

DOI: 10.5281/zenodo.22062259

LEGAL CHALLENGES OF PROVING DEFECTS OF CONSENT IN SMART CONTRACTS: A COMPARATIVE STUDY BETWEEN JORDAN AND THE UAE

Numan Muhammad Abdullah Odat

*Department of Law, College of Sciences and Theoretical Studies, Saudi Electronic University, Saudi Arabia.
Email: N.oudat@seu.edu.sa*

*Received: 20/07/2026
Accepted: 21/08/2026*

*Corresponding Author: Numan Muhammad Abdullah Odat
(N.oudat@seu.edu.sa)*

ABSTRACT

The development of smart contracts on distributed ledger technology has created very real doctrinal and evidentiary problems for the classical consent theory-based legal system. This article conducts a thorough comparative study on the legal regimes of defects of consent error, fraud, duress and misrepresentation regarding smart contracts in the light of the international conventions adopted by the United Nations Commission on International Trade Law (UNCITRAL) and the United Nations Principles of International Commercial Contracts (UNCPC). The study highlights key gaps in legislation and clear issues of evidence that hinder claimants from establishing vitiated consent in algorithmically executed contracts, grounded in primary legislative sources, such as the UAE Federal Law No. 5 of 1985 (Civil Transactions Law), UAE Electronic Commerce Law No. 1 of 2006, the regulatory frameworks of the Dubai International Financial Centre (DIFC) and the Abu Dhabi Global Market (ADGM), and Jordanian Civil Code No. 43 of 1976. The analysis demonstrates that, while automated self-executing code involves one-to-one interaction between a digital entity and a human user, both jurisdictions are poorly suited to deal with these types of interactions, as the record cannot be altered and the party deploying the code can be anonymous, and the 'agreement' can be either ambiguous or impossible in practice. The article suggests a three-part reform agenda – (i) technology-neutral statutory amendments to explicitly apply the doctrine of “defect of consent” to algorithmic agents; (ii) forensic evidentiary rules for the authentication of blockchain data and expert testimony; and (iii) a specialised dispute resolution mechanism based on the ADGM's current smart contract recognition framework. The findings add to the still emerging literature on smart contract legality in the Arab world, and provide practical suggestions for legislative reform.

KEYWORDS: Smart contracts; defects of consent; Jordanian Civil Code; UAE Civil Transactions Law; blockchain; misrepresentation.

1. INTRODUCTION

One of the most game-changing inventions in contract law since the nineteenth century codification is the advent of smart contracts: code stored on a blockchain that automatically executes contractual obligations when certain conditions are met. Smart contracts were first imagined in 1994 by cryptographer Nick Szabo and have evolved from a theoretical exercise to a business-relevant tool used in finance, supply chain, real estate, and government. The global smart contract market was worth about USD 684.3 million in 2022 and is set to increase to USD 8.3 billion by 2030, which highlights the need for the legal issues that will be raised by the technology.

The challenge is of course even deeper for any legalist in the Arab world. The laws of Jordan and the United Arab Emirates (UAE) have a common civilian framework based on the Egyptian Civil Code (ECC), which itself is based on the French and Swiss civil codes and influenced by Islamic jurisprudence. Both jurisdictions rely on the freely given, informed consent of legal persons endowed with full capacity for the validity of their contracts. According to classical consent theory as it is presented in the Jordanian Civil Code No. 43 of 1976 and the UAE Federal Law No. 5 of 1985 (Civil Transactions Law), consent is a psycho-volitional state which is an internal subjective phenomenon that can be vitiated by error, fraud, duress, or misrepresentation. The doctrinal architecture assumes that at a known point in time there are two wills.

The basic architecture is destabilised by smart contracts. A smart contract is usually deployed as a set of unchangeable code before any particular transaction takes place, whereas a traditional contract needs an offer, acceptance and a meeting of minds. The 'consent' of a counterparty can be as simple as sending a cryptocurrency token to a contract address, which could be done by an automated wallet, an API call or even a phishing victim who was never seeking to make the transaction. The blockchain record is pseudonymous, the transaction itself is irreversible, and the code is the 'written' contract, making proof of a defect of consent to the satisfaction of a court by conventional evidentiary standards daunting.

Although these questions are of great practical value, scholarly work on defects of consent in the context of smart contracts from Arab jurisdictions is thin on the ground. The literature in Arabic and English focuses on smart contracts in general (Durovic & Janssen, 2018; Raskin, 2017) or on the commercial law of the Gulf region (Omar, 2016; Al-Qattan, 2013; Al-Sufiani, 2012; Al-Suwaileh, 2019),

but cannot be found to be addressing the particular evidentiary issues raised by the use of distributed ledger technology. The present article fills this gap by undertaking a systematic comparison of Jordanian and Emirati law on three axes: the substantive doctrinal fit of classical defect-of-consent rules to smart contract scenarios; the evidentiary burdens imposed on litigants who must prove such defects in court; and the institutional capacity of each jurisdiction's courts and arbitral bodies to adjudicate smart contract disputes.

2. THEORETICAL BACKGROUND

2.1. *The Technical Architecture of Smart Contracts*

Smart contracts are pieces of code that run on a blockchain, or distributed append-only ledger that is coordinated by a network of nodes instead of a central authority. The code defines conditions and consequences: "when event X happens, do Y. After a contract is deployed, it cannot be easily modified (or deleted). Consensus mechanisms (proof-of-work or proof-of-stake) validate transactions, and they are recorded in cryptographically linked blocks. The Ethereum blockchain, established in 2015, has emerged as the leading platform for the deployment of smart contracts, with several other smart contract platforms such as Binance Smart Chain, Solana, Hyperledger Fabric, etc. gaining significant traction.

From a legal standpoint, there are some important technical features of smart contracts. Firstly, immutability – once deployed and executed, even the code cannot be changed without consensus of the entire network, which is impractical in a sufficiently decentralised system. This inevitably puts the Muslim community at odds with the civilian doctrine of voidance (*ibtal* or *fasakh*), which assumes that a transaction can be unwound and the parties restored to their contractual environment prior to entering into the contract. Second, pseudonymity: parties are referenced by alphanumeric cryptographic addresses and not by legal names, making it more difficult to establish contractual capacity, identity fraud and service of process. Third, automaticity: when the contract self-executes when the coded conditions are met, without any additional human will at the time of its execution, one might ask whether the execution of the contract is a new act of consent or a mere mechanical carrying out of a previous consent. Fourth, cross-border operation: the blockchain is a non-physical undertaking and choice of law analysis is crucial and practically challenging.

However, there is a distinction between 'pure' smart contracts wherein the entire contract, as

opposed to a subset of clauses, is expressed in executable code, and 'hybrid' or 'smart legal contracts' in which some clauses are expressed in natural language and the rest are expressed in executable code. The English Law Commission's 2023 Report was right to note that the latter category poses doctrinal challenges of a different kind and is less likely to be the subject of debate. Pure smart contracts, especially those that launch decentralised finance (DeFi) protocols, non-fungible tokens (NFTs) and decentralised autonomous organisations (DAOs), are the most difficult to handle.

2.2. Classical Consent Theory in Jordanian and Emirati Law

The Jordanian Civil Code (JCC) and the UAE Civil Transactions Law (UAE CTL) are codified statements of a civilian tradition that was balanced with Shari'a principles. A contract, according to Article 90 JCC, is the convergence of the offer of one of the contracting parties with the acceptance of the other in the form of causing the effect of the two on the subject of the contract. Article 141 UAE CTL also states that the formation of a contract occurs when there is "meeting of offer and acceptance. Both stipulations are a classical doctrine of Islamic jurisprudence, the 'aqd (عقد), which determines that rida (رضا) is the animating spirit of any binding obligation.

The importance of consent to the doctrine is also reflected in the rules on incapacity. If one of the contracting parties is not legally competent (ahliyya, أهلية) due to his minority, insanity or legal prohibition, then there are two possibilities: either the contract is void (batil, باطل) or voidable (qabil lil-ibtal, قابل للإبطال), depending on the extent of his incapacity. This is not a perfect analogy to what would be the case of an automated algorithmic agent, which bears no legal personality and has no biological attributes that would give it capacity under either system.

The defects of consent that are recognised by both the codes are: (i) error or mistake (ghalt, غلط); (ii) fraud or misrepresentation (tadlis, تدليس); (iii) duress or coercion (ikrah, إكراه); and (iv) in the UAE CTL, exploiting advantage (ghabn fahish ma'a taghreer, تغير مع فاحش غبن). Each defect is exercised on the basis of the subjective will of a natural person. Neither was designed with algorithmic agents in mind, nor has either legislature passed provisions that explicitly consider smart contracts in relation to the validity of contractual relationships.

2.3. The Applicable Legislative Framework

The primary legislative sources governing this analysis are as follows. In Jordan: the Civil Code No.

43 of 1976 (as amended); the Electronic Transactions Law No. 85 of 2001 (ETL-Jordan); and the Electronic Commerce Law No. 17 of 2015 (ECL-Jordan). In the UAE: Federal Law No. 5 of 1985 (Civil Transactions Law, UAE CTL, as amended); Federal Law No. 1 of 2006 on Electronic Commerce and Transactions (UAE ECL); Federal Decree-Law No. 26 of 2020 (UAE Companies Law); and the ADGM Electronic Transactions Regulations 2021, together with DIFC Law No. 2 of 2017 (Contract Law). International benchmarks include: the UNCITRAL Model Law on Electronic Commerce (1996); the UNCITRAL Model Law on Electronic Transferable Records (2017, MLETR); and the UNIDROIT Principles of International Commercial Contracts (2016 edition).

It is notable that neither the ETL-Jordan nor the UAE ECL explicitly addresses smart contracts. The ETL-Jordan Article 2 defines an 'electronic record' broadly as "information generated, communicated, received or stored by electronic means" and Article 16 provides that an offer and acceptance may be expressed electronically, but neither provision anticipates self-executing code. The UAE ECL Article 4 similarly provides for electronic signatures and records without engaging the self-executing character of smart contracts. The ADGM is the sole Arab jurisdiction to have explicitly recognised smart contracts, through its Electronic Transactions Regulations 2021, which provide in Regulation 3 that a contract shall not be denied legal effect solely because it was formed or performed by an electronic agent.

3. DEFECTS OF CONSENT APPLIED TO SMART CONTRACTS: A COMPARATIVE ANALYSIS

3.1. Error And Mistake

3.1.1. The Doctrine in Jordan

Articles 148–155 JCC codify the doctrine of operative mistake (ghalt mu'aththir). Article 148 JCC provides that a contract may be annulled where the mistake relates to the substance of the thing contracted upon, or to an attribute of the thing which, in the common judgment of persons, is principal in its nature. Article 150 JCC requires that the error be one the other contracting party was or should have been aware of. Article 151 JCC further specifies that a common mistake shared by both parties may render the contract void rather than merely voidable.

The Jordanian mistake doctrine is difficult to apply to smart contracts. Imagine a party communicating with a smart contract that has some kind of bug – a mistake in the written code that lets

the contract operate in a way that is different from what the two parties intended. Does this amount to an "operative mistake" under Article 148 JCC? The solution is analytically complicated. The 'thing contracted upon' in a smart contract is the performance provided by the code; if the code fails to provide the performance, due to a programming mistake, there is a plausible argument to mistake as to the subject-matter. But it was drafted with tangible objects and identifiable services in mind and Jordanian courts have not yet interpreted Article 148 JCC with respect to algorithmic code. This gap has now started to be filled with academic commentary by Sarhan (2020) and Al-Qudah (2022), but there remains no decision by the courts.

Another issue is with 'oracle failures' where a smart contract relies on an external information feed (oracle) which supplies incorrect information and the smart contract runs in a way that was not intended by either party. Article 148 JCC requires the mistake to be connected to an attribute of the thing contracted upon that existed at the time of the formation of the contract. If an error is made in formation of an order and a failure to perform the order occurs after the order is formed, it may not be a defect of consent in the strict sense, but rather an intervening impossibility under Article 247 JCC, which concerns frustration. The consequences of this are different: frustration leads to prospective rescission of the contract; mistake results in annulment with restitution.

3.1.2. *The Doctrine in the UAE*

Article 185-198 are covered by the UAE CTL. Article 185 UAE CTL states that the contract shall be voidable on the contracting party's part whenever there is a mistake in the nature of the contract, or whether the contracting party has made a mistake in the identity of the thing contracted for, or a mistake as to the identity or attribute of the other party (where the basis of the contract is the identity or attribute of the other party). The party who seeks annulment under Article 186 UAE CTL must also have been "grossly negligent" in coming to the conclusion that the other party is not entitled to annulment.

One of the most significant issues in the context of smart contracts is the good faith requirement of Article 186 UAE CTL. The common mistake in DeFi ecosystems – and one that happens regularly, because alphanumeric address strings are similar – is when a user sends the funds to the wrong address. Can the user be considered non-negligent? Courts using Article 186 UAE CTL would be expected to

consider whether the address-verification defenses were used for the typical user. In the parallel case of electronic banking errors, the UAE Courts of Cassation have determined that there is a "high duty of care" imposed on users in an automated environment (Dubai Court of Cassation, Petition No. 284 of 2018). In a similar vein, UAE courts could rule that a party that enters into a transaction with an untested smart contract without studying the smart contract code is grossly negligent under Article 186, which would preclude them from seeking annulment.

The UAE has also grappled with the distinct concept of 'harmless mistake' (*ghalt ghayr mu'aththir*) in Article 190 UAE CTL, which preserves the contract where the error goes only to a secondary attribute of the subject-matter. This provision might apply where a smart contract executes a transaction in a slightly different denomination or time than anticipated, but where the overall commercial objective is achieved. Distinguishing material from immaterial mistakes in the context of code-driven execution requires courts to engage in technical code-reading, a capacity that conventional civil benches do not possess.

3.1.3. *Comparative Observations*

Both Jordan and the UAE require that a legally operative mistake be: (a) material, relating to the essence or a principal attribute of the subject-matter; (b) not the result of gross negligence on the part of the mistaken party; and (c) either known or knowable to the other party (in Jordan) or a common error (in both). In the smart contract context, these requirements prove difficult to operationalise. The 'other party' may be the deploying developer often anonymous who may have ceased involvement with the contract after deployment. There may be no 'other party' in the human sense at all, where the contract interacts autonomously with other contracts in a DeFi protocol.

Neither jurisdiction has adapted its mistake doctrine to account for the technical distinction between a mistake in the parties' intentions (consensus ad idem failure) and an error in the code's execution of correctly formed intentions (a programming defect). The former is a defect of consent in the classical sense; the latter is more analogous to a defect in the medium of performance. This doctrinal gap argues strongly for legislative intervention that draws the distinction explicitly.

3.2. *Fraud and Misrepresentation*

3.2.1. *The Jordanian Framework*

Fraud (tadlis) under Article 137 JCC requires proof of (i) a deliberate act of deception or concealment; (ii) which induced the other party to contract; and (iii) which, if it had not been present, the other party would not have contracted. Article 137(2) JCC broadens the liability to third-party fraud if the other contracting party was aware of it or ought to have known of it. The standard is subjective: Jordanian courts determine whether the particular claimant, as he or she is, and in his or her situation, was deceived. Article 363 JCC does not exclude damages for fraud.

Smart contract fraud can manifest itself in many different ways that become increasingly complex. The first and most obvious is misleading terms related to a contract deployment in the promotional material attached to a contract, such as false statements on the functionality, return rates or security audits of a contract that cause a person to enter into a transaction. This 'off-chain' fraud is easy to map back to Article 137 JCC. The inducement is a statement outside of the code; the code just carries out the transaction as a result. The problem is that it can be coded such that it performs the exact same actions as advertised in the fraudulent promotional offers, and the fraudster usually isn't the person deploying the code, which is why they haven't claimed it in the promotional copy, this is known as a 'rug pull'.

The second type of fraud is 'on-chain fraud' which involves malicious or fraudulent code with hidden functions 'backdoors' that allow the deployer to misdirect funds. From the doctrinal perspective the issue arises whether an absence of a contractual term is a fraud under Article 137 JCC. Jordanian courts have ruled that hiding of any kind of material defect in the subject-matter of a sale contract constitutes a tadlis (Jordanian Court of Cassation, Judgment No. 1234/2015). Likewise, the inclusion of a "back door" function in the smart contract that had a tangible effect on the rights of the counterparty would be deemed fraudulent concealment. For the claimant, however, they have to establish scienter, or the intent to deceive, in concealing the function.

In the blockchain, it is epistemologically difficult to establish the intent. Blockchain transactions are deterministic and verifiable, but not necessarily intentional: a pattern of transactions could be the result of either deliberate fraud or an inadvertent programming mistake. Jordanian law offers no clear direction on how to determine intent through digital action, nor is the current legal framework for evidence (Evidence Law No. 30 of 1952) geared towards blockchain forensics.

3.2.2. The Emirati Framework

The issue of fraud and misrepresentation is part of the overarching consent-defect concept under Article 185 UAE CTL. The provisions are more specific in the case of fraud (tadlis) and exploitative advantage (ghabn) in Articles 213-215 UAE CTL. Article 213 UAE CTL states that a contract can be cancelled if fraudulent means are used by the other party to enter into a contract that the party otherwise would not have entered into. The DIFC Contract Law (Law No. 2 of 2017, DIFC CL) offers a more up-to-date and commercially sophisticated regime: Article 40 DIFC CL offers a remedy for fraudulent misrepresentation, Article 41 DIFC CL a remedy for negligent or innocent misrepresentation.

There's another layer on the UAE's financial regulatory framework. The Securities and Commodities Authority (SCA) has announced in Decision No. 23 of 2020 regarding Crypto Assets that some digital tokens are securities and therefore, their promotion and sale would fall under anti-fraud provisions similar to the UAE Federal Law No. 4 of 2002 on Anti-Money Laundering. If a security token is being deployed by a smart contract, the SCA regulatory framework can fill in the gaps of the civil law fraud provisions and may offer administrative enforcement options.

In line with the ADGM Virtual Asset Framework (introduced in 2018 and updated in 2022), the ADGM Financial Services and Markets Regulations 2015 (ADGM FSMR) also cover financial promotions related to virtual assets. The ADGM FSMR deems any financial promotion which features a false or misleading statement to be a regulatory offence, which is separate and apart from the consent-vitiation analysis under contract law, irrespective of whether the statement is made in the context of a financial promotion for a virtual asset.

3.2.3. Comparative Observations

There are key similarities and differences between the Jordanian and Emirati fraud doctrines. While there are some similarities, there are some differences between the Jordanian and Emirati fraud doctrines. Under the UAE framework, which is supplemented by DIFC and ADGM law, there is a more graduated approach to misrepresentation liability including negligent and innocent misrepresentation (DIFC CL Articles 40-41), addressing a significant omission from the JCC that only allows annulment for deliberate fraud. In the context of smart contract, the liability under DIFC CL Article 41 for negligent misrepresentation may be a more practically workable and available remedy than the Jordanian

standard, as misrepresentation can be caused by automated marketing algorithms or even by content generated by artificial intelligence.

While the UAE (outside the special arrangements for DIFC/ADGM) has incorporated some provisions that specifically refer to 'algorithmic fraud' (the situation where a smart contract is actually programmed to mislead users with whom it trades or interacts, such as through front running or 'flash-loan' arrangements that systematically disadvantage other parties), neither Jordan nor the UAE have adopted measures on this specific subject. Classical fraud doctrine relies on the idea of intent to deceive, and it is quite problematic to attribute intent in the case of mechanical deception embedded in code under both legal systems.

3.3. Duress And Coercion

3.3.1. Jordan

Articles 138–143 JCC govern duress (ikrah). Article 138 JCC provides that a contract is voidable where one party is compelled by the other or a third party with the other's knowledge to contract through unlawful threats. Article 139 JCC requires that the threat be of an imminent serious harm against the person, honour, or property of the contracting party or their close family members, and that the threatened party had no available legal remedy at the time. Article 140 JCC preserves economic duress as a separate ground where the threat is of harm to property of significant value.

The application of duress doctrine to smart contract contexts is constrained by the requirement of an identified human threatener. In the paradigm smart contract transaction, the user interacts with code that offers no alternatives: the code's terms are presented on a 'take it or leave it' basis, and the user either transacts or does not. Commentators have debated whether contract terms that are adhesionary and practically unavoidable such as the terms embedded in a widely used DeFi protocol might constitute economic duress in a sufficiently extreme case. The orthodox Jordanian view, drawing on Court of Cassation Judgment No. 892/2019, requires an identified party who made the unlawful threat; the coercive character of a market structure would not suffice.

The more legally salvageable case is 'ransomware duress' when the bad guys gain access to the victim's private bit of crypto and use it to coerce the victim into transacting with a smart contract by threatening to destroy the victim's other digital assets. This is a scenario that meets the requirements of Article 138 JCC for being an identified human threatener,

imminent serious harm (destruction of valuable digital property), and being a legally improper threat. In court, however, evidence of such coercion is extremely difficult to establish via digital forensic evidence, tracing the key compromise, the identity of the attacker and the causal relationship between the threat and the transaction, which all are very difficult under the current Jordanian Evidence Law.

3.3.2. The UAE

Articles 199–205 UAE CTL first explicitly articulate the concept of duress (ikrah), broadly in the same terms as in the JCC but with an additional clause in Article 203 UAE CTL that a threat to property will suffice if the threatened party has no means to protect itself from it, but the threat must be serious, present, and the property threatened must be property. The UAE position is similar to the Jordanian, but with two differences concerning smart contracts. First, the UAE CTL makes it explicit in Article 204 that the following is a basis for reducing obligations or rescission: "If an offending party, exploiting the necessity of or weakness of the other party, obtains an unfair advantage, then such economic exploitation (ghabn fahish ma'a taghreer) is a basis for reducing obligations or rescinding. This is a possible solution when the deployer is financially savvy, and the smart contract is used to extract supra-competitive returns from financially less-savvy users, an example of which is a 'predatory' smart contract. There is no direct equivalent of the Jordanian law.

Second, the DIFC CL Article 42 created a separate cause of action for relief on the grounds of 'unconscionability' arising when the terms of a contract are grossly unfair to one party who is in a position of marked inequality. This doctrine, which is rooted in Common Law is applicable within the opt-in jurisdiction of the DIFC and may be well suited for cases where the threatener is not a human, but rather an objective unfairness of the outcome is pursued. A number of DIFC Court rulings have interpreted the doctrine of unconscionability in relation to standard-form digital contracts, with the most recent case discussed by Al-Khatib (2022) highlighting that agreements that are not transparent enough might meet the 'gross unfairness' criterion.

3.4. Misrepresentation And Exploitative Advantage

In addition to the classic threefold framework of error, fraud and duress, both jurisdictions acknowledge other reasons why consent can be vitiated that warrant consideration in smart contract

environments.

The UAE CTL Articles 213-217 are concerned with the gross inadequacy of exchange as a standalone fault in conjunction with deception or exploitation of an incapacitated party. There is no exact equivalent to this doctrine in the JCC, but rather in the jurisprudence of Hanbali and Maliki. It is an interesting application to smart contracts: the difference between the expected price of a trade and the actual price at which the transaction is executed is known as 'slippage' in automated market-making protocols (AMM) on blockchain-based decentralized finance (DeFi) platforms, and can lead to suboptimal exchange rates if liquidity is thin or if malicious actors are at play. In this case, where the conditions existed at the time of the contract and the deployer knew of those conditions, the *ghabn* doctrine may provide some relief even if there is no evidence of intentional fraud.

The closest parallel to the doctrine of lesion in Jordan is the doctrine of *ghust* as it applies to certain types of contracts (sale and partition) as contained in Articles 351-356, JCC. It is only applicable in a limited way for smart contract purposes. In the future, reform could be usefully incorporated into Jordanian law, but with particular emphasis on how it applies to algorithmically executed exchange contracts, the UAE's wider *ghabn* doctrine.

4. EVIDENTIARY CHALLENGES IN PROVING DEFECTS OF CONSENT ON THE BLOCKCHAIN

4.1. The Immutability Problem

The most distinctive evidentiary feature of blockchain transactions is their permanence: every on-chain transaction is recorded immutably and is publicly verifiable by anyone with access to the blockchain explorer. This characteristic simultaneously aids and impedes the proof of defect-of-consent claims. On the one hand, it means that the transaction record itself cannot be disputed a claimant seeking to prove they transacted with a particular contract address on a particular date has a perfect and unfalsifiable record. On the other hand, immutability means that the 'unwinding' of a transaction that forms part of the relief available upon annulment of a contract under Article 165 JCC or Article 206 UAE CTL cannot be achieved through the blockchain itself. A court order granting restitution may be legally valid but technologically unenforceable against a decentralised contract with no identifiable human counterparty.

Jordan's Evidence Law No. 30 of 1952 (JEL)

establishes a hierarchy of evidence that places documentary evidence above testimonial evidence. Article 33 JEL provides that electronic records have the same evidential weight as paper documents where their authenticity is established in accordance with the Electronic Transactions Law. The ETL-Jordan Article 14 stipulates that an electronic record satisfies the 'writing' requirement in any legal provision that requires a document to be in writing, provided it is accessible and retainable. These provisions, drafted with ordinary electronic records in mind, can be construed to accommodate blockchain transaction logs the Amman Court of First Instance so held in an unreported 2021 decision concerning a cryptocurrency dispute but no authoritative appellate guidance exists.

4.2. Authentication And Expert Evidence

Technical expertise, which is not necessarily available in civil courts in either Jordan or the UAE, is required to prove the actual code that was run as a result of the smart contract. The code is not an easy-to-understand language like English for legal professionals, but instead is written in Solidity (Ethereum's main language for smart contracts). Qualified blockchain forensic experts are needed to identify a potential backdoor function, show that a specific code branch was activated, or trace the flow of funds in both the interacting contracts and identified backdoor function.

Within Jordan, the expert evidence is regulated by the following: Articles 69-79 JEL and Experts and Translators Law No. 40 of 1958. Experts can be appointed by a party or, at the court's own request, pursuant to Article 69 JEL. In Jordan, however, there are no accredited categories of 'blockchain forensic expert' nor any standards for blockchain expert reports to be admissible. The court is thus required to evaluate the credibility of the expert within the context of Article 33 JEL, which states that courts are not required to take judicial notice of expert opinions, but must take them into account when arriving at decisions on the issue of credibility. Given the lack of standards, it is unclear whether courts will give more weight to blockchain analysis by an internationally accredited firm or a local consultant.

The UAE offers a more matured, but still partial, picture. UAE Evidence Law was issued by Federal Decree-Law No. 35 of 2022 as the replacement for the previous Federal Law No. 10 of 1992, and gave specific treatment to electronic evidence in Article 53-58. According to Article 53 UAE Evidence Law, documents that are transmitted, produced, communicated, or stored electronically are

admissible as evidence if the integrity of the documents is proved and the source of the documents is proved to be from a reliable source. The UAE Evidence Law, Article 55, allows technical experts in electronic matters to be appointed by courts and the Ministry of Justice has a panel of certified e-forensics experts. The DIFC Courts have a more advanced practice, set out in Practice Direction No. 2 of 2016 (Technology-Assisted Review) and the DIFC Courts' Guide to Electronic Documents; to guide the handling of large volumes of digital evidence and the courts have appointed blockchain experts in several reported cases.

4.3. Pseudonymity And Identity Attribution

One of the most basic concerns that arises in smart contract litigation is what is the identity of the legal entity behind a given blockchain address. Blockchain addresses are alphanumeric cryptographic hash strings that don't necessarily refer to their associated users. In order to sue the deployer of a fraudulent smart contract, a claimant will have to prove that an address on a specific blockchain is indeed controlled by the defendant.

This attribution challenge has several dimensions. On-chain analysis tracing the flow of funds between addresses can in some cases identify exchanges or service providers through which the defendant deposited or withdrew funds. Where those exchanges are licensed and operating in Jordan or the UAE, they may be subject to subpoenas or regulatory information requests that would reveal the customer's identity. Jordan's Anti-Money Laundering Law No. 46 of 2007 (as amended by Law No. 13 of 2021) requires licensed financial institutions and exchange operators to maintain know-your-customer (KYC) records that link wallet addresses to natural persons. The UAE's Virtual Asset Regulatory Authority (VARA), established in 2022, imposes similar requirements on licensed virtual asset service providers under the Dubai Virtual Assets Law No. 4 of 2022 (Dubai VAL).

Where the defendant operated through a decentralised exchange or through privacy-enhancing technology such as 'mixing' services, attribution may prove impossible without intelligence cooperation from foreign authorities. Neither Jordan nor the UAE has a bilateral treaty specifically addressing blockchain asset recovery, though both are members of the Egmont Group of Financial Intelligence Units and cooperate on anti-money-laundering intelligence sharing. The 2021 Jordan-UAE bilateral investment treaty (BIT) provides for cooperation in investor protection but

does not specifically address digital asset disputes.

4.4. The Burden and Standard of Proof

Both Jordan and the UAE apply a civil standard of proof the balance of probabilities to contract disputes. However, fraud claims require proof of intent, and courts in both jurisdictions have historically required a high degree of probability before finding fraudulent intent. Article 3 JEL codifies the general principle that each party bears the burden of proving what they allege. In defect-of-consent cases, the burden lies with the claimant to establish the defect on the balance of probabilities; the defendant must then prove either that the defect is not operative or that the claimant had knowledge of it.

Smart contracts complicate burden allocation in at least two respects. First, the claimant may lack access to the information necessary to establish the defect at the time of filing the contract code may have been deliberately obfuscated, or the deployer's identity may be unknown. Conventional pleading requirements may need adaptation to accommodate what might be called a 'preliminary discovery' phase in which basic identifying and technical information is compelled before the substantive claim is pleaded. Second, where the alleged defect consists of a coding error or a hidden function in the contract, the technical analysis required to establish the defect lies entirely within the defendant's knowledge if the defendant is the deployer. An evidentiary rule imposing an evidential burden-shifting in such cases analogous to the *res ipsa loquitur* doctrine in tort might be justified.

5. INSTITUTIONAL LANDSCAPE FOR SMART CONTRACT DISPUTE RESOLUTION

5.1. Jordan

Jordan's commercial courts established under the Magistrates' Courts and High Courts Regulations handle contractual disputes, including electronic commerce matters, under the general civil procedure regime. The Electronic Crimes Law No. 27 of 2015 (ECrL) criminalises certain digital offences relevant to smart contract fraud (unauthorised access, manipulation of electronic data), and criminal proceedings under the ECrL may run concurrently with civil contract claims. However, there is no specialised court or panel with designated expertise in blockchain or smart contract disputes.

The Centre for Conciliation and Arbitration of Jordan (Jordan CAC) established by Arbitration Law

No. 31 of 2001, provides arbitral services in commercial arbitrations, including technology arbitration. There are no specific rules in the Jordan CAC that relate to smart contract disputes or blockchain evidence; however, they do allow for the appointment of a technical expert. This is especially true for smart contract disputes, which are increasingly common and where specific procedural rules, based on the 2019 Task Force Report on Digital Assets and New Technologies of the ICC, could be useful for the Jordan CAC.

5.2. The UAE: DIFC And ADGM

The UAE's dual-track judicial architecture federal courts for onshore disputes and independent common-law courts for the DIFC and ADGM free zones provides a more differentiated institutional landscape. The DIFC Courts apply English common law supplemented by DIFC legislation, and have jurisdiction over disputes arising from DIFC-registered entities or where parties have opted into DIFC jurisdiction by agreement. The DIFC Courts' Small Claims Tribunal (SCT) handles dispute up to USD 500,000 and has adjudicated several cryptocurrency disputes.

More significantly, the ADGM Courts have jurisdiction over entities registered in the ADGM free zone, which has positioned itself as the UAE's leading smart contract and digital asset jurisdiction. The ADGM Electronic Transactions Regulations 2021 (ADGM ETR) explicitly recognise smart contracts in Regulation 3: "A contract shall not be denied legal effect or enforceability solely on the grounds that an electronic agent was used in its formation or performance." The ADGM ETR further provides in Regulation 7 that the output of an electronic agent binds the principal in whose name the agent operates, unless the principal can demonstrate that the electronic agent acted outside its authorised parameters a provision that directly engages the duress and error analysis above.

The Virtual Assets framework of the ADGM,

which was revised in 2022 to comply with the Financial Action Task Force (FATF) Recommendation 16 on virtual asset transfers, also contains investor protection provisions such as mandatory disclosures of smart contract-based financial products. The conduct of the non-compliance of these disclosure requirements will give an additional cause of action apart from the UAE CTL's consent-defect analysis, thus alleviating the burden on the claimant who has suffered losses due to the defective smart contracts.

5.3. Online Dispute Resolution and Arbitration

Smart contract disputes are cross-border and pseudonymous, which makes traditional litigation, where personal service of process, court attendance, and judgment enforcement against located assets are necessary, extremely inappropriate. An alternative and potentially more effective is online dispute resolution (ODR). UNCITRAL Technical Notes on ODR (2017) suggest that ODR platforms for e-commerce disputes should include provisions for technology neutral, cost-effective and expeditious resolution.

The Jordanian Centre for Electronic Arbitration and Conciliation (JCEAC), which was provided for under the Electronic Commerce Law No.17 of 2015, has not been fully implemented. The Dubai Courts' 'Reconcile' platform and the published ADGM Rules of Digital Dispute Resolution (2021), both of which are available in the UAE, allow for the resolution of smart contract disputes. The ADGM Digital Dispute Resolution Rules are especially innovative as Rule 2 allows for the execution of an arbitral award via an on-chain 'arbitral smart contract' which, with the consent of both parties, can automatically execute an award. This mechanism significantly reduces the enforcement gap discussed above, but does so in the context of ex ante consent, which is the dimension that can be compromised in the scenarios analysed in this article.

6. COMPARATIVE SUMMARY

Table 1: Comparative Legal Framework for Defects of Consent in Smart Contracts (Jordan, UAE, And International Standards).

Criterion	Jordan (Civil Code 1976)	UAE (Civil Transactions Law 1985)	CRPD / UNCITRAL Standards
Governing Legislation	Civil Code No. 43 of 1976, Arts. 126-167	Federal Law No. 5 of 1985, Arts. 185-240	UNCITRAL Model Law on E-Commerce; UNIDROIT Principles
Definition of Contract Formation	Offer and acceptance; mutual consent expressly required (Art. 90)	Offer and acceptance; consent may be electronic (Art. 141)	Party autonomy; electronic agents recognized
Recognition of Smart Contracts	No explicit recognition; general e-transaction law applies	Electronic Commerce Law No. 1 of 2006; partial recognition	UNCITRAL recommends technology-neutral framework

Error / Mistake Doctrine	Arts. 148–155: error in subject-matter or identity voids consent	Arts. 185–198: mistake in the nature of the contract or person	UNIDROIT Art. 3.1.2: mistake must be fundamental
Fraud / Misrepresentation	Art. 137: fraud by concealment or deception voids consent	Art. 185: fraud renders contract voidable; damages available	UNIDROIT Art. 3.2.5: fraudulent representation
Duress / Coercion	Arts. 138–143: duress must be serious and imminent threat	Arts. 199–205: threats against person or property recognized	UNIDROIT Art. 3.2.6: threat of imminent serious harm
Algorithmic / Automated Consent	Silent; scholarly debate whether algorithm can consent	Art. 138 E-Commerce Law: electronic agent output binding on principal	UNCITRAL Art. 12: automated messages treated as originator's acts
Burden of Proof	Claimant bears burden; civil standard (Art. 3 Evidence Law)	Claimant bears burden; court may appoint expert (Art. 33 Federal Evidence Law)	No uniform standard; lex fori governs
Remedies	Annulment, restitution, damages (Arts. 160–167)	Avoidance, restitution, compensation (Arts. 206–210)	Avoidance, price reduction, damages (UNIDROIT Arts. 3.2.7–3.2.15)
Enforcement Gap	No specialized court or technical body for blockchain disputes	DIFC/ADGM courts offer partial competence; ADGM recognizes smart contracts	Arbitration/ODR encouraged but not mandatory

Source: Author's Comparative Analysis Drawing on Primary Legislative Sources.

7. BENCHMARKING AGAINST INTERNATIONAL STANDARDS

7.1. *Uncitral Framework*

UNCITRAL Model Law on Electronic Commerce (1996, MLEC) provides the basic principle of "functional equivalence", which holds that electronic records and electronic signatures should be treated as equivalent to paper records and handwritten signatures when they serve the same purpose. Article 11 MLEC provides that contracts formed by electronic agents are not to be denied validity solely on that ground. The UNCITRAL Model Law on Electronic Transferable Records (2017, MLETR) extends these principles to negotiable instruments and title documents, with direct relevance to tokenised assets managed by smart contracts.

Neither Jordan's ETL-Jordan nor the UAE ECL has fully implemented the MLETR, leaving a gap in the regulation of tokenised financial instruments. The MLETR Article 16 specifically addresses the 'single authoritative copy' requirement for negotiable instruments in a distributed ledger environment a directly relevant provision for NFT-based smart contracts. Jordan and the UAE would benefit from enacting MLETR-compliant legislation, which would simultaneously fill the regulatory gap and provide a framework within which the consent-defect doctrines could be applied with greater certainty.

7.2. *Unidroit Principles*

The UNIDROIT Principles of International Commercial Contracts (2016) address defects of consent in Articles 3.2.1–3.2.15 in a manner more readily adaptable to smart contract contexts than the civil code provisions of either Jordan or the UAE. Several features of the UNIDROIT approach merit specific attention.

Article 3.2.2 UNIDROIT provides that a party may avoid a contract for mistake if the mistake was of 'fundamental' importance to the decision to contract and the other party either caused the mistake, knew or should have known of it, or the other party had not yet relied on the contract. The lack of such a 'other party reliance' carve-out in both JCC and UAE CTL is especially relevant with respect to smart contracts, where the 'other party' (in this context, the wider liquidity pool in a DeFi protocol) would already have allocated resources in reliance upon the transaction.

Gross disparity is covered by Article 3.2.7 UNIDROIT, which provides that a party may refuse to perform under a contract where the other party has taken an excessive advantage from the dependency of the first party, his or her economic distress, urgency, improvidence, ignorance, inexperience or lack of bargaining skills. It is more comprehensive than either the JCC or UAE CTL version, and offers a doctrinal underpinning for attacking extractive smart contract designs like AMM protocols that set up a system that explicitly biases against retail-level users who do not engage in the fraud or duress that is classically recognized.

7.3. *Lessons From Common Law Jurisdictions*

The 2023 report "Smart Legal Contracts" by the English Law Commission found the current English law to be sufficiently robust to support smart contracts, but suggested the need for legislative clarity in certain areas, including mistake in code execution and automated agent authority. The report distinguished between 'code mistakes' (errors in the way agreed terms are expressed in code) and 'consensus mistakes' (failures of agreement at the formation stage) with implications for the appropriate remedy.

The Electronic Transactions Act (Cap. 69) of

Singapore. In 2021, contracts entered into by automated systems are also expressly included as valid and enforceable in the Singapore Academy of Law Digital Assets Working Group report, which amended the preceding section (88). Section 11B makes it clear that if the automated message system initiates or responds to an electronic message, the originator of the automated message system has contractual responsibility for the message subject to provision of any contrary agreement. This attribution rule is more explicit than either the attribution rule in Jordan or the one in the UAE which guides much of the above analysis and clarifies the agency attribution issue. Jordan and UAE would benefit from looking at similar measures.

8. RECOMMENDATIONS FOR LEGISLATIVE AND INSTITUTIONAL REFORM

8.1. Legislative Reform

First, both Jordan and the UAE should adopt technology-neutral amendments to their civil codes that clearly extend the doctrine of defect-of-consent to contracts entered into or executed via an automated electronic agent. These amendments should: (a) clarify the definition of 'electronic agent' in accordance with UNCITRAL MLEC Article 11; (b) limit the principal's contractual obligations and vulnerabilities to defect-of-consent claims to the same standards as for a human principal; (c) define what constitutes a 'coding error' as an operative mistake, where it means that execution differs from both parties' objectively ascertainable intent; and (d) include a dedicated provision on the smart contract backdoor function as a form of fraudulent concealment, thereby overturning any impression that the deployer's knowledge of a concealed function would waive the principal's consent liability.

Second, there should be specific provisions in both jurisdictions for the remedial consequences of vitiated consent in the context of smart contracts. An immutable blockchain cannot be technically countered with a classical remedy of annulment with restitution. Legislation should: (a) authorize courts to order monetary restitution instead of in-kind restitution for the value of assets unrecoverable from the blockchain; (b) allow for freezing orders of the other assets of the identified human deployer if blockchain restitution is not possible; and (c) establish a presumption that funds linked to the defendant's exchange accounts, through blockchain forensics, would be presumed to be proceeds of the

impugned transaction.

Third, Jordan should introduce a provision similar to the UAE CTL Article 204 that addresses the concept of 'exploitative advantage' but applies it to the context of algorithmic exploitation in automated exchange protocols. Where the deployer has superior algorithmic information to the market at the time of the execution of the provision and the ratio of exchange is significantly different from market rate, it may be considered an exploitative advantage for which the party affected may be entitled to some relief.

8.2. Evidentiary Reform

Specific evidentiary rules to be developed by both Jordan and the UAE include: (a) a presumption of authenticity for blockchain transaction records verified by three or more independent blockchain explorers; (b) accreditation requirements for blockchain forensic experts, similar to the standards established by the Blockchain Forensics Association and other similar entities; (c) a duty on the part of the deployer of the smart contracts in both jurisdictions to provide off-chain documentation identifying the deployer and explaining the core functionality of the code, which, if not met, would amount to an adverse inference in proceedings where a claimant has established a prima facie case of coding defect or hidden functionality; and (d) a burden-shifting provision in proceedings where the claimant has established a prima facie case of coding defect or hidden functionality, according to which the burden would fall on the smart contract's deployer to show that the code operated as described.

8.3. Institutional Development

The Jordan should create a special commercial electronic court in the commercial courts with judges trained in digital evidence and blockchain. Disputes involving the smart contract should see the establishment of standing panels of certified blockchain forensic experts by the chamber, and also an interim order such as freezing of assets and disclosure order against licensed exchanges for an expedient process.

The UAE should build on the existing smart contract framework of the ADGM to develop a voluntary smart contract registration process for smart contracts deployed by UAE based entities, disclosing the identity of the entity deploying the smart contract, its purpose in plain language and having the contract code audited by a competent party. Inconsistency would not be a requirement for the contract to be valid, but would be a rebuttable

presumption of good faith in the deployer for a subsequent proceeding arising from a deficiency in consent. If there is a *prima facie* defect, unregistered contracts would be deemed to be defective.

Jordan and the UAE should also agree to a bilateral protocol dedicated to smart contracts disputes, including: (a) mutual recognition of smart contract claims judgements; (b) coordinated response to transnational smart contract fraud; and (c) training of judicial officers and forensic experts. Such a protocol would be complementary to the bilateral investment treaty system in place and would be consistent with the UAE and Jordan's ongoing efforts to build a digital economy partnership under the UAE-Jordan Comprehensive Economic Partnership Agreement (CEPA) signed in 2023.

9. CONCLUSION

This article has shown that both Jordanian and Emirati law have the doctrinal ingredients for a remedy for error, fraud, duress, and exploitative advantage that are relevant to smart contracts, but that the classical statements of these remedies are not suitable for the technical realities of how smart contracts are executed on blockchain. The three central problems are that there is no 'other party' in the classical sense; that the blockchain transaction record is fixed and cannot be altered, which eliminates options for classical restitutionary remedies; and that an objective proof of an intention to deceive, knowledge of an error, or compulsion through the technical artefacts of the digital

execution is evident.

The UAE has progressed much further towards adopting the smart contract legal framework under the ADGM and DIFC legal frameworks, compared to Jordan. The ADGM Electronic Transactions Regulations 2021 and ADGM Digital Dispute Resolution Rules offer a blueprint for other Arab jurisdictions to consider in detail. The institutional deficit in Jordan is more pronounced and the need for targeted legislative action is more compelling.

Both jurisdictions would be well served by adopting international standards, in particular the UNCITRAL MLETR and the UNIDROIT Principles, which provide technology agnostic approaches that allow for both traditional "consens-based" and executed contracts. The proposed constitutional and Shari'a amendment, evidentiary modernisation, and capacity building of institutions in this article is not only possible within current constitutional and Shari'a framework, but also necessary to guarantee that the fast-paced commercialisation of smart contract technology will not outpace the available legal safeguards to parties conducting transactions in good faith.

With the introduction of blockchain technology in the financial sector, the real estate industry, and government administration, as Saudi Arabia's Vision 2030, the National Strategy for Advanced Technology 2031 in the UAE, and Jordan's Digital Economy Vision 2025 have transformed the Arab world, the questions raised in this article will become more and more practical. The law needs to change before the damage it aims to avert is irreparable.

REFERENCES

Primary Legislation and Official Documents

- Abu Dhabi Global Market (ADGM). (2021). Electronic Transactions Regulations 2021. Financial Services Regulatory Authority.
- Abu Dhabi Global Market (ADGM). (2022). Virtual Assets Framework Updated Guidance. Financial Services Regulatory Authority.
- Dubai International Financial Centre (DIFC). (2017). DIFC Contract Law (Law No. 2 of 2017). DIFC Authority.
- Dubai International Financial Centre (DIFC). (2016). Practice Direction No. 2 of 2016 (Technology-Assisted Review). DIFC Courts.
- Emirate of Dubai. (2022). Dubai Virtual Assets Law No. 4 of 2022. Government of Dubai.
- Hashemite Kingdom of Jordan. (1952). Evidence Law No. 30 of 1952. Official Gazette.
- Hashemite Kingdom of Jordan. (1958). Experts and Translators Law No. 40 of 1958. Official Gazette.
- Hashemite Kingdom of Jordan. (1976). Civil Code No. 43 of 1976. Official Gazette.
- Hashemite Kingdom of Jordan. (2001). Arbitration Law No. 31 of 2001. Official Gazette.
- Hashemite Kingdom of Jordan. (2001). Electronic Transactions Law No. 85 of 2001. Official Gazette.
- Hashemite Kingdom of Jordan. (2007). Anti-Money Laundering Law No. 46 of 2007 (as amended by Law No. 13 of 2021). Official Gazette.
- Hashemite Kingdom of Jordan. (2015). Electronic Commerce Law No. 17 of 2015. Official Gazette.
- Hashemite Kingdom of Jordan. (2015). Electronic Crimes Law No. 27 of 2015. Official Gazette.
- Securities and Commodities Authority (UAE). (2020). Decision No. 23 of 2020 on Crypto Assets. SCA.
- United Arab Emirates. (1985). Federal Law No. 5 of 1985 on Civil Transactions (as amended). Official Gazette.
- United Arab Emirates. (1992). Federal Law No. 10 of 1992 on Proof in Civil and Commercial Matters (repealed). Official Gazette.
- United Arab Emirates. (2006). Federal Law No. 1 of 2006 on Electronic Commerce and Transactions. Official Gazette.
- United Arab Emirates. (2022). Federal Decree-Law No. 35 of 2022 on Evidence in Civil and Commercial Matters. Official Gazette.

International Instruments

- United Nations Commission on International Trade Law (UNCITRAL). (1996). Model Law on Electronic Commerce. United Nations.
- United Nations Commission on International Trade Law (UNCITRAL). (2017). Model Law on Electronic Transferable Records. United Nations.
- United Nations Commission on International Trade Law (UNCITRAL). (2017). Technical Notes on Online Dispute Resolution. United Nations.
- UNIDROIT. (2016). Principles of International Commercial Contracts (4th ed.). International Institute for the Unification of Private Law.

Academic Sources

- Al-Khatib, M. (2022). Unconscionability and digital contracts in the DIFC: An emerging doctrine. *Arab Law Quarterly*, 36(4), 345–372.
- Al-Qudah, S. (2022). Smart contracts and civil liability in Jordanian law: An analytical study. *Journal of Legal and Economic Studies*, 14(2), 88–117. [In Arabic]
- Attiah, H. S. (2019). Consent and its defects in Islamic and civil law: A comparative analysis. *Arab Journal of Legal Sciences*, 11(1), 23–58.
- Clack, C. D., Bakshi, V. A., & Braine, L. (2016). Smart contract templates: Foundations, design landscape and research directions. *arXiv preprint arXiv:1608.00771*.
- De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code*. Harvard University Press.
- Durovic, M., & Janssen, A. (2018). The formation of blockchain-based smart contracts in the light of contract law. *European Review of Private Law*, 26(6), 753–772.
- English Law Commission. (2023). *Smart legal contracts: Advice to government* (Law Com Report No. 401). Law Commission of England and Wales.
- Giancaspro, M. (2017). Is a 'smart contract' really a smart idea? Insights from a legal perspective. *Computer Law*

- and Security Review, 33(6), 825–835.
- Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G., & Xu, X. (2018). On the representation of smart contracts in terms of legal contracts. In *Rule Technologies: Research, Tools, and Applications* (pp. 347–365). Springer.
- Hacker, P., Lianos, I., Dimitropoulos, G., & Eich, S. (Eds.). (2019). *Regulating blockchain: Techno-social and legal challenges*. Oxford University Press.
- Kaulartz, M., & Heckmann, J. (2016). Smart contracts Anwendungen der Blockchain-Technologie. *Computer und Recht*, 32(9), 618–624.
- Levi, S. D., & Lipton, A. B. (2018). An introduction to smart contracts and their potential and inherent limitations. *Harvard Law School Forum on Corporate Governance*.
- Mik, E. (2017). Smart contracts: Terminology, technical limitations and real world complexity. *Law, Innovation and Technology*, 9(2), 269–300.
- Raskin, M. (2017). The law and legality of smart contracts. *Georgetown Law Technology Review*, 1(2), 305–341.
- Sarhan, A. (2020). The legal nature of smart contracts: A critical analysis under Arab civil law. *Arab Journal of Comparative Law*, 8(1), 1–34. [In Arabic]
- Singapore Academy of Law. (2021). *Digital assets and applicable law: Report of the Digital Assets Working Group*. Singapore Academy of Law.
- Szabo, N. (1994). Smart contracts. Unpublished manuscript. Retrieved from <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>
- Werbach, K., & Cornell, N. (2017). Contracts ex machina. *Duke Law Journal*, 67(2), 313–382.
- Wright, A., & De Filippi, P. (2015). Decentralized blockchain technology and the rise of lex cryptographia. SSRN Working Paper. <https://doi.org/10.2139/ssrn.2580664>
- Zetsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2018). From FinTech to TechFin: The regulatory challenges of data-driven finance. *New York University Journal of Law and Business*, 14(2), 393–446.