INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 13, Issue 5, (2023) E-ISSN: 2222-6990

Manipulation of Smart Contracts From an Islamic Perspective

Azlin Alisa Ahmad, Mat Noor Mat Zain
Centre for Shariah, Faculty of Islamic Studies, Universiti Kebangsaan Malaysia.

Ranitya Ganindha, Reka Dewantara
Faculty of Law, Brawijaya University

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v13-i5/16898 DOI:10.6007/IJARBSS/v13-i5/16898

Published Date: 08 May 2023

Abstract
Smart contracts are contracts that are executed using blockchain technology and operate in a decentralized, pseudonymous manner and recorded digitally based on computer protocols. However, their implementation raises concerns from an Islamic perspective due to potential ethical and legal issues, such as ambiguous contractual terms, lack of transparency, and potential manipulation of the system by malicious parties. These issues can lead to activities that contradict Islamic principles. This qualitative study, which employs the content analysis for collecting data, aims to examine the potential for manipulating smart contracts from an Islamic perspective. Smart contracts are permissible in Islam as long as they fulfill all the fundamentals and requirements of a contract as well as do not contain elements that may contradict an Islamic contract, including uncertainty of the contracting parties, as well as manipulation of the autonomous system, contract's subject matter, and the contract's objectives. This paper found that smart contract transactions contain several elements that are inconsistent with Islamic contract principles, including elements of uncertainty on the part of the contracting parties, as well as manipulation of the autonomous system, and the contract's subject matter and objectives. Therefore, the controller of smart contracts needs to design an approach that is Shariah-compliant to prevent conflicts and enable its widespread use, especially by Muslims.
Keywords: Manipulation, Smart Contracts, Blockchain, Autonomy, Islamic Contracts

Introduction

A smart contract is a contract executed by contracting parties in a decentralized manner and digitally recorded based on a computer protocol. The idea of a smart contract was sparked in 1996 by Nick Szabo through a paper entitled 'Smart contracts: Building Blocks for Digital Markets Smart Contract'. Szabo's definition of a smart contract is a transaction that executes a contract in a computer protocol with certain criteria. Szabo also suggested that smart contracts should be created to expand electronic transactions involving the point of sale (POS) in the digital industry. The computer protocol proposed in a smart contract is a cryptographic

protocol, which is a programme based on mathematical formulas. This protocol is formulated around the foci of obscurity or also known as keys, which is divided into two parts, namely private and public.

In 2014, Vitalik Buterin used Szabo's theory in Ethereum. Ethereum is a smart contract implemented cryptographically in blockchain technology to facilitate the transfer of ownership of a contracted subject matter. The input programmed into the smart contract is based on the decentralized concept that allows only two parties to interact in the contract without involving an intermediary. Every transaction recorded in a smart contract is charged based on 'gas'. The value of the 'gas' is the service charge that is based on the size of the transaction used in the software, which uses its own cryptocurrency payment system called ether (ETH or Ξ). Ethereum is the second largest cryptocurrency after bitcoin in the crypto market. Hence, the smart contract is a Blockchain 2.0 revolution that gives users the ability to record every transaction cryptographically.

The development of smart contracts as a digital transaction innovation has perfected various types of transactions, including those in the financial sector (The World Bank Group, 2020). Nevertheless, the innovation of smart contracts implemented in blockchain technology has restricted the authority's ability to control and monitor the technology. This is because blockchain creates a decentralized concept in every transaction carried out in the technology including smart contracts. The decentralization concept refers to the transfer of enforcement and control from a centralized entity to the contracting party.

Hence, the smart contract concept also needs to be seen in terms of its compliance to Islamic contract principles. An Islamic contract must fulfil the principles and conditions as well as relevant Syariah law. Islamic contract law protects each and every contracting party involved and ensures that each contract is carried out fairly and in complete trust. In addition, an Islamic contract also needs to be free from any form of dishonor or influence that might affect the objective of a contract.

Islamic contracts should also be free from any form of contractual defect such as fraud, coercion or manipulation etc. Since smart contracts are decentralized and adopt the autonomy and pseudominity concepts, these contracts are easily manipulated by irresponsible parties to carry out activities that contradict Islamic principles. Thus, this study aims to examine the element of manipulation in smart contracts from an Islamic perspective. This study is preceded by a discussion on the formation of smart contracts according to Islamic contract principles. This is followed by a discussion on the elements of uncertainty in the contracting parties, as well as the manipulation of the autonomous system, subject matter of the contract and purpose of the contract.

Drafting a Smart Contract Based on Islamic Contract Principles

Among the smart contracts that were first introduced was the smart contract that acted as a program in the Ethereum blockchain introduced by Vitalik Buterin in 2014. Smart contracts are implemented in blockchain technology to provide users the ability to record every transaction cryptographically. Smart contracts also provide a transaction that is recorded using the solidity language (Venegas, 2017). Use of the solidity language in smart contracts was introduced by Gavin Wood, Hirai Christian Reitweissner and other contributors (Antonopolous & Wood, 2018). *Solidity* is an object-oriented high-level language used in smart contracts. It is influenced by C++, Python and Javacript with the aim of targeting the Ethereum Virtual Machine (EVM) (Asharaf & Adarsh, 2017). The purpose of using *solidity* in smart contracts is to statistically record various agreements in the system. Contracts that can

be recorded in Ethereum include contracts pertaining to sales and purchase, transfer of asset ownership, investments and so on. Hence, Ethereum is able to provide opportunities for developing blockchain technology, including innovation in smart contracts. In other words, Ethereum innovation refers to the development of smart contracts that are converted into written form using the software language called solidity. The following is an illustration of contract writing using the solidity language.

```
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,
35             "\nCheck Alchemy's Mempool to view the status of your transaction!"
```

Diagram 1 Illustration showing the writing of a smart contract using the *solidity language*
Source: The Ethereum.org official website

The diagram above is an illustration of the transcription of a recorded transaction using solidity in a smart contract. The solidity software language used in smart contracts is a form of writing that is used as an offer and acceptance in a transaction.

In Syariah terms, the offer is called *ijab* and the acceptance is called *qabul*. *Ijab* is an offer given by one party and *qabul* is the acceptance of the offer by the other party. *Ijab qabul* is basically carried out by the contracting parties expressing the proclamation. However, it can also be done in other forms, such as writing, actions, or sign language, to convey the intention to execute a contract (Mas'um, 2006). *Ijab qabul* needs to be unequivocal and reflect the wishes of the contracting parties in order to avoid the involvement of *gharar* elements in the contract (Lahsasna, 2012). Therefore, the *ijab qabul*, expressed by the contracting parties, is one of the fundamentals of an Islamic contract, which is *sighah*. The *sighah* method used in smart contracts based on writings in the software language is a consent mechanism permissible in Islam. In reference to Figure 1 above, the message in the 25th row shows that the contracting parties who carried out a transaction known as *'web3.eth.accounts.sgnTransactions'* had signed the above transaction using a private key. A private key is a digital signature to confirm and determine the identity of a contracting party in Externally Own Accounts (EOA) (Yusof, 2016).

Each private key owner has a different private key serial number to distinguish the identity of the key. Private keys are obtained in the form of characters such as a binary code, hexademical code, mnemonic phrase or QR code. The owner of the private key is autonomous so information regarding the key's owner is not disclosed to other contracting parties. Therefore, the contracting parties in the schedule only use the pseudonym 'web3.eth.accounts.sgnTransactions' as their identification in the contract without revealing actual personal information. The private key is required by 'web3.eth.accounts.sgnTransactions' to confirm and agree to submit hash transactions to

other contracting parties. The 30th row shows that the transaction was canceled due to an error in the delivery of the receipt. The party receiving the acceptance (*qabul*) confirmed the bond by replying 'err'. The term 'err' in the 30th row has no meaning in the software that has been input and transferred to the error code. On the other hand, the recipient of the offer needs to confirm it by using the private key to agree to accept (*qabul*) the offer (*ijab*). Nevertheless, each transferred transaction is disclosed using a public address. 'web3.eth.accounts.sgnTransactions' provides a public address in the form of a location to carry out transactions in smart contracts. Public addresses are provided in the form of hash cryptography to compress the size of public keys. Public keys act as a cryptographic system that is able to ensure the authenticity and integrity of the message conveyed in the contract.

Therefore, the *sighah* implemented in a smart contract fulfills the criteria based on Islamic contract principles. The implementation of *sighah* using the writing method is permitted in Islamic law. Furthermore, the use of a private key in the transaction as confirmation of the contract is allowed in order to obtain consent from each party involved. However, contracting parties should be reminded to examine and review the contract first before confirming the transaction. The involvement of *sighah* in the implementation of smart contracts is essential to ensure that the transaction is permitted in accordance with Islamic principles. Each promised transaction must be fair and unequivocal according to the agreement by all parties without creating any doubt. A written *sighah* can also help the contracting parties by using it as proof of a bond between them. The *sighah* bond in a smart contract is comparable to an electronic contract transaction (Abdul Rashid, 2019). Transactions in electronic contracts are regarded as an '*urf*' faced by society today, although society is more inclined to use technology, especially in online sales and purchase transactions. It is also an innovation in the financial industry that helps the development of sales and purchase transactions involving the binding of *ijab qabul* in different locations at the same time. Hence, transactions in smart contracts using the *solidity* language software are valid from the Islamic viewpoint as long as they do not involve elements of contention, fraud or doubt in the contract. The following is a diagram showing the findings of the study on forming *sighah* in smart contracts.

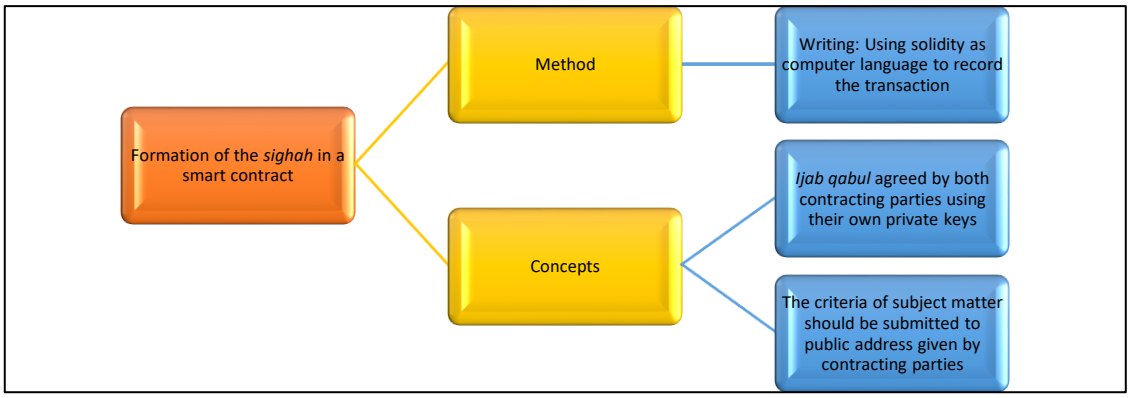


Diagram 2 Forming of the *aqad* in a smart contract

Therefore, results of the study on the formation of smart contracts according to Islamic contract principles indicate the involvement of *sighah* in *ijab qabul*. The *sighah* method used in smart contracts is one of the types of language software, namely solidity, introduced by Gavin Wood. Transactions recorded in the software are verified by the contracting parties using private keys. The use of language software as a *signah* in the implementation of smart contracts does not contradict Islamic contract principles. In fact, the concept is an innovation

in transactions implemented in written form that is permitted under Islamic contract principles. Meanwhile, location of the transaction carried out by using a public address is in the form of hash cryptography. The writing used in the transaction must be unequivocal and explicit to avoid any contradiction and deviation in the agreement. In addition, the contracting parties also need to understand the meaning of each and every word written in the contract and need to learn the language software more thoroughly.

Ambiguity Issues in Contracting Parties

The use of pseudominity by contracting parties creates doubt in recognizing the contracting parties in a smart contract. The main criterion for a contracting party in an Islamic contract is an individual who has the qualifications to carry out the contractual obligations (Salwani 2012). Since the pseudominity concept is maintained in smart contracts, it has made it difficult for the software to track and identify the contracting parties. In fact, the main criteria for contracting parties according to Islamic contract principles are capability (*ahliyyah*) and power or authority (*wilāyah*). Capability in an Islamic contract refers to an individual who has the right to fulfill obligations and responsibilities when implementing a Syariah-compliant contract (Lahsasna, 2012). Whereas the authority refers to an individual who has the authority over the contracting party and is recognized based on Syariah law (Azman, 2016). There is also a general principle regarding the prohibition of an individual involved in the execution of contracts, which includes those who are mentally unsound, improvident, bankrupt, mentally disabled or a minor. Implementation of the pseudominity concept in a smart contract makes it difficult to identify the capability of the contracting parties who engage in a smart contract. This capability creates doubt as to whether the individual is qualified based on Islamic contract principles. Hence, there is doubt about the legal criteria of the contracting party causing the presence of *gharar* in the compliance of the contracting party.

The element of *gharar* in these transactions refers to the existence of the pseudominity concept, which does not require the personal identification of the contracting party registered in a smart contract. Personal identification is used in smart contracts by using language software and hash cryptography. Although smart contract transactions are conducted based on the willingness of the contracting parties, however, the ability of the contracting parties based on Islamic contract principles is not identified and is a question mark.

Therefore, smart contracts do not create a personal identity registration for contracting parties and make it difficult for the parties involved to trace the true identity and status of the individual. Moreover, use of the autonomy concept has restricted the authorities in their efforts to control and monitor the system. This method has created doubt about the status of the contracting parties because it conceals personal information and this leads to the element of *gharar*. This concept is contrary to the fundamentals of an Islamic contract because Islamic contracts emphasize the “Know Your Customer” (KYC) concept (Abdul Rashid, 2019). The KYC concept is also a standard applied in various financial and banking industries to clearly and explicitly verify the customer’s information, which involves their risk and financial profiles (Chen, 2022).

Bank Negara Malaysia (2019) has issued a draft guideline proposal for implementing e-KYC or electronic entry for individuals in the financial sector. The proposal was mooted to ensure that the security of e-KYC transactions is guaranteed, they have structured supervision or monitoring and control measures related to Anti-Money Laundering and Anti-Terrorism

Financing are more effective. The e-KYC standard is also consolidated by incorporating artificial intelligence to detect the user's face and optics (Wee et al., 2021). Contracting parties involved in smart contracts exhibit the element of *gharar* when determining the legal conditions of the contracting parties' qualifications based on Islamic contract principles. Legal conditions must be complied with and is an obligation under Islamic law. However, if a contract contains elements that violate or create doubt in the legal terms of an Islamic contract, then the contract becomes void (Ruzian et al., 2020). Thus, the operator needs to ensure that the contracting parties must followed the requirements of Islamic contracts. The requirements of Islamic contract have been throughout and referring to Sharia compliance to guide and protect every parties involved. Hence, smart contracts able to implement the e-KYC standard issued by the Bank Negara Malaysia for supervise and monitor the credentials of contracting parties in them. This following to ensure the contracting parties has the ability to engage in the execution of the contract.

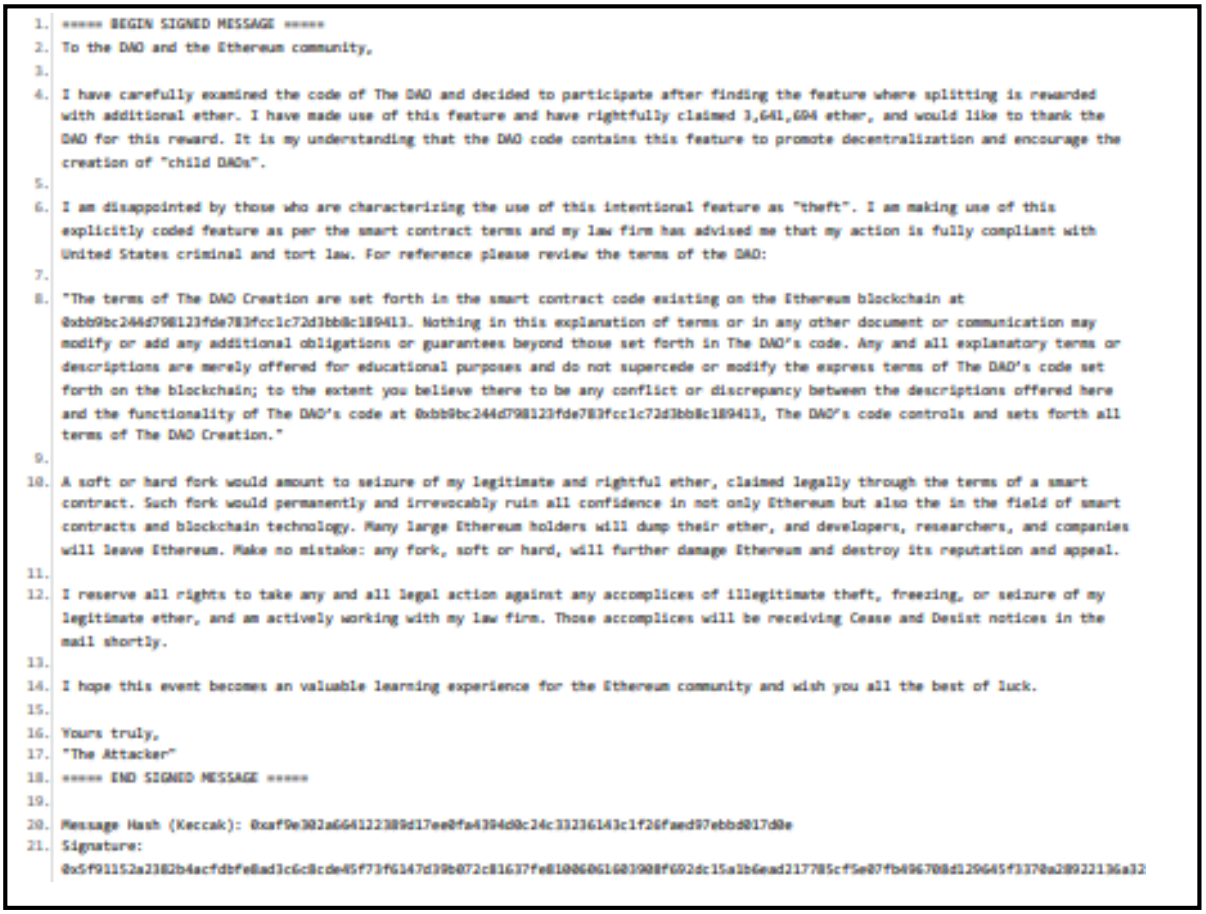
Manipulating the Autonomy Concept in Smart Contract Transactions

The main concept of a smart contract is to practice and provide autonomy to the parties involved in the technology. Autonomy means that the parties involved in any transaction are not controlled by an external entity. Autonomy also means the use of pseudonyms by contracting parties without identifying them or revealing their personal information (Mohd Asri, 2018). The autonomy concept was implemented in smart contracts in 2016 and was better known as Decentralized Autonomous Organization (DAO) (Siegel, 2016; Kuhn, 2020). The DAO was formed as a virtual entity in a smart contract that is responsible for executing each recorded transaction (Falkon, 2017). This is because every activity carried out in the blockchain technology is in the form of algorithms and a mutually agreed upon platform involving virtual and autonomous entities. DAOs are responsible for reducing transaction costs and adopt mutual consent rules that are bound only in crypto tokens. However, the DAO is not bound by any legal provision. In fact, DAO members are individuals with unknown backgrounds, especially with the need to interact openly with the members.

Autonomy is also applied to the contracting parties' personal information. Contracting parties do not need to legally register their names or personal information in order to execute smart contracts. Conversely, contracting parties are only allowed to register using the pseudominity concept. Pseudominity refers a fictional name or pen name or pseudonym used for a specific purpose (Jeetun, 2013). This concept was established to ensure a more practical implementation of providing ideological satisfaction to privacy in a radical manner (Certik, 2022). Unfortunately, this concept has given the opportunity to some irresponsible parties to use this technology for carrying out illegal activities.

The Child DAO under the DAO structure was hacked on June 18, 2016 for 3.6 million ether (Siegel, 2016). A letter was publicly issued by an individual autonomously stating that the money he had hacked was done so 'legally' and in compliance with the rules in Ethereum (Finley, 2021). The party also threatened to take legal action if there was interference from

any party. Until now, the owner of the letter has not been identified because it was written in Ethereum.



```
1.  ===== BEGIN SIGNED MESSAGE =====
2.  To the DAO and the Ethereum community,
3.
4.  I have carefully examined the code of The DAO and decided to participate after finding the feature where splitting is rewarded
    with additional ether. I have made use of this feature and have rightfully claimed 3,641,694 ether, and would like to thank the
    DAO for this reward. It is my understanding that the DAO code contains this feature to promote decentralization and encourage the
    creation of "child DAOs".
5.
6.  I am disappointed by those who are characterizing the use of this intentional feature as "theft". I am making use of this
    explicitly coded feature as per the smart contract terms and my law firm has advised me that my action is fully compliant with
    United States criminal and tort law. For reference please review the terms of the DAO:
7.
8.  "The terms of The DAO Creation are set forth in the smart contract code existing on the Ethereum blockchain at
    0xbb9bc244d798123fde783fcc1c72d3bb8c189413. Nothing in this explanation of terms or in any other document or communication may
    modify or add any additional obligations or guarantees beyond those set forth in The DAO's code. Any and all explanatory terms or
    descriptions are merely offered for educational purposes and do not supercede or modify the express terms of The DAO's code set
    forth on the blockchain; to the extent you believe there to be any conflict or discrepancy between the descriptions offered here
    and the functionality of The DAO's code at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413, The DAO's code controls and sets forth all
    terms of The DAO Creation."
9.
10. A soft or hard fork would amount to seizure of my legitimate and rightful ether, claimed legally through the terms of a smart
    contract. Such fork would permanently and irrevocably ruin all confidence in not only Ethereum but also the in the field of smart
    contracts and blockchain technology. Many large Ethereum holders will dump their ether, and developers, researchers, and companies
    will leave Ethereum. Make no mistake: any fork, soft or hard, will further damage Ethereum and destroy its reputation and appeal.
11.
12. I reserve all rights to take any and all legal action against any accomplices of illegitimate theft, freezing, or seizure of my
    legitimate ether, and am actively working with my law firm. Those accomplices will be receiving Cease and Desist notices in the
    mail shortly.
13.
14. I hope this event becomes an valuable learning experience for the Ethereum community and wish you all the best of luck.
15.
16. Yours truly,
17. "The Attacker"
18. ===== END SIGNED MESSAGE =====
19.
20. Message Hash (Keccak): 0xaf0e302a6641223894d17ee0fa4394d0c24c33236143c1f26faed97ebbd017d0e
21. Signature:
    0x5f91152a2382b4acfdbfe8ad3c6c8cde45f73f6147d39b072c81637fe8100606160139088f692dc15a1b6ead217785cf5e07fb4967088d129645f3370a28922136a32
```

Diagram 3 The autonomous letter pertaining to the hacking of the DAO
Source: steemit.com

The code input into the DAO has various errors leading the emergence of the case (Falkon, 2017). Some think this attack is a maneuver, a movement based on skill and the correct technique, but it is unethical (Price, 2016). After this happened, DAO's founder only issued a statement suggesting that investors who invested in the DAO should transfer their money to another account (Popper, 2016). Until now, this issue has not been resolved and the money has not been returned to the rightful owner.

Based on the statement above, identifying the contracting parties was only made known by using the pseudominity identity to introduce the autonomy concept. Figure 1 shows the use of pesudominity, which is 'web3.eth.accounts.sgnTransactions', in the transaction. The transaction transfer location was based on the public address provided by the contracting parties. The following diagram presents information pertaining to the public address transaction in the smart contract.

Diagram 4: Smart contract transaction information
Source: The official Alchemy website

Figure 4 shows the location and information related to smart contract transactions between two contracting parties. Data were recorded using binary code or *hash* cryptography. '0:' is the public address, while 'from:' and 'to:' are the public keys owned by the sender and receiver of the transaction. This autonomy concept is intended to comply with the establishment of decentralization in the blockchain. The purpose of implementing decentralization in the blockchain is to block the involvement of intermediaries or authoritative parties. In fact, this method has led to the use of technology for activities that are illegal, including non-compliance with Islamic contracts. The analysis of this study is based on a case study of United States v. Ross Ulbritch. Ross Ulbritch used blockchain technology as an illegal trading platform. He provided opportunities for sales and purchase activities, such as illegal weapons, drugs etc. using crypto transactions. Ulbritch chose this technology because blockchain is able to provide an opportunity to the parties involved to carry out transactions autonomously and with pseudominity.

Manipulating the Subject Matter of the Contract in a Smart Contract

The autonomy concept adopted by blockchain technology allows contractual activities to be carried out independently without control from the authorities, which leads to the involvement of a non-Syariah-compliant subject matter. Data analysis obtained from Ulbritch's case study shows that blockchain technology was chosen to carry out black market sales and purchase activities without the knowledge of the authorities. Involvement in the sale and purchase of illicit drugs is not allowed in Islam and has been determined using the legislation that prohibits alcohol consumption. The prohibition of alcohol consumption in Islam mentioned in Surah al-Maidah verse 90 in the al-Qur'an.

Factors that encourage drug abuse can be harmful and risky to one's own health and the lives of the community. Another risk factors for drug abuse are drug availability in black market, loss in external locus of control and sensation-seeking behavior. It also causes financial losses and addicts tend to lose self-control simply to fulfill their addiction desires through stealing, mugging or robbery (Rasidah, 2016). Identified drug abusers in Malaysia are sent for compulsory rehabilitation and treatment programs for two years. This program was mandated by the Malaysian law if the drug abusers was found guilty under Section 15(1) of the Dangerous Act 1952 (Act 234) (Awang & Bernama, 2023).

Manipulating the Objective of the Contract (maqsad)

Smart contracts also allow investment transactions known as ponzi schemes. A ponzi scheme is an investment scheme that promises high profits with low risks to investors (Zhang et al., 2022). However, the profit accruing to investors is not from the sale of a subject matter but

based on deposits (money) received from new investors. The ponzi scheme, introduced by Charles Ponzi, is a fraudulent scheme that has been perpetrated for centuries (Weisman, 2020). This method is thought to be *zaim*, fraudulent, oppressive or deceiving of investors (Muzakarah National Fatwa Committee, 2009). *Forsage* is an application that provides ponzi scheme investments in Ethereum and it managed to earn 2.8 million ether (Redman, 2020). However, ponzi schemes are strongly prohibited in Islamic law because the returns obtained from investors are known as windfall or "baseless" profits (Muhammad Fazli Sabri, 2019). There is also an element of *gharar* in the transactions because the returns are obtained without any effort and is ambiguous. In fact, the risk of loss in a ponzi scheme is higher than the rate of profit because most ponzi scheme investors have to bear high debts due to claims from new investors (Hashim, 2019).

Conclusion

Smart contracts are the latest innovation in the formation of contracts. Basically, it is permitted in Islam as long as it fulfills all the fundamentals and conditions of a contract as well as Syariah principles. However, smart contract transactions contain several elements that are inconsistent with Islamic contract principles, including elements of uncertainty on the part of the contracting parties, as well as manipulation of the autonomous system, and the contract's subject matter and objectives. Flaws in smart contracts are related to the contracting parties due to the pseudominity concept that can restrict information regarding the contracting party's identity, thus, the contracting party's qualifications cannot be determined. Meanwhile, manipulation of the system causes it to be hacked and contravene the law. Manipulation of the contract's subject matter allows irresponsible parties to transact goods that are not permitted by Syariah. The objective of the contract can be manipulated by conducting activities that violate the very purpose of the contract itself. Therefore, smart contract operators need to plan an approach that avoids using such a contract and system in order to be Shariah-compliant and allow it to be widely used, including by Muslims.

Acknowledgement

We would like to express our sincere gratitude to Research Grant Universitas Brawijaya, Grant Code PP-2022-027 for funding the research presented in this article.

References

Al-Quran.

Abdul Rashid, A. (2019). Application of Smart Contracts and Cryptocurrencies. (N. A. Zakaria, Interviewer).

Antonopoulos, A. M., & Wood, G. (2019). *Mastering Ethereum: Building Smart Contracts and DAPPS.* Sebastopol: O'Reilly.

Asharaf, S., & Adarsh. S. (2017). *Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities*. Hershey: Information Science Reference IGI Global.

Awang, B., & Bernama. (2023). Akta Baru Masalah Dadah: Sinar Baru Tangani Kesesakan Penjara. Kuala Lumpur, Malaysiakini.

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

Buterin, V. (2014). *A Next-Generation Smart Contract and Decentralized Application Platform*. White Paper 3(37): 1-36.

Certik. (2022). *What is Pseudonymity and Anonymity?* Didapatkan dari Medium: https://tinyurl.com/4yrekhks

Chen, J. (2022). *Know Your Client (KYC): What It Means, Compliance Requirements*. Retrieved from Investopedia: https://tinyurl.com/vuem4w3c

Committee, M. N. (2009). Hukum Skim cepat Kaya dan Seumpamanya. In *Himpunan Keputusan Muzakarah Jawatankuasa Fatwa Kebangsaan Berhubung dengan Isu-isu Muamalat* (pp. 71-75). Kuala Lumpur: Malaysia National Library.

Dannen, C. (2017). *Introducing Ethereum and Solidity.* New York: Apress.

Falkon, S. (2017, December 24). *The Story of DAO – Its History and Consequences*. Retrieved from Medium: https://tinyurl.com/3bwksepe

Finley, K. (2016). *A $50 Million Hack Just Showed That the DAO Was All Too Human*. Retrieved from WIRED: https://tinyurl.com/mu86tm49

Frankel, T. (2012). *The Ponzi Scheme Puzzle: A History and Analysis of Con Artists and Victims.* United States of America: Oxford University Press.

Gerard, D. (2017). *Attack of the 50 Foot Blockchain: Bitcoin, Blockchain, Ethereum and Smart Contracts.* United Kingdom: David Gerard.

Group, T. W. (2020). *Smart Contract Technology and Financial Inclusion.* Washington: The World Bank Group.

Hashim, H. (2019). *Undang-Undang MLM*. Retrieved from Sinar Harian: https://tinyurl.com/yy76y2bx

Jeetun, P. (2013). *Rebranding For Writers: An Analysis of the Use of Pseudonyms*. Retrieved from Artslaw: https://tinyurl.com/bdh78fsv

Kuhn, D. (2020). *Did Ethereum Learn Anything From $55M DAO Attack?* Retrieved from CoinDesk: https://tinyurl.com/4whtjfz2

Lahsasna, A. (2012). *A Mini Guide to Islamic Contracts in Financial Services*. Kuala Lumpur: Centre for In Research and Training (CERT).

Leng, J., Sha, W., Lin, Z., JIn, J., Liu, Q., & Chen, X. (2022). *Blockchain smart contract pyramid-driven multi-agent autonomous process control for resilient individualised manufacturing towards Industry 5.0*. International Journal of Production Research, 1-20.

Fauzi, M. H., & Faudzi, M. F. M. (2010). *Al-Muamalat Jilid 2*. Kuala Lumpur. Pena Syariah Bank Muamalat.

Billah, M. M. (2006). *Sharia Standard of Business Contract*. Kuala Lumpur: Perpustakaan Negara Malaysia.

Yusof, M. A. (2016). *Undang-Undang Kontrak Di Malaysia*. Gombak: Mus'ab E-Books Publication House.

Sabri, M. F. (2019). *Kenali Dan Fahami Antara Multilevel Marketing (MLM) & Skim Piramid*. Retrieved from Universiti Putra Malaysia: https://tinyurl.com/mry9zhmf

Norry, A. (2020). *The History of Mt. Gox Hack: Bitcoin's Biggest Heist*. Retrieved from Blockonomi: https://tinyurl.com/yyx56vv4

Popper, N. (2016). *A Hacking of More Than $50 Million Dashes Hopes in The World of Virtual Currencies*. Retrieved from New York Straits Times: https://tinyurl.com/35d753ap

Price, R. (2016). *Digital Currency Ethereum Is Catering Because $50million Hack*. Retrieved from Insider: https://tinyurl.com/2pakmmzx

Rasidah. (2016). *Brunei to mark international anti-drug day in August*. Retrieved from BTarchive: https://tinyurl.com/2wjprddt

Redman, J. (2020). *Despite Warnings from Regulators, The Ethereum Fueled Pyramid Scheme Forsage Thrives*. Retrieved from Bitcoin.com: https://tinyurl.com/bdfvrb9c

Abd Razak, S. A. (2016). *Combination of Contracts in Islamic Finance*. Kuala Lumpur: Islamic Banking and Finance Institute Malaysia.

Siegel, D. (2023). *Understanding the DAO Attack*. Retrieved from CoinDesk: https://tinyurl.com/yxb9fefb

Razali, S. S. (2010). *Islamic Law of Contract*. Singapore: Cengage Learning Asia Pte Ltd.

Six, N., Ribalta, C. N., Herbaut, N., & Salinesi, C. (n.d.). A Blockchain-Based Pattern for Confidential Pseu-Anonymous Contract Enforcement. Retrieved from https://tinyurl.com/a8nnrdtm

Solomon, M. G. (2019). *Ethereum for dummies.* New Jersey: John Willey & Sons Inc.

Szabo, N. (1996). Smart Contracts: Building Blocks for Digital Markets. pp. 1-11.

UNITED STATES OF AMERICA v. ROSS WILLIAM ULBRICHT DREAD PIRATE ROBERTS SILK ROAD SEALED DEFENDANT DPR. (2017), 15-1815 (United States Court of Appeals, Second Circuit. Mei 31, 2017).

Venegas, P. (2017). Crypto Economy Complexity. *Journal of Economic Literature G02*. Costa Rica. SSRN: 3073413

Wadhaj, I., Ghaleb, B., Thomsom, C., Al-Dubai, A., & Buchanan, W. J. (2020). Mitigation Mechanisms Against the DAO Attack on the Routing Protocol for Low Power and Lossy Networks (RPL). *IEEE, 8*, 43665-43675.

Wee, R., Ho, W., & Ling, J. Y. (2021). e-KYC in Malaysia. Retrieved from Richard Wee Chambers: https://tinyurl.com/zume8prc

Weisman, S. (2020). *The History of Ponzi Schemes Goes Deeper Than the Man Who Gave Them His Name*. Retrieved from TIME: https://tinyurl.com/35f4tm3v

Zhang, H., Yu, J., Yan, B., Jing, M., & Zhao, J. (2022). Security on Ethereum: Ponzi Scheme Detection in Smart Contract. *Algorithmic Aspects in Information and Management* (pp. 435-443). Guangzhao: Springer, Cham.