Blockchain e o Futuro do Registro de Imóveis Eletrônico – Palestra II

Evento realizado pelo IRIB e pela Academia Brasileira de Direito Registral Imobiliário (ABDRI), no dia 31 de março de 2017, com o objetivo de discutir o potencial, os desafios e as oportunidades da tecnologia de blockchain. Acompanhe a síntese das principais ideias apresentadas em cada palestra

TECNOLOGIAS DE *BLOCKCHAIN*

Palestra proferida por Edilson Osório Junior, cientista computacional, professor e especialista em segurança da informação e infraestrutura, cofundador da Blockchain Academy. Fundador da OriginalMy.com, primeira empresa brasileira a utilizar a tecnologia blockchain.

Entre as inúmeras aplicações de *blockchain* disponíveis estão: compartilhamento de caronas; acesso a *sites* sem o uso de senhas; fechadura inteligente que reserva quartos, envia a chave de acesso, contrata a manutenção, paga pelo serviço e divide o lucro com a empresa mantenedora; e até uma plataforma global de governo descentralizado equivalente a um país na internet com serviços cartorários, advocatícios e de identificação.

Para apresentar o panorama geral da tecnologia *blockchain*, o palestrante abordou as diferenças entre os modelos de *blockchain* disponíveis no mercado, as empresas que utilizam essa ferramenta e a forma como essa tecnologia vem sendo aplicada em áreas como mobilidade urbana e identificação.

***Blockchain*: aplicações descentralizadas**

O principal *blockchain* surgiu em razão de uma demanda de mercado. A partir da crise financeira ocorrida nos Estados Unidos, em 2008, as pessoas passaram a pensar numa forma de dinheiro eletrônico capaz de dispensar a intermediação do sistema financeiro.

Do dinheiro ao *bitcoin*: características

Sabemos que o dinheiro gera direito a se receber algo em troca. Pedras, ouro, sal e papel-moeda são alguns dos itens já utilizados como dinheiro nesse processo evolutivo.

Uma das principais características do dinheiro é sua escassez e dificuldade de falsificação. Sem essas duas características o dinheiro não tem nenhum valor como moeda

de troca.

O dinheiro também tem que ser transportável. Antigamente, as pessoas utilizavam animais como moeda. Hoje, o próprio dinheiro físico pode perder a validade. Recentemente, vimos na Venezuela pessoas carregando pilhas de cédulas para serem pesadas porque o dinheiro já não tinha qualquer valor.

***Bitcoin* é o primeiro dinheiro digital que deu certo**

À medida que o transporte do dinheiro se torna complicado, o dinheiro digital ganha mais espaço. O *bitcoin* é uma evolução das diversas tentativas de introdução do dinheiro digital ao longo do tempo; uma moeda eletrônica e o primeiro dinheiro digital que deu certo; um dinheiro eletrônico equivalente à moeda tradicional. É escasso, tem emissão finita e conhecida.

A recompensa pelo trabalho de mineração representado pelo esforço computacional dispendido para a segurança do negócio é feita com *bitcoins*. O minerador é recompensado com criptomoedas sempre que consegue executar uma tarefa complexa. Essa recompensa tem atraído a atenção de pessoas dispostas a investir em computadores. Trata-se de uma concorrência, é recompensado o minerador que primeiro gerar e inserir o *blockchain* à rede. A cada dez minutos, essa competição é reiniciada. Atualmente, o poder computacional dispendido para a rede do *bitcoin* é equivalente a trezentas vezes o poder computacional do Google.

É consensual. Todos os pontos (máquinas) que se comunicam dentro da rede são capazes de estabelecer um consenso entre o que é certo ou errado.

O Problema dos Generais Bizantinos: a grande questão que o *bitcoin* resolveu

O Problema dos Generais Bizantinos é um experimento mental usado para ilustrar os desafios de planejamento em computação quando se trata de coordenar uma ação por meio da comunicação sobre enlace não confiável.

Dois exércitos se preparam para atacar uma cidade. Cada exército comandado por seu respectivo general acampa em sua própria montanha tendo à frente um vale ocupado pelos defensores da cidade. Para ter êxito, os generais devem atacar ao mesmo tempo. A única forma de comunicar o horário do ataque é enviando mensageiros, mas eles podem ser capturados no vale, o que traz incertezas para a tomada de decisão de ambos os generais. Esse foi o primeiro problema de comunicação de computador que se provou insolúvel na presença de falhas de comunicação arbitrárias.

O Protocolo de Controle de Transmissão (TCP), um dos protocolos em que se apoia a internet, verifica se os dados são enviados pela rede de forma correta, na sequência apropriada e sem erros. No caso das redes de computadores, o problema dos generais bizantinos mostra que o TCP não pode garantir a consistência de estado entre as extremidades, onde falhas de comunicação podem ocorrer.

O *bitcoin* resolveu esse problema matemático replicando cópias de todos os dados do *blockchain* a todos os computadores participantes da rede.

Essa iniciativa possibilitou a identificação de fraudes em qualquer ponto. Uma vez aberto o código (*open source*) e a licença livre, qualquer um pode se autodeclarar possuidor de dez milhões de *bitcoins*, mas uma vez constatada a fraude o participante é excluído automaticamente. Isso é possível graças ao consenso entre os participantes.

Blockchain*: infraestrutura de suporte à rede do *bitcoin

O *blockchain* ainda não era conhecido quando o *bitcoin* surgiu. No próprio documento original de Satoshi Nakamoto (pseudônimo ligado ao desenvolvimento do protocolo do *bitcoin*), o único termo semelhante citado é o *chain-of-blocks*. Essa tecnologia foi explorada de diversas formas. Observada sob outro ponto de vista, notou-se que o grande potencial dela estava em sua própria infraestrutura.

De acordo com essa visão tecnológica, o *bitcoin* é mero insumo. Isso ocorre porque existe um campo de observação no *blockchain* do *bitcoin*, onde é possível jogar uma informação com poucos *bytes*, equivalente à metade de um *tweet*. Com esse pequeno espaço, é possível encadear várias transações, uma atrás da outra, configurando informações mais complexas que poderão ser utilizadas como protocolo.

Uma vez entregue à rede para a transação, o *bitcoin* pode ser recebido por um minerador qualquer, que pode tomar para si aquela transação e inseri-la na rede, fazendo com que diversos especialistas no mundo pudessem olhar para o *blockchain* de forma diferente e para outras finalidades.

E assim fizeram. Criaram satélites à moeda *bitcoin*, criaram plataformas mais inteligentes e capazes de rodar mais aplicações, criaram as chamadas *sidechains*, plataformas que certificam informações esporádicas no *blockchain*, que introduzem um novo conceito de negócio.

Mecanismos de consenso

Alguns exemplos de mecanismos de consenso:

***Proof-of-work* –** O *bitcoin* usa como mecanismo de consenso o *proof-of-work*, prova de entrega ao poder computacional recompensada em caso de sucesso na transação, nos cálculos criptografados complexos. É recompensado o minerador que for mais rápido em dez minutos.

Existe um aspecto ecológico ruim nesse processo. Com trezentas vezes mais poder computacional do que o Google, é imenso o gasto de energia elétrica para o desenvolvimento dessa atividade. No entanto, mesmo com custos altíssimos de energia a recompensa para o registro das informações na rede é em torno de 12,5 *bitcoins* a cada dez minutos.

Proof-of-stake – Enquanto no *proof-of-work* o minerador é recompensado por provar a sua capacidade computacional, no *proof-of-stake* ele precisa provar que é detentor de várias criptomoedas para ser remunerado. O dado preocupante é que se algum milionário adquirir no mercado uma parcela gigantesca das moedas, o consenso ficará sob seu domínio, e a descentralização estará comprometida. Com base nisso, pensou-se em modelos mais democráticos que pudessem favorecer a redução de gastos com a computação.

DPOS – *Delegate proof-of-stake* - um método de consenso que vem sendo testado em algumas criptomoedas de maneira aparentemente satisfatória. Nesse sistema, o computador da comunidade com mais criptomoedas é eleito para fazer a mineração, sendo o lucro obtido dividido com a comunidade. Essa iniciativa visa evitar a centralização por uma única pessoa detentora de muitas moedas.

Leader Elect – Por esse modelo, elege-se um líder para ser seguido por todas as máquinas.

Round-Robin – Algumas máquinas são selecionadas aleatoriamente para fazer a mineração.

***Blockchain*: como funciona essa cadeia de blocos**

Em qualquer tecnologia de *blockchain*,o encadeamento de blocos não é registrado de imediato na rede. No *Bitcoin*, por exemplo, a confirmação do registro ocorre a cada dez minutos. No Ethereum, essa confirmação se dá em aproximadamente dezessete minutos. Em todas elas, a mecânica é a mesma. A transação efetuada fica estacionada em um *pool* de transações pendentes de confirmação. As taxas elevadas das transações são um incentivo para o minerador registrar mais rapidamente a transação no bloco. Supondo que ele seja o primeiro a validar a transação na rede, o bloco é imutabilizado com uma assinatura digital, dando-se início a novo bloco, após dez minutos, para as transações ainda pendentes de confirmação.

É comum as pessoas pensarem que mil confirmações equivalem a mil computadores analisando aquele mesmo bloco. Não, se em quatro blocos abertos a minha transação é a primeira do bloco 1, significa dizer que a minha transação tem quatro confirmações. Quando dizemos que uma transação tem quatro confirmações, significa que a transação 1 do bloco 1 é quatro blocos mais antiga que o bloco atual.

A primeira informação que deve constar a cada novo bloco é a assinatura que fechou o bloco anterior. Essa medida visa evitar fraudes e impedir o minerador de fazer cálculos criptográficos aleatórios, na tentativa de descobrir transações no tempo para encaixá-las no bloco a qualquer tempo.

O encadeamento dos blocos garante a segurança do sistema. Se alguém quebrar uma informação constante da transação 2 do bloco 1,

terá que refazer a assinatura do bloco 2, refazer os blocos 2, 3 e 4, tudo isso no intervalo de dez minutos e antes que todos os computadores do mundo coloquem o bloco 5 na rede. É praticamente impossível.

Descentralização: emissão de criptomoedas pode ser feita em qualquer lugar do mundo

Sabemos que a emissão de dólares é centralizada, mas a de criptomoedas não. Em qualquer ponto do planeta é possível fazer a emissão das criptomoedas, bastando instalar um programa no computador e rodar o *software* de mineração.

No Brasil, a emissão de criptomoedas não é viável. A recompensa em *bitcoins* não cobre o alto custo de energia. Uma máquina de mineração gasta o equivalente a um chuveiro elétrico de 220 volts, ligado por 24 horas. Por conta disso, fazendas de mineração acabaram migrando para locais onde a energia elétrica é barata ou subsidiada. É o caso da maior mineradora da América Latina, uma empresa brasileira sediada no Paraguai graças a um acordo que prevê subsídios em energia elétrica. Essa prática também é comum na África, Islândia e China, onde estão localizadas as maiores fazendas de mineração.

Modelo híbrido: da descentralização à centralização

No modelo híbrido, a descentralização não é total. Os nós se conectam ao minerador, e o principal deles conversa com o restante do planeta, como no caso dos Bancos Centrais.

Desmistificando o paradigma *Bitcoin-Blockchain*

***Bitcoin* moeda/*bitcoin blockchain* –** Há quem entenda que o *blockchain* não existe sem a criptomoeda e vice-versa, mas o fato é que existem sim diferenças entre elas. O *bitcoin-blockchain* é o primeiro que surgiu e apesar de sofrer ataques há oito anos continua no ar graças a sua alta resistência.

***Bitcoin* moeda/não-*bitcoin-blockchain* –** Podemos falar do *bitcoin* como moeda sem mencionar o seu *blockchain*. A Blockstack, por exemplo, criou uma ferramenta de identificação que utiliza o *bitcoin* para registro, mas não o seu*blockchain*. A Blockstream também criou um ambiente paralelo ao *blockchain* do *bitcoin*, mas conectado a ele, para rodar informações mais complexas. Nesses dois casos, o *bitcoin* é utilizado como mero insumo.

Não-*bitcoin*-moeda/*bitcoin*-blockchain – Também é possível usar o *blockchain* sem utilizar o seu *bitcoin*. Esse sistema é adotado pela Factom, de Honduras, pela Counterparty, que utiliza o *blockchain* do *bitcoin*, mas usa a própria Counterparty como moeda; e a NameCoin, que usa o *blockchain* do *bitcoin* para registrar domínio, mas a moeda nativa apenas abastece a sua plataforma.

Não *bitcoin*-moeda/não-*bitcoin-blockchain* – Outra opção é não usar a moeda *bitcoin* nem o seu *blockchain*. É o caso da Ethereum, da Z-Cash, que tem como principal preocupação o sigilo absoluto das transações, além de outras centenas de criptomoedas que surgem a cada dia no mercado.

Consenso sem *blockchain* – É recente o surgimento desses consórcios de instituições. Ripple, Hyperledger *e* R3CEV são alguns deles. O R3CEV é o mais famoso, porque reuniu mais de cem instituições financeiras globais em um único consórcio, utilizando a tecnologia do *blockchain* em prol do sistema financeiro global. Apesar disso, chegou-se à conclusão de que o *blockchain* não é eficiente, não é capaz de manter tantas instituições financeiras conversando entre si, uma vez que a instituição ‘A’ não aceita ver a instituição ‘B’ tendo acesso às suas informações. Com esse entendimento, decidiram criar uma nova terminologia, chamada DL-

Distributed Leadership, para incentivar sua adoção.

***Blockchains* neutros –** Tezos, Peernova, Eris e Original My, são algumas das empresas que utilizam mais de um *blockchain* como complementação. A nossa ferramenta de assinatura de documentos e contratos utiliza dois*blockchains*, o *blockchain* do *Bitcoin* e o *blockchain* do Ethereum. No *blockchain* neutro, não importa qual plataforma está funcionando, mas sim entregar a solução.

O *blockchain* como protocolo: outros usos além da moeda

Em 2013, surgiram várias iniciativas ao redor do *blockchain* do *Bitcoin* visando fins não previstos no *blockchain*. Por não estarem previstas e dependendo totalmente de consenso para sua aplicação, essas iniciativas foram criadas de maneira satélite. Foi quando Vitalik Buterin, fundador do Ethereum, questionou esses sistemas paralelos num documento, discutindo se não seria o caso de criar um *blockchain*único para tudo.

Sob o ponto de vista corporativo, é muito difícil confiar que um *software* de código aberto (*open source*) mantido por um grupo de pessoas desconhecidas funcionará plenamente por um período mais ou menos longo. E que, em caso de pane, a comunidade que dá suporte àquele *software* continuará trabalhando nele. Seria preciso confiar no *software* principal e em todos os outros pontos ao seu redor. Não basta confiar no Blockchain do *Bitcoin*, é preciso confiar também na comunidade Blockstream, Counterparty. Em cada nova conexão, é preciso confiar nas equipes.

Vitalik Buterin desenhou um novo modelo *blockchain* baseado no *bitcoin* com inteligências aptas a rodar aplicações, *tokens* nativos que podem ser criados a partir da própria plataforma e *smarts contracts.*

O contrato inteligente, ou *smart contract*, é um protocolo de computador feito para facilitar, verificar ou reforçar a negociação ou desempenho de um contrato, podendo ser executado ou se fazer cumprir por si só.

Para ser considerado um contrato inteligente, a transação deve envolver mais do que uma simples transferência de moeda virtual entre duas pessoas – como uma transferência de pagamento, por exemplo; deve envolver duas ou mais partes – como todo contrato; e a implementação do contrato não deve requerer envolvimento humano direto a partir do momento em que for firmado.

Dentro da rede do Ethereum, um contrato inteligente é uma aplicação descentralizada, um programa de computador com diversas cláusulas, critérios e linguagens distintas, entre elas a Solidtech, que é semelhante ao Javascript utilizado na criação de *sites*.

A execução desses contratos não ocorre em uma única máquina, mas em toda a rede e ao mesmo tempo. Embora todo o contrato inteligente seja uma aplicação descentralizada, uma aplicação descentralizada não necessariamente é um contrato inteligente.

Na Original My, usamos a plataforma Ethereum para fazer repositório de dados, que são distribuídos por toda a rede e,

consequentemente, imutabilizados. O custo refere-se apenas ao registro da transação. Nenhum valor adicional é cobrado para a leitura posterior dos dados. Mas isso não é interessante quando se fala em grande volume de dados.

Usos potenciais do *blockchain*

Objetos físicos (diamantes, pinturas, árvores etc.) – No final de 2015, a Everledger fez o registro da autenticidade de 850 mil diamantes. O certificado acompanha o percurso do diamante até o seu destino.

Cadeia de fornecedores – Refere-se aos dados de pedidos, acompanhamento de estoque.

Bancos – Os bancos têm olhado para o *blockchain* privado como forma de consolidar a informação e para o *blockchain* público para facilitar as remessas internacionais.

Identificação – As tecnologias do *blockchain* e das DLT's (Distributed Ledger Technology) têm sido utilizadas para a identificação de pessoas/clientes.

Votação – Acompanhamento transparente de votações públicas e privadas. Um grande desafio para o *blockchain* é fazer com que a informação colocada na rede seja vista apenas por aquela pessoa para a qual foi destinada, uma vez que os dados são públicos, transparentes e distribuídos para todo o mundo. É praticamente impossível utilizar o *blockchain* em votações secretas, mas em votação transparente não há nenhuma dificuldade.

Acompanhamento – Fluxos comerciais e dados de transporte.

Registros públicos – Referimo-nos ao registro de qualquer coisa: imóvel, terreno, automóvel, licenças comerciais, passaportes, ID's (RG/CPF), transferências de propriedades etc.

Coleta de intangíveis – são as patentes, marcas, reservas, domínios.

Financeiro – Dinheiro, ações, empréstimos, investimento, *crowdfunding*. A *explosão* do *blockchain* deve muito ao interesse manifestado pelo sistema financeiro. Por essa razão, inúmeras ferramentas estão sendo desenvolvidas para auxílio a esse setor.

No que diz respeito às transferências de valores, é interessante notar que a transferência de 'A' para 'B' fica registrada no *blockchain* sem necessidade de intervenção por terceiro. Além dos registros públicos, também é permitido registrar transferências, isto é, conhecer todos os seus detalhes, por onde passou e pelas mãos de quem passou.

Distributed Ledger

Hyperledger – Ganhou muito mais força a partir de dezembro de 2015, quando a IBM se juntou a Linux Fundation e a Intel.

O Hyperledger não é um *blockchain*. É semelhante a um banco de dados, mas com a característica de se conectar aos nós, sincronizando e distribuindo as informações de forma automática. Ele é todo modular.

Bigchain DB – É um banco de dados com altíssima capacidade de registro (mil por segundo), que possibilita a criação de ativos a partir do *blockchain*. Um bom administrador de sistemas consegue consertar um erro num banco de dados qualquer sem deixar rastro

algum. Com o *blockchain*, no entanto, o rastro não é apagado. Qualquer que seja a ação – um registro, sua eliminação ou uma troca de informações – ela fica registrada no histórico do *blockchain* e não poderá ser alterada nem mesmo por um usuário administrador.

Quorum – Uma bela iniciativa, baseada no Ethereum, que criou um *blockchain* privado e um *blockchain* público, permitindo a troca de informações entre eles. As informações privadas ficam sob o domínio de empresas que em algum momento vão trocar informações com o Ethereum Público. Isso ganhou tanta força que a ConsenSys Ethereum resolveu criar um consórcio para impulsionar ainda mais essa iniciativa. Atualmente, mais de trinta empresas integram esse consórcio.

R3CEV – Consórcio criado inicialmente para pesquisa e experimentação. Bastava associar-se ao consórcio para experimentar *blockchains* diversos, ter contato com as instituições integrantes e acesso irrestrito a todas as suas ferramentas.

A R3CEV considerou o *blockchain* uma ferramenta desinteressante para uso pelo mercado financeiro. Resolveu, então, criar o Corda, um *ledger* distribuído, uma ferramenta *open source* mais apropriada às necessidades do sistema financeiro. Hoje, já existem mais de sessenta projetos sendo desenvolvidos pela R3CEV.

Comparativos entre as principais tecnologias

HYPERLEDGER – rede de consenso: plugável; rede: privada ou pública; *smarts contracts*: programável em múltiplas linguagens.

ETHEREUM – rede de consenso: mineração; rede: pública ou privada; *smarts contracts*: programável em múltiplas linguagens.

***BITCOIN* –** rede de consenso: mineração; rede: pública; *smarts contracts*: limitada a poucos *scripts*. São carteiras multiassinadas em que todos os signatários precisam estar de acordo para que a transferência de fundos seja efetivada.

A transferência de fundos pode acarretar o registro de alguma informação no *blockchain*, portanto, há sim um *smart contract* no *bitcoin* que funciona muito bem e não de forma limitada.

Aplicações: BitNation, Slock.it, Nasdaq, OneName, ArcadeCity

A BitNation tentou introduzir uma plataforma global de governo descentralizado. Podemos dizer que é um país na internet, provê diversos tipos de serviços cartorários, advocatícios, de identificação e outros gerais. Possui um sistema de identificação reconhecido pelo Governo da Estônia (República da Estônia) que possibilita a identificação de refugiados sírios e autoriza o livre trânsito naquele país.

A Slock.it criou uma fechadura inteligente que faz a própria gestão da sua receita e roda o *blockchain* do Ethereum. Por meio dessa fechadura, é possível fazer a reserva de quartos, por exemplo, sem necessidade de intervenção da administração do hotel. O dinheiro da reserva é direcionado à fechadura, que se reserva e envia ao cliente a chave de acesso. Percebendo dano no sensor, a fechadura licita o mercado, contrata a empresa de manutenção e paga pelo serviço. No final do mês, o seu lucro é dividido com a empresa mantenedora, criada pela própria Slock.it.

A Nasdaq começa a fazer testes com leilões privados, e a Estônia já tem algumas empresas licitadas.

A OneName é voltada à identidade global.

A Arcade City é um “Uber” descentralizado. Hoje, a Uber retém 25% do ganho do motorista. No sistema baseado em *blockchain*, o motorista fica com 100% do valor, e a rede toda se comunica, fazendo a qualificação do motorista. Futuramente, o pagamento da corrida poderá ser feito diretamente ao carro. O carro poderá se dirigir à sua estação de abastecimento, pagar pelo combustível, seja elétrico ou derivado do petróleo, e pagar por sua manutenção. No futuro, esse tipo de transporte será feito sem motoristas.

Aplicações: Augur, Ujo Music, La’Zooz, Storj, Transactive Grid

A Augur é uma plataforma de previsões descentralizadas. Por exemplo, prevê-se que haverá um aumento do dólar em determinada data. Todo o embasamento técnico é direcionado para essa perspectiva. Poderão se manifestar, adicionando criptomoedas, todos aqueles que concordarem ou tiverem mais argumentos que fortaleçam essa previsão. Se a previsão se concretizar, os que apostaram nela ganham todas as criptomoedas. É mais uma plataforma de apostas do que de previsões.

A Ujo Music apostou na mudança de lógica da indústria da música. Ela recebe e divide com o restante da cadeia. Nessa cadeia, o último ponto é o autor. Nesse caso específico, paga-se o autor e com o uso do *smart contract* realiza-se o pagamento ao restante da cadeia. Ou seja, todos recebem.

A La’Zooz é uma plataforma de compartilhamento de caronas.

A Storj tem um interessante armazenamento descentralizado que tinha como base a criptografia do *bitcoin*. Hoje, migrou para a criptografia do Ethereum. É uma plataforma semelhante ao dropbox.

A Transactive Grid, de Londres, começou a produzir energia elétrica a partir de painéis solares e passou a vendê-la aos vizinhos da comunidade local, que aceitaram a criptomoeda para o consumo no mercado.

Outras aplicações: SmartID, Trust Stamp, ShoCard’s, UPort, OneName BitNation

Na área de identidade, temos a SmartID, de iniciativa da Deloitte.

A Trust Stamp recebeu alguns milhões da Reach Incubator para o desenvolvimento de um sistema de compartilhamento de informações pessoais. Enquanto o SmartID procura fazer uma identificação única, distribuída e baseada no *blockchain*, a preocupação da Trust Stamp é fazer com que as instituições consumam a informação a partir de um só lugar. É claro que, estando dentro do *blockchain*, não importa muito onde está gravada a informação, o importante é que esse consumo possa se dar por meio da rede.

A iniciativa do ShoCard’s talvez seja a mais interessante, pois visa eliminar a utilização de senhas para acesso a *sites*. Essa iniciativa acaba com os chamados *phishings*, em que pessoas mal intencionadas enviam mensagens eletrônicas com pretextos falsos, induzindo o receptor a fornecer informações e documentos importantes.

Eles desenvolveram uma técnica em que o *site* se comunica com a aplicação do seu celular. Pode até ser que se peça um PIN para confirmação, mas, como já foi feita a identificação anteriormente, o acesso ao *site* é liberado automaticamente.

A *UPort* segue a mesma linha, mas a iniciativa é da *ConsenSys*, grupo comercial pertencente à *Ethereum*.

Por último, a OneName BitNation. Embora tenha só dois anos de atividade, já está defasada em comparação às novas iniciativas que

surgem na área de identificação.

OriginalMy.com – primeira empresa brasileira a utilizar o protocolo *Blockchain*

Sempre estive envolvido com a computação distribuída, com o processamento descentralizado. Em 2011, comecei a trabalhar com a tecnologia do *bitcoin*, mas desisti porque entendi que os altos custos não valiam os poucos centavos que o negócio rendia. Parti, então, para a pesquisa científica.

Em 2013, entretanto, o *bitcoin* deu um inacreditável salto de US$ 100 para US$ 1.200, o que me fez voltar o olhar novamente para essa ferramenta. Meu objeto de estudo não era o valor do *bitcoin* como moeda, eu quis estudar a fundo sua infraestrutura.

Em 2014, li a notícia de que a Universidade de Nicósia tinha registrado no *blockchain* a autenticidade de um certificado de conclusão de curso. Percebi, então, que era isso que eu queria fazer e que aquilo envolvia a segurança da informação, o registro, a autenticidade.

Em julho de 2015, lançamos o OriginalMy. Duas de suas principais funções são: fazer prova de autenticidade de qualquer tipo de documento digital e resguardar a propriedade intelectual. A lei brasileira diz que o direito intelectual nasce com a obra. Em caso de disputa, de questionamentos, é preciso provar a sua antecedência. A função do OriginalMy, por meio de um *timestamp*, é dizer que o documento existe a partir de determinada data, tendo a outra parte que provar a anterioridade do seu.

O OriginalMy também assina contratos. Antigamente, os contratos eram assinados por videodepoimentos. Em breve, os contratos poderão ser assinados por App, de maneira confidencial, vinculando as partes ao documento e garantindo validade jurídica, tudo integralmente registrado em *blockchain*. Aguardamos apenas autorização da Apple para o lançamento do nosso App.

A integridade de documentos também é nossa preocupação. Comprovamos a integridade dos documentos e a data de sua existência, mesmo sem armazená-los.

Também autenticamos conteúdo na web. Emitimos um laudo relatando que determinado conteúdo se encontrava na web em determinado momento, servindo até mesmo como prova em processos judiciais. Há um processo em que foi deferida liminar favorável à parte com base em provas coletadas por meio de nossas ferramentas tecnológicas.

Para atender à demanda, passamos a fazer protótipos e provas de conceito para distribuição em todo o mercado.

O *blockchain* resolve muita coisa. Não resolve tudo por conta dos custos que envolvem o registro do *blockchain*. Se o *blockchain* é privado, não há custos. No *blockchain* público existe custo apenas em relação ao registro, a leitura não gera custos e pode ser feita em

qualquer momento, de qualquer lugar e por qualquer interessado.

O *blockchain* público tem como principais características o seu alto grau de imutabilidade, a transparência, a auditabilidade, o consenso, que garantem que as informações registradas não sofreram alterações, e ainda, a eficiência e a redução de gastos, principalmente de infraestrutura.

Palestra I - proferida por Rosine Kadamani, advogada e cofundadora da Blockchain Academy

Palestra III - proferida por Antonio Carlos Alves Braga Júnior, juiz de Direito substituto em Segundo Grau no TJSP

Fonte: Fátima Rodrigo, jornalista