# Guia básico sobre BITCOIN

TUDO O QUE VOCÊ PRECISA SABER SOBRE A MOEDA DIGITAL QUE ESTÁ MUDANDO O MUNDO

coinBR.net
BlockchainTech

# Uma breve história sobre as moedas

“É muito legal o fato de que dentro do universo Bitcoin um algorítmo substitui as funções de um governo. Eu sou um grande fã do bitcoin”. Esta afirmação saiu da boca de ninguém menos que Al Gore, ex-vice-presidente dos Estados Unidos. A cada dia, mais e mais pessoas importantes tanto na política quanto no mundo dos negócios estão se curvando e aplaudindo esta nova tecnologia, que tem provocado uma mudança radical sobre o conceito do dinheiro.

Por milênios, o ouro foi o ativo financeiro com mais evidência e suas características intrínsecas o fizeram perdurar até os dias de hoje. Com o desenvolvimento das civilizações e, principalmente, após a era da industrialização, as entidades governamentais perceberam que imprimir o seu próprio dinheiro seria um método mais conveniente e fácil de distribuir a riqueza na sociedade.

Entretanto, o papel moeda dos governos não resistiu ao teste do tempo e vários casos de fracasso passaram a ser observados. A história brasileira é um grande exemplo disso: antes do real surgir em 1994, o Brasil possuiu diversas moedas que derrocaram, como o cruzeiro, o cruzado e o cruzado novo.

De acordo com um estudo feito pelo DollarDaze.org com base em 775 moedas, não há qualquer precedente histórico de uma moeda que tenha obtido sucesso em reter seu valor: 20% delas fracassaram devido a hiperinflação, 21% foram destruídas por guerras, 12% destruídas por movimentos de independência, 24% foram monetariamente reformadas e apenas 23% ainda estão em circulação, contudo com fortes indícios de estarem trilhando o mesmo caminho das moedas que não deram certo. Estima-se que, historicamente, a vida média de uma moeda tenha sido de apenas 27 anos.

Criada em 1694, a libra esterlina do Reino Unido é a mais velha moeda em existência. Aos 322 anos de existência, ela pode ser considerada uma moeda de grande sucesso. Contudo, este suposto sucesso é bastante relativo. Quando surgiu, seu valor foi definido a um padrão de uma unidade por 12 onças de prata. A valores atuais, portanto, ela vale 1/200 ou 0,5% de seu valor original. Em outras palavras, a moeda considerada de maior sucesso no mundo perdeu 99,5% de seu valor ao longo do tempo.

De volta ao século 21, em uma época em que existem mais telefones celulares que habitantes no planeta Terra, faz todo sentido existir uma moeda global. O bitcoin é exatamente isso: uma moeda digital universal que funciona a partir de qualquer computador ou dispositivo móvel conectado à Internet.

O bitcoin permite que duas pessoas que nunca se viram realizem uma transação extremamente segura utilizando uma rede global de trocas por meio da Internet. Essa rede foi constituída graças à dedicação de milhares de pessoas espalhadas pelo mundo que passaram anos estudando uma tecnologia computacional que tornou essa realidade possível.

Com isso, utilizando apenas telefones celulares, duas pessoas podem agora fazer uma transação que não depende de uma autoridade central, uma companhia ou um banco intermediando esse processo. Tudo isso de uma maneira muito segura, transparente e incontestável. Bem-vindos à tecnologia Bitcoin.

“

**É muito legal o fato de que dentro do universo Bitcoin um algorítmo substitui as funções de um governo. Eu sou um grande fã do bitcoin**

- Al Gore, ex-vice-presidente dos EUA

”

# O SURGIMENTO DO BITCOIN

O bitcoin entrou em circulação em janeiro de 2009. Seu funcionamento não exige cartão de crédito, conta bancária ou a divulgação de qualquer identificação pessoal para ser utilizado e, em muitos casos, como explicaremos ao longo deste texto, para ser adquirido. A grande sacada é que você não está mais usando uma moeda emitida por um governo central. Ela é uma moeda totalmente nova e revolucionária: dinheiro 100% digital para vidas cada vez mais digitais.

Dois meses antes de o bitcoin entrar em circulação, foi publicado um artigo intitulado “Bitcoin, um sistema de dinheiro eletrônico ponto-a-ponto”. O autor deste artigo é Satoshi Nakamoto, um pseudônimo criado por um sujeito brilhante que até hoje não revelou sua verdadeira identidade e que talvez nunca a revelará.

À época em que o bitcoin foi lançado, o mundo adentrava os primórdios da última grande crise financeira internacional, que eclodiu com a quebra do banco americano Lehman Brothers. O mundo todo temia o colapso do sistema financeiro, das bolsas de valores e das moedas em circulação. O bitcoin, então, conseguiu responder a uma importante questão que todos possuíam: onde alguém pode guardar sua riqueza caso o sistema financeiro fracasse? A resposta: na Internet.

A onipresença da Internet no século 21 é de extrema importância para o surgimento do bitcoin. Dos cerca de 5 bilhões de adultos no mundo, mais de 85% possuem telefones celulares. Todos podem transacionar bitcoins livremente. A acessibilidade global do bitcoin é uma de suas mais importantes características.

Todo ano, mais de 500 bilhões de dólares são enviados para além das fronteiras dos países na forma de remessas financeiras. Isso ocorre porque existem milhões de imigrantes trabalhando em outros países enviando dinheiro para suas famílias em suas terras natal. Muitas dessas pessoas que recebem estes valores são desbancarizadas, tornando esse processo de remessa bastante custoso e ineficiente. De acordo com o Banco Mundial, o custo médio por usuário para enviar dinheiro de algum país pertencente ao G8 a outro país é de cerca de 10%, utilizando populares serviços, como o Western Union, o Money Gram ou até mesmo os bancos tradicionais.

O bitcoin é uma grande disrupção para este mercado de remessas. Ele permite aos usuários enviar dinheiro em minutos, por uma fração do custo, usando apenas um telefone celular, tudo isso de uma maneira simples, bastando apenas alguns toques na tela do seu celular. Considerando que cerca de metade da população adulta no mundo está fora do sistema bancário, o bitcoin torna-se a grande alternativa para envio de valores a outros lugares.

Para quem é bancarizado, apesar dos custos envolvidos, enviar dinheiro para outros países não é assim tão difícil, mas os riscos envolvidos nas transações são relevantes. Crimes digitais e hackers estão por toda parte. Grandes empresas, como a Sony e até o banco JP Morgan, foram alvos de ataques de hackers e viram milhões de contas de seus clientes caírem em mãos erradas, tudo isso porque muitas vezes você é obrigado a passar informações, como o número de seu cartão de crédito, seu nome, seu endereço, dentro outros dados, para concretizar uma transação.

Os cartões de crédito foram inventados na década de 50 e hoje podem ser clonados de maneira muito fácil. Nem mesmo os cartões com chip, criados mais recentemente, são imunes aos ataques de criminosos.

Atualmente, mais de 100 mil companhias em todo mundo já aceitam bitcoins como forma de pagamento. E para utilizar bitcoins você não precisa fornecer qualquer tipo de informação pessoal, o que torna praticamente impossível qualquer ataque criminoso à sua carteira digital de bitcoins.

E não é somente para os usuários de bitcoin que existem benefícios, para quem aceita a moeda digital também é bastante vantajoso. Existem duas grandes vantagens: a primeira é que o comerciante não precisa pagar de 2% a 3% de taxa para a companhia de cartão de crédito que estaria intermediando a transação tradicional. O custo médio para um comerciante aceitar bitcoin e convertê-lo na moeda de seu país é de menos de 1%. Se o comerciante quiser manter os bitcoins consigo, então a transação fica livre de quaisquer taxas, praticamente como um negócio feito com dinheiro vivo; a segunda vantagem é que não existe chargeback, ou o cancelamento da transação por parte do cliente. Muitas empresas sofrem milionárias perdas todos os anos porque os clientes ligam para as companhias de cartão de crédito e simplesmente cancelam a transação realizada. O bitcoin não sofre desses problemas.

# COMO O BITCOIN FUNCIONA

Como já dito, o bitcoin é uma moeda digital que permite ao usuário transacionar, de maneira extremamente segura, sem a necessidade de um intermediário ou autoridade central. Esta é a grande beleza desta invenção.

A interface de funcionamento da tecnologia é similar à forma como o PayPal funciona. Por exemplo, se João quer enviar dinheiro, em forma de bitcoins, à Maria, ele irá acessar sua conta em seu telefone celular ou computador, escolher o montante a ser enviado, o destinatário e apertar o botão enviar. Ele também poderá anexar uma mensagem à esta transação, que poderá conter qualquer tipo de informação importante, como explicaremos mais adiante. Até aqui nada de muito diferente das outras tecnologias

existentes. Mas é o que está por trás do bitcoin que o difere e o torna único.

Assim como o AirBnB e o Uber, o bitcoin faz parte do que chamamos de economia compartilhada, uma maneira de transacionar ponto-a-ponto (peer-to-peer) produtos e serviços. No caso do AirBnB, os usuários podem monetizar sua casa ou seu quarto os alugando por um determinado valor. Enquanto o Uber permite que um usuário monetize seu carro e ofereça caronas a outras pessoas. Com o bitcoin, os indivíduos podem monetizar seus computadores ao compartilhar o poder de processamento na Internet com o objetivo de verificar as transações da rede bitcoin.

Essas pessoas que disponibilizam seus computadores para a verificação da rede Bitcoin são chamadas de "mineradoras" e objetivo principal delas é o de verificar os blocos de transações de maneira rápida e eficiente. Como contrapartida, elas recebem bitcoins caso concluam a verificação de um bloco de bitcoin.

Assim, quando João envia alguma quantidade de bitcoin à Maria, aquela informação é propagada na rede para todos os computadores mineradores que estão distribuídos globalmente e que estão simultaneamente verificando e adicionando transações aprovadas para o livro-registro do bitcoin, conhecido formalmente como "Blockchain".

Os mineradores são partes essenciais para o bitcoin funcionar porque eles garantem a integridade das transações. São eles que registram que aquela quantidade de bitcoins enviadas por João saiu de sua carteira e agora está em posse de Maria.

# A BLOCKCHAIN E A MINERAÇÃO

A blockchain é a grande revolução tecnológica que faz do Bitcoin ser único e disruptivo. É um livro-registro descentralizado que acompanha todas as transações da história do bitcoin.

O fato de ser uma rede descentralizada torna o bitcoin praticamente impossível de ser hackeado. Não existe um computador central ou um grupo de computadores que possa ser alvo de ataque. Os computadores que estão rodando na rede estão espalhados pelo mundo. Diferente do AirBnB e do Uber, o bitcoin não é uma empresa ou entidade.

A melhor maneira de pensar o bitcoin é o relacionando ao e-mail, que é uma tecnologia ponto-a-ponto que existe gratuitamente na Internet com o objetivo de transmitir informações mais eficientemente.

Satoshi Nakamoto programou o algorítmo que sustenta o bitcoin para funcionar de uma maneira que as transações são agrupadas em um bloco a cada 10 minutos. Ele também desenhou um sofisticado e inteligente sistema de recompensas visando incentivar aqueles que validam as transações que estão sendo incorporadas à blockchain, no caso os mineradores.

A cada vez que um novo bloco é resolvido, o que significa que o minerador verificou todas as transações do bloco e que estas foram provadas válidas para mais de 50% do resto dos mineradores, aquele bloco minerado é adicionado ao livro-registro, na sequência de todos os outros blocos que já foram mineradores no passado.

Automaticamente, os registros de todos os mineradores são atualizados para refletir aquela última adição na corrente de blocos, e aquele minerador que realizou o último trabalho de verificação é recompensado. O código do bitcoin é programado para automaticamente liberar um certo montante de bitcoins para o minerador que trabalhar mais rápido naqueles últimos 10 minutos. É assim que novos bitcoins entram em circulação, sem a necessidade de uma autoridade central controlar seu suprimento, como acontece com as moedas tradicionais.

O montante da recompensa foi programado para cair pela metade a cada 210 mil blocos minerados, ou a cada quatro anos. Este mecanismo foi desenhado por Satoshi Nakamoto com o objetivo de controlar o suprimento e limitar a inflação da moeda. Quando o bitcoin foi lançado em 2009, o minerador recebia 50 bitcoins por bloco minerado. Em 2012, o bloco de número 210 mil foi minerado e a recompensa caiu para 25 bitcoins, o que significa que a cada 10 minutos 25 novos bitcoins entram em circulação.

É possível prever quando acontecerá a nova redução de recompensas. No dia 23 de julho de 2016, quando o bloco 420 mil for minerado, a recompensa cairá novamente, agora para 12,5 bitcoins.

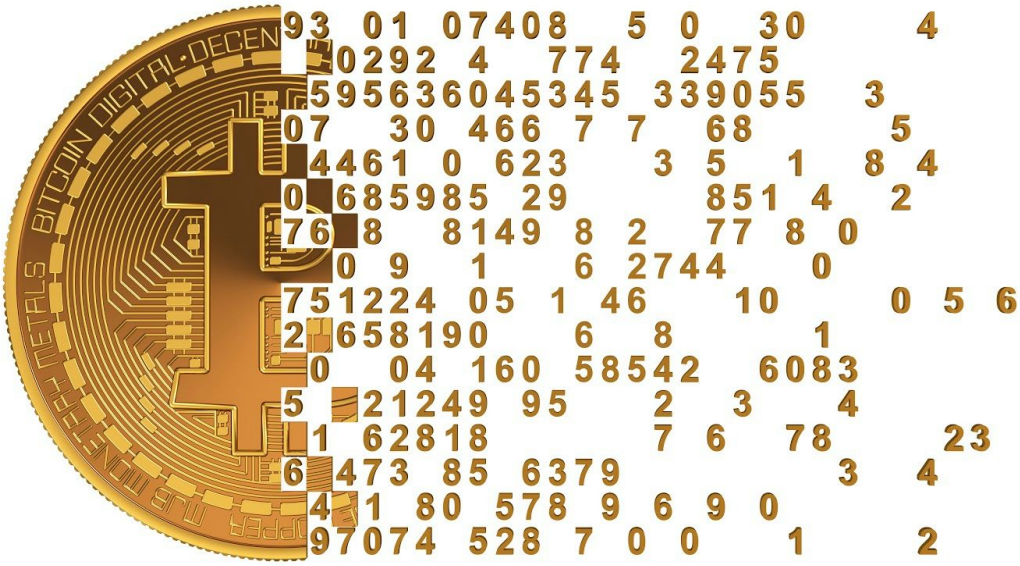
Espera-se que em 2140, a recompensa por bloco minerado chegue a zero e que o montante total de bitcoins atinja seu suprimento máximo, que de acordo com o código criado por Satoshi Nakamoto, será de 21 milhões de unidades de bitcoin. Nenhum outro bitcoin poderá ser criado depois disso.

Isso significa que a recompensa para os indivíduos responsáveis pela verificação das transações, no caso os mineradores, deverá mudar de um sistema de recompensas por bloco minerado, para um esquema baseado em taxas de transação. Atualmente, existem um pouco mais de 15 milhões de bitcoin em circulação.

“

**A Blockchain é a grande revolução tecnológica que faz do Bitcoin ser uma tecnologia única e disruptivo**

”




# COMO A CRIPTOGRAFIA EVITA VIOLAÇÕES NA REDE

Um dos segredos do bitcoin e da blockchain é a criptografia existente nas transações que são adicionadas ao livro-registro. Todo o sistema foi desenhado com base em um conjunto de regras pré-programadas com o objetivo de torná-lo à prova de violação.

Depois que um bloco de transações é verificado, os mineradores pegam todos os detalhes das transações contidas naquele bloco e aplicam uma fórmula matemática que transforma aqueles dados em algo que é conhecido como hash.

O hash é uma sequência aleatória de letras e números e seu grande valor está no fato de que é bastante fácil transformar qualquer tipo de informação (palavras, números, equações, detalhes de transações financeiras) em um hash, mas é praticamente impossível fazer o caminho inverso e transformar o hash nas informações originais.

Outra propriedade característica dos hashes é que se você mudar apenas um dos caracteres ele se transformará em um hash completamente diferente. Cada bloco da blockchain é um hash específico. O hash subsequente é atrelado ao hash anterior, e assim, sucessivamente, fazendo que o hash de um bloco sempre esteja atrelado àquele imediatamente anterior.

Assim, por exemplo, quando foi criado o primeiro bloco, ele serviu de base para o segundo hash, e este último, por sua vez, para o terceiro hash, e assim sucessivamente. Em outras palavras, o segundo bloco possui informações do primeiro. E o terceiro bloco possui informações do segundo.

Se algum bloco anterior for alterado de alguma maneira, os hashes resultantes estariam errados e blocos alterados poderiam ser instantaneamente identificados na rede como falsos ou desconsideráveis.

Parte do processo de mineração requer rodar a função do hash em toda blockchain e provar para mais de 50% de todos os mineradores que o bloco anterior não foi alterado. Isso faz com que o blockchain seja à prova de violação, ou à prova de qualquer tipo de ataque hacker.

Essa criptografia que acontece no âmago do Bitcoin é que o lhe confere a classificação de uma criptomoeda. Isso também evita que existam gastos duplos.

Assim, quando João envia bitcoins à Maria, os mineradores colocam essa transação no algorítmo do hash quando ela é adicionada à blockchain e a posse daquele bitcoin é transferida. Assim, João jamais poderá gastar aquele bitcoin novamente, porque mesmo que ele tentar os mineradores não irão aprovar a operação.

# A FILOSOFIA DO DINHEIRO

Uma das maiores críticas feitas ao bitcoin é que ele não é garantido por ninguém e que não possui valor intrínseco. A crítica vem aliada à argumentação de que as moedas tradicionais são sustentadas pelos governos e bancos centrais, mas os críticos geralmente esquecem que a imensa maioria das moedas não é confiável e estável.

Somente nas economias do mundo desenvolvido é que o papel moeda funciona como uma reserva de valor, uma unidade de conta e um meio de troca. Para algo ser classificado como dinheiro, ele precisa reter valor ao longo do tempo, ser um padrão de medida para o valor relativo das coisas e ser usado para comprar e vender produtos e serviços.

O dólar americano e o euro, por exemplo, possuem essas três características. Mas os países com moedas estáveis perfazem aproximadamente apenas 15% da população mundial. Isso faz com que a maioria do mundo precise de uma moeda em que possa confiar.

# BITCOIN, INFLAÇÃO E DEFLAÇÃO

Como um termômetro da saúde de uma moeda, as melhores economias do mundo apresentam índices de inflação anuais abaixo de 1,5%. Em termos econômicos, quanto mais perto de zero a inflação for, mais confiável é aquela moeda, pois ela não flutua significativamente. Mas em países cujas economias não são tão desenvolvidas, como na América Latina e África, por exemplo, a inflação chega facilmente a dois dígitos por ano, podendo atingir mais de 10 dígitos, como foi o caso do Zimbábue em 2008, quando este país sofreu com hiperinflação. A inflação corrói o poder de compra daquela moeda em comparação com moedas estáveis e faz com que a população busque por alternativas de reserva de valor para preservar sua riqueza.

As razões que levam um país a enfrentar inflação são diversas e variam de lugar para lugar. O mesmo acontece com a deflação, caso atualmente vivenciado pelo Japão, quando as pessoas preferem guardar o

dinheiro ao invés de gastá-lo, provocando um efeito dominó na economia, com queda dos preços, que segue com a perda de empregos e o fechamento de muitos negócios.

Dada a alta volatilidade do bitcoin, pode ser difícil entender como essa nova moeda da Internet pode atuar como um bom mecanismo de reserva de valor. Contudo, comparando a taxa de flutuação do preço do bitcoin com algumas moedas de países subdesenvolvidos, o bitcoin torna-se uma alternativa interessante para reservar valor.

Diferentemente das moedas tradicionais, e principalmente do dólar americano, o bitcoin não pode ser emitido ao bel prazer de uma entidade monetária. Ele segue as regras que estão escritas em seu protocolo e de maneira bastante transparente todos sabem quantos bitcoin estão em circulação e quantos entrarão ao longo do tempo. Assim, está totalmente descartada situações vistas recentemente, como quando o Banco Central dos Estados Unidos decidiu emitir trilhões e trilhões de dólares para incentivar sua economia durante a crise financeira de 2008, desvalorizando sua moeda. O mesmo se passou com a União Europía durante o período. A emissão de mais moeda faz com que o dinheiro depositado pelas milhões de pessoas nos bancos perca valor.

Além disso, países que possuem forte controle de capitais, como são os casos de China e Rússia, também são presa fácil para a tecnologia bitcoin, pois a partir do momento que você compra a moeda digital é possível enviá-la para qualquer parte do mundo em apenas alguns minutos.

# OURO DIGITAL

Assim como o ouro, o bitcoin possui um suprimento limitado. Ninguém pode produzir mais ouro no mundo do que aquele que atualmente existe. O bitcoin funciona da mesma forma. Assim como o ouro, ele é um ativo escasso e é impossível inflar seu suprimento artificialmente.

Para entendermos o que provê valor ao bitcoin, vamos primeiro analisar o que dá valor ao ouro. Este metal precioso tem sido usado por milhares de anos. Ele é raro, mas não tão raro a ponto de ninguém conseguir obtê-lo, ele é maleável e pode ser transformado em moedas, ele é durável o que lhe confere longevidade e é brilhante e lustroso, o que lhe faz um material perfeito para criação de joias. O ouro apenas possui valor porque os seres humanos ao longo do tempo agregaram valor a ele. Qualquer item econômico só possui valor porque as pessoas assim o deram.

O bitcoin é uma versão mais transportável que o ouro. Satoshi Nakamoto pegou as propriedades que fazem o ouro ter valor e as programou na forma do bitcoin, fazendo a moeda digital mais eficiente e fácil de usar que o ouro.

O ouro é pesado e não divisível, o que o torna difícil de carregar e impossível de gastá-lo em pequenas quantidades. O bitcoin é digital, não existe fisicamente, apenas na Internet, e possui o poder de ser infinitamente divisível. Ele não ocupa espaço em nenhum lugar, apenas na rede, e pode ser gasto em um montante de até oito casas decimais, o que o torna perfeito para realizar pequenas transações, que antes não eram possíveis.

# USANDO BITCOIN

Como é possível fazer micropagamentos com bitcoins, pense em centavos de dólar, por exemplo, para qualquer lugar do mundo, isso torna a moeda digital única no mundo atualmente. Uma operadora de cartão de crédito lhe cobraria muito para enviar 10 centavos de dólar para alguém nas Filipinas, por exemplo. Com o bitcoin, isso é possível a um custo extremamente baixo.

Com micropagamentos será possível otimizar a monetização de conteúdo na Internet, eliminar a necessidade dos banners de anúncios e as chatas telas de pop-up que surgem quando entramos em algum site. Os usuários poderão pagar parcelas muito pequenas conforme eles forem consumindo conteúdo na Internet, como leitura de notícias ou ao assistir vídeos em streaming.

Existem várias maneiras de se obter bitcoin. A primeira delas, já explicada neste texto, é realizando o processo de mineração. Contudo, este é um processo complexo, que exige grande conhecimento do assunto e até mesmo poder de escala, para tornar a operação sustentável.

Outra maneira é utilizar as corretoras de bitcoin, como a coinBR, transferir dinheiro de sua conta bancária para a corretora e comprar bitcoins. Para quem não possui conta em banco, também é possível adquirir bitcoins por meio de um caixa-eletrônico de bitcoin. Outra maneira é convencer seu empregador a lhe pagar em bitcoin ou fazer serviços pela Internet que ofereçam pagamento na moeda digital.

Considerando todos os casos de uso da moeda digital, a grande quantidade de telefones celulares no mundo, e os bilhões de pessoas que estão alijados ao sistema financeiro global, o bitcoin torna-se um importante ativo porque ele serve de propósito e provê soluções para problemas existentes.

# CONCLUSÃO

O bitcoin está apenas em seu começo. A cada dia mais e mais pessoas conhecem a tecnologia e começam a transacionar utilizando a moeda digital, que redefine o conceito do dinheiro e elimina intermediários.

Atualmente, os casos de uso de maior sucesso ajudam aqueles que são desbancarizados, ou os que precisam enviar dinheiro de um país a outro, sem contar a possibilidade de realizar micropagamentos, de forma segura e transparente. Como ativo, o bitcoin também pode ser uma boa opção de investimento, como discutimos neste outro artigo.

Além da moeda digital em si, é importante notar que a tecnologia do blockchain poderá ser utilizada para uma infinidade de outras aplicações. Como cada transação de bitcoin pode ter uma mensagem anexada, será possível fazer registros de praticamente tudo na blockchain utilizando uma transação de uma pequena fração de bitcoin. Algumas pessoas já registraram o nascimento de seus filhos na blockchain e espera-se que muito em breve possamos registrar a compra e a venda de nossas casas, carros ou de qualquer outros itens.

Por ser uma tecnologia nova, comparável à Internet no início dos anos 90, ainda é impossível imaginar quais serão as grandes revoluções provocadas tanto pelo bitcoin quanto pela blockchain. Mas é certo que esta revolução já começou e seus primeiros resultados começam a aparecer.

O dinheiro da Internet chegou para ficar, para sempre.