JUN/NOV 2018
Revista Semestral

Pi

nº 9
nº 10

Propriedades intelectuais

DOUTRINA

- Entrevista com Antoine Yeretzian (cofundador de Blockchain Partner)
  Delphine Knafo
- *Blockchain* será o futuro da música?
  Marie Soulex, Killian Lefèvre, Clara Zlotykamien
- Qual o lugar para a *blockchain* no direito francês da propriedade intelectual?
  Nicolas Bistin
- Breves notas a propósito da tecnologia *blockchain* e a sua aplicação no âmbito do direito da propriedade intelectual
  Vitor Palmela Fidalgo
- Por que razão irá a *blockchain* revolucionar a propriedade intelectual? Uma aplicação prática ao sector da moda
  Vincent Fauchoux, Amélie Couazé
- O futuro da propriedade intelectual com a *blockchain*
  Amélie Farneau
- Bases de dados: o direito do produtor
  João Pereira Cabral
- O novo regime das entidades de gestão coletiva e as licenças multiterritoriais
  Gonçalo Cil Barreiros

CRÓNICAS DE JURISPRUDÊNCIA

- Direito de Autor
  Os casos Tony Carreira

CARTAS DA LUSOFONIA

- Carta do Brasil
  Rafael Viola
- Carta de Moçambique
  Télio Murrum

Entrevista com Antoine Yeretzian (cofundador de Blockchain Partner*)*[*]

DELPHINE KNAFO
REDATORA CHEFE DA REVISTA *PROPRIÉTÉS INTELLECTUELLES*

Antes de entrar na análise das problemáticas da propriedade intelectual relacionadas com a blockchain*, pareceu-nos interessante debater com Antoine Yeretzian, cofundador de Blockchain Partner, o funcionamento desta tecnologia, as suas múltiplas aplicações práticas relativas à nossa área e a amplitude da revolução por ela prometida.*

Paris, 18 de julho de 2017

Se estiver de acordo, vamos começar pelo princípio. O que é a *blockchain*? Que imagem daria para ilustrar o seu funcionamento?

Definimos, na Blockchain Partner[1], a *blockchain* como uma tecnologia de armazenamento e transmissão de informações, transparente, protegida e funcionando sem qualquer órgão central de controlo. Por extensão, uma *blockchain* constitui uma base de dados que contém o histórico de todas as trocas efetuadas entre os seus utilizadores desde a sua criação. Esta base de dados é distribuída: partilhada pelos seus diferentes utilizadores, sem intermediário, o que permite a cada um deles verificar a validade da cadeia.

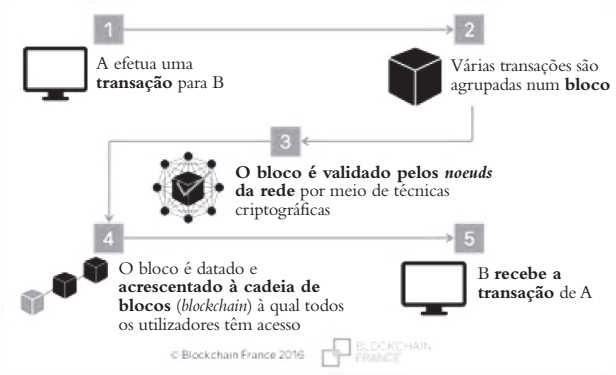
Uma *blockchain* pode por isso ser comparada com um grande livro que rastreia os acontecimentos – um registo – anónimo e infalsificável. Como escreveu o matemático Jean-Paul Delahaye, é preciso imaginar "um grande caderno, que todos podem ler livre e gratuitamente, no qual todos podem escrever, mas que é indestrutível e impossível de apagar".

Como é que isso funciona tecnicamente?

As transações efetuadas entre os utilizadores da rede são agrupadas por blocos. Cada bloco é validado pelos "nós da rede" (os computadores que fazem parte da *blockchain*), de acordo com técnicas que dependem do tipo de *blockchain*.

O esquema mais clássico é o do consenso conhecido por "prova de trabalho" (*proof of work*), no qual diferentes nós da rede (utilizadores que participam na manutenção da infraestrutura) se defrontam para propor a sua versão do bloco em validação. Uma única versão é escolhida à sorte entre esses agentes de validação chamados "mineiros", e a competição recomeça para o bloco seguinte. Esta competição (mineração) assegura a impossibilidade de conluio dos atores e a descentralização efetiva do processo de validação.

Uma vez o bloco validado, é datado e acrescentado à cadeia de blocos. A transação torna-se então visível tanto para o recetor como para o conjunto da rede.



Concretamente, como ocorre uma transação?

Os utilizadores da rede estão identificados por um par de chaves: chave pública/chave privada. A chave pública é um equivalente do IBAN, isto é, um número de identificação que pode enviar a qualquer pessoa para que tenha a sua "morada"; a chave privada é um equivalente do código PIN, e que permite identificar que está na origem da transação. Se quiser agora enviar-me dinheiro *via* uma *blockchain*, deve introduzir a minha chave pública numa aplicação – Bitcoin por exemplo – definir quantas *bitcoin* quer enviar-me, e depois assinar com a sua chave privada.

A sua transação vai então ser agrupada com outras transações num bloco. A rede vai verificar se a transação é válida (quer dizer, que não me está a enviar *bitcoins* que nunca recebeu) antes de enviar esse bloco a todos os exemplares do registo, o que incluirá, definitivamente, a sua transação numa cadeia global. Se me está a seguir, a expressão "enviar *bitcoins*" é, portanto, um abuso de linguagem, uma vez que se trata apenas de um jogo de escrita com um -1 de um

[*] Tradução de Dr. José Martins.

1. Blockchain Partner é a *start-up* líder em França no acompanhamento das tecnologias *blockchain*. Desde a sua fundação em 2015, a equipa organizada em três pólos – formação e aconselhamento, desenvolvimento técnico e acompanhamento jurídico – mobiliza-se na transformação *blockchain* de organizações de referência, nomeadamente o Banco de França, BNP Paribas, a SNCF ou ainda a Renault-Nissan.

lado e um +1 do outro. Resumindo, duplica-se esse jogo de escrita num grande livro de contas que é partilhado um número incalculável de vezes.

A fiabilidade da base de dados que constitui a *blockchain* parece ser o seu melhor trunfo e a razão histórica do seu desenvolvimento. Pode explicar-nos de que forma é que um registo é considerado protegido?

Graças ao carácter descentralizado da *blockchain*. A mudança de paradigma operada pela *blockchain* reside no facto de o registo não ser um exemplar único. O registo deixou de ser um tesouro bem guardado por um terceiro de confiança ao qual os utilizadores enviam solicitações. Trata-se, pelo contrário, de uma multitude de exemplares armazenados nos servidores dos seus utilizadores. Esses exemplares dialogam entre eles ponto a ponto, e o sistema funciona assim sem intermediário centralizador. Os utilizadores validam cada transação graças a um processo transparente que impede qualquer manipulação. Verificam, por exemplo, graças ao registo, que o remetente é realmente proprietário do que foi enviado, e que o recetor dos dados é o correspondente adequado. Só uma vez validados é que os grupos de transações podem finalmente ser inscritos no registo, na forma de uma cadeia de blocos inalteráveis: a *blockchain*.

Sendo o registo conservado e atualizado em tempo real e independentemente por todos os utilizadores, constitui um histórico das transações que não pode ser falsificado. Para manipular esse registo, seria necessário ter acesso e modificar ao mesmo tempo dezenas de milhares de bases de dados, independentes umas das outras – o que seria bem mais caro em material do que o que se poderia ganhar com um ataque desse tipo…

Para lá da descentralização do sistema, da desintermediação das transações, da rastreabilidade de todas as inscrições, e portanto da imutabilidade da rede, quais são as outras características da *blockchain*?

De todas essas características decorre a integridade do dado: o facto de poder provar que o dado é autêntico é capital. Uma outra característica que me parece verdadeiramente interessante é a resiliência do sistema. A rede *blockchain* tem, com efeito, a capacidade de absorver qualquer perturbação que ocorra na cadeia, de se reorganizar e de continuar a funcionar da mesma forma que antes da perturbação ter ocorrido. Esse é incontestavelmente um dos seus maiores trunfos.

Mas a principal característica da *blockchain* é evidentemente o baixo custo de transação que ela possibilita. Da mesma forma que a Internet possibilitou a transmissão de informações a baixo custo e acessível a todos, a *blockchain* vai permitir transferir qualquer tipo de valor com poucos gastos.

Quais são os diferentes tipos de *blockchain*? Como escolher o tipo de *blockchain* a utilizar?

Há uma distinção técnica que nem sempre existiu, mas que faz todo o sentido sobretudo depois destes últimos anos, entre *blockchains* públicas e privadas. Por exemplo, no caso da Bitcoin, a regra de funcionamento é a de que qualquer um pode entrar na rede para fazer transações: é uma rede aberta, uma *blockchain* pública.

O princípio da "rede" ponto a ponto, que são as *blockchain*s, implica que os membros estejam de acordo com as regras do jogo que enquadram a transferência do valor. Por exemplo, uma das regras estruturantes de Bitcoin implica que se acrescente um bloco a cada dez minutos. Para estabelecer estas regras, múltiplas, é evidentemente necessário estabelecer uma arbitragem. Uma das arbitragens mais interessantes é a que apelidamos de "espectro de confiança": uma escolha situada algures entre a segurança e a fluidez das transações que podemos representar desta forma:

Vou dar-lhe dois exemplos.

Podemos dizer que Bitcoin é uma rede de paranóicos: foi construída inicialmente por ciberativistas que queriam enviar dinheiro a pessoas que não conheciam necessariamente, por vezes no outro lado do mundo. Na Bitcoin estamos em presença de transações pontuais operadas entre membros da rede que não têm qualquer laço entre eles. O interesse de cada uma das partes é a de tentar maximizar o seu lucro a curto prazo e, portanto, extorquir o outro… em qualquer caso é isso o que nos diz a teoria dos jogos, a que os criadores da Bitcoin fazem explicitamente referência. Na base destas hipóteses, a Bitcoin foi construída como uma rede ultrassegura de uma ponta à outra, ainda mais do que a do cartão bancário por exemplo, mas neste caso as transações são demasiado lentas e caras.

Na outra ponta do espectro, por exemplo, a nossa *start-up* concebeu uma *blockchain* para o Banco de França. O Banco de França possui um nó e só há nessa *blockchain* alguns outros bancos parceiros que possuem um exemplar desse registo (nó). Trata-se de uma rede fechada – é necessária uma acreditação para poder entrar – e portanto encontra-se num outro nível de confiança, porque obviamente nenhum outro banco tentará extorquir o Banco de França nesta rede! Neste tipo de *blockchain* em que os seus parceiros são de total confiança, pode-se ser menos exigente na verificação das transações e ganhar em fluidez.

Trata-se de começar por definir as arbitragens antes de desenhar a arquitetura de uma *blockchain*.

Qual é o potencial da *blockchain*? Quais são as suas aplicações e os possíveis domínios de aplicação?

A primeira *blockchain* apareceu em 2008 com a moeda digital *bitcoin*. É, por isso, essa a arquitetura subjacente. Mas se a *blockchain* e Bitcoin foram construídas em conjunto, atualmente numerosos atores (empresas, governos, etc.) encaram a utilização da tecnologia *blockchain* noutros sectores além da moeda digital.

O carácter descentralizado da *blockchain* que acabámos de referir, aliado à segurança que daí resulta e à sua transparência, promete aplicações mais vastas do que as do domínio monetário.

Podemos classificar a *blockchain* em três categorias: as aplicações para a transferência de ativos (utilização monetária, mas não só: títulos, votos, ações, obrigações…), as aplicações enquanto registo – também chamadas função de ancoragem – (assegura por isso uma maior rastreabilidade dos produtos e dos ativos), e os *smarts contracts*[2] (trata-se de programas autónomos que executam automaticamente as condições e os termos de um contracto, passando potencialmente para lá da intervenção humana uma vez desencadeados).

Os campos de exploração, esses, são imensos: a saúde, a indústria musical, os votos… De um modo geral, a maior parte dos "terceiros de confiança" centralizados (profissionais da banca, do notariado e dos registos) podem beneficiar da *blockchain*, propondo uma alternância de uma parte da sua atividade nesses sistemas informáticos distribuídos. Com garantias acrescidas (segurança e transparência) e custos reduzidos.

Então porque é que a *blockchain* não tem uma maior expansão? Quais são os limites ou as fraquezas desta tecnologia?

A *blockchain* tem três grandes limites. Antes de mais, a "escalabilidade" – ou dimensionamento – isto é, a capacidade de a *blockchain* se adaptar à mudança da ordem de grandeza da procura. Há, com efeito, e ainda hoje, limites quanto ao número de transações que podem ser realizadas em cada segundo. Na Blockchain Partner pensamos que, se essas limitações técnicas puderem ser rapidamente resolvidas graças ao desenvolvimento das tecnologias, seremos confrontados com o obstáculo inerente a qualquer tomada de decisão numa *blockchain* – a ausência de um poder central decisório. Sendo um protocolo de trocas ponto a ponto cujas regras do jogo estão à partida definidas, não há por isso um grande chefe da *blockchain* que decida como é que vai ser concretizado esse protocolo. Por exemplo, na rede Bitcoin, que se encontra completamente saturada, foram propostas numerosas soluções para redimensionar e resolver o problema da saturação, mas os membros da rede nem sempre estão de acordo entre eles para saber qual delas aplicar, mesmo que ultimamente tenha havido progressos neste domínio. Este é o grande problema das redes descentralizadas, deparamo-nos com questões de *governance* muito fortes relativamente às quais os nossos modelos (negociações bilaterais, democracias representativas, etc.) não respondem de forma adequada.

O segundo limite é o da experiência do utilizador, uma vez que ainda hoje estamos nesta fase muito a montante. Há muita investigação e desenvolvimento neste sector, experimentações, mas para o utilizador final, não é ainda nem simples nem transparente.

Finalmente, falta resolver os problemas de regulação relativamente aos quais não vou insistir, uma vez que eminentes juristas abordam esse tema nesta revista.

Há o hábito de apresentar a *blockchain* como um novo desafio a encarar, uma nova revolução à qual o direito da propriedade intelectual se deveria adaptar. Não fornecerá esta tecnologia, antes de mais, novas soluções e utensílio suplementar para proteger esses direitos? Quais poderiam ser as aplicações concretas da *blockchain* no domínio da propriedade intelectual?[3]

Há, antes do mais, a técnica da ancoragem (ou datação), que é uma das mais belas aplicações de uma rede íntegra descentralizada. Trata-se de registar metadados – sobre o que estamos a trabalhar – na *blockchain*. A ancoragem consiste no registo da prova do documento numa *blockchain*, o que permitirá em seguida provar que eu estava na posse desse documento no instante T (o momento da ancoragem). Isso não é suficiente para mostrar que fui eu a criar esse documento, mas apenas que o tinha nesse instante T. A vantagem da *blockchain* é a de podermos constituir este tipo de provas de existência com muita frequência, fazendo um grande número de registos a preços muito reduzidos em comparação com o tipo de registo que podemos fazer num notário, num oficial de justiça ou num escrivão, por exemplo[4]. Que eu saiba, não há, neste momento, em França, jurisprudência que reconheça a posse de um documento graças a esta ancoragem, mas ninguém dúvida de que isso será aceite pelos juízes, desde que lhes seja explicado o funcionamento da *blockchain*. Há já atualmente dezenas de milhares de milhões de dólares que estão seguros graças a esta técnica.

Pode explicar-nos como é que funciona tecnicamente? O que é a célebre função "hash"?

Para ancorar um documento numa *blockchain*, aplica-se uma função *hash* a um documento digital. A função *hash* é uma função matemática estandardizada. O resultado de uma função *hash* é um código informático, uma sequência de 64 caracteres. Assim, um documento, seja ele uma foto, um *pdf*, uma apresentação *powerpoint*, uma imagem… que é submetida à função recebe um *hash* preciso. Por exemplo, se alterarmos um pixel de uma foto, ou se suprimirmos uma vírgula a um texto, tal dará lugar a um *hash* diferente. Ao contrário, se passarmos o mesmo documento dez anos na função *hash*, obteremos exatamente o mesmo *hash*.

Deste modo, se eu "*hash*" um *pdf* no qual se encontra um esboço de um vestido, obtenho uma série de caracteres. Se registar esse resultado numa *blockchain* pública, estarei em condições de provar que no momento em que essa ancoragem se realizou, estava na posse desse esboço de vestido em particular, uma vez que perante um juiz vou poder demonstrar que o *croquis* de vestido "*hashisado*"[5] apresenta exatamente o mesmo resultado, a mesma série de caracteres

2. A questão dos *smarts contracts* é tratada mais adiante na resposta à pergunta sobre o gestão da propriedade intelectual através da *blockchain*.

3. Esta questão é igualmente abordada pelo Professor Nicolas Binctin nesta revista, no artigo "Quelle place pour la *blockchain* en droit français de la propriété intelectuelle?"
Este artigo está, também, incluído neste número 9.

4. Para maiores desenvolvimentos da *blockchain* enquanto registo que assegura a prova de existência das criações de moda e *know-how*, ver nesta revista o artigo de V. Fauchoux e A. Gouazé, "Porquoi la *blockchain* va revolutionner la propriété intelectuelle? Application pratique au secteur de la mode". Este artigo está, também, traduzido neste n.º 9.

5. NT: "hashé", no texto original francês.

do que aquele que eu "*hashei*"[6] no momento da ancoragem, momento que tem igualmente um data precisa graças à fiabilidade da *blockchain*.

Ao invés, e o que é interessante, desta série de caracteres, do resultado do *hash*, não se pode regressar ao esboço do vestido. Há evidentemente um desperdício de informação entre os 64 caracteres que compõem o resultado do *hash* e o esboço do vestido, ou uma foto. A função de *hashisação*[7] criptográfica é o que chamamos uma função de sentido único, o que quer dizer que o cálculo da função de *hashisação* é fácil e rápido, enquanto o cálculo da sua função inversa não é na prática possível. Por isso, quando ancoramos o documento na *blockchain*, só um cunho digital desse documento é conservado (o resultado do *hash*), mas não o documento em si. É impossível encontrar o documento original apenas a partir de um único registo. Esta técnica permite por isso assegurar a confidencialidade dos dados enviados para a *blockchain*, tornando assim público, e verificável, o facto de termos ancorado um documento num momento preciso. Só dados não sensíveis são, portanto, ancorados na *blockchain*.

Resumindo, o interessante é que perante um juiz podemos demonstrar que estávamos na posse desta criação, ou conhecimento, uma vez que podíamos ancorar a sua representação na *blockchain* num momento preciso. Diante de um juiz apresentamos a criação em litígio, passamo-la à função *hash* e mostramos-lhe que obtivemos exatamente a mesma sequência de caracteres que ancorámos na *blockchain* no momento T. A enorme vantagem do recurso à *blockchain* reside no facto de o número de ancoragens ser ilimitado…

Exatamente. E com efeito, quase que podemos registar as criações de forma contínua.

O procedimento base será fazer um *hash*, depois uma transação, por ancoragem, por documento. Mas na utilização de uma *blockchain* pública, como Bitcoin ou Ethereum, a transação é paga, e se queremos ancorar o trabalho dos gráficos de uma empresa é melhor fazer "*hash de hash*" para agrupar todos os documentos num *hash* único por dia. Graças a alguns protocolos, como *Chainpoint*, podemos fazer 1 milhão de ancoragens por dia pelo custo de uma transação, o que significa 10 ou 15 cêntimos por dia. Comparado com os atuais custos de prova, compreende-se o interesse financeiro. É o que aliás explica que sejamos contactados sobre este tema por um grande número de instituições e atores económicos.

Quais são os limites desta função de ancoragem?

Para o vosso sector, o principal limite prático é o facto de a ancoragem não provar que quem ancora o documento é o seu autor. Nada prova que foi ele que criou o que o documento contém, só atesta que a pessoa que fez a ancoragem do documento o tinha em seu poder, tinha conhecimento do que ele continha, num momento determinado. Evidentemente que isso não constitui prova da sua propriedade.

E, tecnicamente, existem ainda alguns limites práticos à ancoragem. Reportam sobretudo ao formato do ficheiro. Se realizo uma ancoragem do mesmo conteúdo em *pdf* ou em *jpg*, tal não dará lugar ao mesmo *hash*, o que é uma verdadeira limitação prática. Do mesmo modo, se aparecer uma nova versão de *pdf*, não se obterá o mesmo *hash*. Tudo isto coloca o problema das atualizações.

O segundo limite técnico reside no facto de, mesmo assim, a ancoragem na *blockchain* não emancipar a gestão documental. Graças à *blockchain* podemos provar que no instante T estávamos na posse de um documento que responde aquele *hash*, mas isto pressupõe poder produzir o documento de base, o que impõe ter de conservar os documentos ancorados à margem da *blockchain*.

Estes dois limites são, entretanto, os que já se encontram entre os meios digitais – custosos – de prova de existência que conhecemos atualmente, e que repousam sob o mesmo princípio. Quando alguém nos diz "autenticamos a integridade dos vossos ficheiros sem os retermos" utiliza um *hash*, mas é essa pessoa que os armazena em vez de os colocar na *blockchain*.

No futuro, o limite da ancoragem reside no facto de, infelizmente, não ser de todo impossível que daqui a 20 ou 100 anos, os algoritmos que estão na origem desta prova de existência, sejam "quebrados", isto é, que se torne "fácil" produzir documentos cujo *hash* seja exatamente igual a um *hash-cible* (e provocar deste modo o que designamos de colisão). Um falsário poderia então forjar um documento que correspondesse a um *hash* anteriormente por ele ancorado na *blockchain*, e assim antedatar um documento. Apesar de tudo, será necessário por uma revolução tecnológica e matemática superior à que conhecemos no decurso dos últimos 100 anos, uma vez que, neste momento, isso necessitaria, para um único *hash*, utilizar toda a potência de cálculo do planeta em regime pleno durante alguns milhares de milhões de anos…

Existem outros impactos possíveis da *blockchain* na propriedade intelectual?

A segunda aplicação que me parece interessante é a da gestão da copropriedade. Trata-se de algo que o nosso direito, os nossos sistemas e as nossas instituições gerem atualmente muito mal, mas que está no cerne da ideia da *blockchain*, no próprio facto da sua origem simultaneamente *open source* e descentralizada. Existe uma criatividade espantosa neste domínio para redefinir o que significa realmente "possuir" um bem. E o mesmo se aplica à questão de saber a quem pertence uma rede, um código, um serviço, e que direito é que tal possibilita; e os utensílios desenvolvidos podem ser aplicados a outros tipos de propriedade, nomeadamente a intelectual. A *blockchain* pode, por exemplo, ajudar a identificar um autor que contribuiu, e a determinar em que medida, e ainda ajudar a gerir os resultados da exploração. A diminuição do custo de transação permite também valorizar financeiramente pequenas contribuições que não eram, até então, localizadas, uma vez que o montante que

6. NT: idem.
7. NT: "hashage", no texto original francês.

originavam era inferior ao necessariamente utilizado para as localizar e compensar.

Tomemos um exemplo muito simples: um pintor decide apelar a mecenas para financiar uma obra e propõe-lhes a copropriedade. Abre um *smart contract*, e a troco de dinheiro (criptomoeda), devolve ao remetente "fichas" que simbolizam uma parte da propriedade. Trata-se de um ativo digital tangível, seguro, vendável, oponível. Quanto mais eu tiver contribuído mais fichas tenho. É universal, barato e quase instantâneo. O pintor pode, em seguida, redistribuir aos possuidores dessas "fichas" uma parte ou a totalidade dos lucros da venda da obra, transformar essas "fichas" em convites VIP na inauguração da sua próxima exposição e até solicitar a esses possuidores *via* um sistema de voto (facilmente realizável, com 1 "ficha" = 1 voto) sobre o futuro próximo da sua obra-prima… Analisada sob este ângulo, a *blockchain* liberta o financiamento tradicional das suas barreiras técnicas e contrapartidas "clássicas" e, por conseguinte, reinventa a copropriedade.

E como é que funciona a gestão da propriedade intelectual via a *blockchain*, por exemplo a gestão dos contratos e das *royalties* que referiu?

Os membros da *blockchain* podem organizar-se em ponto a ponto (isto é, sem intermediário) para estabelecer a gestão da propriedade intelectual. Podemos inscrever as copropriedades no registo *blockchain*, afetando percentagens de detenção das propriedades intelectuais a diferentes membros da cadeia. Graças às transações que podemos realizar via *blockchain*, podemos alugar, ceder ou vender uma parte dessa propriedade intelectual. Podemos igualmente gerir licenças cujos direitos de utilização podem ser representados por *token* ("fichas"). O *token* pode ser diretamente cedido ou ligado a um *smart contract* que preveja as condições de circulação entre os membros da cadeia. Podemos, por isso, a cada momento ver quem detém a propriedade intelectual em causa.

Além disso, a partir do momento em que somos capazes de gerir a propriedade com *tokens*, é possível afetarmos diretamente os resultados de exploração comercial do direito em causa ao possuidor da ficha se, nessa mesma *blockchain*, ou numa *blockchain* conectável, existirem fluxos monetários em criptomoeda. O caso clássico é o da música. Os *tokens* podem, por exemplo, corresponder a percentagens de criação de valor de um excerto de música. Imaginemos que a repartição desse excerto seja a seguinte: 50% para o produtor, 25% para o cantor e 25 % para o guitarrista; por isso, afetaremos 2 *tokens* ao produtor, 1 *token* ao guitarrista e 1 *token* ao cantor. Assim que o dinheiro chegar ao *smart contract* dedicado a receber *royalties* por esse excerto, haverá instruções para distribuir esse dinheiro pelos possuidores de *tokens*. O *smart contract* permite por isso uma gestão *adequada*, segura e automatizada dos *royalties*.

É possível imaginar que a *blockchain* possa trazer soluções em matéria de combate à contrafação?

Podemos muito bem imaginar haver amanhã um registo mundial que faça o recenseamento dos atores do mundo da criação, da sua integridade em matéria de respeito da propriedade intelectual ou da confidencialidade das transações. As economias da reputação podem trazer novas soluções em matéria do combate à contrafação. Podemos no quadro de uma *blockchain* pormo-nos de acordo sobre as características da reputação dos atores. Esse registo permitiria aos respetivos membros filtrar os seus eventuais parceiros em função da sua reputação na *blockchain*, podendo as arbitragens realizar-se de forma automatizada. Esse sistema seria seguramente mais eficaz do que as sanções económicas. Podemos muito bem imaginar que os grandes grupos de luxo se reúnam para desenvolver entre eles uma aplicação na qual inseririam todos os contenciosos ou problemas com que se têm deparado com fornecedores ou parceiros de uma forma geral, permitindo aos outros atores da cadeia interagir com eles com conhecimento de causa. Isto não é mais do que um exemplo; podemos ainda imaginar uma caderneta digital individual para cada bem de luxo, que trouxesse uma autêntica rastreabilidade a todas as etapas da vida do produto ou da obra. A *blockchain* não é mais do que um tijolo tecnológico, cujas utilizações estão ainda por explorar, exatamente como o TCI/IP e a *web* no final dos anos 90.