CIÊNCIA DA INFORMAÇÃO

Industrial Secret Transfer via Smart Contracts: Addressing Arrow's Information Paradox

Felipe Octaviano Delgado Busnello
Master of Intellectual Property Law, Università Degli Studi di Torino (UNITO) and World Intellectual Property Organization (WIPO) Academy, Turin, Piedmont, Italy.
Master's Student in Intellectual Property, Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul, Porto Alegre, RS, Brazil.
http://lattes.cnpq.br/2902342207984367
felipe@busnello.com.br

Erik Schüler
PhD in Electrical Engineerin, Universidade Federal do Rio Grande do Sul (UFRGS), Porto Alegre, RS, Brazil.
Professor EBTT, Instituto Federal do Rio Grande do Sul (IFRS), Veranópolis, RS, Brazil.
http://lattes.cnpq.br/1046844040379714
erik.schuler@ifrs.edu.br

Anderson Ricardo Yanzer Cabral
PhD in Computer Science, Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS), Porto Alegre, RS, Brazil.
Professor EBTT, Instituto Federal do Rio Grande do Sul (IFRS), Viamão, RS, Brazil.
http://lattes.cnpq.br/0148615078864622
anderson.yanzer@ifrs.edu.br

Submitted on: 06/29/2022. Approved on: 04/30/2024. Published on: dd/mm/yyyy.

ABSTRACT

In the current state of the art, systems exist for the transfer of intangible assets protected by Intellectual Property, consolidated through legal monopolies, either by attributive systems (such as patents and industrial designs) or automatically protected (such as copyrights and related rights). Some of these systems, or their respective methods, are described in scientific literature. Among these, some methods use blockchain technology, and a smaller subset (entirely contained within the former) also uses smart contract technology, though these are independent tools. Although industrial secrets also constitute monopolies, the computerized or cryptographic solutions applied to other types of assets protected by different forms of intellectual property cannot be applied to these assets due to their sui generis nature, lacking a monopoly that exists independently of their non-disclosure. The need to maintain secrecy arises from Arrow's Information Paradox, a phenomenon in which revealing the secret implies its transfer. This phenomenon hinders the potential transfer of industrial secrets and makes it impossible to adopt existing systems applicable to other types of intangible assets. The

research employed a mixed methodology. This paper presents a method for transferring industrial secrets using smart contracts instantiated on blockchain to solve two of the three elements of the Paradox, specifically reliability and capacity, assuming the third, relevance.

Keywords: industrial secret; Arrow's Information Paradox; smart contract; blockchain; technology transfer; patents; technological information.

INTRODUCTION

Unlike attributive monopoly systems for assets protected by other forms of intellectual property (e.g., patents), the use of knowledge as an asset is not governed by public policy (Leppälä, 2013; Burstein, 2013). No mechanisms with *erga omnes* efficacy[1] guarantee a monopoly over knowledge. These exclusivities are therefore protected solely by *de facto* monopolies (rather than legal monopolies), relying on secrecy and the legal frameworks that support it. In essence, preserving knowledge hinges on the holder's ability to maintain confidentiality. Once disclosed (or independently discovered), its use is generally unprotected.

Industrial secrets represent a crucial aspect of intellectual property. As Barbosa (2010, p. 635)[2], observes, "[...] o contrato de know-how tem muito mais importância econômica do que a licença de patentes", underscoring the significance of knowledge transfer in commercial contexts. This is further underscored by the protection afforded to traditional knowledge within intellectual property regimes. The economic activity surrounding the production of applicable knowledge (Benkler, 2006) and its commercialization fuels innovation and economic growth (Burstein, 2013). Consequently, technology transfer, as a means of knowledge commercialization, is intrinsically linked to industrial development. This link is particularly evident in the comparatively greater economic impact of transferring applicable knowledge within industrial sectors. For this reason, this paper focuses specifically on these types of secrets.

Knowledge transfer, particularly involving industrial secrets, is fundamentally shaped by Arrow's Information Paradox, identified by economist Kenneth Arrow (Arrow, 1962). This paradox describes the dilemma faced by those acquiring secret knowledge: its value remains unknown until revealed, yet upon disclosure, its value diminishes as it has been transferred without cost. As Arrow (1962, p. 615)[3] states, "[...] existe um paradoxo fundamental na determinação da demanda por informação; seu valor para o adquirente não é conhecido até que ele saiba da informação, mas neste momento ele efetivamente a adquire sem custo [...]". To facilitate such transactions, legal and technical mechanisms are typically employed to address this paradox.

From a legal standpoint, externalities arise from legal norms such as intellectual property rights granted by states and inter partes agreements (Dyrhovden, 2019; Leppälä, 2013; Burstein, 2013). These include state-guaranteed monopolies or other exclusive rights (in Brazil, notably those under Law 9,279) and contracts containing confidentiality or exclusivity clauses (Burstein, 2013). These legal tools are widely employed in Intellectual Property and Technology Transfer contexts.

1 *Erga omnes* ("against all") denotes general applicability, whereas *inter partes* ("between parties") indicates applicability restricted to specific parties, usually those directly involved in a legal transaction.

2 Translation: "[...] the know-how contract is of much greater economic importance than the patent license" (Barbosa, 2010, p. 635, editorial translation).

3 Translation: "there is a fundamental paradox in determining the demand for information; its value to the purchaser is not known until they have the information, but at that point, they have effectively acquired it without cost" (Arrow, 1962, p. 615, editorial translation).

Addressing Arrow's Information Paradox in industrial secret transfers often involves technical strategies like staged disclosures with corresponding payments. However, mitigating the paradox's effects generally requires economic analyses to determine negotiation equilibrium points concerning disclosures (Anton & Yao, 2002) and the application of situation-specific economic models (Leppälä, 2013). As Burstein (2013, p. 280)[4] notes: "[...] "[...] as condições sob as quais um mecanismo ou outro para superação do paradoxo da revelação seja o mais adequado tendem a variar significativamente com base nas circunstâncias específicas da troca da informação" [...]". This variability necessitates the development and implementation of tailored models for each situation.

In other contexts, such as cryptography and computational applications, problems akin to Arrow's Paradox (where proof of knowledge is required without revealing the underlying information) can be addressed through Zero-Knowledge Proofs. These cryptographic techniques allow one party to prove to another that they possess specific knowledge without disclosing any details that would reveal it (Wang *et al*., 2021). Such proofs typically involve demonstrations by the knowledge holder, often involving problem-solving tasks that require mastery of the concealed information. These acts serve as compelling evidence to the uninformed party, confirming the existence and possession of the secret knowledge. Essentially, this type of proof involves "a protocol between two or more parties, that is, a series of steps that two or more parties must follow to complete a task" (Wang et al., 2021), where the demonstration effectively proves the capability of the party holding the secret.

Within the computational realm, and relevant to the present work, is the technology of smart contracts, developed in the mid-1990s (Szabo, 1997). These "contractual codes" can be incorporated into, executed by, and monitored through computerized systems (Clark, 2018). From an information technology perspective, Kõlvart *et al*. (2016, p. 133)[5] define them as "[...] protocolos de transação computadorizados que implementam as disposições do contrato [...]". Essentially, they represent a digital implementation of legal transactions. As envisioned by their original proponent, smart contracts can be used for the "negotiation, acceptance, operation, and adjudication" of contracts (Szabo, 1997).

In parallel with and complementing smart contracts, blockchain technology enables two parties to transact directly, replacing the need for trust in a third party with cryptographic proofs (Nakamoto, 2008). It functions as a protocol for "creating a reliable and transparent record," where information is added and validated by the participants themselves (Clark, 2018).

The potential – and even the necessity – of developing technological products based on these technologies for specific applications in Technology Transfer has already been recognized as viable. The literature highlights that "para uma aplicação em transferência automática de tecnologias, novas pesquisas utilizarão da temática para desenvolver novas plataformas distribuídas de ativos com base em blockchains e smart contracts" (Basso *et*

4 Original: "[...] the conditions under which one or another mechanism for overcoming the disclosure paradox is optimal are likely to vary significantly with the specific circumstances of the information Exchange" (Burstein, 2013, p. 280).

5 Original: "[...] is a computerised transaction protocol that implements the terms of the contract" (Kõlvart *et al*., 2016, p. 133).

al., 2019)[6]. This undersocres a research problem that directly addresses the use of emerging technologies (specifically, smart contracts and blockchain) to resolve issues (specifically, Arrow's Paradox) inherent in knowledge transfer (specifically, industrial secrets).

Building upon the concepts previously presented (industrial secret transfer, Arrow's Paradox, zero-knowledge proofs, smart contracts, and blockchain), this study proposes a method for partially resolving Arrow's Information Paradox to facilitate the transfer of knowledge and technologies protected as industrial secrets. This method employs zero-knowledge proofs, executed through a smart contract on a blockchain, to control the information presented as proof and automatically execute reciprocal obligations, ensuring simultaneous delivery of the knowledge and payment to the contracting parties. It is important to acknowledge that the Paradox operates continuously, even before research and development begins, creating a context of disincentives (Benkler, 2006) and potentially hindering deal completion due to the uncertainty it generates (Leppälä, 2013). This paper aims to develop a tool applicable to the secret transfer process itself. The supplier provides the secret (without revealing its content), presents proof of possession to the acquirer, and upon satisfaction, the acquirer receives the secret, triggering automatic payment. This approach, as demonstrated herein, minimizes or resolves various aspects of Arrow's Paradox. Earlier stages (such as technology valuation) and later stages (such as enforcing contractual clauses) fall outside the scope of the solution proposed here.

METHODOLOGY

This study employed a mixed-methods approach, incorporating both numerical analysis and conceptual understanding. Due to the limited availability of scientific literature on this specific topic, the research is primarily exploratory. aiming to gain a deeper understanding of the problem, clarify its nuances, and generate hypotheses for future investigation (Gil, 2008). The project methodology comprised the following steps:

a) A comprehensive review of scholarly and gray literature to assess the state of the art concerning technologies and methods used for negotiating and transferring industrial secrets; and

b) The development and presentation of a proposed method.

For the bibliographic review, searches in specialized databases using the keywords "trade secrets" and "smart contracts" yielded fewer than a dozen results, even when varying the search terms and languages, including Portuguese, Italian, French, and Spanish. However, a significant amount of gray literature related to these topics was freely available on the Internet.

To identify existing technologies and methods for addressing the Paradox, a comprehensive review of scientific databases and gray literature was conducted. The scientific literature confirmed the theoretical foundation for the Paradox's occurrence and

6 Translation: "for applications in the automatic transfer of technologies, new research will explore this subject to develop new distributed asset platforms based on blockchains and smart contracts" (Basso *et al*., 2019, editorial translation).

its relevance to contemporary information economies (see Benkler, 1999, 2006), while also highlighting the absence of a practical method that fully resolves it (see Leppälä, 2013), despite the existence of general strategies and techniques (see Anton & Yao, 2002). Notably, the review revealed no established method for transferring technology protected by industrial secrets using computerized or cryptographic solutions (Santos, 2003; Basso *et al*., 2019), nor any documented application of emerging technologies like blockchain for similar purposes (Conoscenti et al., 2016). This gap persists despite the demand for knowledge protected as industrial secrets (Leppälä, 2013) and the recognized negative impacts of Arrow's Information Paradox on such negotiations, despite "[...] importância para inovação e crescimento econômico" (Burstein, 2013, p. 230)[7]. These impacts include the suppression of demand. The apparent absence of a similar method, coupled with its potential applicability, provided the impetus for developing the method proposed in this work.

The proposed method for industrial secret transfer was developed using a flowchart that outlines the steps involved in the transfer process. This flowchart[8], created with Draw Io[9], underwent several revisions before a final algorithm was established. This algorithm addresses both the capacity and reliability requirements, making the method accessible to individuals at any stage of the transfer process.

THEORETICAL FRAMEWORK

This theoretical framework is divided into four subsections, each addressing a key concept underpinning this work: industrial secrets, Arrow's Information Paradox, zero-knowledge proofs, and smart contracts and blockchain technology.

Industrial Secrets

From a utilitarian perspective, Intellectual Property rights are justified by their positive impact on technological and creative production. This perspective posits that creators and inventors are incentivized by the *ex ante*[10] guarantee of future exclusivity afforded by intellectual property rights (Scotchmer, 2004; Burstein, 2013). Crucially, these rights are granted for a limited duration, after which exclusivity (and the associated economic monopoly) ends. This allows society as a whole to benefit from the social welfare generated by these innovations (Fischer, 2001).

7 Original: "[...] importance to innovation and economic growth" (Burstein, 2013, p. 230).
8 Available at: https://drawio-app.com/.
9 Software for graphic design used to create diagrams such as flowcharts, wireframes, UML diagrams, organizational charts, and network diagrams. Available at: https://drawio-app.com/.
10 The Latin maxim ex ante means "from before" or "anticipated" in transliteration. In economic sciences, it refers to values or forecasts established before an event occurs (e.g., a monetary inflation forecast or a budget projection). This contrasts with *ex post*, meaning "from after," which refers to outcomes confirmed afterward (e.g., a specific result of the Consumer Price Index – IPCA or a budget that is verified after the fact). In legal sciences, ex ante is used to describe legal acts, facts, or systems based on prior forecasts (e.g., violations of economic order that involve acts "intended to or capable of producing effects, even if not yet realized"). The ex post parallel would be, for example, the establishment of market dominance when a particular agent or group comes to control 20% or more of a given market.

The incentive to create new technologies, which underpins utilitarian theory, does not appear to depend fundamentally on legally mandated or declared monopolies. This is evident in practice through investments in technologies maintained as industrial secrets. It follows, then, and is empirically observable, that the de facto nature of exclusivity surrounding industrial secrets does not necessarily diminish the incentive for investment.

Industrial secrets are intellectual property assets encompassing "qualquer matéria que possa ser mantida em segredo" (Scotchmer, 2004, p. 79)[11]. As Denis Borges Barbosa (2010, p. 45)[12] explains "Não se trata de um direito exclusivo, pois não houve concessão pelo Estado de uma patente ou algo do mesmo efeito. 9.279/96". In essence, a industrial secret is not a right of exclusivity granted by law, but rather an exclusivity derived from factual circumstances supported by legal frameworks.

Due to the inherent conflict between maintaining secrecy and the disclosure required to obtain a publicly granted monopoly, industrial secrets are not protected by legally established monopolies. Assigning a time limit to the protection of undisclosed knowledge is inherently impossible, rendering such rights unjustifiable even under utilitarian theory. Therefore, industrial secrets cannot be protected by declaratory or attributive rights systems like other intellectual property assets.

From the holder's perspective, the primary aim of maintaining knowledge as a secret is to preserve exclusivity, potentially leading to a monopoly and providing economic incentives. However, from a societal perspective, safeguarding these secrets can hinder technological advancement. This is because the transfer of industrially applicable knowledge hinges on disclosure and the recipient's ability to comprehend and utilize it. It is crucial to consider that:

> [...] conquanto a cópia e a modificação de esquemas seja a opção mais trivial para a transferência de tecnologia, essa opção às vezes não é viável. Os esquemas podem ser mantidos em segredo, ou podem ser ininteligíveis a alguém não familiarizado com a tecnologia. (Diamond, 1997, p. 228, our translation)[13].

Maintaining knowledge as a secret directly obstructs its dissemination, indirectly creating disparities in technological understanding and appropriation. Since comprehending technology depends on accessing relevant knowledge, a positive feedback loop emerges. As the transfer of such knowledge tends to promote economic growth (see Burstein, 2013), public policies concerning the protection of industrially applicable secrets (and, more broadly, all intellectual property) become crucial determinants of economic development, capable

11 Translation: "any subject matter that can be kept secret" (Scotchmer, 2004, p. 79, editorial translation).

12 Translation: "It is not an exclusive right, as there has been no grant by the State of a patent or anything of similar effect. 9.279/96" (Barbosa, 2010, p. 45, editorial translation).

13 Original: "While blueprint copying and modification are the most straightforward option for transmitting technology, that option is sometimes unavailable. Blueprints may be kept secret, or they may be unreadable to someone not already steeped in the technology" (Diamond, 1997, p. 228).

of exerting either positive or negative influences (Chang, 2002). Indeed, the retention of technologies as secrets is "[...] sempre socialmente desaconselhável, eis que dificulta o desenvolvimento tecnológico da sociedade." (Barbosa, 2010, p. 295)[14].

Even without a legally established monopoly, protection against the unauthorized appropriation of industrial secrets exists, creating a *de facto* monopoly. In Brazil, protection against the unauthorized use of industrial secrets does not require explicit contractual provisions. While "poorly regulated" (Barbosa, 2010) by Law 9.279/96 (online), this legislation stipulates that the unauthorized use of industrial secrets obtained through contractual relationships constitutes unfair competition:

> Art. 195. Comete crime de concorrência desleal quem: (...)
>
> XI–divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato (...) (Brasil, 1996, online)[15].

Therefore, only a "contractual relationship" is necessary for legal protection against unauthorized disclosure. As Barcellos notes:

> [...] a ocorrência de sanções penais ou civis só atingem as divulgações não autorizadas estabelecidas em desacordo com vínculo contratual pré-estabelecido ou o contrato de trabalho. (Barcellos, 2015, p. 29)[16].

Notably absent are references to formal contracts like Non-Disclosure Agreements (NDAs) (Burstein, 2013), explicit contractual provisions, or formal acceptance of confidentiality obligations.

This *sui generis* protection allows, "os segredos industriais permitem aos seus detentores suprimir conhecimento" (Scotchmer, 2004, p. 81)[17], seemingly contradicting utilitarian theory and negatively impacting economic development. To mitigate this detrimental effect, "the law encourages the sharing and sale of industrial secrets" through mechanisms like NDAs (Scotchmer, 2004). However, despite legal protection and encouragement, such transactions encounter practical obstacles.

---

14 Translation: "[...] always socially undesirable, as it hinders society's technological development." (Barbosa, 2010, p. 295, editorial translation).

15 Translation: "Art. 195. The crime of unfair competition is committed by anyone who: (…) XI–discloses, exploits, or uses, without authorization, knowledge, information, or confidential data usable in industry, commerce, or the provision of services, excluding those that are public knowledge or evident to a specialist in the field, to which they had access through a contractual or employment relationship, even after the termination of the contract (...)" (Brasil, 1996, online, editorial translation).

16 Translation: "[...] penalties, whether civil or criminal, only apply to unauthorized disclosures that violate a pre-established contractual or employment relationship" (Barcellos, 2015, p. 29, editorial translation).

17 Translation: "industrial secrets allow their holders to suppress knowledge" (Scotchmer, 2004, p. 81, editorial translation).

Arrow's Information Paradox

Arrow's Information Paradox highlights the dilemma faced by potential buyers of secret knowledge: they cannot ascertain its value without disclosure, yet this very act of revelation constitutes a transfer, effectively reducing the transaction's value to zero. As Arrow (Arrow, 1962, p. 615)[18] explains, "[...] existe um paradoxo fundamental na determinação da demanda por informação; seu valor para o adquirente não é conhecido até que ele saiba da informação, mas neste momento ele efetivamente a adquire sem custo" While the "relevance," or value of knowledge to the buyer, might be estimated beforehand, "Enquanto o valor do conhecimento é dado pela sua relevância, isto não é o mesmo que o valor da informação, pois este último é a expectativa de que a informação será adquirida após o pagamento [...]" (Leppälä, 2013, p. 7, our translation)[19].

This paradox hinders the transaction itself. As Benkler (2006, p. 446)[20] observes "A informação em si considerada não é rival. Seu custo marginal é zero. " Therefore, producing "a unit of knowledge" incurs no additional cost, meaning the buyer has no financial obligation to cover production expenses. Consequently, disclosing knowledge before the contract negates its purpose, leaving no basis for negotiation. Fundamentally, this is an issue of lost exclusivity—the inability of the disclosing party to prevent the receiver from using the revealed knowledge. It becomes a "zero-sum game," an impasse where the knowledge holder has no incentive to disclose the information, as their potential gain (corresponding to the knowledge's value) would be nullified by the act of revelation.

The price of a secret is also influenced by supply and demand dynamics. A monopoly (with a single potential discloser) tends to drive the price closer to the buyer's maximum willingness to pay, compared to an oligopoly (with a few potential disclosers). In a perfectly competitive market, the price theoretically converges with the marginal cost (Benkler, 2006), which, for knowledge, equates to the communication cost—effectively zero (Benkler, 1999). This phenomenon extends beyond knowledge to encompass information itself, as

> Se há apenas um custo fixo na produção de informação, e o custo marginal de vendê-la é zero, segue que em razão da competição o preço de mercado da informação irá a zero após a primeira compra. (Leppälä, 2013, p. 10, our translation)[21].

This has also been observed by Arrow (1962). However, there is a clear untapped potential for the commercial exploitation of knowledge protected by industrial secrets, caused by Arrow's Information Paradox (Burstein, 2013; Leppälä, 2013; Scotchmer, 2004; Anton

18 Translation: "[...] there is a fundamental paradox in determining the demand for information; its value to the buyer is not known until they have the information, but at that moment they have acquired it without cost." (Arrow, 1962, p. 615, editorial translation)

19 Original: "[…] the value of knowledge is given by relevance, this is not the same as the value of information as the latter is the expectation of whether the knowledge will be gained after the payment [...]" (Leppälä, 2013, p. 7).

20 Original: "The information itself is nonrival. Its marginal cost is zero" (Benkler, 2006, p. 446).

21 Original: "If there is only a fixed cost of producing information and the marginal cost of selling it is zero, then due to competition the market price of information will go to zero after the first purchase" (Leppälä, 2013, p. 10).

& Yao, 2002). Indeed, "[...] enquanto o Paradoxo da Informação de Arrow diagnostica um problema genuíno, a natureza do problema é mal-entendida. Apesar da incerteza inerente, a demanda por informações não reveladas é raramente inexistente" (Leppälä, 2013, p. 2, our translation)[22]. Therefore, the prospect of future exploitation through knowledge transfer can incentivize industrial innovation.

However, the paradox hinders potential transactions (Burstein, 2013), even when parties successfully value the asset (Leppälä, 2013; Akerlof, 1970). Resolving or mitigating this paradox could improve market efficiency for knowledge, enabling a price minimally higher than its marginal cost. However, as Benkler (2006, p. 446)[23] notes, "[...] um bem como informação [...] nunca poderia ser vendido ao mesmo tempo por um preço positivo (maior que zero) e seu custo marginal", due to the paradox (Arrow, 1962) and its characteristics as a public good—non-rivalrous and non-scarce (Benkler, 1999, 2006).

More broadly, this paradox creates entry barriers for businesses specializing in industrial secret transfers. The limited supply of industrial secrets results in suppressed demand, as potential buyers struggle to find the knowledge they seek. This constitutes a market failure, for, as Burstein (2013, p. 282, our translation)[24] asserts "para que ideias beneficiem a sociedade, elas precisam ser desenvolvidas e comercializadas".

While "[...] simplesmente não existam dados suficientes para traçar quaisquer conclusões sobre os relativos benefícios ao bem-estar social dos vários mecanismos que as partes podem usar para minimizar ou superar o paradoxo" (Burstein, 2013, p. 276, our translation)[25], the underlying issue remains critical. Knowledge production is an economic phenomenon (Benkler, 2006), and "[...] a comercialização de informações é de crítica importância para inovação e crescimento econômico" (Burstein, 2013, p. 229, our translation)[26].

While Arrow's Information Paradox hinders the negotiation of industrial secrets to varying degrees, including those with known potential value based on their utility to the buyer (Leppälä, 2013), no general solution has been found to consistently overcome its effects. Although legal and technical solutions exist and are applied in practice, they do not fully resolve the issue. Further research and the development of specific methods are needed to mitigate or address the paradox in the negotiation of such knowledge (Burstein, 2013).

The fundamental characteristics of the paradox and its constitutive elements are as follows (Leppälä, 2013):

- Capacity: The likelihood that the holder of the knowledge can effectively communicate it;
- Reliability: The likelihood that the knowledge shared is truthful and will eventually be transmitted; and

22 Original: "[...] while Arrow's information paradox diagnoses a genuine problem in trading information, the nature of the problem is misunderstood. Despite the inherent uncertainty, the demand for undisclosed information is seldom non-existing" (Leppälä, 2013, p. 2).
23 Translation: "[...] an asset like information [...] could never be sold simultaneously at a positive price (greater than zero) and its marginal cost" (Benkler, 2006, p. 446, editorial translation).
24 Original: "For ideas to benefit society, they must be developed and commercialzed" (Burstein, 2013, p. 282).
25 Original: "[...] simply not enough data to draw any conclusions about the relative social welfare benefits of the various mechanisms that parties can use to minimize or overcome the disclosure paradox" (Burstein, 2013, p. 276).
26 Original: "Exchanging information is critical to innovation" (Burstein, 2013, p. 229).

- Relevance: The usefulness of the correct information when received, as well as the value of the knowledge to the buyer.
- These are the key characteristics that must be addressed for the successful transfer of industrial secrets, as their presence signifies the operation of the paradox.

As demonstrated in various case studies (Benkler, 2006; Scotchmer, 2004; Leppälä, 2013), the paradox permeates the entire transfer process, even before the actual transaction. It manifests as a lack of incentives to generate the knowledge ultimately transferred and can hinder deal completion due to the uncertainty it creates. In this context, where the secret holder is disincentivized from offering knowledge due to the anticipated effects of Arrow's paradox, successful transactions involving such assets rely on externalities. These externalities facilitate the transaction without requiring knowledge disclosure before the transfer – the point at which disclosure does not diminish the knowledge's value.

To address Arrow's Information Paradox in industrial secret transfers, the literature suggests techniques employing differential equations and Bayesian statistics[27] to analyze the relative incentives between parties and determine the Nash Equilibrium[28] (Leppälä, 2013; Anton; Yao, 2002) or Perfect Bayesian Equilibrium[29] (Anton; Yao, 2002) for these incentives. These tools enable the calculation of optimal strategies for both the discloser and the acquirer, focusing on the act of revelation and allowing for successive partial disclosures or "incremental know-how" releases. Each partial disclosure reduces the impact of the paradox. However, this solution is imperfect and doesn't eliminate the paradox's effects entirely, as partial revelation diminishes the value of the remaining undisclosed know-how (Anton & Yao, 2002). This is particularly true considering that the sum of the parts' values may not equal the value of the whole body of knowledge. Furthermore, the complexity of these techniques presents a barrier to their practical application.

It is important to note that the specific characteristics of each deal can influence the extent to which Arrow's Paradox affects them. Factors such as norms of reciprocity, attribution, and reputation" (Burstein, 2013) within the industry may mitigate the challenge of overcoming the paradox. For instance, "[...] empresas de capital de risco parcialmente superam o Paradoxo da revelação por apoiar-se em suas reputações" (Burstein, 2013, p. 270)[30]. Similarly, in the biotechnology sector, the "consolidação na indústria farmacêutica resultou em um número pequeno de empresas que têm a capacidade de realizar desenvolvimento clínico em larga escala e comercialização de medicamentos" (Burstein, 2013, p. 233)[31]. This allows biotechnology firms to "[...] a empresa de biotecnologia possa revelar informação a respeito do composto sem revelar o composto em si" (Burstein, 2013, p. 233)[32]. In such

27 A theorem used to determine the probability of an event's occurrence, based on specific knowledge related to that event.

28 A mathematical model proposed by John F. Nash represents a situation in which, in a game involving two or more players, none can gain anything by unilaterally changing their strategy.

29 A specific case of the Nash Equilibrium, where (a) each player's strategy results in optimal actions based on their beliefs and the strategies of the other players, and (b) the players' beliefs are consistent with Bayes' Theorem whenever applicable (Fiani, 2015).

30 Original: "[...] venture capital firms overcome the disclosure paradox in part by relying on their reputations" (Burstein, 2013, p. 270).

31 Original: "Consolidation in the pharmaceutical industry has resulted in a small number of firms that have the capability to do large-scale clinical development and drug marketing" (Burstein, 2013, p. 233).

32 Original: "[...] the biotech can disclose information about the compound without revealing the compound itself".

cases, the reputational context presumes the veracity of the information, partially addressing the *capacity* element of the paradox. As a result, revelation strategies vary depending on the parties' context, making it difficult to establish a universally applicable economic model. The need to develop tailored strategies for each transfer represents a cost, which in turn suppresses demand for the transfer of industrial secrets.

Legal mechanisms can mitigate some aspects of the Information Paradox by providing assurances that the recipient, even after acquiring the knowledge, cannot freely use it until the contract is finalized (Burstein, 2013). These mechanisms include state-granted monopolies and the enforcement of exclusive rights (in Brazil, specifically under Laws 9.279/96, 9.610/98, and 9.609/98). In contractual relationships, these mechanisms encompass confidentiality agreements (even if implied), as well as exclusivity and non-competition clauses. These legal tools are widely used in intellectual property and technology transfer contexts. These rights and their enforcement create ex-ante incentives for disclosure (Scotchmer, 2004). In practice, confidentiality agreements are a common strategy for industrial secret transactions (Burstein, 2013; Dyrhovden, 2019), mitigating disincentives similar to legal monopolies, but with a scope limited to the contracting parties.

These legal guarantees create an artificial scarcity, encouraging innovation by incentivizing agents to invent and protecting them from the disincentives posed by the Information Paradox (Scotchmer, 2004; Fischer, 2001; Benkler, 1999). However, as previously noted, this is not the case with industrial secrets, where the "monopoly" arises from factual circumstances rather than legal rights. For industrial secrets, which lack this legal framework, the only protections are those conferred by law, contingent upon maintaining secrecy.

It is widely recognized that both legal norms and technology regulate interpersonal relationships, including monopolies and transactions like technology transfer. As Harvard professor of intellectual property law, Lawrence Lessig (2004), famously stated, "code is law." In the digital realm, programming code can regulate behavior much like legal codes. Consequently, legal transactions that do not rely on legally established monopolies, but instead depend on de facto monopolies, can still provide comparable security through technological means (see Benkler, 2006; Anton; Yao, 2002).

Technological solutions, particularly those based on information technology, can potentially render legal monopolies unnecessary. As Leppälä (2013, p. 3, our translation)[33] suggests, "[...] a fonte original de novas informações pode ter algum poder de mercado natural mesmo sem direitos de Propriedade Intelectual" This is because, as Benkler (2006, p. 415) observes:

> Criptografia e outras técnicas de proteção de cópias não são limitadas pelas definições legais do Direito. Elas podem ser usadas para proteger todos os tipos de arquivos

33 Original: "[...] the original source of new information might have some natural market power even without IPR" (Leppälä, 2013, p. 3).

> digitais – sejam seus conteúdos ainda cobertos por direitos autorais ou não, e sejam os usos que usuários desejem fazer excepcionalmente permitidos ou não (Benkler, 2006, p. 415, our translation)[34].

In abstract terms, a 'complete' contract would, in theory, enable the parties involved in an exchange to avoid issues related to unauthorized use. Under such a contract, legal protections, such as patents, would be unnecessary, as contractual guarantees would suffice (Anton & Yao, 2002). However, implementing methods that achieve this, especially those bypassing legal monopolies, requires further development. As Santos (2003) notes, "the topic under study still needs significant theoretical advancements, such as solving the information asymmetry paradox." Despite these challenges and the lack of technology offering perfect exclusivity for proprietary knowledge, technical solutions are already employed for these purposes. Examples include the computer program registration system used by the Instituto Nacional da Propriedade Industrial (INPI) and various Technological Protection Measures used to control the use of digital goods, regardless of their intellectual property status (see Benkler, 2006).

Industrial secrets, whose substance is "knowledge" and essence is "secrecy," can benefit from the application of cryptography, as noted in the literature (Benkler, 1999; Santos, 2003; Basso et al., 2019), as well as from techniques that complement cryptography, such as Zero-Knowledge Proofs. However, these methods still require further research and development, as no solution currently offers complete exclusivity, particularly in relation to the knowledge acquirer, due to the inherent nature of Arrow's Paradox.

Zero-Knowledge Proofs

In essence, a zero-knowledge proof allows one party to prove to another that they possess certain information without revealing the information itself.

In communication between parties with different data, the simplest way to demonstrate possession of a specific piece of data is to transmit it. Receiving the data inherently implies the sender possessed it. However, a party can also demonstrate possession of data without directly revealing it by transmitting different, but related, information.

Consider that knowledge of a piece of data ("D1") is itself another piece of data ("D2"), representing the assertion of D1's existence. If party "A," possessing D1, transmits it to party "B," who does not possess it, this triggers Arrow's Information Paradox.

To inform "B" of D1's existence without transmitting it directly, "A" can convey the assertion "D2." However, only "A" knows that "D2" is true, while "B" remains uncertain. Since "D2" asserts the existence of "D1," if "D2" is true, then "D1" must exist. Conversely, if "D2" is false, "D1" cannot exist.

34 Original: "Encryption and other copy-protection techniques are not limited by the definition of legal rights. They can be used to protect all kinds of digital files—whether their contents are still covered by copyright or not, and whether the uses that users wish to make of them are privileged or not" (Benkler, 2006, p. 415).

For "B" to accept "D2" as true, and thereby confirm the existence of "D1," "D2" must be information necessarily derived from "D1" but distinct from it, and "B" must be able to understand and verify this derivation. If "B" knows that "D2" necessarily implies "D1," they will also know that the assertion of "D1"'s existence is true, confirming D1's existence.

This concept can be illustrated by a well-known anecdote (Quisquater *et al*., 1990): imagine a cave with two separate tunnels connected only by a hidden door. Ordinary people entering either tunnel can only return the way they came, but one person knows about the connecting door. In a discussion about the possibility of exiting through a different tunnel than the one entered, the knowledgeable person could reveal the secret, but chooses not to. As an alternative, the others propose a test: for 40 consecutive trials, they will instruct the knowledgeable person on which tunnel to enter and exit. If the person consistently emerges from the designated exit, they prove their claim without revealing the secret. The knowledgeable person successfully completes this task, demonstrating the existence of the connecting passage without disclosing its location.

In the context of industrial secrets, Zero-Knowledge Proofs are information conveyed by the potential discloser to the potential acquirer, serving as unequivocal evidence that the discloser possesses specific secret knowledge ("Proof") without revealing its content ("Zero-Knowledge").

Information that merely suggests a probability of possessing the knowledge or requires assumptions about its truthfulness does not constitute proof. Similarly, "Zero-Knowledge" excludes information that reveals parts of the secret or allows for inferences about the knowledge, even partially. Therefore, the set of Zero-Knowledge Proofs is a subset of information in general, subject to stricter criteria.

Smart Contracts and Blockchain

Smart contracts represent the digital implementation of contractual agreements, where obligations are encoded as "contractual codes" that can be incorporated into, executed by, and monitored through computerized systems (Clark, 2018). From a computational perspective, Kõlvart *et al*. (2016) define them as "computerized transaction protocols that implement the provisions of a contract." Essentially, they translate legal transactions into an informatics-based framework. As envisioned by their original proponent, smart contracts can facilitate the "negotiation, acceptance, operation, and adjudication" of contracts (Szabo, 1997).

While smart contracts are often implemented within blockchain environments, the two technologies are not inherently interdependent. Notably, smart contracts (Szabo, 1997) predate blockchain technology (Nakamoto, 2008). One advantage of combining blockchain with smart contracts lies in blockchain's use of encryption for enhanced security. However, other environments, even those without cryptographic features, can also support smart contracts. For instance, legal frameworks and institutions, like those provided by the INPI, can fulfill similar functions to blockchain in ensuring trust and security.

Several blockchain platforms facilitate smart contract implementation through simplified programming languages (Buterin, 2014). The Ethereum blockchain, for example, relies entirely on smart contract technology for its operation (Ethereum Foundation, 2015). This is a significant use case, as the associated cryptocurrency, Ether, managed through these embedded smart contracts, boasts a market capitalization exceeding $316 billion at the time of writing.

Therefore, blockchain represents an environment where assets with significant value are already exchanged. As Dyrhovden (2019, p. 6, our translation)[35] observes "*Smart contracts* conectados ao *blockchain* estão sendo usados para aplicar automaticamente acordos de licenciamento de PI, que permitem a transmissão de *royalties* em tempo real". Specifically, regarding technology transfer, as Basso *et al*. (2019) suggest:

> [...] a tecnologia de blockchain pode promover uma ruptura em como essas negociações e integrações podem ser realizadas, necessitando investigações em termos de metodologias, ferramentas ou plataformas e de formação de base de conhecimento na área (Basso *et al*., 2019, p. 8)[36].

ANALYSIS AND DISCUSSION OF RESULTS

Initial Considerations

This paper explores the potential of blockchain-based smart contracts as tools for transferring intangible assets protected by intellectual property rights. The initial focus was on investigating the feasibility and benefits of using these systems for registering and transferring intellectual property assets. This included exploring the potential for enhancing existing systems by incorporating established computing technologies like Zero-Knowledge Proofs.

During the initial research phase, it became evident that blockchain-based smart contracts are already effectively employed for transferring intangible assets protected by legally established intellectual property rights. However, no applications of these tools were found for intangible assets whose exclusivity derives from factual circumstances rather than legal recognition.

Therefore, the study's scope narrowed to focus on industrial secrets, which are considered intellectual property and hold significant economic relevance compared to other similar assets like traditional knowledge. Given the inherent "secrecy" of industrial secrets, the

35 Original: "Smart contracts connected to blockchain is being used to automatically enforce IP licencing-agreements which allow the transmission of royalties in real time" (Dyrhovden, 2019, p. 6).

36 Translation: "[...] blockchain technology can disrupt how these negotiations and integrations are conducted, requiring further investigation in terms of methodologies, tools, platforms, and the development of a knowledge base in the field" (Basso *et al*., 2019, p. 8, editorial translation).

research further concentrated on the transfer of these assets, excluding their registration. It was assumed that earlier stages (e.g., technology valuation) and later stages (e.g., enforcement of contractual clauses) could be addressed using existing methods.

Proposed Method

The use of Zero-Knowledge Proofs allows for the verification that the potential discloser of a secret indeed possesses the knowledge and can transmit it without revealing the secret itself. The final transfer occurs only after an intermediate stage, during which the potential recipient confirms to the system their confidence that the discloser truly holds the knowledge and can transmit it. This approach effectively addresses both the issues of capacity and trustworthiness (Leppälä, 2013) in a seamless and straightforward manner.

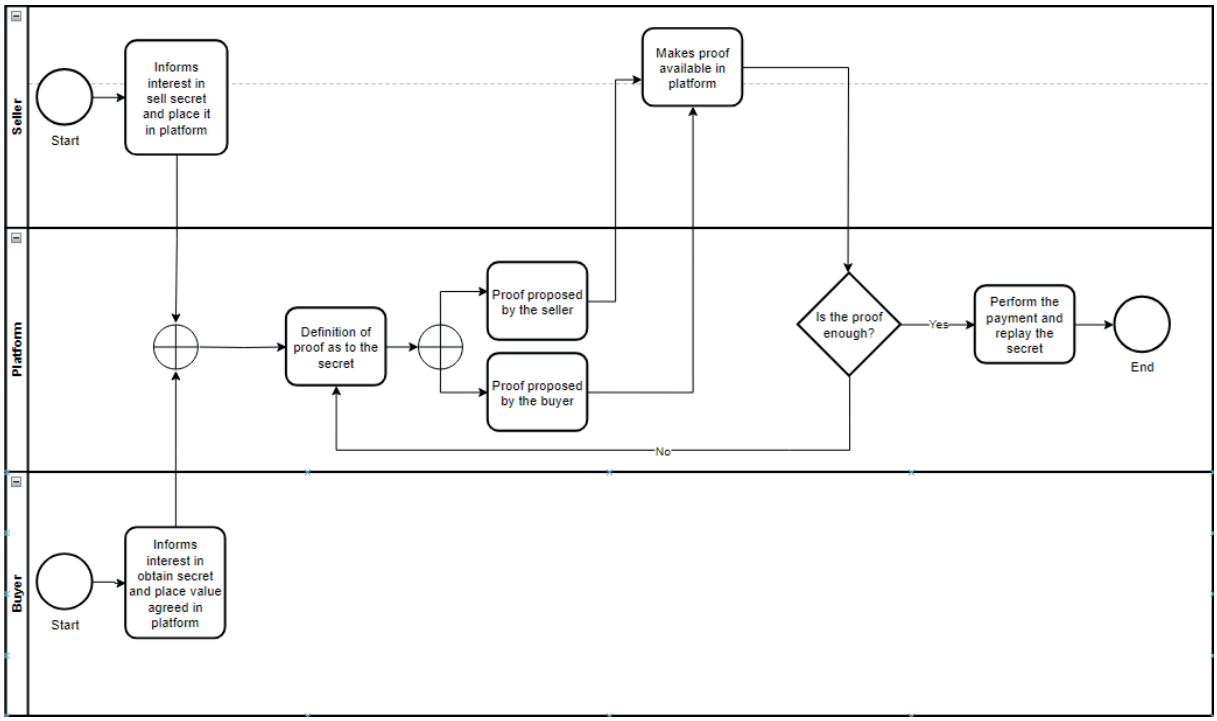
The proposed method assumes that both parties (discloser and acquirer) have already evaluated the asset to be transferred. This requires a relative absence of information asymmetry regarding the asset's value—both parties must understand the knowledge's utility and relevance (Leppälä, 2013). As Baron (2019) notes, smart contracts "help to limit [...] information asymmetries." The method further presumes that the acquirer has some prior knowledge (regardless of its reliability) about the secret's existence and the discloser's possession of it. This assumption becomes unnecessary if the secret is offered publicly on an exchange platform.

Therefore, the method requires a minimum level of information symmetry between the parties regarding the knowledge's value (see Akerlof, 1970). Assuming the knowledge's relevance is established, the remaining challenges are addressing capacity and reliability

Algorithm of the Method

The algorithm, or series of instructions, for the proposed method can be visually represented in the flowchart shown in **Figure 1**.

Figure 1–Flowchart illustrating the proposed method.



Source: Authors' elaboration (2022).

Assuming the existence of information about the secret and the parties' knowledge of its value or prior negotiation, the method begins with both parties actively expressing their interest in the transaction. This requires both parties to signal their willingness to proceed, even if they do so at different times. If their interests align—that is, if both express interest—the smart contract automatically initiates the next step.

The holder of the secret knowledge first converts it into one or more digital files, securing them using standard cryptographic and technological protection mechanisms commonly employed for industrial secrets. These files are then hosted in an appropriate environment, depending on the chosen platform. Next, the holder registers references to these files, or the files themselves, on the blockchain (or an equivalent environment) via the smart contract.

Simultaneously, the potential recipient deposits funds into a wallet linked to the smart contract. This deposit is essential for the process to proceed. The potential recipient retains full control over this wallet and can manage the funds throughout the smart contract's execution, up until the final stage.

When both parties express interest, the smart contract automatically advances the process. This initial exchange of information marks the commencement of the method's execution. Two conditions must be met simultaneously to trigger this stage: (1) a record referencing the secret exists (indicating the discloser's interest), and (2) the potential recipient executes the smart contract with reference to that specific secret (indicating their interest).

Next, to assure the potential recipient of the discloser's capability, the platform automatically requests proof of knowledge from the discloser. This proof, relevant to Arrow's Information Paradox, can be uploaded beforehand or provided at this stage, allowing both parties to deliberate on the information submitted. The discloser can submit the proof to the platform at any point. The platform then automatically forwards it to the potential recipient for evaluation and records the transaction reference on the blockchain.

If satisfied with the proof, the recipient signals their intent to proceed to the smart contract. Upon receiving this confirmation, the smart contract verifies the following: (1) the recipient's wallet holds sufficient funds, and (2) the secret-containing file exists on the remote server. If both conditions are met, the smart contract executes the transfer of the secret to the recipient and the payment to the discloser simultaneously. Finally, the smart contract records the entire transaction history on the blockchain, ensuring a public and immutable record of the transaction and completing the method's execution.

Importantly, these steps describe the method's execution, which is independent of any external context or relationship between the parties. The method does not assume the parties are unfamiliar with each other or have not communicated through other channels. The initial exchange of interest via the smart contract simply provides the platform with the necessary information to function; it does not necessarily represent new information for the involved parties.

Overcoming the Element of Capacity

This stage addresses two of the three elements of the Paradox identified by Leppälä (2013): the discloser's capacity (i.e., their ability to provide the knowledge) and their trustworthiness (i.e., the reliability of the information provided). One strategy for resolving Arrow's Information Paradox in industrial secret negotiations involves disclosing intrinsic information about the knowledge without revealing the knowledge itself. This prevents the recipient from acquiring the knowledge without cost. However, this information's value depends on the recipient's trust in its veracity, highlighting the importance of the discloser's trustworthiness.

In specific contexts, such as capital markets, Silicon Valley, and biotechnology, where reputation plays a crucial role, companies can leverage trust to partially overcome the Paradox (Burstein, 2013). By disclosing intrinsic information about the knowledge without revealing the knowledge itself, companies rely on their established reputation and the potential negative

consequences of false disclosures to build trust with potential recipients. This trust allows the recipient to presume the discloser's capacity and reduces the risk associated with the transaction.

Alternatively, the knowledge can be disclosed incrementally through a series of partial revelations, partially mitigating the Paradox. However, this approach presents an imperfect solution. As Anton and Yao (2002) argue, each partial disclosure diminishes the value of the remaining undisclosed knowledge, potentially discouraging the complete transfer of the secret.

To address the capacity element in the proposed method, the potential discloser must provide the recipient with information that demonstrates the existence of the knowledge and their mastery of it. This is done using intrinsic information about the knowledge, rather than through successive partial revelations, thereby preserving the value of the know-how (Anton & Yao, 2002). The innovation of this method lies in using intrinsic information as proof—rather than relying on presumption or external factors—ensuring its applicability regardless of the parties' particularities or the industries they operate in, such as depending on the discloser's reputation. In this approach, the capacity element is resolved using Zero-Knowledge Proofs.

The method applies intrinsic information derived from the secret knowledge. This information must meet specific criteria: it must be generatable only by the knowledge holder, distinct from the secret itself, and impossible to reverse-engineer. In essence, it is a product of the secret knowledge that does not reveal the secret itself. Furthermore, the proof must be comprehensible to both parties, ensuring they understand the information and its probative value. This establishes the information as verifiable proof, independent of external context or reputation, rather than mere presumption.

To strictly qualify as a Zero-Knowledge Proof, the information must represent an effect directly dependent on the secret knowledge, serving as unequivocal evidence of the discloser's mastery and capacity. Simply providing information about a result is insufficient. For example, disclosing the efficacy and toxicity of a compound, with the recipient relying on the discloser's reputation for validation (as in Burstein, 2013), does not meet this standard.

The solution employing Zero-Knowledge Proofs offers greater generality than those found in the literature. It is independent of specific market characteristics, potentially broadening its practical applicability, and suitable for knowledge that cannot be fractioned. Furthermore, it does not nullify the effects of reputation but rather complements them. Reputation can contribute to establishing both capacity and trustworthiness, as explored later. This method, therefore, presents a sufficient standalone solution while also offering an incremental benefit in situations where other solutions exist.

This method offers a simpler solution compared to the complex revelation strategies based on differential equations and Bayesian statistics found in the literature (Anton; Yao, 2002; Leppälä, 2013). Its straightforward approach eliminates the need for specialized expertise, making it a more accessible technology tool. As Leppälä (2013) notes, a lack of understanding of Arrow's Information Paradox can hinder industrial secret negotiations. Resolving the Paradox through complex techniques presents an even greater barrier. This

method, with its inherent simplicity, is likely to reach a wider audience and lower the barrier to entry for those seeking to transfer industrial secrets. Furthermore, this method can be used independently or complementarily with existing solutions, including those based on differential calculus, without any disadvantage.

The accessibility of this method also extends to the trustworthiness element. Zero-Knowledge Proofs are widely used in computing, particularly in user access control and authentication algorithms. This familiarity among programmers, coupled with the widespread use of Zero-Knowledge Proofs, facilitates their implementation in smart contracts and allows for easier auditing by both professionals and amateurs.

Moreover, as a mature and extensively tested technology, Zero-Knowledge Proofs carry minimal risk of unforeseen adverse effects. The synergy between Zero-Knowledge Proofs and blockchain technology further strengthens the method's reliability. Blockchain's public-key cryptography employs a method similar to Zero-Knowledge Proofs for validating cryptocurrency transactions, specifically in verifying the sender's identity.

Overcoming the Element of Trustworthiness

The application of Zero-Knowledge Proofs in this method serves a dual purpose. It not only resolves the issue of the discloser's capacity to provide the secret knowledge but also establishes the trustworthiness of the information used in the proofs. Because this information functions as verifiable proof, readily understood by both parties, it inherently conveys reliability to the recipient.

Beyond the proof itself, trustworthiness also hinges on the actual exchange of the secret for payment. The method addresses this by guaranteeing the simultaneous transfer of the secret and the payment upon confirmation of the proof. While the recipient must initially trust that the proof sufficiently demonstrates the discloser's capacity and the trustworthiness of the information, this trust is reinforced by the automated and simultaneous exchange mechanism. This built-in guarantee helps overcome the trustworthiness concerns inherent in the initial phase of the transaction.

The finalization of the process, from proof confirmation to the simultaneous exchange of assets and the recording of the transaction history, occurs atomically and is immutably recorded on the blockchain. This ensures a secure and verifiable record of the transaction, further bolstering trustworthiness in terms of actual delivery and the fulfillment of reciprocal obligations.

While the possibility of a bad-faith discloser providing false information remains, the method, coupled with the properties of blockchain technology, effectively addresses this risk. Good faith does not need to be assumed for the method to function effectively.

A key feature of blockchain technology is the creation of a public, timestamped record (Nakamoto, 2008; Buterin, 2014; Clark, 2018). This ensures that the recipient can challenge the accuracy of the information submitted as proof, even in a legal setting, thus

rendering the fundamental information asymmetry of Arrow's Paradox irrelevant after the fact. Moreover, blockchain guarantees the accurate and complete delivery of the secret knowledge and confirms the relationship between the information and the knowledge itself. By using blockchain for all exchanges, a harmed recipient can demonstrate to any third party – if necessary – that the final delivery did not match the promised knowledge or that the outcomes cannot be derived from the secret based on the Zero-Knowledge Proofs. This approach overcomes the trustworthiness element for all data: the information submitted as proof, the secret knowledge itself, and the connection between the two. The public nature of the transaction allows the recipient to prove fraud, whether extrajudicially (through reputational consequences) or judicially (via legal claims).

Therefore, the integration of smart contract technology in the Method addresses the trustworthiness of the information provided as proof, thereby overcoming the capacity element. It also ensures the trustworthiness of the payment from the recipient to the discloser, as it guarantees the fulfillment of the monetary obligation in exchange for the secret.

Beyond their inherent security, these tools eliminate the need for third parties to finalize or validate transactions, unlike some of the legal solutions mentioned earlier. This minimizes the necessity of disclosing the secret to additional individuals. From the perspective of an external observer (anyone outside the negotiation with access to the blockchain), the two possible objects—a cryptographically protected secret or a method to access it—are indistinguishable, effectively achieving security through obscurity.

Furthermore, referencing the secret knowledge recorded on the blockchain provides proof of prior knowledge in patent nullification proceedings, demonstrating a lack of novelty. It also signals the discloser's innovative capacity, much like how "[...] Propriedade Intelectual pode servir como um 'sinal', congregando muitos usuários complementares" (Burstein, 2013, p. 243, our translation)[37]. Importantly, this signaling doesn't require disclosing the secret itself; Zero-Knowledge Proofs effectively achieve this – generating value (through signaling) without compromising the secret's value (through disclosure).

Another desirable consequence is that the public nature of the negotiation via this method allows one to assume (with a reasonable degree of certainty) that the discloser isn't simultaneously negotiating the secret's disclosure with multiple potential buyers through the same public channel. This introduces the influence of external factors like "attribution and reputation," which incentivize reliable information and knowledge transfer—an assumption some markets leverage to overcome the information paradox (Burstein, 2013), particularly concerning trustworthiness.

Moreover, as discussed previously, exclusivity is a key determinant of potential price, distinguishing an oligopolistic market from one with free competition. Consequently, mitigating the risk associated with exclusivity (and therefore the knowledge's value) can foster a sense of security, encouraging parties to engage in negotiations. This is particularly crucial in large,

37 Original: "[...] intellectual property can serve as a "beacon"; "drawing together [...] many complementary users" (Burstein, 2013, p. 243).

anonymous markets, where "[...] os consumidores não sabem quem comprou a informação anteriormente, e não são aptos a executar uma estratégia coordenada puramente baseada em equilíbrio" (Leppälä, 2013, p. 15, our translation)[38].

CONCLUSIONS

This study proposes a method for overcoming Arrow's Information Paradox, offering broad applicability as either a standalone solution or a complement to existing methods. By leveraging Zero-Knowledge Proofs and smart contracts on a blockchain, it simultaneously addresses two fundamental elements of the Paradox – capacity and trustworthiness – often sufficient for its resolution.

While theoretically applicable to other forms of confidential knowledge, such as trade secrets, the method may require modifications. These applications involve distinct characteristics that fall outside this project's scope and were not explicitly addressed during the method's development. Unlike industrial secrets protected by international treaties and legislation, other secrets rely on confidentiality agreements (which cannot always be reliably presumed or verified) or alternative mechanisms to address their specific challenges. This introduces uncertainty, as the method's success hinges on the utility of these secrets and the presence of specific legal guarantees. Consequently, the method's applicability to general secrets may be limited due to these external factors. Additionally, state or military secrets are rarely transacted in a manner where this method would be relevant, as those transactions typically involve inherent capacity and trustworthiness. Therefore, the method is not designed for such applications.

Creating an ad-hoc blockchain specifically for industrial secret transactions could potentially circumvent the access barrier imposed by the costs associated with existing blockchains. Traditionally, miners are incentivized to create new blocks by generating cryptocurrency linked to that blockchain. However, this monetary incentive, while motivating miners to maintain the blockchain, is not technically essential. Alternative incentives could be introduced to eliminate these costs. However, creating ad-hoc blockchains presents the well-known bootstrap problem: a blockchain's security depends on widespread adoption, but this adoption hinges on perceived security.

Although this method considers the current state-of-the-art, with extensive investigation conducted throughout the research phase, it is not intended to replace or improve upon existing solutions for overcoming Arrow's Information Paradox. Instead, it is presented as a complete and self-sufficient proposal – a standalone tool – implementable in suitable environments, regardless of other existing methods, models, techniques, or strategies. While independent, the method can be applied in conjunction with other solutions.

38 Original: "[...] the consumers do not know who has bought the information previously and are unable to play a coordinated pure strategy equilibrium" (Leppälä, 2013, p. 15).

Future studies could focus on comparing this method to other state-of-the-art approaches for general negotiations and exploring their applicability to industrial secrets based on the findings presented here. Additionally, investigating methods that address the pre-contractual and negotiation stages could enhance the developed method. Future research could also aim to develop methods tailored to general secrets or specific types like corporate or trade secrets. Further studies could quantify the unmet demand that this method could address. Future developments may include creating other methods or instantiating them in various environments, such as those prioritizing security. New versions of this method, incorporating modifications or additions like standardized contractual instruments generated by the smart contract and recorded on the blockchain, could also be developed.

BIBLIOGRAPHY

AKERLOF, G. A. The market for “Lemons”: quality uncertainty and the market mechanism. **The Quarterly Journal of Economics**, [*s. l.*], v. 84, n. 3, p. 488-500. Aug. 1970.

ANTON, J. J.; YAO, A. D. The sale of ideas: strategic disclosure, property rights, and contracting.” **Review of Economic Studies**, [*s. l.*], v. 69, n. 3, p. 513–531, July. 2002.

ARROW, K. J. Economic Welfare and the Allocation of Resources for Invention. *In*: National Bureau of Economic Research. (org.). **Rate and Direction of Inventive Activity**: Economic and Social Factor. Princeton: Princeton University Press, 1962.

BARBOSA, D. B. Do direito de propriedade intelectual das celebridades, em Revista de Propriedade Intelectual. **Direito Contemporâneo e Constituição**, Aracaju, ano 1, p. 1-99, out./dez., 2012a. Edição n. 01/2012.

BARBOSA, D. B. **Uma Introdução à Propriedade Intelectual**. 2. ed. rev. atual. São Paulo: Lumen Juris, 2010b.

BARCELLOS, C. A. L. Know How e segredos industriais. *In*: AZEVEDO, R. (org.). **Cartilha da Propriedade Intelectual**. Porto Alegre: Ordem dos Advogados do Brasil, 2015. p. 28-29. Available at: http://www.oabrs.org.br/arquivos/file_55d349cb980bb.pdf. Accessed at: 20 fev. 2022.

BARON, R.; CHAUDEY, M. Blockchain and Smart-contract: a pioneering approach of inter-firms relationships? The case of franchise networks. **HAL**: open science, Lyon, 2019. Available at: https://halshs.archives-ouvertes.fr/halshs-02111603. Accessed at: 13 jun. 2022.

BASSO, F. P.; KREUTZ, D.; RODRIGUES, E.; BERNARDINO, M. Automated technology transfer in MDE as a Service: experiences and research directions. *In*: WORKSHOP EM MODELAGEM E SIMULAÇÃO DE SISTEMAS INTENSIVOS EM SOFTWARE (MSSIS), 1., 2019, Salvador. **Anais** [...]. Porto Alegre: Sociedade Brasileira de Computação, 2019. p. 84-93. Available at: sol.sbc.org.br/index.php/mssis/article/view/7563. Accessed at: 7 abr. 2021.

BRASIL. **Leis 9.279/96, DE 14 DE MAIO DE 1996**. Regula direitos e obrigações relativos à propriedade industrial. Brasília: Presidência da República, 1996.

BRASIL. **Lei Nº 9.610, de 19 de fevereiro de 1998**. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Brasília, DF: Presidência da República, 1998.

BRASIL. **Lei Nº 9.609, de 19 de fevereiro de 1998**. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Brasília, DF: Presidência da República, 1998.

BENKLER, Y. Free as the Air to Common Use: First Amendment Constraints o closure of the Public Domain. **New York University Law Review**, New York, v. 74, n. 354, p. 354-446, 1999. Available at: benkler.org/Free%20as%20the%20Air.pdf. Accessed at: 10 ago. 2021.

BENKLER , Y. **The Wealth of Networks**: how social production transforms markets and freedom. London: Yale University Press, 2006.

BURSTEIN, M. J. Exchanging information without intellectual property. **Texas Law Review**, New York, v. 91, p. 227, 2013. Available at: heinonline.org/HOL/LandingPage?handle=hein.journals/tlr91&div=12&id=&page=. Accessed at: 9 ago. 2021.

BUTTERIN, V. A next-generation smart contract and decentralized application platform. **Ethereum White Paper**, [*s. l.*], v. 3, n. 37, p. 2-1, 2014.

CHANG, H.-J. **Kicking away the ladder**: development strategy in historical perspective. London: Anthem Press, 2002.

CLARK, B. Blockchain and IP Law: a match made in crypto heaven? **WIPO Magazine**. [*S. l.*], 2018. Available at: wipo.int/wipo_magazine/en/2018/01/article_0005.html. Accessed at: 7 abr. 2021.

CONOSCENTI, M.; VETRO, A.; MARTIN, J. C. Blockchain for the internet of things: a systematic literature review. *In*: IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 13., 2016, Morocco. **Conference** […]. Morocco: IEEE/ACS, 2016. Available at: ieeexplore.ieee.org/abstract/document/7945805. Accessed at: 9 ago. 2021.

DIAMOND, J. **Guns, Germs, and Steel**: the fates of human societies. New York: Norton & Company, 1997.

DYRHOVDEN, S. **Blockchain and trade secrets**: a match made in heaven? London: King's College, 2019.

ETHEREUM FOUNDATION. **Ethereum Whitepaper**. [*S. l.*], 14 Mar. 2015. Available at: ethereum.org/en/whitepaper/. Accessed at: 7 abr. 2021.

FIANI, R. **Teoria dos jogos**. 3. ed. [*S. l.*]: Campus, 2015.

FISCHER, W. W. Theories of Intellectual Property. *In*: MUNZER, S. (ed.). **New Essays in the Legal and Political Theory of Property**. Cambridge: Cambridge University Press, 2001. p. 168-199. Available at: https://cyber.harvard.edu/people/tfisher/iptheory.pdf. Accessed at: 13 Jan. 2021.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2008.

KÕLVART, M.; PULLA, M.; RUUL, A. **Smart Contracts**: The Future of Law and eTechnologies. Genebra: Springer, 2016.

LEPPÄLÄ, S. Arrow's Paradox and Markets for Nonproprietary Information. **Cardiff Economics Working Papers**, [*s. l.*], n. E2013/2, 2013. Available at: https://orca.cardiff.ac.uk/77948/1/e2013_2.pdf. Accessed at: 10 ago. 2021.

LESSIG, L. **Code version 2.0**. Nova Iorque: Basic Books, 2006. Available at: codev2.cc/download+remix/Lessig-Codev2.pdf. Accessed at: 7 abr. 2021.

NAKAMOTO, S. **Bitcoin**: a Peer-to-Peer Electronic Cash System. [*S. l.*], 2008. Available at: bitcoin.org/bitcoin.pdf. Accessed at: 7 abr. 2021.

QUISQUARTER, J.-J.; MURIEL, M.; GUILLOU, L.; GAÏD, M. A.; SOAZIG, A. G. ; BERSON, T. A. **How to Explain Zero-Knowledge Protocols to Your Kids**. *In*: Advances in Cryptology — CRYPTO' 89 Proceedings, 89., 1989, New York. **Proceedings** […]. New York: Springer, v. 435. Available at: http://www.cs.wisc.edu/~mkowalcz/628.pdf. Accessed at: 7 abr. 2021.

SANTOS, J. C. **Propriedade intelectual com ênfase em trade secrets**: Criptologia, Performance Econômica. 2003. Dissertação (Mestrado em Economia)–Centro de Ciências Jurídicas e Econômicas, Universidade Federal do Espírito Santo, Vitória, 2003.

SCOTCHMER, S. **Innovation and Incentives**. Cambridge: MIT Press, 2004.

SZABO, N. Formalizing and securing relationships on Public Networks. **First Monday**, [*s. l.*], v. 2, n. 9, 1997. DOI: doi.org/10.5210/fm.v2i9.548.

WANG, D.; ZHAO, J. WANG Y. A Survey on privacy protection of blockchain: the technology and application. **IEEACCESS**, [*s. l.*], v. 8, 2019. Available at: https://ieeexplore.ieee.org/document/9093015. Accessed at: 10 ago. 2021.

ZHENG, Z.; XIE, S.; DAI, H.-N.; CHEN, W.; CHEN, X.; WENG J. IMRAN, M. An overview on smart contracts: challenges, advances and platforms. **Future Generation Computer Systems**, [*s. l.*], n. 105, p. 475-491, 2020. Available at: arxiv.org/pdf/1912.10370. Accessed at: 10 ago. 2021.