Intellectual Discourse

Volume 31 Number 2 2023

Intellectual Discourse

Intellectual Discourse is a highly respected, academic refereed journal of the International Islamic University Malaysia (IIUM). It is published twice a year by the IIUM Press, IIUM, and contains reflections, articles, research notes and review articles representing the disciplines, methods and viewpoints of the Muslim world.

Intellectual Discourse is abstracted in *SCOPUS, ProQuest, International Political Science Abstracts, Peace Research Abstracts Journal, Muslim World Book Review, Bibliography of Asian Studies, Index Islamicus, Religious and Theological Abstracts, ATLA Religion Database, MyCite, ISC* and *EBSCO*.

Intellectual Discourse
Vol. 31, No. 2, 2023

Contents

Review Article

Transliteration Table: Consonants

Arabic	Roman		Arabic	Roman
ب	b		ط	ṭ
ت	t		ظ	ẓ
ث	th		ع	ʿ
ج	j		غ	gh
ح	ḥ		ف	f
خ	kh		ق	q
د	d		ك	k
ذ	dh		ل	l
ر	r		م	m
ز	z		ن	n
س	s		ه	h
ش	sh		و	w
ص	ṣ		ء	ʾ
ض	ḍ		ي	y

Transliteration Table: Vowels and Diphthongs

Arabic	Roman		Arabic	Roman
◌َ	a		◌َا، ◌َى	an
◌ُ	u		◌ُّو	un
◌ِ	i		◌ِّي	in
◌َا، ◌َ، ◌َى،	ā		◌َوْ	aw
◌ُّو	ū		◌َيْ	ay
◌ِّي	ī		◌ُّوّ	uww, ū (in final position)
			◌ِّيّ	iyy, ī (in final position)

Source: ROTAS Transliteration Kit: http://rotas.iium.edu.my

Legitimacy of Smart Contracts Written in Encrypted Code on Blockchain Technology Under Current Contract Law: A Comparative Study

Ghassan Adhab Atiyah*
Nazura Abdul Manap**
Saidatul Nadia Abd Aziz***

Abstract: Using smart contracts as a new technology for online contracting has become the best option today when working in non-trustworthy environments to execute automated irreversible agreements. However, such contracts have issues relating to the language used for expressing the obligations of the involved parties. Additionally, smart contracts have no legal recognition of blockchain as a means of record-keeping for smart contract transactions. Parties engaged in smart contracts face difficulties in terms of incompatibilities with current legal frameworks. The objective of this article is to evaluate the legality of smart contract language and the validity of blockchain as an electronic medium from the perspectives of current laws. This article adopts a qualitative doctrinal legal research approach. The findings indicate that there is a need to enact laws that recognise the language used for smart contracts and the transactions recorded on the blockchain.

* Ph.D. Candidate, Faculty of Law, Universiti Kebangsaan Malaysia (UKM). Email: ghassanadhab@gmail.com. *Corresponding author.*
** Associate Professor of Law, Accredited Mediator (Malaysian Bar Council), Department of Intellectual Property Law, Computer Law, Information Technology Law and Cyber Law, Faculty
of Law, Universiti Kebangsaan Malaysia Malaysia (UKM). Email: nazura@ukm.edu.my
*** Senior Lecturer, Faculty of Law, Universiti Kebangsaan Malaysia (UKM). Email: nadia_aziz@ukm.edu.my

Abstrak: Menggunakan kontrak pintar sebagai teknologi baharu untuk kontrak dalam talian telah menjadi pilihan terbaik hari ini apabila bekerja dalam persekitaran yang tidak boleh dipercayai untuk melaksanakan perjanjian tidak boleh ditarikbalik dan automatik. Walau bagaimanapun, kontrak sedemikian mempunyai isu yang berkaitan dengan penggunaan bahasa bagi menetapkan tanggung jawab pihak yang terlibat. Selain itu, kontrak pintar tidak mempunyai pengiktirafan undang-undang terhadap blockchain sebagai cara penyimpanan rekod untuk transaksi kontrak pintar. Pihak yang terlibat dalam kontrak pintar menghadapi kesukaran dalam menyesuaikan transaksi tersebut dengan kerangka undang-undang semasa. Objektif artikel ini adalah untuk menilai keesahan bahasa kontrak pintar dan blockchain sebagai medium elektronik dari perspektif undang-undang semasa. Artikel ini menggunakan pendekatan penyelidikan undang-undang doktrin kualitatif. Penemuan menunjukkan bahawa terdapat keperluan untuk menggubal undang-undang yang mengiktiraf bahasa yang digunakan untuk kontrak pintar dan urus niaga yang direkodkan dalam blockchain.

Kata kunci: Kontrak pintar, kontrak tradisional, bahasa komputer, blockchain, kod

Introduction

The formality of writing contracts is one of the topics that is of great importance in legal studies. It is important to the extent that researchers have described it as the fourth essential element to the contract, and the formality of writing in smart contracts should be the same as in traditional or other electronic contracts. (Abd, 2015)Written contracts require an 'official formality' which means that the parties must commit to them through mutual consent. This consent takes a certain formality in some kinds of contracts in addition to the key elements of the contracts. The purpose of a written contract is to protect the parties of the contract and alert them to the seriousness of the legal behaviour they provide by showing the parties the possible consequences of their actions. This is meant to protect them by concluding the contract, certifying it as proof of existing rights and reliable evidence in case of any dispute arising between them in the future.

The required formality of a written contract is intended here to be the formality to conclude or the formality required as proof that a contract follows certain procedures, such as registering contracts for

selling real estate in the Department of Real Estate Registration. (Hsyn, 2016) Faced with this legal situation, the difficult challenge for Iraqi legislators lies in the difficulty of issuing laws stimulating innovation and at the same time safeguarding consumer welfare as well as meeting their requirements. This article hopes to solve these challenges by compiling a large body of disparate literatures relating to smart contract regulation in selected jurisdictions. Thus, the researcher first examines the issue of whether writing smart contracts using encrypted codes can be valid for contracting and then analyses how blockchain technology could potentially revolutionise the rules of evidence for smart contracts, where the application of it in electronic evidence may also indicate the difficulty of the fusion between decentralised technology and traditional, centralised juridical mechanisms. (Wu & Zheng, 2020).

Smart Contracts and Blockchain

The idea of smart contracts was invented for the first time when proposed by the American legal scholar, computer programmer, and cryptographer, Nick Szabo (Rohr, 2019) in the mid-1990s. Smart contracts are defined as automatic electronic instructions written in a computer program which enables the computer to "read" the contract and perform the terms of an agreement or a business contract between two or more parties. Through automated algorithms, the contract will be self-executable when certain conditions are met by effectuating the instruction and hence the "smartness" of the contract (O'SHIELDS*, 2017).

Szabo described a vending machine purchase as a basic form of a smart contract which includes the spontaneous transfer of ownership of any assets, such as a candy bar or a can of cola, following the receipt of a preset input of a specific amount of coins. Smart contracts could be used for a variety of things, according to Szabo, such as automated digital assets transfers like shares following a certain incident, motor vehicle inactivation (in which the vehicle will only resume functioning upon fulfillment of the contract's security protocols) and peer-to-peer asset lending (in which the lent asset is returned to the lender upon the borrower's failure to meet certain requirements) (Giancaspro, 2017). In order to secure relationships on public networks, Szabo sought to use smart contracts to prevent parties from reneging on a contract, according to his notion. A contractual provision may be built in the

utilised hardware and software which renders a breach of contract costly for the party committing the breach (Rohr, 2019). It is noteworthy that smart contracts were stymied and utilised before the invented blockchain theology due to general ambiguity, issues with identity and transaction verification, challenges, and concerns with unsecured transactions(McKinney et al., 2017).

However, with the introduction of Bitcoin and its underlying technology blockchain, smart contracts can now automate the agreement terms upon fulfillment of the set conditions. The contractual parties utilise cryptographic security for "signing" the smart contract and subsequently use it on the blockchain. When the criteria specified in the code are satisfied, the software performs the specified action. For instance, if a product or service is provided, the smart contract might compel payment through the blockchain. It may commence the recovery of the product or suspension of the service in the case of non-payment. This technology has a plethora of possible applications, including financial instrument trading, syndicated loan operations, and securities settlements.

Blockchain is the technology that invented the first cryptocurrency called Bitcoin, which was founded in 2008 by an anonymous person or group using the moniker called Satoshi Nakamoto. Where the popularity of cryptocurrencies as a means of payment has grown over the past two years, most of the current attention, notably in the banking and financial sectors, has been on enabling blockchain technology. The blockchain is a public record, or ledger, of all cryptocurrency transactions ever made. A computer network validates each transaction, or block, prior to adding it to the chain of past transactions. This is accomplished via the use of cryptographic algorithms and a significant amount of computational power. Blockchain is open and clear to anyone; however, the addresses shown may not always correspond to the individual linked with the address, where the system is structured, constructed or built in a standardized manner. This prevents the data from being hacked, thus making blockchain secure and immutable (Nick Barney, 2023).

The blockchain record is meant to be everlasting and unchangeable. The technology's security, permanence, and immutability have piqued the interest of the world's major banks as well as financial startups.

For security, blockchain employs encryption and a mix of public and private "keys". For each participant in a transaction, the system uses mathematical algorithms that take a public address and matches it with a private security access key. If these two things are the same, the transaction is broadcast to the other blockchain participants for verification and recording on the blockchain (distributed ledger). For security reasons, cryptocurrencies like Bitcoin use the "proof of work" mechanism, although there are various methods for ensuring that transactions are genuine and not repeated. The capacity to monitor ownership and property transfers sans a middleman, as well as the capability to conduct direct peer-to-peer property transfer have been cited as two advancements of blockchain. Smart contracts work along with blockchain technology by ensuring the record-keeping of transactions on blockchain as trusted ledger (O'Shields*, 2017).

Nowadays, smart contracts are considered to be a step above typical electronic contracts whereby the actual agreement is computer coded instead of written in conventional languages such as English or Arabic. However, smart contracts are not unique in many other aspects, such as the fact that they must originally consist of a detectable agreement between persons having legal ability to create that agreement. As a consequence of the characteristics of smart contracts built on the blockchain, global financial institutions have started utilising automated computer processes to perform transactions that are devoid of human involvement. Dispensing with the need for physical presence and other rigorous traditional pen and paper work and cumbersome processes.

Problem Statement

The problem addressed by this paper is that the terms of a smart contract are conveyed via encrypted computer programming codes using limited and absolute contractual terms written by programmers or computer experts instead of lawyers or legal consultants. Legal issues may occur due to this in which the contractual parties will have a problem understanding the analogous obligations when any of the parties fail to fulfill the smart contract obligations because of the coded logic (Eenmaa-Dimitrieva & Schmidt-Kessen, 2019) or scheme of 'if x pay, then y will release subject matter of contract (e.g., If.../Then...) (Cuccuru, 2017). In light of this background, this paper inquires about the legality of encrypted codes under the current legislation and how

such coded smart contracts would hold in the court of law. Additionally, this paper aims to elucidate the legality of the registered writing or transactions of blockchain smart contracts.

Methodology

This study is qualitative in nature, adopting a pure legal research methodology; hence, a comparative doctrinal approach or library research is applied. The aim of this doctrinal study is to systematically discover, clarify, and examine the work of certain legislations. It will attempt to evaluate and analyse the legitimacy of legal writing by encrypted codes in smart contracts from the perspective of current contract laws in the USA, the UAE, and Iraq. The reason for the choice of these three jurisdictions is because, smart contracts originated form the USA from the works of Nick Szabo the American cryptographer. Smart contracts have equally developed over the years since inception and is gradually having legal backing in the USA. As such Iraq has a lot to learn from that jurisdiction. While the UAE just like Iraq are both Arab countries and are both in the Middle East. They share similar culture and the religion, which is Islam, is the same. However, the UAE have advanced technologically including its openness and acceptance of smart contracts as a new form of contractual agreement. Having UAE as a model, becomes easier for Iraq to adapt smart contracts and incorporate into its financial system without much difficulty.

The data are analysed to examine the nature of smart contracts in Iraq focusing on: i) the challenges in developing and using encrypted language in writing smart contracts; ii) whether the coding language is considered valid according to the provisions of Iraqi legislation, and iii) how written transactions recorded for smart contracts on the blockchain will be proven.

Findings and Discussion

Legal Challenges of Writing Smart Contracts

The legal inquiries about code are not new. Lawrence Lessig discussed the topic in 1999 in his book Code is Law. He argued that the code-based regulation theory was mainly established, along with the "open code" or open-source software, as a structural guarantee to protect the related parties (Weber, 2018). What brought the topic back again was the emergence of the expression of smart contracts in code, where the

terms require translation from human to computer language, which is accomplished by the programmer via a sequence of written steps to be carried out automatically through code (Eenmaa-Dimitrieva & Schmidt-Kessen, 2019). The programmer must write what must be done and how to execute it (Governatori et al., 2018). The issue faced by the parties to the contract is how the translation of contractual expressions to instructions is parsed by computers. Computer language removes the disadvantages of traditionally ambiguous contractual terms which allow for the flexibility of interpretation in fulfilling the commitments of the parties to smart contracts as well as allowing them to adapt contracts to unforeseeable future scenarios, including to the obligation to good faith, standards of best efforts, force majeure or permitting non-performance and hardship (Tai, 2018). Another issue is the incapacity of judges to understand the contents of smart contracts. Resultantly, there will be an increase in the costs and length of legal proceedings in relation to smart contracts owing to the requirement for experts to translate written codes (Eenmaa-Dimitrieva & Schmidt-Kessen, 2019).

In contrast to that, there is the view of other researchers in support of smart contracts, referring to them as contributing to reduce ambiguity by way of written terms in computer language. This is seen as reducing misunderstandings of contractual terms in cases of disputes in relation to the interpretation of smart contract codes that could possibly lead to lawsuits.

Furthermore, the self-executing, automated and decentralised nature of smart contract code on the blockchain poses various repercussions for the obligatory trust in closing a contract between individuals; hence, agreements have usually been concluded between parties in a more conventional, traditional manner. In brief, the parties must trust each other. This does not change anything in a normal sales contract; the purchaser must trust that the seller will be timely in delivering the purchased product and ensure the quality and quantity agreed upon. The seller also needs to trust that the purchaser will accept and pay for the product as agreed. Upon the closing of a smart contract, each contracting party must trust that the performance of the smart contract code will be in accord to the expectations of the counterparty. A party has no obligation to trust the other party's ability to meet its duties as the repercussion for fulfilling or not fulfilling those duties has been

programmed into the smart contract; upon execution, the smart contract can no longer be stopped.

A good example of using smart contracts is in a gambling transaction. The correct programming of a code will enable the self-execution of the smart contract only if both sides of the transaction have paid their agreed-upon wager to the contract account. Once the event has been concluded and a winner has been established, the smart contract meets the obligation of the losing party to pay via the disbursement of the wagers to the winning party. Whilst traditional contracts necessitate trust between the contracting parties, smart contracts shift the trust to the code (de Graaf, 2019).

In order to overcome these obstacles, parties to the smart contract must conduct lengthy negotiations and agree on all the details. Therefore, it would be reasonable to assume there are PDF documents written in natural language that describe the essence of the agreement. Otherwise, the terms and conditions of a coded contract may also be considered a type of adhesion contract that takes the form of a ready-made template designed by a seller who wishes to provide the buyer with a take-it-or-leave-it contract. Lastly, the researcher sees smart contracts as a means of providing a legally binding contractual solution through the computer codes that are fully or partly self-executing, aided by the use of the internet in an environment like Iraq that is affected by insecurity and political instability. Compared to other jurisdictions, litigation procedures are complicated and lengthy but adopting smart contracts in financial transactions would help to reduce to complexities associated with litigations in Iraq.

Formalities in the Written Contract

The formalism of writing contracts is in the form required for the contract to be validly concluded. In this regard, the Parliament of England adopted An Act for the Prevention of Frauds and Perjuries in 1677, considered to be the first law of its kind, which required a signature on a written contract for the sale of goods in excess of ten pounds. Likewise, American law in the Uniform Commercial Code adopted a similar doctrine, requiring the writing of contracts in some types of contractual agreements because such contracts come under the Statute of Frauds (Camero, 2013).

These contracts were determined as: 1) contracts for marriage, 2) contracts for a suretyship, 3) contracts for an executor or administrator, 4) contracts for land sale, and 5) contracts extending performance to more than one year since the contract's formation date. Apart from the Statute of Frauds, Article 2 of the Uniform Commercial Code (UCC) necessitates signed written contracts for moveable goods sales of more than $500 in value(Camero, 2013).

It is worth noting that the US Uniform Electronic Transaction Act (UETA) is congruent with Articles 5 and 6 of the UNCITRAL Model Law on Electronic Commerce, which considers most of the digital messages contained in well-formatted written contracts as acceptable pursuant to the UETA. These articles also specify that digital symbols and emails composed of writing in as much as they can be retrieved in an understandable form would be recognised. Moreover, UETA Section 7(c) states that an electronic record can be used to satisfy laws that require a record to be written. Additionally, according to UETA Section 2(7), a typical "electronic record" is any record that is created, developed, transferred, sent, disseminated, obtained, or stored by any electronic means. Also, UETA Section 2(13) describes a "record" as any written information on a physical channel (or electronic mediums and the likes) that can be retrieved in a comprehensible form (Ramberg, 2001).

Likewise, Iraqi and Emirati legislators have determined that some contracts whose value exceeds a certain amount are required to be written in order to be used as evidence of contractual obligations. Furthermore, according to Article 112 of the UAE Civil Transactions Law, it is considered that one of the best evidences as proof of existing rights is a written contract in that contracts expressed in writing are undeniable ("the Civil Transactions Law," 1987). UAE law demands that contracts be created by the exchange of mutual intentions accomplished through the integration of an offer by one party that is subsequently accepted by the other pursuant to Article 125 of the UAE Civil Code. The expression of intent may be made orally or through contracts which require the expression of the intent of parties to be in written form or by acts demonstrating mutual intent (Nazanin Aleyaseen). Despite the importance of traditional written contracts, the Federal Law of the UAE No. (1) of 2006 on Electronic Commerce and Transactions and Electronic Transactions (ETC, 2006) as well as the Commerce Law

in Dubai No.2/2002 cover a mix of electronic writing and electronic documents. Though the above-mentioned laws do not contain an explicit definition of writing, the Federal Evidence Law No. 36 of 2006 (Article 17 Section 2) defines electronic documents as all documents involving an instance of the diffusion, receipt, or storing of symbols, signals, writing, images, sounds, or information via an information technology medium (Mshtfaee, 2020).

The ETCL of the Emirate of Dubai addresses the concept of "writing" in the context of Article 9 of the law, stating the following: In cases where the law stipulates that any data, document, record, or explicit transaction should be produced in writing (or a stipulation for the arrangement of certain results in the absence of this writing), the document or electronic record adheres to the law as long as it abides by the provisions of Article 7, Section 1 of the same law, which allows electronic communication. In such cases, no legal effect or enforcement shall be denied for any electronic communication based merely on the fact that it is in electronic form.

In the Iraqi position, the Electronic Signature and Electronic Transactions Law No. 78 of 2012 (Article 1, Section 5) provides its own definition of electronic writing. According to this law, when writing is stored electronically, its meaning should be perceptible and understandable. In other words, every letter, number, symbol, and any other mark affixed using an electronic, digital, optical, or other similar means gives a connotation and understandable indication (Electronic Signature & Electronic Transactions Law, No. 78, 2012. Article (1) section 5). According to what has been discussed supra, it should be noted that the requirements and conditions of the written contract must be met, whether the language of the contract is expressed via legal prose or by codes. These requirements are discussed in the following paragraphs.

Electronic Writing must be Readable and Understandable

Electronic writing of smart contracts or transactions must be clear and understandable, whether in the form of encrypted codes or letters, pursuant to US contract law and takes into account the rule of the duty to read doctrine. According to that, the contracting party must read an agreement before assenting to its terms, which is considered a key element of the US contract law. Although duty to read is generally a

contract law doctrine, it poses significant repercussions to consumer standard contracts in that consumers, as well as consumer law academics, prominent law professor, and the Chief Justice of the US Supreme Court do not read such contracts. Furthermore, courts typically enforce the duty to read to consumer agreements inclusive of online boilerplate contracts.

Although some states have enacted laws requiring the writing of contracts in clear language, the United States legislation has not provided criteria or a general explanation or definition of what constitutes a "readable" text (Benoliel & Becher, 2019). However, the courts typically enforce the duty to read to consumer contracts inclusive of standard online agreements. Consequently, in US law, the duty to read doctrine is unilateral. Hence, despite the notion that individuals do read contracts, suppliers are not generally required to provide readable contracts to consumers (Benoliel & Becher, 2019).

In addition, the duty to read binds individuals to the contract's terms despite not reading them in cases of smart contracts written by code (Benoliel & Becher, 2019), and the courts typically enforce the execution of these agreements even if the parties have not read them. Contracting by electronic means permits online firms to make contracts with millions of users, with no negotiation, and without verifying that the contract was read or was understandable; hence, sellers are not obliged to provide purchasers with readable contracts (Benoliel & Becher, 2019). The UCC does not determine the manner in which a signature needs to be represented, whereas the courts assent to a valid signature by assessing whether there is evidence that the parties accepted or adopted the writing. Thus, a seller or purchaser of a good relying on a smart contract could effectively indicate the parties' assent to an agreement when they sign with their private keys on a smart contract (DLx Law LLP October 16, 2018).

Cases involving disputes before the courts could present great difficulties in examining smart contracts because they do not have the necessary experience for this. Since most of the contract terms are represented by codes on a blockchain and judges at present, do not have the expertise to interpret these codes. As such the parties to a contract would not be able to dispute that they have not read the contract because the signature is evidence before the court regarding the acceptance of

the conditions of the contract written in code. But from the perspective of Iraqi and UAE legislation and jurisprudence, the reading condition is fulfilled if it can be read using an electronic computer or by any other mediator such as a programmer (Sahb, 2016). Therefore, potentially, developers could create artificial intelligence applications to translate the code language to the English language in order to make smart contracts understandable and readable for anyone in the future. Recent trends advocates the use of AI to enhance smart contracts (Krichen, 2023).

Electronic Writing must be Characterised by Permanence and Stability

This condition means the writing by code of contracts or transactions in electronic media must have stability and permanence so that its content can be referred to and inferred from it before the court in the event of a dispute between the parties, and it is stated in Article 13/Section (1) of the Iraqi Electronic Signature and Electronic Transactions Law that electronic documents, electronic writing and online contracting have the same legal validity to their paper equivalents according to conditions stipulated by the law. One condition for this is that the writing be preserved and kept to enable its retrieval at any time (Electronic Signature & Electronic Transactions Law, No. 78, 2012. Article (13) section 1).

In the same vein, the UAE law in Article 5(1)(A) states that for any law requiring the retention of documents, records or information due to any purposes, the necessity is fulfilled by keeping electronic records in the form in which they were formed, disseminated or received, or in a form proven to be accurately representative of the information created, sent or received (Federal Law No. (1) of 2006 on Electronic Commerce and Transactions (ETC) 2006). With regards to Iraq and the UAE, the lawmakers need to regulate the recognition of recordkeeping or documents on the blockchain, specifying the recognised type of blockchains, whether private or public, to ensure the permanence and stability of transactions and written smart contracts.

The United States has recognised in some states, such as Illinois, the regulated use of blockchain in transactions and procedures, as per state law (i.e., Act House Bill 3575), which pointed out that when the statute requires documents or records to be in writing, the evidence

electronically recorded on a blockchain is sufficient. But the recognition of transaction records on blockchains is not absolute, such as where Act House Bill 3575 of the state of Illinois imposes a limitation on evidence recorded on the blockchain. The legal validity of a smart contract may be rejected if the blockchain contains transactional records that are not storable or reproducible for all the parties (Pollacco, 2020). Thus, there could be consequences leading to losing the character of permanence and stability of the electronic writing.

Electronic Writing must be Immutable to Adjustment and Change

This condition means that all contracts must contain zero defects (e.g., changes, additions, deletions, amendments) pursuant to the Iraqi Electronic Signature and Electronic Transactions Law. As stated in Article 13 (Sections A and B), the electronic writing must be kept either in the form it was formed, disseminated, or received or in some other form that proves that no part of the text has been amended, added, or deleted since being sent. The law also mentions that the information contained must indicate who created it and the receiver of it as well as the date and time on which the information was sent and received (Electronic Signature & Electronic Transactions Law, No. 78, 2012. Article 13(B&C).

As for UAE legislation, there is a blend between the phrases "electronic writing" and "electronic document". In cases like this, the law often requires a document, record, or information to be preserved. Therefore, if any document, record, or information is saved electronically, the following rules must be followed:

> a. The electronic record must be kept in the form in which it was created, sent, or received or in some other form that proves that it accurately represents the original information. In other words, the original document or record cannot be changed in any way when it is saved electronically.

> b. The information should be kept in ways in which it can be used for subsequent reference.

> c. Any information must be retained that identifies the origin of the electronic message, its destination, and the date and time of its dissemination and receipt (ETC, 2006 Article 5).

In the case of smart contracts, the writing would be recorded and saved on the blockchain, where it is not subject to change and adjustment and is thus compliant with the provisions of the Iraqi and UAE laws. Rather, the blockchain will be decentralised and the parties involved in a smart contract are anonymous, so the parties must use a platform relying on private blockchains to ensure that authentication of transactions are not taking place unless the parties are known.

The American position is different, wherein some states such as Nevada and Arizona in 2017 enacted laws that apply to smart contracts. Per these laws, records that are available only in electronic form will not be considered unenforceable because of their electronic nature. Meanwhile, in cases where records are legally required to be provided in writing, an "electronic record" satisfies the law. For this purpose, in addition, an electronic record is defined as a "record created, generated, sent, communicated, received or stored by electronic means" in order to include blockchain transactions (McKinney et al., 2018). Therefore, registering written transactions on a blockchain ensures that writing cannot be modified. The nature of blockchains makes information immutable, decentralised, consensus-driven, and transparent. Moreover, all transactions on blockchains would be open files, meaning that any user can access them and evaluate the validity of any transactions associated with them.

Admissibility of Written Smart Contract as Transaction Recorded on Blockchain

Usually, online contracts are written on electronic devices or physical mediators that are certified or authenticated by bodies approved by governments. The relevant laws of a state may determine permitted organisations or individuals, such as notaries public, to certify electronic records or written documents. These may fall under the authority of the contracting parties or a legally recognised central authority. But in the case of a smart contract, the content of the contract is an encrypted program written in a programming language documenting the will of the parties and the terms of the agreement via digital signatures represented by private keys. These signatures grant approval to users of blockchains or miners to implement smart contracts using blockchain technology so that solely miners or users of the blockchain network can access them. Establishing a new block that documents the smart

contract and digital signatures involves solving mathematical problems and algorithms, which will establish the new block in the blockchain on which the smart contract is recorded. In this regard, the blockchains substitute the (electronic) records that document electronic transactions and smart contracts. Therefore, the courts will need to recognise the blockchain technology as an electronic record in order to use it as evidence proving the terms of the written smart contract using many of the traditional legal principles that are currently used in adjudicating disputes involving electronic contracts. Because of the decentralised nature of record-keeping with blockchain technology, there is a need to legally recognise the record-keeping or transactions relating to smart contracts that are created, stored, or verified via blockchains by the legislative authorities in the selected jurisdictions in order to help the courts deal with disputes arising about smart contracts.

From another standpoint, the researcher envisions that the presentation of blockchain technology as proof will face no objection (as being the same as any electronic evidence) before a court provided that its reliability is provable (e.g., via expert admission of the blockchain's reliability as written evidences in front of the courts). Nevertheless, this would lead to monetary and time losses, thereby limiting the advantages of the blockchain. To avoid these losses, a jurisdiction could acknowledge the permissibility of the blockchain and electronic evidence by firstly allowing the evidence at the legislative level and secondly using the blockchain technology implicitly at the government level (Polydor, Jan 05, 2020).

In the next section, this paper discusses the extent to which written and recorded smart contracts on blockchains can be accepted as evidence of the existence of the terms in written smart contracts by codes on the blockchain and their recognition before a court of law. Therefore, in the following discussion, the researcher examines and analyses the uses of the blockchain as an electronic medium.

United States of America

In the United States, the federal government has not yet acted on its constitutional power to introduce legislation that regulates blockchain admissibility as written record-keeping as evidence before courts of law as there is an overlap in jurisdiction due to the presence of multiple authorities trying to regulate the admissibility of the blockchain.

Therefore, the federal government has taken two methods to regulate the recognition of evidence on the blockchain, firstly by taking the legal principle known as the "best evidence rule"(Pollacco, 2020).

Prior to the invention of the blockchain, a specified minimum requirement was established in the Federal Rules of Evidence (FRE) which stipulates that, at trial, it is necessary to use the best available evidence. In accordance with rule 1002 of the FRE, this rule is applied upon the desire of a party to use the contents of a written document, recording, or photograph as evidence at trial, despite the unavailability of the original document. As such, the court could accept a secondary evidence the demonstrate the document's contents and utilise it as permissible evidence (Institute). Unless otherwise provided in federal law or the FRE, and by the measurement of that, the transactions or documents recorded on blockchains are considered sufficient evidence before the courts according to the "best evidence rule". Otherwise, this could be accomplished through the US federal government allowing the freedom of states to independently enact laws, state by state. Thus, several states have begun individually issuing laws on admissible record-keeping of transactions on blockchain technology, allowing its admission as evidence before the courts.

Consequently, an initial legal recognition of transactions stored on the blockchain was enacted in the state of Vermont in June 2016 with House Act 868, which is an act related to various economic developments, containing a specific section on the acknowledgement of the validity of blockchain records and their court-related permissibility. According to the act, an electronically-registered digital record on the blockchain self-authenticates if it comes with a written declaration of a capable individual. In the same vein, a number of states have established state-specific rules and legislation for blockchain regulation, especially in the area of cryptocurrency. Such as California (Zain et al., 2019) and New York which was the first state to begin legislation in this area by regulating cryptocurrency organisations, and 32 other states soon proceeded along the same path. Furthermore, New York, Illinois, Vermont, Virginia, Arizona, Washington, and Ohio introduced or passed legislation to regulate the admissibility in court of all evidence stored on the blockchain, smart-contract validity, and the recognition of the blockchain as secured storage for the record-keeping of transactions (Pollacco, 2020). Thus, from this perspective, the statutes require any

written records or documents digitally recorded on the blockchain to be
regarded by courts as acceptable evidence.

UAE (United Arab Emirates)

The Emirati legislature did not refer to the electronic media used to
store or record electronic transactions or writings in explicit form, but
referred to it implicitly as stipulated in Article 2 of the ETCL of the
Emirate of Dubai No. 2/2002. This defines an electronic "record" or
"document" as an established, kept, retrieved, copied, sent, notified, or
received record or document, all of which are electronically performed
via a physical medium, or via other electronic mediums where it
would be retrievable in an understandable form (ETCL, Article 2).
The tangible medium is considered an electronic medium for storing
electronic writing or an electronic "record" or "document". In the same
vein, "electronic medium" is defined by the ETC, 2006 in Article No. 1.

Additionally, the amendment to the Federal Evidence Law No.
36 of 2006 has defined electronic documents, in Article 17 Section 2
Duplicated, stipulating that an "electronic document" is any diffusion,
receipt, or keeping of symbols, signals, writing, images, sounds, or
information in any form that is conducted through an information
technology medium. "It is clear through the definition that the UAE
legislator has mixed between electronic writing and the electronic
document, as well as merging between the electronic record and the
electronic document, although jurists assert that there is a difference
between them"(Mshtfaee, 2020).

Emphasising this, there are several conditions mentioned in Article
5 of the ETC, 2006 which provide that if the law requires preservation
of a written document, record, or information for any reason, then this
condition will be fulfilled if that document, record or information is
saved in the form of an electronic record, provided it takes into account
the following:

> a. Keeping the electronic record in the form it was developed,
> disseminated or received, or in any form, which can prove,
> that it accurately represents the information originally
> created, sent or received.
>
> b. Preserving saved or stored the information in a manner
> that enables it to be used for subsequent reference.

> c. Preserving any information – if found – which allows for
> the origins of the electronic data message, its destination, and
> the date and time of sending and receiving it to be identified
> (ETC, 2006 Article 5).

It is clear from the supra discussed and from the definition of electronic "record" or "document" including the term any other "electronic medium" that it would be valid and deemed as evidence pursuant to law regardless of whether this medium is tangible or not. Hence, the UAE law may accept the recognition of transactions on blockchains without needing to explicitly state the fact. The documents specifically referred to in this article will be in a form that is not possible to change as they will be kept in new blocks and nodes within the blockchain, which can only be viewed by the participating or licensed parties in the case of private blockchains. Therefore, they are considered valid documents and records, as long as they adhere to the conditions mentioned in Article 5 of the ETCL.

Notwithstanding the fact that the current laws of the United Arab Emirates do not deny the authenticity of transactions recorded on blockchains, the government has initiated practical steps using blockchains in the field of government and judicial transactions. This began in April 2018 when the government launched the Emirates Blockchain Strategy 2021, with a target to make the UAE the first government in the world to use blockchain technology. This strategy aims on capitalising on blockchain technology for the purpose of transforming 50 percent of governmental transactions into blockchain by 2021.

With regards to the judicial domain, the Dubai government is planning on launching blockchain-based services in the judicial and financial fields, where it will launch the first court in the world depending on the blockchain in the Dubai International Financial Centre (DIFC). This system also provides automated dispute resolution of smart contracts to solve issues between involved parties, which increases the efficiency and reliability of record-keeping. This technology will perform an important role in simplifying judicial processes, avoiding duplication of documents by enabling the parties to access the same versions of the documents, thus achieving greater efficiency across the

entire judicial system. This is in addition to Dubai's launching of Dubai Pay, an online payment portal with the integration of blockchain, thus enabling real-time reconciliation (Southon, May 1 2019). All of this will contribute to achieving Dubai's endeavours regarding the adoption of advanced technologies to support the process of transforming the UAE into the happiest and smartest country, worldwide.

Iraq

Electronic writing or code is stored, transactions are recorded, and electronic records are maintained in order to present them as legal arguments before the courts and to prove the existence of the contracts and record them as electronic documents that are immutable in the event of disputes. Although the Iraqi legislature did not recognise blockchains, the lawmakers defined the electronic medium in Article (1) Section 7 of the law on an attestation of the Convention on the Regulation of the Provisions of the Electronic Signature in the Field of Electronic Transactions in the Arab Countries as a physical mediator for the preservation and circulation of electronic writing, such as CDs, other types of optical disk, magnetic disks, electronic memory, or any other similar medium (law of an attestation of the Convention Regulation the provisions of the electronic signature in the field of electronic transactions in the Arab countries No. (101) for the year 2012 Article 1(7). It is evident from the previous definition that structured writing of information cannot be valued as proof except by installing it on a physical medium such as an optical disk (e.g., CD or DVD), a hard drive, flash drive, or any modern electronic means. Although the electronic medium, as defined by the Iraqi law, has to be digital, optical or of any other similar means that is understandable, it would be commendable if the Iraqi legislature made room for any developments that may occur in the future in the field of technology due to the nature of some electronic media on which electronic data are carried may be damaged due to technical reasons beyond the user's control. Technical defects or misuse may lead to the destruction of electronic data, which makes it impossible to resort to it again for any purpose whatsoever (Sahb, 2016).

It can however be said that the technological development that is taking place now in terms of storage methods, as well as the volume of

electronic data storage in blockchain, confirms the reduced risks of the exposure of electronic written evidence to damage or loss, especially where the possibilities of preservation and storage in different memories are within one electronic medium. Thus, the form in which electronic documents are stored on the blockchain fulfils the conditions of continuity and stability necessary for admissibility as written evidence or proof.

Nevertheless, and despite all the advantages of blockchain technologies, it is clear from the foregoing that the electronic medium in the case of smart contracts relating to the blockchain cannot have legal standing unless the blockchain technology is explicitly recognised by Iraqi legislation. This is because Iraqi legislation narrowly defined an electronic medium in Article 1(7) as a ''material medium'' in order to conserve the deliberate nature of electronic writing, therefore considering the blockchain a virtual, non-physical medium.

Conclusion and Recommendations

A majority of jurisdictions deem a written agreement as the best proof of a contract's rights, as exemplified by the US's UETA legislation as well as the Iraqi legislation that have explicitly defined electronic signatures and electronic transactions in the law. Most applicable existing laws have specifications on pictures and different forms of writing, generally specifying that any writing should indicate meaning to capable individuals, regardless if it is coded. Emirati legislation has not defined electronic writing in any separate legislation; however, there is text on it in a section on electronic records. UAE law stipulates that writing and electronic documents do not lack legal effect or enforceability simply because they are in electronic form. Laws generally recognise writing in the form of code or programming language in smart contracts if they can be read by a computer after the decoding of the encryption by experts or via a program so that the content of the contract becomes legible, clear, and understood by the parties concerned. But the written code's validation as proof of the smart contracts' terms would be the key stumbling block in Iraqi law which requires for the writing to be kept in electronic media (physical media) to preserve it. Yet, smart contract terms are contractually recorded or are written transactions in the blockchain, whilst the blockchain technology is deemed as an

intangible medium. Hence, smart contracts written in coded language and kept in blockchain are not deemed as legal evidence usable in court except if the legislation overtly acknowledges the blockchain via new law enactment.

In conclusion, this paper suggests several recommendations. Firstly, it is necessary to add a new curriculum in law schools to familiarise students with any programming language utilised in smart contracts so that lawyers and lawmen in the future are able to convert the legal language or legal prose of contracts, including conditions and obligations, for storage and use in blockchain implementations. At the very least, infrastructure for legal expertise should be initialised that will enable understanding of the computer implementation of smart contracts. Secondly, there is a need to amend the article related to electronic media, specifically its restrictive concept of requiring the physical existence of an electronic storage medium for legal documents such as contracts. Alternatively, new legislation could be enacted such as that of some states in the US, where lawmakers have recognised smart contracts and transactions on the blockchain and given legitimacy to them to be used as evidence admissible before the courts.

Acknowledgement

References

Statutes and Conventions

Iraqi Civil Code, No. 40, 1951.

Electronic Signature & Electronic Transactions Law, No. 78, 2012.

Law of an attestation of the Convention Regulation the provisions of the electronic signature in the field of electronic transactions in the Arab countries No. (101) for the year 2012.

Law of Electronic Transactions and Commerce No.2/2002.

Federal Law No. (1) of 2006 on Electronic Commerce and Transactions 2006.

Journal Articles

Abd, R. F. (2015). Formalism in the electronic contract (condition for convening or for proof). *The islamic college university journal* (33), 531.

Benoliel, U., & Becher, S. I. (2019). The duty to read the unreadable. *Boston College Law Review*, *60*, 2258-2259. https://heinonline.org/HOL/License

Camero, J. (2013). Zombieland: Seeking Refuge from the Statute of Frauds in Contracts for the Sale of Services or Goods. *UMKC LAW REVIEW*, *82*, 3. https://heinonline.org/HOL/License

The Civil Transactions Law, (1987).

Cuccuru, P. (2017). Beyond bitcoin: an early overview on smart contracts. *International Journal of Law and Information Technology*, *25*(3), 7.

de Graaf, T. (2019). From old to new: From internet to smart contracts and from people to smart contracts. *Computer law & security review*, *35*(5), 8.

DLx Law LLP , B. R., et al. (October 16, 2018). *"SMART CONTRACTS" & LEGAL ENFORCEABILITY* (CARDOZO BLOCKCHAIN PROJECT Issue. C. L. School. https://cardozo.yu.edu/programscenters/blockchainproject

Eenmaa-Dimitrieva, H., & Schmidt-Kessen, M. J. (2019). Creating markets in no-trust environments: The law and economics of smart contracts. *Computer law & security review*, *35*(1), 81. https://doi.org/https://doi.org/10.1016/j.clsr.2018.09.003

Giancaspro, M. (2017). Is a 'smart contract' really a smart idea? Insights from a legal perspective. *Computer law & security review*, *33*(6), 2. https://doi.org/doi: 10.1016/j.clsr.2017.05.007

Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G., & Xu, X. (2018). On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artificial Intelligence and Law*, *26*(4), 13.

Hsyn, b. f. (2016). The formal in the electronic civil contract, a comparative analytical study In the light of the Iraqi electronic signature and electronic transactions law No. (78) of 2012. *TIKRIT UNIVERSITY JOURNAL FOR RIGHTS*, 266.

Institute, L. I. *Best Evidence Rule*. Cornell Law School. https://www.law.cornell.edu/wex/best_evidence_rule#:~:text=The%20best%20evidence%20rule%20applies,acceptable%20excuse%20for%20its%20absence.

Krichen, M. (2023). Strengthening the security of smart contracts through the power of artificial intelligence. *Computers*, *12*(5), 10. https://doi.org/https://doi.org/10.3390/computers12050107

McKinney, S. A., Landy, R., & Wilka, R. (2017). Smart contracts, blockchain, and the next frontier of transactional law. *WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS*, *13*, 317.

McKinney, S. A., Landy, R., & Wilka, R. (2018). Smart Contracts, Blockchain, and the Next Frontier of Transactional Law. *Washington Journal of Law, Technology & Arts*, *13*(3), 20. https://digitalcommons.law.uw.edu/wjlta/vol13/iss3/5.

Mshtfaee, S. (2020). *Means of proof and their argument in electronic commerce contracts in the Algerian and comparative legislation* [PHd, Ahmed Draia University of Adrar].

Nazanin Aleyaseen, J. P. e. a. *Settlement (civil litigation) Q&A: United Arab Emirates* Practical Law https://uk.practicallaw.thomsonreuters.com/w-006-5990?lrTS=20220408024957477&transitionType=Default&contextData=(sc.Default)&firstPage=true

Nick Barney, M. K. P. A. S. G. (2023). *Blockchain for businesses: The ultimate enterprise guide*. TechTarget. https://www.techtarget.com/searchcio/definition/blockchain

O'SHIELDS*, R. (2017). Smart contracts: Legal agreements for the blockchain. *NC Banking Inst.*, *21*, 179.

Pollacco, A. T. (2020). *The Interaction between Blockchain Evidence and Courts – A cross-jurisdictional analysis*. https://blockgeeks.com/guides/blockchain-evidence.

Polydor, S. (Jan 05, 2020). Blockchain Evidence in Court Proceedings in China – A Comparative Study of Admissible Evidence in the Digital Age (as of June 4, 2019). *Stanford Journal of Blockchain Law & Policy*, *3*(2), 2. https://stanford-jblp.pubpub.org/pub/blockchain-evidence-courts-china/release/1

Ramberg, C. H. (2001). The e-commerce directive and formation of contract in a comparative perspective. *Global Jurist*, *1*(2), 6.

Rohr, J. G. (2019). Smart contracts and traditional contract law, or: the law of the vending machine. *Cleveland State Law Review*, *67*, 72.

Sahb, N. H. (2016). Legal arguments for electronic documents and methods for appeal In it(comparative study). *Lark Journal for Philosophy , Linguistics And Social Sciences*, *1*(22), 297.

Southon, E. (May 1 2019). *Rise of the Blockchain: A Middle East legal perspective*. Lexology. https://www.lexology.com/library/detail.aspx?g=a3f9c5e0-28c6-41f8-9846-3b488cdf3aee.

Tai, E. T. T. (2018). Force majeure and excuses in smart contracts. *European Review of Private Law*, *26*(6), 19.

Weber, R. H. (2018). "Rose is a rose is a rose is a rose"–what about code and law? *Computer law & security review*, *34*(4), 701.

Wu, H., & Zheng, G. (2020). Electronic evidence in the blockchain era: New rules on authenticity and integrity. *Computer law & security review*, *36*, 9.

Zain, N. R. B. M., Ali, E. R. A. E., Abideen, A., & Rahman, H. A. (2019). Smart contract in blockchain: An exploration of legal framework in Malaysia. *Intellectual Discourse*, *27*(2), 609.

GUIDELINES FOR AUTHORS

Intellectual Discourse is an academic, refereed journal, published twice a year. Four types of contributions are considered for publication in this journal: major articles reporting findings of original research; review articles synthesising important deliberations related to disciplines within the domain of Islamic sciences; short research notes or communications, containing original ideas or discussions on vital issues of contemporary concern, and book reviews; and brief reader comments, or statements of divergent viewpoints.

To submit manuscript, go to http://www.iium.edu.my/intdiscourse

The manuscript submitted to Intellectual Discourse should not have been published elsewhere, and should not be under consideration by other publications. This must be stated in the covering letter.

1. Original research and review articles should be 5,000-8,000 words while research notes 3,000-4,000 words, accompanied by an abstract of 100-150 words. Book review should be 1,000-1,500 words.

2. Manuscripts should be double-spaced with a 1-inch (2.5 cm) margins. Use 12-point Times New Roman font.

3. Manuscripts should adhere to the *American Psychological Association* (APA) style, latest edition.

4. The title should be as concise as possible and should appear on a separate sheet together with name(s) of the author(s), affiliation(s), and the complete postal address of the institute(s).

5. A short running title of not more than 40 characters should also be included.

6. Headings and sub-headings of different sections should be clearly indicated.

7. References should be alphabetically ordered. Some examples are given below:

Book
In-text citations:
Al-Faruqi & al-Faruqi (1986)

Reference:
Al-Faruqi, I. R., & al-Faruqi, L. L. (1986). *The cultural atlas of Islam*. New York: Macmillan Publishing Company.

Chapter in a Book
In-text:
Alias (2009)

Reference:
Alias, A. (2009). Human nature. In N. M. Noor (Ed.), *Human nature from an Islamic perspective: A guide to teaching and learning* (pp.79-117). Kuala Lumpur: IIUM Press.

Journal Article
In-text:
Chapra (2002)

Reference:
Chapra, M. U. (2002). Islam and the international debt problem. *Journal of Islamic Studies, 10*, 214-232.

The Qur'ān
In-text:
(i) direct quotation, write as 30:36
(ii) indirect quotation, write as Qur'ān, 30:36

Reference:
The glorious Qur'ān. Translation and commentary by A. Yusuf Ali (1977). US: American Trust Publications.

Ḥadīth
In-text:
(i) Al-Bukhārī, 88:204 (where 88 is the book number, 204 is the ḥadīth number)
(ii) Ibn Hanbal, vol. 1, p. 1

Reference:
(i) Al-Bukhārī, M. (1981). *Ṣaḥīḥ al-Bukhārī*. Beirut: Dār al-Fikr.
(ii) Ibn Ḥanbal, A. (1982). *Musnad Aḥmad Ibn Ḥanbal*. Istanbul: Cagri Yayinlari.

The Bible
In-text:
Matthew 12:31-32

Reference:
The new Oxford annonated Bible. (2007). Oxford: Oxford University Press.

Transliteration of Arabic words should follow the style indicated in ROTAS Transliteration Kit as detailed on its website (http://rotas.iium.edu.my/?Table_of_ Transliteration), which is a slight modification of ALA-LC (Library of Congress and the American Library Association) transliteration scheme. Transliteration of Persian, Urdu, Turkish and other scripts should follow ALA-LC scheme.

Opinions expressed in the journal are solely those of the authors and do not necessarily reflect the views of the editors, or the publisher. Material published in the *Intellectual Discourse* is copyrighted in its favour. As such, no part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, or any information retrieval system, without permission in writing from the publisher.

In This Issue

2289 5639