



Transferência de segredos industriais por meio de *smart contracts* considerando-se o Paradoxo da Informação de Arrow

Felipe Octaviano Delgado Busnello

Mestre em Direito da Propriedade Intelectual, Università Degli Studi di Torino (UNITO) e Academia da Organização Mundial da Propriedade Intelectual (OMPI), Turim, Piemonte, Itália.

Mestrando em Propriedade Intelectual, Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul, Porto Alegre, Rio Grande do Sul, Brasil.

<http://lattes.cnpq.br/2902342207984367>

felipe@busnello.com.br

Erik Schüler

Doutor em Engenharia Elétrica, Universidade Federal do Rio Grande do Sul (UFRGS), Porto Alegre, RS, Brasil.

Docente EBTT, Instituto Federal do Rio Grande do Sul (IFRS), Veranópolis, RS, Brasil.

<http://lattes.cnpq.br/1046844040379714>

erik.schuler@ifrs.edu.br

Anderson Ricardo Yanzer Cabral

Doutor em Ciência da Computação, Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS), Porto Alegre, RS, Brasil.

Docente EBTT, Instituto Federal do Rio Grande do Sul (IFRS), Viamão, RS, Brasil.

<http://lattes.cnpq.br/0148615078864622>

anderson.yanzer@ifrs.edu.br

Submetido em: 29/06/2022. Aprovado em: 30/04/2024. Publicado em: dd/mm/yyyy.

RESUMO

No estado da arte existem sistemas para transferência de ativos intangíveis protegidos por Propriedade Intelectual, consolidados por monopólios jurídicos, seja por sistemas atributivos (como para patentes e desenhos industriais) ou automaticamente protegidos (como direitos autorais e conexos). Alguns desses sistemas, ou seus respectivos métodos, são descritos na literatura científica. Deste conjunto, alguns métodos utilizam a tecnologia de *blockchain*, e um conjunto menor (inteiramente contido no anterior) também utiliza a tecnologia de *smart contracts*, embora sejam ferramentas independentes entre si. Apesar de os segredos industriais também consistirem em monopólios, as soluções informatizadas ou em ambientes criptográficos aplicadas para outros tipos de bens protegidos por outras formas de propriedade intelectual não podem ser transpostas a esses ativos, em razão de sua natureza *sui generis*, carente de monopólio que independa de sua não revelação. A necessidade de manutenção do segredo decorre do Paradoxo da Informação de Arrow, fenômeno pelo qual a revelação do segredo implica sua transferência. Esse fenômeno

Transferência de segredos industriais por meio de smart contracts considerando-se o Paradoxo da Informação de Arrow prejudica a potencial transferência de segredos industriais e inviabiliza a adoção dos sistemas existentes aplicáveis aos demais tipos de ativos intangíveis. A investigação utilizou a metodologia mista. Este trabalho apresenta um método para transferência de segredos industriais utilizando-se *smart contracts* instanciados em *blockchain* para solução de dois dos três elementos componentes do Paradoxo, especificamente a confiabilidade e a capacidade, pressupondo o terceiro, a relevância.

Palavras-chave: segredo industrial; Paradoxo da Informação de Arrow; *smart contract*; *blockchain*; transferência de tecnologia; patentes; informação tecnológica.

INTRODUÇÃO

Ao contrário do que ocorre com sistemas atributivos de monopólios sobre bens protegíveis por outros institutos da Propriedade Industrial (e.g. patentes), o aproveitamento do conhecimento como bem não é resolvido por políticas públicas (Leppälä, 2013; Burstein, 2013). Não há mecanismos com eficácia *erga omnes*¹ que garantam o monopólio sobre conhecimentos, fazendo com que estas exclusividades sejam protegidas apenas por monopólios de fato (em detrimento de monopólios jurídicos), dependentes da manutenção do segredo e das garantias legais que possibilitem isso. Ou seja, a manutenção de determinado conhecimento depende exclusivamente da capacidade do detentor deste em mantê-lo em segredo, pois, uma vez revelado (ou descoberto de forma autônoma por outrem), sua utilização não estará, em princípio, resguardada.

Os segredos industriais, por sua vez, são objeto da Propriedade Industrial de enorme relevância, inclusive sendo que “[...] o contrato de *know-how* tem muito mais importância econômica do que a licença de patentes” (Barbosa, 2010, p. 635), e que os conhecimentos tradicionais, também protegidos pela Propriedade Intelectual. De fato, o fenômeno econômico da produção de conhecimentos aplicáveis (Benkler, 2006) e das suas comercializações acarretam em geração de inovação e crescimento econômico (Burstein, 2013), portanto, sendo a própria comercialização de conhecimentos, por transferência de tecnologia, uma atividade relacionada à indústria – como de fato geralmente constata-se pela relativa maior dimensão econômica da transferência de conhecimentos aplicáveis na indústria, em detrimento de segredos em geral. Por esse motivo, o escopo deste trabalho trata desses segredos em específico.

Em casos de transferência de conhecimento, como ocorre com os segredos industriais, um conceito basilar de sua teoria é o Paradoxo da Informação de Arrow, identificado pelo economista Kenneth Arrow (Arrow, 1962). Em conceituação simplificada, trata-se do fenômeno em que o adquirente de um conhecimento secreto não sabe o seu valor até que o referido conhecimento o seja revelado; porém, quando revelado, o seu valor tende a zero, pois efetivamente já terá sido transmitido sem custo. Nas palavras do autor, “[...] 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 [...]” (Arrow, 1962, p. 615). Tradicionalmente, de modo a possibilitar negócios dessa natureza, esse Paradoxo é resolvido de maneiras jurídica e técnica.

De maneira jurídica, introduz-se como externalidade as normas legais, como os direitos de Propriedade Intelectual conferidos por Estados e acordos inter partes (Dyrhovden, 2019; Leppälä, 2013; Burstein, 2013). São, respectivamente, os monopólios ou outros direitos

1 *Erga omnes* (lit. “contra todos”) denota aplicabilidade geral, conquanto *inter partes* (lit. “entre partes”) denota aplicabilidade restrita a certas partes, geralmente correspondentes aos diretamente envolvidos em um negócio jurídico.

garantidos por Estados (no Brasil, em especial pela Lei 9.279), e os contratos que envolvem cláusulas de confidencialidade ou exclusividade (Burstein, 2013). Trata-se de recursos jurídicos amplamente utilizados em matéria de Propriedade Intelectual e Transferência de Tecnologia.

Para a resolução de maneira técnica do Paradoxo da Informação de Arrow em transferências de segredos industriais, estratégias específicas podem ser adotadas, como a prática de revelações parciais sucessivas intercaladas com as parcelas de suas contraprestações, mas geralmente a superação dos efeitos do Paradoxo depende de análises econômicas dos pontos de equilíbrio negociais relativos às revelações (Anton; Yao, 2002) e da aplicação de modelos econômicos específicos a cada situação (Leppälä, 2013). Em decorrência das diferenças entre mercados, “[...] 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” (Burstein, 2013, p. 280, tradução nossa)², o que implica não haver uma estratégia geral, aplicável a todos os casos, sendo necessária a formulação e adoção de modelos específicos a cada situação.

Em outros contextos, inclusive na criptografia e em aplicações computacionais, a resolução de problemas da natureza do Paradoxo (quando é necessária a comprovação do domínio de uma informação sem que essa informação seja revelada), pode ser resolvida pelo emprego de Provas de Conhecimento-Nulo, ou Provas de Conhecimento-Zero. Trata-se de técnicas pelas quais uma pessoa pode provar à outra que detém um conhecimento, sem transferir informação que o revele (Wang *et al.*, 2021). Essas provas geralmente consistem em demonstrações, feitas pelo detentor do conhecimento, mediante resoluções de problemas que não poderiam ser resolvidos sem o domínio desse conhecimento. Tais atos servem como informação inequívoca à parte não conhecedora (i.e. provas) de que o segredo existe, e de que a outra parte de fato o detém. Esse tipo de prova consiste em “essencialmente um protocolo envolvendo duas ou mais partes, a dizer, uma série de passos que duas ou mais partes devem tomar para completar uma tarefa” (Wang *et al.*, 2021), cuja demonstração efetivamente comprova a capacidade da parte detentora do segredo.

Também no ambiente computacional, em contexto contratual e, portanto, em sintonia com este trabalho, em meados da década de 1990 foi desenvolvida a tecnologia de *smart contracts* (Szabo, 1997). Tratam-se de “códigos contratuais”, que podem ser incluídos, executados e monitorados de maneira computadorizada (Clark, 2018); ou, do ponto de vista da informática, “[...] protocolos de transação computadorizados que implementam as disposições do contrato [...]” (Kölvart *et al.*, 2016, p. 133, tradução nossa)³. São de uma implementação informática dos negócios jurídicos e, conforme vislumbrado por seu primeiro proponente, *smart contracts* podem ser utilizados para “negociação, aceite, operação, e adjudicação” de contratos (Szabo, 1997).

2 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).

3 Original: “[...] is a computerised transaction protocol that implements the terms of the contract” (Kölvart *et al.*, 2016, p. 133).

Paralelamente, e de forma complementar aos *smart contracts*, o *blockchain* se trata de uma tecnologia informatizada pela qual duas pessoas podem transacionar diretamente, substituindo a confiança em um terceiro por provas criptográficas (Nakamoto, 2008). Trata-se de um protocolo para “criar um registro confiável e transparente”, pelo qual as informações são incluídas e validadas pelos próprios pares (Clark, 2018).

A possibilidade e a carência de desenvolvimento de produtos tecnológicos com base nessas tecnologias com aplicação específica à Transferência de Tecnologia já foram vislumbradas como possibilidade de fato. Consta-se na literatura que “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 al.*, 2019). Identifica-se, pois, um problema de pesquisa a ser desenvolvido, que trata justamente da utilização de tecnologias emergentes (especificamente, *smart contracts* e *blockchain*) para a solução de questões (especificamente, Paradoxo de Arrow) envolvendo a transferência de conhecimento (especificamente, segredos industriais).

Alinhado aos conceitos então apresentados (transferência de segredos industriais, Paradoxo de Arrow, provas de conhecimento-nulo, *smart contracts* e *blockchain*) por este trabalho, propõe-se um Método para superação parcial do Paradoxo da Informação de Arrow, a fim de possibilitar a transferência de conhecimentos e tecnologias protegíveis por segredos industriais. O Método incorpora o uso de Provas de Conhecimento-Nulo, operadas por *smart contract* instanciado em *blockchain*, para controle de informações apresentadas como provas e para efetivação automática das contraprestações sinalagmáticas, com simultâneas entregas do conhecimento e do pagamento às partes contratantes. Deve-se considerar o que o Paradoxo se opera perenemente, desde antes de qualquer pesquisa e desenvolvimento, na forma de um contexto com ausência de incentivos (Benkler, 2006) até a potencial não conclusão de um negócio em razão da incerteza gerada por ele (Leppälä, 2013). Objetiva-se desenvolver ferramenta aplicável ao procedimento de transferência do segredo em si, na qual a parte fornecedora disponibiliza o segredo (sem revelá-lo), apresenta as provas que evidenciem a posse desse segredo à parte adquirente; a parte adquirente, uma vez satisfeita, recebe o segredo e o pagamento é efetuado de forma automatizada. Com isso, como será mostrado, diferentes aspectos envolvendo o Paradoxo de Arrow são minimizados ou resolvidos. Etapas anteriores (valoração da tecnologia, por exemplo) e posteriores à transferência (manutenção de cláusulas contratuais) não fazem parte do escopo da solução aqui proposta.

METODOLOGIA

Para o presente trabalho a abordagem utilizada foi a mista, havendo sido empregadas tanto representatividades numéricas quanto compreensões de conceitos. Na medida em que pouco se encontra em termos de literatura científica acerca do tema desenvolvido, trata-se de um trabalho baseado em pesquisa exploratória, cujo objetivo foi buscar maior

familiaridade com o problema, com objetivo de torná-lo mais explícito e com possibilidade de criar hipóteses (Gil, 2008). A metodologia utilizada para desenvolvimento do projeto baseou-se, de forma sucinta, nas seguintes etapas:

- a) revisão bibliográfica e documental, em literatura científica e cinzenta, para a identificação do estado da arte referente às tecnologias e aos métodos empregados para negociação e transferência de segredos industriais; e
- b) desenvolvimento e apresentação de uma proposta do método.

Em consideração à revisão bibliográfica, pesquisas em bases de dados especializadas, por meio das palavras-chave “*trade secrets*” e “*smart contracts*” retornaram menos de uma dezena de resultados, mesmo em permutas com os termos no singular e nas línguas portuguesa, italiana, francesa e espanhola. Em sentido contrário, verificou-se profícua literatura cinzenta livremente acessível na Internet a respeito desses temas.

Para levantamento das tecnologias existentes no estado da arte, também foi realizada pesquisa, em bases de dados científicas e na literatura cinzenta, sobre os métodos de resolução do Paradoxo. Na literatura científica foi identificada a base teórica para a sua ocorrência e pertinência de investigação no cenário atual, da economia da informação (ver Benkler, 1999 e 2006), a inexistência na prática de método que resolva completamente (ver Leppälä, 2013), bem como estratégias e técnicas em geral para (ver Anton; Yao, 2002). Em especial, identificou-se não haver, no estado da arte, método para a transferência de tecnologia protegida por segredos industriais utilizando-se soluções informatizadas ou em ambientes criptográficos (Santos, 2003; Basso *et al.*, 2019), tampouco para potencial aplicação de novas tecnologias, como a *blockchain*, para fins semelhantes (Conoscenti *et al.*, 2016). Essa carência ocorre apesar da existência de demanda para conhecimentos protegidos por segredos industriais (Leppälä, 2013), e da identificação clara dos impactos negativos causados pelo Paradoxo da Informação de Arrow nessas negociações, apesar da sua “[...] importância para inovação e crescimento econômico” (Burstein, 2013, p. 230, tradução nossa)⁴, inclusive em repressão de demanda. A aparente inexistência de método congênere, e sua potencial aplicabilidade, justificou a criação deste Método.

O desenvolvimento da proposta do método para transferência de segredos industriais, em si, baseou-se na elaboração de fluxograma com a descrição dos passos a serem seguidos para cumprimento do processo de transferência de segredo industrial. Tal fluxograma foi desenvolvido com auxílio da ferramenta⁵ Draw Io⁶, e, após reformulações, foi determinada uma série de instruções (um algoritmo) que resolvesse simultaneamente os problemas da capacidade e da confiabilidade, e que pudesse ser aplicada por pessoas comuns em qualquer etapa do processo de transferência.

4 Original: “[...] importance to innovation and economic growth” (Burstein, 2013, p. 230).

5 Disponível em: <https://drawio-app.com/>.

6 *Software* de desenho gráfico para criação de diagramas, tais como fluxogramas, *wireframes*, diagramas UML, organogramas e diagramas de rede.

Referencial teórico

O referencial teórico está subdividido em quatro subseções, contendo explicações atinentes a cada um dos tópicos envolvidos no trabalho: segredos industriais, Paradoxo de Informação de Arrow, Provas de Conhecimento-Nulo e *smart contracts* e *blockchain*.

Segredos industriais

Conforme a sua teoria utilitária, os direitos de Propriedade Intelectual são fundamentados e justificados no efeito positivo na produção de tecnologia e arte, pois os criadores e inventores seriam incentivados pela garantia *ex ante*⁷ de exclusividade futura: os próprios direitos de Propriedade Intelectual (Scotchmer, 2004; Burstein, 2013). Fundamentalmente, quando constituídos juridicamente, esses direitos são conferidos por prazos determinados, após cujos términos cessa-se a exclusividade (portanto a situação econômica de monopólio), de modo que toda a sociedade possa se beneficiar do bem-estar social gerado por essas inovações (Fischer, 2001).

O incentivo à criação de novas tecnologias, em que a utilitária teoria se baseia, não parece essencialmente depender que o monopólio seja constituído ou declarado juridicamente. Isso se confirma na prática pelo investimento em tecnologias que são mantidas como segredos industriais. Portanto, decorre (e constata-se empiricamente) que a natureza fática da exclusividade sobre segredos industriais não necessariamente elimina o incentivo ao investimento.

Segredos de indústria são ativos relacionados à Propriedade Intelectual, sobre “qualquer matéria que possa ser mantida em segredo” (Scotchmer, 2004, p. 79). Nas palavras de Denis Borges Barbosa (2010, p. 45), “Não se trata de um direito exclusivo, pois não houve concessão pelo Estado de uma patente ou algo do mesmo efeito. 9.279/96”. Em sua natureza, o segredo industrial não é um direito de exclusividade, mas uma exclusividade decorrente de situações fáticas amparadas no Direito.

Pela incongruência entre a manutenção de um segredo e a necessária revelação para que seja conferido monopólio por ente público, os segredos industriais não são protegidos por monopólios juridicamente constituídos. Pela impossibilidade de atribuir limite temporal a objetos de proteção desconhecidos, a atribuição de direitos sequer seria justificável, conforme a teoria utilitária. Portanto, os segredos industriais não são passíveis de serem protegidos por sistemas atributivos ou declaratórios de direitos, como ocorre com os demais objetos de proteção da Propriedade Intelectual.

7 Brocardo latino. Em transliteração, “de antes”, lit. “antecipado”. Nas ciências econômicas, como no caso, denota valores previstos definidos anteriormente a um evento (e.g. a previsão da inflação monetária, ou uma previsão orçamentária). Cf. *ex post*, “de após”; o resultado verificado posteriormente (e.g. certo resultado do Índice Nacional de Preços ao Consumidor Amplo – IPCA; ou certo orçamento verificado posteriormente). Também utilizado nas ciências jurídicas para descrever atos e fatos jurídicos, ou seus sistemas, baseados em previsões (e.g. as infrações da ordem econômica que consistem em atos “*que tenham por objeto ou possam produzir efeitos, ainda que não sejam alcançados*”, de que um paralelo *ex post* é a configuração de posição dominante no mercado quando certo agente ou grupo passa a representar mais de 20% ou mais de algum mercado.

Pelo ponto de vista do detentor, o propósito direto da manutenção de um conhecimento como segredo é a manutenção da exclusividade. Essa exclusividade potencialmente traduz-se em um monopólio, que representa incentivo econômico para o detentor do conhecimento. Pelo ponto de vista da sociedade em geral, a manutenção desses segredos pode ser prejudicial ao desenvolvimento tecnológico. Isso porque a possibilidade de transferência de conhecimento aplicável industrialmente depende da sua revelação, e da possibilidade de apropriação desse conhecimento (sua compreensão) pelo receptor. Diga-se:

[...] 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, tradução nossa)⁸.

A manutenção de um conhecimento como segredo, portanto, tem o efeito direto de obstruir a sua cópia, o que indiretamente também cria discrepância na possibilidade de compreensão tecnológica, a apropriabilidade.

Sendo que a compreensão da tecnologia depende do acesso aos conhecimentos pertinentes, tem-se um ciclo de *feedback* positivo. Como a transferência desses conhecimentos tende a fomentar crescimento econômico (ver Burstein, 2013), políticas públicas sobre a proteção de segredos aplicáveis na indústria (como, em geral, toda propriedade intelectual) são fatores determinantes para o desenvolvimento econômico, podendo ter efeitos positivos ou negativos sobre ele (Chang, 2002), sendo a manutenção de tecnologias em segredo “[...] sempre socialmente desaconselhável, eis que dificulta o desenvolvimento tecnológico da sociedade.” (Barbosa, 2010, p. 295).

Mesmo ausente o monopólio juridicamente constituído, existe proteção contra a apropriação desautorizada de segredo industrial, o monopólio de fato. A garantia contra o uso não autorizado de segredos de indústria, no Brasil, independe de disposição expressa em instrumento contratual. No Brasil, a matéria é regulada “de maneira pífia” (Barbosa, 2010) pela Lei 9.279/96 (*online*), que estipula como crime de concorrência desleal o uso desautorizado de segredos industriais revelados mediante relação contratual:

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*).

8 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).

Portanto, apenas a “relação contratual” é requisito para essa garantia. Assim,

[...] 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).

Notadamente, estão ausentes menções a contrato formal – como os “Contratos de Revelação Confidencial” (Burstein, 2013), – a disposição expressa em instrumento contratual, ou a aceite solene sobre obrigação de confidencialidade.

Em decorrência dessa proteção *sui generis*, “os segredos industriais permitem aos seus detentores suprimir conhecimento” (Scotchmer, 2004, p. 81), em aparente discrepância à teoria utilitária, e em efeito negativo ao desenvolvimento econômico. A mitigar esse efeito nocivo, “a Lei encoraja o compartilhamento e a venda de segredos industriais”, como por meio dos referidos contratos de confidencialidade (Scotchmer, 2004). Entretanto, embora protegidos e encorajados, esses negócios encontram óbice fático.

Paradoxo da Informação de Arrow

Pelo Paradoxo da Informação de Arrow, o potencial adquirente de um conhecimento secreto não sabe o seu valor a não ser que esse conhecimento seja a ele revelado; porém, o próprio ato da revelação constitui sua transferência, o que reduz o valor do negócio a zero. Nas palavras do autor, “[...] 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” (Arrow, 1962, p. 615). De fato, sabe-se que a relevância, “o valor do conhecimento para o comprador”, pode ser conhecida antes da sua revelação, mas “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, tradução nossa)⁹.

Trata-se de um problema que impede a própria realização do negócio. Isso porque, em sua natureza, “A informação em si considerada não é rival. Seu custo marginal é zero.” (Benkler, 2006, p. 446, tradução nossa)¹⁰. Portanto, não há custo de produção agregado a “uma unidade de conhecimento”, o que implica não haver necessidade de dispêndio financeiro por parte do adquirente para cobrir custos de produção. Desta forma, a transferência de conhecimentos anteriormente ao contrato esvazia seu objeto, não havendo mais sobre o que contratar. Em sua natureza, trata-se de um problema de perda de exclusividade; da possibilidade de o revelador impedir o uso, pelo adquirente, do conhecimento revelado.

9 Original: “While 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).

10 Original: “The information itself is nonrival. Its marginal cost is zero” (Benkler, 2006, p. 446).

Consiste em um “jogo de soma-zero”, impasse pelo qual não há incentivo para que o detentor do conhecimento o revele – porquanto o seu ganho corresponde ao valor, que, por sua vez, seria de fato eliminado pelo seu ato de revelação.

Igualmente, o preço do segredo depende da oferta, o que implica que uma situação de monopólio (oferta de apenas um potencial revelador) tenda a resultar em um preço mais próximo ao limiar da disposição a pagar do potencial receptor (o preço máximo que pagaria), em comparação a uma situação de oligopólio (oferta de uma pequena pluralidade de potenciais reveladores). Por completude, também referimos que uma situação de livre concorrência tende a resultar em um preço igual ao custo marginal (Benkler, 2006), que, no caso de conhecimento, corresponde unicamente ao custo de comunicação desse segredo – que também corresponde a zero (Benkler, 1999). Esse fenômeno ocorre não apenas relativamente ao conhecimento, mas também sobre a informação em si, porquanto

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, tradução nossa)¹¹.

conforme também identificado por Arrow (1962). Entretanto, efetivamente constata-se um potencial reprimido para o aproveitamento comercial de conhecimentos protegidos por segredos industriais, causado pelo Paradoxo da Informação de Arrow (Burstein, 2013; Leppälä, 2013; Scotchmer, 2004; Anton; Yao, 2002). De fato, “[...] 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, tradução nossa)¹². Condizentemente, a perspectiva de aproveitamento futuro dos segredos por meio de transferência pode contribuir como fator de estímulo à inovação industrial.

O Paradoxo mencionado inibe possíveis negócios jurídicos (Burstein, 2013), mesmo quando superada a possibilidade de valoração do bem pelas partes (Leppälä, 2013; Akerlof, 1970). Ergo, a resolução desse Paradoxo ou a mitigação dos seus efeitos tende a tornar o mercado para conhecimentos mais próximo de um mercado eficiente, no qual o preço do bem é minimamente maior do que seu custo marginal, ainda que “[...] um bem como informação [...] nunca poderia ser vendido ao mesmo tempo por um preço positivo (maior que zero) e seu custo marginal” (Benkler, 2006, p. 446), em razão do Paradoxo (Arrow, 1962) e da sua natureza como bens públicos (no sentido econômico) – não rivais e não escassos (Benkler, 1999, 2006).

Em um contexto amplo, a ocorrência desse Paradoxo tende a criar barreiras de entrada para negócios cujo objeto é a transferência de segredo industrial. Nesse estado, a

11 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).

12 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).

ausência de oferta por segredos industriais, simetricamente traduz-se em demanda reprimida por estes bens: os potenciais receptores não encontram oferta dos conhecimentos que os interessam. Esse é um fenômeno de falha de mercado, pois “para que ideias beneficiem a sociedade, elas precisam ser desenvolvidas e comercializadas” (Burstein, 2013, p. 282, tradução nossa)¹³.

Embora “[...] 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, tradução nossa)¹⁴, o objeto subjacente é de grande relevância. Isso porque a produção de conhecimentos é um fenômeno econômico (Benkler, 2006) “[...] a comercialização de informações é de crítica importância para inovação e crescimento econômico” (Burstein, 2013, p. 229, tradução nossa)¹⁵.

Conquanto o Paradoxo da informação de Arrow seja prejudicial (em qualquer grau) à negociação de segredos industriais, inclusive sobre segredos cujos potenciais valores – decorrentes da utilidade para o adquirente (Leppälä, 2013) – são conhecidos pelas partes contratantes, não existem soluções gerais que consistentemente superem seus efeitos. Os empregos de soluções jurídicas e técnicas são conhecidos e aplicados na prática, mas não solucionam completamente o problema. Maior pesquisa sobre o tema, e potencial desenvolvimento de métodos específicos, são necessários para a mitigação ou resolução dos efeitos do Paradoxo na negociação desses conhecimentos (Burstein, 2013).

As características elementares do Paradoxo, seus elementos constitutivos, são (Leppälä, 2013):

- capacidade: a probabilidade de o revelador deter o conhecimento e de ser capaz de transmitir informação sobre ele;
- confiabilidade: a probabilidade de revelar informação fidedigna sobre o conhecimento, e de finalmente transmiti-lo; e
- relevância: a utilidade da informação correta quando recebida, e do conhecimento em si ao adquirente.

Essas são características de cujas superações a transferência de segredos industriais depende, pois, cujas presenças implicam a ocorrência do Paradoxo.

Com base nas identificações casuísticas específicas encontradas na literatura, o Paradoxo se opera durante todo o processo de transferência – desde mesmo antes dele, na forma de um contexto com ausência de incentivos a originar o conhecimento a eventualmente ser transferido (ver Benkler, 2006; Scotchmer, 2004) até a não conclusão de um negócio em razão da incerteza gerada pelo Paradoxo (Leppälä, 2013). Neste contexto, quando pela perspectiva de futura ocorrência do Paradoxo de Arrow não há incentivo para que o detentor do segredo o ofereça, os negócios sobre esses bens dependem da introdução de

13 Original: “For ideas to benefit society, they must be developed and commercialized” (Burstein, 2013, p. 282).

14 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).

15 Original: “Exchanging information is critical to innovation” (Burstein, 2013, p. 229).

externalidades que possibilitem as suas transações sem que seja necessária a revelação do conhecimento durante todas as fases anteriores à sua transmissão: o momento no qual a efetiva transferência do conhecimento não causa que seu valor seja eliminado.

Para a resolução de maneira técnica do Paradoxo da Informação de Arrow em transferência de segredos industriais, a literatura descreve técnicas que empregam o uso de equações diferenciais e estatística baseada no Teorema Bayesiano¹⁶ para descobrir os incentivos relativos entre as partes, e determinar o Equilíbrio de Nash¹⁷ (Leppälä, 2013; Anton; Yao, 2002) ou Equilíbrio Bayesiano Perfeito¹⁸ (Anton; Yao, 2002) para esses incentivos. Por esses artifícios é possível calcular estratégias ideais para o revelador e para o adquirente, que se operam sobre o ato da revelação e possibilitam sucessivas revelações parciais, ou revelações de “*know-how* incremental”, de modo que cada revelação seja feita na proporção em que o Paradoxo se opere em menor grau. Porém, essa prática é solução imperfeita, que não elimina o efeito do Paradoxo, pois a revelação parcial reduz o valor do *know-how* não revelado remanescente (Anton; Yao, 2002), sobretudo considerando-se que o somatório dos valores das partes não necessariamente corresponde ao valor de todo conhecimento. Salienta-se que essas técnicas são de difícil apropriação, o que representa barreira de acesso aos seus empregos.

Note-se que particularidades de cada negócio podem determinar o grau em que o Paradoxo os prejudica. Fatores como “normas de reciprocidade, atribuição e reputação” (Burstein, 2013) no contexto da indústria em que as partes estão inseridas podem atenuar a dificuldade de superação do Paradoxo. A exemplo, “[...] empresas de capital de risco parcialmente superam o Paradoxo da revelação por apoiar-se em suas reputações” (Burstein, 2013, p. 270, tradução nossa)¹⁹. É também o caso de empresas de biotecnologia, pois a “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, tradução nossa)²⁰, possibilitando que “[...] a empresa de biotecnologia possa revelar informação a respeito do composto sem revelar o composto em si” (Burstein, 2013, p. 233)²¹, e o contexto reputacional desse mercado atribui presunção de veracidade dessa informação a respeito do composto – que se traduz em superação parcial do elemento da capacidade. Congruentemente, as estratégias de revelação variam conforme o contexto das partes, não sendo possível a criação de um modelo econômico

16 Teorema a partir do qual determina-se a probabilidade de ocorrência de determinado evento, levando-se em consideração determinado(s) conhecimento(s) relacionado(s) ao evento.

17 Modelo matemático proposto por John F. Nash que representa uma situação em que, em um jogo envolvendo dois ou mais jogadores, nenhum deles tem algo a ganhar alterando sua estratégia de forma unilateral.

18 Caso específico do anterior, no qual (a) as estratégias de cada jogador resultam em ações ótimas, dadas a crença do jogador e as estratégias dos demais jogadores; e (b) as crenças dos jogadores são consistentes com o Teorema de Bayes sempre que possível (Fiani, 2015).

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

20 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).

21 Original: “[...] the biotech can disclose information about the compound without revealing the compound itself”.

de aplicação geral. A necessidade de estipulação de estratégias para cada transferência constitui custo, portanto também representa repressão à demanda pela transferência de segredos industriais.

De maneira jurídica, algumas características do Paradoxo são evitadas pela introdução de garantias de que o receptor, embora tornando-se detentor do conhecimento, não poderá livremente utilizá-lo antes que o contrato seja concluído (Burstein, 2013). Com alcance geral, são os monopólios conferidos por Estados e as garantias de cumprimento dessas exclusividades (no Brasil, em especial estipuladas pelas Leis 9.279/96, 9.610/98 e 9.609/98). Com alcance entre as partes, os contratos que envolvem confidencialidade – mesmo que implícita, ausente disposição expressa em instrumento contratual, se essa confidencialidade puder ser inferida (Burstein, 2013), – exclusividade e não-competição. Todos são recursos jurídicos amplamente utilizados em matéria de Propriedade Intelectual e Transferência de Tecnologia. Esses direitos e suas garantias de cumprimento criam incentivos *ex ante* para o revelador (Scotchmer, 2004). Na prática, para segredos industriais, acordos com estipulações de confidencialidade são adotados como estratégia (Burstein, 2013; Dyrhovden, 2019), visando a produzir efeito de eliminação do desincentivo semelhante ao dos monopólios legais, conquanto com escopo restrito aos contratantes.

Essas garantias se traduzem de fato em uma rivalidade artificial, de modo que agentes são encorajados a inovar – e.g. o inventor em um direito de patente é incentivado a inventar (Scotchmer, 2004; Fischer, 2001; Benkler, 1999). Igualmente (e crucialmente, para este trabalho), não sejam desincentivados a tal pela perspectiva de ocorrência futura do Paradoxo. Entretanto, não é o caso dos segredos industriais, como já afirmado, pois o seu monopólio decorre de situação fática, em detrimento de constituição ou declaração jurídica. Sobre os segredos industriais, carentes de monopólio jurídico, restam apenas as garantias conferidas pela Lei, que dependem da manutenção do conhecimento como segredo.

Igualmente consolidado, e atualmente desenvolvido na ciência, é o fato de que tanto as normas legais quanto a tecnologia servem para regular relações interpessoais, inclusive monopólios e negócios jurídicos, como a transferência de tecnologia. Nas palavras de Lawrence Lessig, professor de Propriedade Intelectual da Universidade de Harvard, “Código é Lei” (Lessig, 2004), no sentido de que, no ambiente virtual, o código de programação regula conduta de maneira semelhante a um código de leis. Nesse sentido, negócios jurídicos que prescindam de monopólios legais, portanto dependam apenas de monopólios de fato, podem efetivamente conferir semelhante segurança (ver Benkler, 2006; Anton; Yao, 2002).

O emprego de soluções técnicas para esse problema, em especial por meio de informática, pode mesmo tornar supérfluos ou redundantes os monopólios jurídicos, de modo que “[...] a fonte original de novas informações pode ter algum poder de mercado natural mesmo sem direitos de Propriedade Intelectual” (Leppälä, 2013, p. 3, tradução nossa)²², pois

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

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 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, tradução nossa)²³.

Em abstrato, quanto ao alcance de suas possíveis implementações, um contrato ‘completo’ permitiria às partes imediatas à troca evitar os problemas de uso não autorizado e, portanto, nenhuma proteção legal (e.g. patentes), além das garantias ao cumprimento do contrato, seria necessária (Anton; Yao, 2002).

A implementação de métodos que possibilitem essa realidade, em especial que prescindam de monopólio jurídico, ainda carece de desenvolvimento, sendo que “o tema estudado ainda necessita de grandes avanços teóricos, como, por exemplo, resolver o paradoxo da simetria de informações” (Santos, 2003). Inobstante à carência identificada e à inexistência de tecnologia que confira perfeita exclusividade aos conhecimentos proprietários, a adoção de meios técnicos para esses fins é realidade, como empregado e.g. no sistema de registro de programa de computador pelo Instituto Nacional da Propriedade Industrial (INPI) e em diversos Mecanismos de Proteção Tecnológica empregados para controlar os usos de bens digitais, independentemente da suas proteções por Propriedade Intelectual (ver Benkler, 2006).

Segredos industriais, com substância “conhecimento” e essência “segredo”, podem se valer da utilização de criptografia, como consolidado na literatura (Benkler, 1999; Santos, 2003; Basso *et al.*, 2019), ou de técnicas empregadas em conjunto com a criptografia, como as Provas de Conhecimento-Nulo. Esses métodos ainda carecem de pesquisa e desenvolvimento, não havendo uma solução que confira exclusividade, em especial oponível ao adquirente do conhecimento, a natureza do Paradoxo.

Provas de Conhecimento-Nulo

Em abstrato, as Provas de Conhecimento-Nulo são informações que atestam o domínio de um conhecimento por parte de uma pessoa, mas, para tanto, não o revelam.

Em uma comunicação entre entes com dados diversos, a maneira trivial de um ente demonstrar a outro que possui um dado é transmiti-lo, pois, receber tal dado implica que o doador o detinha naquele momento. Não trivialmente, um ente que afirma possuir certo dado pode indicar que sua afirmação é verdadeira por meio de transmissão de informações diversas do dado.

23 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).

Considerando-se que o conhecimento de um dado (“D1”) é em si outro dado (“D2”), que consiste na afirmação da existência do primeiro, caso o ente possuidor desses dados (“A”) transmita ao não possuidor (“B”) o dado “D1” em si, opera-se o Paradoxo da Informação de Arrow.

Para informar a existência do dado “D1”, sem transmiti-lo, a afirmação “D2” pode ser transmitida por pelo ente “A” ao ente “B”. Entretanto, apenas o ente “A” sabe que sua afirmação “D2” é verdadeira, enquanto o ente “B” desconhece a veracidade. Como o dado “D2” é em si a afirmação da existência de “D1”, se a afirmação “D2” for verdadeira, por implicação “D1” existe. Simetricamente, a falsidade da afirmação “D2” implica a inexistência de “D1”.

Para que a afirmação “D2” transmitida por “A” seja compreendida como verdadeira por “B” e, por implicação, a informação da existência do dado “D1” também seja verdadeira, a afirmação “D2” deve consistir em dado que necessariamente decorra de “D1”, e isso seja compreensível por “B”. Isto é: “D2” deve ser uma informação que só possa ser extraída de “D1”, porém, não sendo “D1” em si; e “B” deve ser capaz de compreender isso e verificar “D2” quando for recebido. “B” saber que “D2” necessariamente implica “D1” também saberá que a afirmação de que “D1” existe é verdadeira, portanto que “D1” existe.

O conceito pode ser explicado por célebre anedota: em uma hipotética caverna composta de dois túneis distintos, apenas uma porta secreta os liga. Pessoas leigas que entrem em qualquer dos túneis podem apenas voltar pelo mesmo caminho, porém existe um detentor do conhecimento sobre a porta de ligação. Em discussão sobre a possibilidade de uma pessoa sair por qualquer um dos túneis, independentemente de por qual tenha entrado, seria possível ao conhecedor transmitir aos leigos o seu *know-how*, mas ele deseja mantê-lo em segredo. Como alternativa, os leigos determinam que admitiriam provada essa possibilidade de sair por túnel diverso se, por arbitrárias 40 vezes consecutivas, indicassem ao indivíduo um dos túneis pelo qual entrar e posteriormente um pelo qual sair, e, em todas, os túneis corretos fossem utilizados. O indivíduo realiza essa tarefa com sucesso, e por conseguinte prova aos leigos a possibilidade, sem transmitir qualquer conhecimento (Quisquarter *et al.*, 1990).

Em relação aos segredos industriais, configuram Provas de Conhecimento-Nulo as informações transmitidas pelo potencial revelador ao seu potencial receptor, e sejam por ele compreendidas como demonstração inequívoca de que o potencial revelador efetivamente detém certo conhecimento secreto (portanto, “Prova”); porém não o revelando (portanto, “de Conhecimento-Nulo”).

Não configuram provas as informações prestadas para serem presumidas verdadeiras com necessária confiança, ou as que meramente indiquem probabilidade (sobre a qual o potencial adquirente possa presumir o domínio sobre o conhecimento, ou calcular a chance de tê-lo), mas não provem tal fato. Igualmente, não configuram Conhecimento-Nulo as informações que consistam em revelações parciais do conhecimento secreto, ou pelas quais

se possa inferir ou deduzir o conhecimento em si, ainda que parcialmente. Assim, o conjunto das Provas de Conhecimento-Nulo está inteiramente contido no conjunto das informações em geral.

Smart Contracts e Blockchain

Os *smart contracts* consistem na instanciação de contratos em ambiente digital, de maneira que as obrigações contratuais consistam em “códigos contratuais”, passíveis de serem incluídos, executados e monitorados de maneira computadorizada (Clark, 2018) nesse ambiente; ou, do ponto de vista da informática, “protocolos de transação computadorizados que implementam as disposições do contrato” (Kölvart *et al.*, 2016). São de uma implementação informática dos negócios jurídicos e, conforme vislumbrado por seu primeiro proponente, *smart contracts* podem ser utilizados para “negociação, aceite, operação, e adjudicação” de contratos (Szabo, 1997).

Embora a utilização de *smart contracts* seja popularmente implementada em ambientes de *blockchain*, não se trata de tecnologias necessariamente interdependentes. Note-se que a primeira (Szabo, 1997) é mais antiga que a segunda (Nakamoto, 2008). Uma vantagem do uso da tecnologia de *blockchain* conjuntamente aos *smart contracts* decorre de aquela representar uma implementação corrente de criptografia, mas outros ambientes – mesmo não criptográficos – podem ser utilizados para tanto. Por exemplo, as mesmas garantias legais utilizadas pelos Estados (e.g. via INPI) podem suprir as necessidades que geralmente se enfrentam por meio de *blockchain*.

Diversas soluções em *blockchain* suportam a implementação de *smart contracts* por meio de programação simples (Buterin, 2014). Em particular, a *blockchain* Ethereum utiliza exclusivamente a tecnologia de *smart contracts* para sua operação (Ethereum Foundation, 2015). Esse caso de uso é especialmente expressivo, pois a criptomoeda associada a essa *blockchain* e operada pelos *smart contracts* nela embarcados, a Ether, na data consultada durante a escrita deste documento está capitalizada em mais de 316 bilhões de dólares.

Portanto, se trata de ambiente no qual já são alienados bens com valores agregados positivos. De fato, “*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” (Dyrhovden, 2019, p. 6, tradução nossa)²⁴. A respeito especificamente de transferência de tecnologia,

[...] 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).

24 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).

ANÁLISE E DISCUSSÃO DOS RESULTADOS

Considerações Iniciais

Partindo-se da ideia do emprego de *smart contracts* embarcados em sistemas de *blockchain* como ferramenta para transferência de ativos intangíveis protegidos por Propriedade Intelectual, o projeto almejou, inicialmente, investigar oportunidades desses sistemas para registro e transferência desses ativos. Especificamente, imaginou-se investigar a pertinência da adoção desses sistemas para aplicação específica no contexto de registro e transferência de bens protegidos por Propriedade Intelectual e,, potencialmente, aprimorar sistemas existentes pela incorporação de outras tecnologias consolidadas na computação, como as Provas de Conhecimento-Zero. Ainda na formulação do problema de pesquisa identificou-se o efetivo emprego eficaz desses sistemas, geralmente sem modificações ou incorporação de outras tecnologias, aplicados em relação a todos os ativos intangíveis protegidos por direitos de Propriedade Intelectual com natureza de exclusividade ou monopólio jurídicos. Notadamente, não foi identificado emprego dessas ferramentas em relação a ativos intangíveis cuja exclusividade não decorre de serem juridicamente constituídos ou declarados; mas, sim, como decorrência fática.

Desta forma, o escopo limitou-se aos segredos industriais, por serem objeto da matéria da Propriedade Intelectual (em detrimento e.g. de segredos em geral) e também a mais economicamente relevante dentre as demais com características semelhantes (e.g. conhecimentos tradicionais). Limitado o escopo a este objeto de estudo, decidiu-se explorar a própria natureza dos segredos industriais. Sendo eles por definição “segredos”, optou-se por excluir o uso das tecnologias para registro, focando-se exclusivamente na transferência desses ativos, partindo-se do pressuposto que etapas anteriores (valoração da tecnologia, por exemplo) e posteriores à transferência (manutenção de cláusulas contratuais) são resolvidas entre as partes, de formas já experimentadas.

Método Proposto

O emprego de Provas de Conhecimento-Nulo, especificamente, permite a comprovação de que o potencial revelador do segredo de fato detém o segredo e pode revelá-lo. Por sua vez, a transferência final ocorre apenas após estágio intermediário, no qual o potencial adquirente confirma ao sistema seu convencimento de que o revelador de fato detém o conhecimento e tem condições de transmiti-lo ao adquirente. Dessa maneira, resolvem-se pelo mesmo método os problemas da capacidade e da confiabilidade (Leppälä, 2013), de forma harmônica, em um método simples.

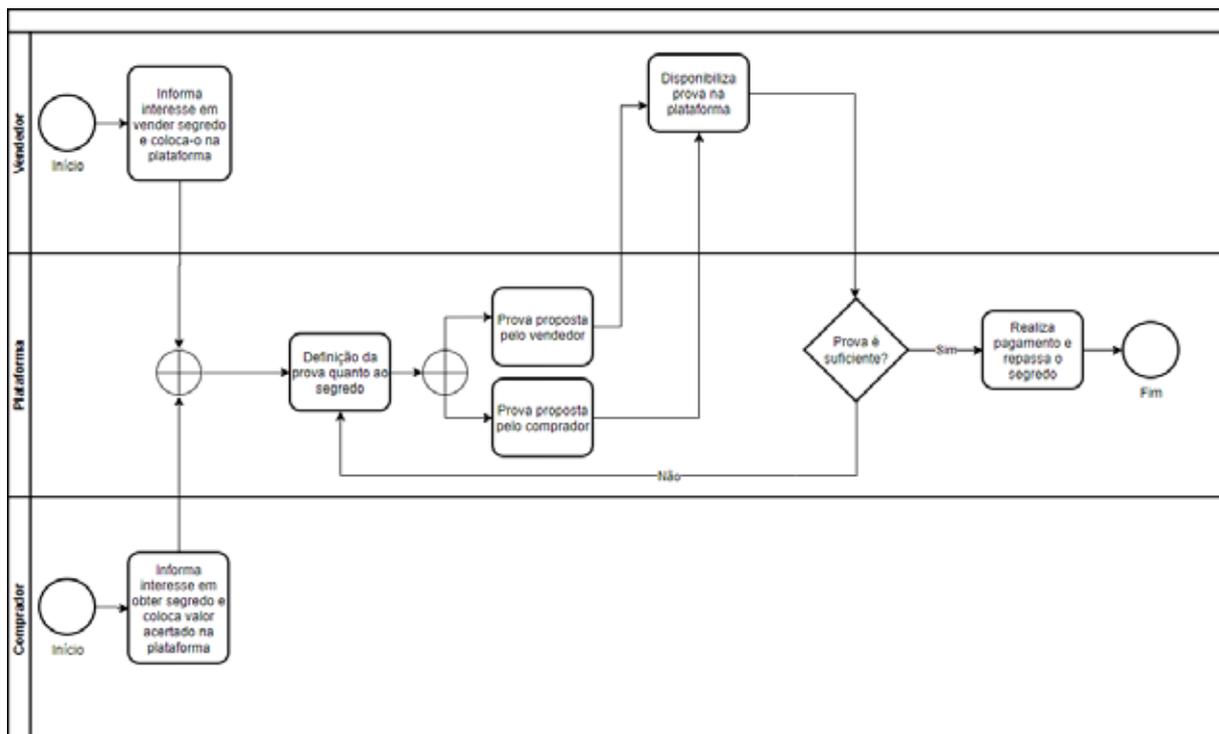
A execução do método pressupõe que o ativo a ser transferido possa ser e de fato tenha sido previamente avaliado por ambas as partes do negócio (os potenciais revelador e receptor), o que, por sua vez, depende de relativa inexistência de assimetria de informações

sobre a capacidade de valoração do bem, ou seja, a capacidade de identificação da utilidade do conhecimento pelas partes, sua relevância (Leppälä, 2013). De fato, conforme (Baron, 2019), a utilização de *smart contracts* “[...] ajuda a limitar [...] assimetrias de informação”. O método apresentado pressupõe que a parte interessada no segredo já tenha informação (independentemente de sua confiabilidade) de que o segredo existe e o potencial revelador o possui (indo-se mais além, em casos em que o segredo já está previamente disponível na plataforma de troca, configurando uma oferta pública do segredo, essa suposição é dispensável). Por decorrência lógica, o método pressupõe mínima simetria de informações entre as partes (ver Akerlof, 1970) sobre o valor do conhecimento para si mesmos. Desta forma, presumida a relevância, restam dois elementos fundamentais do Paradoxo a serem superados: a capacidade e a confiabilidade.

Algoritmo do Método

Visualmente, o algoritmo (série de instruções) do método pode ser representado conforme apresentado na figura 1.

FIGURA 1–Fluxograma apresentando o método proposto.



Fonte: Elaborada pelos autores .

Presentes esses pressupostos, atinentes à existência de informação sobre o segredo e conhecimento do valor ou negociação, o método inicia pelos atos de informação do interesse em transacionar, por ambas as partes. É necessário que ambas, colateralmente, demonstrem o interesse em transacionar, mesmo que assincronamente. Se houver, em determinado

tempo, coexistência dos interesses das duas partes (isso é, se simultaneamente houver interesse), segue-se ao próximo passo do método, que é executado automaticamente pelo *smart contract*.

O detentor de conhecimento secreto deve transformá-lo em um ou mais arquivos digitais, e hospedá-los no ambiente pertinente (conforme a instanciação), fazendo da criptografia e dos mecanismos tecnológicos de proteção normais para guarda de segredos industriais. Em seguida deve, por meio do *smart contract*, registrar referências a esses arquivos, ou os próprios, na *blockchain* ou ambiente equivalente escolhido.

Paralelamente (e não necessariamente concomitantemente) o potencial receptor do segredo deve depositar saldo em uma carteira vinculada ao *smart contract*, como requisito para prosseguimento. Essa carteira é livremente acessível pelo potencial receptor, que pode livremente dispor de seus fundos durante toda a execução do *smart contract*, até a sua derradeira etapa.

Se houver, em determinado tempo, coexistência dos interesses das duas partes (isso é, se simultaneamente houver interesse), segue-se ao próximo passo do método, que é executado automaticamente pelo *smart contract*. Essa inicial troca de informações feita pelo *smart contract* é o começo da execução do método. O início é disparado apenas na presença concomitante de dois estímulos: a existência de um registro que remeta a um segredo (que indica interesse por parte do potencial revelador); e a execução do *smart contract*, por um interessado, com menção à referência que identifica esse segredo (que indica interesse por parte do potencial receptor).

Em seguida, para satisfação do potencial adquirente sobre a existência de capacidade, a plataforma automaticamente requisita ao potencial revelador prova do conhecimento. Essa prova, que é a informação a que se refere o Paradoxo da Informação de Arrow, pode já haver sido hospedada previamente, ou ser fornecida ainda nesse estágio, permitindo às partes deliberar sobre a informação a ser transmitida como prova. Em qualquer momento o potencial revelador pode submeter as Provas à plataforma, que automaticamente as repassa ao potencial adquirente para avaliação, e registra na *blockchain* referência a essa transação.

Caso o potencial receptor se satisfaça pelas Provas, e deseje prosseguir com a transação, deve confirmar sinalizar isso ao *smart contract*. Ao receber essa confirmação, o *smart contract* verifica se há saldo suficiente na carteira do adquirente e a existência do arquivo contendo o segredo no servidor remoto. Na presença de ambos os bens, o *smart contract* automaticamente e simultaneamente transfere o segredo ao adquirente e o pagamento ao revelador. Finalmente, o *smart contract* registra na própria *blockchain* o histórico das operações, a fim de consolidá-las de maneira pública e imutável. Assim, conclui-se a execução do método.

Note-se que todos os passos, conforme aqui descritos, são apenas os referentes ao Método em si. Trata-se de descrição que tem como referencial o Método, ao qual é irrelevante o contexto externo em que sua execução é operada, inclusive o conhecimento das partes que o operam. De maneira alguma pode-se inferir que as partes não se conheçam ou não

tenham mantido contato por outros meios. Em especial, a troca inicial de informações de interesse e contato eletrônico, por meio do *smart contract*, não significa que as partes careçam de tais informações. Trata-se apenas de informação à plataforma, para que possa realizar sua funcionalidade; não necessariamente sendo essas informações novas às partes.

Superação do elemento da capacidade

Neste estágio ainda são operados dois dos três elementos do Paradoxo identificados na literatura (Leppälä, 2013): a capacidade do vendedor (a probabilidade de deter o conhecimento e ser capaz de transmitir informação sobre ele), e sua confiabilidade (a probabilidade de revelar tal conhecimento e de transmitir informações fidedignas a seu respeito).

Para a resolução do Paradoxo da Informação de Arrow em negociações de segredos industriais, uma estratégia utilizada é a revelação de informações intrínsecas ao conhecimento, porém de forma que o conhecimento em si não seja inteiramente transmitido – portanto, o receptor não efetivamente o adquire sem custo. Essas informações, em geral, dependem de presunção de veracidade por parte do recipiente (portanto, boa-fé do revelador), o que incorre no elemento da confiabilidade.

De fato, contextos específicos relativos às partes ou ao mercado em que estão inseridas, como a dependência na reputação nos mercados de capitais, no Vale do Silício, e na biotecnologia, possibilitam que essas empresas revelem informações intrínsecas ao conhecimento, embora não o revelando em si (Burstein, 2013), como forma de superação parcial do Paradoxo. No caso, o contexto de confiança inerente às partes e ao meio representa incentivo à presunção de veracidade das informações prestadas pelo revelador, lastreadas em sua reputação, e nos efeitos negativos que a falsidade dessas informações geraria ao revelador (Burstein, 2013). Portanto, nesses casos específicos, a capacidade pode ser presumida pelo adquirente, representando risco diminuído.

Alternativamente, o próprio conhecimento pode ser fracionado, e sofrer uma série de revelações parciais, o que parcialmente supera o Paradoxo; mas essa prática é solução imperfeita, pois a revelação parcial reduz o valor do *know-how* não revelado remanescente (Anton; Yao, 2002), o que representa desincentivo para a transmissão do conhecimento.

Para superação do elemento da capacidade pelo Método, o potencial revelador também deve disponibilizar, ao potencial receptor, informações como demonstração da existência do conhecimento e de seu domínio. Portanto, aplica-se o uso de informações intrínsecas ao conhecimento em si, mas que não o revelem, em detrimento e.g. de revelações parciais sucessivas, para que não ocorra efeito negativo no valor (Anton; Yao, 2002). A inovação instituída pelo Método, para superação da capacidade, consiste no uso dessas informações intrínsecas ao conhecimento como meio de prova (em detrimento de presunção), independentemente de particularidades das partes ou das indústrias em que se inserem, como a dependência na reputação do revelador. Nesse Método, a superação do elemento da capacidade é feita pelo emprego das Provas de Conhecimento-Nulo.

Especificamente, utiliza-se a introdução de informação intrínseca ao conhecimento. Essa informação necessariamente deve ter a característica de ser passível de ser gerada apenas pelo detentor do conhecimento, mas diferente dele e sem a possibilidade de operação inversa (isso é, uma informação que seja necessariamente produto do conhecimento secreto; que partindo da qual não se possa deduzir ou inferir o conhecimento em si). Igualmente, a Prova deve ser passível de compreensão pelo adquirente. Ou seja: pressupõe capacidade de compreensão da informação, e seu valor probatório, por ambas as partes. Deve, portanto, constituir efetiva prova (compreensível como tal pelas partes), em detrimento de presunção, e independentemente de externalidades contextuais.

Para caracterizar Prova de Conhecimento-Nulo, estritamente, informação admissível como essa Prova deve consistir em um efeito que necessariamente dependa do conhecimento secreto, como demonstração inequívoca de seu domínio pelo revelador – a sua capacidade. Não basta a mera informação sobre um resultado – e.g. revelar os resultados sobre eficácia e toxicidade de um composto, que com base na reputação do revelador são presumidos verdadeiros pelo adquirente (ver Burstein, 2013).

A solução pelo emprego de Provas de Conhecimento-Nulo é comparativamente mais geral que as encontradas na literatura, por ser independente de características de mercado (portanto tende a ter maior aplicabilidade fática), e por ser aplicável a conhecimentos não passíveis de fracionamento. Ademais, a existência dos efeitos da reputação, não é anulada, e inclusive contribui para a superação do elemento da capacidade (e do elemento da confiabilidade quanto às informações, em certos casos, como será analisado adiante). Não se trata de circunstância e método mutuamente exclusivos, mas sim de elementos que se somam. Portanto, essa inovação trazida pelo Método configura-se solução em si suficiente, que também pode configurar solução incremental nos casos de existência de outras.

Admitidamente, trata-se também de uma solução simples (embora não trivial) em comparação ao delineamento de estratégias de revelação com base em cálculos de equações diferenciais e estatística bayesiana (Anton; Yao, 2002; Leppälä, 2013), descritas na literatura. Justamente essa característica (a ausência de necessidade de formulação de estratégias complexas dependentes de conhecimentos raros) torna o Método proposto uma ferramenta comparativamente mais fácil de acesso à tecnologia. Considerando-se que a falta de compreensão do próprio Paradoxo representa barreira de entrada para negócios sobre Segredos Industriais (Leppälä, 2013), e que a resolução desse Paradoxo por essas técnicas é uma barreira maior que a sua não compreensão em si (porque logicamente a resolução depende de sua compreensão), o método tende a atingir mais *stakeholders* do que as soluções existentes, diminuindo o limiar da barreira de acesso. Ademais, como ocorre com as anteriormente identificadas, as soluções com base em cálculo diferencial e o Método proposto podem ser aplicados complementarmente, não havendo desvantagem na aplicação desse Método, complementarmente a elas, para a superação do elemento da capacidade.

A respeito da acessibilidade do Método, e em relação ao elemento da confiabilidade, explicita-se que a aplicação de Provas de Conhecimento-Nulo é comum no contexto da

computação, sendo um método amplamente utilizado em ambientes de controle de acesso de usuários com privilégios. São mecanismos na prática incorporados em algoritmos de autenticação de usuários (“*logins*”) como prova de identidade), em comunicação máquina-a-máquina. Existente esse contexto, a familiaridade de programadores com essa técnica e o seu uso disseminado também contribui para que o método seja mais facilmente instanciado em *smart contracts* e auditável por uma pluralidade de profissionais e amadores já existente. Relacionado a isso, por se tratar de tecnologia em estágio de desenvolvimento avançado, já aplicada e testada extensivamente, existe relativamente menor risco inerente ao desconhecimento sobre potenciais efeitos prejudiciais. Relacionalmente, aponta-se que há sinergia entre a utilização de Provas de Conhecimento-Nulo e *blockchain*, na medida em que a execução de transações criptografia por chaves públicas, utilizada na *blockchain*, emprega método similar ao das Provas de Conhecimento-Nulo para validação da transação de criptomoedas, especificamente na prova da identidade do transferidor.

Superação do elemento da confiabilidade

Primeiramente, ressalta-se que a aplicação de Provas de Conhecimento-Nulo, além de resolver o problema da capacidade quanto ao conhecimento secreto, também resolve o problema da confiabilidade quanto à informação utilizada nessas provas. Isso porque se a informação consiste em efetiva prova (e é compreendida como tal pelas partes), essa informação é por definição confiável ao seu receptor.

Quanto à confiabilidade relativa ao conhecimento (a probabilidade de o revelador transmitir o conhecimento, e em contrapartida o seu adquirente pagar por esta transmissão), o Método resolve o problema por garantir que o segredo incluído pelo potencial revelador será automaticamente transferido, em fase posterior, concomitantemente ao pagamento. Após disponibilizada a prova, o potencial adquirente deve considerar que a informação disponibilizada como prova é suficiente para garantir a capacidade e a confiabilidade, pressupostos da transação. Trata-se de uma garantia futura que serve para superar o problema relativo a esse pressuposto ainda nessa fase inicial.

Pela natureza do funcionamento da *blockchain*, a perfectibilização dos passos desde a confirmação das provas até as transferências finais e registro do histórico ocorrem de fato simultaneamente. Isso porque todas essas informações são realizadas em um único bloco, e o tempo de suas ocorrências corresponde à data e horário precisos (o *timestamp*) da mineração desse bloco. Desta maneira, supera-se a confiabilidade quanto às efetivas entregas; o cumprimento das obrigações sinalagmáticas.

Permanece existente a possibilidade de um revelador de má-fé manter nesse arquivo informação diversa do segredo. Isto é: de os dados fornecidos pelo suposto revelador, e entregues ao receptor, não corresponderem ao conhecimento pretendido. Entretanto, a boa-fé não necessita ser pressuposta. Mesmo em casos de má-fé, o Método é útil à resolução da confiabilidade.

Crucialmente, pois o uso de *blockchain* também propicia um registro público com prova temporal, característica essencial à tecnologia de *blockchain* (Nakamoto, 2008; Buterin, 2014; Clark, 2018). Isso garante ao receptor a possibilidade de disputar, inclusive judicialmente, a veracidade das informações prestadas como Provas (portanto tornando irrelevante, *ex post facto*, a assimetria de informações fundamental ao Paradoxo), bem como a entrega efetiva e completa do conhecimento secreto, e a relação das informações com o conhecimento. Portanto, o emprego de *blockchain* em relação a todas as informações faculta ao receptor eventualmente prejudicado a possibilidade de comprovar, a quem ele quiser, que a entrega final não corresponde ao conhecimento, ou que pelo seu conteúdo não pode se chegar aos mesmos resultados demonstrados pelas Provas de Conhecimento-Nulo. Dessa forma, supera-se o elemento da confiabilidade quanto a todos os dados – as informações prestadas como Prova, o conhecimento em si, e o nexos entre eles. Assim, o caráter público da transação permite que receptor eventualmente prejudicado comprove a fraude, seja extrajudicialmente (e.g. pela influência dos fatores externos de pressão reputacional), seja judicialmente (com base no Direito).

Portanto, a incorporação da tecnologia de *smart contracts* conforme aplicada no Método serve para superar o elemento da confiabilidade nas informações prestadas como Provas para a superação do elemento da capacidade. Igualmente, também supera o elemento da confiabilidade quanto ao pagamento, pelo adquirente, ao revelador, por garantir o cumprimento da contraprestação pecuniária pelo recebimento do segredo.

Além da inerente segurança dessas ferramentas, seu uso pode acabar por dispensar, a exemplo das soluções jurídicas supracitadas, a necessidade de terceiros para perfectibilizar ou validar a referida negociação. Isso em si elimina a eventual necessidade de revelação a mais pessoas. Note-se que, do ponto de vista de um terceiro (qualquer pessoa estranha à negociação com acesso ao bloco), esses dois possíveis objetos – um conhecimento criptografado em si, ou o caminho para encontrá-lo – são indistinguíveis entre si, em um fenômeno de *security by obscurity*.

Finalmente, como para-efeito benéfico, a referência ao conhecimento secreto registrada na *blockchain* pode ser utilizada como prova de anterioridade e.g. em processos de nulidade de patentes, como demonstração da inexistência de novidade. Igualmente, como sinalização da capacidade de inovação do detentor do conhecimento, da mesma maneira como a “[...] Propriedade Intelectual pode servir como um ‘sinal’, congregando muitos usuários complementares” (Burstein, 2013, p. 243, tradução nossa)²⁵. Note-se que essa sinalização não necessariamente depende da revelação do segredo, sendo perfeitamente adequadas as Provas de Conhecimento-Nulo – o que possibilita a geração de valor (pela sinalização) independentemente da perda do valor do segredo (por sua revelação).

Em harmonia, como outro para-efeito desejável, a própria natureza pública da negociação pelo Método torna-se possível (independentemente do grau de certeza) presunção

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

de que o potencial revelador não esteja simultaneamente negociando a revelação do segredo com uma pluralidade de potenciais adquirentes pelo mesmo método público. Assim, introduz-se a influência dos fatores externos de “atribuição e reputação”, que representam incentivos para a transmissão de informações e conhecimentos de modo confiável, cuja presunção é maneira como alguns mercados superam os efeitos do Paradoxo (Burstein, 2013), em especial quanto à confiabilidade.

Ademais, conforme discorrido, a exclusividade é fator de que depende o potencial preço, pois representa a diferença entre um mercado oligopolístico e um mercado em livre competição. Por decorrência, o menor risco sobre a exclusividade (portanto, sobre o valor do conhecimento) pode representar perspectiva (conquanto não expectativa) de segurança; que pode gerar incentivo às partes a negociar. Isso é especialmente relevante em casos de mercados grandes e anônimos, em que “[...] 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, tradução nossa)²⁶.

CONCLUSÕES

O método proposto neste trabalho pode ser adotado para superação do Paradoxo da Informação de Arrow, com aplicabilidade geral, seja com plena eficácia por si só ou de maneira complementar a outras soluções. O emprego de Provas de Conhecimento-Nulo e o emprego de *smart contracts* instanciados em *blockchain* possibilitam a resolução concomitante de dois dos três elementos fundamentais do Paradoxo, em muitos casos suficientes para sua superação: a capacidade e a confiabilidade.

Em tese, o método pode ser aplicável a demais tipos de conhecimentos secretos ou restritos, como os segredos comerciais, talvez dependente de modificações. Entretanto, trata-se de aplicação a objeto com características diversas, que não compuseram o escopo do projeto, e, portanto, não foram especificamente enfrentadas durante o desenvolvimento desse método. Ausente a proteção industrial conferida pelos tratados internacionais e legislação de segredos industriais, esses outros tipos de segredos dependem de contratos que estipulem confidencialidade como obrigação da parte receptora (o que não pode ser presumido ou verificado consistentemente e com alto nível de confiança) ou outros artifícios para superação de problemas específicos a esses tipos de conhecimentos, o que torna incertos os pressupostos específicos do método relatado (a superação do elemento da utilidade e a existência de garantias legais específicas aos segredos industriais), potencialmente causando problemas pela dependência na existência, validade e eficácia desses acordos. Portanto, sendo essas verificações extrínsecas ao nosso método, a aplicabilidade dele a segredos em geral pode ser prejudicada. Ainda quanto ao escopo de aplicação, por fim, segredos de

26 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).

Estado ou militares não costumam ser transacionados; quando são, não costuma se operar o Paradoxo resolvido pelo nosso método, porquanto tende a haver capacidade e confiabilidade – por esse motivo, nosso método também não é desenvolvido para fins dessa aplicação.

A criação de uma *blockchain ad-hoc* para a implementação de transações de segredos industriais potencialmente eliminaria a barreira de acesso imposta pelos custos inerentes às *blockchains* já existentes. Isso porque tradicionalmente o incentivo para que os pares minerem novos blocos é a geração de certa quantidade da criptomoeda associada à *blockchain*. Isto é: ao minerar um novo bloco, o minerador gera para si quantidade pré-determinada da criptomoeda associada a *blockchain* em específico, o que é escrito no próprio bloco minerado. Esse incremento monetário, entretanto, não decorre de necessidade técnica; apenas representa incentivo aos mineradores para que realizem a operação da *blockchain*. Outros incentivos podem ser empregados em substituição, de modo a eliminar o custo monetário relacionado. Entretanto, a criação de *blockchains ad-hoc* incorre no conhecido *bootstrap problem*. Em síntese, trata-se da situação paradoxal de que a segurança de uma *blockchain* depende de sua adoção por uma pluralidade de pares, porém essa adoção massiva recursivamente só ocorre quando os mesmos potenciais pares nela identificam segurança.

Embora tenha se levado em conta todo o estado da arte, por meio de pesquisas extensivas durante todo o projeto, mesmo durante as fases finais de desenvolvimento, pelo Método desenvolvido não se busca substituir ou aprimorar os demais artifícios existentes para superação do Paradoxo da Informação de Arrow. Trata-se de uma proposta completa e suficiente em si mesma (uma ferramenta *standalone*), implementável em ambientes já existentes propícios, independentemente da existência de outros métodos, modelos, técnicas ou estratégias. O Método constitui ferramenta independente de outras soluções, e que pode ser aplicada em conjunto a elas.

Futuros estudos podem focar na comparação de outros métodos existentes no estado da arte para negociação em geral, e como tornar esses métodos aplicáveis a segredos industriais, com base nos resultados aqui relatados. Sugere-se também a investigação da possibilidade de métodos que envolvam as etapas negociais e pré-contratuais, que gerem vantagens ao método desenvolvido por nós. Por fim, também é possível pesquisa e desenvolvimento de métodos semelhantes melhor aplicáveis a segredos em geral, ou segredos de outras naturezas específicas, como os segredos de empresa ou comerciais. Futuras pesquisas também podem buscar quantificar a demanda reprimida que pode ser aproveitada pela adoção do Método. Futuros desenvolvimentos podem consistir na criação de outros métodos, ou suas instanciações em ambientes diversos, e.g. com foco na segurança. Novas versões do Método podem ser desenvolvidas, com modificações ou adições de outros elementos, e.g. a inclusão de instrumentos contratuais padronizados gerados pelo *smart contract* e registrados na *blockchain*, como passo final.

REFERÊNCIAS

AKERLOF, G. A. The market for “Lemons”: quality uncertainty and the market mechanism. **The Quarterly Journal of Economics**, [s. /], 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. /], 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. Disponível em: http://www.oabrs.org.br/arquivos/file_55d349cb980bb.pdf. Acesso em: 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. Disponível em: <https://halshs.archives-ouvertes.fr/halshs-02111603>. Acesso em: 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. Disponível em: sol.sbc.org.br/index.php/mssis/article/view/7563. Acesso em: 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. Disponível em: benkler.org/Free%20as%20the%20Air.pdf. Acesso em: 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. Disponível em: heinonline.org/HOL/LandingPage?handle=hein.journals/tlr91&div=12&id=&page=. Acesso em: 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. Disponível em: wipo.int/wipo_magazine/en/2018/01/article_0005.html. Acesso em: 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. Disponível em: ieeexplore.ieee.org/abstract/document/7945805. Acesso em: 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. Disponível em: ethereum.org/en/whitepaper/. Acesso em: 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. Disponível em: <https://cyber.harvard.edu/people/ffisher/iptheory.pdf>. Acesso em: 13 Jan. 2021.

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

KÖLVART, 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. Disponível em: https://orca.cardiff.ac.uk/77948/1/e2013_2.pdf. Acesso em: 10 ago. 2021.

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

NAKAMOTO, S. **Bitcoin: a Peer-to-Peer Electronic Cash System**. [S. l.], 2008. Disponível em: bitcoin.org/bitcoin.pdf. Acesso em: 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. Disponível em: <http://www.cs.wisc.edu/~mkowalc/628.pdf>. Acesso em: 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. Disponível em: <https://ieeexplore.ieee.org/document/9093015>. Acesso em: 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. Disponível em: arxiv.org/pdf/1912.10370. Acesso em: 10 ago. 2021.