Samarah: Jurnal Hukum Keluarga dan Hukum Islam
Volume 8. No. 1. March 2024
ISSN: 2549 – 3132; E-ISSN: 2549 – 3167
DOI: 10.22373/sjhk.v8i1.16372

The Position of Smart Contracts in the Light of Islamic Contract Theory

Azlin Alisa Ahmad
Faculty of Islamic Studies, Universiti Kebangsaan Malaysia
Mat Noor Mat Zain
Faculty of Islamic Studies, Universiti Kebangsaan Malaysia
Nur Diyana Amanina Zakaria
Faculty of Islamic Studies, Universiti Kebangsaan Malaysia
Email: azlinalisa@ukm.edu.my

Abstract: Smart contracts are simply programs stored in a blockchain that run under predetermined conditions; however, they are yet to be implemented commercially in the financial industry, including the Islamic financial industry. It has not been entirely implemented in the Islamic financial industry because it is unstable and there are debates regarding its conformity with Shariah principles. Since the development of the smart contract is still in the preliminary stages, its position in an Islamic contract is yet to be determined. Does a smart contract blockchain comply with Islamic contract theory? This qualitative study aims to analyse the smart contract's position based on Islamic contract theory. Data were obtained using content analysis and interview methods, in which the semi-structured interview involved Islamic financial experts and industry players. Data were then analysed using the QDA Miner version 5.0.31 software. Findings indicate that a smart contract differs from other contracts because it records every transaction using hash cryptography and computer codes known as *solidity*. Besides that, transactions did not adhere to two principles of an Islamic contract, namely the existence of autonomy in the contracting parties and the ability to manipulate the contract. Hence, Shariah-based risks in a smart contract can be decreased by improving the Shariah compliance aspect in the transaction to solve autonomy issues and the manipulation of contracts. The study implies that a smart contract has the potential to become an innovation in the Islamic financial industry if it can adhere to the principles of an Islamic contract and it can be monitored by relevant authorities.

***Keywords*:** Smart contract, blockchain, Islamic contract, Islamic finance

‖ Submitted: December 25, 2022 ‖ Accepted: January 27, 2024 ‖Published: January 27, 2024

Abstrak: *Kontrak pintar ialah program yang disimpan dalam blockchain yang berjalan di bawah kondisi yang telah ditentukan sebelumnya. Namun, hal tersebut belum dapat diimplementasikan secara komersial pada industri keuangan, termasuk industri keuangan syariah. Kontrak pintar belum sepenuhnya diterapkan di industri keuangan Islam karena tidak stabil dan ada perdebatan mengenai kesesuaiannya dengan prinsip syariah. Karena perkembangan kontrak pintar masih dalam tahap awal, posisinya dalam kontrak Islam belum ditentukan. Apakah kontrak pintar blockchain sesuai dengan teori kontrak Islam? Penelitian kualitatif ini bertujuan untuk menganalisis posisi kontrak pintar berdasarkan teori kontrak Islam. Data diperoleh dengan menggunakan metode analisis isi dan wawancara, dimana wawancara semi terstruktur melibatkan pakar keuangan syariah dan pelaku industri. Data kemudian dianalisis menggunakan perangkat lunak QDA Miner versi 5.0.31. Hasil penelitian menunjukkan bahwa smart contract berbeda dari kontrak lain karena mencatat setiap transaksi menggunakan kriptografi hash dan kode komputer yang dikenal sebagai soliditas. Selain itu, transaksi tidak menganut dua prinsip akad Islam, yaitu adanya otonomi pihak yang berkontrak dan kemampuan untuk memanipulasi akad. Oleh karena itu, risiko berbasis Syariah dalam kontrak pintar dapat dikurangi dengan meningkatkan aspek kepatuhan Syariah dalam transaksi untuk mengatasi masalah otonomi dan manipulasi kontrak. Implikasi dari kajian ini adalah kontrak pintar berpotensi menjadi inovasi dalam industri keuangan syariah jika dapat mematuhi prinsip-prinsip kontrak syariah dan dapat dipantau oleh otoritas terkait.*

Kata Kunci: *Kontrak pintar, blockchain, kontrak Islam, keuangan syariah*

Introduction

There is an increase in the development of blockchain technology in the financial industry, especially after the first cryptocurrency was introduced using this technology in 2008. [1] Bitcoin, as a form of cryptocurrency, plays a significant role in a transaction that creates an element of decentralization. The decentralization concept in blockchain has created competition, while restricting the element of centralization required for carrying out tasks and responsibilities. [2]

[1] Aicha Larfi, "Bitcoin Between The Economy and Islamic Law," *International Conference on Islamic Economic* (ICIE) 1, No. 1 (2022), p. 42-56. Mohammad Rashed Hasan Polas, et.al., "Is Bitcoin Halal or Haram in the Islamic Banking and Finance? An Overview," *Journal of Economics, Business and Market Research* 1, No. 2 (2020). Hayes, A. Satoshi Nakamoto. (2021) https://tinyurl.com/5734yv9h [September 1, 2021].

[2] Mohammad Hamed Shahab, et.al., "Cryptocurrencies: A Critical Analysis from the Perspective of Islamic Law, " *Change Management* 22, No. 2 (2022), p. 343-356. Abdulloh Hamid, "Bitcoin As A Means of Transaction and Investment in the Perspective of Islam," *Iqtishoduna: Jurnal Ekonomi Islam* 10, No. 2 (2021).

A smart contract is a transaction in a computer program that is recorded using blockchain technology.[3] Each transaction is recorded in a smart contract summarized in the form of computer code. This type of transaction, which was introduced by Nick Szabo in 2014, provides users the ability to record various transactions in cryptography. The implementation of smart contracts without any control and monitoring from the authorities causes the contract to move freely without any law enforcement because it is a decentralized concept.[4] Research on the relationship between smart contracts and Islamic contracts has yet to be comprehensively conducted by researchers.[5] The existence of blockchain in the financial industry has provided opportunities for irresponsible parties to carry out covert transactions in the black market. For example, the Silk Road crime case introduced by the 'Red Dread Pirates'.[6]

Non-Shariah-compliant activities have been actively carried out in smart contracts beginning in 2015 and 2016[7], such as digital Ponzi scheme activities that promise extraordinary profits to investors. Ponzi schemes contain elements of usury (*riba*), gambling, uncertainty or risk (*gharar*)[8] as well as deception by concealment (*tadlis*) and involve the taking of deposits without permission from authorized parties, which is illegal under the Money Exchange Control Act 1953.[9] Ponzi schemes implemented using smart contracts have caused huge losses to investors. In 2018, investors in this type of scheme had experienced losses estimated to be in the millions of US Dollars caused by hackers who had attacked the smart contract.[10]

[3] Najahudin BIN Lateh and Siti Noorbiah Md Rejab, "Sharia Issues About Bitcoin Cryptocurrency Transactions," in Enhancing Halal Sustainability (2021). p.119-128. Venegas, P. "Crypto Economy Complexity," *Journal of Economic Literature G02*, (2017).

[4] Vitalik Buterin, What Are Smart Contracts & What Is Their Function? (2017). https://www. youtube.com/watch?v=r0s4qimf4pg [June 5, 2018].

[5] Ricard Marc Lacasse, et. al., "Islamic Banking-Towards a Blockchain Monitoring Process 6, no. 1 (2017).

[6] Greenberg, A. In Silk Road Appeal, Ross Ulbritch's Defense Focuses on Corrupt Feds, (2016). https://www.wired.com/2016/01/ross-ulbrichts-defense-focuses-on- corrupt-feds-in-silk-road-appeal/ [July 15, 2019].

[7] Bartoletti, Massimo and Livio Pompianu, "An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns," *Frontiers in Blockchain*, 3 no. 27 (2020).

[8] Qazeem Adedamola Adebumiti and Abdullahi Saliu Ishola, "Beyond Riba, Maysir and Gharar Transactions: The No-Go Areas for Islamic Finance Industry," International Seminar on Islamic Jurisprudence in Contemporary Society at Universiti Sultan Zainal Abidin, Terrengganu, Malaysia (2017).

[9] Abdul Muhaimin Mahmood, "Konsep Akad Dan Jenisnya Dalam Muamalat Islam", Jabatan Kemajuan Islam Malaysia, 2020, https://e-muamalat.islam.gov.my/en/bahan-ilmiah/artikel/156-konsep-akad-dan-jenisnya-dalam-muamalat-islam.

[10] Humiston, P. Smart Contract Attacks [Part 2] – Ponzi Games Gone Wrong, (2018). https://medium.com/hackernoon/smart-contract-attacks-part-2-ponzi-games- gone-wrong-d5a8b1a98dd8 [July 6, 2019].

Smart contracts have been used in money laundering activities as well. This issue was perpetrated by a company that operated a cryptocurrency exchange known as Mt. Gox.[11] Action must be taken if there are elements that involve the violation of Islamic contract principles in a smart contract. Based on a report by the Islamic Financial and Services Board,[12] a scientific study is required to examine whether smart contract innovations are categorized as innovations in Islamic financial technology.

This qualitative study applied the case study approach and data were collected using the content analysis and interview methods. Among the documents used in the content analysis included the al-Qur'an, al-Hadith, conference reports, journal articles, legal acts, newspapers, media, books, videos, memos, and so on. As for the interview method, five respondents were selected comprising Respondent A (economist), B and C (founders of Blocklime) as well as D and E (blockchain technology players). Data were analysed using the QDA Miner version 5.0.31 software, which is capable of handling various types of data as well as providing regular and accurate data analysis in a short time. Data from the interview were then transcribed based on codes or themes. The coding process is described in the form of a table to systematically summarize the information. The objective of this study is to analyse the position of smart contracts based on Islamic contract theory. The study analysis was based on Islamic contract principles agreed upon by the majority of contemporary scholars.

The Blockchain Technology Concept

Blockchain is a technology network that allows various types of transactions to be carried out in a decentralized manner. Consumers are allowed to carry out transactions involving only two parties without the involvement of intermediaries representing lawyers, banks, etc. In order to maintain the decentralization concept, certain tokens known as cryptocurrency are used as a medium of exchange or in lieu of the current currency. Cryptocurrencies only work in the blockchain network and each transaction is subject to a transaction fee based on the value of the cryptocurrency.[13]

Blockchain is an innovation capable of digitally developing every business industry. The implementation of smart contracts in a blockchain is the

[11] Norry, A. The History of Mt. Gox Hack: Bitcoin's Biggest Heist, (2020). https:// blockonomi.com/mt-gox-hack/ [April 1, 2020].

[12] Islamic Financial Services Board, *Islamic Financial Services Industry Stability Report,* (2017).

[13] Pilkington, Marc. "Blockchain technology: principles and applications" Research Handbook on Digital Transformations. Edited by F. Xavier Olleros and Majlinda Zhegu, Northampton: Edward Elgar Publishing, Inc. (2016), p. 225–253.

best alternative to a classical contract.[14] The innovation and implementation of smart contracts in the blockchain are able to automate every classical contract executed manually that requires complicated procedures.

Each execution of a transaction in the blockchain uses a cryptographic encoding called a cryptographic hash. Hash cryptography was introduced by Harber and Stornetta in their first paper on a chained block that protects cryptography using time-stamped document theory.[15] Next, Harber and Stornetta upgraded the study to a new method called hash cryptography. Some of the important elements in blockchain technology are autonomy, transparency, immutability, and pseudonymity.

1. Autonomy

Autonomy means that the parties involved in this application are not controlled by factors external to the organization. Autonomy also means that the parties involved in the transaction only use pseudonyms. Autonomous applications were introduced into a smart contract in 2016 and were called a Decentralized Autonomous Organization (DAO).[16] Buterin stated that the incorporation of DOAs into a smart contract is a virtual entity concept where a group of members carry out the transaction.[17] Each transaction in the blockchain is executed by algorithms and platforms through consensus or as an autonomous virtual entity and executed autonomously.

In other words, a DAO has a group of anonymous members who interact openly. The DAO is responsible for ensuring the reduction of transaction costs and adopting rules of consensus that are bound only by crypto tokens. The DAO is not involved in any legitimate legal corporation; however, smart contracts are managed automatically based on tokens and protocols that have been established in the blockchain.

2. Transparency

Every transaction recorded in a smart contract is transparent, which means that anyone can see the transaction. Transactions that can be seen by outsiders are processed using computer codes.

[14] Meijer, Carlo De, "Blockchain and derivatives: Re-imagining the industry". Treasury XL. (2017), https://treasuryxl.com/blog/blockchain-and-derivatives-reimagining-the-industry/.

[15] Abraham, I. "The First Blockchain or How to Time-Stamp a Digital Document." (2020), https://decentralizedthoughts.github.io/2020-07-05-the-first-blockchain-or-how-to-time-stamp-a-digital-document/

[16] Siegel, D. "Understanding the DAO Attack", (2016), https://www.coindesk.com /understanding-dao-hack-journalists [March 1, 2018].

[17] Ben van Lier, Can Cyber-Physical Systems Reliably Collaborate within a Blockchain? Blockchain And Cyber-Physical Systems, *Metaphilosophy,* 48 no. 5 (2017).

Figure 1: Smart Contract

```
6080604052 6aa56fa5b99019a5c80000006003553480156 1001f57600080fd5b50600
```

Source: Scott 2019

Observing transparency in smart contracts can foster the element of trust because every information and logic of the transaction can be seen by all blockchain users. In fact, the transaction can only be seen by outside parties but they cannot change anything because it is tied to other blocks.

3. Immutable

The immutability concept is applied in blockchain based on chain bonding that uses hash cryptography. Hash cryptography consists of alphanumeric bonds that are generated differently in each block. This concept aims to ensure that no one tampers with the system or alters the data stored in each block.[18] The immutability concept also plays a role in maintaining each transaction in the blockchain ledger.[19] It also has the potential to transform the audit process involving the data used into a more efficient, faster, cost-saving and integrity-based process.[20]

4. Pseudominity

Pseudominity refers to a nickname,[21] recipients and senders of cryptocurrency in the blockchain are registered using pseudonyms. The

[18] Srivastava, Akash. Understanding Blockchain for Beginners. https://levelup.gitconnected.com/understanding-blockchain-for-beginners-f0aaab7ffcf7

[19] Stephen J. Bigelow, Blockchain: An immutable ledger to replace the database, (2021). https://www.techtarget.com/searchitoperations/tip/Blockchain-An-immutable-ledger-to-replace-the-database.

[20] Politou, E., Casino, F., Alepis, E., & Patsakis, C., Blockchain Mutability: Challenges and Proposed Solutions, *IEEE Transactions on Emerging Topics in Computing*, (2019).

[21] Oettler, M. Anonymity vs Pseudonymity. (2021). https://blockchain-academy.hs-mittweida.

pseudominity concept is similar to the autonomy concept. According to this concept, parties who perform transactions in the blockchain do not have to register a valid identity and are allowed to only use a pseudonym. The pseudominity concept is more practical because it provides a certain ideological satisfaction for radical privacy. Implementation of the pseudominity concept has provided an opportunity for money laundering activities, one example is the Ross Ulbritch case in 2015. Ross Ulbritch used blockchain for money laundering purposes, which concerned buying and selling activities that were illegal.[22]

An Analysis of Smart Contracts Based on Islamic Contract Theory

Islamic contract theory is construed based on the three pillars (fundamentals) of the Islamic contract, namely mutual consent (*sighah*), the contracting parties and the subject of the contract, which have been agreed upon by the majority of the Islamic sects.[23]

Compliance with Smart Contracts Based on the Fundamentals of an Islamic Contract

In order to determine whether smart contract transactions affect the three pillars of an Islamic contract or vice versa, 5 respondents (A, B, C, D, E) were selected for an interview that focused on the smart contract concept involving the interrelationship of the three pillars of an Islamic contract.

Table 1: Respondents' views on the *ijab qabul* method in a smart contract

Question 1	How is a handover implemented in a smart contract?	Code/Theme
Respondent A	Agreement in a smart contract is recorded using the *solidity* language and the transaction is verified by the contracting parties using a *private key*	• Form of *ijab qabul* • *Ijab qabul* method
Respondent B	Transactions are carried out using computer codes and are *permissionless* and *trustless*	• Form of *ijab qabul* • The smart contract concept
Respondent C	A smart contract transaction differs from a classic	• Form of

[22] Greenberg, A. 2016. In Silk Road Appeal, Ross Ulbritch's Defense Focuses on Corrupt Feds. https://www.wired.com/2016/01/ross-ulbrichts-defense-focuses-on- corrupt-feds-in-silk-road-appeal/.

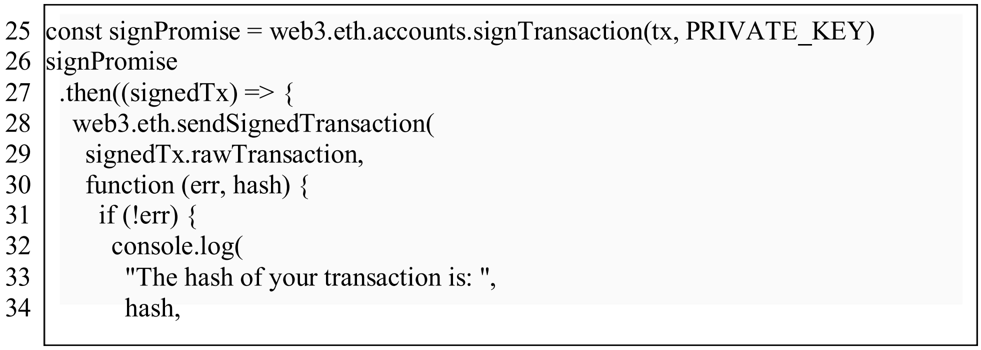
[23] Azlin Alisa Ahmad and Mat Noor Mat Zain, "A Comparative Analysis of Smart Contracts and Islamic Contracts," *International Journal of Advanced Research* 8, No. 10 (2020), p. 316-325. Nor Razinah Mohd Zain and Khairul Azmi Mohamad, "An Evaluation of Smart Contracts: Practices, Legality, and Sharīʻah," In *Islamic FinTech* (2021), p. 91-110.

	contract. Smart contracts are digitalised based on the *blockchain.* *Smart contracts* are written using computer codes and stored in the *blockchain*.	*ijab qabul*
Respondent D	Basically, a smart contract is a contract clause converted into computer code. Post-Bitcoin is a term recreated from Nick Szabo's original term. The redesigning of post-bitcoin aimed to create more than two contracting parties involved in a smart contract. The implementation of smart contracts is agreed upon by the parties involved using a contract code that is *peer-to-peer* and *trustless*	• Form of *ijab qabul* • Background of a smart contract • Principles of the contracting parties Smart contract concept
Respondent E	*Digital media* based on *blockchain* to manage the objective of certain information	• Smart contract concept

Data analysis of the interview session

Findings from the interview sessions, as shown in Table 1, indicate that the *ijab qabul* method implemented in a smart contract is in the written form. The form of writing used in a smart contract is a computer code or computer language, such as solidity, C++, and JavaScript. Solidity is a computer language used in a smart contract drafted by Gavin Wood in 2014. Figure 2 shows an illustration of an *ijab qabul* confirmed by the contracting parties in a smart contract using solidity.

Figure 2: Illustration of an *ijab qabul* in a smart contract



```
25 const signPromise = web3.eth.accounts.signTransaction(tx, PRIVATE_KEY)
26 signPromise
27   .then((signedTx) => {
28     web3.eth.sendSignedTransaction(
29       signedTx.rawTransaction,
30       function (err, hash) {
31         if (!err) {
32           console.log(
33             "The hash of your transaction is: ",
34             hash,
```

Data Source: Ethereum.org official website.

Based on Figure 2, the message on the 25th line shows that the contracting party web3.eth.accounts.sgn. Transactions has signed the transaction using a private key. The confirmation is proof that web3.eth.accounts.sgn.Transactions agreed to submit hash transactions to other contracting parties. However, the transaction was cancelled because there was an error in the execution of the *qabul*. The other contracting party confirmed the binding of the *qabul* by replying 'err', as indicated in the 30th line. The word 'err' in the contract has no meaning but it is known as an error code. On the other hand, the other contracting party needs to confirm the agreement using a private key as a sign of agreement between the *qabul* and *ijab*.

In general, the formation of *ijab qabul* in written form is one of the pronunciations (*lafaz*) methods permitted in Islam. The pronunciation of *ijab qabul* is verified by all parties involved using their respective private keys. However, the purpose of the private key is only meant to confirm transactions in smart contracts. The wording of the transaction must be clear and carefully thought before it is confirmed using the private key. The involvement of *ijab qabul* in smart contracts is important to ensure that the transaction is permitted from an Islamic perspective in accordance with the exhortations of Allah s.w.t[24] regarding the formation of pronunciations (*lafaz*) in writing. The verse explains that every written agreement must be fair and clear, as promised by all the contracting parties involved. A written agreement is permanent and can be used as evidence of the bond between the parties involved. According to Aimi Zulhazmi, the law of *ijab qabul* in smart contracts is comparable to acceptance in electronic contracts. This transaction is presumed to be a *ᶜurf* (customary practice) of a community, where the community is more inclined to carry out online transactions as long as it does not involve elements of *gharar*, fraud or disputes.[25]

Therefore, findings on the similarity between smart contracts and the pillars (fundamentals) of an Islamic contract involve the formation of the pronunciation of *ijab qabul*. Transactions using smart contracts are written using the solidity computer code. The handover in each transaction needs to be accurately and clearly recorded before it is confirmed by the contracting parties using a private key. Thus, there should be no contradictions to Islamic contract principles when the wording of the contract is expressed in a smart contract. Findings show that smart contract transactions are recorded using computer code as a form of an innovation to the formation of written contracts based on Islamic contract principles.

Non-Compliance of Islamic Contract Principles in Smart Contracts

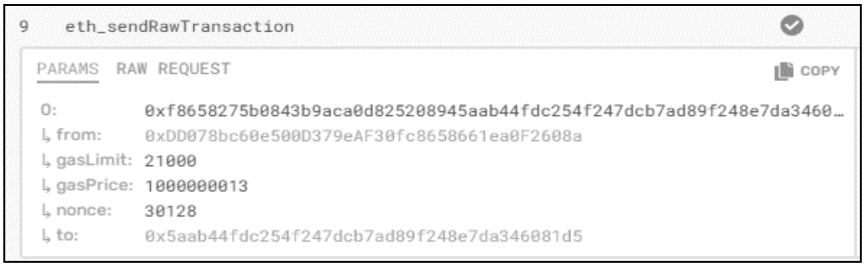
Figure 3 shows the autonomous identity of contracting parties in a smart contract. The contracting parties record their identification as 'web3.eth.accounts.sgnTransactions' and do not use their real names, as shown in Figure 3. The purpose of the introduction is to maintain the concept of autonomous smart contracts. Therefore, the contracting parties are allowed to use a pseudonym in the transaction and the identity of the contracting parties are only based on a nickname and a private key. Each contracting party has a different private key. However, the private key cannot be disclosed publicly and is only known to the owner of the private key. Each transaction in a smart contract is

[24] Al-Quran al-Karim, al-Baqarah 2: 282

[25] Interview with Aimi Zulhazmi, Kuala Lumpur, July 9, 2020.

given a *public address* by the selector of the private key, which is used as the point of delivery for the contact's subject matter in the transaction. Figure 3 shows the handing over (submission and acceptance) of the smart contract using the public address.

Figure 3: Information on the implementation of a smart contact between two parties



```
9    eth_sendRawTransaction

PARAMS   RAW REQUEST                                              COPY

0:           0xf8658275b0843b9aca0d825208945aab44fdc254f247dcb7ad89f248e7da3460…
↳ from:      0xDD078bc60e500D379eAF30fc8658661ea0F2608a
↳ gasLimit:  21000
↳ gasPrice:  1000000013
↳ nonce:     30128
↳ to:        0x5aab44fdc254f247dcb7ad89f248e7da346081d5
```

Source: Alchemy official website

Based on Figure 3, information regarding the contracting parties is not specified in the transaction but it is replaced using a public address. A public address is similar to the user's bank account number or the delivery location and the sender of the transaction. The public address could be in the form of binary code numbers or hash cryptography. The public address will be issued and decoded by the owner of the private key. Table 2 depicts the methods of owning a private key.

Table 2: Private key ownership in a smart contact

Question 4	**How to own a private key?**	**Code/Theme**
Respondent A	Each individual has a different *private key*. The *private key* is found in the c*rypto wallet*	• Method of owning a *private key*
Respondent B	*Crypto wallet*. There are various types of *private keys* used, such as *binary code*, QR code and others	• Method of owning a *private key* Type of *private key*
Respondent C	*Crypto wallet* consists of binance, coinomi and others	• Method of owning a *private key*
Respondent D	All users of the *crypto wallet* are given different private keys	Method of owning a *private key*
Respondent E	*Crypto wallet*	

Data analysis of the 2019 interview

Table 2 explains the methods used by contracting parties to obtain a private key from a crypto wallet, including coinomi, binance and trust crypto wallet. So far, there are no conditions stipulated for obtaining an e-crypto wallet and the conditions of engagement of contracting parties. Transactions can be executed by every crypto wallet and ether token owner. Following is the data analysis of the contracting parties in smart contracts.

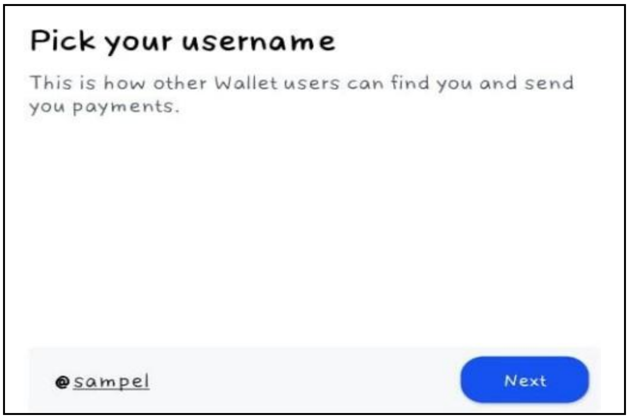
Table 3: Involvement of Contacting Parties in A Smart Contact

Question 2	**Which contracting party is eligible to carry out a smart contract transaction?**	**Code/Theme**
Respondent A	Anyone qualifies to use the application as long as they have an *ether crypto wallet*	• Principles of contracting parties
Respondent B	No conditions are stipulated and anyone is free to use it	• Principles of contracting parties
Respondent C	Have to first buy an ether token. The price of an ether token is affordable and everyone can participate in the transaction	• Principles of contracting parties
Respondent D	A smart contract is open to all regardless of age provided the individual possesses an ether token	• Principles of contracting parties
Respondent E	No conditions are stipulated and there is no legal provision for enforcing this transaction. Hence, there are no qualifying conditions for anyone who wishes to enter a transaction	• Smart contract concept • Principles of contracting parties

Data analysis of the 2019 interview

Table 3 explains the principles observed by contracting parties in a smart contract. The contracting party's involvement in the transaction is open and there are no pre-set conditions. Each contracting party in a smart contract needs to upload a crypto wallet to indicate the possession of crypto money before choosing to execute a smart contract transaction. The crypto wallet can be downloaded in the user's smartphone or personal gadget. Users do not need to verify personal information in the crypto wallet; therefore, the identity of the contracting party is not a priority in this type of transaction. Conversely, the identity of the contracting party is kept confidential by using pseudonyms and does not require verification of personal information. Here are the steps involved in registering a crypto wallet using a trust wallet.

Figure 4: Steps involved in registering a *trust crypto wallet*



Pick your username

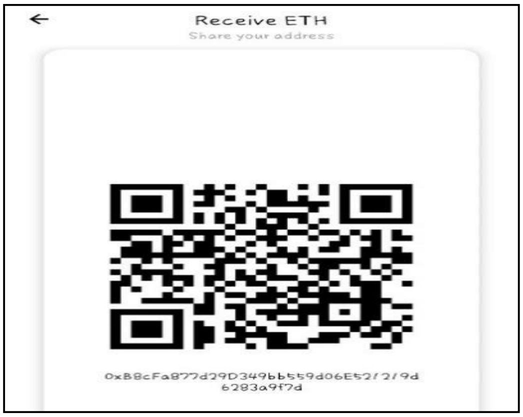
This is how other Wallet users can find you and send you payments.

@sampel

Source: *Trust wallet* application

Figure 4 shows the first step in registering the trust wallet. Users are given the option of selecting a username as the user account's identity. Next, the user is given a mnemonic phrase as a security code and a private key. Users need to memorize the mnemonic phrase to confirm the registration of the crypto wallet. Once the mnemonic phrase is verified in the system, users can carry out crypto transactions using the crypto wallet. Acceptance and transfers can be done using a QR code or binary code as a public address. Figure 5 is an example of a QR code and binary code in a trust crypto wallet.

Figure 5: A sample of a public address in a trust crypto wallet



Receive ETH

Share your address

0xB8cFa877d29D349bb559d06E52/2/9d
6283a9f7d

Source: Trust crypto wallet application

Figure 5 is a sample of a public address in the form of QR and binary codes. QR codes are used only for token transfers between crypto wallets, while a binary code is used in smart contracts and for token transfers between crypto wallets. However, the existence of crypto wallet tokens acts as a transaction involving the buying and selling of crypto tokens. In addition, a crypto wallet is used for gas charge payment transactions, as well as receipt and payment of transactions. The identity of the crypto wallet owner is also affected when involved in a smart contract transaction because the autonomy concept is applied in the transaction. Table 4 depicts the views of respondents regarding the nature of autonomy possessed by contracting parties.

Table 4: The nature of autonomy possessed by contracting parties

Question 3	**Are contracting parties involved in the element of autonomy?**	**Code/Theme**
Respondent A	Correct. The contracting parties have the autonomy because of the decentralisation concept	Autonomy factor
Respondent B	Yes	
Respondent C	Contracting parties in a transaction are identified using the *public address*	Principles of contracting parties
Respondent D	Since the smart contract transaction is recorded using computer codes, the question adduced is correct. Contracting parties have the autonomy. In a smart contract transaction, selling and buying follows the *public address* given to the contracting parties. A *public address* can only be issued and accessed by the owner of a *private key*.	Autonomy factor
Respondent E	Autonomy is the main concept in a smart contract	Autonomy factor

The main purpose of implementing autonomy in smart contracts is to comply with the decentralization concept established in blockchain technology. The decentralization concept was created to protect the rights and priorities of contracting parties.[26] The main purpose of decentralization is to restrict the involvement of authorities and intermediaries in blockchain applications. The method also accords freedom to users to form various types of contracts without any limits. Thus, due to the influence of decentralization in blockchains, there are several issues regarding the abuse of this technology involving buying and selling transactions.

There are case studies that reflect errors in the autonomy concept applied in Islamic contracts. In *United States v. Ross Ulbritch*, the issue involved the abuse of sales contracts in the blockchain. The background of the case has been discussed in Chapter II. An analysis found that the use of blockchain technology in commercial transactions concerning the Silk Road was solely meant to mislead the authorities. Second, Ulbritch choose this technology to

[26] Paech, P., Law and Autonomous Systems Series: What Is a Smart Contract? 2018, https://www.law.ox.ac.uk/business-law-blog/blog/2018/07/law-and- autonomous-systems-series-what-smart-contract

enable the contracting parties to possess the element of autonomy. Therefore, the autonomy concept in a blockchain does not comply with Islamic contract principles because this concept applied in a contract leads to the element of *gharar* among the contracting parties.

Gharar, in this situation, refers to the aim of autonomy, which is to conceal information regarding the contracting parties in a smart contract transaction. The information regarding the contracting parties is concealed by replacing it with a computer code as a pseudonym. Second, the autonomy concept also allows the contracting parties to disregard Islamic contract principles or criteria. Although the criteria depend on the willingness and wish of the contracting parties, however, the concept poses difficulties and problems to other contracting parties. Third, the autonomy concept also allows commercial (buying and selling) transactions involving subjects that do not comply with Islamic principles. An analysis of Ulbritch's case study also found that Ulbritch's purpose in choosing the blockchain was to conceal the black-market activities, including illegal weapons, drugs etc[27]. The subject matter allowed in the transaction violates law enforcement and does not comply with Islamic contract principles. Commercial (buying and selling) transactions involving drugs is not allowed in Islam because drug abuse leads to numerous other deleterious social ills. The religious precedent on drug abuse has been subjected to *qiyas* (deductive analogy) by comparing drug abuse to the prohibition of alcohol consumption by Muslims, as mentioned in the al-Quran (QS. Al-Maidah verse 90). In addition, the law on the prohibition of drug abuse is also mentioned in the Islamic Religious Administration Enactment (State of Selangor) 2013, as follows:

1) Syabu and other new types of drugs that have the same harmful effects as ecstasy, ketamine dan Gamma Hydroxybutyric Acid (GHB).[28]
2) Therefore, the abuse of syabu and other new drugs is illegal and all activities related to the abuse of these drugs, such as growing, processing, possessing, selling, distributing, buying or allowing the premises to be used to abet their use, are also prohibited.[29]

Drug abuse is banned because it is harmful and deleterious to the health and lives of the community. In fact, drug abuse also causes losses in various forms and the uncontrolled desire of addicts to satisfy their cravings usually lead to

[27] Burgess, Matt. “Silk Road creator Ross Ulbricht loses appeal against life sentence”. *Business*. 2017. https://www.wired.co.uk/article/silk-road-ross-ulbricht-life-sentence.

[28] Islamic Religious Administration Enactment (State of Selangor). Section 47 (1). 60 no. 1. (2013)

[29] Islamic Religious Administration Enactment (State of Selangor), Section 47 (2). Vol. 60. No. 1 (2013).

crimes, such as stealing, mugging, robbery and even murder.[30] Therefore, it is an error to involve a subject matter in a smart contract that transgresses Islamic contract principles. The types of subject matter allowed are not filtered and therefore, could be disallowed in an Islamic contract that involves a smart contract. Table 5 depicts respondents' views on the subject allowed in a smart contract.

Table 5: Type of subject matter allowed in a smart contract

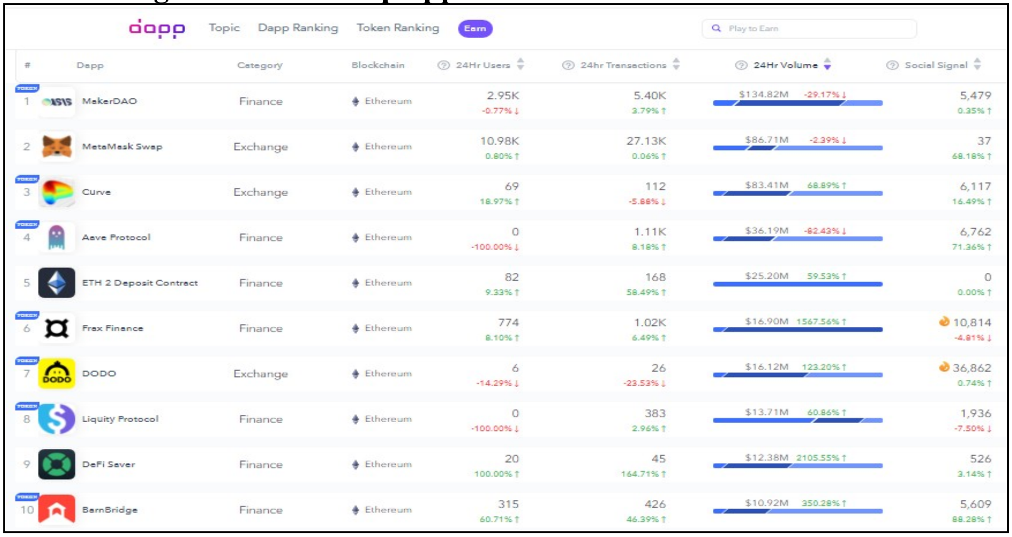
Question 4	**What types of subject matter are allowed in a smart contract transaction?**	**Code/Theme**
Respondent A	Can surf the dapp.com. website. There are various types of transactions there. The most popular applications are investment, games, gambling etc.	Type of subject in an *aqad* found in a smart contract
Respondent B	Various types of goods are permitted and there are no conditions stipulated but rather based on the wishes of the contracting parties	
Respondent C	All types of subjects are permitted in a smart contract	
Respondent D	No conditions are stipulated. One is free to conduct transactions without any impediments	
Respondent E	Any subject is permitted based on the agreement between the contracting parties	

Results of the interview (2019)

Data analysis based on Table 5 supports the type of subject matter implemented in Ulbritch's case study. Subjects of a contract in independent smart contracts are carried out without any monitoring by the authorities due to the decentralization concept. However, the contracting parties need to agree upon the subject of the contract. Thus, if one of the contracting parties do not agree on the subject of the contract, then the contracting party has the right to cancel the contract. In fact, smart contract transactions also provide a variety of applications in the form of gambling, currency exchange, finance and games that have not yet been verified as being Shariah compliant. Here is a list of famous applications implemented in the Ethereum smart contract.

[30] Kementerian Hal Ehwal Ugama Brunei Darussalam. 2016. Penyalahgunaan Dadah. http://kheu.gov.bn/lists/khutbah/newdisplayitem.aspx?id=447&contenttypeid=0x0100ee34442fd552cc4faece608c6a2c143b

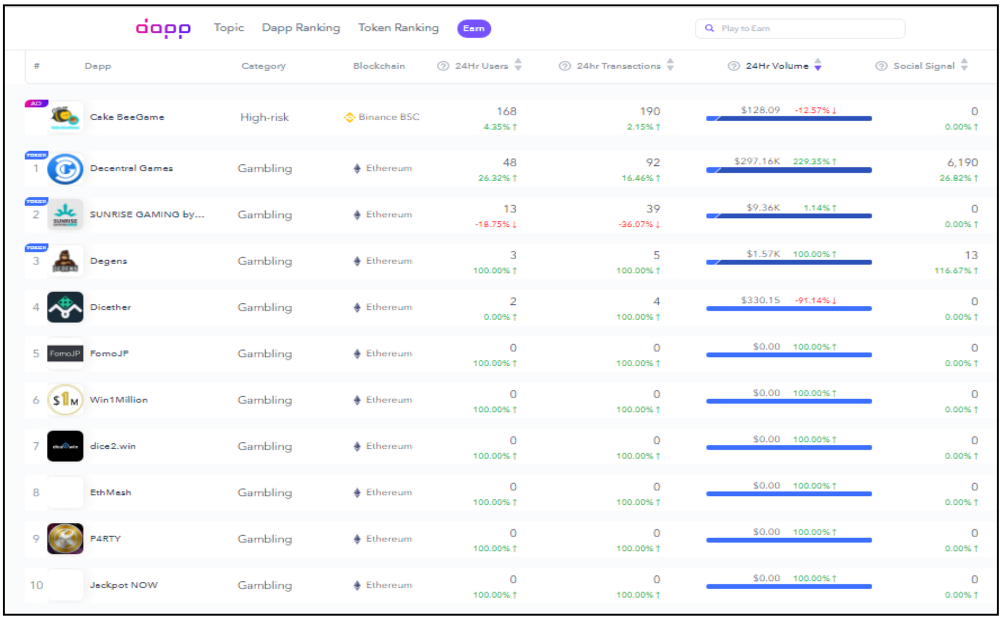
Figure 6: List of top applications in the *Ethereum* network



#	Dapp	Category	Blockchain	24Hr Users	24hr Transactions	24Hr Volume	Social Signal
1	MakerDAO	Finance	Ethereum	2.95K -0.77% ↓	5.40K 3.79% ↑	$134.82M -29.17% ↓	5,479 0.35% ↑
2	MetaMask Swap	Exchange	Ethereum	10.98K 0.80% ↑	27.13K 0.06% ↑	$86.71M -2.39% ↓	37 68.18% ↑
3	Curve	Exchange	Ethereum	69 18.97% ↑	112 -5.88% ↓	$83.41M 68.89% ↑	6,117 16.49% ↑
4	Aave Protocol	Finance	Ethereum	0 -100.00% ↓	1.11K 8.18% ↑	$36.19M -82.43% ↓	6,762 71.36% ↑
5	ETH 2 Deposit Contract	Finance	Ethereum	82 9.33% ↑	168 58.49% ↑	$25.20M 59.53% ↑	0 0.00% ↑
6	Frax Finance	Finance	Ethereum	774 8.10% ↑	1.02K 6.49% ↑	$16.90M 1567.56% ↑	10,814 -4.81% ↓
7	DODO	Exchange	Ethereum	6 -14.29% ↓	26 -23.53% ↓	$16.12M 123.20% ↑	36,862 0.74% ↑
8	Liquity Protocol	Finance	Ethereum	0 -100.00% ↓	383 2.96% ↑	$13.71M 60.86% ↑	1,936 -7.50% ↓
9	DeFi Saver	Finance	Ethereum	20 100.00% ↑	45 164.71% ↑	$12.38M 2105.55% ↑	526 3.14% ↑
10	BarnBridge	Finance	Ethereum	315 60.71% ↑	426 46.39% ↑	$10.92M 350.28% ↑	5,609 88.28% ↑

Data Source: dapp.com

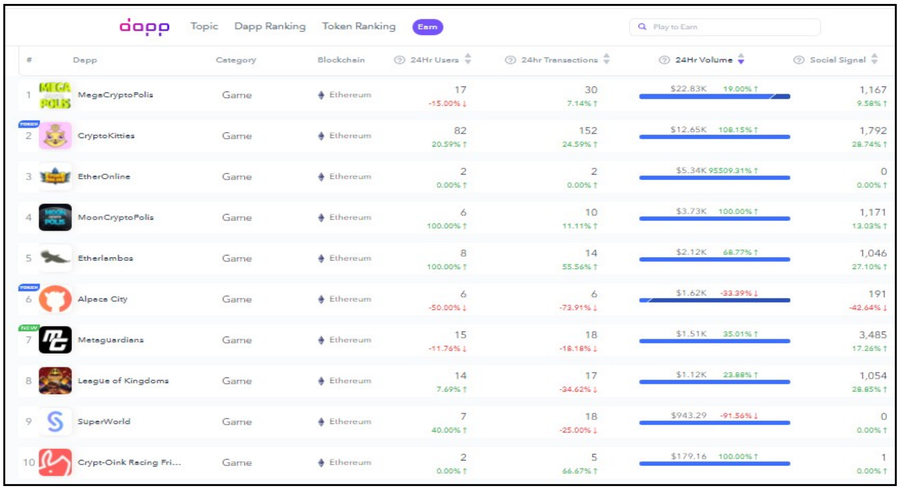
Figure 7: List of gambling applications in the *Ethereum* network Data



#	Dapp	Category	Blockchain	24Hr Users	24hr Transactions	24Hr Volume	Social Signal
AD	Cake BeeGame	High-risk	Binance BSC	168 4.35% ↑	190 2.15% ↑	$128.09 -12.57% ↓	0 0.00% ↑
1	Decentral Games	Gambling	Ethereum	48 26.32% ↑	92 16.46% ↑	$297.16K 229.35% ↑	6,190 26.82% ↑
2	SUNRISE GAMING by...	Gambling	Ethereum	13 -18.75% ↓	39 -36.07% ↓	$9.36K 1.14% ↑	0 0.00% ↑
3	Degens	Gambling	Ethereum	3 100.00% ↑	5 100.00% ↑	$1.57K 100.00% ↑	13 116.67% ↑
4	Dicether	Gambling	Ethereum	2 0.00% ↑	4 100.00% ↑	$330.15 -91.14% ↓	0 0.00% ↑
5	FomoJP	Gambling	Ethereum	0 100.00% ↑	0 100.00% ↑	$0.00 100.00% ↑	0 0.00% ↑
6	Win1Million	Gambling	Ethereum	0 100.00% ↑	0 100.00% ↑	$0.00 100.00% ↑	0 0.00% ↑
7	dice2.win	Gambling	Ethereum	0 100.00% ↑	0 100.00% ↑	$0.00 100.00% ↑	0 0.00% ↑
8	EthMash	Gambling	Ethereum	0 100.00% ↑	0 100.00% ↑	$0.00 100.00% ↑	0 0.00% ↑
9	P4RTY	Gambling	Ethereum	0 100.00% ↑	0 100.00% ↑	$0.00 100.00% ↑	0 0.00% ↑
10	Jackpot NOW	Gambling	Ethereum	0 100.00% ↑	0 100.00% ↑	$0.00 100.00% ↑	0 0.00% ↑

Source: dapp.com

Figure 8: List of gaming applications in the *Ethereum* network Data



dapp Topic Dapp Ranking Token Ranking Earn Play to Earn

#	Dapp	Category	Blockchain	24Hr Users	24hr Transactions	24Hr Volume	Social Signal
1	MegaCryptoPolis	Game	Ethereum	17 -15.00% ↓	30 7.14% ↑	$22.83K 19.00% ↑	1,167 9.58% ↑
TOKEN 2	CryptoKitties	Game	Ethereum	82 20.59% ↑	152 24.59% ↑	$12.65K 108.15% ↑	1,792 28.74% ↑
3	EtherOnline	Game	Ethereum	2 0.00% ↑	2 0.00% ↑	$5.34K 95509.31% ↑	0 0.00% ↑
4	MoonCryptoPolis	Game	Ethereum	6 100.00% ↑	10 11.11% ↑	$3.73K 100.00% ↑	1,171 13.03% ↑
5	Etherlambos	Game	Ethereum	8 100.00% ↑	14 55.56% ↑	$2.12K 68.77% ↑	1,046 27.10% ↑
TOKEN 6	Alpaca City	Game	Ethereum	6 -50.00% ↓	6 -73.91% ↓	$1.62K -33.39% ↓	191 -42.64% ↓
NEW 7	Metaguardians	Game	Ethereum	15 -11.76% ↓	18 -18.18% ↓	$1.51K 35.01% ↑	3,485 17.26% ↑
8	League of Kingdoms	Game	Ethereum	14 7.69% ↑	17 -34.62% ↓	$1.12K 23.88% ↑	1,054 28.85% ↑
9	SuperWorld	Game	Ethereum	7 40.00% ↑	18 -25.00% ↓	$943.29 -91.56% ↓	0 0.00% ↑
10	Crypt-Oink Racing Fri...	Game	Ethereum	2 0.00% ↑	5 66.67% ↑	$179.16 100.00% ↑	1 0.00% ↑

Source: dapp.com

Figures 6, 7, and 8 depict the list of applications provided by the Ethereum network based on the official dApps website. The list of applications includes financial activities, currency exchange, gambling, gaming etc. The 'Maker DAO' application is the top application that involves currency exchange activities. A total of 1.65 million users, 11.4 million transactions and 224,033 smart contracts were executed in the application. The application is a financial institution that provides exchange services, financial loans, and storage of crypto tokens or cryptocurrencies. It was established to create a financial institution based on decentralized finance or better known as DeFi. The use of cryptocurrency in Malaysia based on the Shariah compliance framework has been widely debated by various Islamic finance experts.

The use of cryptocurrency is a confirmed legal tender but not a legal currency for the exchange of goods and services. Cryptocurrency is not suitable for use as a general instrument for payment because it does not show the universal characteristics of money and it has limitations, including uncontrolled price fluctuations and vulnerability to cyber threats.[31] Therefore, the cryptocurrency's instability makes it difficult for the technology to position itself in the FinTech industry. The implementation of cryptocurrencies is still at a precautionary stage and requires a concise decision by the authorities about its position in the FinTech industry.

Figure 8 shows the implementation of non-Shariah compliant applications in smart contracts. The 'Decentral games' application is a game

[31] Malaysian Securities Commission, 2020. Kenyataan Bersama BNM Dan SC Berkenaan "Kekeliruan Dasar Terhadap Mata Wang Kripto".

application based on the concept of gambling. The game is implemented using crypto mining, which is mainly the placing of bets and earning profits using Ethereum smart contracts. Before joining this application, users need to have a 'MetaMask crypto wallet' to earn crypto money as a betting medium. 'MetaMask Swap' is the top application in Ethereum cryptocurrency exchange activity. A total of 6.3 million transactions and 832,606 users are on 'MetaMask'.

Findings on the position of subjects in smart contracts show that subjects that do not comply with the pillars of Islamic contracts are allowed. Control over the subject's position in a smart contract depends on the decisions of the contracting parties. Nevertheless, smart contract transactions involve matters that violate the criteria of an Islamic contract, which invalidates the contract because of non-Shariah compliance even though the contract is allowed in the blockchain. This is because the decentralization concept in smart contracts has been manipulated in the transaction by allowing subjects that violate the law as well as being non-Shariah compliant to be implemented in a covert manner. In other words, the decentralization concept restricts the power of the authority to monitor and control the movement of smart contract transactions. The restrictions have facilitated the contracting parties to manipulate the contract without being subject to any enforcement and thus, move uncontrollably.

An Analysis of a Smart Contract based on the Islamic Contract Theory

Contracts have been practiced in various industries including the *muamalat* (commercial) sector since the early days of Islamic development until now. From a Shariah perspective, the execution of contracts is practiced mainly by the Muslim community in order to protect their rights based on Maqasid Syariah.[32] Therefore, a smart contract is an innovation to existing contracts, especially in the business and financial industries. This study aimed to analyse the relationship between a smart contract and Islamic contract as well as determine whether smart contract transactions are Shariah-compliant or otherwise. Table 6 depicts the data analysis related to the relationship between smart contracts and Islamic contracts.

[32] Ayup Suran Ningsih and Hari Sutra Disemadi, "Breach of Contract: An Indonesian experience in credit akad of Sharia Banking," *Ijtihad*: *Jurnal Wacana Hukum Islam dan Kemanusiaan* 19, No. 1 (2019), p. 89-102.

Table 6: Smart Contract and Islamic Contract

Category	**Smart Contract**	**Islamic Contract**	**Discussion**
Contracting parties	▪ Autonomy ▪ There are no criteria for the involvement of contracting parties ▪ Contracting parties' identities are not mentioned in the contract but location of the transaction is given using the *public address*	▪ Know Your Customer (KYC) concept ▪ There are certain criteria pertaining to the involvement of contracting parties from a Shariah perspective	▪ A smart contract allows the involvement of contracting parties, which is not allowed in an Islamic contract ▪ The autonomy concept in a smart contract leans towards the element of *gharar* compared to the affirmed qualification criteria for contracting parties in an Islamic contract
Pronunciation (*Lafaz*)	▪ Handing over transaction is implemented in the form of writing using computer codes. A *Private key* is used by contracting parties to confirm a transaction	▪ Pronunciation of the *aqad* (contract) involves the *ijab qabul*	▪ Pronunciation of the *ijab qabul* in a smart contract is in a written form (computer code) ▪ There is an element of *khiyār* in a smart contract where contracting parties have the right to make choices
Subject of the *aqad* (contract)	▪ No objections to the type of subject matter in the *aqad* (contract) of a smart contract	▪ The subject in an *aqad* (contract) has benefits and does not transgress any condition stipulated in the Syarak	▪ A smart contract involves subject matter that are not allowed in an Islamic contract
	▪ Example of a subject implemented in a smart contract: ▪ PoWH3D –Ponzi scheme transaction ▪ Fomo3D – Gambling-type of game transaction ▪ Silk road – Black market transaction, including	▪ Examples of subjects not permitted by Syarak are alcohol, pork meat, usury, *gharar* etc.	▪ The element of manipulation exist in a smart contract and it obscures transactions that involve prohibited subjects, mainly the issue of Shariah compliance based on the decentralisation concept

the smuggling of firearms, drugs and false identification cards.
Decentralized Games: *mining games* based on gambling

Table 6 depicts the relationship between smart contracts and Islamic contracts from a Shariah compliance perspective. The relationship between the two contracts involves the three pillars of an Islamic contract that are based on Shariah compliance. Based on a study that compared smart contracts and Islamic contracts, it was found that the implementation of smart contracts violates the conditions set by the three pillars of an Islamic contract. There are differences in smart contracts in comparison to Islamic contracts, namely concerning the contracting parties and the subject matter of the contract.

Violation of Islamic contract principles in smart contracts involves violations of Shariah law. First, the data analysis shows non-uniformity of Islamic contract principles regarding the involvement of contracting parties in smart contracts. The study found that the main concept in smart contracts is to create autonomy or anonymity between contracting parties. The purpose of the concept is to hide the contracting parties' personal information by using pseudonyms in the form of computer codes. This purpose violates the legal criteria of an Islamic contract because concealing information pertaining to the contracting parties falls under the element of *gharar*. An Islamic contract should adhere to several criteria that might act as an obstacle for those who are wanting to execute a contract. Islamic contracts emphasize the concept of 'Know Your Customer' (KYC). This concept is a standard applied in various industries to verify detailed customer information regarding their risk and financial profiles.[33]Bank Negara Malaysia has issued a draft proposal for implementation guidelines for e-KYC or electronic entry involving individuals in the financial sector.

The proposal allows safe and secure use of e-KYC technology, exercise of effective supervisory oversight and ensure effective Anti-Money Laundering and Anti-Terrorism Financing control measures.[34] E-KYC is a standard applied in financial systems in Malaysia, including e-Wallet, Grab Pay, Touch and Go, Shopee Pay and so on. The e-KYC standard is strengthened by incorporating

[33] Chen, J. 2022. Know Your Client (KYC). https://www.investopedia.com/terms/k/know yourclient.asp [July 31, 2022].

[34] Bank Negara Malaysia, Electronic Know-Your-Customer (e-KYC) (Exposure Draft), Kuala Lumpur: Bank Negara Malaysia, December 16, 2019. Part A (bnm.gov.my).

artificial intelligence into the system to detect faces and optics to verify the user's existence.[35]

In reference to the involvement of contracting parties in smart contracts, this platform adopts the autonomy concept, which aims to conceal the existence or identity of contracting parties. At the same time, this concept allows transactions to be executed in a centralized manner, while the exchange of subjects in the contract are kept confidential. This concept has become a challenge, especially when preventing money laundering as well as monitoring the parties involved on this platform. In fact, the exchange of transactions in smart contracts only uses certain cryptocurrencies that are exposed to volatile prices. Moreover, the use of cryptocurrencies is vulnerable to cyber threats and is still not recognized in Malaysia when used in transactions.[36]

In addition, smart contracts do not set conditions for the participation of contracting parties and anyone is free to execute the contract. While the legal condition for qualification is a sense of obligation and the contract becomes invalid if there are violations and doubts in the qualification.[37] With the existence of the autonomy concept, there are no restrictions on unqualified individuals as a legal criterion in an Islamic contract. Hence, users who fail to qualify based on legal criteria of an Islamic contract are free to engage in smart contract transactions. The transaction cannot be monitored by the authorities because of the decentralized concept enforced in the technology. The autonomy concept is also risky and harmful to other contracting parties. Thus, if there is an issue with the Islamic contract, it is difficult for the contracting parties to detect the other contracting party due to the autonomy concept and also the use virtual technology. This is because the contracting parties involved in the transaction are not registered or affirmed by the authorities that the contracting parties do exist and are eligible based on Islamic principles. There is *gharar* in relation to the existence of the contracting parties and the qualification of the contracting parties based on the legal criteria of an Islamic contract. The autonomy concept in a smart contract has a negative impact on the contracting parties based on Ulbritch's case study. Therefore, the contracting parties in a smart contract are not Shariah compliant because it involves the element of *gharar* due to the existence of the autonomy concept.

[35] Wee, R., Ho, W., & Ling, J. Y. 2021. e-KYC in Malaysia. https://www.richardweechambers.com/e-kyc-in-malaysia/ [July 1, 2021].

[36] Musa, Y. H. 2021. [PARLIMEN] Mata wang kripto tidak diiktiraf di Malaysia. https://www.utusan.com.my/terkini/2021/12/parlimen-mata-wang-kripto-tidak-diiktiraf-di-malaysia/

[37] Ruzian Markom, et.al., "Pelaksanaan Kontrak Muamalat Oleh Golongan Orang Kelainan Upaya (OKU) Buta Dalam Sistem Kewangan Islam," *Journal of Contemporary Islamic Law* 5, No. 2 (2020), p. 29-41.

Smart contracts do not comply with the legal requirements of an Islamic contract because they allow the transaction of the subject matter in an *aqad* (contract), which is not allowed by Shariah. One example of a subject matter of a contract that is not allowed in Islam is a Ponzi scheme. A Ponzi scheme is a plan that usually offers a high rate of return without relying on any business activity; instead, it manipulates the money invested by participants as a return on the investment (Bank Negara Malaysia).[38] Profits are paid from money invested by new investors. Ponzi schemes originated from Charles Ponzi, who conducted a scheme to deceive investors by promising high returns by using new investors' money to pay previous investors.[39] This type of investment does not involve the subject matter of a contract but instead uses new investors' money as profit payments. This type of a Ponzi scheme investment is tyrannical, fraudulent and oppressive to the investors involved.[40] The characteristics of this scheme have been prohibited by Allah s.w.t.[41] The verse affirms the prohibition of using other people's property based on methods prohibited by Islam. Profits are obtained from other investors without involving the contract’s subject matter. This activity makes investors feel that they do not need to work because they can earn money easily without exerting any effort. In addition, a Ponzi scheme is considered an illegal activity based on the Banks and Financial Institutions Act (ABIK), 1989.

Act 372 states that deposits can only be collected by any institution authorized under the law, which includes financial and banking companies. The implementation of a Ponzi scheme using smart contracts is an investment innovation using cryptocurrency. The Ponzi scheme concept still uses the same concept as the Classic Ponzi scheme. This technology is used to attract new investors for the development of blockchain technology relevant to the financial industry.[42] *Forsage* is one of the applications that provides Ponzi scheme investment. *Forsage* promises passive income to investors using the Ponzi scheme concept. Although *Forsage* is a high-risk investment application, it

[38] Bank Negara Malaysia (BNM). 2007. Common questions regarding the Get Rich Quick schemes. http://www.bnm.gov.my/index.php?ch=104&pg=457&ac=551&lang=bm.

[39] Eley Suzana Kasim, Norlaila Md Zin, Hazlina Mohd Padil and Normah Omar, Ponzi Schemes and its Prevention: Insights from Malaysia. In *Management & Accounting Review*, (2020), p 89-118.

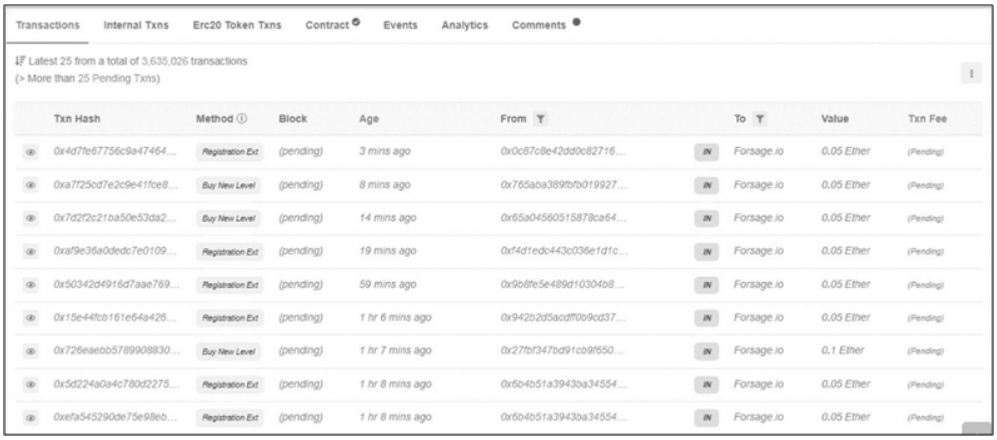
[40] National Muzakarah Fatwa Council, 2005. Hukum Skim Cepat Kaya Dan Seumpamanya. Himpunan Keputusan Muzakarah Jawatankuasa Fatwa Kebangsaan, Berhubungan Dengan Isu-Isu Muamalat, pp. 71-75

[41] Al-Quran, an-Nisa’ 4: 29.

[42] Sokolin, L. 2020. Weed Out the Soviet-Era Ponzi Scheme Eating Ethereum. https://www.coindesk.com/business/2020/07/07/weed-out-the-soviet-era-ponzi-scheme-eating Ethereum/ [3 September 2020].

managed to earn 2.8 million ether.[43] Figure 9 depicts a sample of a smart contract transaction that is still implemented in *Forsage*.

Diagram 9: A sample of a smart contract transaction in the *Forsage* application



Latest 25 from a total of 3,635,026 transactions
(> More than 25 Pending Txns)

	Txn Hash	Method	Block	Age	From		To	Value	Txn Fee
	0x4d7fe67756c9a47464...	Registration Ext	(pending)	3 mins ago	0x0c87c8e42dd0c82716...	IN	Forsage.io	0.05 Ether	(Pending)
	0xa7f25cd7e2c9e41fce8...	Buy New Level	(pending)	8 mins ago	0x765aba389fbfb019927...	IN	Forsage.io	0.05 Ether	(Pending)
	0x7d2f2c21ba50e53da2...	Buy New Level	(pending)	14 mins ago	0x65a04560515878ca64...	IN	Forsage.io	0.05 Ether	(Pending)
	0xaf9e36a0dedc7e0109...	Registration Ext	(pending)	19 mins ago	0xf4d1edc443c036e1d1c...	IN	Forsage.io	0.05 Ether	(Pending)
	0x50342d4916d7aae769...	Registration Ext	(pending)	59 mins ago	0x9b8fe5e489d10304b8...	IN	Forsage.io	0.05 Ether	(Pending)
	0x15e44fcb161e64a426...	Registration Ext	(pending)	1 hr 6 mins ago	0x942b2d5acdff0b9cd37...	IN	Forsage.io	0.05 Ether	(Pending)
	0x726eaebb5789908830...	Buy New Level	(pending)	1 hr 7 mins ago	0x27fbf347bd91cb9f650...	IN	Forsage.io	0.1 Ether	(Pending)
	0x5d224a0a4c780d2275...	Registration Ext	(pending)	1 hr 8 mins ago	0x6b4b51a3943ba34554...	IN	Forsage.io	0.05 Ether	(Pending)
	0xefa545290de75e98eb...	Registration Ext	(pending)	1 hr 8 mins ago	0x6b4b51a3943ba34554...	IN	Forsage.io	0.05 Ether	(Pending)

Source: Etherscan.io (2021)

A sample of a smart contract transaction used in the *Forsage* application was obtained from the public address: 0x5acc84a3e955Bdd76467d3348077d003f00fFB97. The study sample showed that the *Forsage* application was still active in the smart contract as of July 9, 2021. A total of 3,635,026 transactions were carried out in the application and a total of 39840.590458367298119451 ether equivalent to USD 156,710,970.54 was obtained as a charge for fees due.

Although this application can be freely applied in a smart contract, however, the implementation violates Islamic contract principles and contains elements that are prohibited by Shariah. Therefore, Muslims are strongly prohibited from participating in this type of transaction because there is a high risk for suffering losses. In addition, findings indicate that there is an element of usury and gambling in this type of transaction because the investor has to pay the member's fee at the initial stage and obtain a greater return using the new investor's money. The return earned from investors is also called a windfall profit. In fact, most Ponzi scheme investors have to bear the burden of high debt due to claims from new investors.[44]

[43] Redman, J. 2020. Despite Warnings from Regulators, The Ethereum Fueled Pyramid Scheme Forsage Thrives. https://news.bitcoin.com/despite-warnings-from-regulators-the-ethereum-fueled-pyramid-scheme-forsage-thrives/

[44] Haeme Hashim, Undang-Undang MLM. (2019). https://www.sinarharian.com.my/article/63149/KOLUMNIS/Undang-Undang- MLM [December 30, 2019].

This study found that the contracting parties and the subject of the *aqad* in a smart contract had violated Islamic contract principles. However, the wording used in the contract complies with the implementation of *ijab qabul* based on Islamic contract principles. *Ijab qabul* is pronounced clearly in the contract using the *solidity* language. The *ijab qabul* structure used in the contract is an online writing structure. A written contract is permanent and can be used as a reference by contracting parties. The *ijab qabul* is then confirmed by the contracting parties using a private key. This method provides space to contracting parties to make choices when executing *Ethereum* smart contract transactions. Hence, if the contracting parties do not agree to use a smart contract, then either contracting party has the right to cancel the contract.

Data analysis regarding the relationship between an Ethereum smart contract and an Islamic contract found non-Shariah-compliant elements involving the contracting parties and the subject of the contract. Although a smart contract is presumed to be an innovation in financial technology, users have other options when executing online contracts. Moreover, this type of transaction is highly risky and is capable of causing financial losses and transgressions to Islamic principles. This transaction adopts a decentralized concept, which makes it difficult for authorities to better control of the transaction. The decentralization concept also affords freedom to users to carry out various types of transactions, including non-Shariah compliant transactions without any hindrance.

Conclusion

This study strongly suggests that there are non-Shariah compliant elements in smart contracts. Two of the pillars of an Islamic contract used in smart contracts do not comply with Shariah principles, namely the contracting parties and the subject of the contract. Contracting parties possess the element of autonomy, which involves the element of *gharar*, found in the criteria that determines the eligibility of the contracting parties. *Gharar* is also involved in the use of cryptocurrency as a medium of exchange in smart contracts. Meanwhile, the subject of the contract in a smart contract involves the act of manipulation, which causes the contract to create non-Shariah compliant subjects, such as usury, *gharar* drugs, illegal firearms trade and so on. The involvement of such subjects in smart contracts creates risks that are difficult for users to control and thus, oppresses the contracting parties. Although a smart contract is said to be an innovation of the classic contract, however, it does not meet the criteria of an Islamic contract. Lastly, the study also found that smart contracts should be avoided for now until enforcement by Islamic financial authorities ensures that these contracts are guaranteed to be safe for use in accordance with Shariah principles.

References

Journals and Books

Al-Quran al-Karim.

Adebumiti, Qazeem Adedamola and Abdullahi Saliu Ishola, "Beyond Riba, Maysir and Gharar Transactions: The No-Go Areas for Islamic Finance Industry," International Seminar on Islamic Jurisprudence in Contemporary Society at Universiti Sultan Zainal Abidin, Terrengganu, Malaysia (2017).

Ahmad, Azlin Alisa and Mat Noor Mat Zain, "A Comparative Analysis of Smart Contracts and Islamic Contracts," *International Journal of Advanced Research* 8, No. 10 (2020). DOI:10.21474/IJAR01/11859.

Bank Negara Malaysia, *Perbankan Islam,* Kuala Lumpur: Percetakan Asas Jaya (M) Sdn. Bhd. 2016.

Bartoletti, Massimo and Livio Pompianu, "An Emperial Analysis of Smart Contracts: Platforms, Applications, and Design Patterns," *Frontiers In Blockchain* 3, No. 27 (2020).

Buterin, Vitalik, "A Next-Generation Smart Contract And Decentralized Application Platform." *White Paper* 3, no. 37 (2014).

Hamid, Abdulloh, "Bitcoin As A Means of Transaction and Investment in The Perspective of Islam," *Iqtishoduna: Jurnal Ekonomi Islam* 10, No. 2 (2021). DOI:10.36835/iqtishoduna.v10i2.944

Islamic Financial Services Board, *Islamic Financial Services Industry Stability Report*. Kuala Lumpur: IFSB, 2017.

Lacasse, Ricard Marc., et.al., "Islamic Banking - Towards a Blockchain Monitoring Process," *Journal of Business and Economics* 6 no 1 (2017).

Larfi, Aicha, "Bitcoin Between The Economy and Islamic Law," *International Conference on Islamic Economic* 1, No. 1 (2022). DOI:10.58223/icie.v1i1.106.

Lateh, Najahudin BIN and Siti Noorbiah Md Rejab, "Sharia Issues About Bitcoin Cryptocurrency Transactions, in *Enhancing Halal Sustainability* (2021). DOI:10.1007/978-981-33-4854-7_11.

Lier, Ben van, "Can Cyber-Physical Systems Reliably Collaborate within a Blockchain? Blockchain and Cyber-Physical Systems," *Metaphilosophy* 48, No. 5 (2017). DOI: 10.1111/meta.12275.

Markom, Ruzian, et.al., Pelaksanaan Kontrak Muamalat Oleh Golongan Orang Kelainan Upaya (OKU) Buta Dalam Sistem Kewangan Islam." *Journal of Contemporary Islamic Law* 5 no. 2 (2020).

Moh Zain, Nor Razinah and Khairul Azmi Mohamad, "An Evaluation of Smart Contracts: Practices, Legality, and Sharīʻah," In *Islamic FinTech* (2021). DOI:10.1007/978-3-030-45827-0_6

Muzakarah Jawatankuasa Fatwa Kebangsaan, Hukum Skim Cepat Kaya Dan

Seumpamanya. Himpunan Keputusan Muzakarah Jawatankuasa Fatwa Kebangsaan, Berhubungan Dengan Isu-Isu Muamalat, 2005.

Ningsih, Ayup Suran and Hari Sutra Disemadi, "Breach of Contract: An Indonesian experience in credit akad of Sharia Banking," *Ijtihad*: *Jurnal Wacana Hukum Islam dan Kemanusiaan* 19, No. 1 (2019). Doi: 10.18326/ijtihad.v19i1.89-102

Polas, Mohammad Rashed Hasan, et.al., "Is Bitcoin Halal or Haram in the Islamic Banking and Finance? An Overview," *Journal of Economics, Business and Market Research* 1, No. 2 (2020).

Politou, E., Casino, F., Alepis, E., & Patsakis, C., Blockchain Mutability: Challenges and Proposed Solutions, *IEEE Transactions on Emerging Topics in Computing*, (2019). https://www.researchgate.net/publication/336822518.

Shahab, Mohammad Hamed, et.al., "Cryptocurrencies: A Critical Analysis from the Perspective of Islamic Law, " *Change Management* 22, No. 2 (2022).

Internet Data

Abdul Muhaimin Mahmood, Konsep Akad Dan Jenisnya Dalam Muamalat Islam. E-Muamalat Jabatan Kemajuan Islam Malaysia, 2020. https://e-muamalat.islam.gov.my/en/bahan-ilmiah/artikel/156-konsep-akad-dan-jenisnya-dalam-muamalat-islam

Abraham, I. 2020. The First Blockchain or How to Time-Stamp a Digital Document. *Decentralized Thoughts*. https://decentralizedthoughts.github.io/2020-07-05-the-first-blockchain-or-how-to-time-stamp-a-digital-document/

Abdul Muhaimin Mahmood, Konsep Akad Dan Jenisnya Dalam Muamalat Islam, Jabatan Kemajuan Islam Malaysia, 2020, https://e-muamalat.islam.gov.my/en/bahan-ilmiah/artikel/156-konsep-akad-dan-jenisnya-dalam-muamalat-islam.

Burgess, Matt. "Silk Road creator Ross Ulbricht loses appeal against life sentence". Business. 2017. https://www.wired.co.uk/article/silk-road-ross-ulbricht-life-sentence.

Buterin, Vitalik., "What Are Smart Contracts & What Is Their Function?" 2017. https://www. youtube.com/watch?v=r0s4qimf4pg [June 5, 2018].

Chen, J. 2022. *Know Your Client (KYC)*. https://www.investopedia.com/terms/k/know yourclient.asp (July 31, 2022).

Greenberg, A. In Silk Road Appeal, Ross Ulbritch's Defense Focuses On Corrupt Feds, 2016. https://www.wired.com/2016/01/ross-ulbrichts-defense-focuses-on- corrupt-feds-in-silk-road-appeal/ [15 Julai 2019].

Haeme Hashim, Undang-Undang MLM, 2019,

https://www.sinarharian.com.my/ article/63149/KOLUMNIS/Undang-Undang- MLM (December 30, 2019).

Humiston, P., Smart Contract Attacks [Part 2] – Ponzi Games Gone Wrong. 2018, https://medium.com/hackernoon/smart-contract-attacks-part-2-ponzi-games- gone-wrong-d5a8b1a98dd8 (July 6, 2019).

Kementerian Hal Ehwal Ugama Brunei Darussalam. 2016. Penyalahgunaan Dadah. http://kheu.gov.bn/lists/khutbah/newdisplayitem.aspx?id=447&contentt ypei d=0x0100ee34442fd552cc4faece608c6a2c143b (September 1, 20210.

Muhammad Hafis Nawawi, M., & Mohamed, S. 2011. Janji Untung 1000 Ganda. Kuala Lumpur: Harian Metro.

Musa, Y. H., *[PARLIMEN] Mata wang kripto tidak diiktiraf di Malaysia*, 2021, https://www.utusan.com.my/terkini/2021/12/parlimen-mata-wang-kripto-tidak-diiktiraf-di-malaysia/ (December 31, 2021).

Norry, A., The History of Mt. Gox Hack: Bitcoin’s Biggest Heist, 2020. https:// blockonomi.com/mt-gox-hack/ (April 1, 2020).

Oettler, M., Anonymity vs Pseudonymity. Blockchain Acdemy Mittweida, 2021, https://blockchain-academy.hs-mittweida.

Paech, P., Law And Autonomous Systems Series: What Is A Smart Contract?, 2018, https://www.law.ox.ac.uk/business-law-blog/blog/2018/07/law-and- autonomous-systems-series-what-smart-contract [September 12, 2018].

Redman, J., Despite Warnings From Regulators, The Ethereum Fueled Pyramid Scheme Forsage Thrives, 2021, https://news.bitcoin.com/despite-warnings-from-regulators-the-ethereum-fueled-pyramid-scheme-forsage-thrives/ (December 15, 2020).

Srivastava, A., n.d. Understanding Blockchain for Beginners. https://levelup.gitconnected.com/understanding-blockchain-for-beginners-f0aaab7ffcf7

Scott, J. 2019. Smart Contract Transparency Decentralized The World. https://medium.com/@jeffwscott/smart-contract-transparency-in-the-decentralized-world-309abfe8f14a (April 12, 20200.

Siegel, D. 2016. Understanding The DAO Attack. https://www.coindesk.com /understanding-dao-hack-journalists (Mach 1, 2018).

Sokolin, L. 2020. Weed Out The Soviet-Era Ponzi Scheme Eating Ethereum. https://www.coindesk.com/business/2020/07/07/weed-out-the-soviet-era- ponzi-scheme-eating-ethereum/ (3 September 2020).

Suruhanjaya Sekuriti Malaysia, Kenyataan Bersama BNM Dan SC Berkenaan "Kekeliruan Dasar Terhadap Mata Wang Kripto", 2021.

Wee, R., Ho, W., & Ling, J. Y. 2021. *e-KYC in Malaysia*. https://www.richardwee chambers.com/e-kyc-in-malaysia/ (July 1, 2021).

Interviews

Interview with Aimi Zulhazmi Abdul Rashid, Kuala Lumpur, July 9, 2020.
Interview with Harpreet Singh, M., Kuala Lumpur, August 9, 2020.
Interview with Muhamad Reza Zaaba, Kuala Lumpur, August 21, 2020.
Interview with Sasinthran, Kuala Lumpur, April 21, 2020.
Interview with Shubham Joshi, Kuala Lumpur, December 15, 2020.