Tecnologia Blockchain: uma visão geral.

01 Introdução

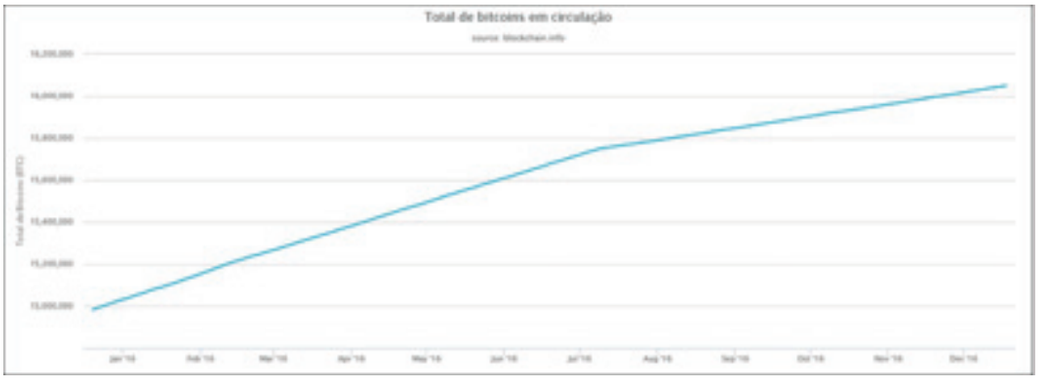
Em 2008, foi apresentado ao grupo de discussão “The Cryptography Mailing” um artigo[1] técnico contendo os princípios de funcionamento de uma cripto-moeda denominada Bitcoin, cuja proposta era a criação de uma moeda digital mundial que funcionasse em uma rede peer-to-peer e que permitisse o envio de pagamentos online de forma totalmente segura, sem o envolvimento de instituições financeiras para todos os participantes da rede. A autoria desse artigo é anônima e está sob o pseudônimo de Satoshi Nakamoto.

Desde então, muita coisa aconteceu. O software original foi disponibilizado abertamente sob a licença do MIT. Em 2009, a rede Bitcoin começou a funcionar com o lançamento do primeiro cliente bitcoin open source e a emissão das primeiras moedas bitcoins. Atualmente, estima-se que existam mais de 16 milhões de bitcoins em circulação.

---

1 Fonte: “Bitcoin: A Peer-to-Peer Electronic Cash System”. Satoshi Nakamoto. satoshin@gmx.com. www.bitcoin.org/bitcoin.pdf , acessada em 27/12/2016

As figuras a seguir mostram a quantidade de bitcoins em circulação e a cotação da moeda em dólar americano até dezembro de 2016[2].



Uma questão curiosa está relacionada com a autoria do artigo.

A primeira suspeita foi que se tratava de um grupo de programadores. Em versão mais recente, de maio de 2016, um empresário australiano denominado Craig Wright se identificou como o mentor da criptomoeda. Gavin Andresen, cientista-chefe da Bitcoin Foundation, confirmou em seu blog que está convencido de que Craig e Satoshi são a mesma pessoa[3].

---

2 Fonte: "Bitcoin: A Peer-to-Peer Electronic Cash System". Satoshi Nakamoto. satoshin@gmx.com. www.bitcoin.org/bitcoin.pdf , acessada em 27/12/2016

3 Fonte: http://www.techtudo.com.br/noticias/noticia/2016/05/quem-e-satoshi-nakamoto-identidade-do-Portanto, criador-do-bitcoin-e-revelada.html, acessada em 20/12/2016.

No entanto, qual é a relação entre Blockchain e Bitcoin? É muito comum as pessoas confundirem essas duas coisas e é natural que façam, uma vez que Blockchain é a plataforma tecnológica utilizada para o funcionamento da rede Bitcoin e de várias outras criptomoedas. Bitcoin é a primeira e a mais conhecida aplicação da tecnologia Blockchain.

Atualmente, existe uma enorme quantidade de criptomoedas em circulação no mundo, porém o Bitcoin é a com o maior marketshare. As aplicações da tecnologia Blockchain associadas às criptomoedas fazem parte da primeira geração dessa tecnologia e são denominadas Blockchain 1.0.

Após a implantação das primeiras criptomoedas, vários especialistas observaram que propriedades intrínsecas à tecnologia Blockchain (tais como segurança, resiliência, inviolabilidade e imutabilidade) poderiam ser usadas em vários outros tipos de aplicações. Neste sentido, as plataformas de desenvolvimento Blockchain evoluíram e permitiram a inserção de transações mais complexas através dos contratos inteligentes (smart contracts).

A partir de 2013, surgiu uma nova geração da tecnologia denominada Blockchain 2.0.

Atualmente, existe uma expectativa muito grande em relação ao futuro da tecnologia Blockchain. Segundo o Gartner, ela encontra-se próxima do topo do Gartner Hype Cycle for Emerging Tecnologies[4], conforme mostrado na figura a seguir. Ainda, segundo a revista britânica The Economist, a tecnologia é considerada "The Next Big Thing[5]".

---

4 Fonte: http://www.gartner.com/smarterwithgartner/3-trends-appear-in--the-gartner-hype-cycle-for-emerging-technologies-2016/, acessada em 20/12/2016.

5 Fonte: http://www.economist.com/news/special-report/21650295-or-it-next-big-thing. Maio de 2015. Acessada em 20/12/2016.

Além disso, investimentos significativos têm sido feitos na tecnologia.

Muitas startups estão sendo criadas com foco na tecnologia e as grandes empresas do mundo das tecnologias de informação e comunicação (TIC) têm investido grande quantidade de recursos, como, por exemplo, a IBM que, recentemente, transferiu o código da sua plataforma de desenvolvimento Blockchain para a Linux Foundation, constituindo, junto com outras iniciativas, a plataforma Hypeledger[6].

Distributed Ledger Technology (DTL) é a outra forma se referenciar à tecnologia Blockchain. Alguns especialistas colocam-na como o próximo passo evolutivo da internet, sendo denominada Internet do Valor, e que permitirá fazer com que o dinheiro flua na rede tão livremente como os dados estão fluindo atualmente. Neste sentido, os entusiastas esperam que a tecnologia possa

6 Fonte: https://www.hyperledger.org/about, acessado em 26/12/2016.

afetar as aplicações relacionadas com transações da mesma forma que o GPS mudou o transporte pessoal, através dos aplicativos de navegação[7].

Este whitepaper tem por objetivo apresentar uma visão geral da tecnologia Blockchain, abordando, de modo introdutório, os temas que julgamos mais relevantes. O texto está organizado do seguinte modo: a **seção 2** explica conceitos associados à tecnologia; a **seção 3** aborda áreas de aplicação promissoras. A **seção 4** relata algumas iniciativas de uso da tecnologia; a **seção 5** aborda as plataformas de desenvolvimento de aplicações. Finalmente, a **seção 6** oferece considerações e comentários finais.

Para uma visão mais detalhada sobre a tecnologia, o CPqD publicará, no curto prazo, uma série de whitepapers com os seguintes temas:

— Conceitos sobre a tecnologia Blockchain, tecnologias e desenvolvimento de aplicações.

— Aplicações, iniciativas e mercado da tecnologia Blockchain.

— Blockchain e Internet das Coisas (Internet of Things – IoT): aplicações e iniciativas.

---

7 Fonte: A Strategist's Guide to Blockchain. Price Whaterhouse Cooper. ISSUE 82 SPRING 2016. BY JOHN PLANSKY, TIM O'DONNELL, AND KIMBERLY RICHARDS.

02 Conceitos

A tecnologia Blockchain pode ser entendida de várias formas. Em linhas gerais, pode-se dizer que se trata de um sistema distribuído de base de dados em log, mantido e gerido de forma compartilhada e descentralizada (através de uma rede peer-to-peer, P2P), na qual todos os participantes são responsáveis por armazenar e manter a base de dados.

A tecnologia foi construída tendo em mente quatro principais características arquiteturais: segurança das operações, descentralização de armazenamento/computação, integridade de dados e imutabilidade de transações.

Dito de outra forma, Blockchain é uma “ledger of facts” replicada em computadores que participam de uma rede peer-to-peer, onde:

— O ledger é um livro de registros digital, no qual uma vez validado um registro, este nunca mais poderá ser apagado;

— Um fato (fact) pode significar várias coisas, desde uma transação monetária, a um conteúdo de determinado documento, ou até mesmo um programa de computador, contendo, em algumas plataformas, até uma base de dados pequena;

— Os membros participantes da rede podem, ou não ser anônimos e são chamados peers ou “nós”;

— Toda operação ou transação dentro da ledger é protegida por tecnologias criptográficas de assinatura digital, inclusive para identificar os nós emissores e receptores das transações;

— Quando um nó deseja adicionar ao ledger um fato novo, é necessário um consenso entre todos ou alguns nós previamente determinados da rede, para decidir se um fato pode ser registrado no ledger;

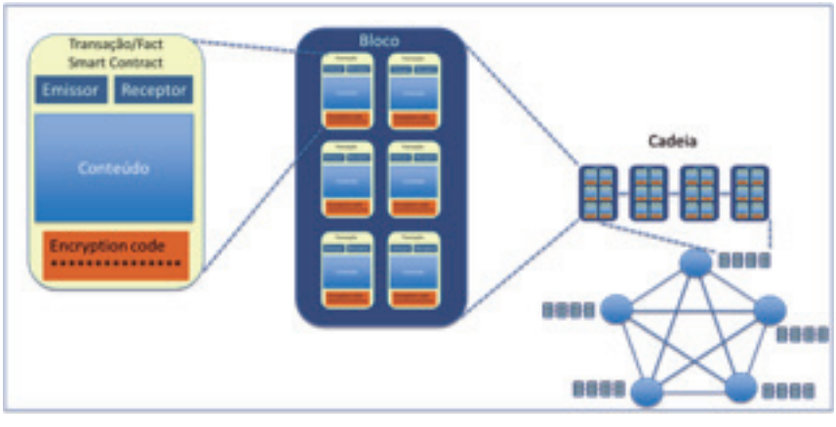
— Havendo consenso, o fato será escrito e nunca mais poderá ser apagado, em tese, um processo levemente semelhante à escritura e registro de um imóvel no Brasil.

Conforme mostrado na figura a seguir, uma rede Blockchain possui os seguintes elementos essenciais:

— **Fato (Fact):** pode ser uma transação, um conteúdo digital ou um programa de computador, este último também denominado contrato inteligente (smart contract);

— **Bloco:** é um conjunto de fatos, geralmente em um número fixo predefinido;

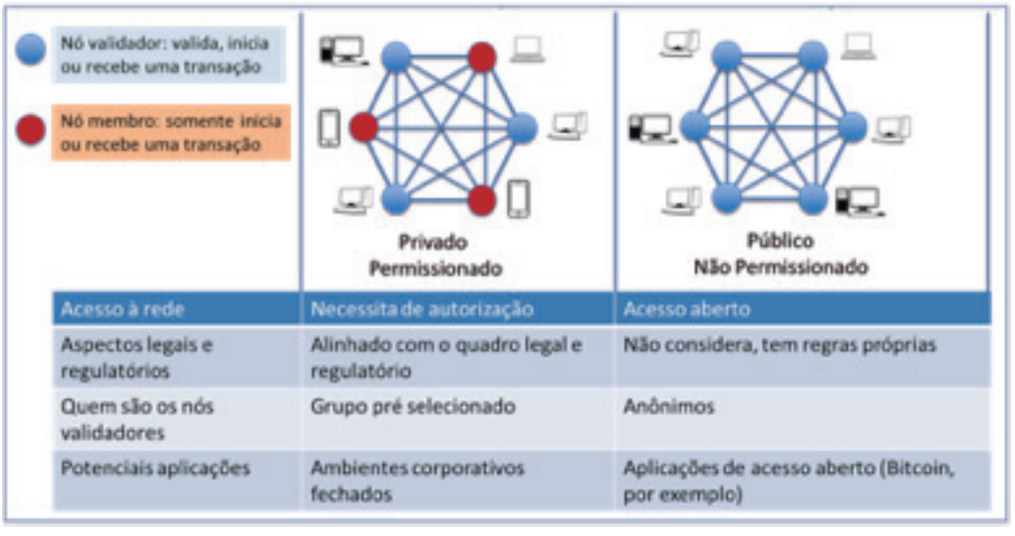
— **Cadeia de blocos (Blockchain):** conjunto de blocos encadeados (conectados um a um) seguindo uma lógica matemática, ou seja, não são independentes.



Do ponto de vista de aplicação, a tecnologia Blockchain passou por uma grande evolução com a possibilidade de uso dos contratos inteligentes.

Eles são programas de computador replicados e executados por todos os nós da rede, ou por um conjunto predeterminado de nós denominados validadores. Aplicações baseadas em contratos inteligentes são chamadas Decentralized Applications ou Dapps.

Atualmente, as redes Blockchain são divididas em dois grandes grupos: (i) as redes públicas ou de acesso aberto (permissionless) e (ii) as redes privadas ou de acesso autorizado (permissioned). A figura a seguir mostra algumas características de tais redes.



Acesso à rede	Necessita de autorização	Acesso aberto
Aspectos legais e regulatórios	Alinhado com o quadro legal e regulatório	Não considera, tem regras próprias
Quem são os nós validadores	Grupo pré selecionado	Anônimos
Potenciais aplicações	Ambientes corporativos fechados	Aplicações de acesso aberto (Bitcoin, por exemplo)

Eles são programas de computador replicados e executados por todos os nós da rede, ou por um conjunto predeterminado de nós denominados validadores. Aplicações baseadas em contratos inteligentes são chamadas Decentralized Applications ou Dapps.

O processo de validação ocorre quando um nó da rede, seguindo um conjunto de regras bem definidas, consegue montar um bloco que, neste exemplo, é um conjunto de transações monetárias utilizando a criptomoeda. Vale lembrar que o nó validador escolhe um número definido de transações não processadas da rede para montar o bloco.

Vários nós estão fazendo a mesma coisa simultaneamente, mas não necessariamente com as mesmas transações, ou seja, o processo de montagem do bloco depende das transações ainda não processadas visíveis ao nó. Há uma competição entre os nós para validar determinadas transações antes dos concorrentes. No Bitcoin, tal processo de validação é denominado mineração, em que o nó finaliza o processo de montagem do bloco quando resolve uma expressão matemática computacionalmente custosa.

Quando isso ocorre, todos os nós da rede são informados e o bloco, após passar por um processo de autenticação pelos demais nós, baseado nas regras de consenso, é inserido na cadeia com as transações devidamente validadas e um novo processo de construção de bloco se inicia em cada nó.

Uma pergunta frequente nas discussões sobre Blockchain está relacionada com as vantagens que a tecnologia possui em relação às outras tecnologias na resolução de problemas semelhantes. As principais vantagens do Blockchain sobre as tecnologias ditas convencionais[8] são:

— **Economia de tempo:** em algumas situações, como sistemas de pagamentos globais, o processamento de transações com Blockchain pode durar apenas minutos no lugar de dias, como outros sistemas convencionais;

— Minimização de custos: o acesso confiável a uma base de dados distribuída e consistente elimina custos operacionais (tais como de integração de sistemas heterogêneos) e, principalmente, de intermediários;

— Redução de riscos: a mitigação de fraudes, de adulterações e de outros crimes cibernéticos é facilitada pelo acesso transparente a dados imutáveis e íntegros;

— Aumento da confiança: processos e registros compartilhados com segurança e, se necessário, maior transparência, facilitam a verificação, a auditoria e a asseguração do bom funcionamento da infraestrutura tecnológica da qual dependem os parceiros de negócios.

---

8 Fonte: Blockchain: uma realidade para o mundo dos negócios. Luiz F. Jeronymo. IBM. Outubro de 2016.

03 Aplicações

Com a possibilidade de se utilizar os contratos inteligentes nas plataformas de desenvolvimento Blockchain atualmente disponíveis, as possibilidades de aplicações cresceram de modo significativo, indo além das já conhecidas criptomoedas, permitindo aplicações avançadas, tais como controle de imóveis, cadeias de produção e até mesmo a gestão de identidade digital de pessoas e coisas. Apresentamos, a seguir, um resumo destas possibilidades em diferentes setores.

A - Governo

Benefícios da tecnologia, tais como maior transparência, redução de fraudes, e compartilhamento de dados, favorecem o desenvolvimento de várias aplicações de extrema importância para o governo. Seguem alguns exemplos:

— **Votação eletrônica:** pode ser utilizada para impossibilitar a realização de dois votos pela mesma pessoa e a garantir a imutabilidade dos registros das zonas eleitorais;

— **Gestão de identidade de pessoas:** permite a implantação de programas confiáveis de abrangência nacional para a gestão de identidade digital dos cidadãos, permitindo o registro seguro de parâmetros biométricos;

— **Controle de acesso:** controle de acesso lógico e físico de diferentes serviços públicos e órgãos da administração com caraterísticas de rastreabilidade e imutabilidade de registros;

— **Pagamento de programas sociais:** permite a implantação de programas sociais com o rastreamento de recursos distribuídos;

— **Controle de ativos:** implantação de sistemas de controle de ativos em diferentes níveis da administração, mantendo o histórico de vida dos ativos cadastrados, desde o momento da sua compra até o seu descarte.

B - Telecomunicações

As aplicações da tecnologia Blockchain em telecomunicações são fortemente baseadas nos contratos inteligentes. A tecnologia pode ajudar as operadoras a cortar custos e ofertar serviços digitais a preços mais competitivos. Seguem alguns exemplos de aplicações[9]:

— **Processos internos:** billing, aprovisionamento de eSIM, bases de dados de portabilidade numérica e gestão de ativos;

— **Roaming:** implementação de bases de dados para autenticação de usuários em roaming;

— **Aprovisionamento de conectividade:** pagamentos e autenticação em Wi-Fi públicos;

— **Gestão de identidade:** autenticação entre dispositivos, aplicativos e organizações;

— **Cidades inteligentes:** transparência e auditoria para iniciativas de cidades inteligentes.

Outra aplicação que está sendo avaliada no âmbito do ITU, mais especificamente nas atividades do SG11 (subgrupo de trabalho 11), questão 15, é a utilização de solução de Blockchain para mitigar o problema de falsificação e de roubo de celulares no mundo.

---

9 Fonte: Enrique Velasco-Castillo. Nine Blockchain opportunities that telecoms operators should explore. Analysys Mason, jun. 2016.

O MMF (Mobile Manufacturers Forum) calcula que 20% dos celulares em operação no mundo são adulterados e/ou falsificados e utilizam IMEIs (International Mobile station Equipment Identity) falsos[10]. A solução permitiria o rastreamento e controle de acesso ao equipamento móvel desde a sua fabricação até o seu descarte[11].

C - Setor Elétrico

Assim com como setor de telecomunicações, a tecnologia Blockchain pode ajudar as concessionárias de energia na redução do custo operacional e na oferta de novos serviços. Seguem alguns exemplos de aplicações[12]:

— Controle e monitoramentos de ativos: sua implementação é feita através de combinação de redes mesh + Blockchain;

— Gestão descentralizada da compra e venda de energia na geração distribuída, eliminando necessidade de intermediários;

— Pagamento de car sharing para veículos elétricos;

— Diminuição do custo de compliance junto à agência reguladora de energia e outros órgãos de controle.

---

12 Fonte: How Blockchain Technology Can Reinvent the Power Grid. May, 2016. http://fortune.com/2016/05/15/Blockchain-reinvents-power-grid/, em 20/12/2016.

D - Setor Financeiro

É o setor que mais tem investido na tecnologia Blockchain. Calcula-se que 80% dos bancos terão, em 2017, algum projeto utilizando a tecnologia. Atualmente, mais de 90 bancos centrais estão discutindo a tecnologia, suas aplicações e seus impactos no arcabouço legal e regulatório. Isso vale para as instituições incumbentes e para os novos bancos virtuais. Principais benefícios esperados com o uso da tecnologia:

— Simplificação da operação e diminuição de custo operacional;

— Menor número de intermediários;

— Diminuição de custo de compliance, propiciando menor tensão entre reguladores
e regulados;

— Mitigação de fraudes;

— Oferta de novos serviços.

Algumas potenciais aplicações:

— Gestão de identidade digital (Know Your Customer);
— Implantação de criptomoedas;
— Gestão de empréstimos consignados;
— Rastreamento e liquidação de cartas de crédito;
— Pagamentos globais;
— Seguros de acidentes e propriedades.

E - Internet das Coisas

Um grande problema associado à Internet das Coisas (Internet of Things – IoT) são os aspectos relacionados a segurança e privacidade. A utilização da tecnologia Blockchain contribui para a mitigação do problema. Seguem alguns benefícios:

— Rastrear a história única de cada dispositivo, registrando a troca de dados com outros dispositivos, serviços web e usuários humanos;

— Permitir que dispositivos inteligentes atuem de forma autônoma em uma variedade de transações.

Exemplos de aplicação:

— Monitoramento remoto de ativos de elevado valor para verificar, por exemplo, se estão sendo usados corretamente;

— Monitoramento, controle e autorização de solicitação de determinado equipamento para reposição de alguma peça ou matéria-prima (máquina de lavar solicitando sabão, por exemplo);

— Controle de identidade dos dispositivos IoT para registro e controle de acesso lógico a diferentes aplicações.

F - Outros Exemplos

A tecnologia Blockchain pode ser aplicada em projetos estruturantes, que envolveriam diferentes atores de uma cadeia de valor. Seguem alguns exemplos:

— Monitoramento e rastreamento de uma cadeia de produção, por exemplo, fabricação de automóveis, produção de vinhos, produção de equipamentos de informática, dentre outros;

— Sistema de gestão de logística reversa de diferentes produtos. Exemplos: produção de medicamentos, produtos eletroeletrônicos e seus resíduos;

— Sistemas de gestão e controle da distribuição e venda de medicamentos de uso controlado.

04 Iniciativas de Empresas e Governos

EMPRESAS

Várias empresas têm investido na tecnologia Blockchain. Nos últimos anos, observou-se o surgimento de um grande número de startups, sendo muitas delas financiadas por grandes empresas. Calcula-se que existam mais de 140 empresas de capital de risco que estão apoiando iniciativas nesta tecnologia, sendo quase 30% oriundas do Vale do Silício na Califórnia, com um investimento estimado, até o momento, em cerca de US$ 1,3 bilhões[13].

O setor que mais vem investindo é o financeiro através das fintechs (Financial Technology). Além disso, vários bancos e algumas bolsas de valores investem em provas de conceito, tais como:

— 14 dos 30 maiores bancos estão com projetos, como: Bank of America, BNP Paribas, Barclays, HSBC, JP Morgan, Santander e Bradesco;

13 Fonte: http://www.coindesk.com/research/state-of-Blockchain-q3-2016/.

— Bolsas de valores, como Nasdaq (em parceria com a Chain, totalizando US$30 mi de investimentos), JPX, ASX e Swiss Exchange, BM&F Bovespa.

No grupo das grandes empresas de TIC, destacam-se: Microsoft, HP, IBM e Intel. A Microsoft tem investido na tecnologia Blockchain de diferentes formas. Uma delas é o desenvolvimento de uma plataforma de Blockchain como serviço (Blockchain-as-a-Servise – BaaS).

Em agosto de 2016, a plataforma foi disponibilizada para testes e, em setembro, foi lançado o grupo de trabalho denominado “Smart Contracts Security Working Group - Kinakuta”, com o objetivo de compartilhar as melhores práticas de desenvolvimento de contratos inteligentes. Ainda em setembro, a empresa revelou sua participação na nova versão do consórcio “Blockchain software Bletchley”. Além disso, a Microsoft também é parceira da R3CEV no desenvolvimento de provas de conceito.

A Samsung, em parceria com a IBM, investe no desenvolvimento de aplicações em IoT no projeto denominado ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry). A Samsung SDS investe em startups denominadas Bloko e Darktrace. Além disso, o Samsung Strategy and Innovation Center, em parceria com a Canonical e Slock.it, desenvolve soluções para trazer a tecnologia Blockchain para dentro das casas.

O Wal-Mart recentemente anunciou um projeto com a IBM para testar o uso da tecnologia Blockchain para melhorar a segurança alimentar. Ainda em outubro, começou a rastrear um produto embalado nos EUA e carne de porco na China.

GOVERNOS

A Comissão Europeia (CE) está investigando o potencial da tecnologia. Seguem algumas iniciativas recentes do segundo semestre de 2016:

— CE aprova uma força tarefa dedicada ao estudo de criptomoedas;

— Grupo de especialistas do parlamento divulga um “discussion paper” sobre aplicação da tecnologia em processos eleitorais;

— Incentivo, através do Horizon 2020, às startups juntamente com potenciais investidores, parceiros de negócio, universidade e centros de pesquisa no desenvolvimento de soluções utilizando a tecnologia.

O governo do Reino Unido tem tratado o assunto de forma bastante estruturada. No final de 2015, divulgou um relatório denominado “Distributed Ledger Technology: beyond blockchain”[14]. Seguramente, trata-se de um dos melhores relatórios sobre a tecnologia, suas aplicações, aspectos regulatórios e perspectivas.

---

14 Fonte: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf, acessado em 21/12/2016.

— Bolsas de valores, como Nasdaq (em parceria com a Chain, totalizando US$30 mi de investimentos), JPX, ASX e Swiss Exchange, BM&F Bovespa.

O estudo foi coordenado e elaborado pelo “UK Government Chief Scientific Adviser” e contou com a participação de especialista do governo, universidades e de empresas. O estudo teve por objetivo avaliar o potencial da tecnologia na maximização dos benefícios quando aplicada aos serviços públicos, assim como identificar as novas oportunidades de negócio através de parcerias internas e externas.

Neste mesmo ano, foram investidas cerca de 10 milhões de libras em atividades de pesquisa para estudar criptomoedas e outras inovações associadas à tecnologia, tais como a transferência de ativos digitais na internet[15].

Vale um destaque para o US Federal Reserve, o banco central dos EUA, que lançou, no início de dezembro de 2016, o relatório sobre a tecnologia denominado “Distributed ledger technology in payments, clearing, and settlement”. Na visão do banco, as aplicações da tecnologia ainda estão em estágio inicial, havendo ainda uma série de desafios para o desenvolvimento e adoção de plataformas baseadas em Blockchain, incluindo questões em torno de casos de negócios, barreiras tecnológicas, considerações legais e de gerenciamento de risco.

---

15 Fonte: Blockchain: Powering the Internet of Value. Evry. https://www.evry.com/globalassets/insight/bank2020/bank-2020-
---Blockchain-powering-the-internet-of-value---whitepaper.pdf em 20/12/2016.

Vários governos ao redor do mundo trabalham com diferentes iniciativas de aplicações. Citam-se três das mais conhecidas:

— **Estônia:** e-residency program com digital ID e plano de saúde com registro médicos rastreados;

— **Suíça:** registro de transações imobiliárias;

— **Reino Unido:** distribuição de benefícios, departamento de trabalho e pensões.

05 Ambiente de Desenvolvimento

Atualmente, é possível desenvolver aplicações de Blockchain utilizando plataformas de desenvolvimento com código aberto ou proprietário, porém predomina a tendência de desenvolvimento sobre plataformas de código aberto. Tais plataformas podem ser classificadas, quanto a disponibilização de uma ledger pública, em duas modalidades:

— Públicas (public Blockchain): Bitcoin, Ethereum, Coinbase, entre outras;

— Privadas (enterprise Blockchain): Ripple, Chain, Hyperledger, DAH (Digital Asset Holdings), etc.

Os fundamentos da plataforma foram apresentados no artigo de 2008 e posteriormente seu código foi disponibilizado. Atualmente, vários desenvolvedores de aplicação a utilizam, tais como fornecedores de carteira eletrônica, processamento de pagamentos, mineradores, empresas de seguros, dentre outros.

O protocolo e o software Bitcoin são publicados abertamente e estão disponíveis para qualquer desenvolvedor revisá-lo ou fazer a sua própria versão modificada do software Bitcoin.
Atualmente, o código Bitcoin é mantido como Bitcoin Core por uma comunidade de programadores, seguidores e voluntários[16].

Os fundamentos da plataforma foram apresentados no artigo de 2008 e posteriormente seu código foi disponibilizado. Atualmente, vários desenvolvedores de aplicação a utilizam, tais como fornecedores de carteira eletrônica, processamento de pagamentos, mineradores, empresas de seguros, dentre outros.

O protocolo e o software Bitcoin são publicados abertamente e estão disponíveis para qualquer desenvolvedor revisá-lo ou fazer a sua própria versão modificada do software Bitcoin.
Atualmente, o código Bitcoin é mantido como Bitcoin Core por uma comunidade de programadores, seguidores e voluntários[16].

Existem três formas de utilização da plataforma, onde o desenvolvedor poderá rodar sua aplicação[17]:

— Utilizando um provedor de serviço de pagamento, com o qual a sua aplicação será capaz de aceitar o Bitcoin como forma de pagamento. Tais empresas geralmente disponibilizam APIs e ferramentas para integrar às aplicações;

— Utilizando um provedor de serviço que fornece API para um Blockchain nó da rede, tornando a rede Blockchain Bitcoin mais acessível para os desenvolvedores;

— Escrevendo a sua própria integração, acessando diretamente a rede Bitcoin.

---

16 Fonte: bitcoin.org.

17 Fonte: DEVELOPING BITCOIN APPLICATIONS – AN OVERVIEW. Fonte: https://www.rails-love.com/stories/developing-bitcoin-applications-an-overview. Acessado em 22/12/2016.

A plataforma Ethereum foi proposta no final de 2013 por Vitalik Buterin, um pesquisador e programador de criptomoedas, e é considerada uma evolução da plataforma Bitcoin. Seu funcionamento foi descrito no whitepaper denominado "A Next-Generation Smart Contract and Decentralized Application Platform"[18].

Trata-se de uma plataforma pública e de código aberto, lançada em 2015, que suporta contratos inteligentes. Ela provê uma plataforma computacional com máquinas virtuais descentralizadas denominadas Ethereum Virtual Machines (EVM), que executam contratos usando uma criptomoeda denominada ether. Na Ethereum, os contratos inteligentes são escritos em linguagens de programação como Solidity e Serpent (derivação do Python).

O uso de recursos como aplicação descentralizada e de contratos inteligentes permite o desenvolvimento de diferentes tipos de aplicação não só para o setor financeiro. Tal característica aumentou o interesse das grandes empresas pela plataforma. Por isso, Ethereum é uma das plataformas mais utilizadas em projetos pilotos atualmente. Por exemplo, a Microsoft e o Santander estão com projetos piloto e a Thompson Reuters lançou recentemente uma solução de gestão de identidade denominada BlockoneID.

18 Fonte: https://github.com/ethereum/wiki/wiki/White-Paper, acessada em 22/12/2016.

A criptomoeda Ether está na segunda posição na divisão de mercado de criptomoedas, perdendo somente para o Bitcoin, com um volume pouco superior a US$ 1 bilhão em julho de 2016. Existe a Ethereum Foundation, uma fundação sem fins lucrativos que tem como objetivo promover e buscar recursos para pesquisa, desenvolvimento e capacitação da tecnologia.

HYPERLEDGER

É uma plataforma de código aberto, porém sem uma ledger pública, lançada em 2015 e voltada para ambientes empresariais e diferentes tipos de aplicação. Atualmente está na sua versão 0.8 e sofre ainda com instabilidades em seu desenvolvimento. Prevê-se o lançamento da versão 1.0 para o início de 2017.

Trata-se de um projeto colaborativo com a participação de várias empresas de grande porte e, atualmente, sua gestão é feita pela Linux Foundation. As principais colaborações de código vieram de trabalhos prévios feitos pela Digital Asset Holdings (Blockstream's libconsensus) e a OpenBlockchain da IBM. Atualmente, é a plataforma de desenvolvimento Blockchain da IBM, juntamente com o Bluemix. A comunidade conta com 81 membros.

A plataforma de desenvolvimento Hyperledger é menos voltada para criptomoedas (embora possa ser utilizada para tal) e promove aplicações baseadas em sua versão de contratos inteligentes, denominados de chaincodes, que podem ser escritos em linguagens de programação de uso geral como Go e Java.

É uma empresa focada no desenvolvimento de soluções para o mercado financeiro, parte destas utilizando a tecnologia Blockchain. Desenvolve tais soluções sobre um protocolo denominado Interledger Protocol ou ILP para suportar pagamentos entre diferentes ledgers de uma rede global.

Possui mais de 50 parceiros, sendo 19 do setor financeiro.
Apresentou um crescimento de 25% de crescimento nas parcerias no terceiro trimestre de 2016.

06 Comentários Finais

Existe grande expectativa do mercado, de governos, assim como das comunidades acadêmica e de desenvolvedores de solução, em relação ao futuro da tecnologia Blockchain. Alguns especialistas a consideram o quinto paradigma disruptivo da computação, que poderá trazer uma experiência ubíqua de internet do valor[19].

Em entrevistas realizadas no segundo semestre de 2016, durante o Consesus Summit[20], com 243 especialistas em Blockchain de startups e empresas de grande porte, concluiu-se que:

— 86% dos entrevistados acreditam que a tecnologia terá impacto nos serviços financeiros, enquanto 14% acreditam que é muito cedo para concluir algo;

— 70% acreditam que a tecnologia terá impacto em aplicações de governo e outras áreas não financeiras;

— 52% acreditam que será necessário ainda de 5 a 10 anos para a uma adoção ampla da tecnologia.

Falando especificamente das aplicações da tecnologia Blockchain para o setor financeiro, avalia-se que esta poderá trazer mudanças estruturais no médio e longo prazo para este mercado. Porém, vale ressaltar que o desenvolvimento de tais aplicações se encontra no seu estágio inicial, ainda distantes do mundo real[21].

---

19 Fonte: Swan,M (2015); Blockchain: Blueprint for a new economy.

20 Fonte: http://www.coindesk.com/events/consensus-2016/.

21 Fonte: http://www.ibtimes.co.uk/us-federal-reserve-industry-understanding-fintech-Blockchain-still-its-infancy-1595107.

Em relação aos investimentos, ainda não existe muita clareza sobre qual é a tendência. Os investimentos na tecnologia caíram 18% neste último ano (2016), apesar de atingir US $114 milhões no terceiro trimestre[22].

Uma das razões para as quedas pode ser uma mudança na forma como start-ups estão abordando o mercado. Como evidenciado pelos financiamentos nas empresas Ripple e Juzhen, mais dinheiro está sendo concedido às startups que estão procurando trabalhar ao lado e não contra os grandes bancos[23].

O interesse dos bancos centrais está em alta e estas instituições provavelmente seguirão avaliando os impactos tecnológicos, regulatórios, oferta de novos serviços, assim como nos modelos de negócios atuais. As principais instituições financeiras em todo o mundo estão agora explorando a tecnologia, com destaque para um aumento no interesse dos governos na Ásia.

No Brasil, o assunto também vem ganhando atenção no setor financeiro.

Várias palestras sobre Blockchain foram apresentadas no Ciab FEBRABAN 2016. No evento, os bancos Itaú e Bradesco anunciaram a associação ao consórcio R3. Os especialistas que se apresentaram no evento foram categóricos ao afirmar que: a Distributed Ledger Technology é uma ruptura tão importante para os serviços financeiros como foi a Internet[24].

Em setembro de 2016, foi realizado o primeiro “Hackathon Internacional de Blockchain” no Brasil[25]. O evento foi organizado pelo Blockchain Center, um grupo focado em reunir empresas com atividades relacionadas ao Blockchain e tecnologias similares. Seu objetivo é fomentar a adoção e o desenvolvimento

destas tecnologias, para ajudar a tornar o Brasil referência em tecnologia e inovação na área.

O CPqD vem estudando a tecnologia desde meados de 2016. Neste período, especialistas das áreas de tecnologia de segurança da informação e computação cognitiva analisaram algumas plataformas de desenvolvimento e, atualmente, desenvolvem provas de conceito utilizando contratos inteligentes. Além disso, foi iniciado um processo de criação de parcerias para desenvolvimento de aplicações, assim como proposição de projetos de pesquisa e desenvolvimento para diferentes setores do mercado.

---

22 Fonte: http://www.coindesk.com/research/state-of-Blockchain-q3-2016/.

23 Fonte: http://www.coindesk.com/coindesk-research-state-Blockchain-q3-six-takeaways/.

24 Fonte: Decifrar para não ser devorado. Ediane Tiago. Revista Ciab FEBRABAN. Julho/agosto de 2016. Edição 64. http://www.ciab.com.br/pt/publicacoes/revistas#publicacoes, acessado em 23/12/2016.

25 Fonte: http://www.brasscom.org.br/brasscom/Portugues/detNoticia.php?codArea=2&codCategoria=51&codNoticia=1603, acessado em 23/12/2016.

JOSÉ REYNALDO FORMIGONI FILHO

Graduado em 1984 em engenharia elétrica pela Universidade de Campinas. Em 1995 obteve o título de mestre em engenharia de sistemas pela mesma universidade. Ingressou no CPqD em 2000, atuando como consultor e pesquisador em diferentes projetos nos setores de telecomunicações, financeiro e elétrico. De 2004 a 2010 foi gerente de estratégia e inteligência regulatória. Do final de 2010 até o presente é o gerente da área de Tecnologias de Segurança da Informação e Comunicação. Atualmente, coordena atividades relacionadas com a tecnologia Blockchain no CPqD.

ALEXANDRE MELLO BRAGA

Bacharel em ciência da computação (UFPA, 1996), mestre em ciência da computação (UNICAMP, 1999) e especialista no desenvolvimento de aplicações para Internet (UNIRIO, 2004). Está concluindo o doutorado no Instituto de Computação da UNICAMP com o tema desenvolvimento de software criptográfico seguro. No CPqD desde 2000, já atuou como desenvolvedor de software e consultor em segurança da informação em projetos para os setores financeiro, governo, forças armadas, varejo, telecomunicações e saúde.

Atualmente atua como pesquisador em segurança da informação e criptografia aplicada. Possui publicações científicas sobre segurança da informação, segurança de software e criptografia aplicada, em conferências nacionais e internacionais, com mais de 200 citações acadêmicas e um prêmio de melhor artigo. Professor em cursos de graduação e de pós-graduação em Campinas, São Paulo, desde 2001, nas disciplinas de criptografia aplicada, desenvolvimento de software seguro, segurança em redes e segurança na Internet. Possui as seguintes certificações profissionais: PMP, CSSLP, CISSP, SCJP, SCMAD, SCWCD.

RODRIGO LIMA VERDE LEAL

Possui graduação em Engenharia Elétrica pela UNICAMP (1995), especialização em Administração pela FGV-SP (2002) e mestrado em Política Científica e Tecnológica pela UNICAMP (2007). Atualmente é pesquisador da Fundação CPqD responsável pela formulação de projetos de P&D com parceiros industriais e governamentais. Tem experiência na área de gestão da inovação e marketing de produto, atuando principalmente nos seguintes temas: TIC (telecomunicações e TI), modelos de negócio, design thinking, gestão de portfólio e roadmaps tecnológicos.