B979 Busnello, Felipe Octaviano Delgado

Método para transferência de segredos industriais por meio de Smart Contracts / Felipe Octaviano Delgado Busnello – Porto Alegre, 2022.
59 f. : il., color.

Orientador: Dr. Erik Schüler
Coorientador: Dr. Anderson Ricardo Yanzer Cabral

Dissertação (mestrado) – Instituto Federal do Rio Grande do Sul Campus Porto Alegre, Mestrado em Propriedade Intelectual e Transferência de Tecnologia para a Inovação, Porto Alegre, 2022.

1.Propriedade industrial. 2. Transferência de tecnologia. 3. Smart contracts. I. Schüler, Erik. II. Cabral, Anderson Ricardo Yanzer. III. Título.

CDU: 347.77

Elaborada por Débora Cristina Daenecke Albuquerque Moura - CRB10/2229

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO SUL – IFRS

Programa de Pós Graduação em Propriedade Intelectual e Transferência de Tecnologia para a Inovação – ProfNit

FELIPE OCTAVIANO DELGADO BUSNELLO

MÉTODO PARA TRANSFERÊNCIA DE SEGREDOS INDUSTRIAIS POR MEIO DE SMART CONTRACTS

PORTO ALEGRE – RS

2022

FELIPE OCTAVIANO DELGADO BUSNELLO

MÉTODO PARA TRANSFERÊNCIA DE SEGREDOS INDUSTRIAIS POR MEIO DE SMART CONTRACTS

RELATÓRIO TÉCNICO CONCLUSIVO

Relatório técnico conclusivo sobre método para transferência de segredos industriais por meio de *smart contracts* apresentado ao Programa de Pós Graduação em Propriedade Intelectual e Transferência de Tecnologia para a Inovação do Ponto Focal do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul, como requisito para obtenção do título de Mestre em Propriedade Intelectual e Transferência de Tecnologia para Inovação.

Dr. Erik Schüler (Orientador)

Dr. Anderson Ricardo Yanzer Cabral (Co-orientador)

PORTO ALEGRE – RS

2022

FELIPE OCTAVIANO DELGADO BUSNELLO

MÉTODO PARA TRANSFERÊNCIA DE SEGREDOS INDUSTRIAIS POR MEIO DE SMART CONTRACTS

RELATÓRIO TÉCNICO CONCLUSIVO

Relatório técnico conclusivo sobre método para transferência de segredos industriais por meio de *smart contracts* apresentado ao Programa de Pós Graduação em Propriedade Intelectual e Transferência de Tecnologia para a Inovação do Ponto Focal do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul, como requisito para obtenção do título de Mestre em Propriedade Intelectual e Transferência de Tecnologia para Inovação.

Dr. Erik Schüler (Orientador)

Dr. Anderson Ricardo Yanzer Cabral (Co-orientador)

Dra. Kelly Lissandra Bruch (Membro Interno / UFRGS)

Dr. Irineu Afonso Frey (Membro Externo / UFSC)

Dr. Milton Lucídio Leão Barcellos (Membro Externo)

PORTO ALEGRE – RS

2022

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ETH Ether

Mb Megabyte

RESUMO

No estado da técnica 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 estes 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 em sua transferência. Este fenômeno prejudica a potencial transferência de segredos industriais e inviabiliza a adoção dos sistemas existentes aplicáveis aos demais tipos de ativos intangíveis. Por este trabalho propõe-se um método para transferência de segredos industriais, em resolução ao Paradoxo da Informação de Arrow, para solução de dois dos três elementos componentes do Paradoxo, especificamente a *confiabilidade* e a *capacidade*, pressupondo o terceiro, a *relevância*. Utilizando-se de *smart contracts* instanciados em *blockchain*, e também provas de conhecimento-nulo, o Método é capaz de realizar o proposto. Testes feitos em ambiente controlado concluem pela viabilidade tecnológica do método, e as simulações de transferências realizadas indicam sua utilidade.

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

ABSTRACT

The state of the art contains systems for the transfer of intangible assets protected by intellectual property rights, consolidated by legal monopolies, be them attributive systems (such as patents and industrial designs) or reliant on automatic protection (such as copyright and neighbouring rights). Some of these systems, or their respective methods, are described in the scientific literature. Of this set, some methods employ *blockchain* technology, and a smaller subset also employs *smart contracts* technology, despite both technologies being mutually independent. Although trade secrets also constitute monopolies, computerized solutions or cryptographic environments used for other types of goods protected by other forms of intellectual property can not be transferred to these assets, due to their *sui generis* nature, lacking of monopoly regardless of its non-disclosure. The need for maintenance of secrecy is due to Arrow Information Paradox, the phenomenon by which the disclosure of the secret constitutes by itself its transference. This phenomenon impairs the potential for transference of industrial secrets and prevents the adoption of the existing systems applicable to other types of intangible assets. Through this work a method for transferring industrial secrets is proposed, for resolving two of the three component elements of the Paradox, namely *capability* and *reliability*, and presupposes the third, *relevance*. By using *smart contracts* embarked in a *blockchain*, as well as zero-knowledge proofs, the proposed Method is capable of delivering the proposed result. Tests conducted in a controlled environment conclude for the technological viability of the method, and the simulations indicate its usefulness.

Keywords: trade secret; Arrow Information Paradox; *smart contract*; *blockchain*; technology transfer.

SUMÁRIO

1. 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 (SAMULI, 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), 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 este motivo, o escopo deste trabalho trata destes segredos em específico.

---

[1] Expressões latinas referentes ao escopo do alcance, em especial de obrigações. *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.

Em casos de transferência de conhecimento, como é o caso de segredos industriais, um conceito basilar de sua teoria é o Paradoxo da Informação de Arrow, identificado pelo economista Kenneth Arrow[2] (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). Tradicionalmente, de modo a possibilitar negócios desta natureza, este 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; SAMULI, 2013; BURSTEIN, 2013). São, respectivamente, os monopólios ou outros direitos garantidos por Estados (no Brasil em especial pela Lei 9.279), e os contratos que envolvem cláusulas de confidencialidade ou exclusividade (BURSTEIN, 2013). Todos se tratam 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 parcial dos efeitos do Paradoxo depende de análises econômicas dos pontos de equilíbrio negociais relativos às revelações (ANTON *et al.*, 1998) e aplicação de modelos econômicos específicos a cada situação (SAMULI, 2013). Em decorrência das diferenças entre mercados, “as condições sob as quais um

[2] Vencedor do Prêmio Nobel de Ciências Econômicas de 1972

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), o que implica em 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 esta informação seja revelada), pode ser resolvida pelo emprego de Provas de Conhecimento-Nulo, ou Provas de Conhecimento-Zero. Tratam-se de técnicas pelas quais uma pessoa pode provar à outra que detém um conhecimento, sem transferir informação que o revele (WANG *et alii*, 2021). Estas provas geralmente consistem em demonstrações, feitas pelo detentor do conhecimento, mediante resoluções de problemas que não poderiam ser resolvidos sem o domínio deste 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. Este 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 alii*, 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" (KÕLVART *et alii*, 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).

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 nestas tecnologias com aplicação específica à Transferência de Tecnologia já foi vislumbrada como possibilidade de fato. Constata-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 alii*, 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. Considerando-se 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 (SAMULI, 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 comprovem 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.

Após a programação de protótipo, constatou-se a viabilidade tecnológica do método. Verificou-se a possibilidade de programação e execução do método no ambiente proposto; em linguagem computacional em meio informatizado.

2. OBJETIVOS

2.1. Objetivo Geral

O objetivo geral deste trabalho é desenvolver uma solução para transferência de segredos industriais utilizando-se *smart contract* embarcados em *blockchain*, baseado na utilização de Provas de Conhecimento-Nulo, levando-se em conta as limitações impostas pelo Paradoxo de Arrow.

2.2. Objetivos Específicos

Especificamente, por este trabalho buscam-se os seguintes objetivos:

- Propor um método passível de implementação em plataforma computacional, que auxilie na solução do problema da capacidade de

provar que o conhecimento existe, o revelador o detém e é capaz de transmiti-lo.

- Propor um método passível de implementação em plataforma computacional, que auxilie na solução do problema da confiabilidade na revelação de informações fidedignas e conhecimento útil ao receptor.

- Propor um método passível de implementação em plataforma computacional, que solucione o problema da confiabilidade no pagamento pelo conhecimento transferido.

- Desenvolver o método proposto (na forma de um Produto Mínimo Viável - PMV) em um *smart contract*, na *blockchain* Ethereum; bem como testá-lo e avalidá-lo, em ambiente controlado, como prova de conceito.

3. REFERENCIAL TEÓRICO

O referencial teórico está subdivido 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*.

3.1. 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*[3]

[3] 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

de exclusividade futura: os próprios direitos de Propriedade Intelectual (SCOTCHMER, 2004, BURSTEIN, 2013).[4] Fundamentalmente, quando constituídos juridicamente, estes 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 estas inovações (FISCHER, 1987).

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. Isto 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.[5]

Segredos de indústria são ativos relacionados à propriedade intelectual, sobre "qualquer matéria que possa ser mantida em segredo" (SCOTCHMER, 2004). Nas palavras de Denis Borges Barbosa (2010), "não se trata de um direito exclusivo, pois não houve concessão pelo Estado de uma patente ou algo do mesmo efeito." Em sua natureza, o segredo industrial não é um direito de

---

configuração de posição dominante no mercado quando certo agente ou grupo passa a representar mais de 20% ou mais de algum mercado.

[4] Garantias futuras, amplamente utilizadas em direitos positivos e negócios jurídicos diversos, são a base da teoria utilitária da Propriedade Intelectual. Conforme esta teoria, as garantias de monopólios temporários a criadores, por parte dos Estados, se justificam como incentivos de estímulo à criação de obras e invenções que em tese não seriam criadas sem a garantia de monopólio futuro – *i.e.* se um mercado em livre competição não seria adequado para que o criador recuperasse seu investimento – o que tende a resultar em efeito positivo ao bem-estar social (FISCHER, 2001).

[5] Utiliza-se o duplo negativo neste conceito porque a língua portuguesa não contém artifício para denotar a relação lógica "*non nunquam*" (*lit.* "não nunca"): a não-adjunção que não implique em disjunção. Denis Borges Barbosa (2013), ao comentar sobre um conceito cuja fonte latina utiliza "*nonnumquam*", resolveu a estrutura frasal como "(...) de fabulação, *se não* de ficção." Embora "se não" seja possível, neste caso pela pragmática a frase "incentiva se não desincentiva" denotaria sentido diverso do aqui exposto, errôneo, de que a ausência de desincentivo implicaria em incentivo. O conceito crucial (necessário para a compreensão de todo este artigo) é o de que a ausência de direitos "não elimina, bem como também 'não não elimina' o incentivo, embora ambos os efeitos, ou nenhum, possam ocorrer" – *i.e. non nunquam*.

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.

Pelo ponto de vista do detentor, o propósito direto da manutenção de um conhecimento como segredo é a manutenção da exclusividade. Esta 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 destes 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 deste 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). 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 destes 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).

Mesmo ausente monopólio juridicamente constituído, existe proteção contra a apropriação desautorizada de segredo industrial, 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 n.º 9.279/96, 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 (...)”.

Portanto, apenas a “relação contratual” é requisito para esta 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). Notadamente, estão ausentes menções a contrato formal[6] – como os

[6] Embora não exista necessidade de instrumento contratual para a proteção contra o uso desautorizado de conhecimentos confidenciais utilizáveis na indústria, por pessoa que a ele teve acesso mediante relação contratual, a mesma Lei estipula a necessidade de registro destes instrumentos para que produzam efeitos fora desta relação: “Art. 211. O INPI fará o registro dos contratos que impliquem transferência de tecnologia, contratos de franquia e similares para produzirem efeitos em relação a terceiros.” Em congruência, o Ato Normativo INPI nº 135/97 estipula, em seu art. 2.º, que “O INPI averbará ou registrará, conforme o caso, os contratos (...) de aquisição de conhecimento tecnológico”. Estes efeitos, entretanto, não

"Contratos de Revelação Confidencial" (BURSTEIN, 2013), – a disposição expressa em instrumento contratual, ou a aceite solene sobre obrigação de confidencialidade.

Em decorrência desta proteção *sui generis*, "os segredos industriais permitem aos seus detentores suprimir conhecimento" (SCOTCHMER, 2004), em aparente discrepância à teoria utilitária, e em efeito negativo ao desenvolvimento econômico. A mitigar este 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, estes negócios encontram óbice fático.

3.2. 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). 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" (SAMULI, 2013).[7]

---

incluem a garantia do art. 195 da Lei 9.279/96, que expressamente limita seu escopo ao "acesso mediante relação contratual ou empregatícia".

[7] Prossegue o autor comentando que este aspecto "é onde a distinção entre informação e conhecimento fica aparente" (SAMULI, 2013). Embora as demais fontes de nosso referencial teórico não façam distinção entre os termos, e o presente trabalho independa da clareza destas definições, neste relatório o termo "informação" em geral se refere a dados sobre o segredo (que permitam sua avaliação ou indiquem características suas ou do seu detentor), em detrimento do conhecimento em si. Especificamente sobre esta confusão em BENKLER, 1999, ver HAMILTON, 2000.

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). Portanto, não há custo de produção agregado a “uma unidade de conhecimento”, o que implica em 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. 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).[8] Por completude, também referimos que uma situação de livre concorrência[9] tende a resultar em um preço igual ao custo marginal (BENKLER, 2006), que no caso de conhecimento corresponde unicamente ao custo de comunicação deste segredo – que também corresponde a zero (BENKLER, 1999). Este 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” (SAMULI, 2013), conforme também identificado por Arrow (ARROW, 1962).

---

[8] *Cf.* BENSEN, 2012, conforme citado em BURSTEIN, 2013, sobre esse efeito nos casos em que a informação é parcialmente exclusiva, *i.e.* não apenas em livre concorrência.
[9] Idem.

Entretanto, efetivamente constata-se um potencial reprimido para o aproveitamento comercial de conhecimentos protegidos por segredos industriais, causada pelo Paradoxo da Informação de Arrow (BURSTEIN, 2013; SAMULI, 2013; SCOTCHMER, 2004; ANTON *et al*, 1998). 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*" (SAMULI, 2013). 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 (SAMULI, 2013; e ver AKERLOF, 1970). Ergo, a resolução deste Paradoxo ou 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,[10] 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), em razão do Paradoxo (ARROW, 1962) e da sua natureza como bens públicos (no sentido econômico) – não rivais e não escassos[11] (BENKLER, 1999 e 2006).

---

[10] O custo adicional, ou incremental, por unidade produzida.

[11] Conceitos econômicos. Rivalidade denota a impossibilidade de uso de certo bem simultaneamente por uma pluralidade de pessoas; a escassez denota a finitude da disponibilidade de um recurso em determinado tempo. *E.g.*, um copo d'água é um bem rival, porquanto o uso por uma pessoa prejudica que outras tenham acesso a ele, simultaneamente; e escasso, pois quanto maior o consumo de água por uma pessoa, menor a quantidade de água restante para as demais (ou para si mesmo). Em geral, essas características possibilitam que o valor de um bem seja maior que o de seu custo marginal, quando há demanda. Bens imateriais, no entanto, geralmente constituem *bens públicos*, *i.e.* não-rivais e não-escassos. Uma obra literária, por exemplo, pode ser utilizada simultaneamente por uma infinidade de pessoas (portanto não é rival), e o seu uso não implica em consumo: a quantidade de usos não afeta a existência ou disponibilidade da obra (portanto não é escassa). A propriedade intelectual confere rivalidade a bens públicos, e a possibilidade de seu titular a eles atribuir também escassez, de modo a proporcionar a possibilidade de seu valor não corresponder exatamente à soma de seu custo marginal – que no caso desses bens é zero – e seu custo de transmissão. Para maior aprofundamento sobre estes conceitos, e sua relação à Propriedade

Em um contexto amplo, a ocorrência deste este Paradoxo tende a criar barreiras de entrada para negócios cujo objeto é a transferência de segredo industrial. Neste estado, a 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. Este é um fenômeno de falha de mercado, pois “para que ideias beneficiem a sociedade, elas precisam ser desenvolvidas e comercializadas" (BURSTEIN, 2013).

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), 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).

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 (SAMULI, 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 destes conhecimentos (BURSTEIN, 2013).

Intelectual, ver ARROW, 1962; AKERLOF, 1970; BENKLER, 1999 e 2006; e SCOTCHMER, 2004.

As características elementares do Paradoxo, seus elementos constitutivos, são (SAMULI, 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.

Estas são características de cujas superações a transferência de segredos industriais depende, pois cujas presenças implicam na 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 e SCOTCHMER, 2004) até a não conclusão de um negócio em razão da incerteza gerada pelo Paradoxo (SAMULI, 2013). Neste contexto, quando pela perspectiva de futura ocorrência do Paradoxo de Arrow não há incentivo para que o detentor do segredo o oferte, os negócios sobre estes bens dependem da introdução de 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 Bayesiano para descobrir os incentivos relativos entre as partes, e determinar o Equilíbrio de Nash (SAMULI, 2013; ANTON *et al*., 1998) ou Equilíbrio Bayesiano Perfeito (ANTON *et al*., 1998) para estes incentivos. Por estes 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, esta prática trata-se de solução imperfeita, que não elimina o efeito do Paradoxo, pois "a revelação parcial reduz o valor do *know-how* não revelado remanescente" (ANTON *et al*., 1998), sobretudo considerando-se que o somatório dos valores das partes não necessariamente corresponde ao valor de todo conhecimento. Salienta-se que estas 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). 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), possibilitando que "a empresa de biotecnologia possa revelar informação *a respeito* do composto sem revelar o composto em si" (BURSTEIN, 2013), e o contexto reputacional deste mercado atribui presunção de veracidade desta 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 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 esta confidencialidade puder ser inferida (BURSTEIN, 2013), – exclusividade, e não-competição. Trata-se de acordos feitos entre as partes envolvidas, para assegurar entre elas a manutenção do *status quo* quanto às possibilidades de aproveitamento do segredo, apesar de seu conhecimento ser revelado. Todos se tratam de recursos jurídicos amplamente utilizados em matéria de Propriedade Intelectual e Transferência de Tecnologia. Estes 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 aos 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; e 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, carente 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, "*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; e ANTON *et al*., 1998).

O emprego de soluções técnicas para este 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" (SAMULI, 2013), pois "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)." 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 seriam necessárias" (ANTON *et al*., 1998).

A implementação de métodos que possibilitem esta 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 a inexistência de tecnologia que confira perfeita exclusividade aos conhecimentos proprietários, a adoção de meios técnicos para estes 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 “secreto”, 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 a criptografia, como as Provas de Conhecimento-Nulo. Estes 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.

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 do destes 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.[12] Simetricamente, a falsidade da afirmação “D2” implica na inexistência de “D1”.[13]

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 isto seja compreensível por “B”. Isso 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 isto 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.

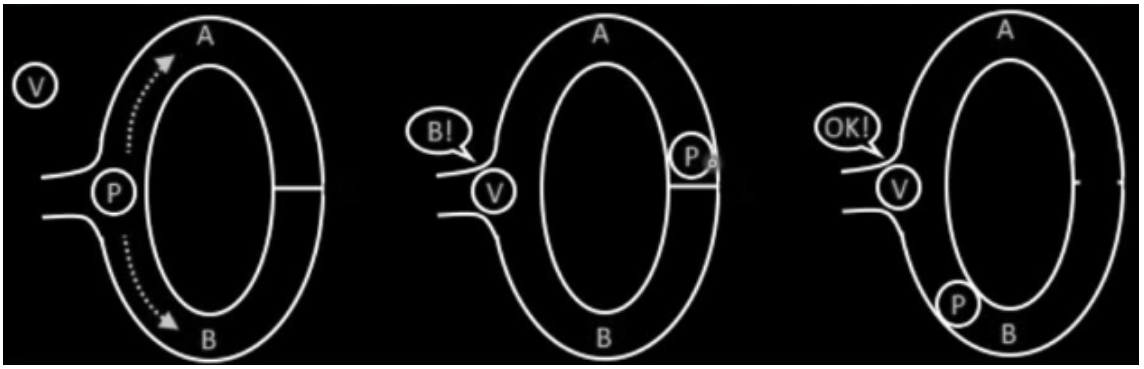
O conceito pode ser explicado por célebre anedota: em uma hipotética caverna composta de dois túneis distintos, apenas uma porta secreta os liga. Pessoas leigas que entrem em qualquer dos túneis podem apenas voltar pelo mesmo caminho, porém existe um detentor do conhecimento sobre a porta de ligação. 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 esta 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 esta tarefa com sucesso, e por conseguinte prova aos leigos a

[12] Na lógica proposicional, esta é a inferência *modus ponens*: “Se ‘P’, então ‘Q’. ‘P’. Então, ‘Q’.“ Em referência ao texto: “Se ‘P’ (a existência de D1) é verdadeiro, então ‘Q’ (a afirmação da existência de ‘D1’) é verdadeiro. ‘P’ (D1 existe) é verdadeiro. Então ‘Q’ (a afirmação da existência de D1 é verdadeira).

[13] Em paralelo, esta inferência *modus tollens*: “Se ‘P’, então ‘Q’. Não ‘P’. Então, não ‘Q’.“ Em referência ao texto: “Se ‘P’ (a existência de D1) é verdadeiro, então ‘Q’ (a afirmação da existência de ‘D1’) é verdadeiro. ‘P’ (D1 existe) é falso. Então ‘Q’ (a afirmação da existência de D1 é falso).

possibilidade, sem transmitir qualquer conhecimento (QUISQUARTER *et al*, 1990). A figura 1 apresenta tal explicação ao caso da caverna.

Figura 01. Explicação do conceito de Prova de Conhecimento-Nulo.



(Fonte: Varutra Consulting)

Figura 01. Explicação do conceito de Prova de Conhecimento-Nulo.

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.

3.3. *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) neste ambiente; ou, do ponto de vista da informática, “protocolos de transação computadorizados que implementam as disposições do contrato” (KÕLVART *et alii*, 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 enfrenta 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). Este caso de uso é especialmente expressivo, pois a criptomoeda associada a esta *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, ou 1,6 trilhões de reais (valores de conversão calculados conforme preço médio de 15/03/2022).

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). 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 alii*., 2019).

4. 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. Esta revisão foi baseada em pesquisas nas plataformas Scopus, Web of Science, e ScienceDirect;

b) Desenvolvimento e apresentação de uma proposta do método;

c) Teste do método, em ambiente controlado, como prova de conceito; e

d) Avaliação do método por uso experimental.

Tratam-se de etapas conhecidas no desenvolvimento tecnológico, comuns no desenvolvimento de soluções informatizadas. Portanto, a metodologia proposta justifica-se por empregar os procedimentos logicamente necessários, também habituais neste tipo de trabalho.

Em consideração à revisão bibliográfica, pesquisas em bases de dados especializadas, por meio das palavras-chave “*trade secrets*” e “*smart contracts*” nos bancos de dados 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 destes temas.

Para levantamento das tecnologias existentes no estado da técnica, 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 SAMULI, 2013), bem como estratégias e técnicas em geral para (ver ANTON *et al.* 1998). Em especial, identificou-se não haver no estado da técnica método para a transferência de tecnologia protegida por segredos industriais utilizando-se soluções informatizadas ou em ambientes criptográficos (SANTOS, 2003; e BASSO *et al*., 2019), tampouco da potencial aplicação de novas tecnologias, como a *blockchain*, para fins semelhantes (CONOSCENTI *et alii*, 2016). Esta carência ocorre apesar da existência de demanda para conhecimentos protegidos por segredos industriais (SAMULI, 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), inclusive em repressão de demanda.[14] A aparente inexistência de método congênere, e sua potencial aplicabilidade, justificou a criação deste Método.

Paralelamente à revisão bibliográfica e de literatura cinzenta, que foi mantida durante todo o tempo do projeto, foi iniciado o desenvolvimento de método que pudesse resolver os elementos que causam o fenômeno do Paradoxo, com o objetivo de ser aplicado como ferramenta para a resolução do problema.

Para a criação de um método com potencial inovador, como proposto, logicamente cada etapa posterior depende de cada etapa anterior a ela. Para a validação do método por uso experimental é necessária a sua testagem, que por sua vez depende de seu respectivo desenvolvimento, que é necessariamente baseado no conhecimento do estado da arte. Inexistente método congênere, buscou-se desenvolver uma série de instruções para a resolução deste problema – mesmo que não necessariamente a mais eficiente

[14] A identificação de efetiva demanda reprimida não foi objeto de investigação específica, pois o referencial teórico (BURSTEIN, 2013; SAMULI, 2013; SCOTCHMER, 2004; ANTON *et al*, 1998; *et alia*; *et cetera*) pressupõe a sua existência, inclusive explicitamente: "a demanda por informações não reveladas é raramente inexistente" (SAMULI, 2013).

possível, ou um paradigma. Este objetivo foi definido como o *framework* do projeto, e por sua vez delimitou o seu escopo.

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 ferramenta *Draw Io*, disponível em <https://drawio-app.com/> 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.

Desenvolvido o fluxograma, foi descrito um *smart contract* para efetivamente implementar o fluxograma. Este *smart contract*, descrito em linguagem própria *Solidity*, foi desenvolvido com características de um PMV, ou seja, com características mínimas de funcionalidade que permitam a validação do método.

Além do *smart contract* em si, desenvolveu-se, também com características de um PMV, uma plataforma *web*, a fim de tornar “amigável” a relação entre as partes envolvidas na transferência do ativo. A referida plataforma foi descrita em linguagem *PHP*.

Finalmente, utilizou-se uma API (*Application Programming Interface*) para comunicação entre o *smart contract* e a plataforma *web*. A referida API, descrita em linguagem *Java*, é comumente utilizada para este tipo de interface entre diferentes aplicativos, tendo sido utilizada uma API já disponível, em código aberto.

A etapa de avaliação teve por princípio a utilização do método fora do ambiente controlado de testes. Ou seja, são simulados negócios jurídicos sobre segredos industriais pela aplicação no mundo real, em instanciações já existentes da

tecnologia de *blockchain* que permitam o uso de *smart contracts*. Preferencialmente, a *Ethereum*, que foi utilizada na etapa de testes.

Por constrições de tempo e necessidade de dispêndio financeiro[15] a validação em específico será feita futuramente. De qualquer forma, o ambiente controlado utilizado na etapa de testes é idêntico à verdadeira *blockchain* que emula (simula), a *Ethereum*. Por este motivo, considera-se que o próprio resultado positivo dos testes constitui sua avaliação.

5. RESULTADOS E DISCUSSÃO

5.1. 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

[15] Pelo próprio meio de funcionamento da blockchain, para embarcar o smart contract, e para executá-lo em uma transação, é necessário oferecer aos pares mineradores na Blockchain valores em criptomoeda. Estes valores são o incentivo para que os mineradores incluam a transcrição do *smart contract* e a transação com base nele no bloco minerado.

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 destes 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.

5.2. 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. Desta maneira, resolve-se pelo mesmo método os problemas da *capacidade* e da *confiabilidade* (SAMULI, 2013), de maneira 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,[16] ou seja, a capacidade de identificação da utilidade do conhecimento

[16] A respeito da assimetria de informações como elemento de formação de preço, ver AKERLOF, 1970. Sobre a valoração de um conhecimento poder ser diferente para diferentes

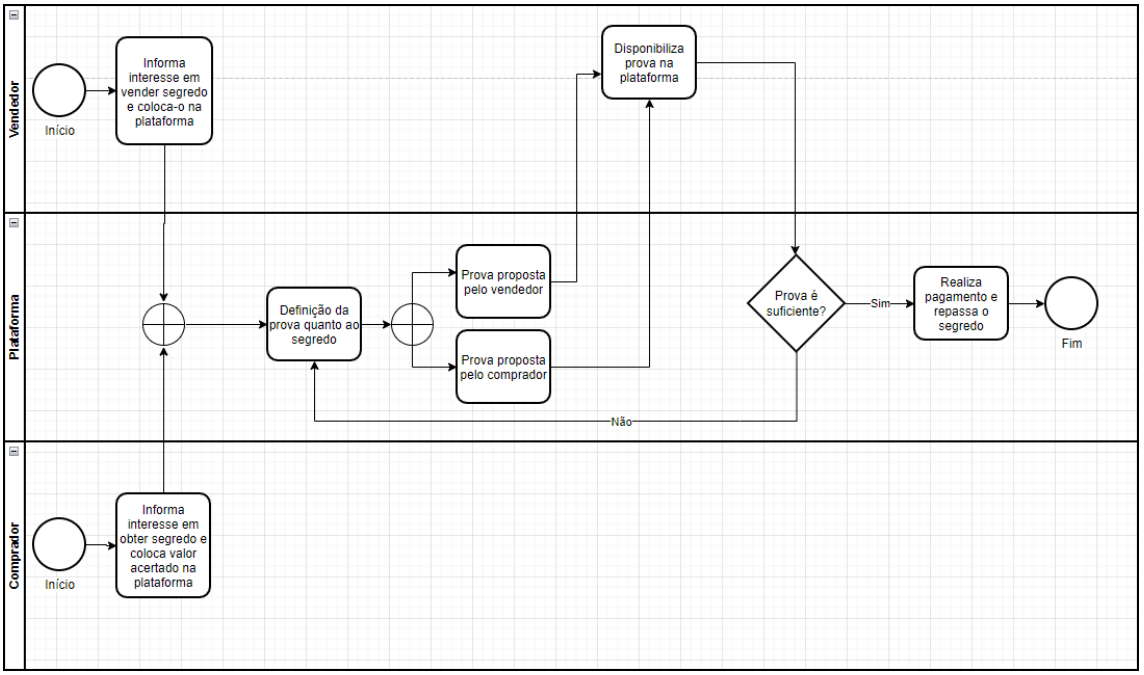
pelas partes, sua *relevância* (SAMULI, 2013). De fato, conforme (BARON, 2019), a utilização de *smart contracts* "...ajuda a limitar (...) assimetrias de informação". O método apresentado pressupõe que a parte interessada no segredo já tenha informação (independentemente de sua confiabilidade) de que 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, esta 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.*

5.2.1. Algoritmo do Método

Visualmente, o algoritmo (série de instruções) do método pode ser representado conforme apresentado na figura 02.

Figura 02. Fluxograma apresentando o método proposto.

agentes econômicos, e em caso de informação incompleta poder ser baseada em critérios como experiência passada e média de mercado, ver ARROW, 1962.



(Fonte: elaborada pelo autor)

Presentes estes 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 estes 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. Esta 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*. Esta inicial troca de informações feita pelo *smart contract* é o início 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 este 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. Esta prova, que trata-se da *informação* a que se refere o Paradoxo da Informação de Arrow, pode já haver sido hospedada previamente, ou ser fornecida ainda neste 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 a repassa ao potencial adquirente para avaliação, e registra na *blockchain* referência a esta transação.

Caso o potencial receptor se satisfaça pelas Provas, e deseje prosseguir com a transação, deve confirmar sinalizar isto ao *smart contract*. Ao receber esta 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 estes 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.

5.2.2. Implementação do *smart contract* e plataforma *web*

Devido à constrição de tamanho dos blocos nas *blockchains* existentes (na Ethereum, atualmente aproximadamente 2 Mb), o correspondente custo em criptomoeda para registrar o volume de dados correspondente a um bloco (na Ethereum, atualmente 5 ETH; aproximadamente R$75.000,00), pode em si representar barreira de acesso ao uso de método que dependa do registro dos dados exclusivamente em blockchain. Por esta razão, neste Método são empregados dois ambientes distintos para registro de dados.

Para implementação da estrutura, dividida entre uma *blockchain* e ao menos um servidor externo, é necessário que haja possibilidade de comunicação entre estes dois ambientes lógicos. Isto implica na necessidade de um meio de comunicação máquina-a-máquina entre o *smart contract*, consistente em um ambiente, e o servidor externo, consistente em outro. Esta comunicação é feita por meio de uma API (*Application Programming Interface*) embarcada na parte da plataforma hospedada externamente.

Especificamente, o *smart contract* com as instruções de operação do método (o *algoritmo*) deve ser escrito uma única vez na *blockchain*. Neste programa, sempre que seja necessário a incorporação de dados (no caso, o conhecimento e as informações), o *smart contract* se reporta a um servidor externo, onde se encontram.

Para que possam ser utilizados diversos servidores, a possibilitar que os próprios detentores dos conhecimentos secretos possam hospedar seus dados em seus próprios ambientes controlados (assim eliminando a necessidade de confiança em terceiro), ou em ambiente de terceiro em quem confiam, é necessário que haja mecanismo que possibilite este apontamento. Para isso, o *smart contract* pode ser programado de duas formas.

Por uma maneira, registra-se no *smart contract*, uma única vez, link direto a ambiente fora da *blockchain*, no qual está hospedado um índice com os endereços eletrônicos dos servidores em que estão hospedados os dados relativos a cada segredo. Quando executado, o programa acessa este índice, também enviando duas informações: qual segredo é procurado, e para onde o índice externo deve responder este endereço ao solicitante (seu contato eletrônico). Por sua vez, do lado do servidor externo, deve haver programa que, ao receber a requisição enviada pelo *smart contract*, consulte o índice e envie como resposta o endereço buscado ao contato indicado pelo potencial adquirente. Quando executado, o *smart contract* acessa este índice, também enviando duas informações prestadas a ele pelo usuário: qual segredo é procurado, e para onde o índice externo deve responder este endereço ao solicitante (seu contato eletrônico). Por sua vez, do lado do servidor externo, deve haver programa que, ao receber a requisição enviada pelo *smart contract*, consulte o índice e envie como resposta o endereço buscado ao contato indicado pelo potencial adquirente.

Por outra maneira, o *smart contract* deve conter código que permita a qualquer pessoa registrar, na própria *blockchain*, conjuntos dos seguintes dados: uma

identificação única para um segredo, e o endereço direto do servidor externo onde ele pode ser encontrado (em detrimento de um índice centralizado contendo todos os endereços). Desta maneira, a própria *blockchain* funciona como o catálogo de endereços. Quando executado, o *smart contract* repassa a este servidor duas informações prestadas a ele pelo usuário: qual segredo é procurado, e em que endereço eletrônico encontra-se o potencial adquirente.

Em resumo, no *smart contract* deve ser programada a funcionalidade de registro, em um bloco, de um endereço externo – que pode consistir em um único registro contendo o endereço de um servidor externo específico; ou múltiplos registros, criados por cada potencial revelador, a uma pluralidade de servidores. Desta maneira, o segredo em si existe em arquivo remoto, em um servidor específico, não necessariamente sendo em si escrito na *blockchain.*

Por este formato, o Método reserva o uso da *blockchain* apenas quando estritamente necessário. Além da ocorrência única da instanciação do *smart contract*, apenas três passos ocorrem neste ambiente: o passo inicial do potencial revelador, o do potencial receptor (e imediata execução do *smart contract* para troca de informações iniciais), e o passo final, de transferência sinalagmática. Isto acarreta que a *blockchain* seja utilizada os absolutos mínimos de vezes e volume de dados necessários para a superação do elemento da *confiabilidade*, sem prejuízo na eficácia do Método para tanto.

Com a troca de informações iniciais, correspondente ao início da execução do Método, forma-se a interface de comunicação necessária e comum a qualquer transação, que na instanciação por nós proposta (implementada, testada, e validada) ocorre por meio da plataforma. Os nexos de comunicação, ligações que correspondem ao caminho lógico das comunicações entre os elementos da plataforma, são os seguintes:

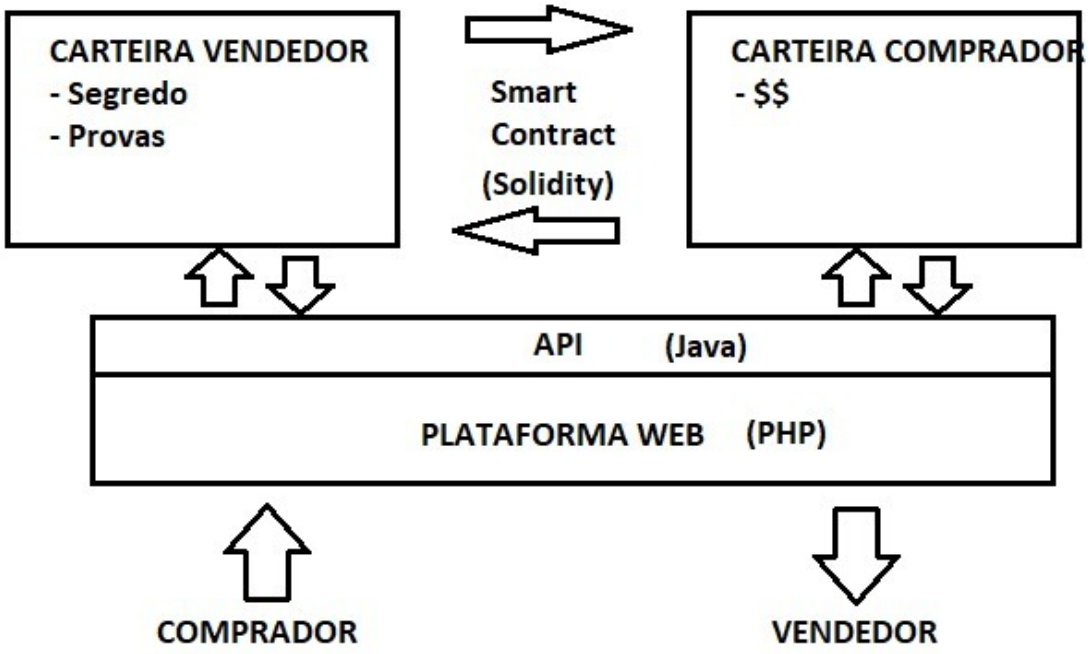
- Os potenciais revelador (“vendedor”) e adquirente (“comprador”) comunicam-se diretamente com a parte instanciada fora da *blockchain*: o programa que gerencia as referências (cujo *frontend*, sua interface

com os usuários, é a “plataforma web”; e em cujo *backend*, interface com o servidor, está embarcada a API para comunicação com a *blockchain*).

- O programa externo, “plataforma *web*” e “API”, comunicam-se diretamente com os pares da *blockchain*, na qual está embarcado o *smart contract*.
- Internamente, o *smart contract* gerencia a comunicação entre as representações do revelador (“vendedor”) e adquirente (“comprador”) na *blockchain*, consistentes em carteiras de suas respectivas propriedades.
- Na carteira do revelador (“vendedor”) constam como entradas o conhecimento secreto (“segredo”) e as informações utilizadas para superação do elemento da *capacidade* no Paradoxo, consistentes em Provas de Conhecimento-Nulo (“provas”); ou as referências a eles no servidor externo.
- Simetricamente, na carteira do adquirente (“comprador”) estão registradas as criptomoedas (“$$”) pertinentes à *blockchain* empregada.

Estas relações estão representadas na figura 03, onde são apresentadas, na forma de um diagrama simplificado, os blocos que formam a plataforma e as respectivas linguagens de programação utilizadas em cada um.

Figura 03. Estrutura para implementação e comunicação entre as partes.



(Fonte: elaborada pelo autor)

Todos os passos são realizados por meio desta interface.

5.2.3. Superação do elemento da *capacidade*

Neste estágio ainda operam-se dois dos três elementos do Paradoxo identificados na literatura (SAMULI, 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 adquira 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 estas 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 diminuto.

Alternativamente, o próprio conhecimento pode ser fracionado, e sofrer uma série de revelações parciais, o que parcialmente supera o Paradoxo; mas esta prática trata-se de solução imperfeita, pois “a revelação parcial reduz o valor do know-how não revelado remanescente” (ANTON *et al*., 1998), 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 *et al.*, 1998). 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. Neste 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. Esta 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).[17] 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 esta 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, *etc*. 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

[17] Sobre este fenômeno, ver em literatura da área das Ciências da Computação sobre o denominado “problema P versus NP". Em síntese, este problema refere-se à discrepância entre as dificuldades de cálculo inerentes a um algoritmo de *resolução* de um problema (mais difícil) e ao algoritmo de *verificação* desta resolução (mais fácil). É uma questão aberta nestas Ciências, que é relacionada (e provavelmente dependente) da veracidade da conjuntura matemática denominada Hipótese de Riemann. Diversas tecnologias, inclusive a própria criptografia utilizada na *blockchain*, pressupõem esta discrepância, e a veracidade da conjuntura mencionada; e também estes são dois dos seis problemas ainda não resolvidos cujas provas são elegíveis para prêmios de um milhão de Dólares. Este nível de abstração, entretanto, foge do escopo deste Método, portanto não será objeto de análise neste relatório técnico.

trata de circunstância e método mutuamente exclusivos, mas sim de elementos que se somam. Portanto, esta 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, *et al.*, 1998; SAMULI, 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 (SAMULI, 2013), e que a resolução deste Paradoxo por estas 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 deste 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 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 este contexto, a familiaridade de programadores com esta 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.[18]

5.2.4. 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 nestas provas. Isto porque se a informação consiste em efetiva prova (e é compreendida como tal pelas partes), esta 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

[18] Especificamente, a transação é realizada mediante uma espécie de assinatura digital. Esta assinatura consiste na multiplicação da soma da chave pública (escrita na blockchain) e sua mensagem, e da chave privada (mantida em segredo pelo proprietário das criptomoedas). O resultado desta operação é uma *hash* que necessariamente só pode ser produzida com o conhecimento de ambas as chaves, ou demandaria impraticável tempo de computação para ser replicado por tentativa e erro (ver nota de rodapé nº 17). Ao contrário, a verificação desse resultado é trivial a qualquer pessoa com base na chave pública, mas tal verificação não torna possível a descoberta da chave privada. (NAKAMOTO, 2008; BUTTERIN, 2014). Desta maneira, consiste em uma informação que necessariamente depende do domínio do conhecimento secreto – a chave privada – mas que não a revela. Portanto, entendemos que trata-se de método de prova semelhante ao incorporado ao Método, no mesmo ambiente também incorporado pelo Método, o que representa sinergia.

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 nesta 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 estas informações são realizadas em um único bloco, e o tempo de suas ocorrências corresponde à data e horário precisos (o *timestamp*) da mineração deste 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 neste arquivo informação diversa do segredo. Isso 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; BUTTERIN, 2014; e CLARK, 2018). Isto 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. Desta forma, supera-se o elemento da *confiabilidade* quanto a todos os dados – as informações prestadas como Prova, o conhecimento em si, e o nexo 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 destas ferramentas, seu uso pode acabar por dispensar, a exemplo das soluções jurídicas supracitadas, a necessidade de terceiros para perfectibilizar ou validar a referida negociação. Isto 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) estes 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). 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 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. Isto 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” (SAMULI, 2013).

5.3. Teste e avaliação

Para teste e avaliação, o Método foi programado em meio informático, utilizando-se a linguagem PHP em ambiente de servidores privados e simulação da *blockchain* Ethereum. Neste ambiente controlado foi replicada a interface descrita no item 5.2.2. para instanciação do Método.

Após a criação deste PMV, uma série de simulações foi realizada para testar diversos cenários de transferência de segredos industriais por este meio.

A mera criação do produto foi conclusiva pela viabilidade tecnológica do método. Especificamente, que ele pode ser transposto para linguagem

computacional, sendo algoritmo computável em meio informatizado. O produto criado serve como prova de conceito sobre o efetivo funcionamento do Método.

O resultado positivo do teste em ambiente controlado indica a viabilidade da adoção para efetivo emprego em aplicações reais. Dados desses usos poderão ser usados para avaliar sua utilidade para superação parcial do Paradoxo da Informação de Arrow em casos concretos, bem como o potencial aproveitamento de demanda reprimida (ver nota de rodapé 14) ou potencial impacto positivo nos valores dos bens negociados.

6. CONSIDERAÇÕES FINAIS

Embora não haja como prever mercados futuros baseados na demanda por informação (BENKLER, 2006; BURSTEIN, 2013; SAMULI, 2013), a adoção das técnicas utilizadas para superação dos elementos da *capacidade* e da *confiabilidade* podem radicalmente modificar o potencial deste mercado, pois "toda nossa compreensão da economia da informação esteve construída sobre o pressuposto tecnológico de que derrapagem[19] ocorre. Nós não temos ideia de como um mundo em que bens de informação sejam perfeitamente exclusivos —como os dispositivos de proteção tecnológica prometem torná-los— se parecerá" (BENKLER, 1999). A exemplo, antevendo possíveis mudanças de mercado, autores mencionam que em conjunto a "uma linguagem de representação comum para ativos denominada RAS++" as tecnologias de *blockchain* e *smart contracts* podem promover "a ruptura total na forma como se aborda credibilidade em relação a ativos, por meio de uma

[19] Embora o termo "slippage" (do original) ou "derrapagem" (em nossa tradução) seja geralmente empregado no contexto financeiro para definir a diferença entre o preço que uma parte espera o preço final do negócio, nesta fonte o autor parece utilizar o conceito de slippage em relação ao vazamento de conhecimentos (portanto, externalidades excepcionais à exclusividade), em detrimento do uso mais comum no contexto do mercado financeiro. Sobre outra "derrapagem" terminológica do autor, em sua obra de 1999, ver HAMILTON, 2000.

relação mais direta entre fábricas de software e micro-fornecedores de tecnologias” (BASSO *et alii*., 2019).

Este Método pode ser adotado para superação parcial 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* possibilita 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 deste método. Ausente a proteção industrial conferida pelos tratados internacionais e legislação de segredos industriais, estes 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 estes 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 destes 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 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 este motivo, nosso método também não é desenvolvido para fins desta 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 o 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 à blockchain em específico (*e.g.* 5 Ether, no caso da Ethereum), o que é escrito no próprio bloco minerado. Este 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*.[20] Em síntese, trata-se da situação paradoxal de que a segurança de uma *blockchain* depende de sua adoção por uma pluralidade de pares, porém esta adoção massiva recursivamente só ocorre quando os mesmos potenciais pares nela identificam segurança.[21]

Embora tenha se levado em conta todo o estado da técnica, 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, independente da existência de outros métodos, modelos,

[20] “Problema do cadarço das botas”, em alusão à impossibilidade de levantar-se pelos cadarços das próprias botas.
[21] A ocorrência deste fenômeno foi vislumbrada pelo Prof. Dr. Marco Conoscenti (o mesmo de CONOSCENTI, Marco *et alii*., 2016) em conversa privada com este pesquisador, realizada em 12 de março de 2021, pela plataforma Jitsi.

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 técnica para negociação em geral, e como tornar estes 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.

7. REFERÊNCIAS

ANTON, James *et al*. **The Sale of Ideas**: Strategic Disclosure, Property Rights, and Incomplete Contracts. 1998. Disponível em: <faculty.fuqua.duke.edu/~jja1/bio/PDF/salewp1298.pdf>. Acesso em: 10 de agosto de 2021.

ARROW, K. J. **The Economic Implications of Learning by Doing**. The Review of Economic Studies, 29 (3): 155-173, 1962. Disponível em: <jstor.org/stable/2295952>. Acesso em: 07 de abril de 2021.

_____. **Economic Welfare and the Allocation of Resources for Invention**, em Rate and Direction of Inventive Activity: Economic and Social Factor. Princeton: Princeton University Press, 1962.

BARBOSA, Denis Borges. **Do direito de propriedade intelectual das celebridades**, em Revista de Propriedade Intelectual - Direito Contemporâneo e Constituição, OUT/DEZ 2012. Aracaju: 2012.

_____. **Uma Introdução à Propriedade Intelectual**. Segunda Edição Revista e Atualizada. São Paulo: Lumen Juris, 2010.

BARCELLOS, César Alexandre Leão. Know How e Segredos Industriais, *in* **Cartilha da Propriedade Intelectual 2015** (org. Rodrigo Azevedo). Porto Alegre: Ordem dos Advogados do Brasil, Conselho Seccional do Rio Grande do Sul, Comissão Especial de Propriedade Intelectual, 2015. Disponível em: <http://www.oabrs.org.br/arquivos/file_55d349cb980bb.pdf>. Acesso em: 20 de fevereiro de 2022.

BARON, Richard; CHAUDEY, Magali. **Blockchain and Smart-contract: a pioneering Approach of inter-firms Relationships? The case of franchise networks**. 2019. Disponível em <https://halshs.archives-ouvertes.fr/halshs-02111603>. Acesso em: 13 de junho de 2022.

BASSO, Fábio Paulo *et alii*. **Automated Technology Transfer in MDE as a Service**: Experiences and Research Directions. Alegrete: UNIPAMPA, 2019. Disponível em: <sol.sbc.org.br/index.php/mssis/article/view/7563>. Acesso em: 07 de Abril de 2021.

BENKLER, Yochai. **Free as the Air to Common Use**: First Amendment Constraints o closure of the Public Domain, Nova Iorque: 74 N.Y.U. L. REV. 354, 1999. Disponível em: <benkler.org/Free%20as%20the%20Air.pdf>. Acesso em 10 de agosto de 2021.

_____, **The Wealth of Networks**: How Social Production Transforms Markets and Freedom. Londres: Yale University Press, 2006. Disponível em: <jstor.org/stable/j.ctt1njknw>. Acesso em: 09 de agosto de 2021.

BENSEN, James. **From Knowledge to Ideas**: The Two Faces of Innovation. Boston: Boston University School of Law Working Paper 10-35, 2012. Disponível em <http://www.bu.edu/law/faculty/scholarship/workingpapers/2010.html>. Acesso em 30 de janeiro de 2022.

BURSTEIN, Michael J. **Exchanging Information without Intellectual Property**. 91 Tex. L. Rev. 227, 2013. Disponível em: <heinonline.org/HOL/LandingPage?handle=hein.journals/tlr91&div=12&id=&page=>. Acesso em: 09 de agosto de 2021.

BUTTERIN, Vitalik. **A next-generation smart contract and decentralized application platform**. 2014. Disponível em: <https://translatewhitepaper.com/wp-content/uploads/2021/04/EthereumOrijinal-ETH-English.pdf>. Acesso em 10 de agosto de 2021.

CHANG, Ha-Joon. **Kicking Away the Ladder**: Development Strategy in Historical Perspective. Londres: Anthem Press, 2002.

CLARK, Birgit. **Blockchain and IP Law**: A Match Made In Crypto Heaven? WIPO Magazine 2018/1, 2018. Disponível em: <wipo.int/wipo_magazine/en/2018/01/article_0005.html>. Acesso em: 07 de Abril de 2021.

CONOSCENTI, Marco *et alii*. **Blockchain for the Internet of Things**: a Systematic Literature Review. Agadir: IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016. Disponível em:

<ieeexplore.ieee.org/abstract/document/7945805>. Acesso em: 09 de agosto de 2021.

DIAMOND, Jared. **Guns, Germs, and Steel**: the fates of human societies. Nova Iorque: Norton & Company, Inc., 1997.

DYRHOVDEN, Sindre. **Blockchain and Trade Secrets**: A Match Made in Heaven?. King's College London, 2019. Disponível em: <static1.squarespace.com/static/5bb3ced9b9144976a1d4cb49/t/5de67fbecd1f1d1da57d7829/1575387075162/Blockchain+and+Trade+Secrets+A+Match+Made+in+Heaven.pdf>. Acesso em: 07 de Abril de 2021.

ETHEREUM FOUNDATION. **Ethereum Whitepaper**. 2015. Disponível em: <ethereum.org/en/whitepaper/>. Acesso em: 07 de Abril de 2021.

FISCHER III, William W. **Theories of Intellectual Property**. New Essays in the Legal and Political Theory of Property. Cambridge, UK: Cambridge University Press, 2001. Disponível em: <https://cyber.harvard.edu/people/tfisher/iptheory.pdf>. Acesso em: 13 Jan. 2021.

HAMILTON, Marci. **A Response to Professor Benkler**, Berkeley: 15 Berkeley Tech, 2000. Disponível em: <lawcat.berkeley.edu/record/1117217/files/fulltext.pdf>. Acesso em 10 de agosto de 2021.

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

KÕLVART, Merit; PULLA, Margus; e RUUL, Addi. **Smart Contracts, em The Future of Law and eTechnologies**. Genebra: Springer. 2016.

LESSIG, Lawrence. **Code version 2.0**. Nova Iorque: Basic Books, 2006. Disponível em: <codev2.cc/download+remix/Lessig-Codev2.pdf>. Acesso em: 07 de Abril de 2021.

NAKAMOTO, Satoshi. **Bitcoin**: a Peer-to-Peer Electronic Cash System, 2008. Disponível em: <bitcoin.org/bitcoin.pdf>. Acesso em: 07 de Abril de 2021.

QUISQUARTER, Jean-Jacques; GUILLOU, Louis C.; BERSON, Thomas A. *et alia*. **Como explicar protocolos de conhecimento zero para seus filhos**. Advances in Cryptology — CRYPTO' 89 Proceedings. CRYPTO 1989. Lecture Notes in Computer Science, vol 435. New York: Springer. Disponível em: <http://www.cs.wisc.edu/~mkowalcz/628.pdf>. Acesso em: 07 de Abril de 2021.

SANTOS, Júlio César dos. **Propriedade Intelectual Com Ênfase em *Trade Secrets***: Criptologia, Performance Econômica. Vitória: Universidade Federal do Espírito Santo, 2003. Disponível em: <portais4.ufes.br/posgrad/teses/nometese_277_50-J%FAlio%20C%E9sar%20dos%20Santos.pdf>. Acesso em: 07 de Abril de 2021.

SAMULI, Leppälä *et alii*. **Arrow's Paradox and Markets for Nonproprietary Information**. Cardiff Economics Working Papers, No. E2013/2. Cardiff: Cardiff University, Cardiff Business School, 2013. Disponível em: <https://orca.cardiff.ac.uk/77948/1/e2013_2.pdf>. Acesso em: 10 de agosto de 2021.

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

SZABO, Nick. **Formalizing and Securing Relationships on Public Networks**. First Monday, 2(9), 1997. Disponível em: <doi.org/10.5210/fm.v2i9.548> Acesso em: 07 de Abril de 2021.

WANG, Dan *et alii*. **A Survey on Privacy Protection of Blockchain**: The Technology and Application.Internet of Things, Volume 8, 2019. Disponível em:

<https://ieeexplore.ieee.org/document/9093015>. Acesso em 10 de agosto de 2021.

ZHENG, Zibin *et alii*. **An overview on smart contracts**: Challenges, advances and platforms. Future Generation Computer Systems, 2019. Disponível em: <arxiv.org/pdf/1912.10370>. Acesso em: 10 de agosto de 2021.