

JE MAIS TIC

Empresas revelam aplicações práticas da blockchain

| PIV

Um sistema construído de raiz para ser seguro

| PVI



Kim Hong-Ji/Reuters

Blockchain: tecnologia da bitcoin está a chegar a múltiplas indústrias

Segura, distribuída, sem intermediários. A tecnologia blockchain nasceu associada a uma criptomoeda, mas, em menos de uma década, amadureceu e começa a ser aplicada à logística, à rastreabilidade de produtos alimentares, e, pelo menos em tese, aos registos prediais ou à informação académica.

INOVAÇÃO

Blockchain: tecnologia da bitcoin está a chegar a múltiplas indústrias

Nasceu associada a uma criptomoeda, mas começa a ser aplicada em diferentes setores. Até 2022, acredita-se que o mercado aumente mais de 30 vezes, para mais de 6 mil milhões de euros.

MAFALDA SIMÕES MONTEIRO
mmonteiro@jornaleconomico.pt

O mercado de blockchain deverá crescer de 241,9 milhões de dólares em 2016 para 7,68 mil milhões de dólares em 2022, apresentando uma taxa de crescimento anual composta (CAGR) de 79,6%, segundo os dados da Markets & Markets, citado pela SAP.

A tecnologia tem pouco mais de 10 anos, e tem vindo a tornar-se mais conhecida nos últimos meses, devido à valorização (e desvalorização) fora do comum que a bitcoin – a criptomoeda que nasceu praticamente em simultâneo com a tecnologia – tem vindo a registar nos mercados financeiros.

Por estar a dar os primeiros passos, a tecnologia apresenta uma tendência de crescimento acentuado. Segundo Bruno Padinha, partner da EY, o investimento na tecnologia propriamente dita deverá ser atualmente de “1,4 mil milhões de dólares” antecipando-se que, em menos de uma década “10% do PIB mundial esteja assente em tecnologia blockchain, avança o mesmo responsável.

Sobre a bitcoin propriamente dita, valor desta moeda em circulação atingiu, em dezembro, 325 mil milhões de dólares, que compara com 12,5 mil milhões de dólares um ano antes, refere a mesma fonte. E esta é apenas uma das moedas que tira partida daquela tecnologia.

De facto, para além da bitcoin, as tecnologias blockchain são utilizadas por várias outras moedas: ethereum, ripple, litecoin, dash, entre outras, onde se inclui a portuguesa appCoin. A Oferta Inicial de Moeda (ICO) da appCoin, um protocolo blockchain para lojas de aplicações, decorreu durante a Web Summit, no passado mês de novembro, em Lisboa. A criptomoeda portuguesa começou a ser transacionada já durante o corrente mês e no primeiro dia de nego-

ciação valorizou para mais de 600 milhões de euros.

Mas a tecnologia blockchain pode ser aplicada a muitos outros setores de atividade. Depois de alguns anos de testes e provas de conceito começam já a conseguir observar-se alguns casos práticos com resultados demonstráveis. A tecnologia pode servir para gerir serviços tão diversificados como registos prediais, recursos pesqueiros, transportes de mercadorias, serviços financeiros, rastreabilidade de produtos alimentares, saúde, viagens e transportes ou media e entretenimento.

O que é a blockchain?

Antes de mais, importa perceber o que é a blockchain. É uma “tecnologia que permite o armazenamento de informação numa rede de transações, segura e inviolável, sem necessidade de uma entidade

POSSÍVEIS APLICAÇÕES DO BLOCKCHAIN

- Atos administrativos (Registos Prediais, licenças, documentos de identificação);
- Contratos, certificações;
- Cuidados de saúde;
- Diplomas e certificados académicos;
- Eleições (voto eletrónico);
- Empréstimos, incluindo hipotecas;
- Gestão de identidade integrados em dispositivos móveis;
- Gestão de ativos;
- Gestão de programas de fidelidade;
- Monitorização de cadeias de abastecimento;
- Pagamentos internacionais;
- Prevenção de fraude;
- Internet das Coisas;
- Rastreabilidade de bens;
- Registo de emissão de SLA (acordos de níveis de serviço);
- Registo de patentes;
- Segurança da cadeia de abastecimento de medicamentos e alimentos;
- Seguros;
- Liquidação de transações.

central para gestão e manutenção da mesma”, isto é, sem intermediários. Deste modo, ao contrário de outras tecnologias, que centralizam os registos das transações numa base de dados centralizada, a blockchain guarda a informação de uma forma distribuída. E como? “O fator diferencial, e único desta tecnologia”, é a forma como guarda a informação que é partilhada “por toda a rede de computadores”, garantindo a “segurança e a integridade dos dados”, explica Bruno Padinha. Além disso, “para que cada registo seja efetivamente considerado, é necessário que seja validado pela rede, tornando o processo fiável e rastreável”.

Compõem esta tecnologia uma “rede de interligação dos diferentes servidores; um banco de dados distribuído; os blocos ou transações, ou no caso das cibermonedas as carteiras (wallet) e o “hash” que serve de assinatura, ou chave de cada bloco, detalha Rui Duro, diretor de vendas da empresa de soluções de segurança empresarial Check Point Portugal.

Os participantes podem ser de qualquer tipo e geografia, por exemplo, clientes, fornecedores, auditores, bancos, parceiros, instituições”, exemplifica Nuno Miguel Laginha, consultor na CGI.

Por outras palavras, “o princípio é bastante revolucionário, uma vez que pretende descentralizar os registos das transações. Em vez de termos um registo num único local, ou contentor, ele encontra-se presente e distribuído por vários bancos de dados”, acrescenta Rui Duro.

Possíveis aplicações da blockchain

As primeiras aplicações desta tecnologia foram na área das transações financeiras, até porque a tecnologia nasce associada a uma moeda digital. Mas a blockchain poder ser aplicada em qualquer tipo de transação, financeira ou não, que necessite “níveis de con-



BRUNO PADINHA
EY

“A tecnologia terá ainda de fazer algum caminho no sentido de materializar e demonstrar a aplicabilidade dos inúmeros casos de uso sobre os quais se consegue teorizar hoje”.



NUNO MIGUEL LAGINHA
CGI

“Os participantes podem ser de qualquer tipo e geografia, por exemplo, clientes, fornecedores, auditores, bancos, parceiros, instituições”.



PEDRO MANUEL
BITCLIQ

“Estamos a implementar o armazenamento da informação referente à rastreabilidade digital do pescado, desde o ponto de captura até à venda final, passando pelos vários intervenientes da cadeia de valor”.



fiança significativos entre as partes”, explica Bruno Padinha. E estes processos podem ser encontrados em quase todos os setores “desde o retalho até ao legal, passando pela relação entre o Estado e os contribuintes, até à saúde ou educação”, refere.

E exemplifica com um caso muito concreto. “Muitos daqueles que compõem a recente vaga de refugiados oriundos do Médio Oriente possuem cursos superiores. No entanto, não dispõem da documentação necessária para comprovar os seus estudos. A verificação das habilitações académicas destas pessoas teria sido consideravelmente mais fácil em qualquer parte do mundo se o seu diploma estivesse guardado numa blockchain – tal como o próprio MIT já fez, num projeto-piloto, com 100 dos seus alunos”.

Outro caso de aplicação é à indústria vinícola. A EY Itália esteve recentemente envolvida num projeto que permite “ver todos os passos da cadeia de valor da garrafa de vinho que chega às mesas dos consumidores” (ver pp. IV-V).

Gabriel Coimbra, diretor-geral da IDC Portugal apresenta múltiplas possibilidades, mas deixa o



Thilo Schmuegen/Reuters

COMO NASCEU

Satoshi Nakamoto é o pseudónimo de uma pessoa ou de uma equipa, até agora não identificada, que lançou um artigo científico sobre a primeira moeda digital, a bitcoin, em 2007. Dois anos depois, foi lançada e realizada a primeira transação com aquela moeda virtual. Bruno Padinha (EY) refere que o interesse e a utilização da moeda foi crescendo e, rapidamente, se concluiu que a tecnologia subjacente poderia ser utilizada separadamente em diversas aplicações. Em 2013, vários bancos começaram a investir e a estudar a tecnologia, com o objetivo de perceber como aplicar a tecnologia ao setor bancário, mas rapidamente se concluiu que, “pelas características da tecnologia, o interesse e investimento em blockchain é transversal a todo o mercado e é visto como o futuro tecnológico para muitas aplicações transacionais” das áreas financeiras ou não financeiras.

alerta “são apenas alguns dos exemplos atuais em que se pode sentir a mudança fruto da adoção e utilização do blockchain, será expectável que novas e inovadoras aplicações da tecnologia”. Pode ser aplicado nos cuidados de saúde, “em temas de enorme sensibilidade, como a segurança dos dados dos pacientes, a contrafação dos medicamentos, a partilha de dados de pacientes e a gestão de protocolos e dados de testes clínicos”. Também os governos podem tirar partido da tecnologia utilizando-a para “processos de identidade eletrónica, votação eletrónica, registo eletrónico de terrenos e propriedades, transações e finanças eletrónicas, administração de fundos, conformidade com políticas e certificados de educação”.

Na indústria, prossegue Gabriel Coimbra, as aplicações podem passar pela “autenticação de componentes à monitorização de cadeias de abastecimento, registo de patentes”. Na energia, “a sua utilização poderá ser feita na transação e liquidação de transações, certificação e tokenização da geração de energia renovável, carregamento de veículos elétricos e autónomos e automação da energia domésti-

ca”. Finalmente, nos mercados financeiros, “pode ser utilizado para pagamentos internacionais, agilizar o despacho e liquidação de operações, plataformas de negociação e cartas de crédito automático”.

A blockchain é então “uma forma promissora de simplificar os processos multipartidários e complexos e, ainda, de criar confiança entre os participantes”, explica Pedro Ruivo, consultor de soluções para a Transformação Digital, na SAP Portugal, uma empresa que já tem casos de estudo em 25 indústrias distintas. Na SAP, “a blockchain funciona como um serviço na cloud - blockchain-as-a-service (BaaS) - estando nativamente integrada com os sistemas transacionais de backend, tais com o ERP”, acrescenta Pedro Ruivo.

“Identificámos diversas aplicações, nomeadamente: empréstimos sindicados, liquidação e liquidação de valores mobiliários, relatórios, carta de crédito, gestão de ativos, auditoria, dunning, comunicação de contrato, inventário e rastreabilidade de bens, emissão e validação de certificados, lealdade e recompensas ao cliente, classificação e votação, registo de emissão

de SLA (acordos de níveis de serviço), procedimentos de autorização e garantia no sector público, distributed manufacturing (3D-printing), licitação segura no processo de aquisição, seguro de garantia, segurança da cadeia de fornecimento de medicamentos e alimentos, proveniência, operações de proteção civil”, entre outros exemplos, avança Pedro Ruivo (SAP Portugal).

A IBM está a trabalhar em soluções de blockchain em código aberto para empresas desde 2015, disponibilizando aos clientes uma plataforma “integrada baseada na cloud de nível empresarial, desenhada para acelerar o desenvolvimento, gestão e operação de uma rede de negócios multi-instituição”, exemplifica Paulo Rodrigues, responsável de tecnologias global para o sector financeiro na IBM Global Markets, IBM Portugal. Para este responsável, a blockchain “está em franco crescimento, com algumas indústrias específicas a liderar a adoção, sobretudo nas áreas financeira e logística, onde as otimizações de processos resultantes do uso desta tecnologia se traduzem em importantes reduções de custos”.

Num outro registo, Nuno Miguel Laginha (CGI) recorda que “é importante recordar que esta hype em torno da tecnologia já gerou o aparecimento de muitas startups, algumas destas totalmente dedicadas a blockchain”, assinala. Muitas preocupam-se com problemas que a tecnologia pode resolver, especialmente quando “existam transações que, ao dia de hoje, são reguladas e processadas de forma centralizada” e que, no futuro poderão “implementar tecnologia blockchain”, conseguindo-se assim “ganhos para o prestador de serviços e para o utilizador final”.

É o caso, por exemplo, da Bitcliq, uma startup tecnológica portuguesa que está a utilizar blockchain para implementar o armazenamento da informação referente à rastreabilidade digital do pescado, desde o ponto de captura até à venda final, passando pelos vários intervenientes da cadeia de valor, explica Pedro Manuel, fundador e CEO da Bitcliq. (ver pp. IV-V).

No futuro da tecnologia, que poderá não estar muito distante, “novas funcionalidades como os smart contracts irão permitir que contratos parametrizáveis sejam executados entre dois indivíduos, de acordo com condições específicas, sem que sejam necessários intermediários”, detalha Bruno Padinha (EY).

Desafios da tecnologia e da regulação

A questão da (falta) regulação é apontado como um dos maiores desafios que a tecnologia irá enfrentar. Para a EY, este é um dos

dois grandes desafios da blockchain. Por um lado, “a tecnologia terá ainda de fazer algum caminho no sentido de materializar e demonstrar a aplicabilidade dos inúmeros dos casos de uso sobre os quais se consegue teorizar hoje”. O segundo aspeto apontado por Bruno Padinha (EY) é precisamente o desafio regulatório, pois a blockchain poderá ter nos governos e nos reguladores as maiores barreiras à sua adoção”. Segundo Padinha “a resposta regulatória por parte destes stakeholders corre o risco de estrangular o ecossistema que se está a criar em torno desta nova tecnologia”.

Esta é uma opinião partilhada por Nuno Miguel Laginha (CGI) que assinala que “a evolução da tecnologia em si, deverá ter, como principal foco no futuro imediato, questões sobretudo relacionadas com desempenho e legislação”. O consultor recorda que, “por estarmos a falar de transações entre pares que não desempenham funções de intermediação faz com que seja necessária legislação e protocolos que ao dia de hoje não existem em muitos países. Quem é responsável, por exemplo, na falha de uma transação ou num contrato automático (smart contracts) que não funcionou de acordo com o previsto?”.

Paulo Rodrigues (IBM) assinala ainda que é necessária “melhor informação sobre os diversos tipos de blockchain, com um claro entendimento das diferenças entre as plataformas construídas para consumidores (ex: moedas virtuais) e as plataformas empresariais (como Linux Foundation Hyperledger).

A grande oportunidade da blockchain poderá estar relacionada com as empresas que “queiram de facto participar numa economia em rede, onde a imutabilidade e o consenso são fatores decisivos do negócio, explica Pedro Ruivo, da SAP Portugal. Ressalvando que “nem todos os atuais/clássicos negócios deverão ser baseados em blockchain”, o maior desafio da tecnologia prende-se com a necessidade de as empresas mudarem parcial ou totalmente o seu modelo operacional para uma economia em rede, onde todos os agentes têm o mesmo poder”.

Entretanto, é aguardar e continuar a acompanhar o mercado, porque “devido à relativa juventude desta tecnologia, não é possível antever para um futuro próximo a estandardização ao nível de componentes (ex: protocolos e linguagens), porquanto muitos desenvolvimentos estão em curso em diversas empresas e comunidades, com vista a otimizar e refinar a base tecnológica, bem como a criar todo um ecossistema de plataformas, produtos e serviços ao redor da mesma”, explica Paulo Rodrigues (IBM). ●

TECNOLOGIA

Empresas revelam aplicações práticas da blockchain

Nos vinhos, na pesca, no transporte marítimo, na banca e até no mercado dos diamantes. Tecnologia chega a múltiplas indústrias.

MAFALDA SIMÕES MONTEIRO
mmonteiro@jornaleconomico.pt

A Europa é uma das geografias onde a adoção da tecnologia blockchain está mais desenvolvida. Além das grandes empresas, muitas startups e incubadoras de blockchain estão a surgir, avança Gabriel Coimbra, diretor-geral da IDC Portugal. Um dos motivos para este panorama é “a vontade de proporcionar medidas de maior segurança na gestão de dados, algo particularmente relevante devido à implementação do Regulamento Geral de Proteção de Dados (RGPD)” em maio de 2018.

Estão inúmeras provas de conceito em curso, mas também implementações a operar como é o caso do banco holandês ABN AMRO que, através de uma parceria com a IBM, disponibilizou tecnologia blockchain para transações imobiliárias. “Neste sistema, o comprador, vendedor, banco e conservatória do registo predial estão ligados através de um livro de registo distribuído, em que as transações efetuadas geram validações praticamente imediatas de cada uma das entidades”, exemplifica Gabriel Coimbra. A IDC recomenda a participação em diferentes indústrias como forma de ganhar conhecimento e experiência relativamente à tecnologia blockchain. Desta forma, é possível criar o corpo de conhecimento necessário para tirar partido das suas vantagens”.

Nelson Pereira, CTO da Noesis, refere que a blockchain pode ser aplicada na área da cadeia de valor de abastecimento, ao permitir a ligação e acompanhamento dos processos de forma ágil, em sistemas de reservas e mesmo à Internet das Coisas. “A razão é simples: qualquer indústria pode beneficiar, ou ser transformada, por processos seguros de ligação entre pares, o princípio base da tecnologia blockchain. A medida que os contratos definidos em cada bloco evoluem em complexidade, também o potencial de utilização ir-se-á alargando”, explica Nelson Pereira que,

embora ainda não tenha exemplos da sua empresa para apresentar, refere que “a blockchain é mais um exemplo de uma tecnologia que equacionamos vir a utilizar em soluções sofisticadas como as que desenvolvemos com base na Internet das coisas”.

Por seu lado, a SAP dá como exemplo uma empresa sul-africana de diamantes que integrou a tecnologia SAP blockchain nos seus processos de gestão, através do consórcio Everledger. O objetivo é “recolher informação dos seus ativos, definindo as suas características, história e propriedade, com o intuito de criar um registo permanente numa cadeia

de blocos. Esta impressão digital é então usada pelas várias partes interessadas em todo o encanamento da cadeia de fornecimento, não só para garantia da proveniência da forma, como para verificação da sua autenticidade. Esta captura criptográfica de mais de um milhão de diamantes leva a uma transparência total na comercialização de diamantes”, explica Pedro Ruivo, consultor de soluções para a transformação digital na SAP Portugal.

Rastrear o vinho desde o produtor

Uma equipa da EY Itália desenvolveu a Wine blockchain, uma solução que pretende “revolucionar o processo de supply chain na indústria alimentar como o conhecemos”, diz Bruno Padinha, partner da EY.

A solução visa combater a contrafação de produtos vinícolas de qualidade superior, como é o caso das regiões demarcadas da Toscana em Itália ou do Douro em Portugal. “A imutabilidade da informação, característica fundamental da tecnologia blockchain, surge como o meio para fazer face a este desafio”, refere o responsável.

A faturação do mercado vinícola italiano poderá ter tido uma perda anual na ordem dos dois mil milhões de euros, devido à contrafação, o que tem “um impacto significativo nos produtores locais”. A nível mundial, estima-se que 20% do vinho em circulação seja atualmente contrafeito, segundo dados citados pela EY.

A tecnologia blockchain materializa-se num QR Code que encaminha o consumidor para uma página web. Esta página exhibe todo o percurso da produção do vinho, desde o cultivo, ao tratamento, aos fitoquímicos utilizados, à informação geográfica, à colheita, entre outros. “A informação é clara, transparente e imutável, sendo armazenada numa das blockchains públicas mais conceituadas, a Ethereum”, assinala Bruno Padinha.

A implementação do projeto Wine blockchain exigiu a participação



NELSON PEREIRA
NOESIS

“Qualquer indústria pode beneficiar, ou ser transformada, por processos seguros de ligação entre pares, o princípio base da tecnologia blockchain”.



GABRIEL COIMBRA
IDC

“A IDC recomenda a participação em diferentes indústrias como forma de ganhar conhecimento e experiência relativamente à tecnologia blockchain. Desta forma, é possível criar o corpo de conhecimento necessário para tirar partido das suas vantagens”.





Aly Song/Reuters

Francois Lenoir/Reuters

da EY, da empresa de produção de vinhos, e de todos os intermediários da cadeia de valor, para que toda a informação necessária pudesse ser recolhida.

A solução poderá ser aplicada e adaptada a outros produtos alimentares, mas também a bens alvo de elevada contrafação como o retalho ou a relojoaria.

Contribuir para melhorar a logística internacional

A empresa dinamarquesa Maersk e a IBM anunciaram esta semana a intenção de criar uma joint venture, que irá disponibilizar soluções e métodos “mais eficientes e seguros” com o objetivo “melhorar o comércio mundial com recurso à tecnologia blockchain”.

Após os projetos piloto desenvolvidos em parceria, a nova empresa surge como uma solução natural e irá “desenvolver uma plataforma de digitalização do comércio mundial, construída em conjunto a partir de padrões abertos e desenhada para todo o ecossistema do transporte marítimo, proporcionando mais transparência e simplicidade aos processos de expedição e acompanhamento de mercadorias entre diferentes fronteiras e zonas comerciais”.

A tecnologia blockchain será combinada com outras tecnologias de código aberto, com base em cloud computing, designadamente soluções de Inteligência Artificial (IA), Internet de Coisas (IoT) e analítica avançada.

As empresas referem que atualmente são transportados quatro mil milhões de dólares em produtos, sendo que mais de 80% dos bens consumidos diariamente são transportados via marítima. Além disso, estima-se que só o “processamento e a gestão da documentação comercial necessária para gerir muitas dessas mercadorias representem um quinto dos custos reais do transporte físico”. Ao incorporar a tecnologia blockchain nos processos, as transações serão simplificadas, sendo possível “introduzir uma nova forma de controlo e permissão no fluxo de informações, permitindo que os múltiplos parceiros comerciais colaborem e estabeleçam uma visão única e partilhada sobre uma transação, sem comprometer detalhes, privacidade ou confidencialidade”.

As duas empresas já trabalham em conjunto no desenvolvimento da tecnologia blockchain baseada em cloud computing, deste junho de 2016. A plataforma já foi testada por empresas como a Tetra Pak, a DuPont, a Dow Chemical, o Porto de Houston, a Administração Aduaneira dos Países Baixos ou o Serviço de Alfândega e Proteção de Fronteiras dos EUA. Com a joint venture mais empresas poderão tirar partido da plataforma como é o caso da General Motors ou da Procter & Gamble, que procuram agilizar as complexas cadeias de valor que operam.

Michael J. White, ex-presidente da Maersk Line na América do Norte será o CEO da nova companhia.

Acompanhar o pescado desde alto-mar

A plataforma Big Eye – Smart Fishing utiliza a blockchain, entre outras tecnologias de informação. Desenvolvida pela startup Bitcliq, a solução, que começou a ser desenvolvida em 2014, faz a gestão operacional de pesca em tempo real. A plataforma começou por ligar as operações no mar à gestão operacional em terra, explica Pedro Manuel, fundador e CEO da Bitcliq. Deste modo é possível “uma supervisão eficaz que se traduz naturalmente em ganhos de eficiência”. Já foram investidos no projeto algumas centenas de milhares de euros, continuando a empresa a investir na inovação e ampliação da tecnologia, “endereçoando hoje, não só as necessidades das frotas de pesca comercial de maior escala, mas também a rastreabilidade digital e a comercialização antecipada do pescado, na pesca de menor escala e/ou artesanal”, refere.

Num primeiro momento o Big Eye - Smart Fishing deu resposta à necessidade de “gestão eficiente de grandes operações de pesca comercial e industrial” e à “crescente necessidade de transparência e valorização do pescado, através da rastreabilidade”. A solução técnica escolhida foi a blockchain porque “permite resolver uma série de questões importantes em termos de verificação não adulteração dos dados registados ao longo da viagem do peixe, desde a captura no mar até chegar ao cliente final”.

Pedro Manuel acrescenta que “era necessário uma solução que mitigasse a desconfiança entre as partes e a dependência do acesso à informação guardada apenas numa entidade central, então em 2016 decidimos começar a usar esta tecnologia revolucionária para codificar a confiança da informação”.

A solução técnica, desenhada pelos engenheiros da empresa permite “colocar os dados mais relevantes recolhidos a bordo (registo de capturas) no blockchain minimizando o custo das comunicações. Conseguimos também ter um código criptográfico que pode ser partilhado entre diferentes entidades e que lhes dá acesso à informação mais importante, garantindo que esses dados não foram adulterados ao longo do tempo. Neste momento estamos a estudar outras soluções blockchain mais promissoras e escaláveis e a pensar na criação de uma moeda digital para assegurar todas as transações financeiras na nossa plataforma”.

Para este projeto, a Bitcliq utilizou a infraestrutura cloud da Microsoft, a tecnologia Ethereum, uma das primeiras opções blockchain com o conceito de “Smart Contract”, e a Inmarsat nas comunicações de dados mar-terra e terra-mar via satélite, sintetiza Pedro Manuel. ●

OPINIÃO

Blockchain: mais do que uma moeda, uma segurança contratual



RUI RIBEIRO

Diretor Executivo da LISS - Lusofona Information Systems School

Quando ouvimos falar sobre blockchain, imediatamente pensamos na moeda bitcoin. Se esta associação não está errada, certamente peca por muito escassa, dado que na realidade blockchain é muito mais que uma (cripto)moeda. A começar porque, no início de 2018, eram conhecidas mais 1300 criptomoedas e em segundo porque o blockchain é de facto uma nova arquitetura tecnológica disruptiva, que garante de forma simples e pública elevados níveis de segurança sobre a realização de transações. Esta tecnologia garante a unicidade efetiva de relações contratuais entre entidades ou máquinas ou programas.

De forma simples, podemos pensar que o dinheiro existe há muitos séculos para garantir a realização de transações, as quais foram sendo cada vez mais complexos. Essas transações são registadas em “livros-razão” internos das entidades, pelo que é uma informação privada e não conhecida publicamente, pelo que há a necessidade de existirem intermediários, como sejam os bancos ou os governos, nos quais confiamos, para nos garantir a efetividade da transação.

Com o blockchain, este conceito passou a ser alterado, dado que elimina os intermediários na cadeia de valor atrás descrita, através da criação de um registo transaccional aberto e sem controlo efetivo por uma única entidade, dado que o “livro-razão” digital passa a estar disponível na rede de Internet. E, é a

este “livro-razão” digital que se denomina blockchain, no qual todas as transações são registadas, incluindo detalhes da informação da transação: data, hora, entidades envolvidas na transação, quantias envolvidas, entre outras. Adicionalmente, cada nó da rede tem a informação desse “livro-razão” digital, garantindo assim a distribuição da informação e a garantia que o registo é fidedigno, pois caso haja alguma tentativa de alterar uma transação realizada, ela é automaticamente detetada pela rede como uma transação corrupta, e consequentemente inválida.

Por algoritmos matemáticos, os vários sistemas da rede mantêm assim uma cadeia ordenada de transações e de validação dessas mesmas transações, e de forma descentralizada. A esta cadeia de nós existentes na rede, com informação dos “livros-razão” digital, não lhe importa se regista uma transação financeira em euros ou dólares, ou uma transação contratual de imobiliário, ou uma transação informativa de um despachante na entrada num porto marítimo, ou uma participação social numa empresa. Assim, são as entidades que definem a unidade transaccional para registo no blockchain, garantindo-se o compliance de uma transação enquadrada num contrato existente. Pode-se depreender então que esta arquitetura de blockchain permite eliminar muito dos processos burocráticos existentes de validações administrativas, acelerando ainda mais o fecho dos workflows e ciclos transaccionais, isto é, tornando os processos muito mais eficientes.

Estamos só no princípio desta arquitetura, mais inovações disruptivas e evolutivas do blockchain virão em breve. O mundo da automatização está aí. O blockchain é mais uma peça nesse puzzle. ●

SEGURANÇA

Um sistema seguro por natureza

O conceito de blockchain foi desenvolvido de raiz para constituir uma base segura e confiável para transações, e impedir a interferência de terceiros na sua utilização por empresas e particulares. A segurança é por isso indissociável da blockchain.

MAFALDA SIMÕES MONTEIRO
mmonteiro@jornaleconomico.pt

Um dos pilares da blockchain é a segurança. Como resume Gabriel Coimbra, diretor-geral da IDC Portugal: “a tecnologia de livros de registo distribuídos (distributed ledger technologies) é segura por um conjunto de razões, que vão do facto de a rede ser distribuída, não existindo um nó privilegiado que faça a gestão da verificação, pelo que a sua validação é feita de uma forma virtualmente impossível de interferir. Para poder alterar um registo, seria necessário interferir em todos os registos históricos na maioria dos nós em simultâneo”.

Mais detalhadamente, Nuno Miguel Laginha, consultor da CGI, faz um preâmbulo. A tecnologia “não pode ser controlada por uma única entidade”, “uma vez que é descentralizada, não tem um single point of failure. Ou seja, não existe um ponto vulnerável que possa colocar em risco a rede”, os “dados são transparentes, estão embebidos numa rede, são por definição públicos” e, finalmente, “uma blockchain não pode ser corrompida”, salvo se for “reescrita” toda a rede, o que, por se tratar de dados cifrados, levaria uma eternidade e requeria muito poder computacional”, resume Laginha. Sendo assim, e uma vez que os dados são guardados por todos os elementos que compõem a rede, “a blockchain elimina o risco de concentrar toda essa informação numa base de dados centralizada”. Adicionalmente, explica, “todas as transações são criptografadas e todas usam um sistema de chave pública e chave privada. A chave privada é o que permite a utilizador aceder à sua propriedade digital. A segurança, ainda assim, depende do que um utilizador faz com a sua chave privada, alerta Nuno Laginha.

Bruno Padinha, partner da EY, recorda que a tecnologia “assenta no princípio de redes descentralizadas, o que implica que o reconhecimento das transações seja feito por consenso entre todos os participantes na rede”. A tecnologia dispensa reguladores ou intermediários. “Não existe nenhuma entidade ‘supra-rede’ que faça a gestão da blockchain, que concentre as capacidades de administração, verificação e decisão”, sublinha Padinha.



Arnd Wiegmann/Reuters

Deste modo, “a suscetibilidade de corrupção das transações e registos é menor”.

Também Paulo Rodrigues, responsável de tecnologias global para o sector financeiro na IBM Global Markets, IBM Portugal, sublinha a indissociabilidade da segurança da blockchain. “Tanto ao nível de comunicações, como ao nível de proteção da informação registada numa plataforma blockchain, o uso de criptografia não foi pensado como algo opcional como em outras tecnologias de comunicação e armazenamento, mas como um pilar tecnológico fundamental sobre o qual assenta a arquitetura deste tipo de plataformas”.

Por outras palavras, a blockchain é, aparentemente, mais seguro que outras tecnologias, “porque numa eventual tentativa de furto de um

bloco (conjunto de registos), teria de haver também o colossal, e quase impossível, trabalho de alterar e descriptar todos os blocos anteriores a esse, não só em milhares de computadores, como também no mesmo segundo e/ou centésimo de segundo”, ilustra Pedro Ruivo, consultor de soluções para a Transformação Digital, na SAP Portugal.

Adulterar é impossível em termos computacionais

“O conceito do blockchain foi desenvolvido de raiz para constituir uma base segura e confiável para transações”, acrescenta Nelson Pereira, CTO da Noesis. Além do mais, assenta “em sistemas avançados de criptografia, os quais geram uma identificação única calculada de forma criptográfica, recorrendo ao horário da rede (network timestamp) e, desta forma, criando um registo que inviabiliza a alteração das transações, pois estas teriam que ser totalmente recalculadas de forma retroativa em todas as réplicas, algo impossível de fazer em termos computacionais”.

Em suma, “face às soluções atuais, que dependem de um fornecedor e de uma entidade que faz a validação, o blockchain é uma solução de elevada segurança, residindo as suas limitações principais na área de governação, e não no seu desempenho tecnológico puro”, reflete Nelson Pereira.

Comparando então dois tipos de tecnologia, Bruno Padinha (EY) explica que atualmente para um hacker adulterar os registos bancários de uma conta, de modo a aumentar o seu saldo contabilístico, é suficiente atacar a rede centralizada do banco. Se saldo contabilístico “estivesse inscrito na blockchain, este hacker teria de controlar mais de 50% dos participantes da rede durante tempo suficiente para introduzir transações falsas que fossem aceites como boas”.

Seguro pelo menos para já

“Até agora, o protocolo em si tem resistido e mantém-se seguro, se será sempre assim, será difícil prever”, diz Rui Duro, diretor de vendas da Check Point Portugal.

Mas apesar do ceticismo de quem trabalha na área da segurança, contrabalança: “existe um interesse da comunidade hacker, em não atacar este modelo uma vez que, até agora, esta tem sido a sua forma privilegiada para receber pagamentos, não sendo do seu interesse atacá-la”, assinala Rui Duro.

Entretanto, e “à medida que esta tecnologia começa a crescer e a ser utilizada em outras áreas como nas transações bancárias ou no registo de propriedade, ganhando por isso visibilidade e forte interesse comercial, leva outros atores e promotores (como por exemplo os bancos) a tornarem o protocolo ainda mais seguro”, conclui Rui Duro. ●



RUI DURO
CHECK POINT

“Existe um interesse da comunidade hacker, em não atacar este modelo, uma vez que, até agora, esta tem sido a sua forma privilegiada para receber pagamentos, não sendo do seu interesse atacá-la”.



PAULO RODRIGUES
IBM

“Tanto ao nível de comunicações, como ao nível de proteção da informação registada numa plataforma blockchain, o uso de criptografia não foi pensado como algo opcional, como no caso de outras tecnologias de comunicação e armazenamento”.



PEDRO RUIVO
SAP

“Numa eventual tentativa de furto de um bloco, teria de haver também o colossal, e quase impossível, trabalho de alterar e decifrar todos os blocos anteriores a esse, não só em milhares de computadores, como também no mesmo segundo e/ou centésimo de segundo”.

As limitações em matéria de segurança podem residir na área da governação e não no desempenho tecnológico propriamente dito



Inis Kalmins/Reuters

Custos escondidos: o consumo de energia

Uma única transação de bitcoin poderá usar tanta energia quanto uma casa americana durante uma semana. Governos ponderam a regulação.

MAFALDA SIMÕES MONTEIRO
mmonteiro@jornaleconomico.pt

“Um dos mecanismos essenciais de uma qualquer plataforma distribuída consiste na validação da informação que é admitida na plataforma, a qual resulta da execução de determinadas operações com variável complexidade e custo de execução, dependendo da dimensão da rede e do tipo de acesso ad-

mitido”, explica Paulo Rodrigues, responsável de tecnologias global para o sector financeiro na IBM Global Markets, IBM Portugal.

Isto é, as transações são validadas através de um processo chamado mineração (do inglês mining). Bruno Padinha, partner da EY, explica que, aquando de “uma nova transação, os participantes na rede de blockchain irão trabalhar na resolução da função matemática inerente à codificação “criptográfica”

dessa transação. O primeiro participante da rede a fazê-lo gera a aprovação da transação e a consequente inclusão desse registo num bloco da blockchain”.

A título de exemplo, no caso da bitcoin, “o código informático base prevê que a complexidade da equação matemática se adapte automaticamente de acordo com a capacidade de processamento da rede. Assim sendo, quanto maior for o número de participantes na rede

O SEU DISPOSITIVO PODE ESTAR A MINERAR PARA OUTROS

O incremento do valor da bitcoin, que atingiu recentemente máximos históricos de 8.000 dólares, está a atrair as atenções para o blockchain e para possíveis vulnerabilidades do sistema. Rui Duro, diretor de vendas da Check Point em Portugal, assinala que o maior problema poderá estar na obtenção de credenciais de utilizadores que detêm ou trocam criptomoedas”.

“Existem milhares de dispositivos infetados, a minerar moedas de diferentes tipos (bitcoin, monero, litecoin ou ethereum)”. A grande quantidade de recursos necessários para gerar criptomoedas levou ao aparecimento de crypto miners (mineiros de criptomoedas), novas ferramentas de (quase) malware, usadas para gerar receita através dos CPU de utilizadores, quase sempre sem o seu conhecimento ou consentimento”.

Segundo uma investigação recente da Check Point, este “novo tipo de (quase) malware chega aos dispositivos pelos mesmos meios usados para fazer chegar outro tipo de malware. Através do envio de ficheiros infetados por correio eletrónico, campanhas de spam, downloads de exploit kits em sites infetados, em sites e aplicações de download e partilha gratuita de software, filmes e música, entre outros”, assinala. Funcionam como os ataques “Zero Day”, o que na prática significa que “os sistemas tradicionais não têm a capacidade de os detetar”.



BRUNO PADINHA
EY

“A estimativa atual de consumo elétrico para mineração de bitcoin situa-se entre os 35 e os 40 TWh”.



NUNO MIGUEL LAGINHA
GCI

Se o resultado (da mineração) é inferior ao custo da energia necessária para minerar bitcoin (ou outra criptomoeda), isso significa que o indivíduo não só está a perder dinheiro como também a consumir recursos desadequadamente, e isto é muito comum acontecer”.

(i.e., quanto maior a capacidade de computação) maior será a complexidade do processo de mineração”. Naturalmente, esta capacidade de computação tem custos: é necessário um maior investimento em ativos tecnológicos (como placas gráficas, processadores, refrigeração, entre outros) para minerar novas moedas e ter um papel ativo na rede, bem como um maior investimento em energia elétrica”, assinala Bruno Padinha.

Deste modo, “a estimativa atual de consumo elétrico para mineração de bitcoin situa-se entre os 35 e os 40 TWh”. Padinha assinala, para se ter ideia da ordem de grandeza, que “o consumo de energia elétrica em Portugal em 2015 foi de 46 TWh”, de acordo com a Pordata.

Rui Duro, diretor de vendas da Check Point Portugal, estima que “uma única transação bitcoin use tanta energia quanto a média semanal de uma casa americana”.

Nuno Miguel Laginha, consultor na CGI, explica que, pelo menos em relação à bitcoin, o “esforço para minerar”, ou seja, “a capacidade de processamento de dados, em grande escala, exige muita energia que em alguns casos (senão na maioria) é fósfil. Deste modo, o custo/benefício da ‘mineração’ de bitcoin é negativo, ou seja, se o resultado é inferior ao custo da energia necessária para minerar bitcoin (ou outra criptomoeda), significa que o indivíduo não só está a perder dinheiro como também a consumir recursos desadequadamente, e isto é muito comum acontecer”

Medidas regulatórias e plataformas privadas

Para o efeito, alguns “governos estão a preparar medidas regulatórias no sentido de conter a pressão que a mineração trouxe à produção elétrica dos seus países”. É o caso da China, que se tem começado a posicionar política e publicamente no sentido de restringir estas atividade, afinal, “70% da atividade mundial de mineração de bitcoin é feita na China atualmente”.

Entretanto, estão a ser desenvolvidas variantes de blockchain em que a capacidade de processamento necessária para validar registos na cadeia é significativamente menor, como é o caso da litecoin, adianta Bruno Padinha.

Mas nem sempre o consumo é excessivo. Se a plataforma blockchain for pensada para empresas em mercados regulados, “a participação é controlada e o acesso requer identificação, o que efetivamente reduz as necessidades operacionais e permite a utilização de algoritmos mais eficientes, que asseguram a mesma proteção e resiliência e ainda permitem executar maiores volumes de transações”, defende o porta-voz da IBM. ●



**No mundo digital
será que
fazemos melhor
ou apenas mais?**



Quanto melhor a pergunta. Melhor a resposta. Melhor trabalha o Mundo.