

Regulatory Framework on Smart Contracts: A Comparative Analysis

Zulhazmi Bin Yusof¹, *Wan Amir Azlan Bin Wan Haniff¹, Hartini Saripan², Sheela A/P Jayabala Krishnan Jayabalan², Asma Hakimah Ab Halim³

¹Department of Law, Universiti Teknologi MARA, Segamat, Malaysia

²Faculty of Law, Universiti Teknologi MARA, Shah Alam, Malaysia

³Faculty of Law, Universiti Kebangsaan Malaysia, Bangi, Malaysia

zulhazmi@uitm.edu.my, *wamirazlan@uitm.edu.my, ameerazlan@yahoo.com, hartinisaripan@uitm.edu.my, sheela880@uitm.edu.my, hakimah@ukm.edu.my

*Corresponding author: Wan Amir Azlan Wan Haniff

Abstract: Smart contracts use a few contemporary technologies, such as blockchain and digital currency. Due to this, it carries numerous advantages to the consumers due to the nature of the technology such as transparency, quickness, lack of third-party intervention, and decentralization. Although numerous research has been conducted on smart contracts, there isn't currently a tangible remedy to deal with various lacunas in the regulatory framework for smart contracts. In this study, secondary data was gathered by analyzing academic websites and databases like Google Scholar including governmental and non-governmental organizations from various countries. In addition, doctrinal legal research using a comparative analysis approach has also been used in this research. Regulatory frameworks in various countries including but not limited to Malaysia, the United States of America, Malta, Switzerland, and Dubai have been observed. The finding shows that the issue of the legitimacy of smart contracts, capacity as well as validity and certainty of Oracle were the main legal issues with smart contracts. This paper has contributed to our understanding of the existing gap in Malaysia's regulatory systems. Additionally, this improves the corpus of knowledge in this area, assisting legislators and other decision-makers in amending new regulatory frameworks for Smart Contracts.

Keywords: *Smart contracts, blockchain, digital currency, cryptocurrency, regulatory framework.*

1. Introduction

Nick Szabo first outlined what smart contracts are. Long before blockchain technology was created, computer science and law researcher Nick Szabo developed the term "smart contracts" in the mid-1990s. According to Szabo, a smart contract is a collection of digitally specified promises that include protocols that the parties must follow to fulfill these promises (Szabo,1997). On the other hand, Savelyev (2017) describes smart contracts in terms of blockchain technology. Peer-to-peer (p2p) transfers are used by smart contracts, which can be done with or without the use of a trustworthy intermediary. The scope of the study for this research is to analyze regulatory frameworks for smart contracts from various jurisdictions and determine the current hiatus in existing legal frameworks in Malaysia and other countries.

Smart contracts use cutting-edge technology to power their systems. This additionally involves cryptocurrencies. A type of virtual currency is cryptocurrency. A government or central bank does not back electronic money known as "Virtual Currency" (VC). Lower transaction costs and speedier fund transfers for services delivered are among the two benefits that VC might provide (Jafari et al., 2018). Blockchain technology, in addition to cryptocurrencies, is a key technology that was applied in the creation of smart contracts. Blockchains are often decentralized (not typically under the jurisdiction of a firm, bank, or government) and distributed (i.e., lacking a central repository). Digital ledgers are both tamper-evident and resistant (Yaga et al., 2019).

Statista (2023) indicates that by December 2022, there will be 425 million Bitcoin users, up from just 5 million in 2016. This is an increase of 85 times over six years. Because of its many benefits, cryptocurrency has been included in smart contracts. The market for smart contracts is anticipated to rise from its estimated value of USD 1750 million in 2022 to USD 9850 million by 2030, with a projected compound annual growth rate (CAGR) of almost 24% between 2023 and 2030, according to Zion Market Research.

Despite these figures and the increase in the usage of smart contracts worldwide, legislators and policymakers worldwide still face various obstacles and challenges regulating smart contracts for various reasons that will

be discussed further later. According to Yong, Tay & Khong (2022), many legal questions remain unanswered in the present smart contracts. As a result, regulators ought to think about passing enabling laws to provide clarification and remove any lingering questions regarding the legal status of smart contracts including smart tenancy. Various other legal issues surrounding the usage of smart contracts also need to be clarified to remove uncertainty among smart contract users. Therefore, this study's objective is to suggest analyzing and comparing the existing regulatory frameworks from various countries, including Malaysia and other jurisdictions relating to smart contracts.

2. An Overview of Smart Contracts

Szabo (1997) expands on his concept with the introduction of "smart contracts," defining them as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises." Szabo suggested turning contractual clauses (collateral, bonding, etc.) into code and embedding them into a property (hardware or software) that can enforce them. This would lessen the need for trusted intermediaries between parties to transactions and the possibility of malicious or unintentional exceptions. In the context of a blockchain, smart contracts are scripts stored on the distributed ledger. It cannot be easily changed because it is stored on a distributed ledger. As suggested by many writers such as Giancaspro (2017) and Kizza (2020), it is difficult to alter smart contracts once it had been executed. On the Blockchain, every action is recorded, and the data included in those records is available to all users and cannot be changed or deleted. The results of this recording indicate the Blockchain's immutability, reliability, and transparency (Bahga, & Madiseti, 2016).

Smart contracts have been utilized in many industries. For example, in a smart loan contract, the software is set up to automatically create payment instructions in compliance with the rules of the smart contract based on inputs received from reliable data sources via an oracle. The interest rate input is used by the smart contract to determine the right monthly repayment amount for the smart loan contract when it is informed that the final day of the month has passed. The software then initiates a transfer of this sum from Party A's bank account to Party B's bank account by electronically instructing Party A's bank. The automatic instruction is followed by Party A's bank, which sends the amount to Party B's account (Clifford Chance and European Bank for Reconstruction and Development, 2017).

In addition, many sectors have used smart contracts, including energy trading and asset leasing by German startup Slok to share, rent, and sell physical assets without the need for middlemen (Peng et al., 2001). Smart contracts have also been used in managing the power grid. A smart grid is an electricity network that can cost-effectively integrate all users' behaviors and actions, including both customers and generators (Bieser, 2014). Xu, Chong & Chi (2021) list other industries that utilize smart contracts and including agriculture, business, construction & real estate, energy, entertainment, finance, education, healthcare, and not to mention in insurance (Gatteschi, et al 2018).

3. Methodology

This study uses a qualitative approach to its investigation. Examine the available literature critically, including books, scholarly articles, and government and NGO reports. This study employed secondary data based on an analysis of publications on pandemics, non-government organizations, and governmental organizations, websites run by consumer associations, and academic databases like Google Scholar to look critically and examine the relevant literature for any lacuna in the current legal system that is related to the context. The various sources of data inform the approach adopted for literature review or research synthesis (Anthony, et.al, 2012). Additionally, at this stage of the procedure, the definitions, the existing regulatory frameworks, and any legal loopholes in Malaysian law were carefully examined.

Finally, doctrinal legal research by way of a comparative analysis approach has also been applied to critically analyze the laws regulating these procedures, as well as an analysis of Malaysian law with other countries including the United States of America, Malta, Switzerland, and Dubai. This doctrinal legal is vital to determine lacunas in the current regulatory framework.

Development of Smart Contracts from a Contract Legal Perspective

It is necessary to closely examine conventional contracts to comprehend how smart contracts have evolved. According to Crafa et al., (2023), A legal contract is described as "an agreement that is intended to result in a relationship that is legally binding or to have some other legal effect." Theoretically, the parties are free to decide how their contracts will be drafted (party autonomy/freedom of contract). According to the literature, Mesopotamia, Egypt, and ancient Greece are among the prehistoric societies where contract law may have its roots. These early legal systems allowed for simple contract forms and legal remedies (Maine, 2019). Posner asserts that, in early legal systems, severe sanctions were the only practical substitute for compensation since wrongdoers could not, for lack of sufficient cash, afford to recompense their victims (Posner, 1977).

Under Roman civilization, contract law gradually changed. Roman law was especially important to Europe because it provided the theoretical underpinnings for a reasonably homogeneous legal culture, which included the development of the idea of a legally enforceable contract (*pacta sunt servanda*) (Zimmermann, 2009). The same notion has also been applied to international law, where it is known as the *pacta sunt servanda* principle, which calls for treaty parties to fulfill their responsibilities under the agreement in good faith (Jain, 2005). The extensive collection of Roman laws that Emperor Justinian ordered in the sixth century CE serves as both its source and model (Berkeley Law, n.d).

Eventually, contract law underwent further evolution, and the common law-based development of English contract law had a considerable influence on how contracts are currently interpreted. The common law tradition originated in England during the Middle Ages and spread to all of the British colonies worldwide. Civil law was established in the colonies of European imperial powers such as Spain and Portugal concurrently with its development in continental Europe (Berkeley Law, n.d). Common law cases also contributed to developing various legal principles in contracts as well as in the law of tort. For example, *Hadley v. Baxendale*, a significant case from 1854 that developed the principles of remoteness and foreseeability of damages in contract law, is regarded as one of the cases that helped establish tort and negligence law, alongside *Donoghue v. Stevenson*. *Hadley v. Baxendale* was a case, involving a broken mill shaft, the court found that the party in breach is accountable for damages that naturally arise (in the usual course of things) or may have been conceivably expected by both parties at the time of the contract formation. These cases' underlying principles established fundamental contract law ideas that are still relevant today.

Technology advancements now allow for online contract execution, eliminating the need for in-person meetings. With the introduction of Smart Contracts, Nick Szabo advances the concept. "A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises," (Szabo, 1996). Based on this concept, contracts not only be created online but also implemented without the need for human intervention. According to this theory, smart contracts are just software agents that autonomously carry out activities based on blockchain technology and predefined criteria, mimicking the actions of a human user (Nwana & Ndumu, 1999) as well as developing computer applications that assist users in keeping track of events or performing tasks (Maes, 1994).

Nick Szabo's concept of smart contracts came to life with the development of technology and the debut of blockchain technology in 2009. Satoshi Nakamoto was the person who first popularised blockchain technology. Since he published a paper on Bitcoin in 2008 titled "Bitcoin: A Peer-to-Peer Electronic Cash System," He is acknowledged as the one who invented blockchain technology (Sarmah, 2018). The article's goal was to discuss the problem of double expenditure. In other words, the ability to easily replicate and duplicate the use of digital currency is inherent in its design. The uncertainty that resulted prevented the method from being deployed. This issue was addressed by tamper-resistant links between each transaction and the transaction that came before it in the Nakamoto paper (Popovski, Soussou & Webb, 2018).

In July 2015, seven years later, Ethereum was released. This enables developers to create and execute complicated smart contracts with programmable logic, loops, and branching conditions. Ethereum allows for the global execution of distributed software (such as smart contracts), earning it the label of "world computer". Ferretti & D'Angelo (2020) further stress that the blockchain maintains a complete record of everything. As a result, every node synchronizes its replicated state using the blockchain in a fashion that can be fully verified by every system user. For this reason, the distributed program that runs on the blockchain is referred to as a

"smart contract". Once it has been deployed, it cannot be altered. Parties agreeing to utilize this code are therefore aware that no contract breach is possible. Instead of always occurring via a blockchain, the majority of the advantages of digitally recording legal contracts originate from the exact definition and autonomous operation of a piece of programmable software (Crafa et al., 2023).

The subsequent emergence of Turing Complete, in addition to Ethereum, has contributed to the present growth of smart contracts. Turing Complete is a system that can be used to solve any algorithm, regardless of complexity (a computer system, programming language, etc.) (NIST, n.d). Anyone can construct smart contracts and decentralized apps on a blockchain by integrating their own Turing-complete programming language, which enables users to define their own arbitrary ownership rules, transaction formats, and state transition mechanisms (Buterin, 2014).

In essence, the evolution of contract law can be traced back to prehistoric Mesopotamia, Egypt, and ancient Greece. Later, it was incorporated into Roman civilization, and during the Middle Ages, the common law tradition developed in England. Later, it was utilized in the development of the Internet and blockchain technology, ultimately leading to the realization of smart contracts. The primary concern is whether the current regulatory framework can keep up with the rapid growth of this technology, particularly from the standpoint of contract law, given the swift changes in technology and the use of smart contracts for contract execution. Therefore, the existing Malaysian and other countries' regulatory frameworks will be further examined to determine whether Malaysia and other nations are sufficiently prepared to govern smart contracts.

Regulatory Framework for Smart Contracts in Malaysia and Other Countries.

Among the challenges encountered in implementation due to the lack of specific laws governing smart contracts. Most countries rely heavily on the conventional regulatory framework that may sometimes not be suitable to implement and may raise various legal issues on the validity of smart contracts.

For example, in the United States of America (USA), Arizona passed Bill HB 241712 in 2017 which made it clearer how blockchain technology, including smart contracts, can be used in business transactions involving the sale of commodities, leases, and title papers. Amendments to the Arizona Electronic Transactions Act, which formally recognize electronic records and signatures, rather than new legislation, were passed. The new law makes it clear that electronic records, electronic signatures, and smart contracts protected by blockchain technology are recognized by law as existing in an electronic form. The act further states that the legality, validity, or enforceability of smart contract provisions cannot be disputed (Ferreira, 2021). This is the first attempt in the United States of America to legally recognize smart contracts and to eliminate legal uncertainty in that particular state.

In March 2018, Tennessee approved legislation (Bill SB 166213) that grants smart contracts in the marketplace legal legitimacy. Tennessee recognizes that smart contracts cannot be denied legal effect, validity, or enforceability under state law and that they "may exist in commerce." Following Arizona's laws are the definitions of blockchain and smart contracts. The Tennessee law further stipulates that contracts, records, and signatures secured by a party using blockchain technology would be deemed to be electronic records and electronic signatures (Tashakor, 2018).

Bosco (2018) however criticizes the uniformity of the existing smart contracts in the USA a previously universal legislation could become less universal due to different definitions, which would undoubtedly obstruct commerce this is among the weaknesses in terms of the smart contracts in the USA because of different definitions in smart contracts across states in the USA. For example, Nevada does not require blockchains to be "immutable" or to "provide an uncensored truth," records or signatures created, stored, or confirmed. By this definition, a smart contract in Nevada may not be legitimate in Arizona. This is because it might not "guarantee the consistency or nonrepudiation" of the transactions or data recorded on it. This means a blockchain that satisfies Tennessee's criteria might not be accepted or satisfy the criteria and definition of smart contracts in Nevada. In short, when the definition of a smart contract is made too specific and no uniformity between one state to another, it can create confusion and it will affect the legality of smart contracts as a whole due to the differences in the definition between one state and another.

Meanwhile in Malta, to control and develop a legislative framework relevant to distributed ledger technology, blockchain technology, smart contracts, and other connected components, the Malta Digital Innovation Authority Act 2018 was founded. Additionally, this law encourages the consistent execution of laws both locally and beyond boundaries. Section 2 of this Act for example clearly defines smart contracts to avoid uncertainty. According to this section, "Smart contract" refers to a type of creative technology agreement made up of a computer protocol and/or an agreement in an electronic form, which is automatable and enforceable by execution of computer code.

In addition to that, the law also includes immutable cryptography, distributed, decentralized, shared, and/or replicated ledgers, smart contracts, and related applications, among other technology arrangements, when defining technology arrangements. It also fulfills duties mandated by applicable legislation to stop money laundering, safeguard personal information, and uphold consumer rights (Atiyah, Manap & Abd Aziz, 2022).

Apart from that as for Switzerland, this is an example of a country that provides a conducive and smart contracts-friendly environment through its regulatory framework despite not having specific statutes for smart contracts. The main regulatory framework for smart contracts in Switzerland is the Federal Council report-Regulatory Framework for Distributed Ledger Technology and Blockchain in Switzerland. As the doctrine generally agrees, a smart contract is not a contract in the sense of the Swiss Code of Obligations, despite what its name would imply. Instead, from Switzerland's perspective, a smart contract is computer "technology" for contract implementation (Patblaser, 2018). This report also argues that a smart contract is a "computerized transaction protocol that executes the terms of a contract," according to Nick Szobo's definition. Hence smart contracts are considered mere technology to execute the contract, smart contracts itself is not contracts.

As for the United Arab Emirates (UAE), this country is heading towards the formation of a smart city in Dubai. To make this idea into reality, the UAE developed a regulatory framework conducive to the implementation of smart contracts. There are a few regulatory frameworks that are vital to facilitate smart contracts. For example, Law No. 2 of 2002 on Electronic Transactions and Commerce (Dubai ECT), Emirate of Dubai, Article 13 holds that a contract's validity and enforceability cannot be contested just because it was concluded through electronic communication. The Federal ECT and Article 14 of the Dubai ECT both recognize the enforcement of automated electronic transactions as relating to any transactions that are entirely or partially concluded by electronic means, even though neither legislation has a description of a smart contract (Atiyah, Manap, & Abd Aziz, 2022). In addition, the UAE enacted a special regulatory framework namely Smart Contracts on Dubai Blockchain Policy to regulate smart contracts.

This is to ensure that all such Smart Contracts are technically and legally examined for compliance with the applicable laws and regulations currently in effect and that such a Smart Contract. For example, Article (17) Smart Contracts on Dubai Blockchain Policy, states requirements for the smart contracts such as it must be accessible by all the parties to the Smart Contract and must be convertible to Arabic or English and readable in the same way by all the parties to the Smart Contract. The combination of an excellent regulatory framework and policy boosts up trust, certainty, and confidence of all stakeholders and users to use smart contracts, especially concerning the usage of smart contracts in the UAE.

In contrast, Malaysia is also among country that does not have any specific regulatory framework for regulating smart contracts. Under common law, a contract must contain four essential components to be enforceable. These include the purpose of establishing legal connections as well as the terms "offer," "acceptance," and "consideration." The contracting parties must abide by the contract's requirements for offer, acceptance, consideration, capacity, intention to establish a legal relationship, free consent, certainty, formalities, and legality. In the case of *Affin Credit (Malaysia) Sdn Bhd v. Yap Yuen Fui* [1984] 1 MLJ 169, the court decided that the alleged hire purchase agreement was void due to the absence of offer and acceptance.

The Contracts Act 1950 (or "CA"), which is in effect in Malaysia, regulates the creation, performance, and enforceability of contracts. Historically, it has only been used for traditional contracts, but if a smart contract satisfies the Contract Act requirements and meets the basic characteristics of a contract as outlined above, it may arguably be considered valid and lawful in Malaysia (Yi & Singh, 2022).

According to Shariff (2006), the concept of electronic transactions is very similar to traditional business transactions based on paper. However, in practice, the way that electronic contracts are created compared to traditional trade transactions creates additional technological and legal issues. Amin & Nor (2011) suggested that as online contracting is now standard practice, the legislation needs to be changed to account for technology and recognize e-contracting security as a matter that needs to be addressed going forward. The idea of trade in a time of modern technology shows the necessity for a law that explicitly addresses the problem of online contracts. It is hoped that lawmakers will take aggressive measures to create rules that will govern Malaysia's unclear and weak provisions governing the formation of internet contracts (Razak, & Ghadas, 2020). For online contracts that utilize advanced and sophisticated technology like smart contracts, a specific regulatory framework must be created to provide clarity on many issues surrounding smart contracts.

This is because Malaysia only relies on two main considerably outdated laws, namely the Electronic Commerce Act 2006 (ECA) to provide legal recognition to smart contracts and the Contract Act 1950 which was enacted before the independence of Malaysia. Regulators should also consider introducing enabling laws to clarify and remove any uncertainty regarding the status of contracts that use smart contracts including smart tenancies (Yong, Tay, & Khong, 2022). Similarly, when it comes to these modern advancements in blockchain technology and smart contracts, the Malaysian legal system can be regarded as practical and realistic. However, it is advised that the definition of an electronic transaction be broadened to include Blockchain and smart contract transactions.

In a nutshell, regulatory frameworks in above mentioned countries, USA, Malta, Switzerland, and UAE have sufficient regulatory frameworks to regulate the operation of smart contracts in each of their respective countries. In Malaysia however, there is no specific regulatory framework to govern smart contracts. Considering the complex and sophisticated technologies that have been utilized in the formation of smart contracts, there are a few legal issues that require urgent attention from lawmakers.

4. Smart Contracts and Legal Concerns in Malaysia

Legal Status of Smart Contract

A smart contract must fulfill all the elements of a contract generally to be considered one, be legally valid, and be enforceable. A "smart contract" could be used to enable the determination of contractual obligations, the partial performance of a contract, or the implementation of contractual remedies, but it could not be treated as a contract if all of these conditions were not met (Filatova, 2020). Similarly, Durovic (2021) raised a question as to whether algorithmic contracts can fulfill the requirements to form valid contracts. On the other hand, Mezquita et al., (2019) assert that when a Smart Contract is executed in a contractually binding way, it is considered valid because it has a legitimate purpose, a valid cause, and the assent of the persons involved. This indicates that the status of the validity of smart contracts is still being questioned by various authors all around the world.

Despite the existence of these laws, it does not address all the issues emerging in practice, especially in Malaysia. This is due to several factors. First, because the technology that gave rise to smart contracts is still under development, it is difficult to expound on any enduring ideas in the sector because things could change very quickly (Reggie, 2017). Second, since smart contracts were created to be technically resistant to any legal interference and adhere to their technological norms, it is frequently acknowledged that the law itself is an ineffective regulatory instrument (Usha, 2019). For example, the immutability and decentralization nature of smart contracts prohibits the execution of smart contracts by anyone even by the court through an injunction.

Without proper legal recognition of the legality of smart contracts, contracting parties may object to the legality of smart contracts especially when one of the parties wants to find a way to fulfill their contractual obligation (Azlan, et al., 2019). Today, many scholars still debating on the legality of smart contracts. As opposed to countries that had been discussed earlier, each of the countries already indirectly provides legal recognition to smart contracts. In Malaysia to this date, there is no regulatory framework that recognizes whether smart contracts are legal or illegal and Malaysia still relies on the outdated Electronic Commerce Act 2006 (ECA) and the Contract Act 1950 which was enacted before the independence of Malaysia.

The validity of the executed smart contract raises security risks if the data supplied by oracles turns out to be erroneous. Smart contracts may rely on external data sources, such as stock prices or weather reports, which can be challenging to verify and may raise security concerns (Patrick, 2018). But it is strongly advised that a request data from numerous oracles rather than just one to get around this problem. Oracles come in a variety of forms. Provable Oracle is one of them. Designing systems for data authentication has become a core competency for Provable. These methods, which offer the audibility of Oracle's service record in delivering untampered data, are known as authenticity proofs (Provable Oracle, n.d). However, the data that Oracles supply may be restricted and easily manipulated. In the future, more oracle manipulation attacks will undoubtedly appear as the Ethereum network expands and smart contracts depend more and more on oracles for various types of information (Tjiam, et al., 2021).

If the information used by Oracles is contaminated with unwanted information and has been manipulated, it contradicts the consent and initial intention of the contracting parties. This is in line with the prerequisite under s.14 of Malaysian Contract 1950 which states that Consent is said to be free when it is not caused by coercion, undue influence, fraud, misrepresentation, or mistake. To overcome the issue, a specific regulatory framework must be designed to prevent unwanted situations due to the manipulation of the Oracles system. As discussed earlier, once smart contracts have been executed, it is almost impossible to stop them due to the immutability nature of smart contracts.

In summary, while smart contracts may make use of external third-party technology, such as Oracle, it also needs to be regulated to avoid this technology having adverse impacts that could compromise the legality of the contract as a whole.

Capacity

Capacity is another problem with smart contracts. What transpires if persons who lack the necessary capacity enter a smart contract given that such contracts can be entered anonymously? The ability of a party to enter into a contract is referred to as contractual capacity. A minor, or someone under the age of 18, is generally not allowed to enter into a contract under English law because they lack the legal capacity to do so.

Similar to the UAE, where persons can now conduct business at the age of 18 by the recently changed Federal Decree-Law No. 50 of 2022 on Commercial Transactions in the UAE, as opposed to the prior legal age of 21. Similar to other countries, Malaysia's Age of Majority Act of 1971 specifies that an individual must be 18 years old to operate a business. The parties must be competent under Section 10(1) of the Contract Act 1950 to engage in a contract. This must be read in conjunction with section 11, which clarifies further that parties to a contract must be of legal age, of sound mind, and not otherwise barred from entering into contracts (such as being bankrupt).

Capacity is another legal issue that needs to be resolved in a smart contract, especially since a smart contract uses complex and advanced technology to execute this contract. According to the Contract Act 1950, those lacking the ability to consent, such as minors, those with serious mental disorders, and intoxicated people, are not qualified to perform a contract. Although minors are now prohibited from owning credit cards or accounts with payment services like PayPal, William, and Peters (2022) argue that there is no legal limitation on minors having private encryption keys or owning Bitcoin. As a result, even if they do without the legal authority to do so, minors can hold this money and participate in smart contracts. What went wrong with the smart contracts, and how can it be avoided in future ones? This is because, according to the Contract Act 1950 that had been discussed previously, the contract will not be valid.

Recommendations For Regulating Smart Contracts in Malaysia.

There are a few recommendations concerning smart contracts. Firstly, regarding the legality and the legal status of smart contracts, smart contracts must be acknowledged in specific as one form of contract that has been legally recognized by the law of that particular state. Taking UAE as an example, UAE provides conducive regulatory frameworks to foster the development of smart contracts in its country through its statutes and policy including but not limited to Electronic Transactions and Commerce Law No.2/2002, Federal Law No. 1 of 2006 on Electronic Commerce and Transaction as well as Smart Contracts on Dubai Blockchain Policy which cover many important elements of contracts as been discussed priorly.

As highlighted by Reggie (2017), the technology that gave rise to smart contracts is still under development, it is difficult to expound on any enduring ideas in the sector because things could change very quickly. Hence, by taking into consideration this factor, the regulatory framework is not necessarily in the form of rigid and difficult-to-amend statutes, it also can be done in the form of guidelines or policies that have been done in UAE (Haniff et al, 2019). Any necessary amendments can be done through specific government agencies (for example in UAE, the Digital Dubai Authority had been established to create a smart city and to amend policy relating to smart contracts).

Furthermore, issues relating to Oracles' validity and certainty must also be considered. It is strongly suggested that the auditing process needs to be made compulsory to prevent any bugs, malfunctions, or interference with the Oracles system. This must be codified in the regulatory framework. To increase audit efficiency and effectiveness as well as to meet the informational needs of various stakeholders for quicker and more transparent audit reporting, smart audit procedures (such as the analyses of audit evidence) are now included in blockchain smart contracts (Rozario, & Vasarhelyi, 2018). Smart contract flaws could result in significant monetary losses. Before releasing the contract, an audit can be used to find any security flaws in the smart contracts system (He, et al., 2020).

A proper audit is also significant to overcome any cyber-attack on the system. The most well-known smart contract mishap was caused by distributed autonomous organizations or DAOs, the largest blockchain project that uses crowdfunding and with assets valued at around USD 60 million. When the DAO was attacked in 2016, a recursive call in its smart contract that had been ruthlessly altered caused it to incur a large loss (Li et al, 2020). The range of security audit tools available for smart contracts is remarkable, but so is the range of security issues and processing capacities they can support. Only a small percentage of known vulnerabilities can be found by most audit tools, and accuracy still has to be increased (Mense & Fletcher, 2018).

Lastly, in terms of capacity, it is recommended necessary general particular contracting parties be disclosed. This prevents a minor or party that doesn't have the necessary capacity to enter into a contract with each other. For example, the Consumer Protection (Electronic Trade Transactions) Regulations 2012 provides a few business details for contracting parties to know who they contracted to. Among the details that need to be disclosed such as the name of the business, the company name, the business registration number, the phone number, email address, and/or address of the business owner if they operate a website or other online marketplace where they sell goods or services.

5. Conclusion

As previously discussed, Statista (2023) indicates that by December 2022, there will be 425 million Bitcoin users, up from just 5 million in 2016. This is an increase of 85 times over six years. Because of its many benefits, cryptocurrency has been included in smart contracts. This suggests that there is a significant amount of smart contract transactions worldwide. Nevertheless, the number of legal issues that may arise due to the lack of a proper regulatory framework put many smart contracts on edge. Most countries including Malaysia still rely on archaic regulatory frameworks which may not apply to smart contracts due to their unique nature.

This study highlights the existing gap in Malaysia's regulatory systems, particularly in terms of the legal status of smart contracts, the validity and certainty of Oracles as well as the issue of capacity. Recommendations were made to rectify the issue through comparative assessments with different jurisdictions.

Nonetheless, the absence of primary data, particularly in the form of expert interviews within the smart contracts field, highlights the research's limitations. This restricts the possible understanding of the importance of this research. It is advised that to increase the validation and generalizability of this field, future studies incorporate primary data as well to obtain first-hand expert opinions on this matter, particularly from nations that have been examined and discussed.

References

- Amin, N., & Nor, M. R. (2011). Issues on Essential Elements of Formation of E-Contracts in Atiyah, G. A., Manap, N. A., & Abd Aziz, S. N. (2022). Smart Contract in Iraq: A Regulatory Framework. *Journal of Positive School Psychology*, 6385-6392.
- Anthony, J. O., Nancy, L. L. and Kathleen, M. T. C. (2012). The Qualitative Report 2012 Volume 17, Article 56, 1-28, Retrieved October 27, 2021, from <http://www.nova.edu/ssss/QR/QR17/onwuegbuzie.pdf>
- Azlan, W. A., Haniff, W., Hakimah, A., Halim, A., & Ismail, R. (2019). Equity crowdfunding in Malaysia: Legal and Sharia challenges.
- Bahga, A., & Madisetti, V. K. (2016). Blockchain platform for industrial Internet of things. *Journal of Software Engineering and Applications*, 9(10), 533-546.
- Bieser, G. (2014). Smart Grids in the European Energy Sector. *International Economics and Economic Policy*, 11(1-2), 251-259.
- Bosco, A. J. (2018). Blockchain and the Uniform Electronic Transactions Act. *Bus. Law.*, 74, 243.
- Buterin, V. (2014). A Next-Generation Smart Contract and Decentralized Application Platform. *White Paper*, 3(37), 2-1.
- Clifford Chance and European Bank for Reconstruction and Development. *Smart contracts: Regulatory framework and Proposed Guidelines For Lawmakers*. 2017
- Crafa, S., Laneve, C., Sartor, G., & Veschetti, A. (2023). Pacta Sunt Servanda: Legal Contracts in Stipula. *Science of Computer Programming*, 225, 102911.
- Durovic, M. (2021). What are smart contracts? *Digital Technologies and the Law of Obligations*, 121.
- Ferreira, A. (2021). Regulating Smart Contracts: Legal Revolution or Simply Evolution? *Telecommunications Policy*, 45(2), 102081.
- Ferretti, S., & D'Angelo, G. (2020). On the Ethereum Blockchain Structure: A Complex Networks Theory Perspective. *Concurrency and Computation: Practice and Experience*, 32(12), e5493
- Filatova, N. (2020). Smart contracts from the contract law perspective: outlining new regulative strategies. *International Journal of Law and Information Technology*, 28(3), 217-242.
- Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and Smart Insurance Contracts: Is The Technology Mature Enough? *Future internet*, 10(2), 20.
- Giancaspro, M. (2017). Is a 'Smart Contract' Really a Smart Idea? Insights from a legal perspective. *Computer Law and Security Review*, 33(6), 825-835.
- Haniff, W. A. A. W., Halim, A. H. A., & AH A & Ismail, R. (2019). The regulation of equity crowdfunding in the United Kingdom and Malaysia: A comparative study. *Academic Journal of Interdisciplinary Studies*, 8(3), 45-56.
- He, D., Deng, Z., Zhang, Y., Chan, S., Cheng, Y., & Guizani, N. (2020). Smart Contract Vulnerability Analysis and Security Audit. *IEEE Network*, 1-7 Issue), 2219-2229.
- Jafari, S., Vo-Huu, T., Jabiyev, B., Mera, A., & Mirzazade Farkhani, R. (2018). *Cryptocurrency: A Challenge to Legal System*. SSRN Electronic Journal
- Jain, N. (2005). A separate law for peacekeepers: the clash between the Security Council and the International Criminal Court. *European Journal of International Law*, 16(2), 239-254.
- Kizza, J. M. (2020). *Blockchains, Cryptocurrency, and Smart Contracts Technology: Security Considerations*. Springer Nature Switzerland AG
- Li X., Jiang P., Chen T., Luo X., and Wen. Q (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems*, 107, 841-853
- Maes, P. (1994). Agents that reduce work and information overload, *Communications of the ACM*, 37(7), 30-40
- Maine, H. S. (2019). *Ancient Law: Its Connection to The History Of Early Society*. Good Press.
- Mense. A & Fletcher. M. (2018). *Security Vulnerabilities In Ethereum Smart Contracts* in 20th International Conference on Information Integration and Web-based Applications & Services, 375-380
- Mezquita, Y., Valdeolmillos, D., González-Briones, A., Prieto, J., & Corchado, J. M. (2019). *Legal Aspects and Emerging Risks in The Use Of Smart Contracts Based On Blockchain*. In Knowledge Management in Organizations: 14th International Conference, KMO 2019, Zamora, Spain, July 15-18, 2019, Proceedings 14, 525-535. Springer International Publishing
- NIST.(n.d). Computer Security Resource Centre. Definition of Turing Complete. Retrieved June 21, 2023, from https://csrc.nist.gov/glossary/term/turing_complete#:~:text=Share%20to%20Facebook%20Share%20to,complexity%2C%20to%20find%20a%20solution.

- Nwana, H. S. & Ndumu, D. T. (1999). A perspective on software agents research, *The Knowledge Engineering Review*, 14(2) 125-142.
- Patblaser. (2018). Federal Council report "Regulatory framework for distributed ledger technology and blockchain in Switzerland." Blockchain Federation. Retrieved July 15, 2023, from <https://blockchainfederation.ch/federal-council-report-legal-framework-for-distributed-ledger-technology-and-blockchain-in-switzerland/?lang=en>
- Patrick. (2018). Blockchain Oracles Explained. Mycryptopedia. Retrieved July 15, 2023, from <https://www.mycryptopedia.com/blockchain-oracles-explained/>
- Peng, M. W. (2001). How entrepreneurs create wealth in transition economies. *Academy of Management Perspectives*, 15(1), 95-108.
- Peters, R. (2022, July 26). How to Buy Bitcoin When You're Underage in 2023? Retrieved July 16, 2023, from CaptainAltcoin. <https://captainaltcoin.com/buy-bitcoin-underage/>
- Popovski, L., Soussou, G., & Webb, P. B. (2018). *A Brief History of Blockchain*. Legaltech
- Posner, Richard A. 1977. Economic Analysis of Law, 2nd ed. Boston: Little Brown. 1980. A Theory of Primitive Society, with Special Reference to Law, *Journal of Law and Economics* (23) 1-53
- Provable Oracle. (n.d.). Docs.provable.xyz. Retrieved July 16, 2023, from <https://docs.provable.xyz/>
- Razak, F. A., & Ghadas, Z. A. A. (2020). From Barter System to E-Contract: Development on
- Reggie O. (2017). Smart Contracts: Legal Agreements for the Blockchain. 21 NC. *Banking Inst*, 177, 194
- Rozario, A. M., & Vasarhelyi, M. A. (2018). Auditing with Smart Contracts. *International Journal of Digital Accounting Research*, 18.
- Sarmah, S. S. (2018). Understanding blockchain technology. *Computer Science and Engineering*, 8(2), 23-29.
- Savelyev, A. (2017). Contract Law 2.0: 'Smart' contracts As The Beginning Of The End Of Classic Contract Law. *Information & Communications Technology Law*, 26(2), 116-134.
- Shariff, M. R. N. (2006). The Role of UNCITRAL in Regulating E-Contracts in the Emerging ECommerce. *Proceedings of the International Conference on E-Commerce*, 95-103.
- Statista. (2023). Cryptocurrency users worldwide 2020. Retrieved June 21, 2023, from <https://www.statista.com/statistics/1202503/global-cryptocurrency-user-base/>
- Szabo, N. (1997). Smart Contracts: Formalizing And Securing Relationships on Public Networks. *First Monday*, 2(9).
- Tashakor, M. (2018). The New Kid on The Blockchain: Legislative Acceptance of Smart Contracts. *Georgetown Law Technology Review*. Retrieved July 15, 2023, from <https://georgetownlawtechreview.org/the-new-kid-on-the-blockchain-legislative-acceptance-of-smart-contracts/GLTR-04-2018/GE>.
- Tjiam, K., Wang, R., Chen, H., & Liang, K. (2021). Your Smart Contracts Are Not Secure: Investigating Arbitrageurs and Oracle Manipulators in Ethereum. In CYSARM@ CCS (25-35).
- Usha, R. R. (2019). Law and the Blockchain. 104 *Iowa Law Rev*, 679
- Xu, Y., Chong, H. Y., & Chi, M. (2021). A Review Of Smart Contracts Applications in Various Industries: A Procurement Perspective. *Advances in Civil Engineering*, 1-25.
- Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain Technology Overview*. National Institute of Standards and Technology.
- Yi, S. A.F. J., & Singh, H. K. H. (2022). *Enforceability of Smart Contracts in Malaysia*. Lexology. Retrieved July 15, 2023, from <https://www.lexology.com/library/detail.aspx?g=2f54dde8-5980-4aed-9159-86d6ac20eca6#:~:text=The%20Legal%20Status%20of%20Smart%20Contracts%20in%20Malaysia&text=Generally%2C%20if%20there%2>
- Yong, K. J., Tay, E. S., & Khong, D. W. (2022). Application of blockchain smart contracts in smart tenancies: A Malaysian perspective. *Cogent Social Sciences*, 8(1), 2111850
- Zimmermann, R. (2009). *Roman law and the harmonization of private law in Europe. Towards a European Civil Code*, 27-53.