International Journal of Business, Law, and Education
E-ISSN : 2747-1349
Publisher: IJBLE Scientific Publications Community Inc.
Volume 6, Number 1, 2025
https://ijble.com/index.php/journal/index

Can Smart Contracts Have a Legality Valid in Indonesia?

Dina Berliana Bintang Rotua, Reka Dewantara, Yenny Eta Widyanti
Universitas Brawijaya, Universitas Brawijaya, Universitas Brawijaya
dinaberlianaa@student.ub.ac.id, rainerfh@ub.ac.id, yenni.eta@ub.ac.id

ABSTRACT
The development of digital technology has encouraged the use of smart contracts as an instrument for automating agreements in Blockchain-based electronic transactions. In the context of Indonesian law, the validity of a smart contract must meet the legal requirements for an agreement, as stipulated in Article 1320 of the Civil Code, which includes the agreement between the parties, their legal capacity, a transparent object of the agreement, and lawful causes. Additionally, data verification in smart contracts is a key element in guaranteeing the security, authenticity, and transparency of e-commerce transactions, which is related to the provisions in the ITE Law and the PDP Law. This verification aims to prevent data manipulation, reduce the risk of fraud, and increase trust in transactions by utilizing encryption technology, digital signatures, and Blockchain-based identity verification. Smart contracts can be considered valid if they fulfill the terms of the agreement and data security principles, making their use in e-commerce more effective and reliable.

Keywords:
Smart Contract, Blockchain, Legality of Smart Contracts, Personal Data Protection.

INTRODUCTION

Current technological developments are a phenomenon that cannot be avoided and continue to evolve. Society must be able to recognize and adapt to technology to maximize its potential. In today's era, technology has become a tool that simplifies human life. The emergence of various technological products, including computers, the internet, smartphones, social networking sites, blockchain systems, and others, marks a significant development in science and technology today. These technological advancements have made life easier for humans. Therefore, the modern era is often referred to as the era of digitalization, where computer and internet technology have facilitated tasks and enhanced the quality of human life. Electronic commerce (e-commerce) is a legal event between a seller and a buyer, conducted indirectly via the internet network and electronic devices through an electronic agreement or contract. In the development of digital technology, personal data, such as names, email addresses, and cellphone numbers, are valuable assets because they can yield economic benefits and are widely utilized by businesses (Tejomurti et al., 2019).

By the name of the contract, namely Smart Contract, is a digital contract designed with modern technology, combining human needs with advanced technology while keeping up with developments in this rapidly evolving era. The combination of humans and technological advancements has led to Smart Contracts being considered the "contracts of the future." In contrast, other contracts we are familiar with and often use are called "conventional contracts," as they predate the emergence of Smart Contracts. A Smart Contract is not a conventional contract written on paper, nor is it an electronic contract. However, the key difference lies in the agreement clause, which is in the form of programming and requires blockchain as a distributed storage technology.

Smart Contracts differ from electronic contracts because the agreement clause is written as programming code and relies on blockchain for distributed storage.

Furthermore, a Smart Contract is designed to execute the contract automatically (self-executing). This means that the agreement, whose implementation is automatic or self-executing, is carried out through computer code that is necessary to execute the contract's contents. This system allows buying and selling transactions without requiring sellers and buyers to meet directly. In this case, the transaction actors base their trust on each other (Kirana et al., 2019). The legal relationship that arises from buying and selling activities creates an agreement between the parties, and this agreement must be implemented as regulated in Articles 1457–1540 of the Civil Code. However, to date, no regulations or provisions in the Civil Code accommodate the legal requirements of electronic agreements using Smart Contracts. As a result, the regulatory basis remains limited, referring to the provisions of Article 1320 of the Civil Code. Currently, electronic transactions use a new instrument known as a Smart Contract. As previously explained, it is worth reiterating that a Smart Contract is a program or code set based on conditions approved and determined by stakeholders or those who have agreed to execute a digital system mechanism.

Conventional contractual agreements are regulated under the positive law in Indonesia, namely the Civil Code ("Perdata Code"). As is known, contracts or agreements are generally written in a formal, written form. However, the existence of verbal agreements and contracts has been recognized, whether consciously or unconsciously, for a long time in our society. Based on the provisions of Article 1313 of the Civil Code, there is no explicit mention of "written agreements." The Civil Code defines an agreement as an act by one or more people binding themselves to another person. The parties enter into an oral agreement through a verbal agreement, whereas a written agreement is made in written form (a contract), either as an authentic deed or a private deed. The legal strength of these two types of agreements is not in their written or verbal form. A contract is also a voluntary exchange of promises between the parties involved.

Article 1339 of the Civil Code expands the obligations in agreements to include not only what is written in the contract but also things that are reasonably expected based on the nature of the agreement, custom, or law that is informed. Additionally, a Smart Contract qualifies as a valid agreement if there is a voluntary agreement between the parties. Like conventional contracts, the parties' agreement is the basis for validity, as the Pacta sunt servanda principle renders the Smart Contract a valid and binding agreement. Articles 1338 and 1339 emphasize that agreements must be made in good faith and a proper manner. Even though smart contracts are automatically executed by technology, the element of good faith still applies to the interpretation of contract results. Suppose the Smart Contract code results in unfair outcomes or deviates from the parties' initial intentions. In such a case, a dispute may arise that must be resolved in accordance with the principles of propriety as outlined in Article 1339. Based on Articles 1338 and 1339 of the Civil Code, a Smart Contract can be considered valid if it fulfills the requirements of a valid agreement. This article supports the validity of contracts and the obligation to carry out agreements in good faith, as mandated by law. However, considering that Smart Contracts have different technical characteristics from conventional contract concepts, this research will discuss the need for additional regulations related to clear legal interpretation to provide legal certainty in using Smart Contracts. The biggest issue underlying the virtual currency ecosystem in Indonesia is not the misleading definition but the lack of a clear direction

in national policy regarding how to precisely regulate the cryptocurrency market and legally protect the various parties involved (Chang, 2018)

Based on the current laws and regulations, the position of Smart Contracts is equated with electronic transactions, as explained in Article 1, number 2 of the ITE Law. The Second Law, Law Number 1 of 2024, on the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, defines in Article 1, number 2 that "Electronic Transactions are legal acts carried out using computers, computer networks, and/or other electronic media." This means that Smart Contracts can still be used to set out their clauses as instruments for carrying out electronic transactions. The explanation of the article above only illustrates that Smart Contracts can be linked and equated as a form of electronic transaction. Still, the reason is insufficient to understand the Smart Contract's position regarding its validity and the form of responsibility in its use. Based on the explanation above, Indonesia currently lacks specific legislation regarding the legality and legal protection of parties using Smart Contracts. However, the legal regulation that can be used as a reference and normative basis in this case is Article 1, point 2 of the Second Law, Law Number 1 of 2024, on the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions[Undang-Undang Kedua atas Undang-Undang Nomor 1 Tahun 2024 atas Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Bunyi Pasal 1 angka 2 “Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.” Hal ini mengartikan bahwa tetap dapat menggunakan Smart Contract dalam penuangan klausulanya sebagai instrumen dalam melakukan transaksi elektronik.. However, this arrangement can only serve as a legal basis for utilizing Smart Contracts in electronic transactions in a normative manner. The reason is that the regulatory provisions in the ITE Law only regulate the position of Smart Contracts in electronic transactions. In contrast, there is no regulation regarding the legal validity of Smart Contracts themselves in terms of compliance with contract law, specifically by explaining the limitations of the rights and responsibilities of the parties in carrying out Smart Contracts. Additionally, there are no regulations on how standard agreements can be verified and agreed upon when creating Smart Contract clauses. This research focuses on how the security of blockchain technology affects data privacy security when using Smart Contracts.

METHOD

This research will specifically discuss and analyze whether Smart Contract agreements have valid legal force, ensuring their effectiveness compared to conventional contracts. It will also analyze efforts to establish legal norms that complement the provision of legality, rights, and obligations for using Smart Contracts and discuss the form of accountability in the event of a dispute. The research will focus on regulating the parties' obligations and analyzing blockchain security to protect the parties' data. This article focuses on discussing the legality of Smart Contracts and the legal protection of Personal Data that has been incorporated into innovative contract systems using blockchain technology. This article employs a normative juridical method with a conceptual approach and a comparative legal approach.

International Journal of Business, Law, and Education
E-ISSN : 2747-1349
Publisher: IJBLE Scientific Publications Community Inc.
Volume 6, Number 1, 2025
https://ijble.com/index.php/journal/index

RESULTS AND DISCUSSION

1. Concept of Using Smart Contracts as an Instrument in E-Commerce Transactions

1.1 Smart Contract Concept

A Smart Contract is a further development of blockchain applications following the emergence of cryptocurrency. It is a computer program that functions as an electronic agreement in a blockchain database system, designed to execute agreement clauses automatically. However, what differentiates Smart Contracts from other computer programs is that they are stored on the blockchain, making all interactions with Smart Contracts immutable. Smart Contracts can define rules and automatically apply them through code, eliminating the need for a third party to ensure the execution of transactions or activities (Adhijoso, 2019).

Smart Contracts have several characteristics that are used to identify the features contained within them. These characteristics help determine the validity of a Smart Contract compared to other agreement structures. The attributes of Smart Contracts are as follows: First, Smart Contracts are software. According to Imran Bashir, a Smart Contract is secure and uninterrupted software that aims to become a contract that automatically comes into force and is executed. The security and transparency of the Smart Contract itself are ensured on the Blockchain platform, which means that every transaction occurring on the blockchain cannot be altered, and only parties with permission can view the results. Since every blockchain network is public, every transaction and agreement in a Smart Contract is transparent, making it easier to track transactions with much more security, as it does not depend on a central authority.

An agreement must meet several important parameters to be recognized as a Smart Contract. First, Smart Contracts must run and be stored on the blockchain network to ensure security and transparency, allowing all relevant parties to verify the execution of the agreement independently. Second, Smart Contracts must be able to execute their provisions automatically without needing third-party intervention. The logic governing this execution must be clear and codifiable in a programming language, meaning that all terms of the agreement can be expressed as "if-then" instructions. Third, due to the immutable nature of blockchain, each deal in a Smart Contract is unchangeable; therefore, the reliability of the code and the security of the contract are crucial to prevent errors or vulnerabilities. In addition, Smart Contracts must meet the basic requirements of contract law, such as agreement between parties and clarity of the object of the agreement, to be valid in the relevant jurisdiction. Finally, to be utilized in complex business contexts, Smart Contracts must be able to interact with external systems via oracles that provide additional data, such as price information or market conditions, necessary to trigger contract execution. By meeting these parameters, Smart Contracts can be recognized as a valid and automatic form of agreement in the blockchain ecosystem. In blockchain technology, alongside coins, the concept of "tokens" exists. Unlike coins, tokens are not native assets of any blockchain. Their inception followed the recognition of smart contracts within blockchain technology, introduced by the Ethereum blockchain in 2015. Smart contracts enable parties interacting within the blockchain to perform functions beyond simple coin transactions, such as including clauses in each transaction. Consequently,

ownership clauses in contracts give rise to tokens, which represent the owned object or right (Multazam et al., 2023).

The form and function of Smart Contracts differ significantly from conventional agreements and electronic agreements. While electronic contracts are similar to traditional agreements, the key difference lies in their use.

1.2 Concept of Smart Contract Validity

When discussing whether a contract is valid, it must fulfill the conditions for the validity of a contract as outlined in Article 1320 of the Civil Code, which states, "Four conditions need to be fulfilled: the agreement of those who bind themselves, the ability to agree, a certain subject matter, and a cause that is not prohibited." A Smart Contract, which includes an agreement between the parties, has a legal basis in the principle of freedom of contract. The principle of freedom of contract is contained in Article 1338, paragraph (1) of the Civil Code, which states, "All agreements contained are legally binding on the parties as law. Every legal subject is free to make agreements, both in form, content, and the time and method of implementation. A contract can be made by anyone freely, as long as it fulfills the legal requirements of the contract and does not violate the provisions of the law, morality, and public order."

This serves as the legal basis for data verification in smart contracts under Indonesian law.

1. Article 1320 Civil Code - Conditions for the Validity of an Agreement

"Smart Contracts used in e-commerce transactions must fulfill the elements of the agreement, capacity, specific subject matter, and lawful cause. Data verification supports the "agreement" element by ensuring that the parties to the transaction are genuinely legitimate."

2. Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE)
   (1) Article 5: "Electronic information and electronic documents are recognized as legal evidence, including verified data in Smart Contracts."
   (2) Article 28 Paragraph (1) "Prohibit the spread of false information, so the data verification process is important to prevent fraud."
3. Law Number 27 of 2022 concerning Personal Data Protection (UU PDP)

(1) Article 15
"Data controllers are obliged to ensure that the data processed is accurate, relevant, and by its intended use, including the data verification process in the Smart Contract."

(2) Article 16
"Personal data must be protected from illegal access during the verification process."

1.3 Concept of Data Verification in Smart Contracts

The validity of a Smart Contract refers to the conditions for the validity of an agreement, as outlined in Article 1320 of the Civil Code, which includes the agreement of the parties, legal capacity, a specific subject matter, and a lawful cause. A Smart Contract can be considered valid if it meets these four conditions, where the agreement is reflected through digital consent provided by the parties, and the object and purpose of the contract are clearly explained in the programming code. The legal competence of the parties remains a prerequisite, ensuring that only parties who fulfill the legal requirements can enter into a contract. However, the validity of Smart

Contracts raises challenges regarding data verification, a key element in ensuring the automatic execution of contracts as agreed upon. In the context of data verification in Smart Contracts, the validity of the data entered into the contract greatly influences the agreement's implementation. The data must be verified to ensure that it does not contain errors or manipulation, as Smart Contract automation systems cannot assess data validity beyond what has been programmed. Therefore, an oracle mechanism is needed—a third party or system that guarantees the accuracy of real-world data before the Smart Contract uses it. Without a valid and reliable verification mechanism, Smart Contracts could pose a risk of execution that does not align with the parties' wishes, which could lead to the validity of the agreement being questioned. Thus, implementing Smart Contracts requires additional legal regulations that address the validity of the data verification process to ensure the deal is implemented by civil law.

The data verification process in a Smart Contract is a crucial stage that ensures the legitimacy and validity of the data entered into the digital contract. In e-commerce transactions, data verification involves checking the parties' identity, the validity of goods or services information, and the accuracy of payments. Data verification in a Smart Contract has the aim of: (1) Ensuring the authenticity of the data to prevent the use of false data or manipulation of information that could harm one of the parties in the transaction. (2) Reducing the risk of fraud using verification, which can ensure that the parties involved are legitimate entities and have credibility. (3) Increasing trust with verified data, e-commerce transactions become safer and more transparent. This process may include using technology such as encryption, digital signatures, or blockchain-based identity verification. Several things need to be considered in the era of the digital economy, namely the issue of protecting the personal data of e-commerce consumers. In online activities, personal data is one of the essential things and is becoming increasingly important in all aspects of human life. Personal data is data relating to a person's characteristics, name, age, gender, education, occupation, address, and position in the family. In juridical, personal data according to the Government Regulation of the Republic of Indonesia Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions is certain personal data that is stored, maintained, and kept true and protected by confidentiality. Residents' personal data that must be protected includes the Family Card number, Population Identification Number, date/month/year of birth, information on physical and/or mental disability, NIK of biological mother, NIK of father, and several contents of important event records. It is very important to protect personal data related to residence such as the Population Identification Number, Identity Card and Family Card so that it is not easily exploited (Ayunda, 2022).

As for the validity aspect of data verification in Smart Contracts, if analyzed in terms of personal data protection, the verification process in Smart Contracts is essential to maintain user information's security and confidentiality. One of the steps taken is data encryption, where personal data used for verification is converted into an encrypted format so that only authorized parties with specific decryption keys can access it. This step prevents unauthorized parties from illegally accessing the site.

In addition, tokenization techniques are used, namely converting user personal data into anonymous digital tokens. This way, the original data is not immediately visible during the transaction, minimizing the risk of data misuse or theft. Furthermore, implementing decentralized storage based on blockchain technology ensures that

data is not stored on a single centralized server but distributed across various network nodes. This reduces the risk of data leakage due to cyber attacks targeting a single storage point. The combination of these steps creates a strong security layer to protect personal data during the verification process in Smart Contracts.

Data verification in Smart Contracts is crucial in ensuring the security and validity of transactions, particularly in e-commerce. However, this process does not necessarily guarantee complete protection of personal data. The success of data protection depends on several key factors.

Compliance with regulations, such as the Personal Data Protection Law (PDP Law), is one of the main requirements. E-commerce actors and Smart Contract developers must adhere to data protection principles, including transparency and security in data management. Additionally, the security of the technology used in the verification system is a significant challenge. If the system is vulnerable to cyber attacks, users' data remains at risk of exposure. User awareness is also essential, as many users consent without fully understanding how their data is used or protected.

The solution integrates Blockchain, Smart Contracts, and data markets to ensure fairness and independence. It is defined through high-level functional and non-functional requirements and services and an overall architecture diagram.

The "Recycling 4.0" research project is a practical application of data markets to enhance recycling processes. Its implementation includes blockchain, platform security, data integrity, data quality, transactions, and payments. Secure microservices for decentralized data markets are built on permissioned blockchain networks and Smart Contracts, enabling auditable, scalable, and decentralized data transactions.

This method separates the functionality and security of data marketplaces into multiple microservices, which are containerized on each device at low computing costs while ensuring flexibility and scalability. Trustless data trading systems based on blockchain minimize exposure to fraud and reduce the number of executed transactions, thereby lowering associated costs.[J. Meijers, G. Dharma Putra, G. Kotsialou, S. S. Kanhere, A. Veneris. (2021) Cost-Effective Blockchain-based IoT Data Marketplaces with a Credit Invariant. IEEE International Conference on Blockchain and Cryptocurrency, 1-9.]

2. The Relationship between the Validity of Smart Contracts and the Validity of Data Verification on Personal Data Protection

From a software engineering perspective, ensuring the correctness of a Smart Contract requires techniques that make the code immutable once deployed; it is final and cannot be updated. The only way to fix bugs in an already deployed Smart Contract is to release a new version while the old version remains permanently on the blockchain. This approach facilitates verification, validation, and testing (VV&T).

Verification ensures that "we developed the right product" (i.e., it meets specifications), and validation confirms that "we have developed the right product" (i.e., it fulfills its intended purpose). Testing aims to identify "the presence of errors in the product." This process verifies whether the detailed functional VV&T of business logic and processes operates as expected.

The blockchain system operates on a public network known as the leading network, which serves as the final product available for public use. For VV&T purposes, there is also a public test network, which allows anyone to access it through

their clients. The public test network enables the compilation and deployment of Smart Contracts. It facilitates frequently performed tasks such as running tests, automatically checking the code for compilation errors, and interacting with Smart Contracts in a public environment. In the legal sense the contractual will is connected with the concept of the private autonomy. It is obvious that already the internet has changed the frame conditions of the private autonomy for the natural person due to the anonymity of the contractual partners, the speed of the deciding process of the actors in internet contracting situations and the use of filtering technologies like searching machines (Koos, 2021).

2.1 Analysis of the Validity of Smart Contracts and Data Verification Process Based on Article 1320 of the Civil Code and the ITE Law

Bright Contract arrangements in civil law are becoming increasingly important with technological advancements, especially in digital transactions. Smart Contracts utilize blockchain technology to automate and enforce agreements by embedding rules into computer code. Therefore, it is crucial to understand how Smart Contracts function and their legal implications.

The parties agree to use Smart Contracts in digital transactions, which are then recorded in the blockchain system. Since contracts are maintained on the blockchain and can only be modified or canceled with the consent of both parties or when the specified terms and conditions are met, the agreements become more secure due to this verifiable input. Agreed provisions, such as payment, delivery, warranty or replacement, force majeure, and limitation of liability, are executed through a Smart Contract (Muhammad, 2019).

In its application, a Smart Contract has two models: the external model and the internal model. In the external model, the parties create conventional or textual agreements before being converted into cryptographic code. In other words, the contract initially exists physically like conventional contracts, using paper media. Thereafter, the code series supersedes any provisions related to the operation of the contract or the rights and responsibilities of the parties involved. In the external Smart Contract model, the role of the code is to implement the contract provisions that have been converted into code, where, when certain conditions are met, the Smart Contract will automatically execute the agreement.[ISDA.2017. "Whitepaper: Smart Contracts and Distributed Ledger – A Legal Perspective".New York: ISDA, , page 14]

The Civil Code uses the term "Agreement," while other laws and regulations, such as the ITE Law and PP PSTE, use the term "Contract" in "electronic contract" and equate it with "agreement." The equation of "agreement" with "contract" is also supported by Agus Yudha Hernoko, who argues that, in practice, the terms "agreement" and "contract" are used solely to facilitate the preparation and understanding of a series of sentences more clearly and precisely. If a contract is valid, it becomes binding on the parties. To determine whether a contract is valid, it must meet the conditions for validity as outlined in Article 1320 of the Civil Code, which states: "Four conditions need to be fulfilled, namely the agreement of those who bind themselves, the ability to make an agreement, a certain subject matter, and a cause that is not prohibited." Based on these four conditions, an analysis can be conducted for each point as follows:

a) Agreement for those who bind themselves

Agreement or consensus is one of the conditions for the validity of a contract. The agreement referred to in Article 1320 refers to the conformity of will between the parties, specifically the meeting of offer and acceptance. Agreements can be made verbally or in writing, with the purpose of a written agreement being to provide legal certainty for the parties and serve as perfect evidence.

b) Ability to create engagements

The legal competence of the parties is an element of contract validity that determines whether the contract entered into by the parties is legally binding. In this context, competence refers to the ability to perform legal acts, including entering into agreements. In Indonesian contract law, Article 1329 BW states that everyone has the right to perform legal actions except those declared incompetents by law. Based on this provision, parties using Smart Contracts must fulfil the requirement of uploading personal identification to the marketplace platform to demonstrate that they are legally competent as defined in Article 1330 BW.

c) A certain thing;

In Article 1333 of the Civil Code it is stated that

"An agreement must have as its principal an item of which at least the type has been determined, although the quantity of the item does not need to be specific as long as the amount can be determined or calculated later".

In general, the subject of an agreement can involves rights, services, goods, or any entity, whether it currently exists or not, as long as its type can be identified. For example, an agreement to sell a painting that has not been physically created remains valid. However, the agreement can be cancelled if the time limit specified in the contract expires and the contract has not been fulfilled.

In the context of a Smart Contract, a precise specification of the agreed-upon object is required. The subject of a Smart Contract can pertain to a specific digital asset or a digital representation of a physical asset recorded on the blockchain. These assets typically include crypto assets, Non-Fungible Tokens (NFTs), or other digital assets. In conventional contracts, parties often use ambiguous provisions to allow flexibility in interpretation according to their interests. However, this differs from Smart Contracts, as they do not permit using vague terms.

d) A cause that is not prohibited.

The condition for the validity of an agreement is also a lawful cause or lawful legal cause. As stated in Article 1335 jo, namely

"If the object of the agreement is illegal or contrary to morality or public order, the deal is void".

Apart from that, in 1337 of the Civil Code it is explained that

"A cause will be prohibited if it contradicts law, morality or public order".

Implementing Smart Contracts creates unique challenges because transactions carried out within them are not bound by national borders, considering the differences in legal systems between Indonesia and other countries. Therefore, it is essential for the parties to carefully review the contents of the agreement that will be included in the Smart Contract. This is because what is agreed upon by the parties may conflict with applicable legal regulations, moral values, or social order in the jurisdiction of one or both parties.

The validity of Smart Contracts, from the perspective of contract law as regulated in Article 1320 of the Civil Code (KUHPerdata), requires a comprehensive

analysis of the four conditions for the validity of an agreement: agreement of the parties, ability to agree, a particular subject matter, and a lawful cause. These four elements must be fulfilled for a Smart Contract to be considered valid and legally binding. First, the parties' agreement in a Smart Contract is realized through a digital approval mechanism, usually carried out by electronic signature or authentication via a Blockchain-based system. As long as the agreement is given voluntarily, without coercion, mistake, or fraud, then the elements of the agreement can be considered fulfilled. However, in a digital context, the main challenge is to ensure that the deal is genuinely provided by legally valid parties, considering the potential for identity manipulation or misuse of electronic data. Second, the ability of the parties to make agreements in a Smart Contract is also an essential element. The parties involved must have legal capacity, meaning they are legal adults (21 years old or married) and are not under guardianship. Implementing smart contracts requires digital identity verification to ensure the parties have the legal capacity to agree. This requires support from advanced authentication technology, such as digital identity verification, to meet proficiency requirements.

Third, the terms of a particular object in a Smart Contract refer to the clarity of the object of the agreement, whether in the form of goods, services, or specific rights. In the context of a Smart Contract, the object must be defined in detail in the program code used to execute the contract. Unclear or ambiguous object definitions can give rise to potential legal disputes in the future. Therefore, Smart Contract developers must ensure that every parameter and condition regulated in the contract has been designed clearly, transparently, and easily understood by the parties.

Fourth, lawful causes in a Smart Contract mean that the purpose and contents of the contract must not conflict with the law, morality, or public order. For example, Smart Contracts used for illegal activities such as money laundering, drug trafficking, or other criminal acts cannot be considered valid under Indonesian law. Therefore, the use of Smart Contracts must always comply with applicable laws and regulations to ensure that this technology is used for legitimate and beneficial purposes. Although Smart Contracts have great potential to increase efficiency and transparency in various transactions, legal challenges remain, especially in terms of agreement verification, the competence of the parties, and the clarity of the object of the agreement.

In addition, Smart Contracts based on Blockchain technology bring additional challenges related to data protection, network security, and the monitoring of automated transactions. Therefore, more specific and adaptive legal arrangements are needed to accommodate the unique characteristics of Smart Contracts. Furthermore, there should be an understanding of the general requirements for the validity of contracts. The legal requirements of a contract must be fulfilled by the agreement in order to offer certainty and binding to each party who agrees to it. Thus, it is considered valid legally and has legal force. However, the agreement can be terminated if the subjective requirements are not met, but, as long as the court has not terminated the agreement or taken that action, the agreement remains in effect (Iftinaity Shaumi Rahma et al., 2022).

In the Indonesian legal context, the legal recognition of Smart Contracts is still early, and existing regulations do not explicitly regulate this technology. Therefore, collaboration is needed between the government, academics, legal practitioners, and

technology developers to formulate a comprehensive legal framework supporting Blockchain technology development. In this way, Smart Contracts can be recognized as valid agreements, provide legal certainty for the parties, and encourage innovation and efficiency in various economic sectors.

There is a legal vacuum in Indonesia regarding legal protection for consumers in international e-commerce transactions, which often leads to problems related to contracts, consumer protection, taxes, jurisdiction, and digital signatures (Firdaus, 2020). The privacy policy on Smart Contracts in e-commerce transactions, particularly concerning legal protection for consumers across countries, is considered inadequate in addressing the legal issues that often arise in e-commerce. The basic requirements for smart legal contracts, specifically those that serve legal purposes, are discussed (Wilona et al., 2021).

2.2 Rights of Personal Data Subjects Regarding the Validity of Smart Contracts and Data Verification in the Use of Smart Contracts

As technology develops, the quality of human life improves by utilizing existing technology. The existence of increasingly sophisticated technology, combined with human creativity, can produce systems that allow humans to perform tasks without meeting directly (face to face). Smart Contracts are one of the products that emerged due to this combination, as previously explained. A Smart Contract itself is a product of the application of blockchain technology, which has undergone further development following the advent of cryptocurrency.

A Smart Contract is a computer program that essentially contains an electronic agreement within a blockchain database system, aiming to provide a protocol for executing an agreement or contract between parties, capable of automatically enforcing the agreement clauses. The concept of Smart Contract was born from the need to exchange goods and services with intermediaries in an easy, cheap, objective, real-time, and online manner. Additionally, it is supported by the cyber and technology ecosystem, which increasingly influences human life. Therefore, the Smart Contract is an evolution of the agreements and contracts used in electronic transactions, providing convenience for all parties involved. Over time, the use of Smart Contracts has expanded, particularly in the financial, property, and logistics sectors. Examples include peer-to-peer lending, automated payments, and even supply chain management. With the continued development of blockchain technology and further acceptance of Smart Contracts, the possibility of their application will continue to expand across various sectors, opening the door to innovations in electronic contracts and transactions.

The working concept of Smart Contracts relies heavily on blockchain principles. Blockchain is a decentralized ledger that records transactions permanently and securely. Smart Contracts are built on blockchain and use programming code to carry out specific tasks automatically. Blockchain technology is a ledger system, similar to a ledger in financial reporting, where every transaction that has ever occurred is recorded in the form of a decentralized database network. BlockchainBlockchain technology is currently widely applied in smart contracts as it enables contract transparency in Indonesia and worldwide. This contract transparency allows all parties involved to see changes that occur to the contract, the status of the contract, and all transaction history related to the contract. This can reduce the potential for fraud and disagreements in contracts.[Ibid.] Blockchain technology can increase the

effectiveness of Smart Contracts in business agreements between Indonesian companies through transparency, security, and automation. Blockchain transparency allows all parties to view and verify transactions in real time, reducing the potential for conflict or misunderstanding. From a security perspective, blockchain technology's decentralized structure and strong encryption minimise the risk of manipulation or fraud in business contracts and increase trust between companies. In terms of automation, applying blockchain technology to Smart Contracts enables the automatic implementation of contract requirements, such as payment or delivery of goods, reducing administrative costs and increasing operational efficiency. In the first stage, blockchain technology will carry out an Identify Agreement, a process of identifying the agreement that the parties involved want to make clearly and concisely so that both parties have the same understanding regarding the goals expected by making a contract. Then, in the second stage, the conditions will be set, determining the conditions carried out by the parties involved in the agreement. After selecting the conditions, the business logic of the agreement must be coded into the Smart Contract using a programming language. Furthermore, the Smart Contract is encrypted using cryptography to ensure security, and the Smart Contract cannot be changed without approval. This process is crucial because it ensures that the contents of the contract can only be viewed by the parties involved. Once a Smart Contract is available on the network, it can be executed automatically when the predetermined conditions are met. When the Smart Contract has been uploaded to the network, the network will be updated to include the new Smart Contract that the parties can access.

Smart Contracts in blockchain technology are a powerful tool for executing agreements automatically without intermediaries. With the stages previously explained, the parties interested in the contract can ensure that the security of their contract is guaranteed because every change that occurs in the contract will be recorded in the blockchain, making it usable as authentic evidence in the dispute resolution process, as regulated in Law Number 30 of 1999 concerning Arbitration and Alternative Dispute Resolution. In this context, some legal principles and theories support the use of this technology in improving the dispute resolution process, such as the principle of legal certainty, the theory of justice, and the theory of protecting the rights of the parties involved. Legal certainty is essential in ensuring the clarity of the rules governing contracts. The application of blockchain technology in Smart Contracts leads to the decentralization of data and provides certainty of data integrity, which creates a strong basis for the verification process. The theory of justice in the application of blockchain technology focuses on using programmed codes and rules, which can guarantee fair and accurate contract execution because it reduces the involvement of human subjectivity in fulfilling contract terms. Moreover, the application of blockchain technology in Smart Contracts can protect the rights of the parties involved because contract execution will occur automatically once the conditions stipulated in the contract are fulfilled, thereby ensuring that the system indirectly guarantees the rights and obligations of the parties.

Regarding this transformation, blockchain technology can serve as a solution to support data integration in e-procurement and integrate all data with high security in the context of the transition toward an e-procurement system. Blockchain technology is a decentralized ledger used to manage all data between parties in the

network, which is not controlled by one central authority, recording and storing all data between users chronologically (Amalia et al., 2023).

Based on the opinions and definitions of Smart Contracts above, it can be understood that Smart Contracts are unique in that they are self-executing or can execute the provisions contained in them automatically. Apart from that, because the form of this agreement is in the form of programming code distributed via blockchain, the following inherent characteristic is that the clause cannot be changed (immutable).[Sabrina Oktaviani, (2021) Implementasi Smart Contract Pada Teknologi blockchain dalam Kaitannya dengan Notaris dan Pejabat Umum, Jurnal Kertha Semaya, Vol.9, No.11, hlm. 2210-2211.]

Data in e-commerce has specific characteristics that make it essential to protect, especially in terms of use and processing based on agreements. First, e-commerce data is often private and includes sensitive information, such as names, addresses, telephone numbers, payment information, and customer transaction data. This information may result in privacy violations, fraud, or identity theft if misused. Second, e-commerce data is also commercial because it includes purchasing patterns, consumer preferences, and market analysis that are of high value to companies. This data is often a strategic asset that must be protected from theft or unauthorized use by competitors.

Additionally, e-commerce data is dynamic, meaning it is continuously updated over time with transaction volume, which increases the risk of cyberattack exposure if not appropriately managed. Therefore, protecting this data requires clear agreements, such as Terms of Service or Privacy Policies, regulating how data is collected, stored, stored, and shared. These contracts must comply with data protection regulations, such as the GDPR in Europe or the Personal Data Protection Law in Indonesia, to protect customer rights. Due to these characteristics, using agreements in e-commerce data management is crucial for maintaining customer trust, ensuring legal compliance, and protecting companies from potential legal and reputational risks. The right to privacy through data protection is not only important but also a key element for individual freedom and dignity. Data protection is a powerful driver for realization of political, spiritual, religius, and even sexual freedom.the right to self determination, freedom of expression and privacy are important rights to make us human beings. According to Stephens-Daviddowitz, personal data is the same thing as the human body. It means the data is the same thing as part of the body that cannot be touched and owned without permission (Priskarini et al., 2019).

Using Smart Contracts as payment transaction instruments in e-commerce, several data characteristics need to be understood and carefully considered to ensure smooth, secure, and reliable transactions. First, e-commerce data must have high integrity, meaning that recorded information, such as product details, prices, and user identities, must not be changed or manipulated after a transaction has been initiated. Second, data authenticity needs to be maintained, mainly to prevent fraud or fake transactions, so data validation through blockchain mechanisms is crucial. Third, the volume of data in e-commerce tends to be large, covering millions of transactions simultaneously. Therefore, Smart Contracts must be designed to handle large-scale transactions efficiently without sacrificing processing speed. Fourth, the diversity of data formats, such as text, numbers, and metadata, demands high interoperability in Smart Contracts to ensure that all information can be appropriately processed. Fifth,

the privacy and security of customer data, such as credit card information and shipping addresses, must be guaranteed with strong encryption mechanisms to meet personal data protection standards. In addition, data transparency is an essential element, where all parties involved in a transaction can access the transaction history in real time via the blockchain system without compromising the confidentiality of sensitive data. Furthermore, Smart Contracts must also be able to detect and handle anomalies, such as errors in payment calculations or order disputes, through intelligent validation algorithms. Lastly, compliance with local and international regulations, such as GDPR or the Personal Data Protection Law in Indonesia, must be considered to ensure that transaction operations run according to legal provisions. By considering all these characteristics, Smart Contracts can be implemented effectively to create a safe, efficient, and trustworthy e-commerce payment system.

Based on the explanation above, the smart contract in e-commerce aims to provide legal certainty for the implementation of the buying and selling business to be more flexible and efficient, but it has the potential to cause legal problems related to the privacy policy of implementing smart contracts in crossborder e-commerce. In this case, the researcher wants to examine how the legal certainty of the privacy policy of smart contract in e-commerce transactions in Indonesia and the form of legal protection for consumers against the use of smart contracts in crossborder e-commerce transactions based on the perspective of national and international laws. The privacy policy of smart contract in e- commerce transactions emerges because there is no legal certainty in Indonesia. The parties making the contract comply with and respect the agreement stipulated in the Civil Code for both parties or it is called the Principle of Pacta Sunt Servanda (Wilona et al., 2021). Smart Contracts in Indonesia have not been expressly regulated but are instead governed by general contract laws as outlined in the Civil Code. Smart Contracts exist because technological developments have advanced rapidly, prompting the Indonesian government to create legal regulations, namely Law Number 11 of 2008, which was later amended to become Law Number 19 of 2016 concerning Information and Electronic Transactions (Herianto Sinaga & Wiryawan, 2020).he discussion section should not merely restate the findings reported in the result section or report additional findings that have not been discussed earlier in the article. The focus should instead be on highlighting the broader implications of the study's findings and relating these back to previous research. Make sure that the conclusions you reach follow logically from and are substantiated by the evidence presented in your study (Varadarajan 1996: 5).

CONCLUSION

The development of digital technology has encouraged innovation in electronic transactions, one of which is the use of smart contracts as agreement instruments that automate contract execution based on code programming in the Blockchain system. In the context of Indonesian law, the validity of smart contracts must be analyzed based on the provisions in Article 1320 of the Civil Code (KUHPerdata) regarding the legal conditions for agreements and aspects of data verification in Smart Contracts. According to Article 1320 of the Civil Code, an agreement is considered valid if it meets four main requirements: agreement between the parties, the ability to agree, a particular object as the subject of the agreement,

and a lawful cause. Additionally, the validity of data verification in using smart contracts is crucial to ensure the validity and security of transactions in e-commerce. In this context, data verification involves automatically processing information to ensure that transactions are carried out by the terms programmed in the smart contract. In Indonesian legislation, data verification is related to the Information and Electronic Transactions Law (UU ITE) and the Personal Data Protection Law (UU PDP). Smart contracts that use a Blockchain-based data verification system can be considered valid if they meet the principles of security, integrity, and transparency in managing personal information. The validity of a Smart Contract refers to the conditions for the validity of the agreement in Article 1320 of the Civil Code, as explained above, which includes the agreement of the parties, legal capacity, certain things, and lawful causes. A Smart Contract can be considered valid if it meets these four conditions, where the agreement is reflected through digital consent provided by the parties, and the object and purpose of the contract are clearly explained in the programming code. The legal competence of the parties remains a prerequisite so that only parties who fulfil the legal requirements can enter into a contract. However, Smart Contracts' validity raises challenges regarding data verification, which is a key element in ensuring the automatic execution of contracts as agreed upon. Data verification in a Smart Contract aims to (1) Ensure the authenticity of the data used to prevent the use of false data or manipulation of information that could harm one of the parties in the transaction, (2) Reduce the risk of fraud, which through verification ensures that the parties involved are legitimate entities and have credibility, and (3) Increase trust, meaning that with verified data, e-commerce transactions become safer and more transparent. This process may include using technologies such as encryption, digital signatures, or blockchain-based identity verification. As for the validity aspect of data verification in Smart Contracts, when analyzed in terms of personal data protection, the verification process in Smart Contracts is essential in maintaining user information's security and confidentiality. One of the steps taken is data encryption, where personal data used for verification is converted into an encrypted format so that only authorized parties with the appropriate decryption keys can access it. This step prevents unauthorized access by parties without permission.

Acknowledgment

With sincere gratitude, I would like to express my deepest appreciation to all those who have supported and contributed to the completion of this research. First and foremost, I extend my heartfelt thanks to my academic advisors, Dr. Reka Dewantara, S.H., M.H., and Dr. Yenny Widyanti, S.H., M.Hum., for their invaluable guidance, continuous encouragement, and insightful feedback throughout the research process. Their expertise and mentorship have played a crucial role in shaping this study. Lastly, I thank all individuals and parties who have contributed in any way to this research, either through direct assistance, thoughtful discussions, or moral support. Thank you.

Reference

Abidin, M. I. (2023). Legal Review of the Validity of the Use of Smart Contracts in Business Transactions in Indonesia and Its Regulation in Various Countries. *Unnes Law Journal*, *9*(2), 289–310. https://doi.org/10.15294/ulj.v9i2.74957

Adhijoso, B. D. (2019). Legalitas Penerapan Smart Contract Dalam Asuransi Pertanian di Indonesia. *Jurist-Diction*, *2*(2), 395. https://doi.org/10.20473/jd.v2i2.14224

Amalia, R., Amirul Alfan, M., Aliefia, M., Radzi, M. S. N. B. M., & Kurniawan, F. (2023). Digitalization of the Public Procurement System in Indonesia: Challenges and Problems. *Yuridika*, *38*(3), 1–20. https://doi.org/10.20473/ydk.v38i3.51874

Ayunda, R. (2022). Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties? *Law Reform: Jurnal Pembaharuan Hukum*, *18*(2), 144–163. https://doi.org/10.14710/lr.v18i2.43307

Azis, D. E. P., & Nurhaedah, N. (2018). Juridical Review The Implementation of Oral Agreement is associated with the Law of Treaties and Law Number 8 Year 1999 concerning Consumer Protection. *Substantive Justice International Journal of Law*, *1*(1), 56. https://doi.org/10.33096/substantivejustice.v1i1.13

Carona, N., & Shebubakar, A. N. (2023). Legal Status and Implications of Smart Contracts in Indonesia. *Jurnal Pendidikan Tambusai*, *7*, Hlm.6939. https://mail.jptam.org/index.php/jptam/article/download/7314/6052

Chang, S. (2018). Legal Status of Virtual Currency in Indonesia in the Absence of Specific Regulations. *Indonesia Law Review*, *8*(3). https://doi.org/10.15742/ilrev.v8n3.485

Herianto Sinaga, D., & Wiryawan, I. W. (2020). Keabsahan Kontrak Elektronik (E-Contract) Dalam Perjanjian Bisnis. *Kertha Semaya : Journal Ilmu Hukum*, *8*(9), 1385. https://doi.org/10.24843/ks.2020.v08.i09.p09

Iftinaity Shaumi Rahma, Hasiana, E. J., Cantika, S. L., & Octaviona, T. (2022). Indonesian Legal Protection for Consumers on the Validity of Electronic Contracts in the E-Commerce Transactions. *Yuridika*, *37*(3), 697–714. https://doi.org/10.20473/ydk.v37i3.36976

Kirana, N. P. D. C., Westra, I. K., & Indrawati, A. S. (2019). Penyelesaian Sengketa Konsumen Dalam Transaksi Jual Beli Melalui Media Sosial Instagram*. *Kertha Semaya: Journal Ilmu Hukum*, *7*(1), 1–13.

Koos, S. (2021). Artifical Intelligence as Disruption Factor in the Civil Law: Impact of the use of Artifical Intelligence in Liability, Contracting, Competition Law and Consumer Protection with Particular Reference to the German and Indonesian Legal Situation. *Yuridika*, *36*(1), 235. https://doi.org/10.20473/ydk.v36i1.24033

Korintus Wilson Horas Hutapea, & Adi Sulistiyono. (2024). Keabsahan Smart Contract Dengan Teknologi Blockchain Menurut Kitab Undang-Undang Hukum Perdata. *Aliansi: Jurnal Hukum, Pendidikan Dan Sosial Humaniora*, *1*(3), 86–94. https://doi.org/10.62383/aliansi.v1i3.177

Kusumawardani, D., & Kariodimedjo, D. W. (2021). *The Challenges of The Implementation of Smart Contracts Related to Consumer Protection in Electronic Transactions*. *20*(2), 276–291.

Meijers, J., Dharma Putra, G., Kotsialou, G., Kanhere, S. S., & Veneris, A. (2021). Cost-effective blockchain-based IoT data marketplaces with a credit invariant.

IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2021. https://doi.org/10.1109/ICBC51069.2021.9461127

Muhammad, D. (2019). *Jurist-Diction*. *2*(5), 1655–1674.

Multazam, M. T., Phahlevi, R. R., & Purnomo, M. I. (2023). *Securing Blockchain Enterprises : Legal Due Diligence Amidst Rising Cyber Threats*. 26–52.

Priskarini, I. A., Pranoto, & Tejomurti, K. (2019). The Role of The Financial Services Authority in The Legal Protection of Privacy Rights in Connection with Personal Data of Fintech Lending Debtor in Indonesia. *Padjadjaran Jurnal Ilmu Hukum*, *6*(3), 556–575. https://doi.org/10.22304/pjih.v6n3.a7

Tejomurti, K., Hadi, H., Imanullah, M. N., & Indriyani, R. (2019). Legal Protection for Urban Online-Transportation-Users' Personal Data Disclosure in the Age of Digital Technology. *PADJADJARAN Jurnal Ilmu Hukum (Journal of Law)*, *5*(3), 485–505. https://doi.org/10.22304/pjih.v5n3.a5

Tulsidas, T. U. (2018). Faculty of Law Degree in Law Final Degree Work Smart Contracts From a Legal Perspective. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10801 LNCS*, 739–767. https://doi.org/10.1007/978-3-319-89884-1_26

Wilona, M. Z., Latifah, E., & Purwadi, H. (2021). Privacy Policy on Smart Contracts in E-Commerce Transactions. *Law Reform: Jurnal Pembaharuan Hukum*, *17*(1), 47–60. https://doi.org/10.14710/lr.v17i1.37552