Selangor Business Review

Vol. 10, No. 1, p. 181-198
30 June 2025
(ISSN 2716-5876)

BLOCKCHAIN, SMART CONTRACTS, AND DIGITAL SIGNATURES: LEGAL AND MANAGERIAL CHALLENGES FOR BUSINESS IN MALAYSIA

MOHD ASMADI MOHD ANGSOR[1*], NORAINI SARIYON[2], ARIFHA MOHAMAD[3], MOHD NAZIR MOHD ADI[4], NOOR ASLINDA ABU SEMAN[5]

[1,4,5]Johor Business School, Universiti Tun Hussein Onn, Malaysia
[2]Faculty of Technology Management and Business, Universiti Tun Hussein Onn, Malaysia
[3]Faculty of Business, Economics and Social Development, Universiti Malaysia Terengganu, Malaysia

*Corresponding Author: mohdasmadi@uthm.edu.my

Abstract: This paper explores the legal, business, and managerial implications of blockchain-based smart contracts and digital signatures within the Malaysian regulatory framework. Drawing on doctrinal legal analysis, comparative legal review, and qualitative case references, the study assesses the compatibility of smart contracts with existing statutes, including the Contracts Act 1950, the Digital Signature Act 1997, and the Electronic Commerce Act 2006. Beyond legal analysis, the research highlights how smart contract adoption impacts business processes, transaction efficiency, corporate governance, and risk management in Malaysian organisations. Benchmarking against Singapore, the European Union, and the United States reveals Malaysia's relative lack of statutory clarity and limited regulatory innovation, which poses challenges for businesses and policymakers alike. The study proposes a three-layer legal integration framework to facilitate smart contract deployment, ensuring legal certainty while enhancing business operational efficiency. It also introduces visual contract prototypes designed to improve comprehension for both legal practitioners and business stakeholders. The paper concludes with policy and managerial recommendations to modernise Malaysia's legal infrastructure, promote regulatory sandboxing, and establish professional standards for digital contracting. These contributions position the study at the intersection of legal scholarship, business innovation, and digital governance, offering insights for corporate leaders, legal professionals, and policymakers navigating Malaysia's evolving digital economy.

Keywords: Smart Contracts, Blockchain Technology, Digital Signatures, Contract Law

1. Introduction

In recent years, blockchain-based smart contracts have significantly reshaped various sectors, particularly finance and real estate, by enabling automated, cost-efficient transactions through distributed ledger technology (DLT). These innovations reduce reliance on intermediaries, streamlining processes and cutting transaction costs (Ghiro et al., 2021). Beyond cryptocurrency, blockchain applications have expanded into fields like the Internet of Things (IoT), highlighting their growing integration into diverse technological and commercial landscapes. As public familiarity with the term "blockchain" increases, so does societal engagement with its potential and limitations (Heidari et al., 2023).

Vol. 10, No. 1, p. 181-198
30 June 2025
(ISSN 2716-5876)

Blockchain, also known as distributed ledger technology, is the backbone of cryptocurrencies like Bitcoin and a foundational infrastructure for decentralised computing and financial systems (Swan, 2016). Among its most transformative developments is the emergence of smart contracts in the form of self-executing digital agreements with terms directly encoded into software. These contracts operate transparently and autonomously, promising increased efficiency, consistency, and anonymity while lowering transaction and legal costs (Giancaspro, 2017). Despite their technical sophistication, smart contracts raise significant legal concerns, particularly around enforceability within existing legal frameworks across jurisdictions.

The evolution of smart contracts has been closely linked to Blockchain's development. Initially limited in scope through early implementations such as Bitcoin, smart contracts became significantly more versatile with the launch of Ethereum, often dubbed Blockchain 2.0. This advancement enabled the creation of more complex contracts through blockchain-specific programming languages, expanding their utility in financial product trading, syndicated lending, and regulatory compliance (Pereira, 2019; Yufei, 2022). Nonetheless, integrating these digital mechanisms into conventional legal systems remains fraught with regulatory and conceptual challenges.

Legal scholars argue that the rapid adoption of smart contracts must be met with coherent regulatory frameworks capable of addressing their unique features, particularly decentralisation, anonymity, and immutability (Sugam Sharma et al., 2021). The convergence of law and technology is increasingly essential to ensuring smart contracts' security, enforceability, and alignment with established legal norms (Almarwani & Yacoub, 2023; Chau & Livermore, 2024). Smart contracts risk operating in legal vacuums without adequate legal adaptation, especially in jurisdictions grappling with digital transformation.

From a Malaysian legal perspective, these global developments prompt a critical re-examination of conventional contract law, especially regarding digital signatures, visual communication, and the integration of automated systems. As Malaysia navigates the digital age, academic and legislative attention must converge to ensure legal infrastructures evolve with technological innovation (Heng et al., 2021; De Brevern, 2023). This paper explores how emerging technologies such as Blockchain and smart contracts can reshape traditional contract law principles and proposes a contextualised framework for aligning them with Malaysia's legal system. Therefore, this paper seeks to answer the following research questions:

1. To what extent are blockchain-based smart contracts legally valid under Malaysian contract law?
2. How do Malaysian laws on digital signatures and electronic transactions accommodate the use of smart contracts?

2. Literature Review

2.1 Definition & Development of Blockchain

Vol. 10, No. 1, p. 181-198
30 June 2025
(ISSN 2716-5876)

Blockchain technology, first introduced through Bitcoin in 2008, has evolved significantly, advancing from a cryptocurrency foundation to a versatile platform with numerous applications across various industries, including finance, healthcare, and supply chain management. Initially conceptualised as a decentralised and cryptographically secured digital ledger, Blockchain enables the recording of transactions in an immutable manner, facilitating transparency and trust in environments previously reliant on centralised authorities (Agbo et al., 2019; Fen & Ai, 2021). This transformative potential has propelled Blockchain into three developmental phases: Blockchain 1.0, represented by Bitcoin; Blockchain 2.0, which introduced smart contracts exemplified by Ethereum; and the emerging Blockchain 3.0, aimed at broader social applications (Hongfang et al., 2019). Recent advancements combine traditional mathematical and computational techniques such as cryptography and shared databases, culminating in a robust consensus mechanism that empowers automated processes like smart contracts, allowing decentralised applications across various sectors (Markus & Buijs, 2022). As industries increasingly harness their capabilities, Blockchain presents innovative solutions while also posing new regulatory and operational challenges that demand careful consideration (Cumming et al., 2019).

Satoshi Nakamoto came up with the idea of Blockchain technology in 2008. A study from Nor Razinah Mohd Zain et al. (2019) shows that Nakamoto devised a way to make electronic transactions without relying on trust, using coins from digital signatures, which gives strong control over ownership. People use Blockchain technology to run Bitcoin, a digital money or cryptocurrency that has no real value but is still used. Later, the same technology kept improving, allowing it to be used in new ways and spread to other industrial systems. As the platform for making smart contracts, Blockchain is important as a digital ledger system to keep track of changes made to the smart contracts or their terms. This is why Blockchain is so important.

On the other hand, Ghiro et al. (2021) found that the Bitcoin cryptocurrency, which is the most popular use of the Blockchain, made the technology famous. In January of 2021, it set a new record for the amount of money it had in the market. Decentralisation, resistance to powerful cyberattacks, and the protection of users' privacy were all features of Bitcoin's Blockchain. Many research groups were excited about this. This passion resulted in several ideas about using the Blockchain in many applications, including Supply Chain Management, E-voting, Smart Grid, Healthcare, Banking, Smart Cities, and even Vehicular and Aerial Networks. Surveys will be conducted everywhere about how Blockchain is used in many ways to improve the Internet of Things (IoT). The wide range of applications makes the Blockchain seem like a universal technology, not just for cryptocurrencies but also for most IoT applications, which are vulnerable to many things.

2.2 Definition & Development of Smart Contract

Smart contracts are defined as self-executing contracts with the agreement terms directly written into code and were first conceptualised by Nick Szabo in the mid-1990s, highlighting the potential for automation in contractual agreements within digital environments (Zhixiang et al., 2023; Dixit et al., 2022). These contracts operate on blockchain technology, which provides a decentralised, transparent, and immutable ledger, ensuring that

Vol. 10, No. 1, p. 181-198
30 June 2025
(ISSN 2716-5876)

once the contract is deployed, its rules cannot be altered and its execution is reliable and verifiable. The development of smart contracts gained significant traction following the introduction of Ethereum in 2015, which facilitated their broader adoption through a robust programming framework that enables complex operations beyond simple transactions (Agbo et al., 2019). In the years since, smart contracts have been increasingly implemented across diverse sectors such as finance, healthcare, and supply chain management, accentuating their value in enhancing operational efficiency, transparency, and trust in automated transactions (Rustiana et al., 2022). However, the evolution of smart contracts has also surfaced challenges related to security, interoperability, and compliance with existing legal frameworks, necessitating ongoing research and development to harness their full potential while addressing associated risks (Dixit et al., 2022).

According to Giancaspro (2017), Szabo's concept of smart contracting drew more attention after his key work, "The Idea of Smart Contracts," was published in 1997. A purchase from a basic vending machine was characterised as a primitive kind of "smart contract" in this study since it involves the fully independent transfer of ownership of property, such as a food and beverage item or a can of drink, following receipt of a specified input, such as money. Smart contracts could be used for a variety of things, according to Szabo, including the automated transfer of digital property (such as shares) upon the occurrence of a specified event, motor vehicle immobilisation (where the vehicle would not operate unless the contract's security protocols were met), and peer-to-peer property lending (where the lent property would revert to the lender if the borrower defaulted on specified conditions).

Shuai et al. (2019) reveal that smart contracts are computer protocols that allow two or more parties to digitally negotiate, monitor, and implement contracts on the Blockchain. The study also shows that smart contracts are frequently placed on and secured by Blockchain and have several unique characteristics. To begin, the programmed code of a smart contract will be recorded and confirmed on the Blockchain, making the contract tamper-proof. Second, without centralised control or third-party coordination, a smart contract's execution is enforced among anonymous, trustless individual nodes. Third, a smart contract, like an intelligent agent, may have its own Bitcoin or other digital assets to transfer when certain conditions are met.

2.3 Legal Contract

A study by Chalkidis et al. (2017) states that legal texts called "contracts" describe what people agree to do. Many businesses, law firms, government agencies, and so on use contracts to do many different things, like ensuring people follow the rules. They need to be kept track of. For instance, law firms must tell their clients when their contract terms are about to end, or new laws affect their contracts. Huge contractors must keep track of the money they have agreed to pay. Tax authorities may have to pay more attention to contracts involving large amounts of money and many people involved. Many of these tasks can be done automatically by extracting specific parts of the contract, such as the end date, the contracting parties, and the agreed-upon payments. On the other hand, contract element extraction is still done mainly by hand, which is time-consuming and costly.

Vol. 10, No. 1, p. 181-198
30 June 2025
(ISSN 2716-5876)

To be legally binding, a contract must be signed by two or more parties who intend to alter their respective legal status. Some elements should be involved in a contract that can make the contract valid. The first element is agreement. To agree, there must be a serious offer that one person is making to another person. The other person must accept the offer without booking, and the agreement will be made. In addition, the parties might also agree on their own, without limitation or outsized influence, and should act from their free judgment. This offer can only be accepted by people or businesses that are legal under the law. The next element is consideration. Consideration can be defined as, usually, when making a contract legal, both parties must be interested in the contract. So, every party shall guarantee anything of worth to the other for them to be able to make a deal. The next element is competence and capacity. The parties must be competent in deciding whether or not to sign a contract. Suppose a party cannot understand the contract or is assumed to be unable to understand it. In that case, the party lacks the capabilities or potential to choose to enter into the contract.

The legal object and purpose are the following elements in a contract. The contract object and purpose must surely follow the law. A contract can also be imposed if the agreed-upon actions are illegal or immoral. The relevant legal authority is usually where the contract was made, where it was intended to be conducted, or the one mentioned in the contract. All the elements that have been stated are from the study by Governatori et al. (2018). The study also states that if a contract contains all of the above components. Hence, they are not defective (according to the contract's governing law) and are legally acceptable and binding on the parties. The agreement may be void or voidable if a component is lacking or defective. A void contract has no effect (cannot be executed), whereas a voidable contract has an effect that can be performed until a court ends it.

Governatori et al. (2018) also explain the lifecycle of a contract. The first stage of the lifecycle is negotiation and formation. If a legal entity has a "freedom to contract," it should be able to form any contract with any content. Contracts are generally made when one party makes an offer and the other accepts it. This usually happens when one party wants to make a deal with specific terms, and the other party agrees. Next, someone involved in a contract's lifecycle is contract storage and notarisation. A contract can be made by talking, shaking hands, or agreeing. This is true unless the law says a specific formality, such as writing, must be done before it can be made. However, unwritten contracts can be complex to prove. They must not be eyewitnesses or unreliable; the legal system may involve a writer's proof. Next is performance. Once a contract is made, it needs to be carried out. The parties need to do what they need to do to make sure the contract is carried out. Parties can either do the right things themselves or designate them to someone else, as long as it is allowed by the contract.

Other than that, monitoring and enforcement are also involved in the lifecycle. Each party will examine whether the other side has taken the necessary actions. Private enforcement persuades the other parties to do the necessary activities. Suggestions, encouraging words, or provocations to take measures, including resorting to court enforcement, may be involved. If one party fails to meet their responsibilities and acceptable circumstances exist, the other party might quit the arrangement and cease performing their actions. Depending on the circumstances, the innocent person may demand corrective or

Vol. 10, No. 1, p. 181-198
30 June 2025
(ISSN 2716-5876)

punitive damages and contract modification or resolution (termination). These procedures can be compelled by law or, in some cases, initiated voluntarily by the innocent victim. Next is modification. The sides could always agree to change the terms of the contract.

Under certain circumstances, one party may get out of a contract if the other party agrees to change the terms, for example, if compliance has become too complicated or if the agreement was made under duress. Even if one party cannot do what they agreed, the contract can still be changed or ended. Then, dispute resolution. The contract's validity, the understanding or assimilation of its aspects, infractions of its obligations, or how to deal with unpredictable events are some things that can happen when a contract is made. An adjudicative remedy, such as litigation or arbitration, is when a judge or jury decides the case's outcome. A consensual solution is when the parties try to devise a solution that everyone agrees on together. The last one in the lifecycle is termination. When all contractual duties have been fulfilled, when the parties agree to terminate the contract, or when the contract is nullified or settled, the contract is terminated.

In the wide-ranging world, contract law has always required the parties or companies to sign a document. With the rise of the electronic era, the electronic signature has emerged. According to Blythe's (2005) study, in the past, an electronic signature was defined as any letters, characters, or symbols shown by electronic means that the document was signed or accepted by a party to confirm a writing. Because it is more complicated than biometrics, the digital signature is considered a potential degree of security. Many laypeople mistakenly believe that a digital signature is simply a computerised reproduction of a handwritten signature. According to Chen and Xu (2010), digital signatures use cryptographic procedures to construct a series of symbols and codes that comprise the electronic password rather than using a handwritten signature or seal. This type of electronic signature can be verified using technical means. The digital signature on digital information resembles the anti-counterfeit handwriting signature. The sender can easily verify and ensure that the document was not amended after it was signed, ensuring the information's authenticity and integrity.

International standards organisations define a digital signature as extra details in the information on the unit, or some of the data elements in this data, or a password transformation that may be used to convert the recipient to confirm its integrity and protect the data sources from forging. Chen and Xu (2010) also conclude that there has been much growth in the digital signature industry. Security has many risks and crises because of how far development has come and because there are few security products with intellectual property rights. So, the next time we do research, we should work hard to make new information technologies that have their intellectual property rights and set up a security system for the information network. Digital signature technology needs to be improved even more, and much work should be done to improve the technology that helps keep digital signatures safe. Digital signatures are the next big thing in the field of information security. Under these conditions, it is important to keep improving the digital signature atmosphere facilities and deal with technical and legal problems in making digital signatures.

It is important to acknowledge the impact of technology on the formation, execution, and enforcement of contracts in the digital age. The advent of electronic and digital signatures

Vol. 10, No. 1, p. 181-198
30 June 2025
(ISSN 2716-5876)

represents a significant paradigm shift in how contracts are authenticated and validated. Unlike traditional signatures, which are typically handwritten and may require physical presence, electronic signatures can be created using cryptographic techniques that provide greater security and integrity. This shift allows parties to enter into contracts from virtually anywhere in the world, streamlining processes and reducing barriers to entry for contractual agreements (Shcherbyna et al., 2021). Furthermore, implementing digital signatures simplifies electronic document management. It enhances legal certainty, as these signatures hold the same weight as traditional signatures in courts, provided that legal frameworks acknowledge their validity.

Moreover, as contract law evolves, issues surrounding digital signatures and electronic contracts must be addressed to accommodate the changing landscape. Regulations governing these signatures must ensure compliance across different jurisdictions, as seen in the legal readiness of agreements in regions like Indonesia. There remains a need for comprehensive guidelines that clarify the legal status of digital interactions to mitigate risks associated with electronic contracting. The integration of blockchain technology also offers promising avenues for the future of contract enforcement by providing transparent, tamper-proof records that can automate and facilitate compliance with contract terms (Sánchez-Gómez et al., 2021). Consequently, it becomes paramount for legal scholars and practitioners to engage with these technological advancements actively and consider their implications on traditional contract principles, ensuring that legal frameworks can adapt and evolve to meet the demands of modern contractual relationships.

3. Methodology

This study discussed a structured three-pronged methodology comprising doctrinal legal analysis, comparative legal review, and qualitative case study analysis. This combination addresses smart contracts' legal, regulatory, technical, and communicative dimensions under Malaysian law. Each approach complements the others to ensure a holistic understanding of the topic.

3.1 Doctrinal Legal Analysis

A doctrinal legal method examines Malaysian statutory laws and legal principles relevant to contract formation, digital authentication, and electronic communication. The primary legislation analysed includes the Contracts Act 1950, particularly Sections 2(b), 10(1), and 14, which outline the legal requirements for offer, acceptance, consent, and lawful object in contracts (Nor Razinah Mohd Zain et al., 2019). These provisions are foundational in assessing whether smart contracts satisfy the traditional criteria of a valid agreement.

According to the prescribed sections of the Contracts Act 1950, as stated in the study by Nor Razinah Mohd Zain et al. (2019), the following are the most significant and pertinent provisions:

Vol. 10, No. 1, p. 181-198
30 June 2025
(ISSN 2716-5876)

i. Section 10 (1) Contracts Act 1950: all agreements are contracts if they are made with the free assent of contracting parties, for lawful consideration, and with lawful intent, and are not explicitly declared void.
ii. Section 2 (a) Contracts Act 1950 (offer): When one person indicates to another his desire to do or abstain from doing something to acquire the other's consent to the act or omission, he is said to propose.
iii. Section 5(1) Contracts Act 1950: withdrawal is permitted at any moment before the completion of acceptance communication.
iv. Section 2(b) of the Contracts Act 1950: Acceptance constitutes an unequivocal agreement to all of the terms of the offer
v. Section 2 (d) Contracts Act 1950: When the promisor, the promisee, or any other person acts or abstains from acting, or acts or abstains from acting, or promises to act or refrain from acting, something, such act, abstinence, or promise is referred to as a consideration for the promise.

The Contracts Act 1950's abovementioned rules must be strictly followed during the innovative contract process. This is critical to avoiding any contested issue that could bring the smart contract's participants before a court of law. The flow of the smart contracts is illustrated in Figure 1.

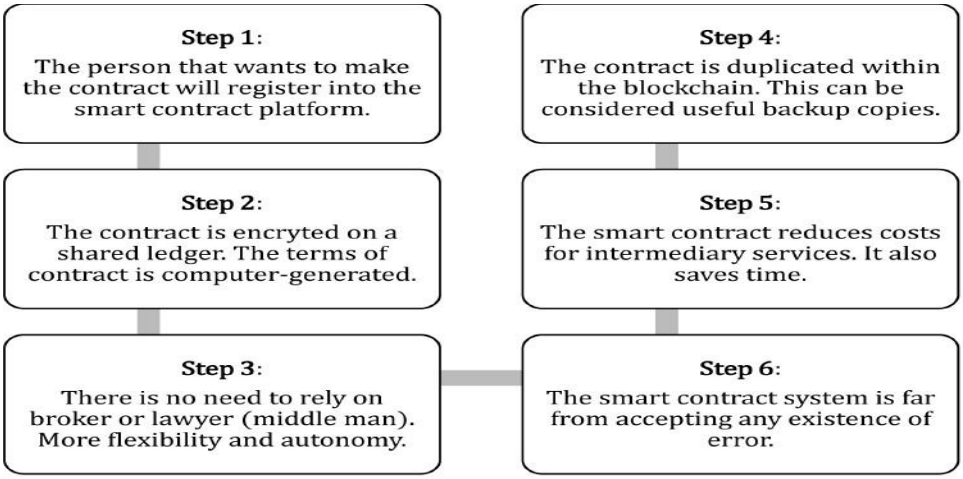

Figure 1. Flow of Smart Contracts (Nor Razinah Mohd Zain et al., 2019)

Malaysia has a broad and diverse legal framework indirectly supports the regulation and application of blockchain technology and smart contracts. According to Nor Razinah Mohd Zain et al. (2019), these legal instruments span multiple domains, as summarised in Table 1. While these laws are not enacted explicitly for Blockchain, they are a foundational basis for assessing its legal viability in the country.

Table 1. Overview of Malaysian Laws Relevant to Blockchain and Smart Contracts

Legal Domain	Relevant Laws/Frameworks
Banking and Financial Laws	- Financial Services Act 2013 - Islamic Financial Services Act 2013 - Development Financial Institutions Act 2002 - Money Services Business Act 2011 - Financial Technology Regulatory Sandbox Framework

Vol. 10, No. 1, p. 181-198
30 June 2025
(ISSN 2716-5876)

Security and Criminal Laws	- Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA) - Penal Code - CyberSecurity Malaysia Guidelines - Computer Crimes Act 1997 - Prevention of Corruption Act 1961
Consumer Protection Laws	- Consumer Protection Act 1999 *(proposed update for digital assets)* - Personal Data Protection Act 2010 - Consumer Protection (Electronic Trade Transactions) Regulations 2012
Digital and Multimedia Laws	- Electronic Commerce Act 2006 - Electronic Government Activities Act 2017 - Digital Signature Act 1997 - Digital Signature (Amendment) Act 2001 - Communications and Multimedia Act 1998 - Copyright Act 1987 - Trademarks Act 1976 - Patents Act 1983
Business and Competition Laws	- Companies Act 2016 - Partnership Act 1961 - Limited Liability Partnership Act 2012 - Contracts Act 1950 - Competition Act 2010
Taxation and Revenue Laws	- Income Tax Act 1967 - Guidelines on Taxation of Electronic Commerce - Goods and Services Tax Act 2014 - Proposed Digital Tax (announced post-2018)
Dispute Resolution Laws	- Mediation Act 2012 - Arbitration Act 2005 (Amended 2011) - The Rules of Court 2012
Shariah Compliance Considerations	- Oversight by the Shariah Advisory Council, focusing on Gharar (uncertainty), Maysir (gambling), and Riba (interest) for blockchain applications involving Ribawi commodities like gold and silver.

As reflected in Table 1, Malaysia possesses a broad spectrum of laws relevant to innovative contract applications. While there is no single legislation governing smart contracts, the Contracts Act 1950 remains the doctrinal cornerstone in determining validity and enforceability. Additional support is found in the Digital Signature Act 1997 and Electronic Commerce Act 2006, which provide statutory mechanisms for recognising electronic contracts and signatures. These instruments collectively suggest that smart contracts could be interpreted as legally valid under existing frameworks, provided they satisfy fundamental requirements such as mutual consent, lawful purpose, and digital authentication. At the same time, sector-specific laws—from consumer protection to Shariah compliance—introduce necessary legal constraints that competent contract developers must navigate.

3.2 Comparative Legal Review

To evaluate Malaysia's legal readiness for blockchain-based smart contracts, this study employs a comparative legal review involving three jurisdictions: Singapore, the European Union (EU), and the United States (US). These jurisdictions are selected due to their relatively mature and well-documented frameworks governing electronic transactions and digital contracts. They serve as regulatory benchmarks from which Malaysia may draw inspiration or caution, especially as it navigates the complexities of integrating decentralised technologies within a centralised legal system.

The comparison focuses on two core dimensions:
(1) the legal recognition of smart contracts, and
(2) the framework for digital signatures, which are often integral to executing smart contracts.

Table 2 summarises the relevant statutes and the extent to which each jurisdiction supports the enforceability of smart contracts and the validity of cryptographic signatures.

Table 2. Comparative Legal Provisions on Smart Contracts and Electronic Transactions

Vol. 10, No. 1, p. 181-198
30 June 2025
(ISSN 2716-5876)

Jurisdiction	Relevant Law(s)	Smart Contract Recognition	Digital Signature Framework
Malaysia	Contracts Act 1950, ECA 2006, DSA 1997	Implicit via ECA & Bar Council views	Covered under DSA 1997
Singapore	Electronic Transactions Act (2010)	Explicitly recognised	Recognised and standardised
European Union	eIDAS Regulation	Supported under digital trust services	Harmonised across member states
United States	UETA, E-Sign Act	Enforceable if it meets consent intent	Cryptographic and legally binding

This table reveals important distinctions. Malaysia's legal stance is indirect; smart contracts are not expressly mentioned in any statute, though the Electronic Commerce Act 2006 may be interpreted to cover such agreements. Similarly, the Digital Signature Act 1997 provides a structure for legally recognising electronic authentication, but it predates blockchain-based implementations and does not expressly accommodate them. Thus, the legal foundation exists but is outdated and ambiguous in scope.

In contrast, Singapore provides explicit statutory recognition of smart contracts under its Electronic Transactions Act 2010, which improves legal certainty and facilitates innovation. Likewise, the European Union's eIDAS Regulation sets out harmonised standards for electronic identification, ensuring cross-border legal interoperability—a crucial aspect for international blockchain-based transactions. The United States, through its UETA and E-Sign Act, adopts a more principles-based approach, enforcing digital contracts so long as they reflect clear intent and consent, regardless of the technology used.

From a methodological perspective, this comparative review allows the study to:

- Identify best practices (e.g., Singapore's legislative clarity, EU's interoperability focus),
- Highlight Malaysia's legal gaps (e.g., lack of explicit recognition, outdated digital signature laws),
- Provide recommendations for legal reform or regulatory sandboxing in Malaysia.

The comparative approach is beneficial in the absence of domestic case law on smart contracts, offering normative direction by examining what has already been tried or proven effective in other legal systems. It also enables mapping legal certainty vs technological innovation across different jurisdictions, which is crucial in fintech, insurtech, and e-government initiatives involving Blockchain. Therefore, the comparative legal review not only frames Malaysia's current regulatory position but also suggests potential pathways for reform. The jurisdictions selected demonstrate a range of legislative strategies, from direct regulation to broad legal principles that can guide Malaysia's legal modernisation process.

3.3 Qualitative Case Study Analysis

To support the qualitative case analysis and provide a technical lens for understanding how smart contracts operate in real-world systems, this study incorporates the six-layer innovative contract framework proposed by Shuai et al. (2019), as shown in Figure 2. The model is an analytical reference to conceptualise blockchain-based smart contracts' structural and functional complexity. Each layer, from infrastructure and operations to applications, illustrates how technical design decisions intersect with legal enforceability, performance,

Vol. 10, No. 1, p. 181-198
30 June 2025
(ISSN 2716-5876)

and risk. This framework provides valuable context for interpreting case studies such as the DAO hack and Malaysian pilot projects like Project Castor. The following subsections summarise the six layers of this framework to support later analysis in the discussion section.

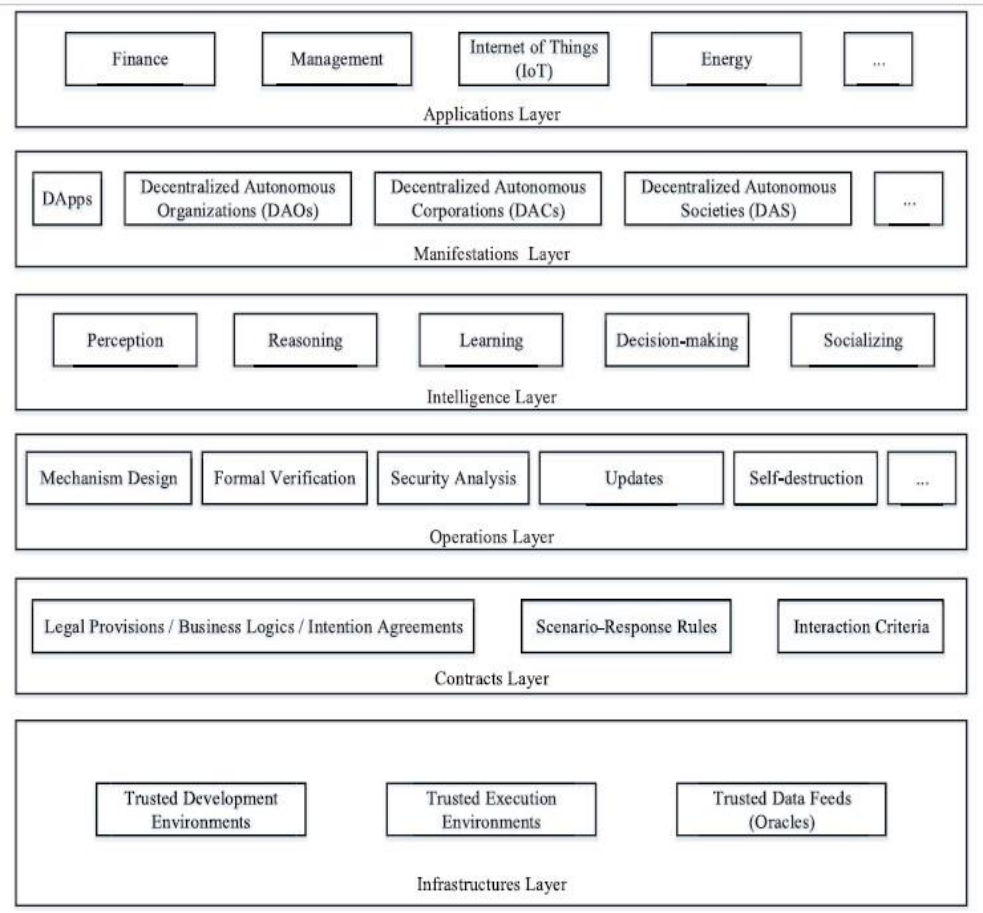

Figure 2. Research Framework of Smart Contracts (Shuai et al., 2019)

The infrastructure layer comprises everything that makes smart contracts and their applications work, like trusted development tools, implementations, and reliable data feeds (Oracles). To some extent, the choice among these infrastructure and services will affect how smart contracts are made and work. The contracts layer holds all contract terms, scenario response rules, and interaction criteria. Thus, this layer can be considered the "static database" of smart contracts, which includes all the rules about how contracts can be called, executed, and communicated.

The production layer contains all dynamic operational processes on the static contracts, such as solid mechanics, validation, security analysis, updates, and self-destruction. This layer is called the "operations layer." Maintaining smart contracts is very important because people using them could lose much money if they are unsafe or do not work correctly. The intelligence layer contains numerous intelligent algorithms, such as perception, reasoning, learning, decision-making, and socialising, that add intelligence to smart contracts based on the preceding three layers.

Vol. 10, No. 1, p. 181-198
30 June 2025
(ISSN 2716-5876)

The manifestations layer encapsulates multiple innovative contract manifestation forms for possible applications, such as DApps, decentralised autonomous organisations (DAOs), decentralised autonomous corporations (DACs), and decentralised autonomous societies (DASs). Smart contracts, which encapsulate the complicated behaviours of network nodes, are analogous to blockchain application interfaces, which allow Blockchain to integrate various application scenarios. The applications layer contains all the application domains constructed on top of the manifestation layer.

In conclusion, the six-layer framework by Shuai et al. (2019) serves as a useful conceptual lens to understand the technical structure of smart contracts, even though it is not directly applied in this study's doctrinal or comparative analyses. It highlights how different technical layers, from coding infrastructure to decentralised applications, may interact with legal issues such as liability, consent, and enforceability. Although this study does not examine each layer empirically, the model offers a structured foundation for future interdisciplinary research to align legal reasoning with intelligent contract system design.

4. Discussion

This section discusses the key legal and technical issues of using blockchain-based smart legal contracts. While smart contracts promise efficiency, transparency, and automation, they also pose significant challenges relating to legal enforceability, immutability of errors, absence of dispute mechanisms, and incompatibility with existing contract laws. These issues must be critically evaluated to assess whether Malaysia's legal infrastructure can adequately accommodate the disruptive nature of this technology.

One of the issues in a smart legal contract is the status of the contract. According to Hulicki's (2017) study, the things to consider regarding the official side of smart contracts are their legal position and how they connect to the real contract. Smart contracts do not have to be real contracts that the parties sign. They can live without each other. Contract law says that a smart contract must meet all of the requirements for a contract, including that both parties agree to be bound by it with all of its consequences. This means that the smart contract must be legal. Specific smart contract qualifications will depend on how they are used in a real-world solution. So, smart contracts can be used to enforce a contract in addition to the actual legal contract, or they can be used to make the contract into a physical document written in a natural language.

Another issue that has been raised from the study by Giancaspro (2017) is the remedial issue. As we know, smart contracts are computer programs that act as channels for commercial transactions. They are written in an immutable programming language that cannot be changed. Once they are on the Blockchain, smart contracts start to work. Smart contracts running on a blockchain network cannot or maybe cannot be changed, even though some parameters can be changed. Computer code is designed to be limited. Accessing and changing its code can be difficult once a smart contract is on the Blockchain. According to the system's rules, blockchain data must be valid. This could be seen as good because human error in execution is eliminated. After all, the data in a blockchain is "guaranteed to be valid" according to these rules, such as there are no double-spends or invalid signatures.

Vol. 10, No. 1, p. 181-198
30 June 2025
(ISSN 2716-5876)

On the other hand, smart contracts can make mistakes that cannot be fixed or take much time to fix. This could have a significant impact on the economy for miners. In addition, because computer programs and their coding can corrupt at any time, neither party is always "responsible." There could be disagreements about who is responsible if there is a risk of technical error. According to a study by Giancaspro (2017), smart contracts, on the other hand, raise many important problems that must be fixed. These contracts are not very vulnerable because they were made to be "permanent" and to work well with what is likely to be a massive record of transactions of the blockchain system. As we said earlier, mistakes that need to be fixed might not be fixable, or at least they might take a lot of time and effort to fix. 68 Traditional non-digital contracts make it easy to fix mistakes. Smart contracts, on the other hand, make it more difficult to fix mistakes. This could be a big problem for courts when using traditional contract law principles to fix mistakes in a smart contract.

Another study by Bodó et al. (2018) addresses the topic of smart contract licensing. According to the study, the most fundamental thing to do to assist individuals in creating blockchain-based smart contracts is to allow the people who develop them to keep all their copyright rights. After that, each author would happily authorise some uses under licenses if and when acceptable. Then, they would utilise Blockchain to license many people to use their work non-exclusively. The smart contracts that allow them to be employed would be legal in every country because each author could keep all 1,760 titles for each of their works in theory. However, this does not eliminate all potential conflicts. Even if both are done on a blockchain, an exclusive licensee may be able to use something that a non-exclusive licensee cannot. Even though both were completed in the exact location, this is the case. Instead of intellectual property law, this might be a contract dispute between the author and the person with the right to utilise his or her work. In this instance, very few, if any, courts would find the nonexclusive licensee accountable, and even if they did, the sanctions would most likely be little.

According to the report, conflicts may be avoided by giving up all non-blockchain licenses or ensuring that the same organising entity is in charge of both. Even if smart contract licenses can be automatically coordinated in the future, this has yet to be done on a large enough scale to be believable. This type of issue with non-blockchain licensing is impossible to avoid using automated tools. It will necessitate human participation and access to all relevant data. People may find it easier to complete this task if they ensure everyone has equal rights. Unlike the study by Sanz (2019), the study reveals that because of smart contracts and blockchain technology, there is less risk that contracts will not be fulfilled. This can be done very quickly and easily. This is done through an automated system that ensures the contract will be done quickly and cheaply if certain conditions are met. This process is done through algorithm programming. The algorithm itself looks for the data it needs and then checks to see if the condition has been met or not based on an oracle, such as a source of outside information, like a website with information on asset prices. In this case, the smart contract makes purchase orders, payments, etc. In this way, Blockchain helps solve problems that might arise when people sign contracts.

Vol. 10, No. 1, p. 181-198
30 June 2025
(ISSN 2716-5876)

People in the network watch an encrypted and decentralised registry that keeps track of the information. This way, everyone in the network can see and keep the information safe. According to this, since the smart contract does not have any central place to store information about how it will work, it would have to hack or break into every network to change the terms of a contract or get its hands on the digital assets that it can. While smart contracts offer promising advancements in automation, efficiency, and transparency, they present substantial legal and technical challenges that cannot be overlooked. The discussion has highlighted four major concerns: the uncertain legal status of smart contracts as enforceable agreements under traditional contract law, the difficulty of addressing coding errors due to their immutability, the complexity of intellectual property licensing within decentralised platforms, and the reliance on oracles and algorithmic triggers, which raise questions of accuracy, trust, and accountability. These issues collectively underscore a critical gap between the technological reality of smart contracts and the legal principles currently governing them. For Malaysia, the path forward requires more than mere adaptation; it demands thoughtful integration of statutory clarity, dispute resolution mechanisms, and recognition of smart contracts within existing legal frameworks. As smart contracts evolve, so must the legal structures supporting their enforceability, regulation, and accessibility.

5. Contribution and Practical Framework

5.1 From Theory to Application

While the conceptual exploration of smart contracts and legal visualisation forms the theoretical foundation of this paper, the contribution must extend beyond abstract discussion to offer value for practice and policy. Recognising this, the study incorporates a practical perspective by aligning smart contract functionality with enforceable legal standards in Malaysia. This is achieved through comparative legal benchmarking, doctrinal analysis, and a visual contract prototyping exercise. These components are not only descriptive but are meant to assist legal practitioners and regulators in conceptualising the integration of smart contracts into Malaysia's digital legal ecosystem.

5.2 Proposed Legal Framework for Smart Contract Integration

To operationalise the ideas discussed, this study proposes a simplified framework for assessing the legal viability of smart contracts under Malaysian law. The framework consists of three progressive layers as follows:

Firstly, Legal Pre-Conditioning Layer. All smart contracts should be assessed for compliance with traditional contract law elements under the Contracts Act 1950—offer, acceptance, consideration, and intention. Additionally, parties must ensure that the contract content does not violate public policy or statutory prohibitions.

Secondly, Technical–Legal Validation Layer. The use of digital signatures (as defined under the Digital Signature Act 1997) and the Electronic Commerce Act 2006 must be verified for enforceability. This layer also involves identifying any automation clauses that may contradict concepts of free consent or legal redress, especially in immutable systems.

Vol. 10, No. 1, p. 181-198
30 June 2025
(ISSN 2716-5876)

Thirdly, Dispute and Regulatory Alignment Layer. Dispute resolution mechanisms (e.g., clauses invoking the Arbitration Act 2005 or Mediation Act 2012) should be embedded within the contract logic. Where blockchain-based governance systems are used (e.g., DAOs), parties should ensure that fallback mechanisms align with Malaysian legal procedures and regulatory expectations. Regulators, fintech developers, and legal advisors can adapt this three-layer model to guide smart contract deployment in real-world scenarios.

5.3 Policy Implications and Legal Reform Opportunities

Based on the comparative review in Section 3.2, several jurisdictions, such as Singapore and the European Union, have enacted explicit frameworks for recognising smart contracts and digital signatures. In contrast, Malaysia's current legal treatment remains implicit and fragmented. To improve clarity and foster innovation, the following policy directions are recommended as follows:

- Legislative Amendment: Amend the Electronic Commerce Act 2006 to include a clear statutory definition and recognition of smart contracts.
- Digital Signature Update: Modernise the Digital Signature Act 1997 to include cryptographic methods used in blockchain environments.
- Regulatory Sandboxes: Expand Bank Negara Malaysia's sandbox initiatives to include smart contract testing with legal oversight.
- Judicial Training: Introduce judicial and regulatory training modules on smart contracts, blockchain governance, and legal automation.
- Visual Contract Standards: Develop soft-law guidelines or professional standards to encourage the adoption of legally valid visual contracts.

These measures are relevant to legal scholarship and provide immediate utility for law reform initiatives, legal practice, and policy development.

5.4 Academic Contribution

This study bridges a gap between legal theory and technology design by combining doctrinal and comparative legal analysis with visual communication prototyping. Including a legal-technical integration model and jurisdictional benchmarking elevates the paper from conceptual commentary to a practically valuable framework. These contributions address the scholarly discourse on smart contracts and offer actionable pathways for policymakers, regulators, and practitioners navigating legal digitisation in Malaysia.

6. Conclusion

Vol. 10, No. 1, p. 181-198
30 June 2025
(ISSN 2716-5876)

This paper has explored the evolving intersection between blockchain-based smart contracts and Malaysian contract law, focusing on doctrinal compatibility, comparative legal benchmarks, and visual communication design. Through a doctrinal analysis, the study identified that while Malaysia lacks specific statutory provisions on smart contracts, existing legislation such as the Contracts Act 1950, the Digital Signature Act 1997, and the Electronic Commerce Act 2006 provide a foundation upon which legal recognition may be inferred. However, the absence of express statutory clarity poses significant uncertainty regarding enforceability, dispute resolution, and consumer protection.

The comparative legal review with jurisdictions such as Singapore, the European Union, and the United States highlights Malaysia's relative legal conservatism. These jurisdictions demonstrate progressive or principle-based approaches that facilitate innovation while preserving legal safeguards. Malaysia may benefit from similar reforms by formally recognising smart contracts, updating digital authentication laws, and adopting regulatory sandbox initiatives. Beyond doctrinal and policy discussions, the paper contributes a practical dimension by integrating a three-layer legal integration framework for smart contracts and presenting visual prototypes that may enhance contractual clarity. These tools aim to bridge the legal theory and implementation gap, particularly in commercial and consumer-facing contexts.

Further empirical research is needed to evaluate how Malaysian courts and regulators handle smart contracts in practice. Future studies could involve interviews with legal practitioners, usability testing of visual contracts, and collaboration with government agencies to pilot digital legal tools. Adopting smart contracts in Malaysia will ultimately depend on technological readiness, legal adaptability, stakeholder education, and public trust.

References

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. *Healthcare, 7*(2), 56. https://doi.org/10.3390/healthcare7020056

Almarwani, A. M. & Yacoub, M. I. (2023). Examining the effect of an educational program on nursing students' informatics competencies. *Nursing Education Perspectives, 44*(6), E59-E61. https://doi.org/10.1097/01.nep.0000000000001106

Blythe, S. E. (2005). Digital signature law of the United Nations, European Union, United Kingdom and United States: Promotion of growth in E-commerce with enhanced security. *Richmond Journal of Law & Technology, 11*(2), 1-20. https://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1238&context=jolt

Bodó, B., Gervais, D., & Quintais, J. P. (2018). Blockchain and smart contracts: The missing link in copyright licensing? *International Journal of Law and Information Technology, 26*(4), 311–336. https://doi.org/10.1093/ijlit/eay014

Chalkidis, I., Androutsopoulos, I., & Michos, A. (2017). Extracting contract elements. In *Proceedings of the 16th edition of the International Conference on Artificial Intelligence and Law* (pp. 19–28). Association for Computing Machinery, New York, NY, USA, 19–28. https://doi.org/10.1145/3086512.3086515

Chau, B. K. & Livermore, M. A. (2024). Computational legal studies come of age. *European Journal of Empirical Legal Studies, 1*(1), 89–104. https://doi.org/10.62355/ejels.19684

Vol. 10, No. 1, p. 181-198
30 June 2025
(ISSN 2716-5876)

Chen, T., & Xu, X. (2010). Digital signature in the application of e-commerce security. *In 2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT)* (pp. 366–369). IEEE. https://doi.org/10.1109/EDT.2010.5496558

Cumming, D. J., Johan, S., & Pant, A. (2019). Regulation of the crypto-economy: Managing risks, challenges, and regulatory uncertainty. *Journal of Risk and Financial Management, 12*(3), 126. https://doi.org/10.3390/jrfm12030126

De Brevern, A. G. (2023). Biomedinformatics is the link between biomedical informatics, biology, and computational medicine. *BioMedInformatics, 4*(1), 1–7. https://doi.org/10.3390/biomedinformatics4010001

Dixit, A., Deval, V., Dwivedi, V., Norta, A., & Draheim, D. (2022). Towards user-centred and legally relevant smart-contract development: A systematic literature review. *Journal of Industrial Information Integration, 26*(2022), 100314. https://doi.org/10.1016/j.jii.2021.100314

Fen, J. & Ai, T. (2021). The effect of Blockchain on the business intelligence efficiency of banks. *Kybernetes, 51*(8), 2652-2668. https://doi.org/10.1108/k-10-2020-0668

Ghiro, L., Restuccia, F., D'Oro, S., Basagni, S., Melodia, T., Maccari, L., & Cigno, R. A. L. (2021). What is a Blockchain? A definition to clarify the role of the Blockchain in the Internet of Things, 1-20. https://doi.org/10.48550/arXiv.2102.03750

Giancaspro, M. (2017). Is a 'smart contract ' really a smart idea? Insights from a legal perspective. *Computer Law & Security Review, 33*(6), 825–835. https://doi.org/10.1016/j.clsr.2017.05.007

Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G., & Xiwei, X. (2018). On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artificial Intelligence and Law, 26*(4), 377–409. https://doi.org/10.1007/s10506-018-9223-3

Heidari, S., Hashemi, S., Khorsand, M-S., Daneshfar, A., & Jazayerifar, S. (2023). Towards standardised regulations for blockchain smart contracts: Insights from Delphi and SWARA analysis. *Amity Journal of Management*, *11*(02), 1–15. https://doi.org/10.48550/arXiv.2403.19051

Hulicki, M. (2017). The legal framework and challenges of smart contract applications. In *Conference on System Sciences* (pp. 3–4).

Hongfang, L., Kun, H, Azimi, M., & Lijun, L. (2019). Blockchain technology in the oil and gas industry: A review of applications, opportunities, challenges, and risks. *IEEE Access, 9*(1), 41426–41444. https://doi.org/10.1109/access.2019.2907695

Markus, S. & Buijs, P. (2022). Beyond the hype: How Blockchain affects supply chain performance. Supply Chain Management: *An International Journal*, 27(7), 177-193. https://doi.org/10.1108/scm-03-2022-0109

Nor Razinah Mohd. Zain, Engku Rabiah Adawiah Engku Ali, Abideen, A., & Hamizah Abdul Rahman. (2019). Smart contract in Blockchain: An exploration of legal framework in Malaysia. *Intellectual Discourse, 27*(2), 595–617. https://doi.org/10.31436/id.v27i2.1435

Pereira, J. C. (2019). The genesis of the revolution in Contract Law: Smart Legal Contracts. *In Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance* (pp. 374–377). https://doi.org/10.1145/3326365.3326414

Vol. 10, No. 1, p. 181-198
30 June 2025
(ISSN 2716-5876)

Rustiana, D., Ramadhan, D., Wibowo, L., Nugroho, A. W., & Mahardika, G. (2022). State of the art blockchain enabled smart contract applications in the university. *Blockchain Frontier Technology*, *2*(2), 70-80.

Sánchez-Gómez, N., Torres-Valderrama, J., Risoto, M. M., & Garrido, A. (2021). Blockchain smart contract meta-modeling. *Journal of Web Engineering*, *20*(7), 2059-2080.

Sanz Bayón, P. (2019). Key legal issues surrounding smart contract applications. *KLRI Journal of Law and Legislation, 9*(1), 63-91. http://dx.doi.org/10.2139/ssrn.3525778

Shcherbyna, V. S., Rieznikova, V. V., Radzyviliuk, V. V., Bevz, S. I., & Kravets, I. M. (2021). Problems of concluding business contracts in electronic form. *Linguistics and Culture Review*, *5*(S2), 751-763.

Shuai, W., Liwei, O., Yong, Y., Xiaochun, N., Xuan, H., Fei-Yue, W. (2019). Blockchain-enabled smart contracts: Architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49*(11), 2266-2277. https://doi.org/10.1109/TSMC.2019.2895123

Sugam Sharma, Samia Gamoura, Deva Prasad, & Arti Aneja. (2021). Emerging legal informatics towards legal innovation: Current status and future challenges and opportunities. *Legal Information Management*, *21*(3-4), 218–235. https://doi.org/10.1017/s1472669621000384

Swan, M. (2016). Blockchain temporality: Smart contract time specifiability with blocktime. *In International Symposium on Rules and Rule Markup Languages for the Semantic Web* (pp. 184–196). Springer, Cham. https://doi.org/10.1007/978-3-319-42019-6_12

Yufei, Z. (2022). The applicability and prospects of CISG on smart contracts. *Proceedings of the 2022 2nd International Conference on Modern Educational Technology and Social Sciences (ICMETSS 2022),* 268–274. https://doi.org/10.2991/978-2-494069-45-9_32

Heng, Z., Grossi, D., & Verheij, B. (2021). Logical comparison of cases. In Víctor, R-D., Monica, P., Michal, A., Pompeu, C., Ugo, P., Giobanni, S. (Eds.) *AI approaches to the complexity of legal systems XI-XII*. AICOL AICOL XAILA 2020 2018 2020. Lecture Notes in Computer Science, vol 13048. Springer, Cham. https://doi.org/10.1007/978-3-030-89811-3_9

Zhixiang, L., Wenglong, F., Yu, Z., & Chengcheng, Z. (2023). Research on the architecture of transactional smart contracts based on blockchains. *Electronics, 12*(18), 3923. https://doi.org/10.3390/electronics12183923