3º PRÊMIO SECAP DE LOTERIAS

Concurso de Monografias

2019

3º LUGAR

Mercado de Loterias no Brasil: Concorrência, Governança e Responsabilidade Social na Era de Blockchain

Autor:
Roberto Domingos Taufick

Realização

Enap

FGV

Idealização

SECRETARIA DE **AVALIAÇÃO, PLANEJAMENTO, ENERGIA E LOTERIA**

SECRETARIA ESPECIAL DE **FAZENDA**

MINISTÉRIO DA **ECONOMIA**

Apoio

OAB CONSELHO FEDERAL Comissão Especial de Direito dos Jogos Esportivos, Lotéricos e Entretenimento

Patrocínio

loterias CAIXA

PÁTRIA AMADA BRASIL GOVERNO FEDERAL

3º PRÊMIO SECAP DE LOTERIAS - 2019

Tema: A Regulação de Loterias no Brasil e Aspectos de Responsabilidade Social Corporativa das Loterias

Subtema: Loterias no Brasil e a Fronteira Tecnológica

Mercado de Loterias no Brasil:

Concorrência, Governança e Responsabilidade Social na Era de Blockchain

ÍNDICE

Introdução

O estudo da regulação pela academia costuma levar em consideração um ambiente relativamente estático: presentes falhas de mercado com externalidades negativas, o regulador intervém, preferencialmente com o objetivo de simular condições verificáveis caso o mercado fosse competitivo. O avanço das tecnologias digitais deixou, porém, esse conceito ultrapassado: a tecnologia tem conseguido corrigir falhas de mercado que antes justificavam a regulação, ou imposto desafios para os quais a regulação posta não está equipada.

Segmentos antes monopolizados têm sido alvo preferencial dos inovadores. essa preferência é bastante intuitiva: se a teoria econômica há muito sustenta que a ausência de competição reduz a qualidade dos serviços e eleva os preços, são esses os mercados em que há maior espaço para que o entrante apresente serviços de melhor qualidade a preços mais baixos -- eventualmente dispondo de margem para, mesmo na condição de entrante, operar no azul.

Essa situação não é diferente para o segmento de apostas. O ultrapassado modelo de desconexão do mundo virtual, pouca transparência, pouca inovação, baixa satisfação do consumidor, baixa competição e elevadas barreiras à entrada foi cenário ideal para a inovação -- primeiro, dos modelos de jogos na rede de computadores (*online*); posteriormente, dos meios de pagamento por moedas virtuais (ou criptoativos, para os países que não reconhecem esses ativos como moeda); finalmente, de uma forma mais ampla, de todo o modelo de negócios.

O presente trabalho visa, na vanguarda regulatória mundial, trazer para a discussão no Brasil a implantação de uma regulação algorítmica em blockchain. E o momento não poderia ser mais oportuno: o Brasil está em movimento de abertura do mercado

de jogos à concorrência a partir de dois importantes segmentos. Nesse sentido, tanto a loteria instantânea, quanto a loteria de apostas de quota fixa foram objeto de autorização à exploração privada, promovendo-se seja uma competição interplataforma[1] (loteria instantânea), seja uma competição também intraplataforma[2] (apostas de quota fixa).

Como se poderá notar, a aplicação da tecnologia blockchain tem o potencial de facilitar o acesso às apostas de forma responsável, com os devidos cuidados para desincentivar o vício. A tecnologia ainda garante, por design, desde que submetida a regulação adequada, o cumprimento dos contratos, o pagamento dos tributos, além de permitir o fechamento do cerco contra a lavagem de dinheiro -- tudo a custos inferiores aos hoje existentes. Ao mesmo tempo, quando o regulador, valendo-se das características de um mercado que passa a contar com serviços de natureza marcadamente credencial, é capaz de implementar uma regulação algorítmica inclusiva (que vise legalizar os negócios que atendam aos requisitos legais e a circulação de criptoativos que atendam à regulação contra a lavagem de dinheiro), ele sinaliza ao mercado que, com a opções legalmente disponíveis no mercado, não é necessário correr riscos desnecessários no mercado paralelo, à margem da lei.

Este trabalho vem consubstanciado em farta doutrina internacional sobre blockchain e sobre a sua aplicação ao mercado de jogos. Para melhor didática, apresenta capítulos introdutórios sobre a tecnologia blockchain, sobre os seus usos potenciais e sobre como vem e pode vir a ser aproveitada no segmento de apostas. Por fim, após

[1] Como o modelo do art. 28, §1º da Lei nº 13.155, de 4 de agosto de 2015, prevê a concessão para um monopolista nessa modalidade, a competição acontecerá entre diferentes modalidades de apostas.
[2] O modelo da Lei nº 13.756, de 12 de dezembro de 2018, prevê concorrência entre diferentes atores autorizados a operar sob essa modalidade.

tecer breves considerações sobre a estrutura geral do mercado de loterias no Brasil, faz-se uma avaliação sobre como aquela tecnologia pode beneficiar também o mercado de apostas no Brasil.

Blockchain: o sistema descentralizado de autenticação, como idealizado

Em 2008 o artigo "*Bitcoin: A Peer-to-Peer Electronic Cash System*" foi publicado sob o pseudônimo Satoshi Nakamoto. Divulgado na esteira da crise financeira global de 2007, o escrito propunha usar a tecnologia, o sistema colaborativo em rede e a dispersão do poder de decisão como alternativa ao sistema financeiro centralizado. O artigo sugeria que o novo modelo reduziria a desconfiança no sistema financeiro, que a eliminação do intermediário[3] (a instituição financeira) reduziria os custos de transação -- possibilitando a inclusão de operações menos volumosas (os chamados micropagamentos) que eram afastadas pelos custos dos serviços bancários -, que o modelo de autenticação algorítmica reduziria os prazos de liquidação das operações. A respeito desse último ponto, para que se tenha uma ideia, Wright e De Filippi (2015) registram que, diversamente de outros sistemas de pagamentos existentes, os quais levam dias para transferir fundos, a moeda digital pode ser transferida ao redor do globo em pouco mais de sete minutos a taxas substancialmente inferiores às impostas pelos bancos[4].

A grande preocupação na criação da moeda digital -- *cryptocurrency* -- residia, naturalmente, na edificação de uma plataforma que garantisse a credibilidade das operações, resolvendo, em particular, o problema da duplicação dos ativos digitais (o

[3] "*Trusted third party*".

[4] *"Unlike existing payments systems, which generally take days to transfer funds, Bitcoin can be sent across the world in a little over seven minutes at fees that are drastically lower than those imposed by existing money transmitters, such as Western Union. All that is needed is an Internet connection and a computer or a simple mobile device."*

chamado gasto duplo, ou *double spending*). Como se sabe, os ativos digitais permitem a criação de cópias perfeitas, a sua multiplicação pela enésima potência e distribuição não represada. Daí que o grande mérito de Nakamoto foi criar uma plataforma que garantisse o reconhecimento e o mapeamento de qualquer procedimento que acontecesse com os ativos no âmbito da plataforma, levando a que qualquer duplicação pudesse ser auditada.

Para garantir a singularidade e a cronologia de cada operação, cada transferência de valor seria autorizada mediante a assinatura de uma chave privada e vinculada às chaves públicas de ambas as partes. Ao mesmo tempo, a plataforma assinalaria uma identidade alfanumérica (criptográfica, ou *hash*[5]) para a operação e iniciaria um sistema descentralizado de liquidação, cuja função seria autenticar operações que ocorressem no sistema. Segundo Nakamoto, uma moeda digital poderia, então, ser definida como uma cadeia de assinaturas: o possuidor da moeda a transferiria digitalmente (fazendo uso da sua chave privada criptografada), enquanto o sistema aporia a identificação da última operação (*hash*) e a chave pública do adquirente (também criptografada) ao final da criptografia da moeda.

Uma vez transferido o valor, seria, entretanto, necessário assegurar que aquela moeda não existe em duplicidade, ou seja, que não ocorreu um gasto duplo. Na ausência de um instituição financeira para liquidar esse valor e assegurar a autenticidade da operação, Nakamoto entendeu que a operação deveria ser tornada pública na plataforma para que os usuários a validassem: na pendência de duas

[5] Citando Pilkinton (2015):
"*A hash (output) is the result of a transformation of the original information (input). A hash function is a mathematical algorithm that takes an input and transforms it into an output. A cryptographic hash function is characterized by its extreme difficulty to revert, in other words, to recreate the input data from its hash value alone. This is called the collision resistance.*"

operações concorrendo pela mesma moeda, a cadeia mais longa de validação (maior quantidade de CPUs, ou de computadores) indicaria a operação que seria validada. Desse modo, qualquer computador com capacidade para processar uma operação poderia verificar a sua procedência e votar pela sua conformidade. Para desconstituir, ou reverter essa operação e outras que dela derivassem, seria necessário, nesse mesmo sentido, que um número superior de computadores aprovasse a substituição da cadeia anterior.

A criação de *hashes* e a autenticação dos blocos demanda, por sua vez, que os autenticadores compitam entre si em provas de trabalho braçal, ou mineração: os computadores que vencessem competições que exigem intensa capacidade computacional, ou intenso trabalho de processamento de dados (e, portanto, consomem muita energia elétrica), mas relativamente baixa capacidade de raciocínio (daí ser um trabalho braçal) seriam premiados com somas da moeda digital, como remuneração pelo trabalho e incentivo a trabalhar pelo desenvolvimento da plataforma[6]. Como bem resumido por Pilkinton (2015), à medida que a capacidade de mineração aumenta, a dificuldade do problema matemático a ser resolvido é ajustada para cima, de tal forma a manter a velocidade de geração do bloco constante, em cerca de dez minutos[7]. Esse modelo de governança baseado na capacidade computacional de resolver problemas matematicamente trabalhosos é conhecido

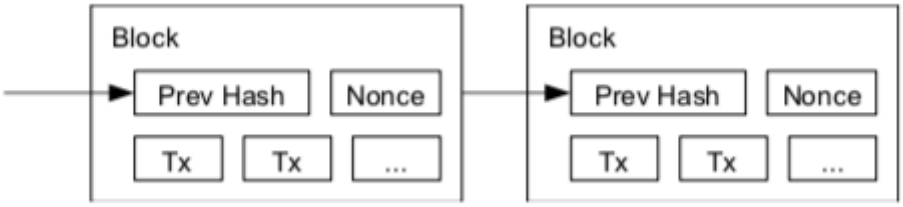
[6] Esse aspecto é reforçado, também, por Catalini e Gans (2019):
"This explains why Bitcoin and its blockchain are "joined at the hip": for the network to operate in a decentralized way without trusted intermediaries, the process of maintaining the shared ledger must generate enough of an incentive in bitcoin for attracting miners."

[7] "*The blockchain is a chain of transactional records that a subset of network participants (also known as 'miners') enriches by solving difficult computational problems. Miners fiercely (and anonymously) compete on the network to solve the mathematical problem in the most efficient way, thereby adding the next block to the blockchain. The block reward (i.e. newly minted coins) is sent to the miner's public address. If the miner wants to spend these coins, (s)he must sign with the corresponding private key. When system wide mining power increases, so does the difficulty of the computational problems required to mine a new block (Böhme et al, 2015, p. 218). This difficulty level is adjusted to keep the block-generation pace constant, roughly ten minutes (Dwyer, 2014, p. 5)*."

como *proof-of-work* e foi originalmente desenhado para o bitcoin. Como veremos, esse modelo veio a ser substituído por outras formas de governança, com diferentes trade-offs.

O trabalho do modelo de governança *proof-of-work* consiste em gerar um número de forma arbitrário, ou randômica (*nonce*) para ser usado uma única vez (identificação criptográfica única de cada bloco). Outro benefício da mineração reside em incentivar a rivalidade entre os nós, evitando que se alinhem contra a integridade do sistema. Ao final de cada prova, o bloco validado pelo maior número de autenticadores (ou *pool* de CPUs) terá a operação incluída na cadeia de operações da plataforma. Cada bloco é identificado por um *hash* que inclui tanto o *hash* do bloco anterior -- o que permite criptografar e identificar a sua precisa posição na cadeia de operações da plataforma -, quanto o *nonce* gerado pela mineração.

Figura 1. Identificação do bloco



Fonte: Nakamoto (2008)

Como definido pelo artigo, enquanto a maioria da energia das CPUs estiver controlada por autenticadores (ou nós) que não cooperem entre si para atacar a rede, essa maioria gerará a linha mais longa de autenticadores de cada operação e superará os ataques contra a sua integridade. A proposta repousa sob a ideia de que os

mineradores que autenticam cada operação sejam atomizados, sem nenhuma ligação permanente com a rede[8].

Como, para desconstituir, ou reverter uma operação, é necessário reverter todas aquelas que lhe sucedam -- o que exige muita energia e uma grande capacidade de coordenação entre os nós "desonestos" -, é possível concluir que a probabilidade de sucesso dos ataques diminui à medida que novos blocos são adicionados. Como bem delineado por Catalini e Gans[9]:

> "Caso um ator mal intencionado desejasse reverter uma operação pregressa, (e.g., uma guardada 'n' blocos atrás), teria de,para tanto, despender uma quantidade desproporcional de recursos."

A ordem dos acontecimentos na plataforma proposta por Nakamoto era a seguinte[10]:

Tabela 1. Cronograma da blockchain de bitcoin

1º	transações são transmitidas para todos os nós.
2º	cada nó analisa novas operações dentro de um bloco.

[8] "*Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone*."
[9] *"If a bad actor wanted to reverse a past transaction (e.g. one that is stored n blocks in the past), it would have to spend a disproportionate amount of resources to do so."*
[10] Todo esse processo é assim resumido por Pilkinton (2015):
"Blockchain technology ensures the elimination of the double-spend problem, with the help of public-key cryptography, whereby each agent is assigned a private key (kept secret like a password) and a public key shared with all other agents. A transaction is initiated when the future owner of the coins (or digital tokens) sends his/her public key to the original owner. The coins are transferred by the digital signature of a hash. Public keys are cryptographically generated addresses stored in the blockchain. Every coin is associated with an address, and a transaction in the crypto-economy is simply a trade of coins from one address to another. The striking feature of the blockchain is that public keys are never tied to a real-world identity. Transactions, although traceable, are enabled without disclosing one's identity; this is a major difference with transactions in fiat currencies that, with the exception of (non-traceable) cash transactions, are related to specific economic agents endowed with legal personality (whether physical or juridical)."

3º	cada nó busca resolver um trabalho de criptografia (mineração) para o seu bloco.
4º	ao concluir o seu trabalho de mineração, o nó transmite o bloco (em cujas operações estão as suas) para todos os nós.
5º	os demais nós só aceitam o bloco de todas as operações desse bloco forem válidas
6º	os nós demonstram aprovar o bloco em questão ao usarem o seu hash como prefixo do seu próximo bloco.

Fonte: elaboração própria, a partir de Nakamoto (2008).

A plataforma em questão veio a chamar-se blockchain e a moeda digital, bitcoin. Talvez a última característica relevante conhecida e ainda não mencionada de blockchain corresponde à proteção da privacidade. Se, por um lado, a plataforma exige a divulgação dos dados da operação -- de tal sorte a que a sua autenticação siga regras objetivas quanto à existência da operação e à disponibilidade da moeda usada para o pagamento -, por outro, a identidade das partes é preservada mediante o anonimato das chaves públicas. Nakamoto explica, ainda, quanto à possibilidade de que um nível adicional de privacidade seja acrescentado, por meio da inclusão de mais um par de chaves a proteger a identidade das partes. Entretanto, adverte ser sempre possível identificar o usuário, ainda que indiretamente, a partir da análise do histórico de todas as suas transações.

Catalini e Gans (2019)[11] ressaltam, entretanto, que, em razão de se tratar de uma tecnologia cujo uso ainda é bastante incipiente, novos protocolos já estão sendo desenvolvidos para elevar o grau de anonimato das transações. Essa habilidade de elevar o anonimato é, aliás, abordada por Haffke *et alli* (2019), segundo os quais o uso de tumblers[12] já permite, hoje, tornar praticamente impossível identificar a origem de uma transação[13].

> "Essa é uma das razões por que os usuários de blockchain demonstram um grande interesse em anonimizar as suas transações. Quando desejam tornar uma transação irrastreável, enviam tokens para serviços de tumbler. O tumbler simula um grande volume de transações enviando tokens de uma chave pública para outra. Todas essas chaves são mantidas pelo serviço tumbler. Na blockchain, essa troca é invisível. Como diversas pessoas usam tumblers para as suas transações, o tumbler mistura, assim, os tokens. Depois desse procedimento, o serviço envia outros tokens de volta para o usuário (geralmente para uma segunda chave pública também mantida por esse usuário), descontada uma taxa. Em blockchain, a origem dos tokens que passaram por um tumbler dificilmente pode ser rastreada. Assim, torna-se praticamente impossível usar as informações da transação para aplicar a lei.
>
> Outras formas de tumbler não enviam tokens de volta para o mesmo usuário. No lugar, são 'misturados' e enviados para terceiros a partir de pedidos do usuário. Desse modo, esse tipo de tumbler é usado como intermediário para a troca de tokens entre partes."

---

[11] "*While this is still an active area of research, new protocols are being developed to obfuscate transaction data, offer full anonymity to users through zero-knowledge cryptography, and implement different degrees of access to transaction information. Although perfect obfuscation might be not always possible to achieve,33 it is clear that different cryptocurrencies will be able to compete also in terms of the privacy level they provide to their users (either at the protocol level, or through a trusted intermediary)*."

[12] A melhor tradução seria "coqueteleiras", como aquelas usadas para misturar shakes.

[13] "*That is one of the reasons why Blockchain users have a strong interest in anonymising their transactions. If they intend to make a transaction untraceable, they send these tokens to a tumbler service. The tumbler then simulates a large number of transactions by sending the users' tokens from one public key to another. All those keys are held by the tumbler service. On the Blockchain, this fact is not visible. Because different people use a tumbler service for their transactions, the tumbler thus 'mixes' the tokens. After this procedure is complete, the tumbler service sends other tokens back to the user (commonly to a second public key also maintained by the user) and deducts a fee. On the Blockchain, the origin of tokens that went through a tumbler can hardly be traced back.33 Thereby, it makes it nearly impossible to use the transaction data for law enforcement.*
Other forms of tumbler services do not send tokens back to the same user from which they initially derived. Instead, upon request of the user and after the 'mixing-service', they are sent to a third party. Thus, this form of tumbler service is used as an intermediary within the transfer of tokens between two parties."

Blockchain e imutabilidade

Nakamoto (2008) construiu um sistema de autenticação inspirado na ideia de dispersão de poder (tecnologia *peer-to-peer*, ou P2P). A diversidade de CPUs autenticadoras criaria um sistema atomizado em que nenhum grupo econômico determinaria os resultados da autenticação, afastando-se, assim, conflitos de interesse que comprometessem a confiança no sistema. O modelo de autenticação de Sakamoto repousa, como antecipado, sob a ideia de que os autenticadores de cada operação seriam atomizados, com dedicação esporádica à mineração de blocos, e de que a dispersão de CPUs autenticadoras elevaria suficientemente os custos de coordenação visando a um ataque contra a integridade do sistema.

Essa ideia, embasada também nos incentivos econômicos que a plataforma trazia ao surgimento de mineradores, foi assimilada pela academia e pelo mercado. Nesse sentido, Wright e De Filippi (2015) definem a tecnologia blockchain, com base em Yochai Benkler (206), como "uma base de dados distribuída, compartilhada, encriptada que serve como registro público irreversível e incorruptível de informação. Ela permite que, pela primeira vez, desconhecidos cheguem ao consenso sem recorrer a uma autoridade central"[14]. Definição semelhante é trazida por Schrepel (2019(b)), segundo quem "blockchain é um registro aberto e distribuído que pode registrar -- manual, ou automaticamente -- qualquer transação entre usuários":

> "Uma vez registradas em blockchain, informações e transações são permanentes. [...] Porque essas transações não podem ser alteradas, fala-se que, diferente de Pinocchio, blockchain não mente".

[14] "*The blockchain is a distributed, shared, encrypted database that serves as an irreversible and incorruptible public repository of information. It enables, for the first time, unrelated people to reach consensus on the occurrence of a particular transaction or event without the need for a controlling authority.*"

Abordando a imutabilidade, o autor reconhece que o estabelecimento de uma relação de confiança é central para a viabilidade da tecnologia e a razão para a sua ampla adoção. Para tanto, a tecnologia blockchain propõe, de forma inovadora, que a confiança decorra da descentralização e da atomização da capacidade decisória[15]:

> "Ao assegurar que cada usuário tenha acesso ao registro e ao estabelecer a relação de confiança, blockchain também soluciona o 'Problema dos Generais Bizantinos', segundo o qual sistemas computacionais não podem gerar consenso sem confiar em uma autoridade central. A solução desse problema é o que define o potencial de aplicação de blockchain. Como consequência da adoção da *lex cryptographia*, blockchain pode fazer tudo o que computador faz, mas de forma descentralizada."

A ideia de imutabilidade está tão arraigada à tecnologia blockchain, que autores como Schrepel (2019(b)) partem desse pressuposto para suscitar algumas das suas mais significativas contribuições aos efeitos do uso da tecnologia blockchain sobre a concorrência nos mercados[16]. Segundo ele, "como blockchain é descentralizada, anônima e imutável, surgem questões relacionadas à habilidade de detectar práticas anticompetitivas e os seus perpetradores".

Como, porém, assinalam Catalini e Gans (2019), a garantia de imutabilidade é diretamente proporcional à capacidade computacional dedicada à mineração de blocos[17]:

> "[...] Isso [a relação entre a segurança dos registros em plataformas blockchain e a capacidade computacional dedicada à rede] gera economias de escala e uma correlação positiva entre efeitos de rede e segurança: quanto maior o número de participantes usando tokens criptografados, maior o seu valor, o que atrai mais

[15] "*By ensuring that every user has access to the ledger and establishing trust, blockchain also solves the 'Byzantine Generals Problem,' according to which computer systems cannot reach consensus without relying on a central authority. Solving this problem is the defining element of blockchain's potential. As a consequence of following the lex cryptographia, blockchain can do everything that a computer does but in a decentralized manner*".

[16] "[...] *because blockchain is decentralized, anonymous, and immutable, questions arise regarding the ability to detect anticompetitive practices and their perpetrators*".

[17] "*This generates economies of scale and a positive feedback loop between network effects and security: as more participants use a crypto token, its value increases, which in turn attracts more miners (due to higher rewards), ultimately increasing the security of the shared ledger.*"

> mineradores (devido a maiores recompensas), em última análise elevando a segurança do registro compartilhado."

O exposto permite sublinhar que a popularidade da tecnologia blockchain se assenta sobre a confiança de que as informações armazenadas não serão alteradas, ou adulteradas após registro do evento[18] -- o que permite o uso do registro descentralizado como forma de substituir o intermediário.

Como veremos, porém, a definição de imutabilidade está arraigada às regras de governança de cada blockchain, incluindo a confiança nos tomadores de decisão de plataformas centralizadas e às garantias oferecidas contra ataques de integridade, também conhecidos como "ataques de 51%"[19], ou, quando associados a criptomoedas, "gasto duplo".

Blockchain como tecnologia

Blockchain é uma tecnologia, "uma inteligente combinação entre criptografia e teoria dos jogos"[20] a partir da qual se desenvolvem outros serviços e produtos. Desenvolvida em código aberto por alguém cuja verdadeira identidade é desconhecida, o seu uso está em domínio público e permite o desenvolvimento, sem custos, de serviços sobre ela.

O desenvolvimento desses novos serviços tem agregado inovações sobre a plataforma original. Dividindo o aprimoramento da tecnologia que se desenvolve sobre a plataforma blockchain em três etapas, Schrepel (2019(b)) denomina blockchain 1.0 o "marco zero" da plataforma via nascimento do bitcoin e das criptomoedas. Para o

[18] Exemplo de alteração de registro é relatado em Eghdami (2019), que cita a alegação pela operadora FanDuel de que o seu sistema teria se equivocado na verificação das chances da aposta.
[19] Segundo Walch (2017), *"[a] 51 percent attack could occur if a party or colluding group controlled at least 51 percent of the computing power of the network, allowing them to determine what is recorded to the network's records, and potentially to revise the existing record.*"
[20] Catalini e Gans (2019).

autor, o surgimento de relações contratuais marca a blockchain 2.0, o que inclui atividades financeiras -- ações, títulos, futuros, empréstimos, títulos -, bens inteligentes e contratos inteligentes. Finalmente, a blockchain 3.0 inclui o que for além de aplicações financeiras, moeda e mercado, como governo, saúde, ciência, alfabetização, cultura e arte.

Parte significativa dos aprimoramentos feitos em blockchain visava elevar o grau de confiança nas operações e a alargar o número de operações que prescindirão de intermediário (1), ou alterar a solução originalmente desenhada para adaptá-la às necessidades de um universo corporativo específico (2). Note-se que a eliminação do intermediário, ao descentralizar as relações econômicas, tem um efeito desgastante para parte significativa das regulações, uma vez que -- por se tratar do meio mais eficiente de atingir todas as operações relevantes, por isso chamado de *least cost avoider* -- o intermediário costuma ser o centro de imputação das normas. Paradoxalmente, a tecnologia destinada a descentralizar a tomada de decisão tem sido utilizada também para aperfeiçoar modelos regulatórios e elevar aderência (*compliance*)[21] (3).

No primeiro caso, os chamados contratos inteligentes (*smart contracts*) permitem a automação de transferências de moeda, ou de outras contrapartidas contratuais, uma

[21] "*Without appropriate legal safeguards, it is plausible that the development of blockchain technology could follow a similar path, leading to increased surveillance. In spite of the opportunities for the development of worldwide systems, the state or other centralized bodies could, indeed, use the technology to exercise a significant degree of control over people's interactions and online communications.192 As more and more of our economic transactions and social interactions occur in a networked environment, the technology could increasingly be used to regulate people's behavior, to ensure that they remain consistent with the law or with the contractual obligations that they have entered into. The blockchain could be used, for instance, to manage identity, making it easier to monitor, surveil,193 or simply keep track of various online activities. Every transfer, vote, purchase can be recorded on the blockchain, creating a permanent record that will potentially push the boundaries of privacy law. Regulators might further require that online operators within the blockchain ecosystem to refuse to deal or transact with unidentified parties that have not satisfied AML or KYC requirements,194 undermining the pseudonymous nature of the blockchain and turning it into a powerful tool of surveillance and control.*"

vez preenchidas determinadas condições. Uma aplicação bastante promissora dos contratos inteligentes está na licença de uso da propriedade intelectual: artistas mais conhecidos podem descentralizar ainda mais a transação econômica com terceiros interessados e conceder acesso ao seu material artístico mediante a imediata transferência de moeda para a sua carteira, sem passar por nenhum intermediário -- seja artístico, ou financeiro[22]. Além da redução dos custos da transação, a eliminação do subjetivismo interpretativo a partir da mudança do jargão jurídico ("*wet code*") para a programação ("*dry code*"), a inalterabilidade e a autoexecutoriedade dos contratos inteligentes têm o potencial de reduzir a judicialização.

No segundo caso, as regras de governança concebidas para o bitcoin têm sido alteradas para manter um sistema decisório centralizado, com alguns *trade-offs* de eficiência, ou para conferir adrede poder de alteração dos registros por parte dos nós. Pilkinton (2015) descreve, por exemplo, que a mudança de um modelo baseado na valorização do trabalho de processamento (*proof-of-work*) para um sistema baseado

[22] O outro lado da moeda reside nos potenciais efeitos negativos da excessiva restrição à propriedade intelectual. A previsão em blockchain de que todo o material será transferido mediante compensação podem levar a que, no limite, mesmo após a expiração dos direitos de propriedade intelectual esse material mantenha restrição de acesso. Como descrevem Wright e De Filippi (2015), os contratos inteligentes podem acabar se tornando meios mais efetivos de controlar o acesso à propriedade intelectual que os próprios direitos de propriedade intelectual:
"*At the same time, these systems could fundamentally challenge the free nature of our online world. Smart contracts could, in effect, be an evolution of digital rights management (DRM) that could jeopardize the open nature of the Internet. These evolved digital contracts have the power to conceivably control access to and consumption of digital content. Content companies could wrap their content and use smart contracts to ensure payment, limit transferability, and protect content that is in the public domain. Taken to its logical extreme, if content creators develop the ability to identify all of their content online, copyright law—including the regime of limitations or fair use —could be rendered less relevant, as self-executing contracts could tabulate and track every reproduction, distribution, derivative work, and display, narrowing the possibility for online copyright infringement.*

While this benefits content creators, if the cost of information is set too high, it may effectively serve as a tax on creativity and consequently chill the development of the arts. Vast swaths of information currently freely available on the Internet could be converted back into a market-based commodity. The mass deployment of micropayments could lead to a situation where 'tiny bundles' of small-scale innovation are protected by strong intellectual property and contractual rights. As well recognized by J.H. Reichman, this could produce "a tangled web of property and quasi-property rights that in itself constitute a barrier to entry."

na riqueza dos mineradores (*proof-of-stake*) eleva a velocidade de processamento das operações e reduz tanto o gasto de energia, quanto a probabilidade de ataques contra a integridade do sistema[23].

A principal distinção entre os modelos de governança em blockchain decorre da diferenciação entre as plataformas públicas e as privadas: se as primeiras são abertas à participação de qualquer indivíduo no processo de decisão de quais blocos serão adicionados à cadeia, descentralizando (ao menos em teoria, como veremos) a tomada de decisão, o processo decisório nas últimas é centralizado e não necessariamente anonimizado. Essa distinção levou a que essas fossem definidas como permissionadas, em contraposição às blockchains públicas. Perceba-se, porém, que entre os dois extremos em graus de publicidade existe uma infinidade de espectros de descentralização da tomada de decisões e, por subsequente, de modelos de governança em blockchain[24].

Pilkinton (2015), ao abordar a proposta de blockchain permissionada trazida por Buterin, fundador da Etherium -- plataforma fechada permissionada de blockchain que oferece, entre os seu produtos, contratos inteligentes -- descreve importantes alterações trazidas pelas redes permissionadas. Segundo ele, a reversibilidade é uma qualidade desejável para o caso de registros de imóveis e ressalta que mesmo em

---

[23] "*Instead of splitting blocks across proportionally to the relative hash rates of miners (i.e. their mining power), proof-of-stake protocols split stake blocks proportionally to the current wealth of miners. Buterin (2014b) argues that proof-of-stake has a number of distinct advantages over proof-of-work (non-wasteful protocol, decreased likelihood of a 51% attack, potentially faster blockchains, etc).*"

[24] Conforme descreve Pilkinton (2015): "*In a fully private ledger, write-permissions are monitored by a central locus of decision-making. Read-permissions are either public or restricted (Buterin, 2015b). A private blockchain amounts to a permissioned ledger, whereby an organizational process of Know-Your-Business (KYB) and Know-Your-Customer (KYC) enables the white listing (or blacklisting) of user identity. The difference between public and private blockchains is the extent to which they are decentralized, or ensure anonymity. Between the two extremes, there exists a continuum (Brown, 2015, Allison, 2015) of "partially decentralized" blockchains (Buterin, 2015b), rather than a strict public/private dichotomy. Partially decentralized, also called "consortium blockchains" (Buterin, 2015b), constitute a hybrid between the low-trust (i.e. public blockchains) and the single highly-trusted entity model (i.e. private blockchains).*"

blockchains públicas não seriam raros os casos de ataques à integridade da rede já registrados. Ademais, as transações em blockchains privadas, ou permissionadas seriam processadas com maior celeridade e menores custos, além de usufruir de maiores garantias de privacidade[25].

A capacidade de processamento é um dos mais importantes gargalos da tecnologia blockchain, quando o assunto são operações que demandam agilidade, sendo a vantagem comparativa das blockchains permissionadas, nesse quesito, destacada também por Catalini e Gans (2019), que fazem um contraponto com a paralela perda de segurança[26]:

> "Se isso [ser uma plataforma aberta] torna o Bitcoin extremamente resiliente a ataques e à censura, também o torna menos eficiente, em sua forma atual, em comparação com as redes centralizadas de pagamento. Blockchains permissionadas, as quais são registros distribuídos nos quais os participantes tipicamente dependem de autorização para adicionar (ou, até mesmo, visualizar) uma transação, podem, por sua vez, ter mais banda disponível em razão de não dependerem de mineração para sustentar o seu registro. Quando a mineração está completamente ausente de uma blockchain privada, o registro de uma auditoria não está protegido pelo trabalho computacional desgastante [da mineração] e se os nós estiverem corrompidos (ou se conspirarem para sobrepor o registro), a integridade do bloco é posta em risco."

---

[25] *"Buterin (2015b) has identified several weaknesses intrinsic to immutable public ledgers. Firstly, in some cases, such as land registries, reversibility is a desirable property of the blockchain, as government-uncontrollable registries risk not being recognized at all. Buterin (ibid.) admits that a public ledger with a smart contract allowing the government to enter the game, nuances this conclusion, without undermining it (ibid.). Secondly, the concept of an anonymous 51% attack arising from a collusion of miners taking control of a public decentralized network is widely documented in cryptoeconomics. The pitfall is eliminated in the event of known validators. Thirdly, transaction costs processed by public ledgers are higher, whereas private blockchains, with their reduced number of high-processing nodes, enable cost-effective transactions. Buterin (ibid.), however, notes that, thanks to scalable blockchain technology, there is an asymptotic trend bringing long-term costs of public ledgers in line with efficient private ones. Fourthly, the connectivity between nodes in public blockchains is lesser than in private ones, which increases the laps of time for total transaction finality. All things being equal, private blockchains are faster. Lastly, regarding the issue of privacy options, public ledgers can hardly compete with private blockchains and their restrictions of read permissions (ibid.)."*

[26] *"Whereas this makes Bitcoin extremely resilient to attacks and censorship, it also makes it less efficient, in its current form, than centralized payment networks. Permissioned blockchains, which are distributed ledgers where participants typically need to be granted permission to add (or even view) transactions, can instead deliver higher bandwidth because they do not need to rely on proof-of-work for maintaining a shared ledger. When mining is completely absent from a private blockchain, the audit trail is not protected by sunk computational work, and if the trusted nodes are compromised (or if they collude to rewrite the ledger), the integrity of the chain is at risk."*

A forma de concentração de poder nas blockchains permissionadas, ou privadas permite classificá-las como blockchains singulares, ou blockchains consorciadas, a depender de se a tomada de decisão -- regra de governança -- é imposta por um único ente, ou fruto da formação de consenso por um grupo limitado de nós (Schrepel, 2019(b)). A governança de uma blockchain privada permite, por exemplo, que as transações sejam visíveis, apenas, para para os seus usuários, criando aquilo a que Schrepel (2019(b)) chama de "efeito opacidade".

No terceiro caso, a integração de contratos inteligentes com bancos de dados públicos pode permitir que restrições a determinados perfis, ou os pagamentos de tributos operem automaticamente (*by design*), facilitando, mas também reduzindo o papel do regulador. Essa relação dicotômica é bem descrita por Wright e De Filippi (2015):

> "A tecnologia blockchain tem o potencial de reduzir o papel de um dos mais importantes atores econômicos e regulatórios na nossa sociedade -- o intermediário. Ao permitir que as pessoas transfiram uma propriedade, ou informação digital única em um modo seguro e imutável, a tecnologia pode criar: moedas digitais sem reguladores estatais; contratos digitais auto-executáveis (contratos inteligentes), cuja execução não exige qualquer intervenção humana; mercados descentralizados desregulados; plataformas de comunicação descentralizadas com crescentes barreiras à gravação; bens ligados à internet que possam ser controlados como propriedade digital (bens inteligentes)."

Ao mesmo, tempo, anotam[27]:

> "Usando a linguagem de programação, contratos inteligentes podem ser usados para pagar empregados por hora, ou por dia de trabalho, com o envio de tributos automaticamente para o Estado. A tecnologia poderia ser empregada para criar contratos inteligentes que verifiquem automaticamente os obituários e repartam os bens conforme a vontade testamental, recolhendo os tributos devidos ao Estado, sem a necessidade de proceder à impugnação do testamento."

[27] Segundo Wright e De Filippi (2015): "*Using these programming languages, smart contracts could be used to enable employees to be paid on an hourly or daily basis with taxes remitted to a governmental body in real time. The technology could be employed to create smart contracts that automatically check state death registries and allocate assets from a testator's estate, send applicable taxes to governmental agencies without the need of administering the will through probate*."

Os autores fazem uma referência similar ao tratar de instrumentalizar a internet das coisa (IoT) para limitar o acesso a armas de fogo[28].

Schrepel (2019(b)) comenta, por outro lado, que a natureza descentralizada de uma blockchain pública permite que ela se mantenha em funcionamento, ainda que o Estado resolva aplicar penas nos desenvolvedores da blockchain. Do mesmo modo, caso a governança da blockchain seja atomizada, contratos inteligentes, mesmo quando instrumentalizem operações ilegais, podem vir a ser indefinidamente executados, caso criados com algoritmo desenhado para não interromper a sua execução[29].

Para resolver esse problema, Schrepel (2019(b)) sugere que o regulador transforme os requisitos legais em código e o integre na tecnologia que se deseja regular. Desse modo, não só será possível regular, como a aplicação da lei e o sancionamento passam ser automatizados (por isso chamado *by design*: poderíamos falar em regulação, ou sanção inteligente). A alternativa ao reconhecimento de que a lei é código e de que o código é lei, segundo Wright e De Filippi (2015), assim como por Schrepel (2019(b)), seria a imposição de filtros na internet, a criminalização do desenvolvimento de certos software, o banimento de organizações autônomas descentralizadas (DAOs), o uso de backdoors nos computadores dos particulares --

[28] "*With the rise of the Internet of Things, it also will be increasingly easy to instantiate laws using blockchain technology. For example, smart contracts could conceivably manage constitutional rights. In the US, they could be used to automatically check a decentralized online identity platform and digitized criminal records to assess whether the person satisfied certain preconditions that define who can and who cannot own or use guns. A person that satisfied these preconditions would be allowed to purchase a gun, whereas failure to meet these requirements would bar the person from completing the purchase. More drastically, smart contracts could be tied to an Internet-connected gun, which could only be operated if these pre-conditions were met.*"

[29] "*No 'technically skilled people of goodwill' are needed to maintain the blockchain. Dapps cannot be shut down because there is no server to shut down. They can only be modified under specific and technical circumstances. In other words, if an anticompetitive smart contract is implemented on a blockchain with no possible entry to order it to stop, the blockchain will continue to perform the transactions. As a consequence, even if antitrust agencies find a way to identify an anticompetitive practice, there is no directly enforceable remedy*."

soluções essas consideradas medidas extremas que ameaçariam seja o aproveitamento da tecnologia blockchain, seja a liberdade do indivíduo[30].

Schrepel (2019(b)) sugere que a imposição de uma regulação algorítmica adequada só será adequada se houver incentivos à integração do código legal à blockchain por parte dos regulados. Para ele, o mesmo deve ser dito para o uso de diretrizes governamentais para as regras de governança de cada blockchain.

Como se nota, os principais benefícios de blockchain repousam na imutabilidade que resulta dos mecanismos de governança desenhados para uma blockchain pública e aberta -- tornando, assim, desnecessário recorrer a terceiros não interessados, inclusive dispendiosos registros públicos, ou advogados, para que confirmem a veracidade das informações. Por sua vez, a descentralização das relações econômicas pode conferir liquidez imediata ao mercado, ao garantir que o fornecedor -- seja ele um artista licenciando a sua propriedade intelectual, seja um comerciante vendendo a sua mercadoria, ou serviço, seja um trabalhador vendendo a sua mão-

[30] A posição do autor tem como fundamento texto anterior de Wright e De Filippi (2015):
"Thus, unless these organizations have been designed to cooperate with the regulatory framework in which they operate, states and regulators might actually lose their ability to regulate them by relying exclusively on the law. To regulate society, laws may need to be directly embedded into code or laws may need to shape social norms, structure markets, and influence architectural design in order to incentivize the proper deployment of decentralized organizations. Left without such alternatives, governments could attempt to preserve their hegemony by resorting to draconian measures, such as filtering internet service providers, blacklisting malicious decentralized autonomous organizations and criminalizing software developers, introducing back doors on everyone's computer to monitor citizen behavior, or adopting more extreme coercive measures. New regulatory approaches therefore need to be taken, else the fundamental principles of an open Internet and permissionless innovation could eventually disintegrate."
Uma vez mais:
"Finally, the open nature of blockchain-based architecture means that most, if not all of the applications deployed on the blockchain could be reproduced and adjusted by anyone, in order to fulfill different functions and satisfy the needs of different groups and communities. As a result, dictating the manner in which software developers design a particular application protocol, or forcing software developers to introduce a particular feature into the code will only work to the extent that the user- base actually agrees to switch to the new protocol. Failure to reach consensus amongst users means that software will remain in use.
Of course, states can always adopt coercive measures in order to force users to update their clients. Yet, in this context, regulating architecture can be a treacherous task and, without careful contemplation, runs the risk of undercutting the powerful interconnectivity of the Internet and traditional notions of free expression."

de-obra -- seja automaticamente compensado por meio de micropagamentos ao final de cada música baixada, produto adquirido, ou dia de trabalho. Como apontado por Rosenberg (2015), micropagamentos viabilizam, ainda, o surgimento de campanhas de *crowdfunding* sem a utilização de intermediários, sendo a plataforma Lighthouse exemplo disso.

Ao lado da descentralização das transações, a confiança nos registros da plataforma blockchain permite, ainda, que, uma vez preenchida a condição contratual, transferências de moeda sejam automatizadas por meio de contratos inteligentes, ou que tarefas sejam realizadas por meio do acionamento remoto de bens inteligentes conectados à IoT. A associação entre contratos inteligentes e bens inteligentes permite, ainda, otimizar o casamento entre a oferta e a procura, levando a que a identificação da escassez de determinado produto, ou serviço seja imediatamente associada à oferta desse mesmo produto, ou serviço pelo fornecedor[31]. Essa última solução já é adotada, por exemplo, pela Alexa da Amazon.

A intersecção entre blockchain e IoT pode permitir, ainda, elevar a efetividade de mecanismos de segurança, ao assegurar que os eletrônicos -- em particular aqueles que carregam dados pessoais, ou concedam acesso a lugares reservados -- sejam acessados somente se determinadas características registradas em blockchain forem

[31] "*The rise of coordinated Internet-enabled machines could also create liquid, transparent marketplaces by enabling real time matching of supply and demand with increased transparency and automation. Conference rooms, hotel rooms, warehouse bays, and factory lines could be made intelligent, reporting capacity, utilization, and availability in real-time.Networks of Internet-enabled sensors could optimize farms by measuring heat, humidity, nutrition levels, light, and weight in order to automatically adjust irrigation and fertilization levels. If every farm used sensors to optimize crop growth, and recorded pseudo-anonymized versions of this information to a searchable blockchain, a public dashboard could be created to measure national or regional crop yields or even areas of over- fertilization, resulting in more efficient farms and commodities markets. Likewise, a mobile phone could securely communicate with a door lock and automatically open if the owner's smartphone had the necessarily credentials to open the lock (such as verified biometric data). Using this technology, real world spaces, such as homes or hotels, could be managed and secured with no human interaction. As these locks become smaller and cheaper, they could eventually be embedded into an increased array of physical objects.*"

averiguadas. Tudo isso passa a ser possível porque blockchain emerge como um registro construído com linguagem algorítmica conectada a fontes externas de informação (conhecidos como "oráculos") na rede de computadores[32], permitindo que a integração do registro com qualquer informação, ou tecnologia igualmente conectada automatize o adimplemento de acordos.

Os autores acentuam, ainda, como a tecnologia pode aprimorar a forma com que a individualidade e a democracia se manifestam. Entre outras aplicações, a tecnologia permite a comunicação direta (*peer-to-peer*, P2P) criptografada entre indivíduos, sem a necessidade de passar por um servidor central, dificultando a violação da comunicação -- seja para censura, seja para investigações. A tecnologia tem, ainda, o inegável potencial de aplicação na votação eletrônica remota[33] e na redução das abstenções, seja nos sufrágios, seja nas decisões assembleares corporativas. No primeiro caso, blockchain pode reduzir os custos para recorrer mais frequentemente a mecanismos da democracias direta[34]; no último caso, a tecnologia pode reduzir o

[32] O recurso aos oráculos é objeto de observação no item A.4.1 de Calini e Gans (2019).

[33] "*Beyond managing data, software developers are exploring the blockchain's potential to enable unrelated people to securely vote over the Internet or on a mobile device. A blockchain can serve as a distributed, irreversible, and encrypted public paper trail that can be easily audited. Voters could verify that their own votes were counted, and—due to encryption—any blockchain-based voting system would be resistant to hacking. Elections and proxy fights would no longer need to rely on the fallibility of paper and hanging chads*."

[34] Segundo Wright e De Filippi (2015):
"*Imagine a small suburban town in the not so distant future. The town's mayor could propose a budget and release it for public vote via blockchain-based software. Inhabitants of the town could be prompted to vote for the proposed budget on their mobile device. People could input their position and those who voted against a proposal could provide feedback directly to the mayor's office. If a sufficient number of votes were cast in favor of the proposed budget, the allocated funds could be immediately released to relevant departments in the town using smart contracts. If the budget did not receive enough votes, the mayor's office could either review the comments and propose a new budget or decide to call a public vote. Elections and public participation in politics could become as mundane as replying to an email.*"

absenteísmo e o problema de agência (relação agente-principal). Segundo Wright e De Filippi (2015)[35]:

> "Modelos de governança corporativa podem ser replicados distribuindo poder de decisão para múltiplos atores, por meio de tecnologia *multiple signature* (*multi-sig*), a qual impede que uma ação seja executada até que múltiplas partes dêem consentimento para uma transação.
>
> Contrariamente a organizações tradicionais, em que a tomada de decisão está concentrada no topo (i.e., no nível executivo), o processo de tomada de decisão de uma organização descentralizada pode ser codificado diretamente no código fonte. Acionistas podem participar da tomada de decisões por meio de votação descentralizada, distribuindo autoridade na organização sem a necessidade de uma autoridade central."

Como se pode notar, a tecnologia blockchain tem o condão de revolucionar a forma com que a sociedade se organiza e a sua aplicação potencial tem ramificações hoje ainda desconhecidas. Uma dessas possibilidade, ainda pouco explorada, encontra-se no ramo da proteção à privacidade e no interesse de que ela aconteça de modo a preservar os incentivos à inovação e os incentivos à concorrência. Nessa seara, a imutabilidade trazida por regras coesas de governança da tecnologia blockchain tem o condão de viabilizar a portabilidade dos dados, resolvendo -- ao eliminar um significativo custo de troca (*switching cost*) -- um dos maiores empecilhos à portabilidade de dados entre plataformas e à entrada de tecnologias com inovações destruidoras[36]. Esse ponto é bem delineado por Schrepel (2019(b))[37], segundo quem,

---

[35] "*Corporate governance models can be replicated by distributing decision-making power to multiple parties using multiple signature (multi-sig) technology, which prevents the execution of an action until multiple parties agree to a transaction.*

As opposed to traditional organizations, where decision-making is concentrated at the top (i.e., at the executive level), the decision-making process of a decentralized organization can be encoded directly into source code. Shareholders can participate in decision-making through decentralized voting, distributing authority throughout the organization without the need for any trusted centralized party."

[36] Esse ponto é mencionado, superficialmente, por Catalini e Gans (2019):
"*From a privacy perspective, the ability to license out subsets of personal information for limited amounts of time and to seamlessly revoke access when necessary has the potential to not only increase security, but also to enable new business models where customers retain greater control over their data and firms can dynamically bid for access*."

[37] "*It is also technically possible to store all data (including that generated by the use of services such as social media) on the user's private blockchain or across many hard drives throughout the blockchain network, leaving the product or service developers with no data in hand. The platforms would have to*

ao segurar a informação, o usuário diminui o poder das plataformas para traçar um retrato mais completo do usuário:

> "É também tecnicamente possível guardar todas as informações (inclusive aquela gerada pelo uso por serviços como mídias sociais) na blockchain permissionada do usuário, ou em muitos drives ao longo da rede blockchain, deixando os desenvolvedores de produtos, ou de serviços sem a guarda de nenhuma informação. As plataformas teriam de encontrar novas formas de incentivar os seus usuários a conceder acesso a dados. Em outras palavras, graças a blockchain, o modelo de negócios de produtos e serviços digitais pode ter a necessidade de ser inteiramente revisto nos próximos anos."

Nesse mesmo sentido, o recurso à tecnologia como forma de reduzir custos é ainda subestimada e tem um enorme potencial ser explorado. Calini e Guns (2019) destacam que a redução dos custos de verificação (de registros, inclusive pessoais) terá externalidade positiva sobre a preservação da privacidade, reduzindo, inclusive, os riscos de vazamento de informações sigilosas que hoje precisam ser guardadas em bancos de dados de terceiros. Segundo os autores, blockchain pode viabilizar o acesso, sem custo, ao volume de informações estritamente necessário para realizar uma operação. A confiança na informação, por sua vez, ocorre em razão da transição de um modelo de confiança no intermediário para um modelo de confiança no algoritmo, ou código.

Ao lado dos custos de verificação, os autores destacam o papel da alteração da dinâmica dos custos de rede. Esclarecem, nesse sentido, que uma plataforma blockchain pode criar incentivos a comportamentos que fomentem externalidades de rede. Conjuntamente, esses comportamentos podem reduzir os custos de financiamento e de funcionamento da plataforma. Esses incentivos visam a criar interesse mútuo no desenvolvimento da plataforma. Exemplo disso está no

---

find new ways to incentivize their users to give access to their data. In other words, because of blockchain, the business model of digital products and services may need to be entirely rethought in the coming years."

pagamento pela mineração, ou, principalmente, na distribuição de moeda aos primeiros entrantes. Uma vez com recursos na plataforma, o usuário passa a ter um custo de oportunidade que influencia o seu comportamento pela valorização dos ativos cuja utilidade é crescente em relação ao número de adeptos (externalidade de rede, p.e., das moedas).

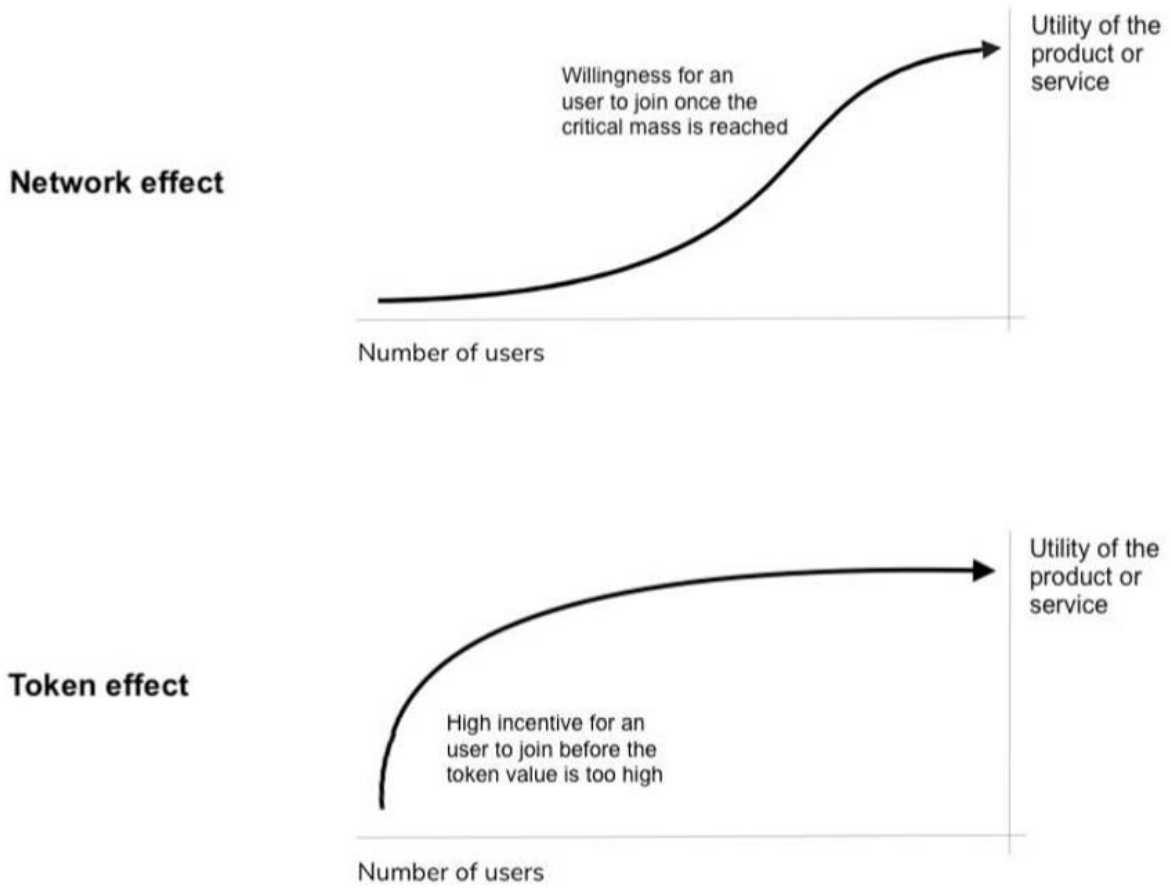
Schrepel (2019(b)) destaca a especificidade da externalidade de rede em blockchain -- que ele denomina “efeito token”. Segundo o professor, o efeito token é criado com maior facilidade em plataformas blockchain do que o efeito de rede é criado em plataformas fora de blockchain, em razão do descasamento financeiro existente entre o incentivo a aderir ao serviço e a sua utilidade.

O exemplo mais claro está nas chamadas Initial Coin Offerings (ICO), a partir das quais os detentores da moeda terão fortes incentivos a sobrevalorizar o ativo para obter ganhos financeiros. Em outros casos, a plataforma oferece *tokens* em troca da adesão a determinada rede social (prática conhecida como “*airdrop*”, ou “*coin drop*”). Mason (2018) cita o exemplo da oferta casada criada pela plataforma Zero Edge, a qual isenta de *house edge* aquele que use a sua criptomoeda (Zerocoin), criada exclusivamente para apostas *online*. Mire (2019) cita o caso de outra plataforma que isenta os apostadores do *house edge*, a Edgeless. Como a aquisição de moedas, ou de *tokens* faz bastante sentido como investimento quando a sua cotação está em baixa para a venda quando a cotação estiver em alta, uma característica do efeito *token* é a volatilidade da cotação do ativo (seja a criptomoeda, seja o *token*).

Como as plataformas digitais “emitem moedas”, essa opção de criar incentivos financeiros ao usuário por meio da associação direta entre crescimento da rede ligada à plataforma e maiores ganhos financeiros para o consumidor é racional -- mas não

costuma ser observada fora de plataformas blockchain, em razão dos elevados custos de sustentar uma política de pagamento dos usuários em moeda fiduciária. Ainda assim, é possível comparar, guardada a diferença de escala, a tentativa de algumas plataformas digitais fora de blockchain -- em particular plataformas de serviços de carona -- em fazer esse casamento, ao oferecer códigos de desconto que passam a valer a partir da adesão à plataforma de um número mínimo de convidados do consumidor. A figura abaixo ilustra a diferença de comportamento verificada entre o efeito *token* e o efeito de rede:

Figura 2. Efeito token v efeito de rede



Fonte: Schrepel (2019(b)).

O mais importante é que, uma vez ligado à plataforma com altos custos de oportunidade para migrar, os custos para a plataforma captar clientes para um produto derivado (como são os contratos inteligentes, em uma plataforma criada para criptomoedas) são extremamente baixos. A situação é similar ao caso clássico dos mercados de dois lados: a oferta do acesso abaixo do custo à plataforma (atraindo clientes de um dos lados da plataforma) cria as condições ideais para atrair os desenvolvedores de acessórios (do outro lado da plataforma).

Calini e Guns (2019) explicam que os custos de rede são menores quando os custos de verificação também são baixos. Nesse sentido, as externalidades de rede podem ser mais facilmente alcançadas em plataformas de blockchain não permissionadas, se comparada a uma plataforma de blockchain permissionada. O grande benefício da externalidade de rede da blockchain não permissionada reside em que o grau de descentralização das decisões em tese existente afasta o abuso de posição dominante e que a tecnologia preserva os dados pessoais em poder dos usuários -- reduzindo os custos de entrada e de competir.

Como se pode notar, a possibilidade de alterar, ou agregar funcionalidades tem permitido o desenvolvimento não só do mercado financeiro, quanto a transformação de outros mercados bastante dependentes de modelos de confiança. As próximas seções visam aprofundar o debate sobre a relevância da governança para o sucesso de blockchain e como a tecnologia pode ser aplicada, de maneira inovadora, nos mercados de jogos e loterias.

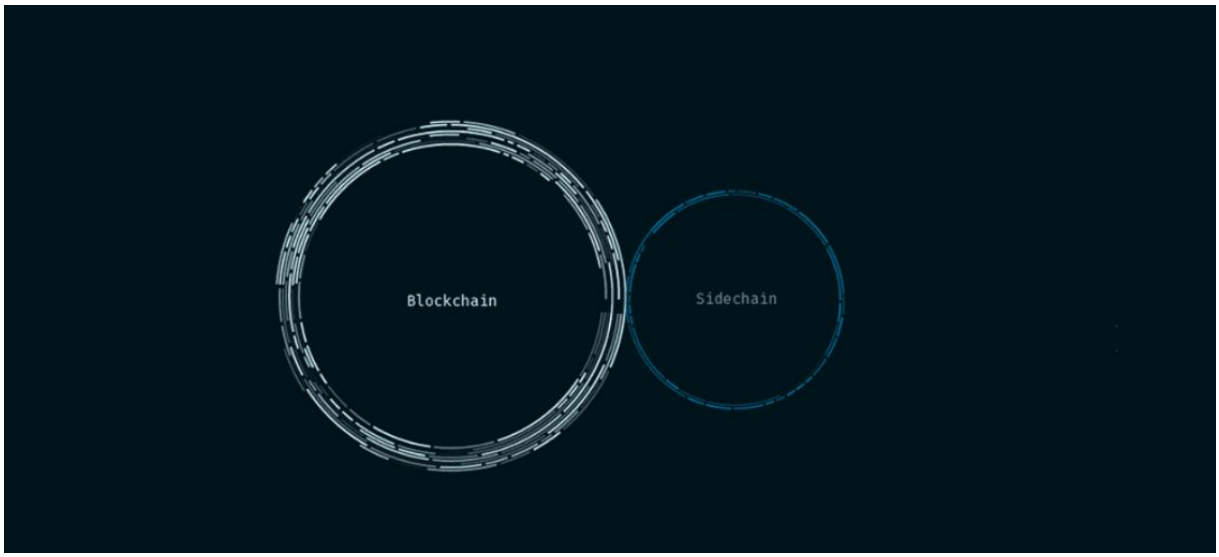
Blockchain: concentração, governança e a mutabilidade

Schrepel (2019(b)) explica que a integridade de blockchain depende da regra de consenso escolhida para liquidar as operações. Juntamente com outros mecanismos

que possam ser utilizados para regular o funcionamento da tecnologia, o consenso define a governança da plataforma[38]. Como ele bem resume, "[q]uem controlar o consenso -- também conhecido como mecanismo de consenso -- controla a governança de blockchain".

Se a regra de consenso permite definir quem controla a governança em blockchain -- e pode afastar uma blockchain da ideia de atomização do poder e imutabilidade dos registros que moldou o seu nascimento -, a escolha de mecanismos que elevam o anonimato das operações, ou de quem realiza as operações -- como o envolvimento de várias camadas em outras plataformas blockchain (mecanismo assim chamado de "*sidechain*") -- abarca regras de governança que afetam o grau mínimo de publicidade para o qual a tecnologia blockchain foi desenhada.

Figura 3. Sidechain



Fonte: Adaptado de Rosenberg (2015).

[38] *"Blockchain integrity relies on the chosen consensus to clear transactions. Together with other potential mechanisms that may be introduced on blockchains in order to regulate it, they form the governance of the latter."*

Nessa linha, se, de um lado, as blockchains públicas priorizam *proof of work* e *proof of stake* como regras de formação de consenso, a governança das blockchains permissionadas não costuma envolver mineração, remuneração pelo trabalho, ou outras outras formas de criar incentivos à dispersão do centro de decisão. Em linhas gerais, as blockchains permissionadas costumam estar associadas à concentração de poder. E, como antecipamos em citação de Buterin, as blockchains permissionadas oferecem, também, soluções diversificadas para o aprimoramento da privacidade e do anonimato.

Schrepel (2019(a)) afirma que mesmo a atomização das blockchains públicas -- que asseguraria a imutabilidade, por exemplo, dos registros em bitcoin -- está ameaçada porque, na prática, as recompensas da mineração acabaram por criar mineradores dedicados à plataforma e a concentração de poder em torno de um oligopólio. A concentração de poder viabiliza o alinhamento de interesses e pode provocar a crise de confiança dos modelos centralizados que a tecnologia blockchain tentou resolver[39]:

> "[...] menos de 10 grupos de mineração dominavam Bitcoin em 2017. Na verdade, os 7 mais poderosos representavam mais de 85% de todas as transações validadas pela blockchain de Bitcoin. Esse dado coloca em cheque a proclamada natureza descentralizada do Bitcoin, pois o domínio sobre mais de 51% do poder de mineração equivale ao controle da blockchain."

Essa tendência à concentração já havia antecipada por Pilkinton (2015), que antecipava os efeitos da profissionalização da mineração[40]:

---

[39] *"[...] fewer than 10 mining pools dominated Bitcoin in 2017. In fact, the 7 most powerful ones accounted for more than 85% of all transactions validated on the Bitcoin blockchain. This calls into question the proclaimed decentralized nature of Bitcoin because the owning of more than 51% of mining power is equivalent to a control of the blockchain."*

[40] *"In the early days, mining was primarily done by individuals on home computers through central (or graphics) processing units. With rising complexity, algorithms have required more powerful mining techniques taken over by application-specific integrated circuits (ASIC), cloud mining and mining pools. 21 Inc, the self-proclaimed first Bitcoin computer, aims to revolutionize both the mining and the semiconductor industries, with its embedded mining innovation (Srinivasan, 2015). BitShare, a mining chip, potentially embedded into millions of Internet devices, works collectively to mine new currency. These new streams of crypto-currency both solve the problem of bearing the cost of micropayments,*

> "No começo, a mineração era operada, primariamente, por indivíduos em computadores domésticos por meio de unidades de processamento centrais, ou gráficas. Com o aumento da complexidade, os algoritmos passaram a exigir técnicas de mineração mais avançadas dominadas por circuitos integrados específicos para cada aplicação (ASIC), mineração em nuvem e associações de mineração. 21 Inc, autoproclamado como o primeiro computador voltado para Bitcoin, promete revolucionar tanto a mineração, quanto a indústria de semicondutores, com a sua inovação de mineração (Srinivasan, 2015). BitShare, um chip de mineração, potencialmente inserido em milhões de aparelhos ligados à internet, funciona coletivamente para cunhar nova moeda. Esses novos modelos de criptomoeda tanto resolvem o problema de custear micropagamentos, quanto trazem à tona um novo modelo criptográfico que ajuda a financiar os próprios chips (Niccolai, 2015). Os detalhes técnicos ainda não estão claros, mas se inovações posteriores forem replicadas e amplamente adotadas, haverá mudanças drásticas em toda a economia baseada em criptografia."

No caso das blockchains privadas, dada o maior grau de estabilidade da concentração de poder, a regra de consenso poderia ser utilizada para encobrir atos ilícitos. Segundo Schrepel (2019(a))[41]:

> "Naquilo que diz respeito às blockchains privadas, elas podem permitir a saída programada do acordo [ilícito], ao mesmo tempo em que garantem que os dados [sobre a existência] sejam apagados. Isso é particularmente atraente para cartéis. De forma mais abrangente, levando em consideração que o criador de uma blockchain privada tem o poder de sobrepor, editar e apagar informações lançadas na blockchain, ou modificar o próprio funcionamento da blockchain, a blockchain privada não poderá ser usada como prova de participação em um colusão."

Como a capacidade de detecção dos ilícitos pelo poder público em uma blockchain pode, ausente a regulação algorítmica, ser muito baixa, os incentivos à defecção em quadrilhas que funcionem sob blockchain é pequeno.

Apesar de os benefícios e os malefícios do uso de plataformas construídas com a tecnologia blockchain dependerem das regras de governança de cada plataforma, o discurso generalista acerca de características não necessárias de blockchain arrisca

---

and bring to the fore a new crypto-business model by helping finance the chips themselves (Niccolai, 2015). The technical details remain unclear, but if the latter innovation were to be replicated and widely adopted, it would be a game changer for the whole crypto-economy."

[41] *"As far as private blockchains are concerned, they may allow an on-demand exit from the agreement while ensuring the deletion of data. This is utterly attractive for potential colluders. More generally, considering the fact that the owner of a private blockchain retains the right to override, edit, and delete the entries on the blockchain, or even to modify the blockchain functioning itself, it cannot be used as intangible evidence to prove participation in collusion."*

criar fortes assimetrias informacionais, em particular com relação ao regulador, impedindo que atue, tempestivamente, por meio de uma regulação algorítmica e de incentivos à transparência. Essa assimetria informacional é retratada por Walch (2017), segundo quem a própria diferenciação entre blockchains públicas e privadas pode não estar totalmente clara.

Walch (2017) também adverte que o recurso ao termo "imutável" para descrever o registro em blockchain é equivocado. Apesar de alguns especialistas usarem "imutável" para expressar a possibilidade de criar regras que praticamente inviabilizem a mudança de registros em blockchain, essa distinção não chegou à academia, tampouco aos reguladores[42].

> "Até mesmo o defensor do Bitcoin Andreas Antonopoulos descreveu Bitcoin como difícil de alterar, em vez de absolutamente inalterável. Ele ainda se refere à blockchain do Bitcoin como imutável, contudo, porque, segundo ele, representa o mais próximo que a humanidade chegou de criar algo verdadeiramente imutável e qualquer coisa mais simples de alterar que Bitcoin não pode proclamar-se imutável. O uso dessa complicada justificativa por uma autoridade em blockchain para continuar a usar a palavra 'imutável' para descrever a blockchain de Bitcoin cria confusão porque o significado implícito de imutável ('de difícil alteração') não confere com o entendimento generalizado da palavra imutável ('inalterável'). O significado implícito de 'difícil alteração' não parecer ter alcançado os acadêmicos, consultores, líderes e reguladores, que continuam a declarar, sem qualquer qualificação, que a tecnologia blockchain cria registros imutáveis, permanentes, inalteráveis, que não podem ser apagados."

Para a autora, essa confusão tem levado a regulações, como a do Arizona, que aceitam a legalidade de contratos inteligentes assinados usando blockchain, definem essa tecnologia como imutável e não sujeitam o contrato -- seja realizado sobre

[42] *"Even prominent Bitcoin advocate Andreas Antonopoulos has described Bitcoin as hard to change, rather than absolutely unchangeable. He still refers to Bitcoin's blockchain as immutable, however, because he says it represents the closest humanity has come to creating something truly immutable, and anything easier to change than Bitcoin has no claim to the word immutable. This convoluted justification for continuing to use the word "immutable" to describe Bitcoin's blockchain from a prominent figure in the blockchain community creates confusion because the hidden meaning for immutable ('hard to change') does not match the general understanding of the word immutable ('unchangeable'). The secret meaning of 'hard to change' does not seem to have reached the academics,consultants, thought leaders, and regulators who continue to state without qualification that blockchain technology creates immutable, permanent, unchangeable, indelible records."*

plataforma pública, ou sobre plataforma permissionada -- ao cumprimento de determinadas regras de governança.

Mercados de jogos e blockchain: retornos crescentes ao apostador, integridade nas apostas e no pagamento

De acordo com Gainsbury e Blaszczynski (2017), o surgimento de produtos inovadores, como eSports betting, skins betting, jogos de mídias sociais e realidade virtual, turvam a fronteira entre apostas, jogos e mídias sociais realizados na internet:

> "A velocidade de entrada desses novos produtos no mercado tem exercido pressão pressão e gerado incertezas com relação ao controle regulatório, às decisões políticas e à proteção do consumidor interna e entre países."

Essa velocidade contrasta com a resposta da academia e do regulador:

> "Ademais, a pesquisa acadêmica está habitualmente atrasada na sua capacidade de avaliar o impacto e as implicações da mudança do ambiente para apostas responsáveis e para a minimização do dano. Na ausência de controles regulatórios e de fiscalização, o consumidor continua exposto aos riscos de jogos, esquemas e jogos de realidade aumentada irregulares, com componentes que aumentam a ilusão de controle e experiências dissociativas."

Segundo Gainsbury e Blaszczynski (2017), a mais direta aplicação de blockchain para apostas ocorre por meio da aceitação de bitcoin como meio de pagamento. O uso de blockchain tem permitido que as apostas sejam feitas de forma anônima:

> "De acordo com um site de apostas que aceita bitcoin denominado BitcoinCasinoPro.com, a maior parte dos sites de apostas com bitcoin parece permitir que os jogadores preservem o anonimato e não exige qualquer identificação para jogar. Nenhuma informação pessoal é transferida com as transações, o que tem levado a capacidade de os usuários evitarem certa regulação, por exemplo, usando bitcoin para jogar online em países nos quais isso é proibido".

Como ressaltam os autores, o anonimato e o seu uso para financiar apostas não fiscalizadas pelo regulador somam-se para associar o bitcoin à seleção adversa[43]:

[43] *"Sites that do not follow AML/KYC protocols, which is typically a regulatory requirement, lends credence to concerns about the legitimacy of bitcoin gambling sites. This is consistent with bitcoin's*

> "Sites que não seguem os protocolos AML/KYC [que identificam o usuário], o que é um requisito regulatório habitual, geram desconfiança com relação à legitimidade dos sites de aposta que aceitam bitcoin. Essa constatação é consistente com a associação de bitcoin com o mercado negro *online*, e.g. a *Silk Road* [Rota da Seda], usado para bens e serviços ilícitos cujos pagamentos se dão quase exclusivamente em bitcoin. Em 2011/12, transações da Silk Road foram estimadas em cerca de 4.5-9% of da atividade comercial com bitcoin. Desse modo, bitcoin e criptomoedas são habitualmente associadas a atividades ilegais."

Por outro lado, a tecnologia blockchain elimina problemas bastante comuns a bancos de dados, particularmente em plataformas que investem pouco na segurança digital: o furto de identidade e a operação de fraudes. A possibilidade de usar oráculos para franquear acessos (como hoje já se faz com o uso de contas de redes sociais para confirmar identidade), ou de guardar as informações pessoais na blockchain permissionada -- deixando os desenvolvedores de produtos, ou de serviços sem a guarda de nenhuma informação -- reduz os riscos de responsabilidade da casa de apostas, de fraudes contra o apostador e, como um todo, da judicialização, ou do recurso ao regulador como esfera de arbitramento[44].

---

association with the online black market, e.g. the Silk Road, used for illicit goods and services with payments almost exclusively in bitcoin. In 2011/12 Silk Road transactions were estimated to account for 4.5-9% of bitcoin trading activity. As such, bitcoin and cryptocurrencies are often perceived to be associated with illicit activity."

[44] Segundo Gainsbury e Blaszczynski (2017):

"The requirement for consumers to share extensive information about their identity and finances for online commerce has resulted in an exponential increase in fraud and identity theft. This is related to companies asking for and storing personal information on systems that can be hacked. Blockchain can be used for online storage and secure identity verification across multiple sites or institutions. A blockchain ID could be linked to existing online accounts (e.g., Facebook, Google) and used to log into applications and sites, for in-person identification, similarly to using a passport or driver's license, and theoretically as a key to real places such as a home or office. Unlike a passport, license, or other online identity, blockchain ID would not rely on a third-party. This would overcome issues of users having to share their data, such as when using a Facebook login to access a third-party site, allowing Facebook and the site to access a wealth of personal information, which is used for marketing or even sold to further third-parties. Customers could share their data with companies, but manage this so only information needed for each purpose is shared, which may boost trust and reduce fraud related to excess data being shared with companies online. This could allow gambling operators to verify customer's identity quickly, cheaply, and easily, without relying on third-parties and long wait-times. It would also allow crossborder gambling as identification could be accepted globally and allow gambling operators to potentially target a wider market. Combining the decentralised blockchain principle with identify verification would allow identity to be checked for all transactions, in real time, which would virtually eliminate fraud."

Catalini e Gans (2019) reforçam a relevância de blockchain enquanto ferramenta que resguarda a privacidade do usuário e, ao transferir para o consumidor a guarda das informações, elimina os custos de troca (*switching costs*) e afasta o *lock-in*, viabilizando a liberdade de escolha[45].

> "A tecnologia blockchain pode prevenir o vazamento de informações ao viabilizar que o mercado verifique os atributos de um transação e faça cumprir contratos sem expor a informação subjacente a terceiros. Isso permite que a veracidade de determinada informação seja escrutinada (e.g., boa nota de crédito), sem que seja necessário desagregar os dados que deram ensejo a tal dado (e.g., registro de operações pregressas): i.e., a tecnologia viabiliza a verificação dos atributos da transação de uma forma que resguarda a privacidade."

Ainda segundo os autores[46]:

> "A tecnologia blockchain pode diminuir o risco [à privacidade] ao permitir a autenticação sem a divulgação de informação sensível. Do mesmo modo que um registro distribuído pode identificar os atributos de operações financeiras, também pode identificar mudanças no status e nas credenciais (ou empresa, bens, serviços) de um indivíduo. A capacidade de um indivíduo realizar (ou não) certa ação poderia ser identificada em blockchain e questionada quando necessário sem que, para tanto, seja necessário divulgar toda a informação subjacente (e.g., um banco poderia verificar o histórico de crédito, uma vez autorizado por um cliente). Do mesmo modo, o acesso ao histórico médico pode ser franqueado, revogado or portabilizado entre prestadores de serviços conforme achar conveniente.
>
> Pela perspectiva da privacidade, a capacidade de autorizar fragmentos de informação pessoal por períodos limitados de tempo e a qualquer momento revogar esse acesso, sempre que entenda necessário, tem o potencial de não só aumentar a segurança, como também viabilizar novos modelos de negócios nos

[45] *"Blockchain technology can prevent information leakage by allowing market participants to verify transaction attributes and enforce contracts without exposing the underlying information to a third-party.5 This allows an agent to verify that some piece of information is true (e.g. good credit standing), without full access to all background information (e.g. past transaction records): i.e., the technology allows for the verification of transaction attributes in a privacy-preserving way."*

[46] *"Blockchain technology can reduce this risk by allowing for authentication without disclosure of sensitive information. The same way a distributed ledger can track the attributes of financial transactions, it can also track changes to an individual's status and credentials (or firm, good, service). An individual's ability to perform (or not) a certain action could be tracked on a blockchain and queried when needed without necessarily disclosing all underlying information (e.g. a bank could verify, after being authorized by a customer, a credit history). Similarly, access to medical records could be granted, revoked or ported between providers as needed.*
From a privacy perspective, the ability to license out subsets of personal information for limited amounts of time and to seamlessly revoke access when necessary has the potential to not only increase security, but also to enable new business models where customers retain greater control over their data and firms can dynamically bid for access."

> quais os clientes detenham maior controle sobre os seus dados e as empresas possam, de forma dinâmica, fazer ofertas por esse acesso."

Um exemplo desse uso é citado por Mason (2018). Segundo ele, os contratos inteligentes da plataforma Zero Edge, criados sobre a plataforma Ethereum, garantem que a operadora não tenha acesso a nenhum dado do apostador além da confirmação de que fundos entraram, ou saíram da sua conta. Rosenberg (2015) cita, por sua vez, a plataforma Twister, desenvolvida pela brasileiro Miguel Freitas.

O recurso a bitcoin também permite o rápido processamento de apostas em qualquer moeda a tarifas mais baratas que as taxas de câmbio habitualmente cobradas para outras moedas. Ademais, a parte da aposta cobrada pelo operador ("*house edge*") costuma ser mais baixa. Para Gainsbury e Blaszczynski (2017)[47]:

> "Uma possível vantagem que sites de apostas em blockchain oferecem aos consumidores é a redução de tarifas. Sites que só aceitam pagamentos em bitcoin têm mais despesas mais baixas quando comparadas a operadores regulados, como, por exemplo, custos de transação, tarifas de licenciamento, custos regulatórios, pagamentos aos comerciantes e taxas mais baixos. Isso pode ser traduzido em maior retorno para os jogadores, por exemplo, em razão de a *house edge* chegar a 1,9%[48]. Bitcoins também podem ser usados com custos mais baixos para os consumidores, em razão de a maior parte dos cartões de crédito e processos de pagamento por intermediário cobrar tarifas de transação, por exemplo, para saques de fundos de terceiros (o que incentiva reapostar o prêmio), ou tarifas de antecipação de recebíveis (3-4%) e juros (de até 29,49%). Finalmente, o saque do prêmio pode ser feito de forma célere, se comparado a outros sites de apostas *online*, que podem levar dias para processar os saques e podem impor valores mínimos para sacar, ou até enviar cheques por correio, em lugar de facilitar transferências eletrônicas. As transações com bitcoin são também

[47] *"A potential advantage that blockchain gambling sites offer consumers is reduced fees and charges associated with gambling transactions. Bitcoin-only sites have lower overheads compared to regulated operators, for example reduced transaction costs, licensing fees, regulatory compliance costs, payment to merchants, and potentially tax. This can be translated into a greater return to players, for example the house edge can be as low as 1.9%. Bitcoins can also be used at a low cost to consumers, which is notable given that most credit card and third-party payment processes charge users transaction fees, for example for withdrawing funds from third-party providers (thus encouraging re-gambling of wins) or cash advance fees (3-4%) and interest (as high as 29.49%). Finally, withdrawing winnings can be done rapidly, as compared to other online gambling sites that can take a few days to process withdrawals, and may have minimum withdrawal amounts and in some cases require a cheque to be mailed rather than facilitating electronic transfers. Bitcoin transactions are also beneficial for operators as payments are irreversible, meaning that there are no issues with fraudulent or non-payment."*

[48] Segundo Mason (2018), Zero Edge isenta de house edge quem use a sua criptomoeda (Zerocoin), criada exclusivamente para apostas online. A plataforma Edgeless também isentaria os apostadores, segundo Mire (2019).

> melhores para os operadores, uma vez que os pagamentos são irreversíveis, o que implica dizer que não há fraude, ou inadimplência."

O uso de blockchain permite, ainda, que os recursos sejam transferidos, de forma bidirecional, da conta do jogador -- ou de terceiro que lhe empreste fundos -- para a casa de apostas e que o prêmio, ou *payout* seja enviado, a partir do desenho de contratos inteligentes, diretamente para a conta *online* do jogador -- e, eventualmente, daquele que lhe emprestou fundos -- em bitcoins. Desse modo, o risco de atraso, ou de inadimplemento por parte da casa de apostas (e, no sentido contrário, por parte do apostador) desaparece, assim como a obrigação da casa de apostas de criar, manter e responder por contas abertas para os apostadores[49]. Mason (2018) traz o exemplo da plataforma Zero Edge, cujos contratos inteligentes criados sobre a plataforma Ethereum garantem que não haja atrasos no depósito do prêmio, com o jogos sendo auditáveis, ou verificáveis por aquela plataforma blockchain.

Apostas com blockchain são, ainda, abertas a verificação, ou auditoria pelos interessados, o que permite que os apostadores instruídos confiram se o jogo é feito segundo as regras. Essa transparência decorre tanto da publicidade do históricos de apostas de outros jogadores, como da possibilidade de inspecionar o algoritmo utilizado pela plataforma. Ademais, os operadores podem usar blockchain como forma de assegurar as autoridades de que não há como interferir no resultado dos jogos, ou

[49] *"Related to this, blockchain sites are differentiated by the lack of a required player account. For example, on one of the earliest established sites, Satoshi Dice, players sent bitcoin to a specified address to place a bet. There was no need to visit a website, download software, or create a registered account. This system was modified such that players now have a unique URL they can use to deposit funds to bet. The service uses a random number generator to determine if the wager wins or loses and payouts are sent immediately to players, rather than deposited into an online gambling account that remains with the operator. For players, as they do not keep funds in an online gambling account, there is no risk that the site will be hacked, seized, or funds stolen from an online account. For operators there is no requirement to manage and protect player funds and accounts. This also reduces associated regulatory issues and compliance regarding player funds and accounts."*

no pagamento dos prêmios -- o que reduz o custo de obedecer a lei e, pelo lado do regulador, os custos de impor e de verificar o cumprimento da lei[50].

Fenech (2019) cita que o mercado de apostas *online* pode, diversamente da maioria das indústrias, colher frutos imediatos com a adoção de blockchain. Isso ocorre em razão de tratar-se de um segmento cuja reputação é afetada por diversas causas facilmente sanadas mediante a aplicação da nova tecnologia. De certo modo, blockchain transforma velho dilemas nesse mercado em *low hanging fruits*.

O primeiro deles consiste em abrir a caixa preta dos cassinos. Com a criação de registros cuja governança é confiável, será possível que qualquer apostador instruído acesse o histórico de apostas e descubra se a plataforma cumpre os seus compromissos e se esse cumprimento é tempestivo. Um sistema mais transparente e eletrônico viabiliza, ainda, que os empréstimos entre apostadores aconteçam de forma eletrônica, instantânea e de forma clara para o operador.

A qualidade dos registros é de particular importância porque, segundo Kozak (2019), os cassinos físicos (*brick-and-mortar*) permanecem populares, tendo os cassinos *online* se tornado uma nova dimensão da clássica experiência com os cassinos -- ou,

[50] Segundo Gainsbury e Blaszczynski (2017):
"The impact of blockchain gambling extends well beyond the use of cryptocurrency for payments. Blockchain gambles are open to verification, so gamblers can ensure that games are fair, provided that they have sufficient technological knowledge to do so. That is, the code used to determine gambling outcomes are transparent and once launched, work automatically without interference. Sites can provide summaries so that all players can see the history of other player's bets and history of bets on the site itself. Even without this, transactions can be searched as records are public. For example, bitcoin transactions can be analysed as the history of these are publicly available and network analysis can help map sets of public keys to individual users and transactions. Since currency exchanges generally require identity verification, anonymity of transactions using cryptocurrency is not guaranteed. This technology and system of records ensures that blockchain gambling is fair to players. Gambling operators can use blockchain to assure customers and regulators that there is no way to interfere with outcomes or payments. This may overcome reluctance among some users to use Internet gambling due to a lack of perceived trust. It also alleviates the requirement for a third-party, such as a gambling regulator, to verify the fairness of a gambling site. This may lead to gamblers becoming comfortable using unregulated sites."

a nossos olhos, uma franja competitiva. Como o grau de fidelidade da clientela dos cassinos varia -- certamente havendo aqueles que migrariam para os cassinos *online* se esses oferecessem alguma dimensão em que a sua experiência fosse mais prazerosa -, é correto concluir que, ao abrir a caixa-preta, blockchain cria incentivos para o aumento do churn dos cassinos *brick-and-mortar* e à migração interplataforma, em caso de os cassinos físicos não aderirem à tecnologia.

Em segundo lugar, blockchain vai tornar o pagamento automático, líquido e certo, assim que a condição -- acerto da aposta -- seja preenchida, prevenindo a revisão, ou a adulteração pelo operador. O mecanismo usado para tanto são os contratos inteligentes, que permitirão o pagamento automático -- cuja liquidação será ainda mais célere se as moedas digitais forem aceitas como meios de pagamento, *tokens*, ou ativos legais, nos termos da legislação do país. Esse ponto também interessa bastante à análise que Kozak (2019) faz dos cassinos físicos. Segundo ele, muitos cassinos ainda não usam tecnologias eficientes, como *software* de contabilidade, tampouco são integrados a apostas *online*. A automatização dos pagamentos, ao refletir uma garantia de recebimento do *payout*, representa o incentivo mais robusto a que o consumidor ostracize o negócio que não adote uma solução que eleve a *accountability* (externa, com relação ao apostador) e a governança (interna, com relação a mecanismos de gestão eficiente) do cassino.

O terceiro consiste no desenvolvimento de sistemas de apostas *peer-to-peer* (P2P), nos quais os usuários poderão adicionar o seus próprios jogos e apostas. Um exemplo está presente no projeto vSlice da plataforma Ethereum, por meio da qual quem tenha *tokens* recebe automaticamente parte dos lucros gerados pela plataforma. Outro

exemplo está na plataforma ZenSports[51], que também recorre aos contratos inteligentes. As apostas desenvolvidas em plataformas descentralizadas podem tanto ter natureza desportiva, quanto ser relativas a eventos da vida. d'Anconia (2017) menciona que os usuários podem apostar em praticamente qualquer coisa, desde o clima até eventos desportivos e eleições. Mire (2019) cita, por sua vez, o exemplo da plataforma Tombola, por meio da qual os apostadores compram bilhetes e a plataforma realiza sorteios com base em algoritmos, enviando o *payout*, sem o pagamento de qualquer taxa, diretamente para a conta dos ganhadores.

d'Anconia (2017) cita que os dados gerados pelas apostas podem ser usados como previsão relativamente certa acerca do resultado do evento. Nesse sentido, cita Magos, um modelo de previsão complexo que usa redes tecnológicas neurais para minerar dados e filtrá-los, criando previsões de alta precisão e elevados retornos para quem tenha tokens.

Apesar da aplicação imediata a plataformas *online* de apostas, os cassinos físicos também teriam muito a aproveitar da adoção de blockchain. Além do que se falou para as apostas *online*, eles agregariam segurança ao conectar o seu sistema de apostas à rede de computadores. Além de viabilizar transferências imediatas, formalizadas por contratos inteligentes entre a casa de apostas e os apostadores, e de dar vazão a maior transparência nas transferências e empréstimos entre apostadores, seria possível alcançar uma base maior de apostadores -- o uso potencial de recursos em moeda digital eleva o acesso a jogos por parte de populações cuja moeda cursiva é fraca, desbancarizada, ou sem acesso local a casas de apostas físicas (*brick-and-mortar*) -- e adicionar sistemas de segurança biométrica, facilitando identificar

[51] Mire (2019).

eventuais fraudadores e colaborar com as autoridades. Por fim, a integração entre cassinos físicos e plataformas *online* permite, ainda, que o apostador continue o seu jogo à distância, quando necessário.

A redução do custo de conformidade da atividade do regulado por parte do regulador pode decorrer, ainda, da potencial redução do número de páginas de apostas[52]. Segundo Gainsbury e Blaszczynski (2017), o número de páginas tem proliferado particularmente em função da necessidade de diferenciação quanto ao grau de segurança da casa de aposta e quanto ao valor das tarifas. Como o uso da tecnologia blockchain reduz as preocupações com a segurança e reduz o custo do operador, a tendência é que os submercados que ofereçam maior risco desapareçam -- ou que arquem com *payouts* cada vez maiores que remunerem o risco tomado, conscientemente, pelo apostador[53].

Ao alocar o dinheiro fora de uma conta de aposta aberta pela casa de apostas, o uso de blockchain pode incentivar a redução do vício em apostas. Recorrendo à teoria do valor social do dinheiro de Viviana Zeliter (1997), Gainsbury e Blaszczynski (2017) alertam que os apostadores não costumam sacar todo o dinheiro ganho em apostas para que esse mesmo dinheiro seja utilizado em apostas futuras. Seguindo a lógica de que esse dinheiro foi o resultado de um prêmio, apostadores contumazes costumam dissociá-lo do restante do seu dinheiro presente em banco, ou portado na

[52] Parece-nos que essa interpretação talvez precise ser reconsiderada, se levada em consideração a tendência à atomização do mercado trazida pela descentralização das apostas em plataformas blockchain.

[53] *"An important implication of a decentralised code providing fair gambling activities means that there will be a reduced need for thousands of identical sites distributed over the Internet. Current estimates suggest that there are 3,504 online gambling sites, many of which offer identical products. Internet gamblers select gambling sites based on reputation, as well as payout rates, and whether their money is safe and will be paid out. Blockchain gambling removes the relevance of concerns about site safety, lowers overheads and likely raises payout rates, which may reduce the relevance of a site's reputation. This may cause a reduction in sites, particularly the many disreputable sites that often target underserviced markets with limited legitimate online gambling options."*

carteira. Ou seja, quanto maior a associação do dinheiro com uma aposta precedente, maiores as chances de que seja utilizado para reapostar. Como a tecnologia blockchain elimina a necessidade de recorrer a uma conta da casa de apostas, esse ciclo vicioso é quebrado[54].

Como contraponto, Gainsbury e Blaszczynski (2017) alertam que o recurso a jogos *online* e a transferências eletrônicas costuma, dada a facilidade de realizar as transações, facilitar o vício. Esse efeito pode ser maximizado quando as transferências eletrônicas são operadas por meio de *tokens* pagáveis com criptomoedas, porque, nesses casos, fica menos nítido para o apostador o quanto ele está gastando[55].

De um lado, a natureza descentralizada de blockchain tem o potencial de, ausente uma regulação algorítmica, impossibilitar o controle do Estado sobre a operação de casas de jogos. Essa limitação pode ser relativizada, como sugerido por Schrepel

---

[54] *"According to Zeliter's Social Meaning of Money theory, money is treated differently depending on its context, such that money won gambling is not seen as neutral, but more likely to be perceived as tied to gambling and therefore re-gambled. This likely accounts for the finding that one-fifth of Britons with an online gambling account stated that they had an inactive account with an average of £14.96 remaining in this holding. Residual money in a gambling account is perceived differently to money in a bank account or wallet – it is tied to gambling rather than being viewed as neutral money to be spent on anything. This is likely also related to minimum withdrawal amounts from many online gambling sites and fees associated with withdrawals and transactions with payment providers. Gambling using blockchain structure may reduce this effect as customers do not have to use a gambling account. Funds are spent and returned directly without the need for these to be stored with a gambling operator. As such, according to Simmel's Philosophy of Money, cryptocurrency, which has many potential uses, would be perceived as neutral and not specifically earmarked for gambling purposes. This may reduce the tendency for online gambling sites to lead to excessive gambling. Clearly, the research is needed to investigate the impact of bitcoin gambling on perceptions of and actual expenditure."*

[55] *"Internet gamblers report that it is easier to spend more money than intended online and that electronic payment methods can obscure the true rate of expenditure, particularly for those at-risk of experiencing gambling problems. Using cryptocurrency for gambling may create similar problems as players are gambling with credits not monetary denominations and may not focus on the monetary value of their bets. This effect may be enhanced with bitcoin as consumers tend to spend more when the nominal value is a fraction of their home currency, which is the case with bitcoin (e.g., 1 bitcoin = $US1189 as of April 2017)"*

(2019(b)), mediante o recurso a uma regulação de incentivos, que confira ao apostador vantagens inegáveis em apostar em operadores em dia com a regulação.

Gainsbury e Blaszczynski (2017) sugerem que, ante as características de blockchain -- transparência, preservação dos registros, segurança, privacidade, autenticação e validação -, o papel do regulador do mercado de jogos e de revistas especializadas -- que hoje ajudam a diferenciar os bons dos maus operadores -- passa a ser desnecessário[56]. Esse entendimento é bastante comum entre entusiastas da tecnologia, como Eghdami (2019), para os quais a identificação de blockchain como *trustless* (prescindindo de um certificador) visa associá-la não só à eliminação do intermediário no mercado (bancos, bandeiras de cartões de crédito e alguns papéis das casas de apostas), como também do regulador. Esse argumento é contrariado por Fenech (2019), segundo quem a qualidade da governança da plataforma em blockchain -- que é, em última instância, o que garante que o contrato não contém *bugs* que afetem a sua execução, ou que os registros são, na prática, imutáveis -- exigirá, em um momento inicial, resguardar a existência de plataformas que avaliam o grau de confiança na plataforma e, no futuro, a transferência do papel de verificador a sistemas descentralizados -- internos, ou externos aos operadores de apostas -- que exerçam uma função regulatória e protetiva.

[56] *"With each transaction or bet visible for verification on the blockchain, bets are paid out automatically when outcomes occur, and with no customer accounts and funds to protect, the technology provides a high level of transparency for the gambling industry. Subsequently, the requirement for a third-party intermediary point of trust, the gambling regulator, becomes redundant. Using cryptocurrency also means that no individual has access to funds transfers, risk of payment failure, and money is secure at all points, meaning that no banking institutions or payment providers are involved; likely to substantially disrupt companies in these industries. Other business models that may be redundant include gambling affiliates and review sites, which help consumers identify which of the thousands of available online gambling sites can be trusted. Sites using blockchain technology should be trustworthy, furthermore, customers are not at risk of losing funds, since these are not stored within accounts of the individual sites."*

Ao mesmo tempo, aqueles autores relatam como os reguladores têm, por outro lado, visto a tecnologia como aliada para facilitar o processo regulatório[57]. Segundo autoridades britânicas -- como UK Gambling Commission, Alderney Gambling Control Commission e Isle of Man -, blockchain pode facilitar o acesso a informações relevantes, levando processos de auditoria e certificação para plataformas construídas sobre a nova tecnologia. Mesmo o efeito de anonimização derivado do uso de criptomoedas pode ser relativizado e usado favor das autoridades: o recurso a casas de câmbio e carteiras de bitcoin, as quais precisam usar protocolos Know Your Customer (KYC) -- que, como antecipado, é um requisito regulatório habitual que, ao mesmo tempo em que visa resguardar a privacidade, permite, sempre que necessário, identificar cada apostador -, permite identificar desde esquemas de lavagem de dinheiro a atividades regulatoriamente indesejadas. É nesse sentido que, segundo Hajdarbegovic (2014), o recurso a blockchain tem também permitido à plataforma de apostas Satoshi Dice limitar as apostas, em Curaçao, a jogadores com mais de dezoito anos. Nesse mesmo sentido, Fenech (2019) traz o exemplo da plataforma Bitbook.ag, que atende a regulações de prevenção à lavagem de dinheiro, combate ao vício em

[57] *"Some gambling regulators are considering the implications of blockchain. André Wilsenach, previously of the Alderney Gambling Control Commission stated that "shared, digitalized, decentralized" information in a blockchain-based ledger system would provide regulators with significantly easier access to important data. The Isle of Man, a prominent regulator of online gambling, has also indicated awareness of how the Internet gambling industry could benefit by moving due diligence, compliance checks, testing and certification to the decentralised ledger. Cryptocurrencies can be obtained somewhat anonymously, and tools are available to help mask consumer identity. However, reputable bitcoin exchanges and wallets do have KYC requirements and blockchain technology uses a unique identifier code, which could potentially contribute to efforts to combat money laundering as well as issues related to match-fixing. The UK Gambling Commission has updated its License Conditions and Codes of Practice to include bitcoin as an acceptable payment option for licensees, with Isle of Man also allowing virtual currency deposits for online gambling. As the nature of blockchain gambling can differ substantially from existing Internet gambling, regulators will have to consider whether their existing regulation is sufficient, or if specific amendments are needed to respond to blockchain gambling sites. Efforts to block or ban blockchain gambling are likely to ineffective, which should prompt regulators to discover and pursue strategies that are consistent with the new reality."*

apostas, bloqueia usuários oriundos de países nos quais as apostas são ilegais e impede que menores de idade façam apostas.

Finalmente, é importante ter em mente o potencial efeito arrecadatório da legalização do uso de moedas digitais. Segundo a plataforma GoCoin[58], contas de jogos representam cerca de 50% do número de todas as transações em bitcoin, ainda que representem somente cerca de 5% do valor total transacionado na criptomoeda. Tendo em mente a velocidade de digitalização da economia -- segundo Mason (2018), apostas *online* representam 25% do total das receitas de apostas -, esses números sugerem, também, um elevado potencial de crescimento. Segundo Fenech (2019), o mercado de apostas tem crescido a um taxa de 9% ao anos -- três vezes mais que o produto interno bruto global.

Tendo isso em mente, tanto a UK Gambling Commission, quanto Isle of Man passaram a admitir o uso de criptomoedas como forma de pagamento[59]. Gainsbury e Blaszczynski (2017) relatam como a plataforma Satoshi Dice, autorizada pelo governo de Curaçao, teria intermediado ganhos de mais de quatro milhões de bitcoins a partir de mais de seis milhões de apostas individuais em blockchain, com *payouts* de 64 mil bitcoins por aposta e *house edge* de apenas 1,9%.

A grande limitação de blockchain, hoje, é, como já antecipado, a sua baixa capacidade de processamento de dados -- sete transações por segundo, vis-à-vis duas mil a dez mil da Visa.[60] Gainsbury e Blaszczynski (2017) entendem, entretanto, que o engajamento de empreendedores cientes da relevância do desenvolvimento da

[58] Hajdarbegovic, Nermin (2014).
[59] Gainsbury e Blaszczynski (2017).
[60] Gainsbury e Blaszczynski (2017).

tecnologia permitirá não só o aumento da sua eficiência, como facilitar a sua interface e, por subsequente, a sua difusão.

A difusão, contudo, dependerá do grande envolvimento de atores de reputação e que tragam confiança no uso de plataformas blockchain pelo público em geral, incapaz de entender, de forma profunda o suficiente, as nuanças do seu funcionamento. Nesse sentido, Morgan Stanley acredita que o reconhecimento pelos reguladores e pelo Estado são necessários para que bitcoin -- e, de forma reflexa, acreditamos, também blockchain -- seja amplamente adotado. Os efeitos que a adoção de uma tecnologia tão disruptiva pode ter sobre a regulação é expressa na conclusão do artigo dos autores[61]:

> "Desse modo, prevê-se que blockchain venha a formar uma sólida base para oportunidades e transações de apostas que impactarão os reguladores, seja promovendo novas formas de olhar a regulação e o cumprimento da lei, seja por meio de colaboração em massa que substituirá a necessidade de reguladores por um sistema de autorregulação."

No limite, a aplicação de blockchain em sistemas de predição pode alavancar até mesmo ideias revolucionárias que dependam de maior segurança no registro. Esse é o caso da futarquia de Robin Hanson. Conforme descrito por Wright e De Filippi (2015)[62]:

---

[61] *"Accordingly, it is predicted that Blockchain will form a strong foundation for gambling opportunities and transactions that will in some way impact regulators, either generating novel approaches to regulatory and compliance issues, or through mass collaboration, eliminate the need for regulators in a self-governing system."*

[62] *"Alternatively, smart contracts could be used to set up decentralized prediction markets that could underpin a Futarchy —an alternative form of government proposed by economist Robin Hanson, using prediction markets as a means to identify the policies expected to yield the most positive outcomes. Under this model, elected representatives would formally define and coordinate an after-the-fact measurement of national welfare, while people speculate on the success or failure of specific policies by placing bets to select the policies they expect will ultimately raise national welfare. By turning prediction markets into decision markets, Futarchy presents itself as a solution to the current apathy and demagoguery of democracy. It provides financial incentives for citizens to participate in the governance process, although only the most skilled individuals (i.e.those who can effectively predict the specific policies' outcomes) will be rewarded, at the expenses of others. Of course, the potential drawback of such systems are most likely to outweigh their benefits."*

> "Alternativamente, contratos inteligentes podem ser usados para estabelecer mercados descentralizados de predição que poderiam ser a base para uma futarquia — forma alternativa de governo proposta pelo economista Robin Hanson, usando mercados de predição como meio de identificar políticas que, segundo se espera, teriam efeitos mais positivos. Segundo esse modelo, representantes eleitos definiriam e coordenariam formalmente a mensuração do bem-estar social, enquanto as pessoas especulariam -- apostando nas políticas que, segundo as suas expectativas, elevariam o bem-estar social -- acerca do sucesso, ou insucesso de políticas específicas. Ao transformar mercados de previsão em mercados de decisão, a futarquia se apresenta como solução para a apatia e demagogia hoje presentes na democracia. Fornece, ainda, incentivos financeiros para que os cidadãos participem na governança, embora apenas os mais qualificados (i.e., aqueles que possam efetivamente prever os resultados das políticas públicas) sejam premiados, às expensas dos demais. Claro que existe uma probabilidade maior de que os defeitos do sistema ultrapassem os seus benefícios."

Blockchain: aplicabilidade ao Brasil

Segundo o art. 51, §2º do Decreto-Lei nº 3.688, de 3 de outubro de 1941 -- Lei de Contravenções Penais -, considera-se loteria toda operação que, mediante a distribuição de bilhete, listas, cupões, vales, sinais, símbolos, ou meios análogos, faz depender de sorteio a obtenção de prêmio em dinheiro, ou bens de outra natureza[63]. No Brasil, a exploração dos jogos de azar ocorre por meio das modalidades lotéricas (consideranda do Decreto-Lei nº 204, de 27 de fevereiro de 1967) autorizadas via legislação especial (art. 51, §3º, da Lei de Contravenções Penais).

Segundo informações apresentadas pela Secretaria de Acompanhamento Fiscal, Energia e Loteria (2018) -- hoje Secretaria de Avaliação de Políticas Públicas, Planejamento, Energia e Loteria -, existem, hoje, de acordo com classificação da World Lottery Association (WLA), quatro modalidades de

[63] Para uma gama maior de definições, v. Secretaria de Acompanhamento Fiscal, Energia e Loteria (2018).

loterias: prognósticos numéricos, instantânea, prognósticos esportivos pari-mutuel e prognósticos esportivos *fixed-odds* (quota fixa).

Tabela 2 - Modalidades Lotéricas (WLA)

Loteria	Descrição	Exemplo
Prognósticos numéricos	o apostador tenta antever quais **números** serão sorteados, seja escolhendo livremente, seja adquirindo bilhete com a combinação pronta.	Mega-Sena Quina Lotofácil Lotomania Dupla Sena Timemania Dia da Sorte
Instantânea	apostador sabe, imediatamente após a escolha da cartela, cupom, ou cartão, se foi, ou não agraciado com alguma premiação.	Lotex
Prognósticos esportivos *pari-mutuel*	apostador tenta prever resultados de jogos esportivos, só conhecendo o quanto ganhará ao final dos eventos esportivos.	Loteca Lotogol
Prognósticos esportivos *fixed-odds* (quota fixa)	apostador tenta prever resultados de jogos esportivos, já conhecendo o quanto ganhará quando realiza a aposta.	prestes a ser explorada no Brasil

Fonte: adaptado da Secretaria de Acompanhamento Fiscal, Energia e Loteria (2018)

A Secretaria de Acompanhamento Fiscal, Energia e Loteria (2018) explica haver, ainda, o chamado sweepstake, definido como “a loteria cujo resultado é vinculado ao resultado de determinado páreo de uma corrida de cavalos”.

Destaque-se que, segundo o art. 60 do Decreto-Lei nº 6.259, de 10 de fevereiro de 1944, o jogo feito fora dos hipódromos, ou da sede e dependências das entidades autorizadas é uma contravenção penal -- o que impede, até seja editada norma superveniente, que seja considerada legal qualquer forma de aposta virtual. Vale recordar que esse mesmo dispositivo reputa contravenções "apostas sobre quaisquer outras competições esportivas", o que veio a cair com a edição de normas que hoje asseguram os prognósticos esportivos.

O caráter retrógrado de normas que ainda regem as apostas no Brasil pode ser confirmado ante a leitura do Decreto-Lei nº 204, de 1967: a norma em questão determina a forma cartular de realização dos sorteios. Ao mesmo, é importante ter em mente que o país tem passado por um movimento de readequação e modernização do seu marco legal, com normas específicas posteriores introduzindo, paulatinamente, em cada modalidade, a possibilidade de apostas virtuais. Exemplos válidos podem ser encontrados na loteria federal (art. 14, §1º, I, da Lei nº 13.756, de 2018) e na loteria de apostas de quota fixa (art. 29, §2º, da Lei nº 13.756, de 2018).

Se a WLA traz a sua classificação quadripartite, a página eletrônica do Programa de Parcerias de Investimentos (PPI) informa existirem três tipos de loteria no Brasil:

a) de sorteio (Mega-Sena, Lotofácil, Lotomania, Dupla-Sena, Timemania e Quina);

b) de números (Loteria Federal);

c) de prognósticos esportivos (Loteca e Lotogol).

A Lei nº 13.756, de 12 de dezembro de 2018, por sua vez, descreve seis modalidades lotéricas. Cinco delas se encontram descritas no seu art. 14, §1º. A derradeira é criada pelo art. 29. O quadro abaixo as resume.

Tabela 3 - Modalidades Lotéricas (Lei nº 13.756, de 2018)

Loteria	Descrição	Previsão legal
Loteria Federal (passiva).	Loteria em que o apostador adquire bilhete já numerado, em meio físico (impresso) ou virtual (eletrônico).	Art. 14, §1º, I, da Lei nº 13.756, de 2018.
Loteria de prognósticos numéricos.	Loteria em que o apostador tenta prever quais serão os números sorteados no concurso.	Art. 14, §1º, II, da Lei nº 13.756, de 2018.
Loteria de prognóstico específico (futebol).	Concurso de prognóstico específico sobre o resultado de sorteio de números ou símbolos ligados a clubes de futebol.	Art. 14, §1º, III, da Lei nº 13.756, de 2018. Lei nº 11.345, de 14 de setembro de 2006 (Lei do Timemania).
Loteria de prognósticos esportivos.	Loteria em que o apostador tenta prever o resultado de eventos esportivos.	Art. 14, §1º, IV, da Lei nº 13.756, de 2018.
Loteria instantânea exclusiva (Lotex).	Loteria que apresenta, de imediato, se o apostador foi ou não agraciado com alguma premiação.	Art. 14, §1º, V, da Lei nº 13.756, de 2018. Lei nº 13.155, de 4 de agosto de 2015.

Loteria de apostas de quota fixa.	Sistema de apostas relativas a eventos reais de temática esportiva, em que é definido, no momento de efetivação da aposta, quanto o apostador pode ganhar em caso de acerto do prognóstico.	Art. 29, §1º, da Lei nº 13.756, de 2018.

Fonte; elaboração própria.

A Secretaria de Acompanhamento Fiscal, Energia e Loteria (2018) esclarece que a modalidade passiva -- na qual o apostador recebe o bilhete já numerado -- é considerado pela WLA como prognóstico numérico.

Segundo essa mesma publicação, a Lei nº 13.756, de 2018, alinhou o *payout* das modalidades lotéricas brasileiras às melhores práticas internacionais.

Tabela 4 - Payout das Modalidades Lotéricas

Modalidade	Payout atual	Payout após Lotex	Prática internacional
Baseados em sorteios	43,35%	43,79%	45-50%
Prognósticos esportivos	37,61%	55%	50%
Passiva	55,91%	60%	50%
Instantânea	65% (médio)	65% (médio)	65% (médio)

Fonte: Secretaria de Acompanhamento Fiscal, Energia e Loteria (2018)

Apesar disso, a Secretaria de Acompanhamento Fiscal, Energia e Loteria (2018) reconhece que a monopolização das apostas dos produtos e serviços já colocados no mercado pela Caixa Econômica Federal mantém a arrecadação das loterias federais abaixo do seu potencial. Segundo a publicação, “a arrecadação real trimestral voltou ao patamar de 2014, depois de um longo período estável ou decaindo ao longo do tempo devido à escassez de estratégias de otimização da comercialização, de distribuição ou mesmo de marketing”. E acresce:

> “Em geral, a arrecadação real das loterias federais mostra responder ‘apenas’ à flutuação econômica, pois aumenta quando a economia melhora e diminui - ou se mantém estável - quando piora, sem apresentar um crescimento estrutural, portanto”.

A Secretaria também ressalta o monopólio elimina a motivação que um mercado competitivo traria para a exploração das apostas em novos formatos:

> “Outras formas de distribuição dos produtos lotéricos poderiam ser adotadas, como, por exemplo, a captação de apostas em meio eletrônico, que passaram a ser feitas no Brasil em larga escala somente a partir de agosto de 2018. [...] No entanto, as apostas online têm valor mínimo de R$30 e máximo de R$500 por dia, sendo que, nas casas lotéricas, os gastos médios costumam ficar entre R$5,25 e R$9,66, segundo a própria CAIXA. Com um público médio de frequentadores de 50 anos, sendo a maioria de homens e com renda abaixo de R$3.000, dificilmente a novidade se espalhará com facilidade.”

Conclui que existe espaço para que as apostas no Brasil avancem no seu modelo de distribuição,

> “[...] tanto no meio físico quanto nesse meio virtual recentemente adotado, especificamente por meio de canais como o mobile (com aplicativos próprios no celular, fazendo uso de todas as características disponíveis no smartphone), autosserviço (com disponibilização de apostas em totens), on-demand (utilizando-se de serviços especializados de assinatura) e com realidade virtual agregada.”

Foi pensando na necessidade de promover a modernização das loterias no país que a Secretaria -- responsável pela regulação das loterias, nos termos da Lei nº 13.756, de 2018 c/c sucessivos decretos de estrutura do Ministério da Fazenda (hoje incorporado ao Ministério da Economia) -- propôs a desestatização da Loteria

Instantânea, ”segunda mais importante modalidade de loteria no mundo”, representando, em média, 25% do mercado mundial. Por meio dessa decisão, objetivava-se criar concorrência entre a loteria instantânea e as demais modalidades lotéricas (competição interplataformas). Ao mesmo tempo, a Lei nº 13.756, de 2018, criou uma nova modalidade lotérica no Brasil -- a loteria de apostas de quota fixa -, explorada, exclusivamente, em ambiente concorrencial, com possibilidade de ser comercializada em quaisquer canais de distribuição comercial, físicos e em meios virtuais (incluindo, também, a competição intraplataforma).

O cenário de anacronismo estrutural histórico conjugado com uma nova mentalidade de promover a inovação por meio da abertura do mercado de apostas à pressão competitiva traz a combinação ideal para a difusão de tecnologias disruptivas com potencial para resolver as maiores ineficiências do mercado e, ao mesmo tempo, colocar o país na vanguarda regulatória. É nessa linha que faz bastante sentido a introdução de uma regulação amigável à tecnologia blockchain e que vise criar incentivos à sua adoção segundo parâmetros de segurança desejáveis.

Em primeiro lugar, blockchain pode criar registros seguros, se atendidos critérios de governança (regras de consenso, em particular) aprovados pelo regulador. Esses registros conferem segurança ao apostador, ao evitar que o operador adultere o resultado, e transparência quanto às atividades das casas e à transações suspeitas de lavagem de dinheiro. Note-se que a tecnologia permite que somente as transações -- e não a identidade dos apostadores -- torne-se pública, evitando a exposição desnecessária das pessoas, em particular nos casos de falsos positivos.

Uma regulação algorítmica permite, ainda, que os *payouts* sejam enviados diretamente, com base em regras predefinidas em contratos inteligentes, para a conta

de cada apostador -- resolvendo não só os empecilhos que as casas de apostas costumam impor para o recebimento do prêmio, como abrindo a possibilidade de que o rateio do prêmio nos "bolões" seja feito de forma contratualmente segura[64]. Esse pagamento automático de conta para conta, com uma auditoria automática realizada pelo cruzamento de dados entre plataformas blockchain, ao afastar a necessidade de procedimento *a posteriori* de *clearance*, aumenta, também, a segurança do apostador-vencedor, cuja identidade poderá ser preservada.

Os contratos inteligentes permitem, ainda, conferir maior segurança ao operador, quando casados com soluções de segurança (por senha, biométrica, ou ótica). Algoritmos podem prever que o *payout* só será transferido para a(s) conta(s) do(s) apostador(es) depois da aposição da assinatura digital, ou da leitura biométrica, ou ótica.

Note-se que a maior aderência à lei (aumento de *compliance*) quanto ao pagamento dos *payouts* decorre, também, de os baixos custos da plataforma tornarem viável a realização de micropagamentos. Assim, ao invés de o *payout* ficar reservado em uma *escrow account* até atingir um "mínimo transferível", a transferência de valores pode ser automática a cada aposta.

Em segundo lugar, regulações inclusivas e tecnologicamente neutras em blockchain tendem a tornar-se o padrão internacional e um importante atrativo para investimentos nos segmentos de apostas no Brasil. Ao sinalizar que as atividades do operador credenciado guardam conformidade com a lei, ao mesmo tempo em que oferecem ao apostador as mesmas vantagens (diversidade, privacidade, ubiquidade e conforto)

[64] Por exemplo: é possível que se preveja uma regra contratual, redigida em contrato inteligente, segundo a qual, se (qualquer) um dos integrantes do bolão depositar o dinheiro até x dias, ou horas antes do sorteio, receberá a sua parte do payout.

dos melhores serviços disponíveis *online*, regulações vanguardistas em blockchain podem colocar a tecnologia a serviço da redução da atividade ilícita, ao mesmo tempo em que se elevam o bem-estar social com a eliminação da seleção adversa.

Nessa linha vanguardista, o item (29).1 da Quinta Diretriz contra a Lavagem de Dinheiro (5AMLD) conduz a que as legislações nacionais dos países-membros da União Europeia internalizem normas que promovam a identificação dos usuários de moedas virtuais, inclusive por parte dos operadores de apostas:

> "Os Estados-Membros asseguram que os prestadores de serviços de câmbio entre moedas virtuais e moedas fiduciárias e os prestadores de serviços de custódia de carteiras digitais estão registrados, que as agências de câmbio e de desconto de cheques e os prestadores de serviços a sociedades ou fundos fiduciários estão sujeitos a licenciamento ou inscrição num registo e que os prestadores de serviços de jogo estão sujeitos a regulamentação."

A necessidade de as casas de apostas identificarem o cliente --- e, ainda, manter o registro das transações -- decorre, também, da aplicação de recomendações do Grupo de Ação Financeira contra Lavagem de Dinheiro e Financiamento do Terrorismo -- GAFI (FAT) -- aos criptoativos e prestadores de serviços de criptoativos[65]. Note-se, nesse particular, que, dadas as suas características, a tecnologia blockchain associada a boas regras de governança (em particular, boas regras de consenso) oferece uma vantagem natural para o registro das operações e para a preservação da sua integridade.

[65] "When a DNFBP engages in VASP activity (e.g., when a casino offers VA-based gaming or engages in other covered VA activities, products, or services), countries should subject the entity to all of the measures for VASPs set forth in the FATF Recommendations. Countries should note, for example, that Recommendations 22 and 23 set out the CDD, recordkeeping, and other requirements for certain types of DNFBPs in the following situations: (a) casinos, (b) real estate agents, (c) dealers in precious metals and stones, (d) lawyers, notaries, other independent legal professionals and accountants, and (e) trust and company service providers. Recommendation 22 specifically notes that the requirements set out in Recommendations 10, 11, 12, 15, and 17 apply to DNFBPs. Thus, in considering how to regulate and supervise and apply the preventive measures to DNFBPs that engage in VASP activities, countries should refer to the application of Recommendations 10, 11, 12, 15, and 17, among other Recommendations relevant to VASPs, and apply the appropriate CDD, recordkeeping, and other measures accordingly."

A esse propósito, estudos do Massachusetts Institute of Technology[66] indicam que o *deep learning* já é capaz de eliminar falsos positivos usando análise gráfica, adicionando eficiência ao método de identificação das contas em moedas digitais que estão mais associadas ao histórico de operações ilegais. Há, a partir dessa constatação, a possibilidade de usar contratos inteligentes para que, preenchidas determinadas condições, as *exchanges* de criptoativos enviem automaticamente (*compliance by design*) alertas com os dados dos donos das contas para as autoridades competentes. No caso do Brasil, seria possível criar regras algorítmicas para que, uma vez preenchidos os requisitos de alerta tradicionalmente usados pelo Conselho de Controle de Atividades Financeiras (Coaf) -- agora Unidade de Inteligência Financeira -, esse órgão recebesse os dados (com as informações estritamente necessárias) das contas suspeitas.

Ainda em termos de segurança, é possível casar o uso de protocolos KYC (*know your customer*) com contratos inteligentes e alguma forma de segurança digital para que a plataforma somente seja acessada por alguém que preencha os requisitos (inclusive etários) legais. Os contratos inteligentes permitem, ainda, que se imponha ao jogador uma pausa necessária, com o objetivo de reduzir a exposição ao vício. Essa redução do vício é também uma decorrência da eliminação das contas que os apostadores precisavam abrir nos operadores e que, ao separar o *payout* do restante do seu patrimônio, criavam incentivos a que o apostador apostasse todo o dinheiro que eventualmente ganhasse[67]. Com a transferência automática, espera-se que o apostador assimile mais rapidamente que o *payout* já integra o seu patrimônio e que esse patrimônio sofrerá uma perda caso esse valor seja alocado para novas apostas.

[66] Weber et alli (2018).
[67] Zeliter (1997).

É necessário ter em mente, contudo, que o aumento da comodidade, a possibilidade de preservar o jogo remotamente e as estratégias digitais de fidelização[68] podem tornar inconclusivo o efeito de blockchain sobre o vício. Parece-nos, entretanto, que em todos esses casos o fator determinante é o tempo de exposição do apostador e que, portanto, a tecnologia blockchain passa a oferecer ao Estado condições de trabalhar em uma forma efetiva de *compliance by design* que auxilie o apostador a apostar em níveis ótimos. Essa capacidade de desincentivar o vício tende a crescer com a progressiva adoção de recursos tecnológicos hoje ainda pouco acessíveis, como mecanismo de aferição do grau de cansaço, de atenção, ou da expressão do jogador.

Terceiro, o uso de blockchain casa-se com a digitalização dos serviços de apostas, seja pela criação de operadores exclusivamente digitais, seja pela incorporação da tecnologia digital por operadores *brick-and-mortar* via integração vertical.

Dada a característica de descentralização da tecnologia blockchain, a digitalização com essa tecnologia permite o desenvolvimento de inúmeros operadores exclusivamente digitais em plataformas blockchain voltadas para apostas em segmentos os mais diversos -- contribuindo para a atomização do mercado. Além de representar, *per se*, o aumento das opções para o consumidor, a digitalização dos operadores e a verticalização das casas de apostas físicas confere maior comodidade

[68] Segundo Oz e Preiss (2019), o uso de recursos que viciam, ou o aumento do apelo de determinado produto, ou serviço fazem parte dos cursos de universidades como Stanford, onde é ministrado o reconhecido Persuasive Technology Lab. Em 2006, por exemplo, os fundadores do Instagram foram alunos do curso, que tem por objetivo usar a tecnologia para incentivar as pessoas a ter bons hábitos. Cursos como esse ensinam como recompensas para cachorros, a apresentação de cassinos, luzes e estratégias de supermercados alimentam o instinto de comprar mais e jogar mais.

para que o apostador faça o seu jogo de qualquer lugar e para que continue remotamente (*online*) o jogo que iniciou no ambiente físico (ou vice-versa).

A digitalização oferece, também, a possibilidade de que apostadores remotos acessem mercados fora do seu país, com taxas de câmbio acessíveis para criptomoedas (ou criptoativos, para países que, como o Brasil, não reconhecem o curso forçado dos ativos digitais). Finalmente, o recurso às criptomoedas traz para o mercado, também, a população desbancarizada e de países com moedas fracas, que utilizam esses ativos como forma de reservar valor (apesar da oscilação inerente a esses ativos, depositam mais valor na capacidade de as criptomoedas cumprirem a função de reserva de valor, ou de, eventualmente, como ativos financeiros, valorizar-se).

Por essa razão, a verticalização não deve ser *per se* proibida no Brasil -- pelo contrário, estamos diante de um momento oportuno para a integração vertical das atividades dos operadores físicos. A verticalização não deve, por outro lado, gozar de isenção concorrencial (licitude *per se*) e, desse modo, deve ser avaliada casuisticamente pelo Conselho Administrativo de Defesa Econômica, nos termos da Lei nº 12.529, de 30 de novembro de 2011.

Quarto, ao conferir mecanismos para lidar com o vício e a lavagem de dinheiro, a tecnologia blockchain ajuda a reduzir a resistência à aprovação de cassinos e outras formas de aposta no Brasil. A ampliação do mercado de apostas, sujeito à aprovação do Estado -- e que retira do setor o estigma de mercado negro e da seleção adversa -- é mais um incentivo a que os agentes do mercado adiram a uma regulação logarítmica.

Sob essa mesma lógica, o uso de contratos inteligentes permite que do valor do *payout* e da *house edge* sejam imediatamente descontados os tributos, que podem ser enviados tanto para a conta única do Tesouro Nacional, quanto, diretamente, para os beneficiários da arrecadação. Em razão de a tecnologia blockchain viabilizar micropagamentos, esses tributos podem ser descontados a cada operação, ou com a sazonalidade definida pelo Estado. De qualquer modo, a tecnologia é capaz de reduzir a sonegação fiscal.

Quinto, o recurso a blockchain reduz os custos de fiscalização -- inclusive por conta do acesso gratuito à tecnologia de protocolo aberto -, os custos operacionais (inclusive pela desnecessidade de assegurar uma conta de apostas para a guarda de valores dos clientes) e facilita, em um mercado competitivo, o repasse desse excedente para o apostador. Lembre-se de que o apostador pode, ainda, fazer uso de moedas digitais (ou critptoativos, como vale lembrar, são chamados no Brasil) para pagar as apostas, eliminando as tarifas que os bancos costumam cobrar para transferências para casas de apostas.

Sexto, o nascimento da modalidade de apostas de quota fixa tem muito a ganhar com a tecnologia. Isso ocorre porque será mais fácil garantir que o resultado do fato em que se apostou não será adulterado. Ademais, a tecnologia permite que os jogadores formulem os seus próprios jogos nas plataformas -- algo bastante útil nos chamados bolões de Copa do Mundo. Ressalte-se, porém, que blockchain será tanto mais útil quanto mais abertas forem as possibilidades de apostar. A limitação das apostas a

esportes[69] restringe, desnecessariamente, o potencial arrecadatório e o bem-estar dos apostadores.

Sétimo, todos esses fatores somados caminham no sentido de aumentar o número de apostadores e facilitar o seu acesso -- de forma responsável e devidamente controlada -, o que permite que o Brasil, finalmente, explore todo o seu potencial arrecadatório.

O quadro abaixo tenta trazer, de forma mais clara, os benefícios da adoção da tecnologia blockchain:

Tabela 5. Soluções blockchain

Problema	Solução
adulteração do registro	"imutabilidade" dos registros.
exposição do apostador	resguarda privacidade, transmitindo somente informações necessárias.
empecilhos para pagamento do *payout*	*compliance by design* -- pagamento é feito automaticamente, quando haja o vencedor.
auditoria morosa e sujeita a fraudes para adulterar resultado.	*compliance by design* -- algoritmo torna o modelo de auditoria transparente e conhecido *ex ante* pelo apostador.
pagamento somente após o fim de todas as apostas	micropagamentos a cada vitória.
obrigação de custódia da conta do apostador	informações e valores continuam na carteira blockchain do apostador.
custos administrativos	eliminação de custos administrativos com guarda de valores, auditoria e operações bancárias, gerando excedente compartilhado com o

[69] Segundo o art. 29, § 1º da Lei 13.756, de 2018, "[a] modalidade lotérica de que trata o caput deste artigo consiste em sistema de apostas relativas a eventos reais de temática esportiva, em que é definido, no momento de efetivação da aposta, quanto o apostador pode ganhar em caso de acerto do prognóstico".

	consumidor em mercados competitivos.
estrutura concentrada	a descentralização típica de blockchain permite a atomização das casas de apostas e dos tipos de apostas dentro de uma mesma plataforma (aumento das concorrências intermarcas e intramarca).
pouca diversidade	a possibilidade de que cada apostador seja também um inovador torna mais atual a definição de *prosumer*[70].
fraude	valor transferido automaticamente para conta em blockchain assim que identidade for digitalmente verificada.
entrega física do prêmio ao vencedor	entrega remota, preservando a identidade do apostador e a sua segurança pessoal.
caixa preta acerca das regras dos operadores	transparência com relação às regras operadas por meio de algoritmo.
erros tipo 1 e tipo 2 no combate à lavagem de dinheiro	a regulação pode permitir o uso do *deep learning* e de regras *compliance by design* para enviar, automaticamente, informações mais precisas aos órgãos de controle.
ausência de mecanismos para desincentivar o vício	uso de tecnologia para desincentivar o vício.
regulação custosa	a regulação em blockchain depender da contratação de quadros especializados em tecnologia, mas reduz os custos operacionais de auditoria *in loco* e digitais (por meio da *compliance by design*, inclusive quanto aos limites etários das apostas).
arrecadação abaixo do potencial	aumento da arrecadação: maior acessibilidade via digitalização, inclusão da população desbancarizada, inclusão de apostadores internacionais.
sonegação fiscal	possibilidade de eliminação da sonegação fiscal nas operações

[70] Expressão cunhada por Alvin Toffler e que identifica indivíduos que não só consomem, mas também produzem serviços na internet, seja fazendo algo novo, seja complementando aquilo que outrem produziu originalmente.

	digitalizadas: contratos inteligentes criam *compliance by design*, inclusive por meio de micropagamentos.

Qual, afinal, o papel do regulador?

Apesar da euforia com que o mercado tem recebido a chegada da tecnologia blockchain e venha asseverando que a tecnologia é capaz de eliminar a necessidade do regulador, essa conclusão é bastante inexata no momento em que nos encontramos. Essa inexatidão decorre essencialmente do equívoco habitual de definir os registros blockchain como imutáveis, o que exigiu a publicação do artigo seminal de Walch (2017).

Como fizemos questão de destacar neste trabalho, o grau de segurança dos registros de uma blockchain depende dos seus mecanismos de governança, em particular das suas regras de consenso. A possibilidade de que ataques de 51% dos mineradores de uma blockchain pública, ou de que decisões dos administradores de uma blockchain privada permitam não só alterar as regras da blockchain, como também apagar os registros dessa alteração, demonstra que a tecnologia, desacompanhada de uma regulação algorítmica inteligente (*smart regulation*) que traga transparência quanto à governança blockchain de cada plataforma e reduza a assimetria informacional, pode não ter o seu potencial plenamente aproveitado.

Fica claro, portanto, que o mercado de jogos, em particular com a chegada de blockchain, exige a presença de um ator que seja capaz de aferir regras de consenso definidas algoritmicamente e assegurar a regularidade de certos negócios e o amparo da lei para o ressarcimento das apostas fraudadas pelos operadores de apostas. Essa

atividade de certificação de blockchains, também defendida por Fenech (2019), deve ficar com um agente a que a população atribua neutralidade e capacidade técnica.

Uma vez que o cidadão comum não tem, hoje, a capacidade de aferir, sozinho, a qualidade de uma casa de apostas em blockchain -- em particular, em razão do elevado volume de operadores de fachada *online* -- e que esse mesmo cidadão-apostador sente-se tecnicamente incapaz de aferir regras de governança definidas em algoritmo, faz bastante sentido, ao menos durante essa fase de transição, incluir os serviços lotéricos digitais entre os bens credenciais (*credence goods*). Bens credenciais são aqueles que, dada a incapacidade técnica de o consumidor aferir, por si só, a sua qualidade, é necessário conferir a terceiro o papel de escolha do produto, ou serviço a consumir. Trata-se de característica inerente ao mercado de medicamentos, por exemplo, no qual o papel de escolha é confiado ao profissional da saúde e ao Estado.

O fato de os bens, ou serviços serem credenciais não impede que o consumidor, na inexistência de regulação (ou certificador), ou na existência de regulação (ou certificador) ruim, resolva escolher por conta própria. Não é à toa que, hoje, na ausência de uma atuação adequada dos reguladores quanto à certificação das apostas digitais e na pouca confiança depositada nas revistas especializadas em certificar os operadores digitais, os apostadores são colocados diante das opções de não apostar, ou apostar no escuro. O apostador contumaz, não é necessário dizer, não raramente opta pelo salto no escuro.

É nesse sentido que uma regulação vanguardista demanda, segundo Shrepel (2019(b)), uma abordagem de incentivos. Na esteira da Lex Cryptographia sugerida por Wright e De Filippi (2015) e encampada pela academia, é ainda necessário que o

regulador incentive a incorporação de algoritmos desenhados pelo regulador no código da plataforma e que, dessa forma -- para citar a expressão de Buterin, tal qual trazida por Pilkinton (2015)[71] -, seja o regulador chamado a entrar no jogo, alterando a sua forma, mas sem destruir o modelo.

Por essa razão, propomos que a regulação de loterias, com a providencial abertura das apostas de quota fixa para a ampla concorrência, adote um viés de inclusão, que confira permissão a qualquer operador que se submeta à sua regulação algorítmica. Essa aderência pode ser incentivada, seja pelos benefícios que traz à própria casa de apostas, seja mediante a aposição de selos de aprovação com diferentes gradações pelo regulador -- *nudges* na direção de indicar ao apostador qual plataforma oferece segurança.

O recurso à regulação logarítmica em blockchain demanda, entretanto, a dedicação de servidores especializados em avaliar a governança das plataformas, escrever códigos para a regulação algorítmica e redigir contratos inteligentes. Ademais, devem ser capazes de acompanhar a evolução da tecnologia para que a regulação do mercado não fique defasada e colaborar com a disciplina internacional do tema -- o que, em última instância, pode ser um argumento favorável à criação de uma agência dedicada a regular o mercado de apostas no Brasil.

[71] *"Buterin (2015b) has identified several weaknesses intrinsic to immutable public ledgers. Firstly, in some cases, such as land registries, reversibility is a desirable property of the blockchain, as government-uncontrollable registries risk not being recognized at all. Buterin (ibid.) admits that a public ledger with a smart contract allowing the government to enter the game, nuances this conclusion, without undermining it (ibid.)."*

Walch (2017) sugere que a regulação de blockchain seja feita levando em consideração os conhecimentos técnicos adequados, que sejam contratados especialistas nas mais diferentes áreas, e que haja frequente cooperação internacional -- o que está em linha com a nossa proposta de criação de uma unidade para criptorregulação. Segundo a professora[72]:

> "Autodidatas não são uma possibilidade. nesse cenário, equipes de reguladores diferentes podem trabalhar para tornar-se especialistas internos naquela tecnologia. De fato, esse tem sido o caso de muitos reguladores, muitos deles criando um time interno para 'blockchain', ou para 'DLT' para guiar o conhecimento e a experimentação. Entretanto, a natureza multidisciplinar da tecnologia cria um desafio grandioso, em razão de a profundidade de conhecimento exigir o domínio de campos como economia, ciência da computação, direito, finanças e criptografia.
>
> Com o objetivo de aliviar o problema da especialização, os reguladores também contratos especialistas internos, trazendo conhecimento para dentro do setor. Mas isso pode ser mais difícil quando o assunto é a tecnologia blockchain, uma vez que desenvolvedores com experiência na área estão sendo muito demandados e os reguladores podem ser incapazes de competir com os salários pagos pelo setor privado. Ademais, há relatos frequentes de que o número de pessoas com verdadeira especialização nesse assunto é extremamente limitado."

Nessa mesma linha, a Financial Action Task Force recomenda que[73]:

> "Os supervisores também deveriam desenvolver um conhecimento profundo do mercado de prestação de serviços a criptoativos, da sua estrutura e do seu papel no sistema financeiro e na economia do país, para melhor embasar a sua avaliação do risco no setor. Isso pode demandar investimento em treinamento, pessoal, ou outros recursos que capacitem os supervisores a ganhar o conjunto de competências e especialidades necessário para regular e supervisionar os

[72] "Self-education is also a possibility. In this scenario, teams within different regulators can work to become internal experts on the technology. Indeed, this has been the case with many regulators,with many creating a 'blockchain' or 'DLT' internal team to steer knowledge and experimentation. However, the multidisciplinary nature of the technology makes its mastery challenging, as deeply understanding the technology requires knowledge of fields including, among many others, economics, computer science, law, finance, and cryptography.
To help remedy the expertise problem, regulators can also hire internal experts, bringing expertise in-house. This could be difficult with blockchain technology, however, as developers with experience in the area are in great demand, and regulators may be unable to compete with high private sector compensation. Further, there are frequent reports that the number of people with true expertise in the topic is extremely limited."

[73] "Supervisors should also develop a deep understanding of the VASP market, its structure, and its role in the financial system and the country's economy to better inform their assessment of risk in the sector. This may require investing in training, personnel, or other resources that enable supervisors to gain the practical skillsets and expertise needed to regulate and supervise the range of VA providers and activities described in the VA services or business models at the onset of this Guidance."

> prestadores de serviços, as atividades, ou o modelos de negócios trazidos por este guia."

Walch (2017) sugere, ainda, tal qual vem sendo adotado no mundo (inclusive no Brasil) em relação a *fintechs*, que sejam criadas *sandboxes* regulatórias ("*regulatory sandboxes*")[74]:

> "Esses porto seguros, que vêm sendo adotados, ou propostos em um número crescente de países ao redor do globo, permitem que certas *fintechs* escapem de sanções regulatórias na sua fase inicial, ao mesmo tempo em que asseguram certa proteção para os consumidores."

Mas adverte que, dadas as restrições impostas ao funcionamento nessa fase inicial (ambiente controlado), as *sandboxes* não permitem tirar ilações sistêmicas[75]:

> "Apesar de a abordagem por *sandboxes* poder contribuir na avaliação dos novos modelos de negócios, ou tecnologias em um ambiente controlado, os reguladores devem estar cientes das limitações dessas conclusões tiradas dos experimentos conduzidos em *sandboxes*. Ao mesmo tempo que as atividades em *sandboxes* podem revelar consequências para o consumidor sob a perspectiva microprudencial, elas não podem revelar as consequências macroprudenciais (sistêmicas) das atividades, uma vez que não foram testadas em uma escala mais ampla que pudesse dar indicações significativas de como interagiriam com o sistema financeiro mais amplo. Assim, o simples fato de uma empresa *fintech* (ou blockchain) passar a impressão de funcionar bem em um teste realizado com um conjunto limitado de consumidores não autoriza que se entenda que o risco sistêmico, ou de contágio esteja completamente afastado."

Considerações finais

Apesar de bastante recente, a tecnologia blockchain já está sendo utilizada, com sucesso, em muitos mercados e tem um potencial inexplorado bastante amplo. O seu benefício, até o presente momento, está associado ao desenvolvimento de registros

[74] "These safe harbors, which have been adopted or proposed in a growing number of countries around the world, allow certain fintech companies to escape regulatory sanction in their startup phase, while protecting consumers in specified ways."

[75] "While the sandbox approach may be helpful in evaluating new business models or technologies in a controlled setting, regulators should be mindful of the limitations of the conclusions they can draw from the experiments conducted in the sandboxes. While the sandbox activities may reveal consequences to consumers from a micro-prudential perspective, they can't reveal the macro-prudential (systemic) consequences of the activities, because they have not been tested on a broad scale that would give meaningful indications of how they would interact with the larger financial system. So, just because a fintech (or blockchain) company appears to work fine in trial run with a limited set of consumers does not mean that it has been vetted from a systemic risk or contagion perspective."

que prescindam de certificadores, ou que reduzam os custos de certificação: com o recurso à tecnologia, cumprirá ao usuário, ou ao certificador o papel de auditar algoritmos, cujo acesso é público.

A tecnologia pode, por outro lado, garantir o anonimato dos usuários e das próprias operações (via *tumblers*). Se associado ao cumprimento da lei, blockchain pode viabilizar, especialmente com o auxílio de contratos inteligentes, *deep learning* e bens inteligentes (viabilizados com o advento da IoT), que a privacidade seja, pela primeira vez na história, garantida, ao mesmo tempo em que o acesso das autoridades aos dados necessários para o cumprimento da lei é escalonado na exata medida necessária (*compliance by design*).

O grande salto, aqui, está em criar incentivos (*nudges*) a que o cidadão e os empreendedores dêem transparência aos seus dados, em lugar de protegê-los de forma irrestrita para viabilizar a realização de transações ilícitas. No mercado de jogos, o acesso às informações essenciais por meio de protocolos KYC pode decorrer do papel de certificador que alguém precisará ocupar, enquanto a tecnologia blockchain não for compreendida pelos apostadores. Ao caracterizarmos as loterias como bens credenciais, não só identificamos que o apostador esteja interessado em receber a indicação de onde apostar por parte de alguém em quem confie, como conferimos a esse certificador o poder de ditar quem estará dentro do mercado e quem está fadado ao insucesso.

A condição de credenciador exige, porém, que o regulador esteja atento ao funcionamento da tecnologia, que ele ampare o consumidor que seja prejudicado pela sua incapacidade de antever desdobramentos da tecnologia e que esteja aberto a implementar uma regulação dinâmica que adapte as normas ao surgimento de

tecnologias disruptivas -- ou de novas funcionalidades disruptivas das tecnologias preexistentes.

Embora vanguardista, a regulação algorítmica de incentivos no mercado de apostas, com incentivos à incorporação da tecnologia blockchain, tem o potencial de trazer os agentes econômicos para a transparência e para o cumprimento da lei, elevando o bem-estar do consumidor (que passa a ter mais opções de entretenimento com qualidade assegurada) e a captação de recursos a serem utilizados para a segurança pública, para a cultura, para o esporte, para a seguridade social, nos termos da Lei nº 13.756, de 2018. Ao mesmo tempo, evita que, à margem da lei, os empreendedores sejam incentivados a usar a tecnologia para fraudar a regulação e servir de instrumento ao crime.

Referências

Arantes, Gladstone (15 de janeiro de 2019). Entenda as Blockchains Públicas e Privadas. *In* Infochain. Disponível em https://infochain.com.br/entenda-as-blockchains-publicas-e-privadas/. Acesso em 16 de julho de 2019.

Benkler, Yochai. The wealth of networks : how social production transforms markets and freedom. New Haven: Yale University Press, 2006.

Catalini, Christian; Gans, Joshua S.. Some Simple Economics of the Blockchain (April 20, 2019). Rotman School of Management Working Paper No. 2874598; MIT Sloan Research Paper No. 5191-16. Disponível em SSRN: https://ssrn.com/abstract=2874598 or http://dx.doi.org/10.2139/ssrn.2874598. Acesso em 29 de agosto de 2019.

Connor. John M. Cartel Detection and Duration Worldwide. CPI Antitrust Chronicle. September 2011 (2).

Connor, John. Global Price Fixing. Springer, 2007.

d'Anconia, Frisco. How Blockchain Technology is Taking Gambling Industry to New Level (4 de setembro de 2017). *In* Cointelegraph. Disponível em https://cointelegraph.com/news/how-blockchain-technology-is-taking-gambling-industry-to-new-level. Acesso em 29 de agosto de 2019.

Dwyer, Gerald P.. The Economics of Bitcoin and Similar Private Digital Currencies (July 8, 2014). Disponível em SSRN: https://ssrn.com/abstract=2434628 or http://dx.doi.org/10.2139/ssrn.2434628. Acesso em 29 de agosto de 2019.

Eghdami, Darius. How blockchain can change sports betting (February 22, 2019). *In* Techtalks. Disponivel em

https://bdtechtalks.com/2019/02/22/blockchain-sports-betting/. Acesso em 29 de agosto de 2019.

European Commission. Commission Staff Working Document accompanying the White Paper on Damages actions for breach of the EC antitrust rules. COM(2008) 165 final {SEC (2008) 404} {SEC (2008) 406}.

European Commission. Commission Staff Working Paper accompanying the White Paper on Damages actions for breach of the EC antitrust rules. COM(2008) 165 final {SEC (2008) 405} {SEC (2008) 406}.

Financial Action Task Force. Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (2019). Paris. FATF, Paris. Disponível em www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html. Acesso em 6 de setembro de 2019.

Gainsbury, S., & Blaszczynski, A. (2017). How blockchain and cryptocurrency technology could revolutionize online gambling. Gaming Law Review, 21(7), 482-492.

Gerald Fenech. Blockchain In Gambling And Betting: Are There Real Advantages? (30 de janeiro de 2019). *In* Forbes. Disponível em https://www.forbes.com/sites/geraldfenech/2019/01/30/blockchain-in-gambling-and-betting-are-there-real-advantages/#55fa673a7c63. Acesso em 29 de agosto de 2019.

Haffke, L., Fromberger, M. & Zimmermann, P. Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them. J Bank Regul (2019).

Hajdarbegovic, Nermin (2014). Regulated Gambling platform Cozy Games accepts bitcoin in industry first. *In* Coindesk (24 de outubro de 2014). Disponível em

https://www.coindesk.com/cozy-games-becomes-first-regulated-igaming-operator-accept-bitcoin. Acesso em 29 de agosto de 2019.

Kozak, Timothy. Blockchain in Casino Industry: On the Verge of Eruption (27 de junho de 2019). *In* Intellectsoft. Disponível em

https://www.intellectsoft.net/blog/blockchain-in-casino-industry/. Acesso em 29 de agosto de 2019.

Lessig, Lawrence. Code -- version 2.0. New York: Basic Books, 2006.

Mason, Bob. How the Blockchain Technology is changing the Gambling Industry. In FXEmpire (2018). Disponível em

https://www.fxempire.com/education/article/how-the-blockchain-technology-is-changing-the-gambling-industry-486080. Acesso em 29 de agosto de 2019.

Mire, Sam. Blockchain In Online Gambling: 12 Startups To Watch In 2019 (28 de janeiro de 2019). *In* Disruptor Daily. Disponível em https://www.disruptordaily.com/blockchain-startups-online-gambling/. Acesso em 29 de agosto de 2019.

Nakamoto. Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System (2008). Available on https://bitcoin.org/bitcoin.pdf. Acesso em 29 de agosto de 2019.

OECD. Blockchain Technology and Competition Policy - Issues paper by the Secretariat. June 8, 2018. Disponível em https://one.oecd.org/document/DAF/COMP/WD(2018)47/en/pdf. Acesso em 29 de agosto de 2019.

OECD. Hard Core Cartels: Third report on the implementation of the 1998 Council Recommendation (2005). Disponível em

https://www.oecd.org/daf/competition/cartels/35863307.pdf. Acesso em 29 de agosto de 2019.

Østbye, Peder, Collusion Risk and Responsibility in Public Cryptocurrency Protocol Development (18 de março 2019). Disponível em https://ssrn.com/abstract=3354868 or http://dx.doi.org/10.2139/ssrn.3354868. Acesso em 29 de agosto de 2019.

Parks, Howard. Is Blockchain Set to Disrupt the Online Gambling Industry? (9 de junho de 2019). In LegitGamblingSites. Disponível em

https://www.legitgamblingsites.com/blog/is-blockchain-set-to-disrupt-the-online-gambling-industry/. Acesso em 29 de agosto de 2019.

Pilkington, Marc, Blockchain Technology: Principles and Applications (18 de setembro de 2015). Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar, 2016. Disponível at SSRN: https://ssrn.com/abstract=2662660. Acesso em 29 de agosto de 2019.

Rosenberg, Scott. How Bitcoin's Blockchain Could Power an Alternate Internet (13 de janeiro de 2015). *In* Wired. Disponível em https://www.wired.com/2015/01/how-bitcoins-blockchain-could-power-an-alternate-internet/. Acesso em 29 de agosto de 2019.

Secretaria de Acompanhamento Fiscal, Energia e Loteria. Por trás da sorte. Brasília: Ministério da Fazenda, 2018.

Programa de Parcerias de Investimentos. Secretaria Especial do Programa de Parcerias de Investimentos (SPPI). https://www.ppi.gov.br/loteria-instantanea-lotex. Acesso em 2 de setembro de 2019.

Shrepel, Thibault. Thibault Schrepel, Collusion by Blockchain and Smart Contracts, 33 HARV. J.L. & TECH. (2019).

Shrepel, Thibault. Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox. 3 GEO. L. TECH. REV. 281 (2019).

Thaler, Richard H.; Sunstein, Cass R.. Nudges: como tomar melhores decisões sobre saúde, dinheiro e felicidade. Rio de Janeiro: Objetiva, 2019.

Understanding Bitcoin Traceability. Available on https://bitcoin.org/en/protect-your-privacy. Acesso em 16 de julho de 2019.

Walch, Angela. The Path of the Blockchain Lexicon (and the Law), 36 REV. BANKING & FIN. L. 713, 713 (2017).

Weber et alli. Scalable Graph Learning for Anti-Money Laundering: A First Look. Disponível em https://arxiv.org/pdf/1812.00076.pdf. Acesso em 5 de setembro de 2019.

Woloshyn, Oz e Preiss, Karah. Sleepwalking (2 de maio de 2019). *In* Sleepwalkers. iHeartRadio.

Wright, Aaron e De Filippi, Primavera, Decentralized Blockchain Technology and the Rise of Lex Cryptographia (March 10, 2015). Disponível em SSRN: https://ssrn.com/abstract=2580664 or http://dx.doi.org/10.2139/ssrn.2580664. Acesso em 29 de agosto de 2019.

Young, Jess. The Benefits of Blockchain in the Online Gambling Industry. In The London Economic (13 de maio de 2019). Disponível em

https://www.thelondoneconomic.com/tech-auto/technology/the-benefits-of-blockchain-in-the-online-gambling-industry/13/05/. Acesso em 29 de agosto de 2019.

Zeliter, Viviana A. Rotman. The social meaning of money: pin money, paychecks, poor relief, and other currencies. Princeton University Press, 1997. Originally published in New York: Basic Books, 1994.