts – The South African Framework 22

(a) Elements of a Valid Contract at Common Law *22*

(b) Legislative Provisions Relevant to Electronic Contracts *23*

3.2 Understanding Smart Contracts through the Common Law and Legislative Framework 26

(a) Is a Smart Contract an "Electronic Agent" within the Meaning and Scope of the ECTA? *28*

3.3 Matters Relating to Smart Contract Formation 30

(a) Assessing Offer and Acceptance *30*

(b) Assessing Capacity and Authority *35*

(c) Assessing Certainty of Terms *36*

(d) Assessing Certainty of Object/Identifying the Object *39*

3.4 Smart Contracts – International Perspective 40

IV. CHAPTER 4 - NON-ENFORCEMENT, NON-PERFORMANCE, AND REMEDIES OF SMART CONTRACTS 45

4.1 Electronic Mistakes and Smart Contracts 45

(a) Legislative Framework *45*

(b) B2C2 Ltd v Quoine Pte Ltd – Electronic Mistakes, Unilateral Mistakes and Smart Contracts *48*

(i) The Facts 48

(ii) The Dispute 49
(iii) The Court on Unilateral Mistake and Smart Contracts 50

(b) Quoine Pte Ltd v B2C2 Ltd - B2C2 Ltd v Quoine Pte Ltd Taken on Appeal *52*

(c) B2C2 Ltd v Quoine Pte Ltd Discussed *53*

4.2 Non-Performance and Smart Contracts 55

4.3 Remedies for Breach and Smart Contracts 59

V. CONCLUSION 64

5.1 Findings and Recommendations 64

I. CHAPTER ONE – INTRODUCTION

1.1 Introduction

> "Our metaphors of law struggling to keep pace with technology reflect an important truth: as technology changes, legal dilemmas arise. As technological change becomes increasingly rapid, the need for a methodical response to these problems becomes increasingly urgent. We need to closely analyse the roles played by different legal institutions and the methodologies they adopt in easing the law's transition to the future."[1]

The advent of electronic commerce has allowed for various transactions to be moved online. Coupled with the dawn of the Fourth Industrial Revolution and the technological progress which precipitated it, traditional modes of commercial transactions have been disrupted by the options available to actors within the marketplace when executing contracts of a commercial nature.[2] Technology is being used to provide efficient and safe digital platforms to a broader range of providers and procurers of products and services; thereby allowing for more users to access the marketplace and enabling transactions across greater geographical areas.[3] The digitalization of the economy has taken place across a wide range of industries and the expansion of transactions capable of being executed online has allowed for this to become commonplace. The expanding digitalization of electronic commerce, the systems by which goods and services are made and supplied, and the opportunities available therein is a crucial component to the Fourth Industrial Revolution.[4]

Moses's above comment speaks to the tension between maintaining a reliable and predictable legal landscape while also allowing for the law to keep pace with rapidly changing technological contexts.[5] As technological innovations become more disruptive of the systems by which we conduct our livelihoods and lifestyles, likewise innovation in legal rules needs to follow in order to ensure that businesses and consumers benefit from technological

---

[1] Lyria Bennett Moses 'Recurring Dilemmas: The Law's Race to Keep up with Technological Change' (2007) 2 *University of Illinois Journal of Law, Technology & Policy* at 285.
[2] Geraint Howells 'Protecting consumer protection values in the fourth industrial revolution' (2020) 43 *Journal of Consumer Policy* at 146.
[3] Ibid at 145.
[4] Ibid at 146.
[5] Moses op cit note 1 at 285.

developments.[6] The legal landscape must respond to the ever-shifting paradigms of technological optimization when engaging in and creating legal obligations.

One manner in which actors are shifting away from more traditional forms of establishing binding arrangements is in the contracting sphere. Smart contracts, and blockchain technology by inclusion, form a significant dimension to the digitalization of the marketplace. Smart contracts are agreements that contain coded, self-executing transaction protocols that operate across a blockchain network. The opportunities which smart contracts and blockchain systems present are vast and capable of significantly transforming commercial transactions. So, too, are the sectors capable of being disrupted by its emergence and development. However, it has necessitated an assessment of where and how these commercial relationships would fall in our present legal schema. Thus, an important concern is the disruption it may cause to how we classify, assess, and understand the legal implications of smart contracting.

1.2 Contextual Background of Smart Contract Technology

Enabling transactions which are secure, transparent, and cost-efficient are a few of the main characteristics of smart contracts. Initially conceived by computer scientist and legal scholar Nick Szabo in 1994, smart contracts were envisioned to respond to the new role of the marketplace; one which facilitated ease-of-access and did away with the costs associated with middlemen.[7] Szabo's writing articulated the necessity for smart contracts from the perspective of the rapidly expanding digital revolution.[8] Here, the interplay between law and technology is highlighted.

Contextualizing his work in the need for laws, institutions and attitudes to adapt to a revolution characterized by the "physics of cyberspace", or the dynamic digital media, Szabo's intention was to address the barriers of high costs associated with global business due to issues of

[6] Christian Twigg-Flesner 'Disruptive Technology-Disrupted Law? How the Digital Revolution Affects (Contract) Law' in A. De Franceschi (ed) *European Contract Law and the Digital Single Market: The Implications of the Digital Revolution* (2016) at 22.
[7] Nick Szabo 'Smart Contracts: Building Blocks for Digital Markets' available at *https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html,* accessed on 30 June 2020.
[8] Ibid.

jurisdiction, security and trust.[9] This digital revolution holds the capacity to change the nature of business relationships and the traditional ways in which these are formalized, the most common of which the commercial contract, characterised by Szabo as "a set of promises agreed to in a 'meeting of the minds'".[10] Visualizing it as a basic building block of the market economy, together the notion of the modern contract and its associated principles are 'encoded' into the common law over the centuries of cultural progression.[11] This highlights the degree of capacity required to redevelop and rederive contract law. Nevertheless, it is Szabo's position that the digital revolution necessitates the development of new institutions and ways of formalizing business relationships.[12]

Viewed alongside traditional forms of contracting, smart contracts, and the protocols which they consist of similarly enable formalized and secured relationships; however, smart contracts also simplify the entire process of contracting. This digital relationship, as laid out by Szabo, is one which brings together the "phases of search, negotiation, commitment, performance, and adjudication" in one realm – that is the smart contract.[13] Thus, they are more functional than paper-based contracts.

(a) Why Smart Contracts? Smart Contracts versus Traditional Contracting Methods

Take a basic sale transaction. Sandile intends on purchasing a necklace from a seller found on a private group on a social media platform. After contacting the seller and settling on a sale price, the parties agree that the seller will organize for the delivery of the necklace. The cost of delivery is charged over and above the sale price of the necklace and will be paid by Sandile via an electronic funds transfer (EFT) transaction in advance of the delivery of the necklace. Sandile is concerned that this may be a hoax; the necklace may not be the same as that posted online, or it may not exist entirely. These concerns may be mitigated if the parties utilised an intermediary which would hold the necklace until the amount has been paid to the seller, after

[9] Nick Szabo 'Formalizing and Securing Relationships on Public Networks' available at *https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/formalize.html ,* accessed on 5 January 2021.
[10] Ibid.
[11] Ibid.
[12] Ibid.
[13] Ibid. See also Nick Szabo 'The Idea of Smart Contracts' available at *https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabs.best.vwh.net/smart_contracts_idea.html*, accessed on 5 January 2021.

which they would ensure that delivery to Sandile has been completed. However, this carries an added cost to both or either of the parties depending on who would bare the expense of this third-party agent. It requires for there to be a further element to their transaction; yet it does address the dimension of lack of trust between the parties to the transaction.

Let us consider the same transaction from the point of view of a platform which operates on a blockchain and utilises a cryptocurrency in fulfilling electronic commercial transactions. Sandile performs an algorithmic search for the sale of a necklace. The private seller has drawn up a simple contract which is computed in code and stored on the blockchain. According to the parameters set out in this coded contract, the agreed amount will be automatically deducted from the buyer's cryptocurrency wallet once the necklace has been sent out for delivery. The delivery feed will be stored on the blockchain, and once delivery has been confirmed, payment will be executed automatically. Smart contracts take on some of the characteristics of the blockchain as they operate on it. The smart contract is immutable: the parties cannot alter or tamper with the code after the parameters have been entered. Thus, it would not be possible for the seller to change the sale price of the necklace; nor would Sandile be able to reverse or prevent payment. A second quality which is applicable to smart contracts is that the output of the contract is distributed. By this, it is meant that the output is validated by everyone on the blockchain network. Validation is decentralized. This prevents tampering by way of, for example, forcing the payment to be released without executing delivery. The need for an intermediary is taken away and the dimension of trust is addressed. The utilisation of this method of transacting is more transparent for both the seller and the buyer. Although the aforementioned is a simple peer-to-peer transaction, it is apparent that a platform which is able to provide transparency in the marketplace would allow for greater ease of access for consumers and suppliers wishing to transact.

The possibilities presented by this method of contracting are broad, making it an attractive means for transacting. Its capabilities are better illustrated when considering larger and more complex transactions. Smart contracts, as applied alongside blockchain technology, are finding application in supply-chain management systems as they allow for merchants to have end-to-end product tracking and monitoring. From product inception to distribution, smart contracts

can enhance the scale and range of digital processes in creating information pipeline systems.[14] These systems are envisioned as "cyber-physical"; they allow for supply chain systems to transcend from the rigid distribution of processes in a physical system towards one which is more dynamic.[15] Supply chain management systems consist of numerous stages and are formed by entities operating in varying extents of independence in the process of product manufacturing and exchange.[16] The complexity of the system is illustrated in its capacity to span sectors, regions, stages, and time.[17] A digital ledger system allows for transactions and the flow of goods to be more transparent and reliable.[18] Where this is coupled with the use of smart contracts, the system becomes autonomous and secure.[19] The movement of goods is smoother and more trustful.[20] Additionally, the traceability of products in the food industry, in so far as the supply chain is concerned, is beneficial to consumers.[21] The benefit to consumers can be seen in the National Livestock Identity System, or NLIS, a livestock tracking system utilised in Australia for the purpose of tracking herds from birth to slaughter.[22] Here, the benefit to consumers is found in the capacity to route safety or quality concerns. Aside from this, a smart contract and blockchain enabled system can overcome the risks of the traditional supply chain model, specifically: the centralization of data in a locally stored system, mistrust between entities arising from the aforementioned, an increase in communication costs to address this, and the tampering of data leading to inconsistent information causing a disruption to product traceability.[23] Such a system would consist of a permanent and unalterable record of transactions and the flow of goods and services, thereby allowing for product traceability.[24] The decentralization of the system and the creation and storage of encrypted data in chronological order aids in making the system more secure and preventing information from

[14] Alexandre Dolgui, Dmitry Ivanov, Semyon Potryasaev, Boris Sokolov, Marina Ivanova & Frank Werner 'Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain' (2020) 58 *International Journal of Production Research* at 2184.
[15] Ibid at 2185.
[16] Shangping Wang, Dongyi Li, Yaling Zhang, and Juanjuan Chen 'Smart contract-based product traceability system in the supply chain scenario' (2019) *IEEE Access* at 115122.
[17] Ibid.
[18] Bhabendu Kumar Mohanta, Soumyashree S. Panda, and Debasish Jena 'An overview of smart contract and use cases in blockchain technology' 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT) at 2.
[19] Ibid.
[20] Ibid.
[21] Wang et al op cit note 16 at 115122.
[22] Ibid.
[23] Ibid at 115123.
[24] Ibid.

being tampered with.[25] Indeed, it allows for transparency between all entities involved and enables the consistent flow of information.[26]

Smart contracts are also envisaged to find application in the transportation and shipping industry through bills of lading, or e-Bills of Lading.[27] Used in the international sale of goods, the bill of lading is a documentary record of transportation that performs the function of providing evidence of carriage terms and receipt of the goods, and additionally acts as a document of title to its holder.[28] Similar to the experience in supply chain management systems, smart contracts can resolve the issue of "closed schemes", or separate systems, by allowing for the broader transaction process to become integrated and, to the extent envisioned by the parties, automated.[29]

Other examples of smart contract application include their use in the diamond industry, where concerns for authentication and ethical sourcing can be addressed by the traceable and immutable nature of smart contracts[30], and the digital rights industry where a smart contract-based system can ensure that royalties are automatically paid through utilising ownership rights in the blockchain system.[31]

Another practical example which illustrates the applicability of smart contracts in our expanding marketplace is that of the freelance or gig economy. The gig economy offers potential for creating diverse sources of income. However, without an intermediary between the employer and the service provider, there is a risk of non- or delayed payment. As smart contracts can hold digital assets, the party who performs the service may receive notification that the amount payable has been transferred to the contract before performing; hence, the paying party cannot delay or prevent payment due to insufficient or non-existent digital assets. Smart contracts can be utilised to execute payment automatically once the service has been

---

[25] Ibid at 115132.
[26] Ibid.
[27] Paul Todd 'Electronic bills of lading, blockchains and smart contracts' (2019) 27 *International journal of law and information technology* at 340.
For further research on electronic bills of lading, see also Niels-Philip Abdellatif 'An Ethereum bill of lading under the UNCITRAL MLETR' (2020) 27 *Maastricht journal of European and comparative law* 250-274.
[28] Roy Goode, Herbert Kronke, and Ewan McKendrick 'Bills of Lading' in *Transnational commercial law: text, cases, and materials* 2015 at 279.
[29] Todd op cit note 27 at 339.
[30] Urvish Thakker, Ruhi Patel, Sudeep Tanwar, Neeraj Kumar, and Houbing Song 'Blockchain for diamond industry: opportunities and challenges' 2020 *IEEE Internet of Things Journal* at 3.
[31] Mohanta et al op cit note 18 at 5.

provided; thereby allowing for service providers a safer environment for the performance of obligations and greater access to economic productivity.

(b) Smart Contracts as Reflecting Fourth Industrial Revolution Modes of Interactions

A brief recount of the development preceding the Fourth Industrial Revolution reveals that not only industrial production has been impacted but also social relations within the commercial transaction setting. Beginning in the late 1700s, the First Industrial Revolution is characterised by the "great divergence of productivity", which saw the move to an industrialist and capitalist society from one characterised by feudalism and farming.[32] The gradual organisation of labour forces resulted in the development of the textile and steel industries, predominantly.[33] The invention of the steam engine during this period lead to further mechanical innovations in the Second Industrial Revolution.[34] Here, industries such as the automotive and metallurgy industry were enabled to develop. Industrial developments saw the speeding up of technological innovations, or leap-frogging, with the Third Industrial Revolution seeing the realization of robotic technology and computers, as well as the rise of nuclear energy and natural gas as energy sources.[35] The shift to the Fourth Industrial Revolution, which is presently underway, is maintained to have begun in the 2000s. Powered by the internet of things and characterised by artificial intelligence, genetic engineering, 3D printing, and the development of high-tech industries, the Fourth Industrial Revolution is set to create an economic paradigm which reflects the possibilities enabled by technology.[36]

1.3 Research Question

The preceding contextualization illustrates that the existing and potential uses for smart contracts are broad. Whether we are to accept the Fourth Industrial Revolution as a revolution

[32] Petre Prisecaru 'Challenges of the fourth industrial revolution' (2016) 8 *Knowledge Horizons – Economics* at 57.
[33] Ibid.
[34] Ibid.
[35] Ibid.
[36] The 'internet of things' entails the connection and integration of devices to collect and exchange data through connection to the internet. It offers the ability to monitor, optimize and automate processes and has transformed business models. See Roberto Grandinetti, Maria Vincenza Ciasullo, Marco Paiola, and Francesco Schiavone 'Fourth industrial revolution, digital servitization and relationship quality in Italian B2B manufacturing firms. An exploratory study' 2020 *The TQM Journal* 647-670 on this.

or are to take it as merely reflecting a change in the context in our technological interactions, it is clear that the innovations it heralds are capable of transforming the marketplace and the manner in which we conduct our business relations therein, in both a practical and normative manner. Furthermore, it is indicative of a change in the dimension of social relations of business transactions, or the culture of contracting if put differently. Certainly, smart contracts provide an appealing alternative to conventional means of contracting, and it is commonly argued that smart contracts will significantly disrupt the legal system as it stands now.[37] Corrales, Fenwick and Happio, for example, argue that it is critical for legal professions to adapt to developments within the space of legal technology or risk being rendered obsolete.[38]

Provocative as the aforementioned argument may be, the objective of the present study is to discuss the nature, scope, and content of smart contracts, as well as blockchain technology in so far as it pertains to the former, with the intention to subjugate it to the South African law of contract as it currently stands. Thus, the primary question which this dissertation intends to address is:

To what extent is South African contract law able to facilitate the recognition and enforcement of smart contracts?

In addressing this question, it aims to speculate potential conflicts and lacunae with existing legal concepts and to assess whether the current regime of commercial contract regulation is well adapted to this mode of exchange. Where such conflict and lacunae vis-à-vis smart contracts and the traditional contract framework exists, proposals for amendments and revision of existing legislation and rules will be provided.

1.4 Framework of Study

This study consists of five chapters. Chapter One provides a contextual introduction to smart contracts, their practical application, and their relevance to commercial transactions. The Chapter outlines the need to interrogate smart contracts in the legal sense and provides a

[37] Twigg-Flesner op cit note 6 at 1.
[38] Marcelo Corrales, Mark Fenwick, and Helena Haapio 'Digital technologies, legal design and the future of the legal profession' 2019 *Legal Tech, Smart Contracts and Blockchain* at 1.

trajectory for the present analysis in addressing that interrogation. Chapter Two discusses the general concept of smart contracts and blockchain technology and the fundamentals thereof in order to explicate their technical and operative framework. The purpose of this Chapter is to provide a baseline understanding of smart contracts to allow for a comparative analysis to be achieved. Chapter Three seeks to provide such a comparative analysis by elaborating on the legal requirements for a valid contract at common law and in terms of legislation. In doing so, it will analyse specific provisions of the legal system and regulations relating specifically to contract formation. It will consider smart contracts according to this framework and anticipate any conflicts or lacunae related thereto. Specific issues relating to contract formation will be highlighted and dealt with. This Chapter will also consider the standing of smart contracts in the legal systems of external jurisdictions in order to provide a cross-border understanding of the possibilities for smart contract inclusion in South African law. Chapter Four considers legal issues in the context of non-enforcement and breach of a smart contract, and possible remedies thereto. Chapter Five offers a conclusion for the analysis and summarizes its findings. A doctrinal research methodology will be employed throughout this research as regard will be had to primary and secondary sources.

The rapidly changing global technological landscape is one which seeks to offer efficiency, simplification of processes and access to more users. Our task, as legal researchers, is to provide a nuanced legal response in anticipation of possible challenges.

II. CHAPTER 2 – UNDERSTANDING SMART CONTRACTS

As of yet, there is no collectively agreed upon definition of a smart contract.[39] Considering Szabo's initial characterisation thereof, his early conceptualization of a smart contract concerned a computer program capable of generating contractual obligations through the embedding of code in a transaction protocol.[40] Accordingly, it carried with it the following identifying factors:

i) a set of promises
ii) in digital form
iii) which includes protocols
iv) that establish the parameters within which performance by the parties is set to occur.[41]

Szabo's writing utilised vending machine contracting as a prototypical smart contract in order to describe the functioning of smart contracts as an automatic machine-based process.[42] The vending machine is coded with protocols: *x* is input in exchange for the output of *y*. Breach by the purchaser is either impossible or expensive: the effort of the risk of detection exceeds justification for breach.[43] The vending machine is a canonical instance of automatic transaction implementation sans the need for a third party; the transaction at hand being to dispense a product in exchange for money.[44] The vending machine is an "asynchronous protocol between the vending machine company and the customer".[45] While a simple transaction, the vending machine illustrates a basic smart contract: property placed in the possession of another in exchange for payment. Importantly, Szabo's initial conceptualization of a smart contract does not include the functioning of the smart contract on a decentralised ledger, as his writing predates blockchain technology and the evolution thereof. Thus, it excludes reference to a ledger system – decentralised or otherwise.

---

[39] Alexander Savelyev 'Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law' (2017) 26 *Information & Communications Technology Law* at 120.
[40] Blaise Carron and Valentin Botteron 'How smart can a contract be?' in Kraus Daniel, Obrist Thierry, Hari Olivier (eds) *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law* (2018) at 105
[41] Szabo op cit note 7.
[42] Ibid.
[43] Jonathan G. Rohr 'Smart Contracts and Traditional Contract Law, or: The Law of the Vending Machine' (2019) 67 *CLEV. St. L. REV.* at 74.
[44] Ibid at 73.
[45] Szabo op cit note 7.

A crucial element of the smart contract is that the contract becomes embedded in the real world, thereby making its breach expensive. It is 'embedded' in the sense that contractual clauses are entrenched in the hardware and software it operates through. Szabo utilizes the example of a digital security system for automobiles. The keys for the operation of the automobile are encrypted and per the protocol of the smart contract may only be operated by the person who owns the property. A smart contract protocol based on a lien arrangement, where the car is used to secure credit, would operate by allowing for the smart contract to invoke a lien protocol to return control of the keys to the creditor if the owner fails to make payments. This does away with the need to employ a third party, in this instance the debt collector. The protocols employed would be different depending on the contractual terms involved. For example, if the automobile contract was a lease arrangement, the final payment would allow for the access of the leaser to be removed.

Four dimensions of contract design are fleshed out by Szabo in making the argument that smart contracts are well-suited to address possible instances of breach.[46] These are observability, verifiability, privity, and enforceability.[47] What is essential to Szabo's argument is the idea of proactive and reactive security.[48] Proactive security entails means by which breach is made impossible or expensive, or contrastingly, either contracting party may drop out with minimal loss in the case of breach.[49] Reactive security pertains to measures which are taken once breach has occurred.[50] These are measures such as physical enforcement through the involvement of third parties or the recovery of damages through the application of the principals of contract law. Reactive security also includes costs to one's reputation.[51] Firstly, observability of performance goes to the ability to observe the other contracting party's performance or to prove performance to others. "Hidden actions" or "moral hazard" goes to the lack of observability and the ability to exit a contract during the performance stage.[52] Where smart contracts are being utilized observability of performance of contractual obligations through the information held in the decentralised distributed ledger would allow for a pro-active form of security.[53]

[46] Ibid.
[47] Ibid.
[48] Ibid.
[49] Ibid.
[50] Ibid.
[51] Ibid.
[52] Ibid.
[53] Ibid.

Secondly, verifiability of performance allows for the confirmation of the performance of obligations.[54] It goes to the ability to prove to an adjudicator that there has been performance or breach. Coupled with observability, it also goes to the capacity to delineate is an error that is taken in good faith in contrast to one which is an deliberate violation.[55] Verifiability of performance through confirmation of actions via the distributed ledger system will allow for differentiating between intentional violations or good faith errors.[56] Thirdly, privity goes to the potential of party vulnerability to external third parties.[57] Security corresponds to this dimension as the contract must be secure against passive observers and malicious interferers.[58] Privity enfolds performance so that the information pertaining to the contract and its control may be maintained by the parties to the contract to the exclusion of third parties, aside from where there are designated adjudicators.[59] The protection of knowledge pertaining to the contract and its parties and obligation are subsumed under this generalized legal principal as applied to smart contracts. Privity of contract through the anonymity attached to electronic signatures and knowledge being restricted amongst parties only as much as necessary for contractual performance allows for the minimization of vulnerability to third parties.[60] Fourthly, enforceability is a dimension that is both an objective to be achieved and minimized. The need for enforceability and reactive security through judicial systems is minimized through the mechanism being self-enforcing.[61] Furthermore, Szabo argues that when improving the other objectives of contractual design, the need for enforceability is again minimized.[62]

2.1 Defining Essential Terms

(a) Smart Contract

A simple definition of a smart contract is a computer program that allows for parties to code their obligations to a transaction; obligations which are, in whole or in part, self-executed by

[54] Ibid.
[55] Ibid.
[56] Ibid.
[57] Ibid.
[58]Ibid.
[59] Ibid.
[60] Ibid.
[61] Ibid.
[62] Ibid.

the program.[63] The coded obligations are executed according to an 'IF (when) this, THEN that' binary with no opportunity for interference with its terms or operation.

Smart contracts are computer programs which ensure the execution of contractual performance while allowing for the bypassing of traditional economic intermediaries[64]; the element of autonomous self-execution allowing for this labelling of 'smart'.[65] Most commonly used with cryptocurrencies, smart contracts allow for users to transact with digital assets in a decentralized, direct, and distributed manner. They have the ability to be more functional than traditional contracts and may usher in an era of contracting institutions suitable for a marketplace that is characterised by greater distance, anonymity of actors, and ease of access for participants.

For present purposes, a brief technical outline of a smart contract is provided. In order to function, the following four elements are required[66]:

- The source code – the computer code details the transaction that is intended to take place
- The wallet – the wallet holds the cryptographic keys. The cryptographic keys may take two forms: a private key or a public key. The former is used to allow access to a digital asset and allows control of an account. The purpose of the latter is to allow for the authentication of messages and the encryption thereof.
- A storage file – the storage file stores the transaction before it is registered.
- The register – the register stores the transaction once it has been registered. This mostly occurs on the blockchain.

Once the smart contract is stored on the blockchain, miners on the network must reach consensus on the conclusion of its execution in order to update it. Furthermore, smart contracts allow for obligations to become automatically enforceable once the parties have set out the

[63] José Carlos Pereira 'The genesis of the revolution in Contract Law: Smart Legal Contracts' 2019 *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance* at 375.
[64] Vassilis Hatzopoulos and Sofia Roma 'Caring for sharing? The collaborative economy under EU law' (2017) 54 *Common Market Law Review* at 81.
[65] Savelyev op cit note 39 at 117.
[66] Gabriel Olivier Benjamin Jaccard 'Smart Contracts and the Role of Law' (2017) 23 *Jusletter IT* at 5.

terms and conditions, or protocols, entailed therein.[67] This, ideally, allows for contractual agreements to be executed in a transparent manner.

(b) Decentralised Ledger

A ledger can be understood as a digital record of transactions.[68] Ledgers can be centralised or decentralised.[69] The former is one which is controlled or run by a central authority, the latter is decentralised so as to eradicate the requirement for an apex authority to process or validate transactions.[70] In a distributed system, the data stored is accessible to all users operating the same protocol and, as such, is replicated and synchronized across multiple sites.[71] A distributed ledger maintains real-time information and communicates with other computers, or nodes, through a peer-to-peer network.[72] The records are cryptographically protected. Within a shared database only relevant users in the network may control it.[73]

(c) Blockchain

One type of distributed ledger that tracks and maintains information about transactions involving digital assets is called a blockchain.[74] Records are grouped in blocks, linearly, and in chronological order. They are encrypted and collectively form a network of transactions that are traceable and unalterable.[75] Blockchain is both decentralised and distributed as it lacks a central authority and relies on distribution in order to reach consensus. There are various methods through which consensus is reached. Proof of work and proof of stake are two such. Blockchain technology is most widely known to be utilised in conjunction with cryptocurrencies such as Bitcoin.[76] A blockchain may also be permissioned or permissionless; the distinction between the two lying in the fact that the former requires participants to be

[67] Jack Gilcrest and Arthur Carvalho 'Smart contracts: Legal considerations' (2018) 2018 *IEEE International Conference on Big Data (Big Data*) at 1.
[68] Greeshma Nair and Shoney Sebastian 'Blockchain technology; centralised ledger to distributed ledger' (2017) 4 *Intl Res J Eng Technol* at 2823.
[69] Ibid at 2824.
[70] Ibid.
[71] Sue McLean and Simon Deane-Johns 'Demystifying Blockchain and distributed ledger technology–hype or hero' (2016) 17 *Computer Law Review International* at 1.
[72] Ibid.
[73] Ibid.
[74] Michael Crosby, Pradan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman 'Blockchain technology: Beyond bitcoin' (2016) 2 *Applied Innovation Review* at 8.
[75] Ibid at 14.
[76] Ibid at 7.

authorized in order to read and write on the blockchain while the latter allows for anyone to do so.[77]

The domain of blockchain has enabled smart contracts to be stored on and operate within its network. The technology employed in the blockchain framework allows for smart contracts to adopt the same characteristics, specifically distributed consensus and access to unalterable, traceable, and verified transactions and records.[78] A smart contract does not necessarily need to operate on a blockchain, or decentralised, network. The present analysis shall focus on the nature of smart contracts which do function on blockchain networks.

2.2 Fundamentals of a Smart Contract

Definitions of smart contracts provided by commentators indicate a variance in understanding thereof and an emphasis on different elements to its characterization. For Greenspan a "smart contract is a piece of code…stored on [a] Blockchain, triggered by Blockchain transactions… which reads and writes data in that Blockchain's database".[79] Central to this definition is, clearly, the element of the blockchain. This seemingly understates the obligatory aspect of a smart contract and focuses instead on the element of data storage. Hingley describes smart contracts as "a piece of computer code that is capable of monitoring, executing and enforcing an agreement"[80] while Jaccard's definition includes the aspect of a distributed ledger by outlining a smart contract as "software, with which computer code binds two, or a multitude, of parties in view of the execution of predefined effects, and that is stored on a distributed ledger".[81] Szczerbowski's description of a smart contract includes the dimension of control over assets by defining it as "an event-driven program…that run[s] on a distributed, decentralized, shared and replicated ledger… that can take custody over and transfer assets on the ledger".[82] Szczerbowski's description and inclusion of digital assets goes to the electronic

[77] Karl Wüst and Arthur Gervais 'Do you need a blockchain?' 2018 *Crypto Valley Conference on Blockchain Technology (CVCBT)* at 45.
[78] Crosby et al op cit note 74 at 13.
[79] Gideon Greenspan 'Beware of the Impossible Smart Contract' available at *https://www.multichain.com/blog/2016/04/beware-impossible-smart-contract/*, accessed on 20 March 2021.
[80] Hingley quoted in Riccardo de Caria 'The Legal Meaning of Smart Contracts' (2019) 6 *European Review of Private Law* at 735.
[81] Jaccard op cit note 66 at 4.
[82] Jakub J. Szczerbowski 'Place of Smart Contracts in Civil Law. A Few Comments on Form and Interpretation' 2017 *Proceedings of the 12th Annual International Scientific Conference New Trends* at 333.

nature of smart contracts. Savelyev identifies this factor amongst six others: solely electronic nature, software, implementation, increased certainty, conditional nature, self-enforcement; self-sufficiency.[83]

- Solely electronic nature

Core to the identification of a smart contract is its electronic form. Furthermore, it is driven by its subject matter or assets: these may be digital assets, or crypto assets, such as cryptocurrencies.[84] The subject matter may also concern digital manifestations of offline assets. The execution of the smart contract is connected to the incidence of certain electronic events and/or by the transmission of certain data.[85] Smart contracts rely upon electronic signatures based in encryption technology.[86] These factors predefine the electronic nature of the smart contract and are core to its self-enforceability.

- Software-implemented

This goes to the term "code is law".[87] The contractual terms of the contract are computer code, and it is this code that is authoritative.

- Increased certainty

Smart contracts have software code at their core; their terms being expressed in a computer logic – a formal language in its substance, with precisely defined semantics and composition.[88] Unlike natural language, it does not allow for discretion.[89] This mitigates issues of inconsistent interpretation, thereby decreasing the chance for ambiguity.

- Conditional nature

Flowing from the aforementioned, conditional statements are fundamental to computer logic. Binary conditions such as "if 'x' then 'y'" are statements central to smart contracts.[90] The

[83] Savelyev op cit note 39 at 124-127.
[84] Ibid.
[85] Ibid.
[86] Ibid.
[87] Ibid.
[88] Ibid at 125.
[89] Ibid.
[90] Ibid at 126.

contract is enforced because of the running of the circumstance through the conditional statement.[91]

- Self-enforceability

Smart contracts execute their protocols independent of the will of the contracting parties.[92] The programme verifies the conditions and makes entries on them in the blockchain network. This occurs *sans* interference from an intermediary.

- Self-sufficiency

Smart contracts exist independently from legal institutions.[93]

Savelyev's sixth element of self-sufficiency can be contested, as it is arguable that a smart contract can be wholly independent from legal institutions. However, this is a matter which will be discussed further on in this contribution when one considers smart contracts from the perspective of legality. Nonetheless, what Savelyev seemingly attempts to highlight is the existence and execution of smart contracts without legal interference. Raskin's commentary on smart contracts goes to this point by distinguishing between "strong" and "weak" smart contracts.[94] Strong smart contracts carry high, inhibitory costs for the cancellation and reformation of its terms and execution by courts, while weak smart contracts carry little to no prohibitive costs; essentially, a court will be able to alter the smart contract with relative ease.[95] This bifurcation is thus based on the costs carried with interference of the smart contract. Larger costs associated with the ability of the courts to alter the smart contract entails that it would not make much sense for the courts to do so, thereby making the smart contract stronger.[96] The ability of the court to alter after it has been executed determines it as weak.

A further way to define smart contracts is to classify them according to a spectrum. Madir adopts such an approach.[97] On one end of the scale, a contract may be coded, entirely or partly, in a programming language.[98] The computer software plays an integral part of the performance

[91] Max Raskin 'The law and legality of smart contracts' 2017 *Geo. L. Tech. Rev. 1* at 313.
[92] Savelyev op cit note 39 at 126.
[93] Ibid at 127.
[94] Raskin op cit note 91 at 310.
[95] Ibid.
[96] Ibid at 311.
[97] Jelena Madir 'Smart Contracts:(How) Do They Fit Under Existing Legal Frameworks?' 2018 at 5.
[98] Ibid., p. 5-6.

of the contract: all or some of the obligations and rights of the parties are expressed in code rather than in natural language. Following this on the spectrum, a contract may be coded in a programming language but have a separate natural language version.[99] Following on from this, Madir's spectrum of contract possibilities then identifies that a smart contract may be a "split" ordinary language contract coupled with encoded automated execution.[100] Finally, the last aspect of the spectrum identifies that smart contract may be a natural language contract with an encoded mechanism for payment, as the case may be.[101] In illustrating this, Madir utilizes the example of an insurance company utilizing software which would review and decide upon complaints made by a client and automatically initiate payments made in respect thereof.[102] Here, the parties would agree that the software would perform and enforce aspects of the contract, that being the assessment of claims and acting upon determinations made in light of.[103] This functioning of automated software is taken in contrast to the encoding of natural language in order to model a legal contract in code.

When the contract was entered into is also relevant here. In the case that the smart contract was executed after a legal contract, that is to say that a legal contract was utilised external to the blockchain system, the legal contract would be legally binding.[104] The parties to the legal contract may agree that their obligations be transposed into a smart contract in part or in whole. However, where a smart contract causes a legal contract to arise, or rather where a legal contract is affected through a smart contract and is embedded in the blockchain from inception, a contractual relationship is entered into and the smart contract – or smart legal contract as it would be termed for ease of reference – is legally binding.[105]

The lack of consensus on a definition for and legal standing of smart contracts can largely be attributed to the tension between accepting smart contracts as legal contracts or considering them merely as computer code capable of self-executing a process in a transaction, in whole or in part. The former refers to smart legal contracts: contractual obligations represented in whole or part by automated software performance.[106] The smart contract creates binding legal

[99] Ibid., p. 6.
[100] Ibid.
[101] Ibid.
[102] Ibid.
[103] Ibid.
[104] Carron op cit note 40 at 111.
[105] Ibid at 113.
[106]Madir op cit note 97 at 3.

obligations. The latter refers to smart contract code, which refers to the embedding of automated transaction processes in code without the requirement of human involvement in performance.[107] Here, authors argue that smart contracts enable execution of a contractual obligation. Accordingly, smart contracts are code and do not create contractual obligations or legal bonds.

Take the sale of the necklace once more. Sandile and the seller entered into a contract of sale prior to entering into the smart contract. They agree that payment will take place once the delivery information has automatically been uploaded onto the blockchain. A part of the transaction will be self-executed by the program once the predefined conditions have been met. Here, the legal contract pre-dates the smart contract. However, if the seller had set up their sale on the blockchain initially, a legal contract is entered into, and the obligations directly executed.

Madir takes the position that smart legal contracts and smart contract be understood under one overarching relationship that generates lawfully enforceable rights.[108] Per this argument, smart contract code is distinct from smart legal contracts; however, the latter is dependent on the former in order for it to be implemented. Pieces of code that are constructed to execute a task, or multiple tasks, according to the logic computed functionally constitute smart legal contracts. In making this case, it is clear that smart contracts require an overarching legal system to operate, as it is this legal system which will determine whether a valid obligation has been created.

In summation, and remaining cognisant of its intricacies, the following working definition based on the preceding notions can be deduced: *a smart contract is an agreement between two or more parties that is coded according to predefined parameters, and which will execute on a subject matter when triggered by the processing of events and/or data on the blockchain database.*

[107] Ibid at 2.
[108] Ibid at 3.

III. CHAPTER 3 – SMART CONTRACTS AND THE EXISTING LEGAL FRAMEWORK

Having fleshed out common attributes of smart contracts and drawn up a working conceptualisation thereof, this paper now moves to the South African contract law framework. The numerous approaches to understanding and defining smart contracts goes to its intricate technological foundations and its novel nature in the realm of electronic transactions. Bearing this in mind, this section will set out the key legal requirements for a traditional, or natural language, contract. South African law of contract is derived from and developed out of Roman-Dutch and English legal principles. Where the common law is insufficient to address changing contexts or fails to provide for such at all, legislation is needed in order to address the chasm in our law. Thus, both the common law and legislation will be used in considering smart contracts according to the framework laid out by our common law and legislation in order to elucidate the position, if any, smart contracts hold in South African law. Lastly, the regulatory approaches of external jurisdictions and international organisations towards the recognition of smart contracts as legally valid contracts will be discussed in order to ascertain any possible insights for the purposes of developing South African contract law in so far as smart contracts are concerned.

3.1 Contracts – The South African Framework

(a) Elements of a Valid Contract at Common Law

A contract must satisfy these conditions in order to be legal and enforceable under South African common law[109]:

(i) consensus – or *consensus ad idem*, a meeting of minds on all material aspects to the agreement;

(ii) capacity – parties to the agreement must possess the requisite legal capacity to contract;

(iii) formalities – contract must adhere to the formalities required for the agreement where such exist, either by statute or as by agreement between the contracting parties;

(iv) legality – the agreement must not be unlawful;

[109] Dale Hutchison 'The Nature and Basis of Contract' in Dale Hutchison and Chris-James Pretorius (eds) *The law of contract in South Africa* 2 ed (2017) at 6.

(v) possibility – the obligations assumed by the parties must be capable of being performed at the time when the agreement was entered into;

(vi) certainty – obligations entailed in the agreement must be capable of being ascertained, defined, and determined.

A contract is formed where its parties have communicated an offer and corresponding acceptance of its terms and obligations, with serious intention to be bound thereto, or animus contrahendi, coupled with their manifestation and concordance of will.[110] Traditional contracts function on the assumption of human volition in the performance of contractual obligations – in so far as there is capacity to contract, the formalities have been met, and the contract is lawful, certain and capable of being performed.[111] Where the parties rely on an electronic agent or electronic means to form and conclude a contract, such requires the intervention of legislation.

(b) Legislative Provisions Relevant to Electronic Contracts

The Electronic Communications and Transactions Act 25 of 2002[112] (ECTA) aims to establish a national strategy for the facilitation and regulation of electronic communications and transactions in South Africa and matters connected thereto. ECTA grants legal enforceability and validity to automated transactions. Nonetheless, as with all contracts, the formation of valid agreements is governed by established common law rules. Here, reference is made to section 3 of ECTA.[113] Thus, although ECTA supplements the common law, automated transactions must continue to fulfil the requirements of a lawful and binding contract at common law. The following sections are relevant to this contribution as they go to contracts which are concluded by electronic means.

i. Section 20 of the ECTA recognises that an agreement may be formed by an automated transaction whereby either one or all parties utilise an electronic agent in order to form an agreement.[114]

[110] Ibid at 4.
[111] Ibid at 6.
[112] Electronic Communications and Transactions Act 25 of 2002
[113] Ibid Section 3.
[114] Ibid Section 20.

ii. Section 22(1) of the ECTA continues on to provide that an agreement formed wholly or partly by means of data messages has legal force and effect; therefore, providing agreements concluded by way of the communication of data messages with the same legal recognition and enforceability as traditional contracts.[115]

iii. Section 22(2) outlines that such an agreement is assumed to have been completed at the time and location where the offeror receives acceptance of the offer.[116]

iv. Section 23 of the ECTA pays regard to the time and place of communications and the dispatch and receipt thereof, and outlines that a data message is deemed to have been transmitted by the originator when it enters an information system that is not under the originator's control or when the originator and addressee are located inside the same information system.[117] The addressee is deemed to have received the data message when it has entered the information system as designated for its purpose and is capable of being retrieved and processed by the addressee.[118]

v. Section 23(3) stipulates that the data message must thereafter be treated as having been sent from or received at the normal place of business or residence of the originator or addressee, as applicable.[119]

vi. Section 25 of the ECTA outlines that a data message will be attributed to the originator if it was sent by the originator personally; or by a person who had the requisite authority to act on behalf of the originator; or an information system programmed by or on behalf of the originator to operate automatically.[120]

vii. Section 26 of the ECTA provides that lack of acknowledgement either by communication, automated or otherwise, or by way of conduct which would indicate receipt of a data message does not affect the legal force of that message.[121] The reception theory therefore applies to electronic transactions.

[115] Ibid Section 22(1).
[116] Ibid Section 22(2).
[117] Ibid Section 23.
[118] Ibid.
[119] Ibid Section 23(3)
[120] Ibid Section 25.
[121] Ibid Section 26.

The ECTA defines essential terms to the aforementioned in section 1 thereof:

- an electronic agent' constitutes a "computer program or an electronic or other automated means used independently to initiate an action or respond to data messages or performances in whole or in part, in an automated transaction"[122]
- a data message is "data generated, sent, received or stored by electronic means"
- the meaning of data is "electronic representations of information in any form"[123]
- an automated transaction is "an electronic transaction conducted or performed, in whole or in part, by means of data messages in which the conduct or data messages of one or both parties are not reviewed by a natural person in the ordinary course of such natural person's business or employment"[124]
- an information system is "system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet"[125]

The ECTA does not define a computer program. However, the Copyright Act might provide elucidation on this as it defines it as "a set of instructions fixed or stored in any manner and which, when used directly or indirectly in a computer, directs its operation to bring about a result".[126]

Section 13 pertains to electronic signatures and stipulates that an electronic signature is not legally ineffective purely due to the fact that is in electronic form.[127] Section 13(4) extends this to an advanced electronic signature and identifies that such a signature is required in relation to a data message in the instance that the signature of a user is required by law but such law does not identify the type of signature.[128] Section 1 differentiates an electronic signature from an advanced electronic signature by defining the former as meaning "data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature" and the latter as meaning "an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37".[129] Section

[122] Ibid Section 1.
[123] Ibid.
[124] Ibid.
[125] Ibid.
[126] Copyright Act 98 of 1978.
[127] ECTA supra note 112 Section 13.
[128] Ibid.
[129] Ibid Section 1. Section 37 of ECTA identifies this as the Accreditation Authority, if read with Section 1 this presumably means the Director General of the Department of Communications. Section 37 of the ECTA further

13(3) further provides that in the case that the parties have agreed to utilise an electronic signature in an electronic transaction but have not identified the type of electronic signature, such a requirement will be met in regards to a data message if the identification of the party and their approval of the information communicated is achieved, and if in the circumstances the method used was suitable for the objectives for which the information was communicated.[130] Thus, in such a situation, regard is had to the intention manifested by the parties to be bound to the contractual terms of the electronic transaction.

Chapter V of the ECTA pertains to cryptography providers and provides for the requirement of suppliers of cryptography products and services to register them with the Department of Communications which will maintain a description thereof in a register.[131] As this section only pertains to the suppliers thereof, it does not provide a regulatory outline that addresses the use of cryptographic products. Section 1 of the ECTA defines 'cryptography product' as "any product that makes use of cryptographic techniques and is used by a sender or recipient of data messages for the purposes of ensuring (a) that such data can be accessed only by relevant persons; (b) the authenticity of the data; (c) the integrity of the data; or (d) that the source of the data can be correctly ascertained".[132] A 'cryptography provider' is any person who provides the aforementioned products or services in South Africa. A 'cryptography service' is that which facilitates the use of cryptographic techniques for safeguarding the access to, or authenticity integrity of, or source of the data or data or message being sent or received or stored.

Notably, the ECTA does not indicate a link between an electronic agent employing the use of cryptographic techniques in performing an automated transaction.

3.2 Understanding Smart Contracts through the Common Law and Legislative Framework

The ECTA employs the principle of technology neutrality in its provisions as it does not identify a specific technology or tool as the medium through which transactions are

pertains to accreditation for authentication products and services for the purpose of advanced electronic signatures.

[130] Ibid Section 13.

[131] Ibid Section 29 – 32.

[132] Ibid Section 1.

conducted.[133] The Act chooses rather to reference electronic contracts as concluded by electronic agents in general. Further, ECTA does not distinguish between electronic agents based on the extent of their relative autonomy. The Act confers upon them passive status in order to achieve the principle of functional equivalence: the principle that paper-based and electronic communications are treated the same by the law.[134] Pistorius further argues that functional equivalence is achieved by the Act through its employment of attribution in Section 25.[135] Attribution, as opposed to authentication, goes to whether an electronic event can be related to a human user whilst authentication goes to the rules relating to the formation, identification, and control of authentication products and services.[136] Attribution is the process of ascertaining whether a data message was sent by the human user designated as originator and the circumstances under which one can assume that it was.[137] In the scope of the contractual relationship, the actions of the electronic agent are attributed to the user in prescribed circumstances as per Section 25.[138] Accordingly, attribution transpires when the data message is effected by the originator personally, or by someone authorized to act on their behalf, or by an information system instructed to function automatically.[139] The caveat to this is expressed in Section 25(c) of ECTA, which provides that attribution will not occur if it is proven that the information system operated incorrectly in executing its programming.[140]

Pistorius argues that this position is concordant with the position at common law as it is commonplace to ascribe the actions of the machine to the user who instructed it to carry out that particular function/s.[141] Reference is made here to *Thornton v Shoe Lane Parking*, a seminal case in which dealt with the issuing of a ticket by an automatic machine – a machine in the style of a vending machine was utilised here.[142] It was held that the automatic contract between the user was concluded at the time the user put their money into the machine: "the act of the customer in causing the ticket to be issued is an irrevocable step… the contract is

[133] Tana Pistorius 'Nobody Knows You're a Dog: The Attribution of Data Messages' (2002) 14 *South African Mercantile Law Journal* at 737.
[134] Ibid at 738.
[135] Ibid at 738 & 746.
[136] Ibid at 739.
[137] Ibid.
[138] Ibid at 746.
[139] ECTA supra note 112 Section 25.
[140] Ibid.
[141] Pistorius op cit note 133 at 740 & 746.
[142] *Thornton v Shoe Lane Parking* [1971] 1 All ER

concluded as soon as the customer has taken that step."[143] The absence of human involvement in the process does not impede upon the formation and conclusion of the contract.

By assigning electronic agents a passive status, ECTA avoids the issue of full autonomy on the part of computer programs and treats them as a mere conduit or tool for the originator.[144] Indeed, the electronic agent executes electronic contracts without the intervention of human participants, and in so doing changes the legal relationship between the parties. However, it must be noted that for reasons which abound as noted by Weitzenboeck, the imposition of an agency law relationship on electronic agents cannot be justified.[145] Ultimately, computers lack legal personality and thus capacity to contract.[146]

(a) Is a Smart Contract an "Electronic Agent" within the Meaning and Scope of the ECTA?

A broad interpretation of ECTA does well to address the basic facets of a smart contract. While the Act does not define the term 'electronic', which is present in the meaning of 'data' and 'data message' as supplied, Pistorius notes that in previous versions of the Electronic Communications and Transactions (ECT) Bill a definition identifying it as "digital or other intangible form" was provided for.[147] In deciding whether a short message service, or SMS, constituted a 'data message' within the meaning and scope of ECTA, the Court in *Jafta v Ezemvelo KZN Wildlife* held that what is central to determining what a data message is, is its capability "of being generated or created, sent, received or transmitted and stored" and utilised this framework to form a comparison between the two.[148] The meaning afforded to a data message by the Court in *Jafta* corresponds with the definition a data message in the United Nations Commission on International Trade Law (UNCITRAL) Model Law of Electronic Commerce with Guide to Enactment, 1996.[149] Employing the same logic, it can be said that a

[143] Ibid at 687.
[144] On electronic agents and mere tool theory see also Samir Chopra and Laurence White 'Artificial agents and the contracting problem: A solution via an agency analysis' 2009 *U. Ill. JL Tech. & Pol'y* at 370.
[145] Emily M Weitzenboeck 'Electronic agents and the formation of contracts' (2001) 9 *International Journal of Law and Information Technology* at 218.
On electronic agents and principle of agency see also Anthony J. Bellia Jr. 'Contracting with Electronic Agents' (2001) 50 *Emory Law Journal* 1047-1092
[146] Ibid.
[147] Tana Pistorius 'The Legal Effect of Input Errors in Automated Transactions: The South African Matrix' (2008) 2 *Journal of Information, Law & Technology (JILT)* at 4.
[148] *Jafta v Ezemvelo KZN Wildlife* 2008 10 BLLR 954 (LC) para 111.
[149] See UNCITRAL Model Law of Electronic Commerce with Guide to Enactment, 1996, Art. 2(a): " 'Data message' means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy"

'data message', as construed in Section 1, can be taken to mean the electronic coding language that constitute the operative functions of the smart contract, as the code is stored on the blockchain, transmitted through it, and generated by utilizing its software.[150] Secondly, a transaction conducted by means of smart contracts requires all parties involved to utilize its computer program software; thereby meeting the reference to a computer program in the definition of an electronic agent in ECTA.[151] Thirdly, under Section 25 of the Act reference is made to the use of an information system that is programmed to operate automatically in relaying and responding to data messages.[152] Coupled with the definition of an information system in Section 1, it can be argued that this can refer to the blockchain network upon which the smart contract operates. If we are to take this view, it is the electronic agent (smart contract) that operates with the information system (being the blockchain) to access and act upon data messages (being the coded functions and digitally stored assets) within its system. Furthermore, while the Act does not define the term automated, Section 1's reference to the lack of review by a natural person in defining an automated transaction supports the notion that autonomous self-execution is captured in the Act.[153] Regarding attribution once more, the acts of the smart contract will be attributed to the user if it can be shown that the user of the software programmed it to perform the functions automatically. This would be proven by taking into account the smart contract's blockchain-based coded functions. Thus, if the provisions of ECTA are construed in this broad manner, it can be said that a smart contract is an electronic agent for the purposes of Section 20 of the Act.

However, difficulty arises when considering the autonomous functionality of smart contracts. As has been outlined, smart contracts are able to form and perform agreements, and store digital assets in the form of tokens. Moreover, they can compare performance or non-performance to what has been contractually promised, and upon understanding this can act upon their coded parameters.[154] Thus, the complexity at hand lies not as much with the formation and conclusion of a contractual agreement but more so with the self-executing role smart contracts play in the performance thereof. However, it must be pointed out that this self-executing role is within the coded parameters set out within the terms of the smart contract. Hence, the smart contract does

[150] ECTA supra note 112 Section 1.
[151] Ibid.
[152] Ibid Section 1 & Section 25.
[153] Ibid Section 1.
[154] Jerry I-H Hsiao 'Smart Contract on the Blockchain-Paradigm Shift for Contract Law' (2017) 14 *US-China Law Review* at 689-690.

not employ the full extent of artificial intelligence. Actions are triggered once the nodes within the network address transactions to it. Smart contracts are, therefore, event and data driven as the contract executes once conditions are met. Contextualizing the autonomy of smart contracts in this way makes it apparent that it is too simplistic to construe a smart contract as a mere tool or conduit, or as a messenger as argued by Madir.[155] Smart contracts have the capacity to compare what has or what has not occurred and, upon such an analysis, execute with legal ramifications and effects. Taking this into consideration, it can be said that ECTA does not recognise the range of autonomous software capable of executing complex transactions.

3.3 Matters Relating to Smart Contract Formation

(a) Assessing Offer and Acceptance

This section proceeds with the assumption that the smart contract is the original contract and no 'traditional' contracts precedes it. This is, again, distinguished from the automatability of a contractual clause or clauses, in which case the original contract will govern the automated aspect of said clauses.

The terms of the smart contract are entered by the offeror and placed into the network. Its terms are expressed in coding language. Utilising the Ethereum network for example, the contract holds a unique identification number and operates "as an autonomous entity within the system".[156] This then becomes part of the network. Whether the posting of the smart contract is considered as an offer or an invitation to treat is debatable. The general rule is that advertisements are considered as invitations to do business if we are to construe the posting of the contract as such. [157]As Hawthorne and Hutchison note, however, whether a statement is deemed as an offer is depends on the intention of the offeror or on the reasonable impression created in the mind of the addressee.[158] Taken in conjunction with Durovic and Janssen's sentiments, it can be said that when the transaction is expressed in such binary and precise

[155] Madir op cit note 97 at 10.
[156] Mateja Durovic and André Janssen 'Formation of Smart Contracts under Contract Law' in L. DiMatteo, M. Cannarsa, & C. Poncibò (eds) *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (2019) at 65.
[157] Ibid at 67.
[158] Luanda Hawthorne and Dale Hutchison 'Offer and Acceptance' in Dale Hutchison and Chris-James Pretorius (eds) *The law of contract in South Africa* 2 ed (2017) at 51

terms, the posting of the smart contract constitutes an offer.[159] Conversely, the posting of a message on the Blockchain by a proposing party may be considered as a mere invitation to treat and hold similar standing to an advertisement. An offer is made once the details regarding the parameters of the agreement and the nature of the subject matter of the smart contract are entered into the blockchain database. This offer must be firm, complete, clear, and certain.

Per Section 22(2) of ECTA, an electronic transaction concluded by means of data messages is said to have been successfully completed when the offeror receives acceptance thereof.[160] Read with Section 23, the contract is concluded when the offeror obtains notification of acceptance in its information system.[161]

As previously noted, ECTA adopts the reception theory when assessing whether acceptance of the offer was received. This was confirmed in *Jafta v Ezemvelo KZN Wildlife* where it was held that "section 23 of the ECT Act… adopt[s] the reception theory for receipt of electronic communication".[162] The court went on to explain that under the reception theory, the communication of acceptance is considered to have been received by the addressee despite the addressee lacking knowledge of its receival in their inbox.[163] The court goes on to state that:

> "The data message has to be merely capable of being retrieved; the addressee does not have to actually retrieve it. Furthermore, the addressee does not have to acknowledge receipt of a data message for it to have legal effect."[164]

Additionally, what is crucial to the reception theory is the notion of "the sender losing and the recipient acquiring control" of the message of acceptance.[165] Thus, in so far as electronic transactions utilising the transmittance of data messages are concerned, the ECTA supplants the general common law position which adopts the information theory of acceptance.[166] Per the information theory, an agreement is concluded when acceptance thereof comes to the awareness of the offeror; in essence, where the offeror reads the message of acceptance or is

---

[159] Durovic & Janssen op cit note 156 at 67.
[160] ECTA supra note 112 Section 22
[161] Ibid Section 22.
[162] *Jafta* supra note 148 para 79.
[163] Ibid para 91.
[164] Ibid.
[165] Ibid para 84.
[166] L. L. Ramokanate *Modifying contract law principles to accommodate automated transactions in South Africa* (Unpublished Doctoral dissertation, North-West University, 2018) at 202.

informed thereof.[167] The unsuitability of the information theory for electronic contracts is made apparent here. Turning once more to matter of *Jafta v Ezemvelo KZN Wildlife*, Pillay J's comments support the view of this unsuitability and expounds on this position by affirming that acceptance of an offer may not come to the attention of the offeror in circumstances where the merchandise sold is distributed automatically or via a despatch service.[168]

Consequently, the position taken in this analysis is that a smart contract will be deemed to have been concluded when the blockchain updates its ledger system to record the occurrence of the electronic event of acceptance as exhibited by the transmittance of data messages. This accords with the reception theory captured in Section 23 read with Section 26 of the ECTA. The benefit of this provision is that it allows for agreements to become binding and operative despite the offeror's lack of awareness of the receipt of communication of acceptance.

However, despite the advantages afforded by Section 23 and Section 26 of the ECTA, the wording of the provision does not refer to the use of electronic agents. Section 23 and Section 26 refer to data messages transmitted by the originator and addressee.[169] An originator is defined in Section 1 of the Act as "a person by whom, or on whose behalf, a data message purports to have been sent" and an addressee is defined as "a person who is intended by the originator to receive the message".[170] It is herewith submitted that either the terms 'addressee' and 'originator' be interpreted to include the use of an electronic agent, or the ECTA be revised to include reference to an electronic agent. The former submission on interpretation is supported by Ramokanate who posits that such an interpretation is in accordance with the tone of ECTA, in that the Act regards electronic agents as mere tools for their users.[171] However, this author is in disagreement with this view in so far as smart contracts are concerned, as it has been postulated in subsection 3(a) of this Chapter that it would be incorrect to view smart contracts as mere tools for their users if we are to consider smart contracts as electronic agents for the purposes of the ECTA. Nonetheless, the two viewpoints can be reconciled by the fact that the Act allows for the attribution of the actions of electronic agents to their users in the course of contract formation. Here, regard is had to Section 20(c) of the ECTA, which states that "a party using an electronic agent to form an agreement is… presumed to be bound…

[167] Hawthorne & Hutchison op cit note 158 at 57
[168] *Jafta* supra note 148 para 81.
[169] ECTA supra note 112 Section 23 & Section 26.
[170] Ibid Section 1.
[171] Ramokanate op cit note 166 at 207.

irrespective of whether that person reviewed the actions of the electronic agent".[172] Hence, the actions of the electronic agent are attached to the human user; thus, attributing the acts of electronic agent to the user. If such attribution is envisioned in the Act, the logical conclusion is that acceptance communicated by an electronic agent to that of another must be regarded as being received by the user of that electronic agent and thus communicated to that user personally. Receipt of acceptance will be achieved when the data message is received and processed by the electronic agent. Nevertheless, it is submitted that the Act be revised or interpreted in a manner that would bridge the gap between Section 20 and Section 23 read with Section 26, so as to include application of the latter provisions to instances in which electronic agents transmit data messages conveying acceptance.

The offeree may also accept the contract through their conduct.[173] The offeree may accept the contract by transferring control of the digital or tokenised assets to the smart contract or through the authorization of its transfer by using a special cryptographic key or password.[174] Acceptance and performance by the offeree may, therefore, be somewhat intertwined in that they occur simultaneously. This is taken in contrast to a more passive form of acceptance, whereby the offeree enters their signature – the aforementioned special cryptographic password. Section 13 of ECTA recognises the usage of an electronic signature in forming transactions as being valid.[175] Further, if we are to follow Section 22(2) of ECTA, the smart contract is concluded at the time and location where the offeror receives notification of acceptance on the part of the offeree, which may take the form of the aforementioned acts.[176]

Assessing offer and acceptance aids us in determining the basis of contractual liability, in that it allows us to establish the existence of consensus ad idem. The presence of consensus can be inferred from an offer and its corresponding acceptance. The concurrence of will or intention on the part of the offeror with that of the offeree indicates the presence of consensus. However, how is this to be assessed where electronic agents are interacting with each other in the process of smart contract formation? How ought we to assess such shared expression of intent in the context of an entirely technological environment where code in a blockchain is assessed?

[172] ECTA supra note 112 Section 20(c).
[173] Durovic & Janssen op cit note 156 at 67.
[174] Ibid.
[175] ECTA supra note 112 Section 13.
[176] Ibid Section 22.

If one were to employ a purely subjective approach to the analysis of consensus, as encapsulated by the will theory of contractual liability, one would consider the inner will of the contracting parties. The primary question, here, is whether the parties held the subjective intention to be bound by the contract. As consensus is the primary foundation for establishing contractual liability, the absence of authentic accord of wills will render the contract voidable. If such an approach were to be applied to a contracting environment where an electronic agent is utilised in contract formation and execution, difficulty arises. An entirely electronic environment sans human intervention in contract formation can prove to be difficult when applying traditional legal rules to the establishment of contractual intention as electronic agents cannot be said to have an inner state of mind to which one can refer to in order to establish consensus.

If, however, an objective approach is applied, only the outward manifestation of the contractual statements made by a party will be considered. Here, the declaration theory will ask whether there is a concurrence of declarations. Support for this approach is exemplified in the noteworthy dictum of Wessels JA in the case of *South African Railways and Harbours v National Bank of South Africa Ltd*[177] where it was stated that:

> "The law does not concern itself with the working of the minds of parties to a contract, but with the external manifestation of their minds. Even therefore if from a philosophical standpoint the minds of the parties do not meet, yet, if by their acts their minds seem to have met, the law will, where fraud is not alleged, look to their acts and assume that their minds did meet and that they contracted in accordance with what the parties purport to accept as a record of their agreement."[178]

This dictum continues to hold influence in South African law as demonstrated by Harms JA's reference thereto in the matter of *Sonap Petroleum (South Africa) (Pty) Ltd v Pappadogianis* where it was stated that "The law, as a general rule, concerns itself with the external manifestations, and not the workings, of the minds of parties to a contract."[179] Thus, what is relevant when adopting an objective approach is the outward manifestation of assent.

---

[177] *South African Railways and Harbours v National Bank of South Africa Ltd* 1924 AD 704
[178] Ibid para 715 – 716.
[179] *Sonap Petroleum (South Africa) (Pty) Ltd v Pappadogianis* 1992 (3) SA 234 (AD) at 13.

Extending the objective theory to transactions concluded by electronic agents, Weitzenboeck theorises that the objective approach provides legal legitimacy for contracts established by means of autonomous electronic agents in the context of smart contracts.[180] Accordingly, when determining whether consensus has been manifested, the contractual statements made by the electronic agent will be assessed in order to ascertain whether they amount to a firm offer and unequivocal acceptance.[181] The primary concern is whether objective indicia of assent exists. In the smart contract dimension, Stazi provides that such indicia are demonstrated by the sending off of cryptographic private keys when concluding the smart contract.[182] Additionally, it is demonstrated through the conduct of the parties when uploading digital assets or access thereto.[183] This conclusive behaviour amounts to consent, with the signing of cryptographic signatures serving the purpose of establishing intention.[184]

(b) Assessing Capacity and Authority

The issue of capacity and authority presents complications when assessing smart contracts vis-à-vis the conventional legal framework. The parties to a contract need the requisite capacity to be party to the contract.[185] The legal capacity common to all persons entails the capacity to bear, exercise and attain rights and duties.[186] This may be circumscribed and vary according to age, mental stability, insolvency, and criminal conviction where applicable.[187] The legal capacity of the parties is, therefore, determined contextually and in the instance of a traditional contract, this is easily ascertainable. Additionally, in the case where one of the parties is a corporation, it must be clear that the legal representative has the requisite authority to act on behalf of the corporation.[188]

[180] Weitzenboeck op cit note 145 at 227.
[181] Ibid at 226.
[182] Andrea Stazi *Smart Contracts and Comparative Law: A Western Perspective* (2021) at 111.
[183] Ibid at 112.
[184] Ibid at111. It can also be argued that the user has indirectly manifested their assent to be bound by the smart contract by initiating it as an electronic agent. This would allow for the assent of the electronic agent to be inferred to the human user. See Weitzenboeck op cit note 145 at 227.
[185] Birgit Kuschke 'Contractual Capacity' in Dale Hutchison and Chris-James Pretorius (eds) *The law of contract in South Africa* 2 ed (2017) at 149.
[186] Ibid.
[187] Ibid.
[188] Ibid at 155-156.

In the case of smart contracts, the parties are identified by an address. Private encrypted keys serve as the basis for the digital identity system on the blockchain platform.[189] The cryptographic key represents the person; thus, those who lack capacity in the non-digital world would be capable of setting up an account for the purposes of entering into transactions.[190] Without a test for capacity, there is room for users to take advantage of the system's anonymity. This indicates the needed to have an identification process that would allow for the counterparty to be tracked, and supports the argument that the smart contract only be considered validly concluded if tracing to a particular natural or juristic person is possible.[191] Durovic and Janssen propose that should such a situation arise, the transaction be 're-winded' through a reverse transaction or through allowing for an action of unjustified enrichment to be awarded ex post facto.[192] The latter remedy would be available should the transaction be deemed voidable.

(c) Assessing Certainty of Terms

As outlined earlier in this Chapter, one of the general elements required at common law for a contract to be valid is for its obligations and terms to be certain. The legal consequences of the agreement and the delineation of performance to be undertaken risks failure of certainty if the aforementioned is unclear or if it neglects to outline the material aspects of the functioning of obligations.[193] Should such a failure arise and there is an absence of admissible extrinsic evidence to provide detail, and the naturalia of the agreement or other general doctrines of contract do not provide assistance, the agreement may be rendered null and void.[194] Such an agreement may be deemed void for vagueness, should the affected portion not be severable from the agreement in its entirety.[195]

The coded obligations that encompass the smart contract differs from traditional contracts, in that it uses programming – or artificial language – as opposed to natural language. A provision stated in natural language may take the form of source code, which is then translated into assembly language and, lastly, into bytecode for the purposes of being read by the computer

[189] Durovic & Janssen op cit note 156 at 72.
[190] Ibid at 71.
[191] Stazi op cit note 182 at 107.
[192] Durovic & Janssen op cit note 156 at.72.
[193] LF Van Huyssteen, GF Lubbe, and MFB Reinecke *Contract: General Principles 5*e 5 ed (2016) at 217.
[194] Ibid at 217.
[195] Ibid at 237.

system.[196] As is commonly done in internet commerce, natural language may be used as the interface and the coded language 'hidden' as fine print.[197] For the purposes of ECTA, Section 12 thereof notes that the legal requirement that a document or information be in writing is satisfied if such is in the form of a data message.[198] Hence, it suffices that the terms of smart contracts is contained in coded language.

Nonetheless, where the content of the smart contract is entirely written in code and this is relied upon, it risks intelligibility.[199] Here exists the likelihood that a contracting party lacks understanding of the coded language of the smart contract but nonetheless concludes it. Should such a problem arise, the ex post existence of an error may be invoked in order to request that the contract be cancelled.[200] Considering German and Italian law, the risk of concluding a contract without knowledge of the computer code forming its basis is ascribed to the contracting parties according to the general principles of "self-responsibility and entrustment".[201] Indeed, such an approach accords with the adherence to party autonomy as a foundational principle in South African contract law.

The greater the complexity of the intention of the parties and context in which this and the contract fits, the greater the probability of ambiguity and imprecision regarding this – thus increasing the need for interpretive measures should a dispute arise.[202] Here, the benefit of natural language contracts is highlighted as it is more efficient in describing and formulating the intention of the parties regarding their respective obligations.[203] Taken in contrast to the programming of smart contracts, computer code does not allow for more subjective measures of interpretation as natural language does.[204] It must be said, however, that computer code as a universal language allows for common understanding in the context of contractual relations in comparison to the array of national languages.[205] Nonetheless, in practice one can simply adopt

[196] Szczerbowski op cit note 82 at 336-337.
[197] Ibid at 337.
[198] ECTA supra note 112 Section 12.
[199] Stazi op cit note 182 at 118.
[200] Ibid.
[201] Ibid.
[202] Ibid at 119.
[203] Ibid at 120.
[204] Ibid at 121.
[205] Ibid.

the route of "split contracting" or a "hybrid agreement", where the natural language contract is drafted along with its duplicate in computer code.[206]

A further curious concern regarding the operation of terms is in the context of conditions – specifically suspensive and resolutive conditions. A suspensive condition suspends the obligation to perform until the fulfilment of an event, which may either be positive or negative, depending on whether the event must or must not occur.[207] Should the condition be fulfilled, the obligation will operate as if it had always been functioning.[208] Should the condition not be met, the obligation will be treated as if it had never come into existence and be considered as being void ab initio.[209] A resolutive condition is demonstrated where the obligation/s operate until the fulfilment of an event or a failure of the event to occur.[210] In the instance that the condition fails to be realised, the obligation is likewise treated as void ab initio and the contract will terminate.[211]

Stazi proposes that in the context of smart contracts where a suspensive condition is involved, the smart contract be uploaded on to the Blockchain only once the condition entailed is satisfied; whereas where a resolutive condition is concerned, the "ex nunc dissolution of the previous contract" be accompanied by "a subsequent restitutive bargain".[212] First, in so far as suspensive conditions are concerned, this author suggests the 'layering' of smart contracts be utilized. As the length of a period concerning a future event can be encoded as a provision of the contract, this can be linked to a suspensive condition that is certain to occur; thus, allowing for the relative legal consequence to operate upon the expiry of a certain amount of time.[213] Where the condition is less certain, resort could be had to an external source of data which would allow for the confirmation of the occurrence or non-occurrence of the condition. In either example, the programming of the fulfilment or non-fulfilment of a condition would act as a 'trigger' for the declaration of the contract as void ab initio or not. Secondly, with respect to Stazi's comments regarding resolutive conditions, it is unclear what is meant by 'restitutive bargain'. This author interprets the text as positing that where the previous smart contract is

[206] Ibid at 120.
[207] Catherine Maxwell 'Obligations and Terms' in Dale Hutchison and Chris-James Pretorius (eds) *The law of contract in South Africa* 2 ed (2017) at 250.
[208] Ibid at 250.
[209] Ibid at 250.
[210] Van Huyssteen et al op cit note 193 at 282.
[211] Maxwell op cit note 207 at 250.
[212] Stazi op cit note 182 at 132.
[213] Ibid.

dissolved or terminated on the blockchain due to its condition not being fulfilled, a successive contract is 'triggered' which will allow for the parties to have any performance/s that they have made to be restored to them.

(d) Assessing Certainty of Object/Identifying the Object

Jaccard identifies three broad categories of smart contract subject matter: smart contracts that represent data; smart contracts that represent a legal contract; and smart contracts that represent property.[214] Taking each broad category in turn, smart contracts representing data can be broken down into data without legal impact; data protected by law; and data representing a virtual property or digital property.[215] Data without legal impact generally entails data which, for example, forms the infrastructure of a website or functions as greeter – for which the purposes are to say 'hello'.[216] Data protected by law goes to that which involves intellectual property rights, including copyrights or trademarks.[217] Virtual property is distinguished from digital property in that the former has no actual market upon which to concretize its value and the latter does.[218] Cryptocurrencies are an example of digital property, as there is a market for it; thus, it can form part of one's patrimony.[219] Smart contracts that represent legal contracts are those that imitate the contents and behaviour of a legal contract that "was foreseen as falling under the scope of regulation".[220] Jaccard utilises the structure and functioning of a corporation through stacking smart contracts as an example here.[221] Smart contracts representing property entails both movable and immovable property, and also goes to rights which one holds over property.[222] Within this context, the term 'token' is utilised to refer to the legal title of property.[223] A token may represent anything, and when referencing a physical asset, that property is referred to as 'smart property'.[224] A further category is smart contracts representing rights, such as securities or debt obligations.[225]

[214] Jaccard op cit note 66.
[215] Ibid at 13-15.
[216] Ibid at 13.
[217] Ibid.
[218] Ibid.
[219] Ibid at 14.
[220] Ibid at 15.
[221] Ibid at 16.
[222] Ibid at 18-19.
[223] Ibid at 18.
[224] Ibid at 16.
[225] Ibid.

Considering the South African legislative environment, agreements for the sale of immovable property are excluded from the purview of ECTA and are governed by the Alienation of Land Act.[226] Such agreements are prescribed in Section 4(4) of ECTA with reference to Schedule 2 thereof and particularly the first section of the table therein which outlines that an agreement for the sale of immoveable property procumbent to that provided in the Alienation of Land Act is not to be construed as being made valid by ECTA.[227] However, the case *Borcherds and Another v Duxbury and Others* causes some confusion here as the court held that electronic signature utilised on the offer to purchase was a valid form of signing the agreement and constated an effective mechanism to manifest the seller's intention to be bound.[228] This was in conflict with the general position that contracts for the sale of immoveable property may not be signed electronically. The court in that decision did not, however, have regard to Section 4(4) of ECTA; hence, it is unclear what the outcome would have been had such been done. For the sake of certainty, however, it is posited herewith that in the instance of smart contract, where the sale of immoveable property is concerned, the parties should have an off-chain contract that allows for the parties to affix their signatures in 'wet-ink' in order to meet the requirements set out in legislation and the common law. This proposition can equally be applied to the remainder of the agreements and legal documents contained in Schedule 2 of ECTA, namely: agreements for the alienation of immovable property, agreements for the long-term lease of immoveable property for more than 20 years, the execution, retention and presentation of a will or codicil, and the execution of a bill of exchange (notwithstanding other requirements contained in their respective legislative instruments as may apply).[229]

3.4 Smart Contracts – International Perspective

As of yet, no prevailing international framework for smart contracts exists. However, respective legal systems have introduced initial regulatory responses to the recognition and adoption of smart contracts. The purpose of this section is to consider these regulatory approaches in order to ascertain possible guidelines to similar recognition and adoption in South African law.

---

[226] Alienation of Land Act 68 of 1981
[227] Supra note ECTA, Section 4(4) and Schedule 2.
[228] *Borcherds and Another v Duxbury and Others* (1522/2020) [2020] ZAECPEHC 37
[229] ECTA supra note 112 Schedule 2.

The United States of America (USA):

Respective states in the USA have enacted legislation pertaining to the regulation of smart contracts.

a. The State of Arizona has defined a smart contract as "an event-driven program, with state, that runs on a distributed, decentralized, shared and replicated ledger and that can take custody over and instruct transfer of assets on that ledger."[230] Arizona has also given legal effect to agreements containing smart contracts code: "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."[231]

b. The State of Tennessee has built and expanded upon the aforementioned definition by defining a smart contract as:

"an event-driven computer program, that executes on an electronic, distributed, decentralized, shared, and replicated ledger that is used to automate transactions, including, but not limited to, transactions that:

(A) Take custody over and instruct transfer of assets on that ledger;

(B) Create and distribute electronic assets;

(C) Synchronize information; or

(D) Manage identity and user access to software applications."[232]

c. The State of Illinois enacted its Blockchain Technology Act in 2020.[233] The Act provides recognition for smart contract and blockchain databases and signatures in commercial transactions. The Act defines a smart contract as a contract stored as an electronic record that obtains its verifiability through the use of a blockchain.[234] The Act furthermore provides that smart contracts will not be denied legal effect and allows for their inclusion as evidence in legal proceedings notwithstanding the fact that a blockchain was used to create, store or verify the smart contract.[235] A smart contract, however, will not have legal effect if the blockchain on which it runs does not permit a record of the transaction to be saved or

[230] 2017 Ariz. HB 2417 44-7061
[231] Ibid.
[232] 2018 Tenn. SB 1662 47-10-201
[233] 205 ILCS 730, Blockchain Technology Act.
[234] Ibid.
[235] Ibid.

precisely duplicated for the benefit of any parties who might be entitled to a copy of the contract or a record thereof.[236]

Belarus :

Belarus has legislated smart contracts by way of a Presidential Decree, which defines smart contracts as "a programme code intended for functioning in the distributed ledger for purposes of automated performance and/or execution of transactions or performance of other legal actions."[237]

The United Kingdom:

The United Kingdom Jurisdiction Taskforce (UKJT) published a Legal Statement in November 2019 on the legal status of smart contracts and cryptoassets under English Law.[238] While the taskforce concluded that English Law does not preclude the smart contracts from being legally binding nor cryptoassets from having the legal status of property, it decided not to provide a firm definition of smart contracts.[239] Rather, the taskforce cogitated on what is legally distinctive in smart contracts in comparison to traditional contracts per English Law.[240]

Commentary from United Nations Commission on International Trade Law (UNCITRAL) and the International Institute for the Unification of Private Law (UNIDROIT) Joint Workshop on Legal Issues Arising from the Use of Smart Contracts, Artificial Intelligence and Distributed Ledger Technology:

Held in May of 2019, the joint UNCITRAL/UNIDROIT workshop provides some discussion on the use of smart contracts and related legal issues.[241] Some commentary arising from the workshop is useful for this analysis.

---

[236] Ibid.
[237] Decree of the President of the Republic of Belarus No. 8 (21 December 2017), unofficial translation.
[238] United Kingdom Jurisdictional Taskforce, 'Legal Statement on Cryptoassets and Smart Contracts', The Lawtech Delivery Panel, 2019.
[239] Ibid at 35.
[240] Ibid at 35.
[241] UNIDROIT 'UNCITRAL/UNIDROIT Workshop on Smart Contracts, Artificial Intelligence and Distributed Ledger Technology – Summary Of Conclusions Published, Joint UNCITRAL/UNIDROIT Workshop – Summary Report' 2019 available at https://www.unidroit.org/uncitral-unidroit-workshop-on-smart-contracts-artificial-intelligence-and-distributed-ledger-technology-summary-of-conclusions-published/ accessed on 11 July 2021.

1. A smart contract must still meet the standard, general requirements of a contract in order to for it to be deemed a contract.[242]
2. Smart contracts do not exist within a "normative vacuum"; general rules and principles of contract law do not cease to apply to smart contract – they should be equally applied to them.[243]
3. Future legislative work on smart contracts should include a formal approach of updating and adapting the language of existing legal instruments that may pertain to smart contracts as well as a substantive approach that would focus on liability of technological systems relating to smart contracts.[244] Furthermore, legal regulation should develop alongside the establishment of standards on the matter.[245]
4. The discussion emphasised that existing rules and instruments should be applied to smart contracts despite the development of new legislation and legal instruments; hence, the language of existing texts should be updated.[246]
5. Three possible projects on issues relating to liability, execution and remedies were put forward:

   "a. a review of existing provisions enabling the use of automated systems and analysis of their application to autonomous systems with a view to recognising the validity and legal effect of actions performed, and decisions taken, by autonomous systems; this could be complemented by consideration of a provision relating to the attribution of these actions and decisions;

   b. the development of rules on risk allocation in contractual and extra-contractual matters (including, but not limited to, mistakes, malfunctioning, wrong-doing, default or damages caused by autonomous systems); and

   c. the development of a set of substantive and procedural rules in relation to self-executing enforcement and self-executing remedies, aimed at specifying legal requirements or standards that self-executing enforcement of smart contracts and other automated systems and self-executing remedies in case of defaults should meet in order to ensure validity, conformity with the law, and due protection of rights."[247]

[242]Ibid at 1.
[243] Ibid at 4.
[244] Ibid at 3.
[245] Ibid at 3.
[246] Ibid at 4.
[247] Ibid at 6.

The approaches and recommendations outlined above indicate that, by and large, states and international bodies are eager to permit recognition of smart contracts and blockchain technology. Indeed, as is indicated by the legislative routes taken by several states in the USA, there are clear steps being taken to provide legal force and effect to smart contracts and blockchain transactions. The provisions discussed above indicate the necessity for specificity when defining smart contracts, distributed ledgers, and their respective functions. Moreover, the legislative routes followed indicate the need to develop legislation pertaining to blockchain and distributed ledgers as well as smart contracts, as the two function together. To facilitate the legal development of one to the neglect of the other would result in a gap in our law. Furthermore, there must be clarity as to the evidentiary standing of smart contracts in our law should disputes within such contexts arise. The resolution of the standing of smart contracts in our law is particularly necessary where cross-border jurisdictional issues are concerned, and possible disputes over the nature and definition of smart contracts may arise. Additionally, a well-defined legal approach to smart contracts would facilitate cross-border cooperation as there would be a clear framework as to its recognition and application. The sentiments of the UKJT and UNCITRAL/UNIDROIT Commentary find reference here, as it can be said that the most efficient way to produce best practices around smart contracts and blockchain technology is to build upon existing rules and legislation and implement further legislation where necessary. Such would allow for a solid foundation for the development of contract law around the issue of smart contracts.

IV. CHAPTER 4 - NON-ENFORCEMENT, NON-PERFORMANCE, AND REMEDIES OF SMART CONTRACTS

The purpose of this chapter is to cogitate on the application of conventional legal principles to contracts concluded by algorithmic means in so far as such pertains to smart contracts' capacity to self-perform, execute, and enforce.

A defining feature of smart contracts is their ability to secure performance and eliminate the possibility of breach. However, as expressed by Rajah JC in the case of *Chwee Kin Keong and Others v Digilandmall.com Pte Ltd*, mistakes made in the course of electronic transactions are inevitable and may be due to a range of reasons, including but not limited to "human interphasing, machine error or a combination of such factors".[248] The reality remains that the parties to the smart contract cannot foresee all future events that may impact on their ability to perform or affect their expectations regarding the contract. In these circumstances, non-enforcement and non-performance of obligations may arise, which then gives way for arguments regarding excuses for non-enforcement, breach, and any remedies that may find application.

This chapter will first discuss the challenges that smart contracts pose to the application of conventional legal principles in circumstances in which a smart contract may be determined as void or voidable due to mistake. The case of *B2C2 Ltd v Quoine Pte Ltd* [249] arising out of the Singaporean court and its subsequent appeal will be discussed here, as the court's ruling is the first time an apex court has cogitated on the applicability of contractual principles to contracts concluded by algorithmic means through the use of automated trading software.[250] This chapter will then consider these same challenges in the context of non-performance and excuses for non-performance. Thirdly, it will consider possible remedies for breach of a smart contract.

4.1 Electronic Mistakes and Smart Contracts

(a) Legislative Framework

[248] *Chwee Kin Keong and Others v Digilandmall.com Pte Ltd* [2004] 2 SLR 594; [2004] SGHC 71
[249] *B2C2 Ltd v Quoine Pte Ltd* [2019] SGHC(I) 03
[250] Vincent Ooi and Kian Peng Soh 'Rethinking mistake in the age of Algorithms: Quoine Pte Ltd v B2C2 Ltd' (2020) 31 *King's Law Journal* at 1.

The following provisions of ECTA pertain to the nature and circumstances under which mistakes made in the course of electronic transmissions are envisioned to occur:

Section 20(e) broadly provides that "no agreement is formed where a natural person interacts directly with the electronic agent of another person and has made a material error during the creation of a data message".[251] It circumscribes this to situations in which:

- the person was not afforded with an opportunity to avert or correct the error.[252]
- the person notified the other party of the error made "as soon as practicable" after the party gained knowledge of it.[253]
- the person has taken the necessary reasonable steps to return any performance received or destroyed any such performance if instructed to do so by the other party and has followed the instructions of the other party to return any performance received should such be instructed.[254]
- no meaningful benefit or value has been utilised by the party from any performance received from the other party.[255]

Section 25(c) states that a data message will be attributed to the programmer or user of the electronic agent unless it is "proved that the information system did not properly execute such programming".[256]

From these provisions, it can be said that the ECTA identifies two categories of errors. The first, as outlined in Section 20(e) goes to input errors.[257] The second, identified in Section 25(c), goes to errors which have occurred due to the malfunctioning of the computer program utilised and is thus deemed as a machine error.[258]

An input error goes to the instance in which a person interacting with an electronic agent in the course of contract formation accidentally enters incorrect information into the system. For example, a user may make a typographical or keystroke error regarding quantity or

[251] ECTA supra note 112 Section 20(e)
[252] Ibid Section 20(e)(i)
[253] Ibid Section 20(e)(ii)
[254] Ibid Section 20(e)(iii)
[255] Ibid Section 20(e)(iv)
[256] Ibid Section 25(c)
[257] Ibid Section 20(e)
[258] Ibid Section 25(c)

description.[259] A customer may mistakenly enter unintended information into an online form, by for example, double pressing the 'one' button and typing '11' when intending to only enter '1'. ECTA contemplates that agreements in which an input error has been made will be regarded as void ab initio where that error is material, as opposed to errors that are inconsequential in nature and having no real capacity to vitiate the contract. Where the automated transaction is deemed as void ab initio, the parties will be restored to their original position through the restoration of performance – if any has been received.[260]

Machine errors go to defects in computer software. The defect may be software-centric or system-centric. Software-centric defects are those which are caused by internal disfunction.[261] System-centric causes are software failures associated with, for example, defective or incompatible hardware, virus attacks, electrical interferences, improper use, and heavy workloads.[262] Due to any of these or a combination thereof, a computer program may malfunction in the course of use. Such a failure may take the form of performing a function that it was not instructed to, failing to execute a programmed function, or executing a programmed function incorrectly. The malfunction at issue may affect the content of a data message. Per Section 25(c) of ECTA, a data message that results from such a malfunction of an electronic agent will not be attributed to its programmer or user and they will not be bound to its outcomes or results.[263]

Importantly, the two categories of errors identified in ECTA go to circumstances in which either a natural person interacting with an electronic agent made an error when entering certain information or when the computer program being used malfunctioned and failed to perform correctly or entirely. It does not go to instances in which a) electronic agents are interacting with each other sans human interaction and b) the program's performance of the contract is in accordance with its objective programming – hence, no machine error has been made – but its execution of performance is not in line with the subjective intention of a party to the contract. The recent case of *B2C2 Ltd v Quoine Pte Ltd*[264] and the decision of its subsequent appeal in

[259] Ramokanate op cit note 166 at 244.
[260] Ibid at 249.
[261] Ibid at 269.
[262] Ibid at 269.
[263] Ibid at 270.
[264] *B2C2 Ltd* supra note 249.

Quoine Pte Ltd v B2C2 Ltd[265] may provide insight on these two issues in the context of smart contracts.

(b) *B2C2 Ltd v Quoine Pte Ltd* – Electronic Mistakes, Unilateral Mistakes and Smart Contracts

(i) The Facts

Quoine, the defendant in the matter, operated an online platform (the Platform) for the trading of cryptocurrencies such as Ethereum (ETH) and Bitcoin (BTC), in exchange for other cryptocurrencies or fiat currencies.[266] The Platform also allowed for margin trading to take place. Margin traders could enter into trades utilising borrowed funds from Quoine. These loans would be accessed in exchange for collateral held in their accounts. If the assets held as collateral in the account of the margin trader fell below a pre-set percentage of the loan, the Platform would initiate a margin call: market orders would be automatically put on the Platform to force-close out the margin trader's open positions.

B2C2, the plaintiff in this matter, was a trader and market-maker on the Platform. Market-makers place buy and sell orders on cryptocurrencies at a publicly quoted price on a consistent and continuous basis to ensure that adequate liquidity for cryptocurrencies remains on the Platform.[267] Quoine also operated as a market-maker on the Platform and its algorithmic trading software, the Quoter Program, was core to its role as such. The Quoter Program determined the prices at which Quoine was prepared to trade cryptocurrencies. The Quoter Program's capacity to acquire external market values from other cryptocurrency exchanges was essential to its ability to operate.

Quoine failed to update certain passwords and make necessary changes to the Quoter Program, resulting in its incapability to access external market prices and generate new ETH/BTC orders for market-making purposes.[268] As a result, trading on the Platform substantially decreased because Quoine was in charge of over 98 percent of the platform's market-making trades.[269] This malfunction went unnoticed as no error message was generated.

---

[265] *Quoine Pte Ltd v B2C2 Ltd* [2020] SGCA(I) 2
[266] *B2C2 Ltd* supra note 249 para 1.
[267] Ibid para 2.
[268] Ibid para 71.
[269] Ibid para 73.

Two parties, Pulsar and Tomita (the Counterparties), were operating as margin traders on the Platform, selling BTC and buying ETH.[270] The drop in trades triggered margin calls to be made on the Counterparties' positions. The Platform automatically placed market orders on the Counterparties' behalf to buy ETH at the best available market price. This was that offered by the plaintiff, who was selling ETH and buying BTC on the Platform. Several trades were concluded between the plaintiff and the Counterparties, termed 'the Disputed Trades'. The disputed ETH/BTC trades were made at a rate 250 times higher than the prevailing market rate.[271] This was due to the fact that B2C2's software was programmed to input a 'deep price' of 10 BTC to 1 ETH for sell orders in the situation in which insufficient data was available from the Platform's order book from which to generate prices.[272] As the order book on the Platform had thinned out due to Quoine's error, the 'deep price' was triggered.

(ii) The Dispute

Due to the Disputed Trades, the Counterparties' account had a negative BTC balance, and the plaintiff obtained a large windfall from the trades.[273] Upon learning of the trades, the next day Quoine cancelled the trades and reversed the transaction. B2C2 challenged this before the court and alleged that Quoine's unilateral action to reverse the trades was a breach of contract and a breach of trust.[274] Specifically, the plaintiff contended that the defendant breached the express term of their agreement that the fulfilment of an order made via the platform is "irreversible" by reversing the orders on the following day.[275]

Quoine raised six arguments in defence of their decision to reverse the Disputed Trades.[276] Of relevance to the present analysis is Quoine's third defence, that of voidability of the contract based on the doctrine of unilateral mistake at common law.[277]

[270] Ibid para 74.
[271] Ibid para 4.
[272] Ibid para 121 – 124.
[273] Ibid para 252.
[274] Ibid para 136 – 138.
[275] Ibid para 136.
[276] Ibid para 147 – 252.
[277] Ibid para 184 – 231.

(iii) The Court on Unilateral Mistake and Smart Contracts

On the matter of unilateral mistake, Thorley IJ begins by setting out the two requirements to render a contract void for unilateral mistake at common law when applying the doctrine to instances of contracting by electronic means. These requirements were confirmed in the case *Chwee Kin Keong and others v Digilandmall.com Pte Ltd,* which preceded the present matter.[278]

First, in order to prove a fundamental or sufficiently important mistake to a contract term, it must be established that the party that made the mistake did not intend for the terms of the offer to be such that they were on the face of it.[279] Secondly, the party seeking to enforce the agreement must have actual knowledge of the error that the party seeking to prevent enforcement of the agreement has made.[280] In the case of *Chwee Kin Keong*, this was a fairly easy assessment to make.[281] In that instance, the defendant had mistakenly listed Hewlett Packard commercial laser printers for the price of $66 on their website when its actual price was $3,854. The plaintiffs placed orders for 1 606 printers through the website. These orders were processed and confirmed by the automated system of the defendant. After learning the error as to the pricing, the defendant notified the plaintiffs and the 778 others who had placed orders for the printers that an mistake had been made when posting the price and that they would, as such, not be fulfilling the orders. The plaintiffs contested this and asserted that the contract be upheld, claiming that successfully concluded contracts should be upheld for the sake of commercial certainty and that the difference in posted and actual price was irrelevant; ultimately, they were entitled to a good deal. The defendant contended that the doctrine of unilateral mistake protected them in the matter. The court ultimately found on behalf of the defendant, as it was held that the plaintiffs had knowledge of the error that had been made in the price posting. This was due to the fact that it was successfully made apparent to the court that the plaintiffs had actual knowledge of the mistaken price, and here the price was considered to be a material term of the contract of purchase between the parties.

The matter of knowledge of the mistake is one which is significant to the smart contracting context. Indeed, Thorley IJ correctly differentiates *Chwee Kin Keong* from the present matter

[278] *Chwee Kin Keong* supra note 248.
[279] *B2C2* supra note 249 para 188.
[280] Ibid.
[281] *Chwee Kin Keong* supra note 248.

as in the present case, there was no human intervention in the effecting of the disputed trades as they were executed by deterministic algorithm means.[282] The learned judge goes on to draw a distinction between actual knowledge and constructive knowledge.[283] The latter refers to a situation in which the contract enforcer ought to have been aware of the contract denier's error despite not having actual knowledge of it. A further issue identified is who must have had knowledge that a mistake was made by the other party.

The learned judge was cautious when discussing these two concerns, only advancing the law as necessitated by the circumstances of the case in front of the court.[284] In keeping with the position that, in effect, computers used for online trading purposes are mere machines executing the functions that they have been programmed to do, the court held that knowledge of the mistake must have been had by the programmer who caused it to function in the way it did; thus, consideration must be given to the programmer's knowledge and intent at the time the pertinent component of it was written.[285] The error may have developed earlier but it must have existed at the time of the conclusion of the contract. Actual knowledge or constructive knowledge suffices for the nature of the knowledge held by the non-mistaken party of the mistake made by the mistaken party. When determining who made the error, it must be made by the user on whose behalf the computer program placed the order.

Hence, the knowledge of the non-mistaken party to be considered was that of the programmer who had programmed the ‘deep price’ trigger on behalf of B2C2. The mistaken party, here, was the Counterparties. The mistake in issue was the alleged mistaken belief held by the Counterparties that they were placing orders with B2C2 at prices which accurately represented the true market price or did not differ considerably to it.[286] This then raised question as to whether the programmer had knowledge as to this mistaken belief. [287]

Finding, on this issue, the court ruled that while a mistake as to a material term of the contract was made by the Counterparties, the programmer did not have knowledge as to the presence of this mistake.[288] The court found that for the programmer to have actual knowledge that other

[282] *B2C2* supra note 249 para 194.
[283] Ibid para 233.
[284] Ibid para 208.
[285] Ibid para 210.
[286] Ibid para 224.
[287] Ibid para 229.
[288] Ibid para 231.

traders believed that a trade would not be transacted at prices that deviated considerably from actual market prices, it would have been necessary for he himself to hold that belief. The programmer must have believed that trades would not be transacted at that price. However, in this instance, the programmer considered that it was unlikely, but he knew it was a possibility. Thus, the second requirement as to the application of the doctrine of unilateral mistake failed and Quoine's defence was dismissed.[289]

(b) *Quoine Pte Ltd v B2C2 Ltd*[290] - *B2C2 Ltd v Quoine Pte Ltd* Taken on Appeal

Writing for the majority in the matter taken on appeal, Menon CJ continued to consider the matter of knowledge and framed the inquiry to be undertaken as, first, whether the programmer had constructive or real knowledge that the offer would only be accepted by a party acting under erroneous belief and, secondly, whether the programmer acted to benefit from the error.[291] Where the parties to the transaction were unaware of the precise conditions on which the trading contracts would be entered into, how does the doctrine of unilateral mistake apply? The majority concurred with the court a quo's stance that any analysis as to the knowledge of a mistake must take into account the algorithm's programmer's state of mind at the time of programming. The mistake at hand was that of the counterparties' belief that they were buying ETH and BTC under contracts at prices which were fairly represented or did not materially depart from their respective fair market values. B2C2 contested this, asserting that the prices quoted and accepted for the disputed exchanges were accurate and that the software's programmer had not acted in any unconscionable manner when programming it.[292]

In determining the nature of the mistake, Menon CJ advances that the mistake made was in the way the platform functioned due to Quoine's neglect in updating the operating system as required.[293] In actuality, the deterministic algorithmic programs that were used had performed entirely as designed and programmed to.[294] Menon CJ holds, instead, that there was not an error as to the terms on which the contracts could or would be performed.[295] Instead, there was an error in the presumption upon which the buy orders were placed – an incorrect belief held

[289] Ibid para 231.
[290] *Quoine* supra note 265.
[291] Ibid para 124.
[292] Ibid para 112.
[293] Ibid para 11.
[294] Ibid para 115.
[295] Ibid para 115.

by the Counterparties regarding how the platform would function.[296] The Counterparties' true belief was that the platform would not fail; the Platform would function as intended or that there would be sufficient error identification and protection procedures to prohibit trade from continuing if the Platform's operations diverged from the expected state of affairs.[297] Thus, the mistaken belief was a mistaken assumption as to the conditions under which the trade contracts would be finalized.

Continuing on to consider nonetheless that the programmer, Mr Boonen, had actual or constructive knowledge of the mistaken belief held by the Counterparties, Menon CJ held that it was clear that he did not hold such knowledge and that he did not programme the trading software to profit from of any similar mistake as that held by the Counterparties:

> "Mr Boonen would have had to foresee a perfect storm of events that began with the problems with the Quoter Program and ended with the Disputed Trades being concluded at the deep price for him to have had, or be taken to have had, the…Mistaken Belief."[298]

Thus, Quoine's appeal on this issue was unsuccessful.

(c) B2C2 Ltd v Quoine Pte Ltd Discussed

As pointed out by Dhanoa, this matter illustrates the conflict that could develop when a function is carried out by a computer in accordance with an agreement's objective programming, but which is contrary to a party's subjective intention in a smart contract.[299] Furthermore, it illustrates the instance of absence of human interaction in the performance and execution of the contract and provides insight as to who must hold knowledge of the mistake in such an environment. In assessing this, the court has provided direction by concluding that the mistake must be in existence at the time of or prior to the time at which the trades were made; it must be made by the party for whose purpose the computer functioned; and knowledge of the mistake must be actual or constructive on the part of the programmer. Peng distinguishes the

---

[296] Ibid para 115.
[297] Ibid para 115.
[298] Ibid para 126.
[299] Harsimar Dhanoa 'Making Mistakes with Machines' (2020) 37 *Santa Clara High Technology Law Journal* at 100.

latter according to a wide and narrow approach in considering the question of how parties will gain awareness of the mistake after the contract has been entered into where such dealings have been entrusted to computers who do not have consciousness.[300] The wide approach in this case would be to take into account what the parties to the contract were likely to have known and intended if they had met in a hypothetical scenario on the "floor of the exchange" in order to engage in the contract.[301] The narrow approach, contrastingly, rejects the wide approach as artificial and argues that the proper approach to be undertaken where deterministic programming is used, is to determine what the relevant program's writer was thinking when they wrote it.[302] This is the very approach taken by the court.[303] Loke commends the court for establishing the standard for relevant knowledge on the part of the non-mistaken party given the instance where there is a time lapse between the time of the contract and the last time a human agent's mind was engaged.[304] Loke contends that the court's stance is consistent with the common law's subjective knowledge standard for unilateral mistake.[305]

However, Dhanoa, argues that the court's analysis incorrectly restricted itself is to the knowledge and intentions of the programmer, to the exclusion of B2C2 itself.[306] As is posited by Dhanoa, the inquiry should also extend to what the programmer was instructed to do by the relevant contracting party.[307]

Mistakes made in the course of contracting in the online environment is an area of law that is underdeveloped; even more so that which concerns smart contracts. The *B2C2* case illustrates the complexity of the analysis which must be undertaken in the instance in which unilateral mistake is alleged in the context of smart contracting. Nonetheless, the approach of the courts in each instance demonstrates the flexibility of conventional legal principles to the disputes arising in the online environment. Furthermore, it provides useful insight for the development of a South African approach to instances in which mistake is alleged in smart contracting. Importantly, the case demonstrates that the facts must be accurately identified and

[300] Allen Kiat Peng Sng 'Contract formation and mistake in cyberspace (again): The story so far and where to next?:'Quoine Pte Ltd v B2C2 Ltd [2020] 2 SLR 20' (2021) 33 *Singapore Academy of Law Journal* at 712.
[301] Ibid at 713.
[302] Ibid at 713.
[303] Ibid at 714.
[304] Alexander Loke 'Mistakes in algorithmic trading of cryptocurrencies' (2020) 83 *The Modern Law Review* at 1348.
[305] Ibid at 1352.
[306] Dhanoa op cit note 299 at 113.
[307] Ibid.

characterised in order for existing legal principles to apply. This may be challenging for legal scholars when considering the complex technicalities of the matter. Such may necessitate an inter-disciplinary approach to resolving disputes, in that resort may be had to technical experts.

4.2 Non-Performance and Smart Contracts

The inflexible nature of smart contracts is one of its defining features. The immutability of the blockchain prevents the parties from modifying the smart contract to extract advantages from the contract to the disadvantage of counterparties.[308] The blockchain guarantees and enables performance of the terms of the contract, thereby setting smart contracts apart from their traditional contract counterparts due to their capacity to eliminate the possibility of breach of contractual obligations. It is argued that breach is rendered impossible because performance of obligations is secured through automatic execution enabled by blockchain technology. It can be said, therefore, that the machinery of smart contracts adheres firmly to the principle of pacta sunt servanda as there is strict persistence of the primary obligation – the parties are forced to honour their original agreement.

Although smart contracts are intended to secure performance, there may be circumstances in which a party to the contract raises a valid excuse for their non-performance of contractual obligations. This section will therefore consider how smart contracts relate to the law of excuses for non-performance. Specifically, where non-performance of obligations has occurred, can smart contract accommodate existing legal rules, and can these legal rules be programmed into the smart contract itself?

In determining whether an excuse may apply, the cause of non-performance must first be identified.[309] This may be a simple enough assessment, as the cause may be part of the smart contract environment itself. For example, there may be an insufficient balance of cryptocurrency in the wallet of the debtor. In the case of non-delivery of a package, for

[308] Jeremy M. Sklaroff 'Smart Contracts and the Cost of Inflexibility' (2017) 166 *University of Pennsylvania Law Review* at 273.
[309] Eric Tjong Tjin Tai 'Challenges of Smart Contracts: Implementing Excuses' in L. DiMatteo, M. Cannarsa, & C. Poncibò (eds) *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms, Cambridge Law Handbooks* (2019) at 91.

example, detection of the cause of non-delivery may be ascertained by the courier who then performs the function of an oracle.[310]

An oracle is an entity or communication channel that provides a facility to receive input signals from the outside world. Oracles provide the blockchain with information about off-chain events.[311] This information is obtained from external data sources.[312] When the parties to a smart contract chose to utilize an oracle, they not only choose that oracle specifically but also the data source which provides it with the specific information required.[313] Thus, what is apparent is that trust in the oracle and the information which it signals to the blockchain is required.

An oracle may take the form of sensors, a connection to a website or to the Internet at large.[314] Where digital assets are concerned, an oracle may be the signal from a self-driving car that registers if it has been involved in an accident.[315] An oracle may also be connected to a human individual, which would then function as a trusted third party (TTP).[316] For example, in the scenario of a delivery of a package, the courier who signals delivery thereof is the oracle as the signal of delivery provides information for the smart contract system about the off-chain state of affairs.[317] An oracle may also offer more expert services, by assessing the quality of goods or possible damage to them, or by performing a more evaluative role in the execution of performance by providing expert evaluation – known within this realm as surveyors or conformity assessment tools.[318] Where judgement is provided on the evaluation, the oracle functions as an arbitrator or judge.[319] In the future, Artificial Intelligence or advanced algorithms may play such a role.[320] Thus, the smart contract may outsource specific judgements

[310] Ibid at 91.
[311] Eliza Mik 'Smart contracts: terminology, technical limitations and real world complexity' (2017) 9 *Law, Innovation and Technology* at 296.
[312] Ibid.
[313] Ibid.
[314] Tai op cit note 309 at 83.
[315] Ibid.
[316] Ibid.
[317] Ibid at 83 – 84.
[318] Ibid., p. 84.
[319] Ibid. Stazi also hypothesizes the inclusion of reference to a legal oracle in the smart contract code; an oracle who would externally verify the content of the smart code and/or its performances according to any law or regulation which may find possible application. This verification would take place before automatic execution so as to invalidate the need for subsequent termination or cancellation of the contract and any complexities that may arise therewith. See Stazi op cit note 182 at 138.
[320] Ibid.

that may difficult or impossible to program into its code and ultimately add to its process of fairness.

As in the courier example, non-delivery may be the cause of non-performance. Tai postulates that different causes may be relevant to a smart contract depending on the nature of the smart contract involved, as a contract of sale, for example, is different to a credit contract.[321] Best practices may develop on this issue over time.

Non-accountability for non-performance is generally assumed in situations of overpowering circumstances and are commonly termed force majeure. A force majeure clause may stipulate which impediments may be considered as a valid excuse. These clauses are useful in practice as parties may agree beforehand on contractual risks to be undertaken in the event of non-performance.[322] In the case of smart contracts, a general exception of force majeure – if invoked by the debtor – may require the calling of an expert oracle, which may be an outside expert or adjudicator and going through online dispute resolution – an alternative dispute resolution.[323] However, this route goes against the automatic and final execution that smart contracts afford and may be a disadvantage to the parties.[324]

For causes that fall outside of the force majeure clause, it may be an accepted position that the assumption of risk for such causes fall on the part of the debtor. Nonetheless, complications still arise. In determining the relevant cause, complex legal analysis may be required in order to determine the relevant causes that constitute excuse. Furthermore, notification of non-performance which may take place where a party has failed to perform is difficult to do in the smart contracting context as it is difficult to communicate between parties to discuss the cause of non-performance in a predictable rule-based manner as through smart contracts.[325] Therefore, in so far as smart contracts are concerned, force majeure clauses may either have default rules that circumscribes a list of circumstances that can be determined as force majeure where causality is presumed, or it may refer more generally to the use of an expert oracle.[326] If

[321] Ibid at 92.
[322] Ibid at 86.
[323] Ibid at 92.
[324] Ibid.
[325] Ibid at 93.
[326] Ibid at 94.

invoked, force majeure may be considered as an excuse and the contract may be terminated. If, however, it is invoked unsuccessfully, a remedy for non-performance may be awarded.

Impossibility and illegality as excuses may also pertain to smart contract and excuses for non-performance. Impossibility may be analysed similarly to force majeure; however, it goes to a specific kind of impediment – a cause that forms an impediment that cannot be overcome.[327] An impossibility may require resort to an expert oracle.[328]

Assessing illegality may entail a complex analysis.[329] Regard to the regulatory environment must be had. This may include an analysis that crosses the jurisdictional bounds of regulatory concerns around cryptocurrencies, digital assets, and blockchain governance.[330] As has been outlined in chapter three of this discussion, one of the elements of a valid contract is legality. In general, an illegal contract is either considered as void and unenforceable or valid but unenforceable dependent on the extent to which the public deems the contract unacceptable.[331] Under South African law, regard is to be had to the common law and statute in order to determine whether the enforcement of the contract would be contrary to the public interest or statutory provisions.[332] The unenforceability of contracts which are inimical to public policy finds confirmation in the seminal case of *Sasfin (Pty) Ltd v Beukus*[333] where the court held that:

> "The interests of the community or the public are therefore of paramount importance in relation to the concept of public policy. Agreements which are clearly inimical to the interests of the community, whether they are contrary to law or morality, or run counter to social or economic expedience, will accordingly, on the grounds of public policy, not be enforced."[334]

Public prohibition may require expert legal analysis and not mere resort to a factual determination of causes. Regard may have to be had, again, to an expert oracle in these circumstances.[335]

---

[327] Ibid.
[328] Ibid at 94 – 95.
[329] Ibid at 95.
[330] Ibid.
[331] Tomas Floyd 'Legality' in Dale Hutchison and Chris-James Pretorius (eds) *The law of contract in South Africa* 2 ed (2017) at 175-176.
[332] Ibid at176.
[333] *Sasfin (Pty) Ltd v Beukus* 1989 1 All SA 347 (A) para 9.
[334] Ibid.
[335] Tai op cit note 309 at 95.

Another concern is that of breach by the other party and anticipatory breach.[336] As has been discussed above, a major advantage of smart contracts is the certainty of performance which they are able to provide. Yet there may be instances in which performance by the other party is due and the party has breached their obligation by not performing, or there is a reasonable expectation that the other party is not going to perform – thereby, the occurrence of anticipatory breach. It may then be well-suited for a smart contract to automatically determine when it should not perform when the counter-performance is lacking.[337] This may require pre-programming the situations under which performance may proceed and when it should be withheld.[338] Ultimately, it is the philosophy of smart contracts to accept that it is incumbent upon the parties to ensure that the conditions of the contract are sufficiently well-elaborated to match the intentions of the parties.[339]

4.3 Remedies for Breach and Smart Contracts

Poncibò and DiMatteo advance that the self-enforcing capabilities of smart contracts do not prevent such self-enforcement from being subjected to post hoc judicial review.[340] This may be in the instance in which self-enforcement may be characterised as a breach of contract due to performance of obligations not being as expected or as intended by the parties.[341] For example, negligent coding or updating of smart contracts could lead to actions on the basis of misrepresentation or fraud.[342] Ex contractu legal remedies may arise in circumstances in which such self-enforcement may be deemed as breach. This demonstrates the prevailing ex post perspective of contract law in its highlighting of the continuing significance of contract law remedies.

---

[336] Ibid at 96.
[337] Ibid at 97.
[338] Ibid.
[339] Ibid.
[340] C Poncibò & L DiMatteo 'Smart Contracts: Contractual and Noncontractual Remedies' in L. DiMatteo, M. Cannarsa, & C. Poncibò (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, *Cambridge Law Handbooks* (2019) at 121.
[341] Ibid.
[342] Ibid.

Indeed, smart contracts fulfil the need for self-help in the contracting context, as they provide a remedy for non-performance by making enforcement of the contractual terms unavoidable.[343] Furthermore, smart contracts fulfil the usage of contract law as a commitment mechanism as the parties assume voluntary liability for future non-performance.[344] Smart contracts facilitate reliance on the contract through the ability to opt into foreseeable future results.[345] Smart contracts do not, however, remedy grievances in the manner that traditional contract law principles intend to do.[346]

Considering circumstances in which the grievances of complaining parties amounts to breach of the smart contract, the authors Werbach and Cornell argue that claims for restitution will become more prevalent:

> "an action for restitution is very different than an action for breach of contract. At a minimum, the roles of the parties are reversed. In an action for breach, the nonperforming party seeks to enforce a transaction; whereas, in an action for restitution, the performing party seeks to reverse the transaction."[347]

Reflecting on the above with reference to South African law of contract, a party claiming restitution does so on the basis of cancellation of the contract.[348] Where breach of a contract has occurred, the innocent party may elect to cancel the contract but will only be entitled to do so in exceptional circumstances – the breach must be material or sufficiently serious so as to warrant termination of the contract.[349] Materiality is determined with reference to the circumstances of the matter and the nature of the breach at hand.[350] Cancellation impacts the legal consequences of a contract; in that it extinguishes or undoes the obligations that arise from it.[351] Where contractual obligations have not yet been fulfilled or performed, cancellation renders the obligations unenforceable.[352] If obligations have been discharged, there is a duty

[343] Kevin Werbach and Nicolas Cornell 'Contracts ex machina' (2017) 67 *Duke Law Journal* at 346.
[344] Ibid at 360.
[345] Ibid at 360.
[346] Ibid at 363.
[347] Ibid at 376.
[348] Van Huyssteen et al op cit note 193 at 441.
[349] Sieg Eiselen 'Remedies for Breach' in Dale Hutchison and Chris-James Pretorius (eds) *The law of contract in South Africa* 2 ed (2017) at 324-325.
[350] Ibid.
[351] L. F. Van Huyssteen *Contract: General Principles* 6 ed (2020) at 453.
[352] Ibid at 453-454.

on the parties to restore performances received, per restitution.[353] Hence, with reference to the argument presented by Werbach and Cornell, in so far as South African law is concerned, restitution cannot be treated as being wholly separate from an action for breach of contract. This is so as the party seeking restitution and rescission of the contract must necessarily rely on cancellation thereof, and this in turn relies on the existence of sufficient breach. What can rather be said that for present purposes, an action for unjustified enrichment is different from an action for breach of contract. An enrichment claim will be awarded where the contract is void ab initio, whereas breach of a contract requires the contract itself to have a valid foundation.[354]

Considering this in application to smart contracts, for the smart contract to be cancelled and restitution awarded, its breach must be sufficiently material. It is of the view of this author that the smart contract should adopt a lex commissoria, or cancellation clause, that would serve the purpose of outlining the specific instances of breach that would allow a party to cancel the contract. If the smart contract is void, an enrichment claim may be awarded. This may pose a challenge to our understanding of a void contract, as although the smart contract may be deemed void and of no legal effect, it will still exist on the blockchain. A subsequent transaction would need to take place in order to effect an enrichment claim.

Turning to the remedy of specific performance, such may likely only be obtained through a court order.[355] For example, a smart contract effects the transfer of an asset; however, the sale is later invalidated due to fraud or incapacity or illegality and so on.[356] On the blockchain, the asset remains as reflected – it is the property of the transferee; however, in reality, the law takes the position that the title to the property is still held by the transferor.[357] The only way to remedy this diverged ownership dilemma is for the court to order specific performance compelling the transferee to reconvey ownership of the asset through the blockchain.[358]

---

[353] Ibid at 454.
[354] See *Kudu Granite Operations (Pty) Ltd v. Caterna Ltd* 2003 5 SA 193 (SCA) para 15 for justification for this argument.
[355] Poncibò & DiMatteo op cit note 340 at 121.
[356] Ibid.
[357] Ibid.
[358] Ibid.

Eyup notes, however, that the insistence of specific performance of a contractual obligation may be practically and economically inefficient where smart contracts are utilised.[359] Eyup proposes that smart contract developers structure the smart contract so as to allow for incorporation of liquidated damages as a form of compensation.[360] A liquidated damages clause may be coded into the smart contract in a structure which would allow for the parties to choose between the payment of liquidated damages and specific performance.[361] A trigger may be inserted into the smart contract code and an oracle could feed data into the smart contract to determine whether a condition has been fulfilled which may allow for the payment of liquidated damages or the choice between such damages and specific performance to fulfil the obligation.[362] Such a discretion would introduce flexibility into the otherwise inflexible nature of smart contracts in so far as breach is concerned.

The inflexibility of smart contracts deprives parties from being able to adjust in response to changed circumstances. This was revealed in the 2016 hack of the Decentralized Autonomous Organisation (DAO).[363] The DAO was a crowdfunding vehicle that operated on Ethereum and was developed with the aim to conduct corporate governance and operations automatically through smart contracts.[364] Users of the DAO contributed Ethereum (the cryptocurrency used by Ethereum) in exchange for voting tokens that allowed them to choose which projects to fund. Organizations seeking funding would sign up through a different interface and obtain Ether if they received adequate user votes. The DAO raised over $150 million worth of Ether over the course of the few weeks after its launch.[365] The smart contract on the Ethereum blockchain operated as the controlling legal authority of the DAO. Within a few weeks, a hacker was able to exploit a flaw in the code of the smart contract and extract more than $50 million worth of Ether from the DAO.[366] The hack was effected through a sequence of smart contracts that were technically acceptable according to the rules of the DAO; thus, while clearly an attempt at theft, the transactions were technically legitimate within the logic of the smart contract system. Therefore, were a court to order the stolen funds restored, no one could implement that order, nor was there a technical mechanism to recover the funds without

[359] K. U. N Eyup 'Is Insisting on Specific Performance under Smart Contracts Desirable? Inflexibilities of Smart Contracts and Potential Solutions' (2021) 3 *Bilişim Hukuku Dergisi* at 139.
[360] Ibid at 167.
[361] Ibid.
[362] Ibid.
[363] Werbach & Cornell op cit note 343 at 350.
[364] Ibid at 350-351.
[365] Ibid 351.
[366] Ibid.

jeopardising the integrity of the system. The Ethereum Foundation took the decision to intervene on the behalf of the DAO investors and ultimately convinced most of the users to follow with its decision. A 'hard fork' in the Ethereum protocol was created that split the Ethereum blockchain into two incompatible parts, thereby killing off the DAO and allowing for the stolen tokens to be restored and the diverted funds returned.[367]

The DAO hack and the remedy employed by the Ethereum Foundation is an extreme example of alternative technical solutions that need to be applied due to the inflexible nature of smart contracts. Another technical solution discussed by Stazi is the self-destruction function of the smart contract.[368] This function allows for the contracting parties to eliminate the contract.[369] Smart contracts written in the programming language of Solidity on the Ethereum Blockchain are capable of this function, which effectively eradicates the smart contract code from the Blockchain.[370] Such a remedy could be deemed as excessive in specific circumstances, but may be necessary where, for example, an illegal obligation is set to be self-executed yet the code of the smart contract does not include a withdrawal or cancellation mechanism.[371] This presents the need to develop "techno-legal solutions", as termed and explained by Stazi as being "solutions which are… based on technological approaches and…[which]… allow compliance with the contractual regulation" and any remedies which may find application.[372] This position highlights the prevailing need for contract law principles to police smart contract clauses, as they remain subject to doctrines around cancellation, mistake, fraud, and so on.

[367] Ibid.
[368] Stazi op cit note 182 at 133.
[369] Ibid.
[370] Ibid at 75.
[371] Ibid at 133.
[372] Ibid at 146.

V. CONCLUSION

The objective of this dissertation was to determine the extent to which modern South African contract law is able to facilitate the recognition and enforcement of smart contracts. The approach undertaken to address this objective was one of a doctrinal research methodology which employed the use of primary sources and secondary sources in order to produce a finding. In answering the primary research question, the research anticipated the possibility of the existence of lacunae and conflict in the application of existing legal principles to smart contracts. The purpose of this chapter is to provide a summary of the findings on this matter and to postulate possible recommendations where such may find applicability.

5.1 Findings and Recommendations

Chapter two of this research provided a general understanding of what a smart contract is, how it functions, and the primary characteristics which distinguish it from traditional contracts. While highlighting that a plethora of definitions for smart contracts have been supplied by numerous authors, it nonetheless sought to provide a coherent understanding of smart contracts and their structure. This was achieved and a preliminary definition for a smart contract was supplied: *a smart contract is an agreement between two or more parties that is coded according to predefined parameters, and which will execute on a subject matter when triggered by the processing of events and/or data on the blockchain database.*

Having collated a baseline definition and understanding of smart contracts, chapter three progressed to the deliberation of whether traditional contract law principles allow for the legal recognition contracts formed and concluded via smart contracts. In answering this, regard was had to the common law rules around contractual validity as well as statutory requirements for electronic transactions. The ECTA found applicability here. It was found that for that for the ECTA to apply to smart contracts, and thus validate transactions concluded by means of smart contracts, smart contracts would have to meet the definition of an electronic agent under the ECTA. The chapter finds that a broad reading of the ECTA would allow for such application; however, the ECTA does not speak to the range of autonomous capacity which software is capable of holding – a key facet of smart contracts. It is herewith submitted that the ECTA be revised to include such reference so as to allow for smart contracts to be governed under it. Such revision could be comparable to the approaches taken by external jurisdictions, as

discussed subsection 3.4. This author is careful to note that where such revision is sought to take place, there must be a great regard to specificity around the description, nature, and functions of smart contracts so as to provide greater legal certainty. This chapter also considered specific matters relating to smart contract formation and provided several recommendations for revision and interpretation of the ECTA. First, it was posited that the terms 'originator' and 'addressee' be interpreted or revised so as to include reference to an electronic agent and not solely a human user. This would allow for the gap between Section 20 and Section 23 read with Section 26 to be bridged and for it to be abundantly clear and certain that an electronic agent, and hence a smart contract, may validly transmit data messages conveying acceptance of the contract, and thus conclude it. Secondly, the chapter posited that where statute or the common law necessitates those specific contracts be signed in wet ink, the parties to the smart contract should have an off-chain contract that allows for the parties to affix their signatures in the required manner. Although this may hinder the efficiency of the smart contract, it will nonetheless bring about legal validity and certainty in the smart contracting process. Ultimately, this chapter found that conventional legal principles around offer and acceptance, capacity, certainty of terms and certainty of object will continue to facilitate smart contracts and find application thereto.

Chapter four considered the application of traditional legal principles to instances of mistake, non-performance, and remedies for breach. First, on the issue of mistake, regard was had to the Singaporean court and its recent rulings on mistakes made in the context of the smart contract. The discussion found that although the law around mistakes made in the online environment is underdeveloped, the decisions arising from the court are nonetheless useful for South African legal purposes as it provides a formulation for the test for who must hold knowledge of the mistake and when the relevant mistake must have been made. This is significant for our understanding of mistake and smart contracts, as it addresses the instance in which there was a gap between the time of the contract and the last occasion a human actor's mind was engaged with its formation, conclusion, and performance. It provides that mistake must be made by the user on whose behalf the smart contract acted, the mistake must have been in existence at the time of conclusion of the contract or sometime before, and the non-mistaken party must have had actual or constructive knowledge of the mistake of the mistaken party. Secondly, non-performance and excuses for non-performance was discussed, along with the role of oracles in determining the existence of excuses. It was found that excuses may be programmed into the smart contract; thus, allowing for the continued application of traditional legal principles.

Lastly, the chapter considered possible remedies for breach. It was found that, ultimately, techno-legal solutions need to be developed and applied, as traditional understandings of rescission, restitution, and unjustified enrichment where the contract is void ab initio may be difficult to program into the code of the smart contract.

In summation, and remaining mindful of the complexities of the discussion, it can be said that South African contract law is able to facilitate valid recognition of smart contracts to a partial extent. The foundation for such facilitation exists; however, as has been outlined, statute ought to be revised or interpreted in such a way as to facilitate such application. Furthermore, our conventional understanding of remedies is, indeed, challenged by the employment of techno-logical solutions. Nevertheless, the employment thereof would allow for traditional legal principles to persist in conjunction with more technical solutions that suit the smart contract environment.

Bibliography

Primary Sources

Statutes

South African:
Alienation of Land Act 68 of 1981.
Copyright Act 98 of 1978.
Electronic Communications and Transactions Act 25 of 2002.

Foreign/International:
2017 Ariz. HB 2417 44-7061.
2018 Tenn. SB 1662 47-10-201.
205 ILCS 730, Blockchain Technology Act.
Decree of the President of the Republic of Belarus No. 8 (21 December 2017), unofficial translation.
UNCITRAL Model Law of Electronic Commerce with Guide to Enactment, 1996.

Cases

South African:
Borcherds and Another v Duxbury and Others (1522/2020) [2020] ZAECPEHC 37.
Jafta v Ezemvelo KZN Wildlife [2008] 10 BLLR 954 (LC).
Kudu Granite Operations (Pty) Ltd v Caterna Ltd 2003 5 SA 193 (SCA).
Sasfin (Pty) Ltd v Beukus 1989 1 All SA 347 (A).
Sonap Petroleum (South Africa) (Pty) Ltd v Pappadogianis 1992 (3) SA 234 (AD).
South African Railways and Harbours v National Bank of South Africa Ltd 1924 AD 704.

Foreign:
B2C2 Ltd v Quoine Pte Ltd [2019] SGHC(I) 03.
Chwee Kin Keong and others v Digilandmall.com Pte Ltd [2005] 1 SLR(R) 502.
Quoine Pte Ltd v B2C2 Ltd [2020] SGCA(I) 2.
Thornton v Shoe Lane Parking [1971] 1 All ER.

Secondary Sources

Abdellatif, Niels-Philip 'An Ethereum bill of lading under the UNCITRAL MLETR' (2020) 27:2 *Maastricht journal of European and comparative law* 250-274.

Bellia, Anthony J 'Contracting with Electronic Agents' (2001) 50:4 *Emory Law Journal* 1047-1092.

Carron, Blaise and Valentin Botteron 'How smart can a contract be?' in Kraus Daniel, Obrist Thierry, Hari Olivier (eds) *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law* (2018) Edward Elgar Publishing, Neuchâtel 101-143.

Chopra, Samir & Laurence White 'Artificial agents and the contracting problem: A solution via an agency analysis' (2009) *U. Ill. JL Tech. & Pol'y* 363-404.

Corrales, Marcelo, Mark Fenwick & Helena Haapio 'Digital technologies, legal design and the future of the legal profession' 2019 *Legal Tech, Smart Contracts and Blockchain. Springer* 1-15.

Crosby, Michael, Pradan Pattanayak, Sanjeev Verma, & Vignesh Kalyanaraman 'Blockchain technology: Beyond bitcoin' (2016) 2:6-10 *Applied Innovation Review* 6-19.

Dhanoa, Harsimar 'Making Mistakes with Machines' (2020) 37 *Santa Clara High Technology Law Journal* 97 – 118.

Dolgui, Alexandre, Dmitry Ivanov, Semyon Potryasaev, Boris Sokolov, Marina Ivanova & Frank Werner 'Blockchain-oriented dynamic modelling of smart contract design and execution in the supply chain' (2020) 58:7 *International Journal of Production Research* 2184-2199.

Durovic, Mateja and André Janssen 'Formation of Smart Contracts under Contract Law' in L. DiMatteo, M. Cannarsa, & C. Poncibò (eds) *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (2019) Cambridge University Press 61-79.

Eyup, K. U. N 'Is Insisting on Specific Performance under Smart Contracts Desirable? Inflexibilities of Smart Contracts and Potential Solutions' (2021) 3:1 *Bilişim Hukuku Dergisi* 139-175.

Gideon Greenspan 'Beware of the Impossible Smart Contract' available at *https://www.multichain.com/blog/2016/04/beware-impossible-smart-contract/*, accessed on 20 March 2021.

Gilcrest, Jack & Arthur Carvalho 'Smart contracts: Legal considerations' 2018 *IEEE International Conference on Big Data (Big Data)* 1-5.

Goode, Roy, Herbert Kronke, and Ewan McKendrick 'Bills of Lading' in *Transnational commercial law: text, cases, and materials* (2015) Oxford University Press

Grandinetti, Roberto, Maria Vincenza Ciasullo, Marco Paiol & Francesco Schiavone 'Fourth industrial revolution, digital servitization and relationship quality in Italian B2B manufacturing firms. An exploratory study' 2020 *The TQM Journal* 647-670.

Hatzopoulos, Vassilis a& Sofia Roma 'Caring for sharing? The collaborative economy under EU law' (2017) 54:1 *Common Market Law Review* 81-128.

Hawthorne, Luanda and Dale Hutchison 'Offer and Acceptance' in Dale Hutchison and Chris-James Pretorius (eds) *The law of contract in South Africa* 2 ed (2017) Oxford University Press Southern Africa, South Africa 45-49.

Howells, Geraint 'Protecting consumer protection values in the fourth industrial revolution' (2020) 43:1 *Journal of Consumer Policy* 145-175.

Hsiao, Jerry 'Smart Contract on the Blockchain-Paradigm Shift for Contract Law' (2017) 14:10 *US-China Law Review* 685-694.

Hutchison, Dale 'The Nature and Basis of Contract' in Dale Hutchison and Chris-James Pretorius (eds) *The law of contract in South Africa* 2 ed (2017) Oxford University Press Southern Africa, South Africa 3-41.

Jaccard, Gabriel Olivier Benjamin 'Smart Contracts and the Role of Law' (2017) 23 *Jusletter IT* 1-25.

UNIDROIT 'UNCITRAL/UNIDROIT Workshop on Smart Contracts, Artificial Intelligence and Distributed Ledger Technology – Summary Of Conclusions Published, Joint UNCITRAL/UNIDROIT Workshop – Summary Report' 2019 available at https://www.unidroit.org/uncitral-unidroit-workshop-on-smart-contracts-artificial-intelligence-and-distributed-ledger-technology-summary-of-conclusions-published/ accessed on 11 July 2021.

Kumar, Bhabendu, Soumyashree S. Panda Mohanta & Debasish Jena 'An overview of smart contract and use cases in blockchain technology' 2018 *9th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE* 1-4.

Kuschke, Birgit 'Contractual Capacity' in Dale Hutchison and Chris-James Pretorius (eds) *The law of contract in South Africa* 2 ed (2017) Oxford University Press Southern Africa, South Africa 149-157.

Loke, Alexander 'Mistakes in algorithmic trading of cryptocurrencies' (2020) 83:6 *The Modern Law Review* 1343-1353.

Madir, Jelena 'Smart Contracts:(How) Do They Fit Under Existing Legal Frameworks?' 2018 Available at SSRN 3301463 1-18.

Raskin, Max 'The law and legality of smart contracts' 2017 *Geo. L. Tech. Rev. 1* 305-341.

Maxwell, Catherine 'Obligations and Terms' in Dale Hutchison and Chris-James Pretorius (eds) *The law of contract in South Africa* 2 ed (2017) Oxford University Press Southern Africa, South Africa 233-254.

McLean, Sue & Simon Deane-Johns 'Demystifying Blockchain and distributed ledger technology–hype or hero' (2016) 17:4 *Computer Law Review International* 1-8.

Mik, Eliza 'Smart contracts: terminology, technical limitations and real world complexity' (2017) 9:2 *Law, Innovation and Technology* 269-300.

Moses, Lyria Bennett 'Recurring Dilemmas: The Law's Race to Keep up with Technological Change' (2007) 2 *University of Illinois Journal of Law, Technology & Policy* 239-285.

Nair, Greeshma & Shoney Sebastian 'Blockchain technology; centralised ledger to distributed ledger' (2017) 4 *International Research Journal of Engineering and Technology (IRJET)* 2823-2827.

Ooi, Vincent and Kian Peng Soh 'Rethinking mistake in the age of Algorithms: Quoine Pte Ltd v B2C2 Ltd.' (2020) 31:3 *King's Law Journal* 367-372.

Pereira, José Carlos 'The genesis of the revolution in Contract Law: Smart Legal Contracts' (2019) *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance* 374-377.

Pistorius, Tana 'Nobody Knows You're a Dog: The Attribution of Data Messages' (2002) 14:4 *South African Mercantile Law Journal* 737-747.

Pistorius, Tana 'The Legal Effect of Input Errors in Automated Transactions: The South African Matrix' (2008) 2 *Journal of Information, Law & Technology (JILT)* 1-21.

Poncibò, C., & DiMatteo, L 'Smart Contracts: Contractual and Noncontractual Remedies' in L. DiMatteo, M. Cannarsa, & C. Poncibò (eds) *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, *Cambridge Law Handbooks* (2019) Cambridge University Press 118-140

Prisecaru, Petre 'Challenges of the fourth industrial revolution' (2016) 8:1 *Knowledge Horizons. Economics* 57-62.

Ramokanate, L. L. *Modifying contract law principles to accommodate automated transactions in South Africa* (Unpublished Doctoral dissertation, North-West University, 2018), 1-566.

Riccardo de Caria 'The Legal Meaning of Smart Contracts' (2019) 6 *European Review of Private Law* 731-752.

Rohr, Jonathan G 'Smart Contracts and Traditional Contract Law, or: The Law of the Vending Machine' (2019) 67 *CLEV. St. L. REV.* 71-92.

Savelyev, Alexander 'Contract law 2.0:'Smart'contracts as the beginning of the end of classic contract law' (2017) 26:2 *Information & communications technology law* 116-134.

Sieg Eiselen 'Remedies for Breach' in Dale Hutchison and Chris-James Pretorius (eds) *The law of contract in South Africa* 2 ed (2017) Oxford University Press Southern Africa, South Africa 309-350.

Sklaroff, Jeremy M 'Smart Contracts and the Cost of Inflexibility' (2017) 166:1 *University of Pennsylvania Law Review* 263 – 303.

Sng, Allen Kiat Peng 'Contract formation and mistake in cyberspace (again): The story so far and where to next?: Quoine Pte Ltd v B2C2 Ltd [2020] 2 SLR 20' (2021) 33:2 *Singapore Academy of Law Journal* 692-723.

Stazi, Andrea *Smart Contracts and Comparative Law: A Western Perspective* (2021) Springer Nature vii-146.

Szabo, Nick 'Formalizing and Securing Relationships on Public Networks' available at https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/formalize.html , accessed on 5 January 2021.

Szabo, Nick 'Smart Contracts: Building Blocks for Digital Markets' available at https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html, accessed on 30 June 2020.

Szabo, Nick 'The Idea of Smart Contracts' available at https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_idea.html accessed on 5 January 2021.

Szczerbowski, Jakub J 'Place of Smart Contracts in Civil Law. A Few Comments on Form and Interpretation' 2017 *Proceedings of the 12th Annual International Scientific Conference New Trends* 333-338.

Tai, Eric Tjong Tjin'Challenges of Smart Contracts: Implementing Excuses' in L. DiMatteo, M. Cannarsa, & C. Poncibò (eds) *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms, Cambridge Law Handbooks* (2019) Cambridge University Press 80-101

Thakker, Urvish, Ruhi Patel, Sudeep Tanwar, Neeraj Kumar & Houbing Song 'Blockchain for diamond industry: opportunities and challenges' 2020 *IEEE Internet of Things Journal* 2-29.

Todd, Paul 'Electronic bills of lading, blockchains and smart contracts' (2019) 27:4 *International journal of law and information technology* 339-371.

Tomas Floyd 'Legality' in Dale Hutchison and Chris-James Pretorius (eds) *The law of contract in South Africa* 2 ed (2017) Oxford University Press Southern Africa, South Africa 175-203.

Twigg-Flesner, Christian 'Disruptive Technology-Disrupted Law? How the Digital Revolution Affects (Contract) Law' in A. De Franceschi (ed) *European Contract Law and the Digital Single Market: The Implications of the Digital Revolution* (2016) 21-48.

United Kingdom Jurisdictional Taskforce, 'Legal Statement on Cryptoassets and Smart Contracts' 2019 The Lawtech Delivery Panel.

Van Huyssteen, L. F *Contract: General Principles* 6 ed (2020) Juta & Company Pty Limited, Cape Town.

Van Huyssteen, LF, GF Lubbe, and MFB *Reinecke Contract: General Principles* 5e 5 ed (2016) Juta and Company (Pty) Ltd, Cape Town

Wang, Shangping, Dongyi Li, Yaling Zhang & Juanjuan Chen 'Smart contract-based product traceability system in the supply chain scenario' (2019) 7 *IEEE Access* 115122-115133.

Weitzenboeck, Emily M 'Electronic agents and the formation of contracts' (2001) 9:3 *International Journal of Law and Information Technology* 204-234.

Werbach, Kevin and Nicolas Cornell 'Contracts ex machina' (2017) 67:2 *Duke Law Journal* 313 - 382.

Wüst, Karl and Arthur Gervais ‘Do you need a blockchain?’ 2018 *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* 45-54.