Scientific Research Publishing

Journal of Information Security, 2019, 10, 25-44
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

The Hazards of Misusing the Smart Contract: An AHP Approach to Its Risk

Romulo Luciano

Department of Post-Graduation and Research in Administration, IBMEC, Rio de Janeiro, Brazil
Email: romulo.benites@gmail.com

How to cite this paper: Luciano, R. (2019) The Hazards of Misusing the Smart Contract: An AHP Approach to Its Risk. *Journal of Information Security*, **10**, 25-44.
https://doi.org/10.4236/jis.2019.101002

Received: December 14, 2018
Accepted: January 20, 2019
Published: January 23, 2019

Abstract

This article explores four critical groups of systematic risk embedded in smart contract employment using the analytic hierarchy process (AHP). The four principal risk analysis groups include: 1) transparency in the light of corporate governance 2) IT security 3) contract management automation and 4) legality. The AHP assists both decision-makers and stakeholders alike in the evaluation process essential for identifying potential technological constraints posed within a permissioned blockchain environment using peer-to-peer format in the absence of digital currency. Based upon critical assessment, the AHP methodology enables pairwise comparisons among different features and consequently increases the knowledge regarding these attributes in light of the software's risk assessment.

Keywords

AHP, Blockchain, Smart Contract, Software Project Management

1. Introduction

The smart contract has received attention due to both its characteristics and numerous application possibilities, offering users potential cost savings in a variety of conventional commercial aspects. The most advantageous benefits include reducing legal and transactional costs as well as increasing the intangible trust value among dispersed entities. While the technology is developed on the blockchain platform and computer codes have been intensely investigated by technologists worldwide, methodical risks are manifest due the characteristics of the smart contract. The ensuing body of research provides specific information regarding the hazards of misusing the smart contract from an analytic hierarchy process (AHP) risk assessment perspective. The following is comprised of five sections concerned with the identification and exploration of four distinct areas

of risk confronting private smart contract utilization using basic AHP methodology. The objective of this body of research is to provide decision makers with a comparison model in order to assess the identified risks associated with the smart contract. The author will begin with a review of emerging and associated literature in conjunction with exploratory research to provide an understanding of the interrelationship between the smart contract and blockchain, and more importantly, how that relationship impacts risk management in a software project. The second section of this paper will provide a definition of risk and its management within a software project as well as the methodology used to identify the four main risk clusters pertaining to the smart contract. The third section will introduce the AHP method including the elemental framework comprising the AHP followed by an application of the AHP with regards to the four critical groups of systematic risk. Conclusively, the final section will provide a summation and discussion of the author's findings.

2. The Literature on Smart Contract and Software Risk Management

2.1. The Smart Contract

In 1994, Nicholas Szabo became the first author to mention the term smart contract [1]. The smart contract was developed to translate conventional paper-based contracts into secure self-executing digital protocols. Later, in 2008, Bitcoin, was developed using blockchain by Satoshi Nakamoto and became the first digital currency. Its technical characteristics were determined, defined, and subsequently deployed in the public market with reliability. As a result, the bitcoin became synonymous with cryptocurrency; offering users anonymity, transactional transparency, and tamper-proof peer-to-peer operations utilizing hash functions and an inherent value maintained on an open network without a central issuer or bank [2]. This system is not infallible. Adding a new block or transaction in the proof-of-work blockchain to improve the trustworthiness of the system requires caution.

As one of the originating authors of Ethereum, [3] explains the complex interrelationship among bitcoin, blockchain, and smart contract components, as an open platform based upon blockchain technology, enabling software developers to create a computer code that replaces traditional paper-based contracts. The computer code written for the blockchain is immutable and handles the consensus agreement among parties. This code is called a smart contract which is a self-executing code that meets the consensus terms and conditions customarily established in current contracts. It enforces the rules and automates contract management. These terms and conditions may include the payment process between parties, transference of rights and/or goods among participants, or a decentralized autonomous application objecting to eliminate intermediary services such as regulatory compliance and systematic voting. All these transactions are enforced and permissible if predefined conditions written as program code are

satisfied. The smart contract can be programmed and deployed on the private blockchain. Currently, there are consortia of private organizations investigating and generating program codes for smart contracts as well as other blockchain applications such as Hyperledger and R3 entrepreneurial ventures in addition to the numerous technology companies that create customized smart contracts.

The permissioned private blockchain and smart contracts have characteristics and risks distinct from the public network blockchain which does not require permission. The main difference delineating a public blockchain is the trusted participants that are allowed on the network [4]. The permissioned private blockchain demands an invitation that requires authorization by either the network administrator or by a set of rules embedded in the system. Additionally, it specifies restrictions regarding who can join the network, and which transactions they may take part in. The access control mechanism can vary. For example, existing members may select future participants, issue licenses for participation via regulatory authority, or even make the decisions as a preexisting group instead. Once an organization has joined the network, it may play a role in maintaining the blockchain in a decentralized manner. Conversely, having a person, group of persons, or a set of rules acting as network administrator on a permissioned private blockchain and smart contract, naturally make it vulnerable for cyberattacks [4].

In essence, the smart contract is a potentially disruptive innovative tool requiring a thorough understanding of both the benefits and potential harm implementation may render a business.

If smart contract employment is decided, identifying pertinent risks and monitoring their development and/or existence, becomes a matter of constant vigilance due to the clear research gap related to smart contract technology.

The foundation of this study concerns the organizations aspiring for consensus and collaboration in both the exploration and application of a private smart contract. The impetus of this study is a permissioned private blockchain network in conjunction with a smart contract developed for private trade in a peer-to-peer manner free from the use of a digital currency. The purpose for this is to attain a distributed reproduction of auditable transaction logs that are shared among the participants of interest. For clarity, the smart contract examined in this study takes into consideration that organizations and government that are involved in this process are ruled by the same set of applicable laws as shown in **Figure 1**.

2.2. Software Risk Management

Risk exists in all matters, and it is not different in business. Among several definitions of risk, [5] defines risk "as the chance of loss or the perils to the subject matter of an insurance contract." Applying the same definition to information technology, [6] wrote about software risk management, proposing a framework that began with the planning phase and extended to the operational function.

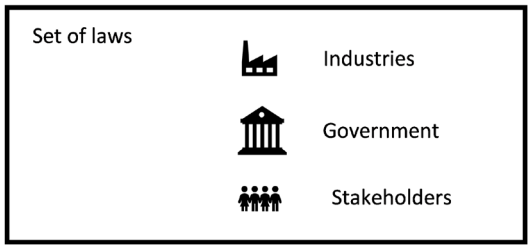

Figure 1. Business environment framework proposed by the author.

Reference [6] objected to prevent software risks in order to safeguard against costly operations and limit frustration to users and other stakeholders. Reference [6] split the risk management into two groups: risk assessment and risk control. The risk assessment is subdivided into three groups as well as the risk control. The risk assessment subgroups are: 1) risk identification, 2) risk analysis, and 3) risk prioritization. The risk control subgroups are: 1) risk management planning, 2) risk resolution, and 3) risk monitoring. Taken together, it is a complete set of checks that a planning team should focus on to minimize risk prior to implementing new software. Another framework developed by [7] for the National Institute of Standards and Technology highlights the importance of information technology risk management. It is a guideline which comprises three processes: risk assessment, risk mitigation, and evaluation assessment. It contains [6]'s framework as a subset.

Corroborating, [8] went further than [6], mentioning that risk management of new software should assess functionality, performance, resource use, safety, reliability, versatility, ease of learning, ease of use, and ease of modification.

Controversial but elucidating, the Chaos Report (1994) issued by [9], showed a high failure of IT application development projects and costliness. The survey interviewed 365 respondents among different industry sizes. Although the methodology applied in the studies and survey was considered debatable, as [10] mentioned, it made the academy and entrepreneurs aware of such bad practices and possibly served to propose improvements in practice and theory afterward. One of the findings in the [9] was the incomplete requirements and specifications for such software development and applicability, which also follows the [8] study.

Additionally, [11] mentioned in his study that most aspects of failure in software projects are foreseeable and preventable. Among the most common factors of IT projects failures, two are noteworthy in this study: unmanaged risks and use of immature technology. The smart contract is an immature technology at the time this study was prepared, and this study attempts to identify the main group of risks.

Furthermore, [12] also wrote about risk management in software projects. He mentioned that one of the most common subjects in software projects found in the literature regarding risk management is risk identification, which might impact on the success of the plan.

In addition, [13] made a comparison among the authors who published studies regarding risk management in software projects. The study was based on the steps described by the Project Management Body of Knowledge (PMBoK) Guide from 2008. One step common to all authors is risk identification, as observed in this literature review.

Enriching the literature, [14] approached the general risk assessment in distributed software development. The aspects identified in the software risk management literature discussed by the authors were grouped as according to the Leavitt organizational model, *i.e.*, task, structure, actors, and technology, which differs from the proposal of this research study. However, it is valuable to highlight the aspects which can be extended to smart contract software. They are the lack of trust in human skills and behavior, lack of security, complexity of code, and software quality.

Thus far, an attempt has been made to clarify that risk identification constitutes a precursor to software risk management. Hence, this study intends to help the decision-maker to fulfill part of the risk management process by identifying the main group of private smart contract risks and evaluating them utilizing the AHP method with the help of expert judgment.

2.3. Risks and Attributes of a Private Smart Contract

As aforementioned, the private smart contracts deployed on the permissioned private blockchain are distinguished by their characteristics and risks when compared to the permissionless blockchain and public network. One of the attributes of the private blockchain and the smart contract is to have a network administrator, either a person, a group of persons or a set of rules, which makes it the target for cyberattacks [4].

Another important feature of the smart contract is the immutability of code [15]. Thus, it does not allow any part from singly changing the code or terms written. It prevents harmful cyberattacks to the code because the network administrator would be alerted about the possible invasion trying to change the code. As an additional attribute, the transactions are traceable and permanently recorded in the blockchain [1].

Reference [16] performed a screening of academic papers and identified four main issues regarding the public smart contract. They are codifying issues, security issues, privacy issues, and performance issues. In addition, the study proposes solutions for each issue. These issues can be extended to the permissioned private smart contract with a fewer minor differences. Codifying issues can be summarized as the difficulty to write or modify the smart contract, which is intrinsically related to the human skills that are necessary to translate the terms and conditions of a regular paper-based contract to programming code. The security issue is the vulnerability of the code as such. If it has breaches, then cyberattacks can invade the network or suspend the network operability. The privacy issue is not relevant to the focus of this study because the transparency is akin to the permissioned private blockchain and smart contract, in contrast to the pub-

lic environment. The unplanned display of data to the public concerns IT security.

The smart contract is encrypted before being deployed on the private blockchain. The performance issues mentioned by [16] are not pertinent since the private smart contract object of this study is unique, and it would run in the private blockchain, *i.e.*, one smart contract to be deployed and run. Reference [16] mentioned performance issues when several smart contracts are deployed and are run on the public blockchain, which might affect the execution time of each transaction, as well as the reference by [1] of the throughput limits in the Ethereum blockchain environment.

Regarding the security of the blockchain system and a smart contract written on Ethereum, [17] performed a systematic inspection regarding its security, which was also addressed by [18]. They explore the literature about blockchain and smart contracts, highlighting the vulnerability observed after the cyberattacks on smart contracts developed using the Ethereum platform. In addition, they propose solutions to minimize the success probability of an attack.

The controversial misuse of the hard fork operation is less appropriate to the private smart contract object of this study [19]. The hard fork became a well-known operation, when in 2016, $60 million was hacked through the public Ethereum blockchain due to a vulnerability in the decentralized autonomous organization deployed on the Ethereum blockchain [20]. Using the soft fork and then a hard fork, it was possible to identify where the crypto money was and recover the stolen digital currency to its rightful owners. However, that created two blockchains: 1) with the fork, Ethereum, and 2) without the fork, Ethereum classic. At that time, it created reputational issues on blockchain usage regarding the security issues and consequently, the risk of financial loss. However, if a similar operation is required in a private consortium, the decision is made through a consensus of the stakeholders [19].

Reference [4] points out the technological challenges in smart contracts without differentiating the permissioned private and the public smart contract. The lack of maturity issue highlighted in the study as well as cybersecurity and governance are common issues to private and public blockchains and smart contracts. Additionally, the legal and regulatory challenges mentioned are different from the public to the private environment since on the private network, the framework of the code would be created in consensus with all stakeholders involved in the program code process, including the government. For instance, the UK Government Office for Science [21] clearly recommends the facilitation of research and use of blockchain and smart contracts and highlights the potential benefits and possible synergies between government and private organizations such as increasing transparency and corporate governance and avoiding frauds in the system. However, it also indicates concerns regarding the infancy of a smart contract. The laws chosen for application to a contract are dependent on several factors, but that discussion goes beyond the objective of this study.

Regarding the contract that should be translated to code, if a contract does not encompass all rules and conditions, it might lead to transaction costs, conflict, or even worse, the ruin of the program if a consensus is not established [1] [22]. Drawing attention to the program code's immutability is important. Despite the code's immutability, another program code can replace the program code without significant interference to the process where the software has been deployed and run, or the code can be altered from what it was programmed for [1] [3].

Regarding the legal perspective, [23] analyzed the legal validity, interpretation, and lifecycle of contracts in either imperative or declarative smart contracts. Imperative language is most commonly used in smart contracts, which "the programmer writes an explicit sequence of steps to be executed to produce the intended result. The programmer has to write what has to be done and how to perform it" [23]. On the other hand, the authors present the alternative declarative language, arguing that it is a more feasible representation of natural language which "the programmer does not have to write explicitly the sequence of steps to specify what has to be done. The programmer only describes what has to be done, without specifying how to do it" [23]. Regardless of the language used, what is essential for this study is to identify the main risks. In addition, the main risks are related to the lack of consensus when writing the code, inadequate verification and testing of smart contracts prior to deploy them in the blockchain, the complexity of writing the smart contract code, the immutability of the code, and the termination of the smart contract.

As mentioned by [22], the smart contracts can be tailored to have flexibility, *i.e.*, have a human factor to judge a specific transaction before its execution, thus classifying the smart contract as semi automated. Reference [3] discussed the use of oracles to overcome problems such as disputes or making the oracle represent the jurors to determine whether certain contractual terms have been met prior to code execution. Thus, the oracle can provide flexibility, but it can compromise the speed of the transaction. As explained by [24], every person or organization can take the liberty to infringe on any contractual conditions. They might be legally responsible for that act, but the oracle can be implemented to minimize the impact of such possibilities and reduce the time to resolve a conflict. Using the previously established framework of existing law and terms, the oracle can settle disputes among parties. To corroborate, [25] cited the risks between common law and civil jurisdiction and the smart contracts, along with other risks such as security, in light of cyber attack risks and scalability. Therefore, it is important to emphasize the framework proposed for this study as per **Figure 1**, where all participants are enclosed under the same set of law and rules. In addition, the object of this study is the private smart contract deployed on the permissioned private blockchain network, without using a digital currency and where the stakeholders are aiming for a consensus agreement.

2.4. Research Gap

The research work calls for conducting the process of risk identification and

analysis on smart contracts deployed on the permissioned private blockchain network for private trade. The topic of assessing the smart contract risks in the literature is still not recognized from this basis [16]; hence, it is considered as a gap in smart contract matters. Furthermore, grouping the main smart contracts' attributes based on their meaning, *i.e.*, to facilitate the risk identification and subsequently, to perform a smart contract attributes' risk analysis, is prudent in software project management [12], and it can be considered a gap in the emergent literature of private smart contracts.

In this context, therefore, a two-phase methodology has been proposed and utilized to meet the gaps mentioned above. The first phase is to group the most common smart contracts' attributes based on their meaning after a review of smart contracts in the literature and resources. The second phase is the analysis of identified risks with expert judgment, with the intention of ranking them for determining their relative areas of concern under uncertain conditions by using the AHP approach.

2.5. Methodology

This research work was performed between December 2017 and March 2018 utilizing the same systematic mapping study used in current research topics regarding smart contracts described by [16], which was previously successfully used by [26] for mapping studies in software engineering, as shown in **Figure 2**.

The search exercise was carried out with queries in ProQuest, Google Scholar, Elsevier, ScienceDirect, and Emerald Insight databases, focusing on quality papers published in conferences, journals, and workshops. The keywords used in the search were blockchain and smart contract, separated and in combination, using the connectors and/or, without excluding the books. Moreover, the search included the words: risk assessment, AHP, software risk management, and project management on the same databases. Additionally, based on the exclusion criteria performed by [16], the author excluded pieces of literature without having the full text available, articles, newsletters, and gray literature.

There is a lack of research on the subject that is associated with risk assessment; therefore, this study is classified as exploratory research [27].

To answer the research questions of which risks are intrinsic to private smart contracts and if they can be grouped, the data collection of smart contract characteristics was carried out based on the emergent literature review and interviews with specialists. The attempt was to group the repeated patterns identified

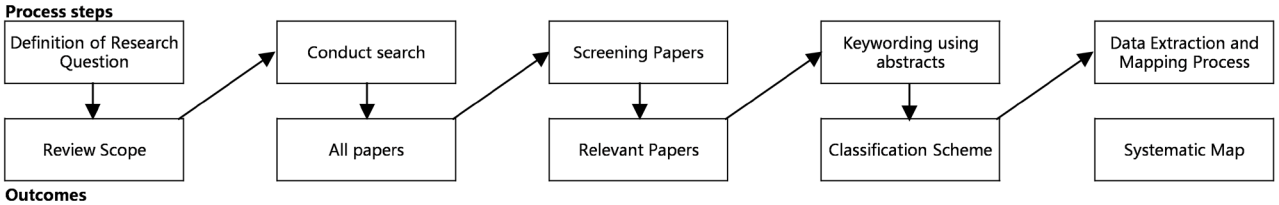

Figure 2. Steps of systematic mapping study by [26].

in the literature and to group them in a significant set. Later, confirmation of the relevance of the proposed four groups by the experts of that phenomenon was conducted during an interview. Thus, an effort was made to avoid the researcher's bias and to confirm the concepts, based on the grounded theory research procedure as described by [28] and corroborated by [29]. The caution taken when grouping the attributes into four significant clusters is a tentative approach to building the information concerning the private smart contracts' risks and to providing a plausible understanding. Nevertheless, a criticism may concern the extent, which cannot be considered exhaustive; however, this research study does not intend to be complete but rather serve as an initial approach to this subject.

The solution methodology applied in this research study is displayed in **Figure 3**.

As seen from the preceding chapters, the literature presents characteristics of the smart contract. To recapitulate and to structure them, the characteristics are organized in **Table 1**.

The software risk management and the features identified in **Table 1** are not part of this study as such, but these characteristics are mentioned in the smart contract literature review and serve as premises to evaluate any software. The literature also highlights the importance of these characteristics when performing a risk identification of specific features that can impact one or more groups of risks.

A decision-making approach should have a consensus-building approach, and it should be natural to our intuition and general thinking. For simplification purposes, grouping the risk characteristics of smart contracts mentioned in **Table 1** is suggested, narrowing them down to the four main sets, as shown in **Table 2**, with their respective meaning and source.

As observed, there are pieces of evidence that indicate that attributes of the smart contract can be set up in four main clusters in order to concentrate the software risk analysis. Consequently, the use of AHP was selected to provide a methodology for pairwise comparison of the aspects identified, which can guide the adoption of decisions. The AHP has been used in different fields such as decision-making in construction management [30], health-safety and environmental risk assessment of refineries [31], safety risk assessment [32], project risk assessment [33] as well as other applications [34].

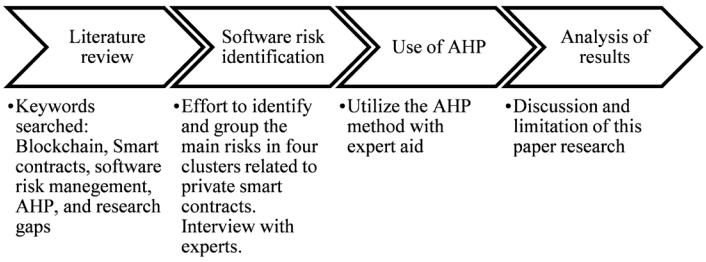

Figure 3. The flowchart of the research.

Table 1. Smart contract's feature within respective categories, summarized risk description, and source.

Smart contract features	Risk description	Source
1. Transparency		
1.1. Transactions are traceable and permanently recorded	In light of corporate governance, it is a risk if the transactions are not traceable.	[1], [15], [17]
1.2. Privacy	Accidental human interference or hacking information is an exposure risk and might have liabilities consequences.	[15] [21] [24]
1.3. Lack of consensus or collaboration	If consensus or collaboration is only partially achieved, then it might cause conflicts during the smart contract lifetime.	[1] [14]
2. IT security		
2.1. Network administrator	Having a network administrator in the private environment becomes a focus of hacking attacks.	[3] [4]
2.2. Immutability of code	Blockchain protocol can be changed through a hard fork, but in the private environment, it only happens through common consensus of the stakeholders	[3] [15] [19]
2.3. Vulnerability of code	Is the risk perception of how easy it is to invade the code and to modify it.	[16] [17] [18] [20]
3. Automation		
3.1. Performance issues	Regarding the speed of transactions in private smart contracts and the requirement to perform the number of transactions. Additionally, the risk of downtime due to performance issues. In addition, the desirable system automation level which can be: 1) fully automated, 2) semiautomated and 3) slightly automated.	[1] [16]
4. Legality		
4.1. Codifying smart contract	Complexity to translate the contract's paper-based terms and conditions to programming code.	[14] [16] [23]
4.2. Framework of code in consensus	If the set of laws and rules are not common to all stakeholders, then there is a clear risk of compliance and can imply legal consequences.	[1] [23] [24]
4.3. Jurisdiction conflicts	If the smart contract does not encompass all required laws and rules, it might have conflicts with governments.	[3] [23] [24] [25] [39]
4.4. Immutability of the code	The immutability and consequently the automated transaction might not follow the civil jurisdiction where the business is established.	[15] [22] [23]
4.5. Termination of smart contract	The risk is the lack of proper evaluation of this possibility.	[23] [24]
5. Software risk management		
5.1. Inadequate smart contract verification	Regarding testing before deployment which can impact or influence one group, partial groups or all groups cited above.	[6] [7] [8]
5.2. Lack of maturity	Intrinsic to actual smart contract infancy.	[4] [11] [21]
5.3. Human skills	Inherent in the programmer's ability to write, codify, and identify risks and its potential consequences. Innumerable threats can be associated with it.	[14]
5.4. Software quality	Risk that is intrinsic to the selected programming code such as the differences among Solidity in Ethereum, NEO and LISK. In conjunction with the human skills related to developing the smart contract on such programming codes.	[11] [13] [14]

Table 2. Defining private smart contract's risks with their meaning and with sources.

Group of smart contract risks	Meaning/Description	Source
Transparency in the context of corporate governance	To be understood as a digital public ledger of time-stamped transactions that is available for every participant in the blockchain network. All transactions are recorded in the blockchain and any transaction can be visited by the eligible user on the network and can verify the validity of any transaction. Therefore, all transactions are visible, accessible and auditable to everyone who is entitled to perform it. The risk is if the code is not translated to be visible or auditable to stakeholders, which might imply a lack of trust in the entire system	[16] [40] [41]
IT Security	A cryptographically secured transaction is possible due to cryptography science and allows the protection of sensitive information either in storage or communication. The use of the hash function allows a digital fingerprint on the block created in the blockchain. The hash function is also time-stamped, which provides additional security design. One block or transaction cannot be erased, copied, replaced or changed once it is registered in the blockchain. The risk is the cyberattacks or hackers trying to destroy, manipulate, disrupt or change the private blockchain environment and its smart contract. That might happen with the temporary suspension or even shutdown of the system in case of a cyberattack. It can incur financial losses, cause a lack of confidence in the system and identity disclosure	[2] [3] [15] [17] [42] [43]
Automation	The smart contract is the translation of the traditional contract to a programming language. Thus, the terms and conditions are machine-readable, enforcing agreed upon rules previously established and agreed in consensus among all the involved parties without the requirement of any hierarchical power structure, *i.e.*, self-executing smart contracts if conditions are satisfied. It will imply an instantaneous settlement, effectively eliminating counterparty risk. Consequently, the process can be classified as automated. However, the parties can determine the extent of the automation process. It was proposed to have three levels: 1) fully automated, 2) semiautomated and 3) little automated.	[1] [3] [44]
Legality	It refers to the legal perspective. The agreed terms and conditions translated to a machine-readable form are possible due to a specific programming language such as Ethereum, avoiding human misinterpretation of contract terms which might lead to a dispute between parties. The smart contract shall encompass all legal agreements made in consensus among the parties. Additionally, it shall respect the applicable laws and regulations regarding the government, society, and organization where the digital contract will be established. There will be a risk if the initial legal framework translated to a machine programming language does not comprehend all necessary rules which would impact the overall system validity. The expected outcomes must be extensively discussed and approved by everyone who is impacted by them.	[22] [23] [24] [39]

3. The Analytical Hierarchy Process—AHP

AHP Method

The AHP developed by [35] is an effective multicriteria decision analysis methodology. By reducing complex decisions to a series of pairwise comparisons and then arranging the results, the AHP helps to capture both objective and subjective aspects to provide support to decision-makers. The AHP involves a relative judgment when making the pairwise comparison, and thus, the result has a relative form depending on the expert judgment and the business environment. It hierarchizes the elements in a primary way so that elements at the same level are of a similar order of scale and must be capable of being correlated to some or all elements at the next higher level. A typical hierarchy has a top level that reflects the overall objective of the decision problem. At the intermediate level, it shows the elements affecting the top-level objective. Similarly, at the lowest level, it encompasses the decision choices. This type of hierarchy provides a clear and simple diagram of all the aspects affecting the decision and their relations. At that point, the prioritization procedure commences, determining the relative importance of the element in each level of the hierarchy. Elements in each level are pairwise compared to their importance in making the decision under consideration. The AHP starts creating a pairwise comparison square matrix A of order $n \times n$ whose elements represent the relative importance of an element i over an element j. These elements that denominate a_{ij} are represented by the ratio w_i / w_j, where $(w_1, w_2, \cdots, w_n)$ are the positive numerical entries which reflect the judgments. The elements a_{ij} of the matrix A_{ij} shall have the following condition according to Equation (1):

$a_{ij} = 1/a_{ji}$ is the generic element of the reciprocal positive matrix A_{ij} (1)Additionally, the matrix A_{ij} shall follow the condition (2) to be considered consistent.

$$a_{ij} = a_{ik} / a_{jk}, \text{ where } a_{ij} > 0 \text{ and } i, j, k = 1, \cdots, n \tag{2}$$

The judgment scale of numbers used in AHP is from 1 to 9 [35], and it helps the decision-maker to verbally express in a natural and intuitive way the intensity of the importance between every two elements as: equally important, moderately important, strongly important, very strongly important or extremely important, as well as allowing transition between these expression words.

Having the comparison matrix, it is possible to obtain a priority vector of a set of alternatives, such that n is the number of elements to be compared, $\lambda_{\max}$ is the priority vector of matrix A, and w is the vector of priorities, where $\lambda_{\max} = n$ and $a_{ij} = w_i / w_j$ if the choices made by the decision-maker are consistent. This being so, the vector must be found to satisfy Equation (2), and by Equation (3), the priority vector is obtained.

After forming the comparison matrices, the process moves to the phase of deriving relative weights for the various elements. The relative weights of the elements of each level with respect to an element in the adjacent upper level are

computed as the components of the normalized eigenvector associated with the largest eigenvalue of their comparison matrix. The composite weights of the decision alternatives are then determined by aggregating the weights through the hierarchy. This is accomplished by following a path from the top of the hierarchy to each alternative at the lowest level and multiplying the weights along each segment of the path. The outcome of this aggregation is a normalized vector of the overall weights of the options. The mathematical basis for determining the weights has been established.

The rank reversal phenomenon is debatable. The criticism has been extensively discussed by many authors such as [36] and [37] but a solution for this limitation is not exhausted yet. The rank reversal phenomenon's criticisms are based on the AHP method's addition of a new irrelevant alternative and subsequent remaking of the model, and the ranking of the alternatives differs from the first classification so that the best-classified alternatives are lowered.

4. Application of the AHP

To evaluate the importance of the characteristics, a first approach to the specialists in information technology (IT) in different organization in Brazil was initiated, but the level of replies and feedback of those questionnaires was insufficient and not completed, which was most likely because of a misunderstanding regarding how to use Saaty's nine-point scale. On the other hand, one company replied and opened a communication channel with the researcher. Consequently, a second effort was made to interview the IT specialists. The company is present in Brazil, and it is an operator in the oil and gas industry. It has a global presence, with its headquarters in Europe. The IT specialists' profile is shown in **Table 3**.

With respect to the qualitative approach on the AHP methodology, during the interview, questions to the interviewees were asked such as: In the context of software risk assessment, how much more important is security compared to transparency?

To construct the decision model and to solve the matrix, Super Decision software was used. This is professional software that can be freely accessed, and it is easy to use for constructing the pairwise comparison and solving the matrix as well as to acquire the consistency ratio. The consistency ratio is a measure of consistency that confirms that the original rates given by the interviewees have been maintained [35]. It is recommended that the consistency ratio remain less than or equal to 0.10. The pairwise comparison matrix was conducted with the interviewees, and the result is shown in **Table 4**.

Based on **Table 4**, it might say that the assigned judgment is realistic consistent because the consistency ratio is 0.06 and it is less than 0.1 [35]. Also, it shows that the IT security feature is the most critical risk following by legality. Subsequently, the transparency in light of corporate governance is more important than automation in the context of smart contract' software risk analysis.

Table 3. IT specialist profile.

	IT specialist 1	IT specialist 2
Years of experience in IT	14	18
Current job position	Project manager	Head of IT department
Working on a future project about blockchain or smart contracts application	Yes	Yes
Working on digitalization or automation	Yes	Yes

Table 4. Pairwise comparison of the smart contract's characteristics.

	Transparency	IT security	Automation	Legality	Weight factor
Transparency	1	1/7	3	1/5	0.095
IT security	7	1	7	2	0.531
Automation	1/3	1/7	1	1/5	0.054
Legality	5	1/2	5	1	0.319
Consistency ratio: 0.06					

After the AHP result, the interviewees did not expose surprise to the result and confirmed their previous expectation mentioned during the interview. Additionally, both experts mentioned the importance of the weight factor because it helps them to decide how internal resources can be allocated focusing on the higher risk. Also, they mentioned the AHP method simplifies communication with internal and external stakeholders.

During the interview, one of the experts highlighted the importance of risk identification of private smart contracts. According to the expert, the private smart contract enables data sharing among participants. However, when information from different sources are gathered and shared, the conjunction of information might trigger a new business insight. That new insight might start a new competitive business or a new business model. If that happens, it brings advantage to those who discovered first.

Additional point cited by both experts was the possibility to include the risk analysis of business intelligence, analytics, and data sharing into overall blockchain utilization. They said that big data is a source of valuable information if correctly used. The risk of utilization of big data available in any blockchain is unknown. Hacking that volume of data is considered a risk on private business. The outcome is unpredictable.

During the interview, the experts mentioned that smart contracts could be used to automate post-trade transactions, replacing the bureaucracy and the paperwork. None of the interviewees could mention further details of this application.

5. Conclusions

Innovative technologies applied to processes often present both potential bene-

fits and risks [38]. Additionally, the organization should be aware of the competition and the expected reward if implementing the proposed software. The smart contract can reshape the business process, but its associated risks should be better understood. Consequently, if the program code is developed in conjunction with other trusted stakeholders and clients, it might provide a competitive advantage for business interests as well as transparency of the whole process, trustworthiness, shared knowledge, shared risks, and consensus.

This research study tackles the primary goal of software risk management, which is risk identification, and second, it confronts the risk factors with the aid of an expert by utilizing the AHP method. It seemed to have served a useful purpose and disclosed the possibility of using a similar methodology for other software risk assessments while helping the decision-maker perform better judgment in a systematic form.

The outcome of the experts' input and the application of AHP show the IT security as the most critical topic following by legality. The experts mentioned the usage of big data in blockchain environment is considered an unknown risk. The smart contract is on early implementation stage, as mentioned during the interview. Another point highlighted during the interview was the proper business segment selection to implement the smart contract. Following the selection of the business segment, it is discussed which part of the business the smart contract could be applied and tested before a full escalation of this IT software. It is the premature usage of blockchain and smart contracts in the business as well as the risk identification of the software. Also, during the interview was possible to identify that the company might take baby steps implementing the smart contract until a full understanding of how the IT software works and how it runs in a permissioned blockchain environment.

Regarding legality, the experts show similar preoccupation if the terms and conditions of the formal and regular paper contract are not translated correctly to program code because it can ruin the business and expose participants to any government agency, then possible penalties. Therefore, it is imperative to reach the consensus among players when writing the smart contract and attain attention to the national laws wherever the business might occur. Also, they mentioned the difficulties when writing the smart contract because it involves different technical areas on the first time such as IT programmers, lawyers, and different stakeholders.

Following the AHP method and result as per **Table 4**, once the IT security and legality reach the consensus among participants, it is considered a natural development of the transparency in light of corporate governance. The transparency of the business and the workflow inside the smart contract is shareable with all stakeholders involved in the permissioned blockchain environment without using digital currency. The participants might have a different type of access to the smart contract, but the process itself can be auditable by any selected participant at any time.

The last risk is the level of automation that smart contract can offer. The experts believe that the automation of the regular paper contract and its terms and conditions are achievable once there is a consensus among parties when writing the computer code. The execution of the computer codes can be defined among the parties. The automation can have three levels: 1) fully automated, 2) semiautomated, and 3) little automated. Having a fully automated smart contract means zero participation of any external resource and the rules are executed as per computer code.

On the other hand, the semiautomated system means that an external resource might be used. The external resource can be a person, a group of persons or another computer code. They can be used to check a few points in the process. After checking those points and having agreement among participants, it is authorized the execution of the computer code in the smart contract.

The little automation level is possible, but it is not desirable, as per interviewees. They said that it would be a regression if the participants choose little automation because it would involve several stops in the process and several checks before any computer code execution. Choosing little automation level would be a paradox after having achieved a good IT security level, legality as well as transparency in the process. Also, the choice of little automation level implies more risk because human errors might occur, and might be a time-consuming task. The smart contract should be designed to reduce the human interpretation of the codes or rules, and its full automation might be appreciated as a benefit to the business.

The proposed methodology in this research study suggests that the literature review was relevant to group of the four main risks based on their meaning as well as the application of the AHP method to compare the risks. It seems to be a feasible technique for identifying the software risks in organizations.

Limitations of This Study and Opportunity for Future Work

A thorough search of the relevant literature yielded no related articles attempting to provide a risk identification of a private smart contract application. One of the limitations is that the study could have been performed with more interviewees to enhance the risk assessment and evaluation. The perception threshold of different experts can vary from business to business, from environment to environment, and from culture to culture. Nonetheless, this study is exploratory and unique regarding the risk perception of private smart contract attributes insofar as this research study does not intend to be complete but rather a provide a primary approach. On the other hand, the proposed convenience sample can be extended to include subcategories for each main group of risks. In addition, other multicriteria decision analysis methods can be selected and applied, and thus, the results can be compared and examined.

Another limitation regards the risk of the human work needed to write the code. Hence, it requires human skills and ability to choose which programming language to code and to fulfill application demands. The point is that there is a

risk of faults while programming the code which might lead to a combination, to some extent, of the risks mentioned in this paper. This particular risk was not assessed as a sole risk of the private smart contract, the object of this study, but it should be evaluated by the decision-maker as an essential factor when deciding on the utilization of the smart contract. Perhaps, utilizing another methodology, such as the PMBoK, will identify other risks as well. Furthermore, each stage in the software development lifecycle should be adequately risk-assessed in favor of identifying risks and problems early on and reacting to them effectively.

An additional constraint might be the protocol used for grouping the risks. First, in the literature review, there are many websites, blogs, white papers, free video-hosting websites and general information about blockchains and smart contracts available on the Internet. Although they are not considered as scientific studies, and they were not considered in this research, it is evident that there are technical discussions around the same topic, involving entrepreneurs and software developers, among others, who are enthusiastic contributors on the same subject. Furthermore, there might be risks not realized by the interviewees or the author, and it can be criticized that proposing the four main groups mentioned in this study is cursory. However, as described by [28] if there are enough indications in the study itself, *i.e.*, the methodology applied for the literature review to identify the risks, then the presented theoretical construction can be evaluated in terms of degrees of plausibility. Thus, this study can be assumed to have achieved its purpose of defining the four main groups based on the literature review and to have performed their qualitative pairwise comparison, enhancing an understanding of the smart contract attributes.

The specificities of private smart contract implementation and usage were not part of this study, as well as the infrastructure of the IT part, but they are recommended areas of research. A valuable extension that would complement the preceding ideas and generally help with the understanding of risk is a case study related to smart contract implementation and an understanding of how the software risks were evaluated.

Acknowledgements

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Swan, M. (2015) Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc., Sebastopol, California.

[2] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[3] Buterin, V. (2014) A Next Generation Smart Contract & Decentralized Application Platform. https://www.ethereum.org/

[4] Natarajan, H., Krause, S. and Gradstein, H. (2017) Distributed Ledger Technology and Blockchain. World Bank Group. https://doi.org/10.1596/29053

[5] Risk. (n.d.). https://www.merriam-webster.com/dictionary/risk?utm_campaign=sd&utm_medium=serp&utm_source=jsonld

[6] Boehm, B.W. (1991) Software Risk Management: Principles and Practices. *IEEE Software*, **8**, 32-41. https://doi.org/10.1109/52.62930

[7] Stoneburner, G., Goguen, A.Y. and Feringa, A. (2002) Sp 800-30. Risk Management Guide for Information Technology Systems.

[8] Fairley, R. (1994) Risk Management for Software Projects. *IEEE Software*, **11**, 57-67. https://doi.org/10.1109/52.281716

[9] Standish Group International. The Chaos Report. https://www.standishgroup.com/sample_research_files/chaos_report_1994.pdf

[10] Eveleens, J. and Verhoef, C. (2010) The Rise and Fall of the Chaos Report Figures. *IEEE Software*, **27**, 30-36. https://doi.org/10.1109/MS.2009.154

[11] Charette, R.N. (2005) Why Software Fails. *IEEE Spectrum*, **42**, 42-49. https://doi.org/10.1109/MSPEC.2005.1502528

[12] Bannerman, P.L. (2008) Risk and Risk Management in Software Projects: A Reassessment. *Journal of Systems and Software*, **81**, 2118-2133. https://doi.org/10.1016/j.jss.2008.03.059

[13] Neves, S.M., da Silva, C.E.S., Salomon, V.A.P., da Silva, A.F. and Sotomonte, B.E.P. (2014) Risk Management in Software Projects through Knowledge Management Techniques: Cases in Brazilian Incubated Technology-Based Firms. *International Journal of Project Management*, **32**, 125-138. https://doi.org/10.1016/j.ijproman.2013.02.007

[14] Aslam, A., Ahmad, N., Saba, T., Almazyad, A.S., Rehman, A., Anjum, A. and Khan, A. (2017) Decision Support System for Risk Assessment and Management Strategies in Distributed Software Development. *IEEE Access*, **5**, 20349-20373. https://doi.org/10.1109/ACCESS.2017.2757605

[15] Christidis, K. and Devetsikiotis, M. (2016) Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, **4**, 2292-2303. https://doi.org/10.1109/ACCESS.2016.2566339

[16] Alharby, M. and Van Moorsel, A. (2017) A Systematic Mapping Study on Current Research Topics in Smart Contracts. *International Journal of Computer Science and Information Technology*, **9**, 151-164. https://doi.org/10.5121/ijcsit.2017.9511

[17] Li, X., Jiang, P., Chen, T., Luo, X. and Wen, Q. (2017) A Survey on the Security of Blockchain Systems. *Future Generation Computer Systems*. (In Press) https://doi.org/10.1016/j.future.2017.08.020

[18] Atzei, N., Bartoletti, M. and Cimoli, T. (2017) A Survey of Attacks on Ethereum Smart Contracts (Sok). *International Conference on Principles of Security and Trust*, Uppsala, 24-25 April 2017, 164-186. https://doi.org/10.1007/978-3-662-54455-6_8

[19] Mendling, J., Weber, I., Aalst, W.V.D., Brocke, J.V., Cabanillas, C., Daniel, F. and Zhu, L. (2018) Blockchains for Business Process Management-Challenges and Opportunities. *ACM Transactions on Management Information Systems*, **9**, Article No. 4. https://doi.org/10.1145/3183367

[20] Luu, L., Chu, D.H., Olickel, H., Saxena, P. and Hobor, A. (2016) Making Smart Contracts Smarter. *Proceedings of the* 2016 *ACM SIGSAC Conference on Computer and Communications Security*, Vienna, 24-28 October 2016, 254-269. https://doi.org/10.1145/2976749.2978309

[21] Walport, M. (2016) Distributed Ledger Technology: Beyond Blockchain. UK Government Office for Science.

[22] Wright, A. and De Filippi, P. (2015) Decentralized Blockchain Technology and the Rise of Lex Cryptographia.

[23] Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G. and Xu, X. (2018) On Legal Contracts, Imperative and Declarative Smart Contracts, and Blockchain Systems. *Artificial Intelligence and Law*, **26**, 377-409. https://doi.org/10.1007/s10506-018-9223-3

[24] De Filippi, P. and Wright, A. (2018) Blockchain and the Law: The Rule of Code. Harvard University Press, Harvard.

[25] Giancaspro, M. (2017) Is a "Smart Contract" Really a Smart Idea? Insights from a Legal Perspective. *Computer Law & Security Review*, **33**, 825-835. https://doi.org/10.1016/j.clsr.2017.05.007

[26] Petersen, K., Feldt, R., Mujtaba, S. and Mattsson, M. (2008) Systematic Mapping Studies in Software Engineering. In EASE, Vol. 8, 68-77.

[27] Creswell, J.W. (2002) Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. Sage Publications, London.

[28] Corbin, J.M. and Strauss, A. (1990) Grounded Theory Research: Procedures, Canons, and Evaluative Criteria. *Qualitative Sociology*, **13**, 3-21. https://doi.org/10.1007/BF00988593

[29] Charmaz, K. (1996) The Search for Meanings-Grounded Theory. In: Smith, J.A., Harre, R. and Van Langenhove, L., Eds., *Rethinking Methods in Psychology*, Sage Publications, London, 27-49.

[30] Erdogan, S.A., Šaparauskas, J. and Turskis, Z. (2017) Decision Making in Construction Management: AHP and Expert Choice Approach. *Procedia Engineering*, **172**, 270-276. https://doi.org/10.1016/j.proeng.2017.02.111

[31] Rezaian, S. and Jozi, S.A. (2012) Health-Safety and Environmental Risk Assessment of Refineries Using of Multi-Criteria Decision-Making Method. *APCBEE Procedia*, **3**, 235-238. https://doi.org/10.1016/j.apcbee.2012.06.075

[32] Aminbakhsh, S., Gunduz, M. and Sonmez, R. (2013) Safety Risk Assessment Using Analytic Hierarchy Process (AHP) during Planning and Budgeting of Construction Projects. *Journal of Safety Research*, **46**, 99-105. https://doi.org/10.1016/j.jsr.2013.05.003

[33] Zayed, T., Amer, M. and Pan, J. (2008) Assessing Risk and Uncertainty Inherent in Chinese Highway Projects Using AHP. *International Journal of Project Management*, **26**, 408-419. https://doi.org/10.1016/j.ijproman.2007.05.012

[34] Mardani, A., Jusoh, A., Nor, K.M.D., Khalifah, Z., Zakwan, N. and Valipour, A. (2015) Multiple Criteria Decision-Making Techniques and Their Applications—A Review of the Literature from 2000 to 2014. *Economic Research-Ekonomska Istraživanja*, **28**, 516-571. https://doi.org/10.1080/1331677X.2015.1075139

[35] Saaty, T.L. (1980) The Analytic Hierarchy Process. McGraw-Hill, New York.

[36] Dyer, J.S. (1990) Remarks on the Analytic Hierarchy Process. *Management Science*, **36**, 249-258. https://doi.org/10.1287/mnsc.36.3.249

[37] Belton, V. and Gear, T. (1983) On a Short-Coming of Saaty's Method of Analytic

Hierarchies. *Omega*, **11**, 228-230. https://doi.org/10.1016/0305-0483(83)90047-6

[38] Davenport, T.H. (1993) Process Innovation: Reengineering Work through Information Technology. Harvard Business Press, Harvard.

[39] Raskin, M. (2016) The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, **304**, 305-341.

[40] Ølnes, S., Ubacht, J. and Janssen, M. (2017) Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing. *Government Information Quarterly*, **34**, 355-364. https://doi.org/10.1016/j.giq.2017.09.007

[41] Yermack, D. (2017) Corporate Governance and Blockchains. *Review of Finance*, **21**, 7-31. https://doi.org/10.1093/rof/rfw074

[42] Kosba, A., Miller, A., Shi, E., Wen, Z. and Papamanthou, C. (2016) Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. 2016 *IEEE Symposium on Security and Privacy*, San Jose, 22-26 May 2016, 839-858. https://doi.org/10.1109/SP.2016.55

[43] Wood, G. (2014) Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper. https://ethereum.github.io/yellowpaper/paper.pdf

[44] De Kruijff, J. and Weigand, H. (2017) Ontologies for Commitment-Based Smart Contracts. *OTM Confederated International Conferences on the Move to Meaningful Internet System*, Rhodes, 23-28 October 2017, 383-398. https://doi.org/10.1007/978-3-319-69459-7_26