Legal Perspectives on Kill Switch Mechanisms in On-Chain Smart Contracts: Lessons for Malaysia from the European Union Data Act

Zulhazmi Yusof[1],Wan Amir Azlan Wan Haniff [2*],Alizah Ali[3], Ahmad Syahmi Ahmad Fadzil[4], Redwan Yasin[5]

[1,2,3,4]University Technology MARA, Johor 85000, Malaysia

[5]university Pertahanan Nasional Malaysia, Kuala Lumpur, 57000, Malaysia

***Corresponding Author**

DOI: https://dx.doi.org/10.47772/IJRISS.2025.909000186

Received: 29 August 2025; Accepted: 04 September 2025; Published: 04 October 2025

ABSTRACT

Smart contracts, built on blockchain technology, provide advantages such as transparency, automation, and reduced third-party intervention. However, their immutable nature creates significant risks when coding errors, malicious attacks, or unforeseen events occur, and such risks are further complicated by their limited compatibility with traditional dispute resolution. In response, several jurisdictions, notably the European Union through Article 36 of the Data Act, require the inclusion of kill switch mechanisms to ensure safe termination and interruption of faulty contracts. This paper examines the relevance of such mechanisms within the Malaysian legal framework. Using doctrinal legal research and comparative analysis with the European Union Data Act (EUDA), the study identifies key regulatory gaps in Malaysia. It argues that amendments to existing statutes, including the Electronic Commerce Act 2006, the Personal Data Protection Act 2010, and the Digital Signature Act 1997, are needed to legally recognize kill switches, mandate multi-factor authentication, and preserve records for audit purposes. The findings highlight the importance of these safeguards in enhancing digital safety, protecting contracting parties, and ensuring Malaysia remains aligned with global best practices in governing blockchain-based smart contracts.

Keywords: Smart Contracts, Blockchain, Kill Switch Mechanism, European Union Data Act, Malaysian Legal Framework, Personal Data Protection Act, Electronic Commerce Act.

INTRODUCTION

The concept of smart contracts was first introduced by Nick Szabo in the mid-1990s, who argued that legal terms such as liens, bonding mechanisms, and property rights could be embedded directly into hardware and software systems (Szabo, 1996). Since then, smart contracts have gained momentum due to their potential to enhance efficiency, transparency, and automation. At the same time, these very features introduce significant legal and technical risks that require careful regulation.

Among the most pressing risks are bugs, coding errors, and malicious exploits. Cases such as *B2C2 v Quoine*, the DAO hack, and the Parity Wallet incident illustrate how flaws in design or code can result in major financial losses and systemic vulnerabilities (Society for Computers & Law, 2023; Wu et al., 2025; Praitheeshan et al., 2019). Other challenges include the inability of automated contracts to accommodate unforeseen events or force majeure circumstances, as well as difficulties in governance, renegotiation, and dispute resolution (Qasse et al., 2025; Ballaji, 2024; Filippi & Wright, 2018; Bassan, 2024; Ibrahim & Jasim, 2024).

These issues are particularly relevant in Malaysia, where existing statutes such as the Electronic Commerce Act 2006 and the PDPA 2010 remain inadequate to address mechanisms like kill switches or the enforceability

of automated obligations. In contrast, the European Union has advanced through the EU Data Act, with Article 36 specifically mandating kill switch provisions in smart contracts.

Against this backdrop, this study seeks to analyse and compare regulatory approaches across jurisdictions, with particular attention to the EU experience, and to identify the legal reforms necessary for Malaysia to balance innovation with effective safeguards in the governance of smart contracts.

What is smart contracts and its application in real life

According to Nick Szabo, the core concept of smart contracts is that various types of contractual terms such as liens, bonding mechanisms, or definitions of property rights can be incorporated directly into the hardware and software we use daily (Szabo, 1996). In contrast to Szabo's foundational definition, the EU Data Act provides a more contemporary and legally framed definition of smart contracts, reflecting their increasing integration into legal and economic frameworks which include protection to consumers as well. According to EU Data Act, a smart contract is defined as a computer program that enables the automated execution of an agreement, or parts of it, through a sequence of electronic data records. In practice, this means that once the parties agree on its use and content, the contract will carry out the terms of the agreement automatically, either wholly or partially. The implication of this definition is that once parties agree on the use and content of a smart contract, its performance, whether in full or in part, will occur automatically, reducing the need for human intervention and fasten the contractual processes.

One of the simplest analogies that been used by founder of smart contracts, Nick Szabo relating to vending machine. When the correct payment is inserted, the machine will automatically perform the contract by delivering the product (Szabo, 1997) Currently, smart contracts had evolved beyond that illustration. Smart Contracts can be implemented in various sectors. For example, authors such as Khan, Loukil, Ghedira-Guegan, Benkhelifa, and Bani-Hani (2021) and Rouhani & Deters (2019) Smart contracts can be applied in multiple sectors beyond finance.

For example, in healthcare, blockchain-based smart contracts have been explored for use in biomedical data management and insurance claim processes, offering secure and efficient handling of sensitive information (Kuo, Kim, & Ohno-Machado, 2017). Similarly, in supply chain management, smart contracts enable tracking, monitoring, and digital integration, which strengthens transparency and trust across different stakeholders (Korpela, Hallikas, & Dahlberg, 2017). Furthermore, in record-keeping, smart contracts leverage blockchain’s tamper-proof features accuracy, reliability, and authenticity, making them highly suitable for maintaining trustworthy digital records (Lemieux, 2017).

The economic potential of smart contracts is undeniable, with recent market forecasts projecting remarkable growth. According to Zion Market Research, the global smart contracts market was valued at approximately USD 2.72 billion in 2024 and is expected to expand to USD 24.67 billion by 2034, reflecting a compound annual growth rate (CAGR) of about 24.67% between 2025 and 2034 (Zion Market Research, 2024). Meanwhile, Precedence Research provides an even more striking projection: the market, valued at USD 2.02 billion in 2024, is anticipated to surge from USD 3.69 billion in 2025 to nearly USD 815.86 billion by 2034, representing a CAGR of 82.21% during the same period (Precedence Research, 2024).

METHODOLOGY

This study adopts a qualitative approach, relying primarily on doctrinal legal research and secondary data analysis. Relevant literature was critically examined, including books, peer-reviewed journal articles, policy papers, and reports from governmental and non-governmental organizations. Secondary data were gathered through academic databases such as Google Scholar, Scopus, and MyCite, along with official government documents and legal instruments relevant to blockchain, smart contracts, and digital safety.

At this stage, existing definitions, statutory provisions, and regulatory frameworks governing smart contracts were carefully reviewed to identify lacunae in Malaysian law, particularly under the Electronic Commerce Act 2006 and the Personal Data Protection Act 2010. Comparative analysis was also employed to evaluate

international practices, focusing on the European Union Data Act (EUDA) and its Article 36 on mandatory termination mechanisms.

The combination of doctrinal research and comparative analysis provides a systematic basis to assess the legal recognition of kill switch mechanisms in Malaysia. This methodological approach is crucial to understand the nature smart contracts and its legal risks, highlight existing gaps, propose necessary statutory amendments, and offer lessons from international experience to strengthen Malaysia's regulatory framework for smart contracts.

Immutable Nature of Smart Contracts and Its Risks.

Smart contracts were introduced by Nick Szabo, a computer scientist and with a juris doctor in 1994 (Vadlamudi, 2020) Smart contracts possessed a few characters, namely automation, immutability: transparency and cost-efficiency, which can be consider as use in eliminating intermediaries, which eventually reduce transaction costs (Akinsola & Liang, 2025). One of the major issues with the immutability of smart contracts is that the contract cannot be deleted or altered, especially for smart contracts that were created using on-chain blockchain infrastructure (Singh et al., 2020; Qasse et al., 2025). Due to this immutable nature, there are few legal issues that may arise, especially regarding termination and auditability of smart contracts.

Once the smart contract has been deployed, it cannot be stopped, interrupted, or terminated. This is detrimental not only to consumers but also to businesses. For example, in the case of B2C2 Ltd v Quoine Pte Ltd [2019] SGHC(I) 3, there was an error in the cryptocurrency trading platform and the blockchain technology. Despite this, the contract was executed, and the platform carried out the B2C2 deals at an exchange rate approximately 250 times higher than the actual market rate, benefiting B2C2. In this case, the defendant refused to return the cryptocurrency to the plaintiff despite the error. This case proves one of the major problems to the smart contracts is that smart contracts once been deployed, it cannot be stopped or interrupted.

Due to the nature of immutability of smart contracts, many scholars have raised their concerns about the irreversible outcomes of smart contracts. Werbach and Cornell (2017) state that this legal rigidity clashes with traditional contract doctrines like equitable relief or the right to rescind a contract if there is a fundamental mistake in the contract. As highlighted before, if an error or mistake happens as in B2C2's case, the contract will become immutable, causing irreparable damage, and bringing the matter to court may be the only option available due to the immutable nature of smart contracts. In addition to that, Souter (2022), for example, argues that smart contracts are "immutable, meaning that without a kill switch, developers must watch on in horror," especially if unexpected issues occur.

Therefore, having a kill switch in smart contracts is crucial to prevent potential legal complications after they are deployed. Generally, smart contracts can be categorized into three types: on-chain, off-chain blockchain, and hybrid storage architectures (Solaiman, Wike, & Sfyrakis, 2021; Eren, Karaduman, & Gençoğlu, 2025). The most challenging one will be on-chain architecture because it cannot be altered once smart contracts been deployed. To prevent this issue, smart contracts must be governed using kill switch. This to ensure that smart contracts can be interrupted or stopped whenever it is required. Implementation of kill switch is not something.

In Malaysia for example, In February 2024, the Minister in the Prime Minister's Department (Law and Institutional Reforms), Datuk Seri Azalina Othman, said that the government is in the process of drafting a new bill to enhance digital safety via improved procedures and enforcement. The government is in the process of formulating new legislation that includes a "kill switch" mechanism to promptly stop fraudulent transactions. In addition, she stated that the current legislation is antiquated and inadequate in addressing this type of criminal activity (Carvalho et al., 2024). One of the ways to overcome this incident, especially for off-chain blockchain, is by introducing the kill switch function in smart contracts.

Kill switch functionality has been made compulsory in European Union (EU) countries following the introduction of its regional regulation called the EU Data Act. The Act came into force on January 11, 2024, with requirements applying from September 12, 2025. One of the most significant aspects of smart contracts relates to how the Act addresses the immutability of smart contracts. This Act serves as a fundamental

regulatory framework in the European region and can serve as a foundation and guideline for other countries, including Malaysia.

The immutability of smart contracts, while offering benefits like transparency and tamper-proof execution, introduces substantial risks when the code contains vulnerabilities or when external circumstances require a deviation from the automated execution. These risks include:

Bugs and Coding Errors:

As demonstrated in the case of B2C2 v Quoine case, even minor coding errors can lead to significant financial losses or unintended outcomes. The inability to patch or halt a faulty contract once deployed means that such errors can spread and cause continuous damage until the contract's intended lifespan ends or its funds are depleted. These trades were executed via autonomous software with minimal human intervention, illustrating how immutable smart contracts can amplify coding mistakes and cause monetary loss and raise legal issues if kill switch is not included in the smart contracts (Society for Computers & Law, 2023)

Malicious Exploits and Attacks:

The decentralized and immutable nature of smart contracts makes them attractive targets for hackers. If there is vulnerabilities in the code can be exploited, this will lead to theft of assets or manipulation of contract logic. As suggested by Wu et al. (2025) and Praitheeshan et al. (2019) famous examples include the DAO hack, where a re-entrancy bug led to the theft of millions of dollars' worth of Ether, and the Parity Wallet multi-sig bug, which resulted in the freezing of substantial cryptocurrency funds, these exploits were came from a combination of technical shortcomings in the design and implementation of the software code (Praitheeshan, Pan, Yu, Liu, & Doss, 2019).

Unforeseen Circumstances and Force Majeure:

As argues by Qasse et al. (2025), Ballaji (2024) and Filippi & Wright (2018), traditional contracts often include clauses for force majeure or unforeseen events that might render performance impossible or impractical. Smart contracts, by their nature, facing difficulty to take into consideration for real-world events, such as pandemic or natural disaster. This is important especially in contract that related insurance claim and healthcare system. Without a mechanism to pause, alter, or terminate a contract in response to these circumstances, parties may be locked into agreements that are no longer feasible or just to them.

Governance and Dispute Resolution:

One of the major risks associated with the immutability of smart contracts is their incompatibility with traditional dispute resolution mechanisms. Unlike conventional contracts, which can be renegotiated, suspended, or terminated in the face of disagreement or unforeseen circumstances, smart contracts are coded to self-execute once deployed, thereby reducing and minimizing human intervention. This rigidity complicates dispute resolution, particularly when disagreements arise from misinterpretations of code, coding errors, external real-world events, or malicious attacks (Bassan, 2024)

Furthermore, a significant challenge arises from the technical nature of smart contracts themselves. Many of these contracts are written in programming code rather than natural language, making them inaccessible and difficult to interpret for non-technical parties, courts, or arbitrators (Ibrahim & Jasim, 2024). This issue increases the risk of disputes because parties may not fully understand the operational logic embedded within the contract at the time of agreement, which can cause further losses to all relevant parties, especially if a kill switch does not exist to stop or pause the contract when needed.

The issue becomes more critical when smart contracts contain bugs or coding errors. Once deployed, the immutable nature of smart contracts prevents developers or contracting parties from stopping or correcting faulty execution. This may eventually lead to major financial losses or continuous harm until the contract naturally concludes or its resources are exhausted. (Köksal, 2024). The author also suggest that Smart Contract Arbitration (SCA) should be introduced as an innovative approach to resolving disputes, designed to reduce

reliance on third parties while cutting down on costs, paperwork, and the risk of tampering with evidence. This issue will not be in questioned if kill switch existence is made mandatory in the first place as required in EU Data Act.

Furthermore, unforeseen circumstances, including force majeure events, often require flexibility in traditional contracts to suspend or adjust obligations. Smart contracts, however, lack built-in mechanisms to address such contingencies, potentially causing deadlock for all contracting parties unless a specific alternative dispute mechanism is in place, as highlighted by Huang & Harrington (2024), such as the use of Kleros, a decentralized arbitration protocol. Nevertheless Kleros faced a few major drawback, primarily because Kleros rulings are executed on-chain, but in real-world disputes for example, in employment, property, or tort claims, the enforcement still requires recognition by traditional courts. Additionally, many jurisdictions have not formally recognized blockchain arbitration including in Malaysia, unless relevant statutes such as Courts of Judicature Act, Subordinate Courts Act or Rules of Court amended to allow this.

Based on the risks associated with the immutable nature of smart contracts discussed above, the immutability of smart contracts offers security, transparency, and also reduces risks when coding errors, hacks, unforeseen events, or disputes arise. However, the same advantages and characteristics make dispute resolution difficult, particularly given the technical nature of smart contracts and their limited legal recognition in many jurisdictions. To address these risks, the introduction of a mandatory kill switch, as required under Article 36 of the EU Data Act, is essential to allow contracts to be paused, reset, or terminated when necessary. Such a safeguard would help prevent financial losses, ensure fairness, and bridge the gap between automated execution and traditional legal protections. This will be elaborated further in the next part, taking into consideration the European Union Data Act, particularly Article 36 that will be elaborated on next part.

Lesson Learned from European Union Data Act in Dealing with Immutability Nature of Smart Contracts

The European Union Data Act, which came into force on January 11, 2024, with requirements applying from September 12, 2025, directly addresses the immutability challenge of smart contracts. Article 36 of EU Data Act sets out the essential requirements for smart contracts used in executing data-sharing agreements. It emphasizes the need for these contracts to operate in a reliable and secure manner, and to include safeguards for termination and access control where necessary**.** For smart contracts for example, this Act not only define smart contracts but also address on how to cater issues relating to the immutability nature of smart contracts. Article 36 (b) of EU Data Act specifically states that:

“Safe termination and interruption, to ensure that a **mechanism exists to terminate the continued execution of transactions** and that the smart contract includes internal functions which can reset or instruct the contract to stop or interrupt the operation…”

This Act play pivotal rule to ensure that all smart contracts can be safely terminated. this is important especially if there is an unexpected problem occurred due to the smart contracts and its autonomous execution. The introduction of this Act may undermine the utilization of smart contracts, this Act contracts is crucial to ensure smooth contractual transaction. Article 36 (b) of the Data Act mandates essential requirements for smart contracts used in data sharing agreements, specifically focusing on:

Safe Termination and Interruption:

According to Schickler (2023) This is a crucial provision requiring smart contracts to include a mechanism to terminate the continued execution of transactions. This effectively introduces a 'kill switch' or 'pause switch' functionality, challenging the traditional immutable nature of on-chain smart contracts. A kill switch is not something uncommon, this is because it is even implemented on a smart device such as a phone. Legislators and public officials seek to discourage theft and stop the theft trend by requiring the installation of a "kill switch" that may remotely disable a phone's vital functionality (Rietfors & Iyengar, 2016). On July 18, 2013, for example, Samsung proposed charging customers extra for its cellphones to include the LoJack security system, which includes a kill switch created by Absolute Software (Williams, 2014).

In addition, Article 36 further elaborate that smart contracts must complied with other technical requirements due to it immutable nature, for example under Article 36 (c) which highlighted the issue relating to :

Data Archiving and Continuity:

The Act also highlights that provisions for data archiving and continuity if a smart contract must be terminated or interrupted. From a legal perspective, Article 36 represents a significant regulatory intervention. It aims to bridge the gap between the technical characteristics of smart contracts and the principles of traditional contract law, which allow for remedies like rescission, termination, or modification under certain circumstances (Werbach and Cornell, 2017). The EU Data Act not only set high standard for protection in the smart contract but also required the data achieving process for auditability (Think Mind, 2025), This means that smart contracts must include a way to store and preserve past transaction data, contract logic, and code so that all previous operations can be reviewed and audited, even if the contract is terminated or deactivated by the kill switch especially for the purpose of an audit. Due to the immutable nature of smart contracts, this serve as comprehensive audit trail that cannot be tamper by anyone (Ullah et al., 2024)

Robustness and access control.

In addition, to ensure that smart contracts cannot be manipulated, Article 36(a) provides that they must be built to be strong, secure, and reliable. They should include access control mechanisms so that only authorized individuals can use or modify them, and they must be designed to avoid errors and withstand tampering by hackers or third parties. This is vital because if an unauthorized person gains access to the smart contract and its kill switch, they could stop or terminate the contract's execution, or even destroy the entire contract. Hence, strong and secure access controls must be implemented.

By requiring a termination mechanism, the EU Data Act aims to reduce risks such as financial losses from coding errors (as seen in B2C2 v Quoine), malicious exploits like the DAO hack, and the inability to adapt to unforeseen circumstances or force majeure events (Qasse et al., 2025; Ballaji, 2024). It also helps make dispute resolution more practical by allowing a contract to be paused or stopped, something that is otherwise difficult given the self-executing and technically complex nature of smart contracts (Ibrahim & Jasim, 2024; Bassan, 2024).

The requirement for a 'kill switch' is seen as a move to protect consumers and businesses from the irreversible consequences of faulty or compromised smart contracts, while introducing a level of flexibility that smart contracts currently lack. This provision is particularly impactful for on-chain smart contracts, which are the most challenging to alter once deployed. The EU Data Act serves as a landmark regulatory framework in this regard and will indirectly influence other jurisdictions, especially in countries that are members of the European Union.

Recommendations for Integrating Kill Switch Mechanisms into Statutory Provisions

Requirement of Safe Termination and Interruption (Kill Switch) Function in existing law.

A kill switch, as explained previously, is a mechanism designed to stop or disable a smart contract. This is crucial for safeguarding autonomy and assets when errors or unforeseen issues arise. Certain existing statutes can be amended to legally recognize the functionality of a kill switch, similar to Article 36 of the EUDA. As discussed earlier, numerous risks may arise if smart contracts cannot be stopped or interrupted, including bugs and coding errors, malicious exploits and attacks, unforeseen circumstances, and force majeure. These risks are further increased by the incompatibility of smart contracts with traditional dispute resolution mechanisms.

Therefore, the implementation of a kill switch and pause switch, as aligned with Article 36 of the EUDA, which requires safe termination and interruption, can serve as an alternative solution to address these challenges. This can be achieved by ensuring that a mechanism is in place to stop a transaction from being executed further. The smart contract must include internal controls that can be used to reset it or instruct it to stop or interrupt an activity, thereby preventing further unintentional executions.

From a Malaysian perspective, this approach also aligns with the government's intention, as highlighted in February 2024 by the Minister in the Prime Minister's Department (Law and Institutional Reforms), Datuk Seri Azalina Othman, who announced that the government is drafting new legislation to enhance digital safety through improved procedures and enforcement, including the introduction of a 'kill switch' mechanism to promptly stop fraudulent transactions. She further emphasized that the existing legislation is antiquated and inadequate in addressing this type of criminal activity.

Some statutes that can be amended to allow for the implementation of a kill switch include the Contracts Act 1950, which can be revised to legally recognize smart contracts as valid agreements and expressly permit safe termination or pausing. Additionally, other laws such as the Electronic Commerce Act 2006 could be amended to require that terminated or deactivated smart contracts retain auditability by preserving contract logic and execution history.

Robustness and Access Control in Smart Contracts.

The B2C2 v Quoine case illustrates how even small coding errors in smart contracts can escalate into severe financial losses or unintended outcomes. Since faulty contracts cannot easily be patched or halted once deployed, such errors may continue to cause damage until the contract naturally expires or its resources are exhausted. To ensure that the kill switch in smart contracts is protected against 3rd party attack, bugs, coding errors, or unwanted attack some legal framework in Malaysia such as the Digital Signature Act 1997 (Act 562) should be amended to explicitly require multi-factor authentication in financial technology (Fintech). This is vital to protect all contracting parties in Malaysia. This will also beneficial to smart contracts users that utilize blockchain. This would ensure that only authorized parties are able to interact with critical contractual functions in smart contracts, and eventually can reduce the risks of manipulation or unauthorized interference.

Multi-factor authentication (MFA) is now an essential tool for protecting sensitive information and strengthening access control. By requiring users to verify their identity with at least two different and unique factors, MFA adds an extra layer of defence Almadani, Alotaibi, Alsobhi, Hussain, & Hussain, 2022). This not only secures individual users but also helps organizations guard against a wide range of potential attacks. Such provisions would also align Malaysia with emerging global standards that required layered security in blockchain-based transactions such EUDA.

Data Archiving and Continuity

As of now, Malaysia does not have a specific regulatory framework to determine the legality of smart contracts. Instead, the country continues to rely on the outdated Electronic Commerce Act 2006 and the Contracts Act 1950, the latter of which was introduced even before Malaysia's independence (Saripan, Yusof, Haniff, Jayabalan, & Halim, 2024). With regard to the Electronic Commerce Act, it is suggested to amend the Act to include the requirement that any smart contracts terminated or deactivated by a kill switch must retain auditability by preserving transactional data, contract logic, and execution history, which is quite similar to Article 36, which requires that when a smart contract is terminated or deactivated, relevant records are properly preserved.

This is vital for auditability, especially for the purpose of improving and enhancing smart contracts in the future, in cases where they are affected by malicious exploits, attacks, bugs, or coding errors. As emphasized by Alharby and van Moorsel (2017), a security breach or coding error could result in significant financial losses, and while the immutability of blockchain makes tampering with smart contracts extremely difficult, it must be noted that without proper mechanisms for audit trails, the accountability and transparency of smart contracts may nonetheless be compromised (Olivieri, Pasetto, Negrini, & Ferrara, 2024). Furthermore, Yusof et al. (2024) argue that Malaysia's reliance on outdated legislation such as the Electronic Commerce Act leaves significant gaps in addressing auditability of smart contracts. Hence, a kill switch in smart contracts must maintain and preserve records of operations on the blockchain, even when activated due to malicious exploits, attacks, unforeseen circumstances, or force majeure, for audit purposes.

Additionally, another recommendation to ensure that data archiving and continuity can be preserved, some existing law should be amended as well especially Personal Data Protection Act. Wong (2023) emphasize that because Data Protection Act 2010 (PDPA 2010) mandates that personal data must be deleted when no longer necessary failure to do so can cause data user to be fined on/or imprison. To resolve this issue, it is recommended that the PDPA 2010 be amended to allow the operation of a kill switch and the preservation of such data for audit purposes, as opposed to the current provisions on PDPA 2010. With amendments to these two statutes, specifically the Electronic Commerce Act and the PDPA 2010, the kill switch could operate at an optimum level and protect the interests of all contracting parties in addressing this issue.

CONCLUSION

As previously discussed, industry projections suggest exponential growth in the smart contracts market. Zion Market Research (2024) reported that the market, valued at USD 2.72 billion in 2024, is expected to reach USD 24.67 billion by 2034, while Precedence Research (2024) provided an even more ambitious forecast, predicting an increase from USD 3.69 billion in 2025 to nearly USD 815.86 billion by 2034. This immense growth highlights the critical role smart contracts will play in the future digital economy.

Nevertheless, the absence of clear and updated legal frameworks continues to present challenges, particularly in Malaysia, where existing statutes such as the Electronic Commerce Act 2006 and the PDPA 2010 remain insufficient to address issues like kill switch mechanisms, Oracle reliability, and the validity of automated contractual capacity. This study highlights the regulatory lacunas in Malaysia's current system and emphasizes the need for reform through comparative analysis with more advanced jurisdictions, such as the European Union and the European Union Data Act, which not only serve as regional guidelines but also as a landmark for incorporating kill switches in smart contracts.

Recommendations have been made to enhance Malaysia's legal framework by integrating mechanisms such as kill switches to balance innovation with accountability. However, this research is limited by its reliance on secondary data and doctrinal analysis, without incorporating primary data such as interviews with industry experts or policymakers. Future research should therefore combine doctrinal and empirical approaches to provide a more holistic understanding of the regulatory challenges and opportunities, particularly by drawing from jurisdictions that have pioneered more robust frameworks.

REFERENCES

1. Akinsola, O. K., & Mary, B. J. (2025). Smart contracts and corporate governance: Automation, legal risks, and benefits. Retrieved from https://www.researchgate.net/profile/Britney-Johnson-Mary/publication/388406514_Smart_Contracts_and_Corporate_Governance_Automation_Legal_Risks_and_Benefits/links/67972b828311ce680c3bc34a/Smart-Contracts-and-Corporate-Governance-Automation-Legal-Risks-and-Benefits.pdf
2. Alharby, M., & van Moorsel, A. (2017). Blockchain-based smart contracts: A systematic mapping study. Computer Science & Information Technology, 7(2), 125–140. https://arxiv.org/abs/1710.06372
3. Almadani, M. S., Alotaibi, S., Alsobhi, H., Hussain, O. K., & Hussain, F. K. (2023). Blockchain-based multi-factor authentication: A systematic literature review. Internet of Things, 23, 100844.
4. Ballaji, N. (2024). Smart contracts: Legal implications in the age of automation. Beijing Law Review, 15, 1015–1032. https://doi.org/10.4236/blr.2024.153061
5. Bassan, F. (2024). From smart legal contracts to contracts on blockchain. Computer Law & Security Review, 52, 105033. https://doi.org/10.1016/j.clsr.2023.105033
6. Buhala, O., Cukerová, D., Dolný, J., Kovalyshyn, O., Maydanyk, R., Mizerski, D., Mrázová, Ž., Pokryszka, K., Rostáš, D., Sishchuk, L., Wyrzykowski, W., & Zozuliak, O. (2025). Evolution of private law: New technologies. Instytut Prawa Gospodarczego Sp. z o.o.
7. De Filippi, P., & Wright, A. (2018). Blockchain and the law: The rule of code. Harvard University Press.
8. Eren, H., Karaduman, Ö., & Gençoğlu, M. T. (2025). Security challenges and performance trade-offs in on-chain and off-chain blockchain storage: A comprehensive review. Applied Sciences, 15(6), 3225. https://doi.org/10.3390/app15063225

9. Huang, J., & Harrington, A. (2024). From code to court and beyond: Alternative dispute resolution on and off the blockchain. Dispute Resolution Journal, 79(1), 22–45. https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2024/11/from-code-to-court-and-beyond--alternative-dispute-resolution-on-and-off-the-blockchain--dispute-resolution-journal--huang-harrington-nov-2024.pdf
10. Ibrahim, A. I., & Jasim, A. A. (2024). Enforcement of smart contracts in cross-jurisdictional transactions. International Journal of Law and Management. https://doi.org/10.1108/IJLMA-06-2024-0220
11. Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-peer Networking and Applications, 14(5), 2901–2925.
12. Köksal, B. (2024). A trade-off in smart contract arbitration: Sacrificing anonymity for transparency. Fordham Intellectual Property, Media & Entertainment Law Journal, 35(1), 95–134. https://ir.lawnet.fordham.edu/iplj/vol35/iss1/3
13. Korpela, K., Hallikas, J., & Dahlberg, T. (2017). Digital supply chain transformation toward blockchain integration.
14. Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211–1220.
15. Lemieux, V. L. (2017, November). Blockchain and distributed ledgers as trusted recordkeeping systems. In Future technologies conference (FTC) (Vol. 2017).
16. Norton Rose Fulbright. (2019). Singapore court's cryptocurrency decision: Implications for trading, smart contracts, and AI. Norton Rose Fulbright.
17. Olivieri, L., Pasetto, L., Negrini, L., & Ferrara, P. (2024). European Union Data Act and blockchain technology: Challenges and new directions. In CEUR Workshop Proceedings (Vol. 3791). https://ceur-ws.org/Vol-3791/paper30.pdf
18. Praitheeshan, P., Pan, L., Yu, J., Liu, J., & Doss, R. (2019). Security analysis methods on Ethereum smart contract vulnerabilities: A survey.
19. Precedence Research. (2025, August 6). Smart contracts market size, growth, and trends — Report 2025 to 2034. Retrieved from https://www.precedenceresearch.com/smart-contracts-market
20. Qasse, I., Ali, I. M., Ahmed, N., Hamdaqa, M., & Jónsson, B. Þ. (2025). The myth of immutability: A multivocal review on smart contract upgradeability. arXiv preprint arXiv:2504.02719. https://arxiv.org/abs/2504.02719
21. Rietfors, M., & Iyengar, V. (2016). Could kill switches kill phone theft: Surveying potential solutions for smartphone theft. Lincoln Memorial University Law Review, 4, 30. https://heinonline.org/HOL/LandingPage?handle=hein.journals/lmulr4&div=5&id=&page=
22. Rouhani, S., & Deters, R. (2019). Security, performance, and applications of smart contracts: A systematic survey. IEEE Access, 7, 50759–50779. https://doi.org/10.1109/ACCESS.2019.2911031
23. Schickler, J. (2023, March 14). EU Parliament passes a bill requiring smart contracts to include a kill switch. Yahoo! Finance. Retrieved June 27, 2023, from https://finance.yahoo.com/news/eu-parliament-passes-bill-requiring
24. Singh, A., Parizi, R. M., Zhang, Q., Choo, K. K. R., & Dehghantanha, A. (2020). Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. Computers & Security, 88, 101654.
25. Society for Computers & Law. (2023, February 3). The weakest link? Contract risk on the blockchain. Society for Computers & Law. Retrieved August 20, 2025, from https://www.scl.org/12792-the-weakest-link-contract-risk-on-the-blockchain/
26. Solaiman, E., Wike, T., & Sfyrakis, I. (2021). Implementation and evaluation of smart contracts using a hybrid on- and off-blockchain architecture. Concurrency and Computation: Practice and Experience, 33(1), e5811.
27. Souter, A. (2023, February 3). The weakest link? Contract risk on the blockchain. Society for Computers and Law. https://www.scl.org/12792-the-weakest-link-contract-risk-on-the-blockchain/

28. Szabo, N. (1996). Smart contracts: Building blocks for digital markets. Retrieved from http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html
29. Szabo, N. (1997). Formalizing and securing relationships on public networks. First Monday, 2(9). https://doi.org/10.5210/fm.v2i9.548
30. Think Mind. (2025). Consequences of the EU Data Act and the EU GDPR: Audit-proof archiving and compliance obligations. In Proceedings of ICDS 2025 (pp. 40–10025). https://www.thinkmind.org/library/ICDS/ICDS_2025/icds_2025_1_40_10025.html
31. Ullah, F., He, J., Zhu, N., Wajahat, A., Nazir, A., Qureshi, S., ... & Dev, S. (2024). Blockchain-enabled EHR access auditing: Enhancing healthcare data security. Heliyon, 10(16).
32. Vadlamudi, H. (2025). Transformation of the legal industry. In Emerging trends in business and management: Issues and challenges (Vol. 2, p. 60).
33. Werbach, K., & Cornell, N. (2017). Contracts ex machina. Duke Law Journal, 67(2), 313–382. https://scholarship.law.duke.edu/dlj/vol67/iss2/2
34. Williams, M. (2014, February 24). U.S. carriers rejected 'kill switch' technology last year. Computerworld. http://www.computerworld.com/s/article/9246557/U.S._carriers_rejected_39_kill_switch_39_technology_last_year
35. Wong, W. W. (2022). The law of smart contracts. Malaysia: Sweet & Maxwell.
36. Wu, J., Xie, L., & Li, X. (2025). Security vulnerabilities in Ethereum smart contracts: A systematic analysis. arXiv preprint arXiv:2504.05968. https://arxiv.org/abs/2504.05968
37. Yusof, Z. B., Haniff, W. A. A. W., Saripan, H., Jayabalan, S. J. K., & Halim, A. H. A. (2024). Regulatory framework on smart contracts: A comparative analysis. Information Management and Business Review, 16(2), 221–230.
38. Zion Market Research. (2024). Smart contracts market size, share, trends, growth & forecast report 2024–2034. Zion Market Research. https://www.zionmarketresearch.com/report/smart-contracts-marke