OS IDIOTAS DO BITCOIN

20 dúvidas legítimas respondidas em 30 minutos, pela primeira vez em uma linguagem acessível

Dennis Zasnicoff

OS IDIOTAS DO BITCOIN

20 dúvidas legítimas respondidas
em 30 minutos, pela primeira vez
em uma linguagem acessível

por Dennis Zasnicoff

Primeira edição, v1.1, Outubro de 2018

zasnicoff.com - Treinamento e Consultoria

criptobomba.com - Verdades in(Convenientes) - Acompanhe criptoBomba para vídeos e discussões sobre Bitcoin, Blockchain e o Universo Cripto.

Capa: Dennis Zasnicoff

Foto: Satoko Nakamoshi

Aos amigos Marco e Viviane Chamsin, Carlos Alberto Sacco e Marcos Pesce Bueno de Castro, pelas conversas, inspirações, dicas, revisões e o grande apoio. À minha mãe, pelo exemplo de conduta contagiante. Ao meu pai, por me despertar a curiosidade e a busca constante pelo conhecimento. Às minhas queridas irmãs, por serem provas da importância de uma família unida. A você, minha amada, por ser a parceira incondicional. Ao meu filho, por ser fonte essencial de amor, virtude e verdade. Sou privilegiado por tê-los em minha vida, muito obrigado!

Índice

Prefácio

por Carlos Alberto Sacco

Nos últimos 18 meses, a grande mídia começou a dar destaque ao Bitcoin, cujo valor ultrapassou a barreira dos US$ 1.000 em janeiro de 2017, chegando ao seu pico em dezembro de 2017, atingindo pouco mais de US$ 19.000. Uma valorização de quase 2.000%. Sim, dois mil por cento!

Bolha ou não bolha, polêmica inevitável, o fato é que economistas e outros formadores de opinião abordam cada vez mais o tema Bitcoin, com visões bem diferentes, influenciando cada vez mais pessoas que se deixam levar por opiniões sem necessariamente compreender a verdade sobre o Bitcoin.

Aí está um grande perigo que este livro vem alertar: quais são as verdadeiras intenções por trás de quem tenta explicar ou vender Bitcoins? Pensar que se compreende o Bitcoin não é suficiente para vivenciá-lo. Bitcoin é mais do que suposições ou conceitos baseados em economia e finanças.

A primeira vez que ouvi falar sobre o tema Bitcoin/Blockchain foi em 2015, quando em um auditório com mais de 2000 pessoas o palestrante perguntou quantas pessoas já tinham ouvido falar em Blockchain. Não mais do que 5 pessoas levantaram timidamente as mãos. A partir desse evento, meu interesse por esse tema aumentou e hoje, não tenho dúvidas de que as criptomoedas serão o nosso futuro, talvez mais breve do que possamos imaginar.

Conheço o Dennis há mais de duas décadas, quando ele ainda cursava engenharia na USP. Eram frequentes os nossos encontros em finais de semana, quando Dennis juntava amigos em sua casa para cantar e tocar vários instrumentos e conversar sobre assuntos realmente interessantes. Saudade dessa turminha!

Pude acompanhar sua evolução profissional por estarmos na mesma área de Tecnologia da Informação. Não raro, o encontrava em eventos onde era um dos palestrantes, sempre abordando, com ousadia e perspicácia, temas ligados à tendências e inovações nas áreas de hardware e software. Aliás, ousadia, franqueza, clareza de propósito são as marcas registradas do Dennis, o que não é diferente neste livro.

Atualmente, muitos eventos têm ocorrido para abordar e tentar explicar o Bitcoin, com as mais diversas intenções e formas. No entanto, raros são os palestrantes que conseguem sair do economês, do sensacionalismo, da estratégia de instaurar o medo ou mesmo deixar de confundir ainda mais as pessoas curiosas ou realmente interessadas em estudar o assunto.

Lembrando que antes de tudo, o Bitcoin é um software – um programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, que permeia nossas vidas desde quando acordamos, passando por informar o melhor caminho para o trabalho, e até solicitando um carro para nos levar ao cinema.

Quando tive a grata surpresa de reencontrar o Dennis, no Natal de 2017, me dei conta da profundidade de conhecimento que ele adquiriu sobre o Blockchain e criptomoedas. Afinal, ele é um apaixonado por esse assunto desde 2010, quando o Bitcoin ainda era um ilustre desconhecido para a maioria de nós.

Ter sido convidado para fazer este prefácio foi uma grande honra e satisfação.

Não tenha dúvida quanto aos inúmeros benefícios que você terá em ler este livro. E tenha a certeza de que, ao final da leitura, sua visão sobre Bitcoin nunca mais será a mesma.

Boa leitura!

Carlos Alberto Sacco

(Empresário, mentor de startups, sócio fundador da ABES Associação Brasileira das Empresas de Software, da qual foi presidente (1991 a 1997) e é, atualmente, diretor de marketing)

Apresentação

Não é fácil entender Bitcoin

Bitcoin não é apenas uma moeda - ou tudo o que se pode fazer com uma moeda, como câmbio, remessas, pagamentos e investimentos - é também uma nova maneira de se estabelecer confiança entre as partes, um modelo descentralizado sem controle central ou intermediários. Bitcoin viabiliza uma liberdade nunca antes experimentada, mas pode acabar pagando caro quem se aventurar sem ter o mínimo de conhecimento. Com razão, o grande público ainda tem desconfianças, medo e até repúdio.

Bitcoin será algo natural para seus netos. E quando chegar esse dia, talvez nem se chame mais Bitcoin. Hoje, Bitcoin é uma cripto-moeda, mas pode se tornar muito mais, porque é precursor de ideias e experimentos que estão transformando profundamente a sociedade.

Não é fácil explicar Bitcoin

Livros extensos foram escritos sobre o tema. Mas quem tem disposição para estudar 150 páginas de conceitos complexos, diferentes de tudo a que estamos acostumados no dia a dia? Para complicar, uma legião de idiotas contribui todos os dias para deixar o assunto ainda mais distorcido, disseminando ilusões e falsas expectativas.

Após estudar Bitcoin por muitos anos, eu ensaiei discursos de cinco minutos para tentar introduzir o assunto aos amigos. Não funcionou. Desenhei palestras de vinte minutos para pequenos grupos… mal conseguimos tocar a superfície. E então compreendi que, quando se trata de Bitcoin, quase tudo é novidade. Eu estava errando na linguagem e no nível de profundidade. Não vamos complicar o que não precisa ser complicado!

Nos anos 90, a Internet também era um conceito difícil de entender. Ninguém poderia imaginar o que viria a acontecer 25 anos depois. Em questão de poucos anos, grandes corporações surgiram - e desapareceram com a mesma velocidade. Durante os primeiros anos, a única utilidade da Internet para a maioria da população era o e-mail. Aos poucos, a Internet passou a fazer parte do cotidiano, nos auxiliando em diversas outras atividades.

Vivemos uma época semelhante, onde os benefícios que o Bitcoin oferece ainda não são muito claros. Você pode esperar pela revolução, ou se antecipar desde já para tirar proveito dessas novas possibilidades. É um bom momento para se aprender os conceitos básicos, não ser manipulado por idiotas, muito menos acreditar nos absurdos que escutamos todos os dias.

Sobre este pequeno livro

Minha missão aqui é tentar explicar o que é Bitcoin, para quê serve e como funciona. Em uma linguagem objetiva, vamos atacar diretamente as dúvidas mais ingênuas, derrubando mitos, distorções e equívocos que os idiotas insistem em propagar.

Há muitos anos, quando o assunto da vez era a Internet, obviamente ainda não existia a Internet para se fazer marketing abusivo e espalhar boatos. Naquele momento, idiotas não tinham tantos seguidores, redes sociais ou alcance para se passarem por especialistas. Agora o cenário é bem diferente. Qualquer pessoa tem o potencial de criar uma aura de autoridade para influenciar milhões de inocentes. As consequências podem ser perigosas.

Nestes últimos anos, aprendi a identificar os idiotas dos quais temos que nos afastar, mas também conheci muitos especialistas no assunto. Uma coisa ficou muito clara: aqueles que realmente entendem Bitcoin são absolutamente fascinado pelo tema. Meu objetivo é que você seja mais um.

Ao final dessa leitura

Não tenho a expectativa que você aprenda a ganhar dinheiro com Bitcoin, porque eu estaria sendo apenas mais um idiota. Mas você poderá deixar de perder dinheiro, algo que infelizmente acontece todos os dias com quem ainda não entendeu os conceitos básicos.

Você compreenderá como o Bitcoin, mais cedo ou mais tarde, impactará sua vida pessoal e profissional. Talvez você encontre, desde já, uma forma de adaptar seu trabalho para se manter competitivo no futuro. Talvez perceba que seu emprego estará ameaçado em poucos anos. Poderá ter ideias de negócios que nunca tenha pensado antes. Ou deseje se aprofundar nos estudos, para investir ou tornar-se um empreendedor de cripto-moedas, consciente dos riscos reais.

Este livro não foi escrito para programadores ou economistas, embora a maioria deles ainda não tenha o mínimo de conhecimento que deveria ter sobre Bitcoin. Nem tudo pode ficar claro na primeira leitura. Absorva aos poucos e tenha em mente que algumas das questões que surgirem ao longo do caminho poderão ser respondidas até o final do livro. Continue lendo, releia, anote e compartilhe comigo as dúvidas que eventualmente permanecerem.

Bem-vindo ao fascinante mundo do Bitcoin

Meu primeiro contato com Bitcoin se deu em meados de 2010. Na ocasião, achei a ideia interessante, mas não fiquei fascinado. Nos meses seguintes, comecei a estudar a fundo e descobri tecnologias que eram totalmente novas para mim, apesar de eu ter trabalhado por mais de dez anos com Tecnologia da Informação. Entre elas: blockchain, proof-of-work e merkle-tree. Tarde demais, eu estava fisgado.

Mas reconheço que ninguém precisa estudar essas tecnologias para entender Bitcoin. É exatamente aí onde muitos livros se enganam. Quem utiliza a Internet não precisa necessariamente aprender conceitos técnicos como TCP/IP ou Certificados Digitais. O que importa é entender o que essas tecnologias trazem de fato para o nosso dia a dia. São fáceis de usar? Como podem melhorar nossas vidas?

Os conceitos fundamentais do Bitcoin - que mudarão o nosso comportamento e a maneira como fazemos transações - são descritos por palavras que já conhecemos: descentralização, consenso, segurança, privacidade, liberdade, imutabilidade, livro-caixa. Bitcoin traz à tona todos esses temas e é neles que devemos nos concentrar para aprender Bitcoin.

Bitcoin será o foco deste texto porque é a primeira aplicação destes conceitos em larga escala, de uma forma integrada, palpável, com utilidades reais e benefícios imediatos. Mas tudo o que você aprender aqui também será útil para compreender outros bens virtuais e aplicações dos mesmos conceitos.

Bitcoin é um experimento que deu certo. Já provou que podemos fazer transações mais rápidas, com segurança e privacidade, sem confiar em terceiros ou pagar taxas abusivas. Como todo experimento, no entanto, Bitcoin pode "quebrar" a qualquer momento. E ainda que isso aconteça, já teremos aprendido lições importantes e irreversíveis.

Bitcoin é um processo dinâmico, desafiado a todo instante, melhorado dia após dia. Uma verdadeira batalha entre o Bem e o Mal onde cabeças brilhantes de um lado atacam, de outro protegem. Passados nove anos, hoje podemos afirmar: o Bem venceu.

Alerta sobre os idiotas

Antes que alguém inocente se sinta ofendido, uma diferença importante: não vamos confundir idiotas com ignorantes. Todos nós nascemos ignorantes e provavelmente vamos morrer ignorantes sobre quase todos os fenômenos que permeiam nossa existência. Não há vergonha alguma em desconhecer sobre um assunto, a menos que você decida ser um idiota.

As vinte dúvidas aqui selecionadas são naturais para qualquer pessoa que nunca teve contato com Bitcoin. O problema é que muitas dessas questões ganharam uma dimensão exagerada, propagando-se como verdades que raramente são confrontadas.

Idiotas têm uma capacidade incrível de aumentar boatos, criar falsos perigos, ignorar perigos reais, vender lucros, seduzir ignorantes, roubar dinheiro de inocentes, cometer crimes, fazer profecias e colecionar seguidores. Quase sempre com má intenção, outras vezes porque simplesmente não têm a menor ideia do que estão dizendo. Mas como são populares (e vale dizer que a culpa aqui não é deles), acabam influenciando seus alvos.

Este livro pode perturbar muita gente. Meu objetivo é transferir conhecimento, mas sei que alguns se ofenderão, porque é isso o que acontece quando idiotas são desmascarados. Na posição de palestrante e consultor, todos os dias sou abordado por idiotas que, na verdade, pensam que o idiota sou eu. Dizem que conhecem investidores e clientes para um negócio fantástico com Bitcoin, embora nunca saibam explicar qual é o negócio ou como criá-lo. Não querem trabalhar, não querem estudar, mas estão certos que podem ganhar muito dinheiro com as comissões dos lucros que conseguirão para seus clientes. O meu papel nesse negócio infalível, claro, seria "apenas“ entrar com o conhecimento.

Do dicionário Michaelis da Língua Portuguesa:

idiota

i·di·o·ta

adj m + f sm + f

1. Diz-se de ou o que demonstra falta de inteligência, de discernimento ou de bom senso; estúpido, imbecil, tanso, tantã, tolo, zote.

2.Diz-se de ou pessoa que se considera superior aos outros; arrogante, presunçoso.

3.Diz-se de ou o que é tolo ou ingênuo.

4.[Med] Diz-se de ou pessoa que sofre de idiotia.

adj

Que não desperta interesse ou que não tem valor; raca.

A receita para se tornar um idiota é simples:

- Tome proveito da existência de um assunto novo que ainda é pouco compreendido. É sua chance de aparecer!
- Quando perceber que domninar esse assunto requer muito mais dedicação e capacidade do que você tem, recorra a outros conhecimentos que você possui para se convencer de que já entendeu.
- Agora só falta convencer o mundo, o que não deve ser difícil, já que muitos querem aprender a mesma coisa e estão desesperados atrás de "experts" como você.

O problema aqui não é querer aparecer. Aparecer é necessário - e até louvável - por aqueles que vivem buscando ídolos e gurus. O mundo precisa de “masterminds”, pena que muitos deles sejam idiotas. Porém, assumir que tudo o que você já sabe (ou acha que sabe) é suficiente para explicar qualquer assunto novo, é a melhor receita para se tornar um idiota.

Há momentos na história da humanidade em que boa parte do que se aprendeu até então deve ser jogada no lixo, não serve mais. Estamos nesse momento, o cenário é perfeito para a multiplicação de idiotas: uma NOVIDADE, COMPLICADA e INTERESSANTE.

Quem são os idiotas?

Um idiota do Bitcoin normalmente está disfarçado de:

- Economista
- Deputado
- Advogado
- Empreendedor
- Banqueiro

- Lobista
- Jornalista
- Personalidade da Internet
- Marketeiro Digital (esses me dão arrepios)

Um verdadeiro conhecedor (infelizmente muitas vezes um péssimo professor) é quase sempre um:

- Engenheiro
- Programador
- Acadêmico
- Cientista

É fácil identificar um idiota. Eles são sensuais. Na internet, filmam seus vídeos na frente de carros esportivos. Na mídia, usam termos técnicos e complicados. Em fóruns e discussões, respondem qualquer pergunta da mesma forma ensaiada, ou fogem completamente da questão para fazer uma dissertação extensa sobre outro conceito técnico que entendam. Como homens de negócio, usam adereços exagerados, exibem o quanto supostamente faturaram na última semana, estão sempre sorrindo e possuem solução para tudo. Fazem promessas, negam os fatos, desafiam a física, a matemática e a razão, querem tomar o controle de qualquer situação, derrubam qualquer ideia que não seja deles e, acima de tudo, não escutam. Só querem falar, falar e falar.

Você deve conhecer alguém assim. E provavelmente vai se deparar com muitos outros, sempre que o assunto for Bitcoin. Ignore-os, idiotas não querem discutir, não querem aprender. Eu não perco mais tempo com eles, desenvolvi a habilidade de simplesmente me levantar para pegar um café e sumir de cena para nunca mais voltar.

Use o conhecimento que adquirir aqui para tomar suas próprias decisões. Encontre fontes seguras de informação e continue estudando, porque tudo ainda é muito novo e vai evoluir rapidamente nos próximos anos. Nem mesmo os especialistas sabem como será o futuro, ou o que acontecerá com o Bitcoin. Quem nega essa verdade já é, automaticamente, um idiota.

As explicações a seguir, por serem intencionalmente práticas e superficiais, podem ser consideradas dúbias ou incompletas. Alguns idiotas tentarão diminuir o valor desse texto. Eles não querem contribuir, querem desacreditar qualquer fonte que prove que eles são idiotas.

O genial criador do Bitcoin, através do documento original publicado em 2008, deixou de prever alguns dos problemas que hoje são conhecidos e que só puderam ser confirmados na prática. Quem, portanto, poderá se dizer infalível ou total conhecedor do assunto? Certamente não eu. Se você encontrar alguma falha, contribua, comunique, e assim teremos um texto cada vez mais útil aos leitores.

Antes de prosseguir, leia, releia e procure entender

- Bitcoin é uma moeda virtual (não palpável), uma cripto-moeda, moeda digital, ou moeda eletrônica;
- Bitcoin é também um sistema de pagamento, um conjunto de regras e um “banco”;
- Bitcoin, sendo uma moeda, pode ser utilizado como meio de pagamento, investimento, reserva de valor ou remessa, entre outras utilidades;
- Bitcoin, como investimento, hoje é considerado de alto risco, oferecendo potencial de grandes lucros e grandes perdas em curtos períodos de tempo;
- Bitcoin não é um projeto para o futuro, já existe e e está sendo utilizado no mundo inteiro, neste exato momento;
- Bitcoin não é 100% seguro, bancos não são 100% seguros, ouro não é 100% seguro, dólar não é 100% seguro.
- Bitcoin não é controlado por nenhuma pessoa ou entidade;
- Bitcoin já pode ser considerado maduro do ponto de vista de desenvolvimento, tempo de vida, comunidade e ecossistema, embora ainda esteja longe de ter uma interface amigável, intuitiva ou fácil de usar;
- Bitcoin, nesse momento, exige um mínimo de estudo e prática para ser utilizado com segurança e agilidade;
- Bitcoin se pronuncia bit + coin, e não bit + com, como muitos insistem em dizer no Brazil, por razões que eu ainda não entendi claramente.

Na sequência, vamos responder, uma por uma, as dúvidas recorrentes que tenho encontrado em fóruns, palestras, treinamentos, convenções, restaurantes e mictórios. Se todo mundo tem o direito legítimo de ter dúvidas, tem também a responsabilidade de entendê-las antes de propagar boatos.

Dúvidas respondidas

1. Bitcoin não é seguro, porque não tem lastro.
2. Quem controla os bitcoins?
3. Bitcoin é uma bolha.
4. Como adquirir bitcoins?
5. Em algum momento vou ser hackeado.
6. O valor do Bitcoin é fictício.
7. O que eu posso fazer com meus bitcoins?
8. Quem determina o preço de um bitcoin?
9. Bitcoin é usado para comprar armas e drogas na DeepNet.
10. Bitcoin é um esquema de pirâmide.
11. Meu celular contém bitcoins e pode ser roubado.
12. Bitcoin é ilegal.
13. Bitcoin pode desaparecer amanhã.
14. Não bastasse o Bitcoin, agora tem o tal do Blockchain.
15. Eu deveria ter comprado bitcoins em 2011.
16. Meu vizinho está minerando bitcoins na garagem, vou avisar a polícia.
17. Eu não acredito nisso aí.
18. Se a NSA é hackeada, Bitcoin também pode ser hackeado.
19. Bitcoin é usado para lavar dinheiro.
20. Minerar é a forma mais segura de se ganhar dinheiro com Bitcoin.

1. Bitcoin não é seguro, porque não tem lastro

Essa começou com um idiota economista e se espalhou rapidamente.

“Lastro”, aqui, significa um bem real, que esteja atrelado ao bem virtual, como forma de garantia e geração de valor.

Bitcoin não tem lastro.

Assim como quase toda moeda no mundo, seja de um banco central ou não.

Moedas não precisam de lastro para possuir valor.

Moedas já não dependem de lastros há muito tempo.

Quem diz essa frase na verdade queria dizer:

“Bitcoin não tem garantias, não tem valor real, não pode se sustentar”.

Nada disso é verdade.

O valor do Bitcoin vem da oferta e da demanda.

O valor de quase tudo vem da oferta e da demanda.

Bitcoin não é diferente nesse sentido.

Um poster assinado por Elvis Presley tem valor para muita gente, porque existem poucos no mundo.

Se Elvis tivesse assinado 50 bilhões de cópias desse mesmo poster, posso garantir que eles seriam usados para limpar as nossas bundas.

Ouro tem valor porque é escasso.

Ouro tem valor porque tem utilidade para as pessoas.

Ouro é amplamente aceito no mundo porque tem valor e utilidade.

Ouro tem valor porque tem utilidade e é aceito.

(fique à vontade para continuar a brincadeira)

E tudo isso é verdade.

E mais:

Ouro pode ser usado como uma moeda de troca.

Ouro pode ser usado como um investimento.

Ouro pode ser usado para armazenar - ou imobilizar - valor.

Bitcoin compartilha dessas mesmas características.

O valor de uma moeda está relacionado a sua escassez.
O valor de uma moeda está relacionado a sua utilidade.
O valor de uma moeda está relacionado a sua aceitação.
O valor de uma moeda está relacionado a sua oferta.
O valor de uma moeda está relacionado a sua demanda.
E tudo isso está relacionado entre si.

O valor da moeda, em última instância, é determinado por forças naturais de mercado.
Ninguém isoladamente determina o preço do ouro, ou o preço de um bitcoin.

Sim, Bitcoin tem valor.
Não se iluda.
Neste exato momento, existem pessoas dispostas a pagar milhares de dólares por um bitcoin.
Essa já é uma prova.

Quanto mais as pessoas compreenderem sobre Bitcoin, mais valor deverá ter o Bitcoin.
Porque entenderão que ele tem escassez.
Porque entenderão que ele tem utilidades.
Porque entenderão que ele é cada vez mais aceito no mundo como moeda de troca.

A falta de lastro do Bitcoin não é uma falha.
É intencional.

2. Quem controla os bitcoins?

Essa questão revela um comportamento condicionado do cidadão: controle, governo, ordem, policiamento, hierarquia. Tire o controle de uma instituição e tendemos a nos sentir perdidos e inseguros.

Vamos traduzir “controle”:

Quem emite os bitcoins?

Quem fiscaliza as transações?

Quem protege as contas dos usuários?

Quem define as regras?

Agora vamos entender (ou pelo menos aceitar) que é perfeitamente possível existir controle - fiscalização, segurança e normas - de uma maneira descentralizada.

Aqui está um dos conceitos mais difíceis de absorver.

Aqui está o conceito que causará a grande revolução dos próximos anos:

Descentralização.

Toda a ideia do Bitcoin partiu deste princípio.

É causa, não é consequência.

Com o objetivo de criar uma moeda sem controle central.

Porque um controle central é perigoso.

Pode ser manipulado, influenciado, atacado e subornado.

Pode agir em seus próprios interesses.

Porque tem grande poder.

Bitcoin é controlado pelos seus usuários.

Todo novo usuário pode (e deve) auxiliar no controle, fiscalizar e melhorar a segurança.

E para tanto, não precisa necessariamente aprender como fazer.

Basta seguir as mesmas normas, usar o mesmo software.

Que por sua vez é controlado pelos mesmos usuários.

Que por sua vez possuem interesses e incentivos para manterem a ordem e a segurança.

A maioria manda.

A maioria vence.

Bitcoin possui um protocolo.

Um conjunto de regras que devem ser seguidas.

Regras impostas pelo software.

Regras que controlam a emissão de moedas.

Regras que controlam o acesso às moedas.

Regras que fiscalizam e validam as transações.

Portanto é o software quem controla o Bitcoin.

Um software que funciona por consenso, está distribuído e descentralizado.

Boa sorte ao tentar manipular, influenciar, atacar ou subornar milhares (ou milhões) de usuários.

Há incentivos para os usuários bem comportados.

Afinal, suas próprias moedas estão em jogo.

Há enormes obstáculos para usuários mal intencionados.

Na prática, é difícil burlar o sistema.

Estatisticamente improvável.

Há mais de nove anos, Bitcoin vem sofrendo ataques a todo segundo, de mentes brilhantes, por todos os lados, tendo sobrevivido muito bem, obrigado.

3. Bitcoin é uma bolha

Uma das preferidas dos idiotas e seus seguidores.

Bolha sugere algo que cresce descontroladamente, sem sustentação.

Algo que piora com o tempo, até explodir.

Bitcoin, ao contrário, melhora com o tempo.

Será tão difícil considerar que o preço do bitcoin tem aumentado simplesmente porque seu valor tem crescido?

Difícil acreditar que esse valor é real?

Incertezas? Sim.

Grandes flutuações? Totalmente esperadas.

100% seguro? Nunca.

Incertezas e flutuações acontecem todos os dias nas bolsas de valores.

Mas ninguém diz que uma empresa é uma bolha simplesmente porque se valorizou tanto em pouco tempo.

Só os idiotas.

Que fique bem claro:

TUDO pode acontecer amanhã e NINGUÉM sabe o que vai acontecer.

Mas não há nada que enquadre o Bitcoin como um fenômeno de bolha.

Se as pessoas compreendessem mais sobre Bitcoin, provavelmente seu valor nesse momento seria ainda maior.

E mais estável.

Porém…

É fato que muitas outras moedas virtuais estão pegando carona no Bitcoin.

Nem todas poderão se sustentar.

Muitas devem desaparecer em pouco tempo.

Nesse sentido, pode-se dizer que existe uma bolha no mercado.

Uma euforia em torno de moedas digitais e tudo o que elas representam.

Cuidado para separar o joio do trigo.

Desconfie de tudo que é novo, que não tem histórico ou volume de usuários.

Nem tudo que é “cripto" é confiável.

Nem tudo que é “blockchain" é seguro.

Idiotas se aproveitam dessas palavras para vender produtos e serviços de péssima qualidade.

E criam bolhas que estouram todos os dias.

4. Como adquirir bitcoins?

Como adquirir ouro? O que fazer para conseguir francos suíços ou dólares canadenses?

Algumas possibilidades:

- Vender um bem ou um serviço por dólares canadenses.
- Comprar ouro em uma loja de penhora.
- Receber uma doação de um tio milionário.
- Fazer uma operação em uma casa de câmbio, utilizando a moeda local.
- Utilizar um cartão de crédito em um caixa eletrônico.
- Receber o salário em francos suíços.

Para possuir bitcoins, basta você criar gratuitamente uma conta e começar a receber bitcoins em troca de bens, serviços, trabalho, outras moedas virtuais, moedas físicas, cheques, cartão de débito etc.

Qualquer usuário que tenha uma conta com bitcoins poderá transferí-los para qualquer outra conta.

Se a conta de destino é de uma corretora, ela aceitará bitcoins em troca de moeda local.

Se a conta de origem é de uma corretora, ela aceitará moeda local em troca de bitcoins.

Qualquer que seja a outra parte, vocês podem combinar uma transação onde uma das partes enviará bitcoins e, em troca, receberá outro bem: moeda local, serviço, produto, ouro, automóvel, imóvel etc.

Repare que você não precisa necessariamente “comprar” bitcoins.

As corretoras operam como casas de câmbio em suas moedas locais.

Você pode comprar bitcoins através delas.

Mas nada impede que você pague diretamente alguém em dinheiro, ou qualquer outro bem, em troca de bitcoins, sem passar por uma corretora.

Quando a Amazon eventualmente começar a aceitar Bitcoin, você poderá transferir bitcoins para uma conta da Amazon e receber a mercadoria em sua casa, da mesma forma que acontece hoje com seu cartão de crédito.

A Amazon, por sua vez, poderá usar os bitcoins para pagar seus fornecedores e prestadores de serviço.

E assim a moeda estará em circulação, movimentando a economia.

Conforme o tempo passa, mais estabelecimentos e pessoas físicas deverão aceitar bitcoins em troca de produtos e serviços.

Bitcoin é uma moeda de troca e tem valor real.

Funciona como dinheiro no seu bolso.

Tem valor ao portador, com a diferença de ser virtual.

Daí a existência de uma “chave” - ou “senha” - que garante que os bitcoins só possam ser gastos por quem possuir a chave correspondente.

5. Em algum momento vou ser hackeado

Se você não cuidar de suas chaves, provavelmente sim.

A descentralização tirou o poder de um controle central (exemplo: banco) e o colocou nas mãos do usuário.

Com o poder, vem a responsabilidade.

Se o usuário não for responsável, vai ser roubado.

Merecidamente.

Bitcoin exige uma mudança de comportamento.

Mais uma vez:

Bitcoin exige uma mudança de comportamento.

A menos que você tenha certeza do contrário, assuma que seu computador está infectado com vírus.

Ele provavelmente está.

Lembre-se que seu celular está o tempo todo conectado à Internet.

E celulares insistem em mergulhar em vasos sanitários todos os dias.

A todo momento, mentes inteligentes estão buscando oportunidades para roubar bitcoins.

Paranóia?

Talvez.

Se você está acostumado - e sente-se à vontade - para ligar no SAC do banco e abrir uma disputa toda vez que seu cartão de crédito é clonado, então Bitcoin ainda não é para você.

Se você perde suas senhas com facilidade e está sempre clicando no link “esqueci minha senha”, Bitcoin ainda não é para você.

Se você utiliza a mesma senha para tudo, insiste em arriscar com “123456”, data de aniversário ou nome do cachorrinho e não está muito preocupado se alguém acessar seus e-mails ou fotos íntimas, então Bitcoin ainda não é para você.

Mas se você está disposto a tomar outra postura em relação à sua segurança e privacidade, então Bitcoin pode ser para você.

Bitcoin não tem telefone de SAC.

Bitcoin não tem link “esqueci minha senha”.

Bitcoin não tem disputa litigiosa.

Perdeu, perdeu.

Para sempre.

Estamos falando das chaves de segurança que controlam os bitcoins.

As senhas.

São elas que devem ser protegidas.

Os bitcoins não ficam armazenados no seu celular ou no seu computador.

Bitcoins ficam armazenados em um local virtual (blockchain), seguro e confiável, desde que você proteja as chaves de acesso.

Muitos usuários criam ou armazenam suas chaves em dispositivos que podem ser facilmente hackeados.

Aí está o grande perigo.

Não é um problema do Bitcoin.

É um problema de usuário.

Na dúvida, crie suas chaves em um dispositivo apropriado.

Armazene-as com segurança (vide Apêndice I - Wallets).

Hackers sempre buscam oportunidades de menor esforço.

Roubar bitcoins diretamente na fonte requer um esforço virtualmente impossível.

Não acontece na prática.

Mas roubar chaves de usuários desprotegidos é como roubar doce de criança.

De novo:

Não é uma falha do Bitcoin.

É uma falha do usuário.

Como usuário, você influencia na percepção e no valor do Bitcoin.

Se você é roubado e isso acaba gerando pânico, todo o ecossistema é afetado.

Seja responsável.

Os casos mais impactantes acontecem quando corretoras são hackeadas e muitos bitcoins são roubados.

Pânico geral.

Quedas de valor.

Todo mundo se prejudica.

Não é falha do Bitcoin.

É falha da corretora que não soube proteger as chaves.

A lição:

Quem mandou deixar suas chaves em poder de um terceiro (corretora)?

A ideia não era justamente tirar o controle (e a vulnerabilidade) de uma entidade central?

Se você usar uma corretora para comprar bitcoins, transfira-os de volta para uma conta SUA assim que possível - uma conta cuja chave esteja somente em seu poder.

Não deixe suas moedas ao acaso do destino, em uma conta controlada pela corretora.

Suas chaves são suas!

Sempre sob seu controle

Compartilhadas com ninguém.

Delegadas a ninguém.

6. O valor do Bitcoin é fictício

Se ainda não ficou claro:

O valor do Bitcoin é o valor que ele tem como bem de troca por outros bens, serviços ou moedas.

Se o mercado aceita um bitcoin em troca de uma banana, ele vale o preço equivalente de uma banana.

Se o mercado aceita um bitcoin em troca de uma casa de R$200.000, então ele vale R$200.000

Em outras palavras:

O valor de um bitcoin é o valor que as pessoas estão dispostas a pagar por ele.

Onde está a ficção nisso?

Estamos acostumados a usar índices econômicos para entender o valor de moedas:

- Bolsas de valores
- Taxas de câmbio
- Produto Interno Bruto
- Dívida Externa
- Déficit Primário

Bitcoin não é uma moeda nacional.

Não tem banco central.

Não está atrelada diretamente a nenhuma economia, de nenhum país.

Mas tem valor real, determinado por oferta e demanda.

Precisamos começar a pensar diferente.

Ninguém precisa converter bitcoins em outra moeda para realizar o seu valor.

O valor já está ali.

A comparação com outras moedas serve apenas para mensurar o valor em um índice que já conhecemos.

Para que você possa, por exemplo, comprar bitcoins com reais ou vender bitcoins por reais.

Talvez porque o Real seja mais estável como investimento.

Talvez porque você precise de reais para fazer outras transações.

São apenas trocas.

A forma mais antiga e natural de se fazer transações.

Com o tempo, cada vez mais as transações deverão ser realizadas puramente em bitcoins.

Sem conversão.

Sem câmbio.

E passaremos a mensurar os preços de bens e serviços em bitcoins.

Não em dólares.

Nem em reais.

7. O que eu posso fazer com meus bitcoins?

Bitcoin é uma moeda de troca.

É também um bem escasso.

Um sistema de pagamento.

Um conjunto de normas.

E um “banco”.

Portanto, pode ser usado para:

- Comprar bens e serviços;
- Trocar por outras moedas (reais ou virtuais);
- Pagar salários de funcionários;
- Investimentos;
- Remessas internacionais;
- …e tudo aquilo que podemos fazer com qualquer outra moeda.

A propósito, ”Bitcoin" pode significar várias coisas: a rede de usuários, o conjunto de normas, o software.

Normalmente, as pessoas se referem à moeda propriamente dita.

Mas Bitcoin possui outros elementos, para não depender do mundo real externo.

Durante os próximos anos, Bitcoin vai precisar interagir com o mundo externo.

Com outras moedas.

Com corretoras.

Porque nem todo mundo aceita Bitcoin.

Porque bitcoins precisam ser convertidos em outras moedas para o pagamento de alguns bens e serviços.

Porque investidores querem realizar seus lucros em outras moedas, mais úteis e estáveis.

No futuro, nada impede que tudo funcione virtualmente.

Lojas de automóveis começarão a aceitar Bitcoin.

E depois disso, automóveis terão uma representação virtual, tão segura quanto um bitcoin - imutável, confiável, transferível, descentralizada.

Títulos de automóveis poderão ser transacionados digitalmente.

Então as lojas já não farão mais sentido.

Automóveis poderão ser vendidos (trocados) por bitcoins, ou por outro bem virtual, sem qualquer interação com o mundo externo.

Sem cartórios.

Sem DETRANs.

Sem espera.

Sem burocracia.

Sem corretores.

8. Quem determina o preço de um bitcoin?

Nenhuma pessoa, nenhuma empresa e nenhum computador em um galpão na Rússia tem poder sobre o preço do Bitcoin. O preço é consequência da oferta e da demanda de bitcoins no mercado, que por sua vez são consequências de:

- Escassez;
- Número de moedas em circulação;
- Moedas retidas como investimento;
- Utilidades práticas para os portadores;
- Notícias (muitas vezes veiculadas por idiotas);
- Análises financeiras (quase sempre feitas por idiotas);
- Ofertas de venda e compra nas corretoras;
- Maturidade e segurança do sistema;
- Número de usuários no mundo;

entre outros fatores.

Não existe um controle centralizado.

Não existe um lastro.

Nem mesmo os usuários ou as normas do sistema determinam diretamente o preço de um bitcoin.

Vale comentar:

Você não precisa comprar, vender, armazenar ou transferir necessariamente 1 bitcoin, ou múltiplos exatos de 1 bitcoin.

Bitcoins podem ser subdivididos em pequenas frações.

Hoje, a menor fração existente se chama Satoshi.

1 bitcoin é composto de 100.000.000 (cem milhões) de Satoshis.

Se 1 bitcoin vale R$30.000 então 1 Satoshi vale R$0,0003 - ou três centésimos de centavo.

9. Bitcoin é usado para comprar armas e drogas na DeepNet

Você acha que dinheiro vivo é utilizado para quê? Somente para transações legais? Somente por cidadãos exemplares?

Onde houver uma moeda, haverá um crime.

Esse rótulo criminoso vem como legado dos primeiros anos de Bitcoin.

Em 2009, pela primeira vez na história, uma moeda eletrônica potencialmente “anônima” começou a ser aceita na Internet.

Uma mão na roda para criminosos que não queriam deixar rastros.

Até então, moedas eletrônicas eram apenas representações de moedas reais.

Eram rastreadas por intermediários (bancos, bandeiras de cartão de crédito, sistemas de pagamento).

Não ofereciam qualquer privacidade.

Mas atenção, isso não significa que transações em Bitcoin podem ser consideradas anônimas.

É verdade que ninguém precisa se identificar para transacionar bitcoins.

Mas ainda existe a possibilidade de se rastrear transações.

Eventualmente revelando a identidade das partes.

Quem deseja - ou precisa de mais privacidade - pode tomar cuidados adicionais nada convenientes para tentar proteger sua identidade (pesquise sobre a rede TOR e os MIXERS de moedas).

Sempre haverá utilizações ilícitas para o Bitcoin.

Ou qualquer outra moeda.

É estimado hoje em dia que a maioria absoluta dos usuários não utilize Bitcoin para fins criminosos.

E mesmo que fosse o caso, Bitcoin continuaria funcionando normalmente, com a mesma segurança e utilidade, para os demais usuários.

10. Bitcoin é um esquema de pirâmide

Bitcoin é um exemplo de sistema totalmente democrático, onde todo usuário tem acesso aos mesmos recursos, às mesmas informações e ao mesmo poder de decisão de qualquer outro usuário.

Um usuário de Bitcoin não tem obrigação nenhuma de vender, comprar ou armazenar moedas.

Não precisa recrutar outros usuários.

Não recebe pontuação.

Não constrói reputação.

Não recebe comissões.

Não tem metas, nem garantias de rendimento.

Qualquer coisa que exista nesse sentido é algo que foi construído SOBRE o Bitcoin.

Por uma pessoa ou entidade que tem seus próprios interesses.

Ninguém é obrigado a participar disso.

E nem deveria.

Todo e qualquer esquema de pirâmide (ou Ponzi) pressupõe hierarquia, controle central e intermediários.

Nada disso existe no Bitcoin.

Descentralização é o nome do jogo.

O que não faltam são idiotas que se aproveitam da ignorância alheia para vender promessas.

É fácil identificar esses idiotas.

Eles garantem lucros.

Possuem uma receita infalível para se ganhar dinheiro rápido (vide Apêndice V - Golpes Idiotas).

NINGUÉM pode garantir lucro.

NINGUÉM pode garantir lucro.

NINGUÉM pode garantir lucro.

NINGUÉM sabe qual será o valor do Bitcoin amanhã.

NINGUÉM sabe qual será o valor do Bitcoin amanhã.

NINGUÉM sabe qual será o valor do Bitcoin amanhã.

Se uma atividade qualquer garante lucro e tem livre acesso ao público, é apenas uma questão de tempo para que todo mundo passe a exercer essa mesma atividade e ela deixe de garantir lucro.

Lei da Economia.

Se alguém está protegendo alguma informação valiosa, com certeza não vai compartilhar o segredo com você sem ter um acordo de não divulgação ou contratos com uma série de interesses financeiros.

No Bitcoin, não há nada escondido.

Todos podem estudar o código e aprender como funciona.

Essa é a definição de “código aberto” ou open source.

Um conceito antigo que talvez nunca tenha ficado tão evidente.

As regras são públicas e objetivas.

Mesmo que você não entenda sobre programação - ou tenha a disposição para estudar o código - o fato de ele ser aberto é um indicativo de que alguém estará fiscalizando e alertando sobre qualquer falha descoberta no software.

Ganhar dinheiro com Bitcoin não é garantido.

A melhor garantia para se ganhar dinheiro chama-se trabalho.

É exatamente isso que os idiotas querem que você faça por eles.

Um trabalho anti-ético, diga-se de passagem.

E se você ganhar algum dinheiro, será às custas de um idiota que perdeu dinheiro.

Até que eventualmente você se torne a vítima.

Pirâmides existem em diversos setores da economia.

Inclusive com moedas virtuais.

Mas não têm nada a ver com Bitcoin.

E só continuam existindo por culpa de quem acredita nos idiotas.

11. Meu celular contém bitcoins e pode ser roubado

Bitcoins não são armazenados no seu bolso, cofre, celular ou computador.

A única informação privada que você deve armazenar, controlar e proteger, são as chaves de acesso aos seus bitcoins.

Ou seja, as senhas que permitem que você gaste os bitcoins, transferindo-os de sua conta para outra.

Muito importante esta distinção:

- Os bitcoins NÃO ESTÃO no seu celular (software wallet) e portanto não dependem dele para continuar existindo.
- Se você perder as chaves e tiver cópias, não perderá seus bitcoins (nesse caso, transfira seus bitcoins para uma OUTRA conta sua para não correr riscos).
- Se roubarem suas chaves, poderão roubar seus bitcoins.

Software wallets (carteiras) não deveriam se chamar wallets, porque dificultam o entendimento.

Deveriam se chamar keychains (chaveiros).

Todas as contas, transações e moedas são armazenadas no blockchain do Bitcoin.

Trata-se de um livro caixa.

Um registro público de transações imutáveis, como se estivessem cravadas em pedra.

O blockchain é imutável.

O blockchain é público.

O blockchain é seguro.

O blockchain é fiscalizado e controlado pelos usuários.

O blockchain armazena os bitcoins.

Para se realizar uma transação no blockchain, efetivamente gastando bitcoins, você precisa:

- Ter saldo na conta origem;
- Possuir a chave da conta origem.

Nada mais.

Se alguém tiver acesso à chave, todos os bitcoins da conta poderão ser roubados (transferidos para uma outra conta, cuja chave naturalmente estará em poder do criminoso).

Simples assim.

Se o seu celular for perdido ou roubado - e as chaves estiverem nele - existe uma chance real de alguém conseguir roubar seus bitcoins.

“Mas calma aí!”, você diz.

"Meu celular tem um PIN de acesso para ser destravado!”

Boa sorte.

Você está disposto a correr esse risco?

Tem certeza que seu celular estava travado quando foi perdido?

Tem certeza que ninguém mexeu no seu celular enquanto ele estava destravado?

Tem certeza que ninguém poderá descobrir a sua senha ou PIN de acesso?

O app que gerou a chave da sua conta Bitcoin é confiável?

Quantos bitcoins você possui na conta?

Este valor é significativo a ponto de você não poder correr o risco de perdê-lo?

Cada um deve responder a essas perguntas e tirar suas próprias conclusões.

Quer o máximo de segurança?

Então terá que perder em conveniência.

Não deixe suas chaves no celular.

Não deixe suas chaves no computador.

Escreva em um papel e guarde-o com segurança.

Faça cópias e guarde-as em outro local secreto.

Porque daqui a alguns anos você irá se esquecer de suas senhas.

Poderá perder suas anotações, drives USB, HDs, computadores e celulares.

Os bitcoins continuarão protegidos no blockchain.

Mas sem as chaves, nunca poderão ser gastos.

Nem por você, nem por ninguém.

A relação segurança vs. conveniência está sendo aprimorada a cada dia.

Fique de olho nas últimas novidades.

Aprenda sobre os dispositivos especialmente desenvolvidos para armazenar e utilizar senhas com segurança, como os hardware wallets (vide Apêndice I - Wallets).

Tenha certeza do que está fazendo para não ter uma surpresa desagradável daqui a alguns anos.

Hackers já podem estar em poder de suas chaves neste exato momento, monitorando os saldos das contas, esperando o momento certo de agir.

Considere-se avisado!

12. Bitcoin é ilegal

Como um cidadão, você está sujeito às leis do seu país. Infelizmente, alguns países idiotas proíbem seus cidadãos de utilizarem Bitcoin.

É verdade que Bitcoin não tem jurisdição.

Não tem geografia.

Mas você tem!

E sua identidade pode ser descoberta.

Então você deve seguir as leis do seu país, mesmo que se trate de um país idiota.

Ainda que seu país permita a utilização de Bitcoin, você continuará sujeito às leis já existentes ou que venham a existir:

- Declaração de remessas;
- Imposto de renda;
- Cadastro de identidade;
- Pagamento de taxas.

Não posso dizer exatamente o que você pode fazer com Bitcoin no seu país.

Muito menos, como fazer.

Na dúvida, consulte um contador.

Ou um advogado especializado (boa sorte para encontrar).

Países ainda estão descobrindo como lidar com Bitcoin.

Como emendar as leis.

Como fiscalizar transações e usuários.

Nem tudo está claro neste momento.

Mas já podemos afirmar:

Para a grande maioria da população, usar bitcoins para simples transferências e compras não representa qualquer problema legal.

Desde que você tenha como explicar como adquiriu ou vendeu seus bitcoins.

Eventualmente, pagando os devidos impostos.

Para refletir…

Governos sabem que não é fácil FISCALIZAR as transações de bitcoins.

Também sabem que não é nada trivial IDENTIFICAR as partes.

Seus maiores aliados são as corretoras.

Porque corretoras normalmente precisam cadastrar seus usuários e reportar transações para o governo.

Mas se um usuário desejar efetuar transações sem passar por corretoras (sem converter bitcoins para outras moedas reais), tomando os devidos cuidados com sua privacidade, teoricamente ele pode permanecer anônimo.

O que significa isso para o governo?

Significa que será muito difícil controlar a população.

Praticamente impossível exigir a identidade das partes.

Quando uma atividade é considerada um direito legítimo, as tentativas de censurá-la normalmente são mal sucedidas.

Porque a população terá motivações para encontrar formas de burlar as proibições.

É natural do ser humano respeitar as leis que fazem sentido e desrespeitar aquelas que são abusivas.

Se eu fosse um governante não-idiota, eu aprenderia logo esta lição.

Tentaria adaptar minhas leis o quanto antes.

Alteraria os modelos de taxação.

Para não cair no mesmo erro das gravadoras musicais quando tentaram impedir o MP3.

Aposta para o futuro?

Bitcoin será ilegal apenas para poucos governos autoritários.

Bitcoin será uma moeda de troca do dia a dia, com boa privacidade.

Bitcoin poderá escalar para um volume muito maior de transações.

Bitcoin poderá viabilizar transações ainda mais rápidas e baratas.

Governos não conseguirão controlar usuários e suas transações.

Não conseguirão fiscalizar remessas.

Não conseguirão taxar ganhos ou transações.

Cabe a cada governo aprender a lidar com a realidade desde já. Se é que vai fazer sentido existir um governo nos moldes em que conhecemos hoje.

Não se engane.

Existe uma revolução pela frente.

13. Bitcoin pode desaparecer amanhã

Sim.

Bitcoin é um experimento que deu certo.

Sobreviveu por nove anos, gerando valor e utilidade para a sociedade.

Ainda que ele desapareça amanhã, foi capaz de nos deixar vários ensinamentos.

Novos conceitos, avanços e modelos de negócios que nunca mais deixarão de fazer parte da sociedade.

Bitcoin é, antes de mais nada, um software.

Um protocolo.

Um conjunto de regras.

Um código.

Amplamente baseado em teorias matemáticas.

Estatística.

Probabilidades.

Teoria de Jogos.

Criptografia.

Tudo isso funciona muito bem no papel.

Mas as provas acontecem na prática.

Bitcoin já se adaptou inúmeras vezes ao longo do caminho.

Sempre melhorando segurança e escalabilidade.

Mas nem todo problema pode ser previsto.

Nem todo problema poderá ser corrigido.

É possível que amanhã alguém descubra uma ferramenta matemática que quebre a segurança do Bitcoin.

Se o Bitcoin conseguir reagir a tempo, os danos serão pequenos e rápidos.

Se o Bitcoin não conseguir reagir, os danos poderão ser catastróficos.

Bugs de software não são exclusivos do Bitcoin.

Todo e qualquer software possui bugs.

Por isso existem os updates regulares, com correções e melhorias.

Quanto mais maduro um software, menor a chance de existir um bug catastrófico.

Mas existe uma chance.

E no caso do Bitcoin, não há uma empresa para você culpar ou processar.

A probabilidade de algo catastrófico acontecer com Bitcoin é desconhecida.

Teoricamente, diminui com o tempo.

Mas teremos sustos ao longo do caminho.

Novas descobertas.

Ameaças.

Falhas de segurança.

Quedas bruscas de valor, que podem ou não se recuperar quando que os problemas forem solucionados.

Bitcoin foi desenvolvido para estimular o bom comportamento do usuário.

E acreditamos que a maioria dos usuários queira de fato protegê-lo.

Tudo indica que existem muito mais cabeças protegendo - desenvolvendo, fiscalizando e aprimorando - o código do Bitcoin, do que cabeças tentando atacá-lo.

14. Não bastasse o Bitcoin, agora tem o tal do Blockchain

Essa é típica dos ranzinzas preguiçosos. Idiotas que não sabem do que estão falando, como se o Bitcoin fosse agora um problema em suas vidas.

Relembrando blockchain:

- Um livro de transações;
- Descentralizado;
- Confiável;
- Imutável.

Um blockchain pode ser público ou privado.

Um blockchain pode transacionar qualquer bem virtual.

Um bem virtual pode ser uma representação única de um bem real, ou apenas um bem abstrato, como um voto.

Pode ser uma moeda, um documento, um título.

Blockchain é uma das tecnologias por trás do Bitcoin.

Mas acabou virando sinônimo de todos os sistemas descentralizados que utilizam essa tecnologia.

Respire, releia este último parágrafo.

Bitcoin utiliza um blockchain PÚBLICO e transaciona uma MOEDA virtual.

Bitcoin possui muitos usuários no mundo - computadores e celulares que já rodam o software do Bitcoin.

Não faz sentido instalarmos um software diferente para cada bem virtual que possuímos ou venhamos a possuir no futuro.

Não faz sentido existir um blockchain para cada bem virtual.

Não seria prático.

Seria um desperdício de recursos.

Porque cada blockchain demanda esforços de seus usuários para se tornar de fato útil e seguro.

Por isso, o blockchain do Bitcoin é utilizado criativamente para transacionar outros bens que não sejam bitcoins.

Isso acontece a todo momento.

Documentos importantes, como contratos e títulos, já são transacionados no blockchain do Bitcoin.

É de interesse geral do público que bens sejam transacionados digitalmente em um blockchain.

Para se ganhar em agilidade, privacidade, segurança e economia.

Um título virtual de imóvel (um bem virtual atrelado a um bem físico) poderia ser vendido por bitcoins (outro bem virtual).

Sem envolver dinheiro tradicional.

Sem cartórios.

Sem corretores.

Sem o risco de títulos dublês, adulterados ou perdidos.

No futuro?

Imaginamos que blockchains sejam multi-funcionais.

Transacionem vários tipos de bens e estejam inter-conectados.

Ou que exista um único blockchain mestre, público e universal.

O blockchain do Bitcoin seria um forte candidato como blockchain mestre.

Ethereum é um outro candidato.

Mas não sabemos o que acontecerá.

Provavelmente, governos criarão seus próprios blockchains para os cidadãos.

Empresas tentarão criar blockchains e convencer usuários a utilizá-los.

E nesse momento estaremos voltando ao modelo centralizado, que foi justamente o que motivou a criação de blockchains descentralizados e moedas como o Bitcoin.

Portanto, improvável que funcione na prática.

Governos já tentaram criar suas moedas nacionais virtuais, sem sucesso.

Neste exato momento, empresas, bancos, cartórios e governos idiotas estão anunciando publicamente que começaram a utilizar blockchain.

Como se isso fosse um grande benefício para o público.

Como se isso fosse um atestado de apoio ao movimento de descentralização.

Não se engane!

Eles continuarão no controle.
Vão trocar seis por meia-dúzia.
Apenas para ganhar uma sobrevida.

15. Eu deveria ter comprado em 2011

Hoje, olhando para trás, sim, você deveria. Mas ninguém sabia o que iria acontecer.

Para evitar lamentações:

Se você tivesse comprado um bitcoin por centavos, muito provavelmente já os teria vendido quando o preço atingiu R$10.

Se você tivesse comprado um bitcoin por R$100, muito provavelmente já os teria vendido quando o preço atingiu R$1.000.

De um jeito ou de outro, seus ganhos seriam bons, mas não seriam o que os idiotas normalmente anunciam: “hoje você poderia ter 500 milhões de reais!”.

Poderia.

Mas provavelmente não teria.

O jogo ainda está valendo.

Tudo pode acontecer.

Existem motivos para o valor continuar aumentando a longo prazo.

Existem motivos para o valor oscilar abruptamente durante muito tempo.

Existem riscos de falhas catastróficas.

Compreenda e aceite o cenário para tomar suas decisões.

O valor máximo do Bitcoin, teoricamente, está limitado pela quantidade de valor existente no mundo.

Existe um teto, não se pode criar valor do nada.

Mas também existe um histórico, um investimento feito pelos usuários, durante todos esses anos de existência.

A menos que aconteça uma falha catastrófica, sempre haverá um piso razoável de valor.

Dificilmente um bitcoin voltará a valer o que valia nos seus primeiros anos.

Exemplo extremo:

Se no futuro todas as moedas do mundo forem abandonadas em favor do Bitcoin e todas as transações do mundo forem feitas com bitcoins, o valor atual está longe de onde poderia chegar.

Tudo pode acontecer entre este extremo e a quebra catastrófica do Bitcoin.

16. Meu vizinho está minerando bitcoins na garagem, vou avisar a polícia

Chame a polícia e torne-se imediatamente mais um idiota.

Minerar, além de uma atividade legal na grande maioria dos países, é ESSENCIAL para o funcionamento do blockchain.

Mineradores merecem todo nosso respeito.

Mineradores investem grandes esforços - trabalho e capital - para aumentarem a confiabilidade do Bitcoin.

Naturalmente, mineradores esperam retornos financeiros de suas ações.

A mineração é uma solução genial para duas grandes necessidades do Bitcoin (ou de qualquer blockchain semelhante ao Bitcoin):

- Imutabilidade das transações;
- Emissão de moedas.

A mineração é uma atividade NECESSÁRIA, prevista, legítima, essencial para a CONFIABILIDADE do sistema e, ao mesmo tempo, responsável pela ESCASSEZ das moedas.

Colocar uma transação no blockchain requer um esforço gigantesco.

Para se ter uma ideia, um computador moderno demoraria centenas de milhares de anos para realizar este esforço computacional sozinho.

Nossos amigos mineradores possuem grande poder computacional e fazem isso por nós.

A todo instante, milhares de usuários estão fiscalizando e verificando as transações realizadas na rede, rejeitando todas aquelas que não são válidas.

Mineradores coletam as transações válidas, trabalham para adicioná-las ao blockchain e recebem bitcoins como forma de recompensa pelo seu esforço.

Uma espécie de agradecimento - ou incentivo - para continuarem protegendo o sistema.

Se um minerador tentar incluir uma transação inválida (mal intencionada ou mal formatada), ela será automaticamente rejeitada pelos demais usuários.

Não será incluída no blockchain.

Não existirá.

Todo o esforço do minerador terá sido em vão e ele não receberá sua recompensa.

São as regras do Bitcoin.

Um usuário comum não possui o esforço necessário para acrescentar transações no blockchain.

E um minerador é fiscalizado pelos usuários para que acrescente somente transações válidas.

No final das contas, é estatisticamente improvável que alguém mal intencionado consiga alterar, apagar, rejeitar ou forjar transações.

Pergunta:

O que impede, portanto, que uma transação legítima seja alterada, ou que uma transação má intencionada seja adicionada ao blockchain?

Resposta:

Força bruta.

Não basta ser inteligente.

Não basta entender o código.

É preciso ter mais poder computacional do que todo o restante dos usuários.

A maioria manda.

A maioria vence.

Outras regras importantes que aumentam a confiabilidade do Bitcoin:

- Não se pode criar bitcoins do nada;
- Contas sem saldo não podem ser gastas;
- As chaves de acesso nunca estão no blockchain.

Isso reduz drasticamente as possibilidades de ataques e portanto os incentivos para se tentar burlar o sistema.

Cada vez que um minerador conclui seu trabalho, sua recompensa é paga com bitcoins transferidos para uma conta sua.

Esses bitcoins são criados pelo software especificamente para este propósito.

Este é o mecanismo de emissão de bitcoins.

Controlado e pré-determinado.

A mineração viabiliza a confiabilidade do blockchain e regula a emissão das moedas.

Em 2140, todos os bitcoins terão sido emitidos.

Serão 21 milhões de moedas.

O sistema continuará funcionando.

E a cada dia haverá menos moedas em circulação, porque usuários perdem suas chaves.

A escassez aumenta com o tempo.

O que tende a aumentar o valor da moeda.

Mito: a mineração desperdiça energia elétrica e é um problema energético para o planeta.

Primeiro: o consumo de energia é necessário para o funcionamento do sistema. Outros soluções mais “verdes" estão sendo estudadas e poderão funcionar no futuro.

Segundo: os bancos - com o mesmo propósito de segurança e agilidade - consomem MUITO mais energia do que o Bitcoin, através de seus escritórios, agências, caixas eletrônicos, carros-fortes, computadores etc.

17. Eu não acredito nisso aí

Bitcoin não é crença, não é fé, não é teoria. Bitcoin existe.
Ponto.

Será utilizado pela maioria da população?
Quando?
Atingirá um valor estável?
Ninguém sabe dizer.

Cada um tem suas próprias expectativas.
Mas são apenas apostas.
Teorias.
Em alguns casos, misticismo.

Há quem ainda enxergue Bitcoin como uma brincadeira de hackers.
Um projeto de escola.
Uma ideia absurda.
Um plano ridículo.

Bitcoin é uma das coisas mais geniais dos últimos tempos.

Você acredita em Agricultura?
Você acredita em Máquinas a Vapor?
Você acredita em Eletricidade?
Você acredita em Internet?

Bitcoin (ou mais precisamente blockchain) é uma tecnologia de propósito geral, como todas estas acima.
Tem potencial de revolucionar a Indústria, o Comércio, a Economia e as relações entre as pessoas.

Ninguém precisa acreditar.
Basta ser sensato e aceitar.

18. Se a NSA(*) é hackeada, Bitcoin também pode ser hackeado

Todo e qualquer sistema pode ser hackeado, não existe segurança absoluta.

O importante aqui é balancear:

- Esforço vs. Recompensa
- Segurança vs. Conveniência
- Incentivos vs. Obstáculos

O que exatamente está sendo hackeado?

Qual o custo dessa perda?

Quantos usuários são prejudicados?

Com que frequência e probabilidade ocorre um ataque efetivo?

Antes do Bitcoin, os alvos de ataque eram centralizados.

Bitcoin é descentralizado.

Isso muda tudo.

Atacar, agora, significa ganhar controle de milhares ou milhões de alvos.

Um dos grandes benefícios da descentralização é justamente melhorar a segurança.

Distribuir os alvos.

Retirar a vulnerabilidade de um ponto central.

Ninguém até hoje conseguiu de fato hackear o Bitcoin para criar moedas do nada, alterar transações dentro do blockchain ou descobrir senhas de usuários para roubar moedas.

Pelo menos não em larga escala, de uma forma sustentável.

Então, sim, nesse sentido Bitcoin é mais seguro do que a NSA.

Hackers procuram alvos de máximo retorno e mínimo esforço.

Como o seu computador.

Ou o seu celular.

Ou o papel com a senha que você deixou sobre a mesa do escritório.

Nada disso tem relação com Bitcoin.

Ou com blockchain.

São falhas do usuário.

Se alguma grande falha de segurança acontecer com Bitcoin, ele se adaptará rapidamente para tentar corrigi-la.

Com uma agilidade comparável às maiores instituições do planeta.

Porque há desenvolvedores querendo proteger suas próprias moedas.

Porque há mineradores que já investiram muito dinheiro no sistema.

Porque há usuários fiscalizando e alertando o ecossistema.

Porque há muito valor em jogo.

(*)NSA - Agência de Segurança Americana

19. Bitcoin é usado para lavar dinheiro

Os bancos são as instituições mais utilizadas no mundo para se lavar dinheiro.

De novo:

Os bancos são as instituições mais utilizadas no mundo para se lavar dinheiro.

A pseudo-anonimidade do Bitcoin traz incentivos para criminosos.

Mas criminosos conhecem maneiras mais anônimas para lavarem dinheiro.

Bitcoin não garante anonimidade.

As transações podem ser rastreadas para se descobrir as identidades de origem e destino.

É uma questão de esforço.

E sabemos que governos não medem esforços quando querem conseguir uma informação.

Bitcoin viabiliza transferências rápidas, de alto valor, sem fronteiras geográficas.

São outros incentivos para criminosos.

Eles vão encontrar maneiras de usar isso a seu favor.

Mas não significa que existam bitcoins falsos.

Embora exista o risco de alguns bitcoins serem considerados “sujos”, devido a seu histórico de transações gravado no blockchain.

As características do Bitcoin podem ser usadas criativamente para se burlar o pagamento de impostos e até mesmo para se lavar dinheiro (justamente através do pagamento de impostos).

Como qualquer outra moeda.

Não confundir a mensagem com o mensageiro.

20. Minerar é a forma mais segura de se ganhar dinheiro com Bitcoin

Talvez fosse verdade no primeiros anos. Mas em pouco tempo, muita gente aprendeu como fazer, a concorrência aumentou e minerar deixou de ser uma atividade econômica atrativa.

Qualquer que seja a atividade lucrativa, é apenas uma questão de tempo para que forças naturais de mercado diminuam sua lucratividade.

Até o ponto onde a grande maioria dos participantes começa a perder dinheiro.

Alguns empatam.

E apenas quem está muito bem aparelhado com informação e capital continua a ter vantagens competitivas.

Com mineração, não é diferente.

Minerar bitcoins requer poder computacional.

Investimento em hardware.

Muito hardware, se você quiser ter boas chances de retorno.

Minerar consome energia elétrica.

Muita energia elétrica.

Hardware gera calor, que precisa ser resfriado.

Mais energia elétrica.

Se você entrar no jogo com pouco dinheiro, não terá muitas chances de retornar seu investimento.

Porque estará competindo com aglomerados gigantescos de computadores que só fazem isso, 24 horas por dia.

Muitos deles em regiões frias do planeta, onde é mais fácil se livrar do calor gerado.

Muitos deles ao lado de usinas de energia que foram reativadas com o único propósito de alimentar os computadores dos mineradores.

Jogo de gente grande.

Computadores evoluem em um ritmo tão acelerado que precisam ser substituídos em questão de meses para que o minerador permaneça competitivo.

Mais investimento.

E ainda estima-se que os fabricantes de computadores especializados para mineração utilizem seus próprios produtos recém desenvolvidos para minerar, antes de os lançarem no mercado.

A essa altura, boa parte do tempo de vida do hardware já terá sido gasta.

Não tenha a expectativa de que minerar na garagem de casa seja um bom negócio.

Quase todos os mineradores hoje em dia participam de pools.

Onde usuários e seus computadores juntam forças e dividem os lucros, proporcionalmente à quantidade de poder computacional com que cada um contribui ao pool.

Mas, na ponta do lápis, pools não aumentam necessariamente a possibilidade de ganhos ou retorno de investimento.

As leis de mercado sempre se ajustam naturalmente.

Mineradores pequenos podem melhorar suas chances de retorno minerando moedas alternativas (vide Apêndice II - Altcoins).

Porque a concorrência tende a ser menor.

Mas assim que se essas moedas se mostram interessantes para a mineração, imediatamente a concorrência aumenta.

Não existe mágica no Bitcoin.

Não existe garantia de lucro.

Tudo é uma questão de risco, informação, competitividade, trabalho e investimento.

E já que estamos falando de atividades econômicas e negócios…

Diariamente, ao redor do mundo, start-ups estão tentando criar modelos de negócios sustentáveis utilizando Bitcoin e blockchains.

A questão é: como lucrar em um sistema onde, por definição, os usuários não querem uma empresa controlando o serviço?

Existem muitas questões abertas que ainda precisam de tempo para maturação.

A grande bola da vez parece ser a emissão e a venda de moedas virtuais (tokens) que funcionam como ações de uma empresa autônoma e descentralizada.

Os chamados ICOs (Initial Coin Offerings).

Esses tokens supostamente retornarão dividendos ou benefícios aos seus portadores - os quais atuam efetivamente como sócios do negócio.

Antes de considerar qualquer investimento nesse sentido, questione-se:

Você costuma investir em start-ups?

Tem o hábito de colocar seu dinheiro em fundos de investimentos arrojados?

Confia em produtos de empresas que acabaram de entrar no mercado?

Então por que investir em um negócio ainda mais experimental e arriscado do que os tradicionais?

A grande maioria desses novos negócios não conseguiu entregar os lucros esperados por seus sócios-investidores.

Muita gente está perdendo dinheiro por falta de informação.

Seduzidas e iludidas.

Para muitas dessas novas empresas, utilizar blockchain é apenas um diferencial de marketing, atrativo e moderno.

Elas nem precisariam de blockchain para fazer o que fazem.

Blockchain não é a solução para tudo.

Mas esse é um assunto mais avançado, talvez um dos temas para o próximo livro.

Missão cumprida

A esta altura, talvez você entenda muito mais de Bitcoin do que a maioria da população mundial. Se você se assustou, ótimo, pode evitar problemas futuros. Se você se animou, melhor ainda, continue estudando, experimente na prática.

Todos os dias eu aprendo algo novo e dedico boa parte do meu tempo para estudar esse assunto fascinante. Recomendo que faça o mesmo. Tudo ficará mais fácil e intuitivo ao longo dos próximos meses, conforme novos softwares sejam desenvolvidos e utilizados em larga escala, conforme os negócios insustentáveis, as informações desencontradas e os mitos sejam derrubados.

Escolha um software carteira (Apêndice I - Wallets), crie contas, adquira alguns Satoshis e comece a fazer transações. Experimente outros wallets, compare a conveniência e a segurança das opções existentes. Conheça outras moedas virtuais (Apêndice II - Altcoins), pesquise sobre Ethereum e as funcionalidades que essa moeda oferece em seu blockchain. Acompanhe notícias de fontes confiáveis (Apêndice III - Notícias e Publicações). Aceite que, por muito tempo, haverá grandes oscilações de preço em todas as moedas virtuais.

Indique este livro para sua rede de contatos, procure transmitir o que aprendeu. Quanto mais usuários conscientes existirem no mundo, mais valor, segurança e utilidade terá o Bitcoin. Esteja preparado para uma reviravolta na legislação, tentativas de controle por parte de governos e organizações, escândalos e notícias assustadoras, mas duvide de tudo que escutar. Para mais detalhes técnicos sobre blockchains e o funcionamento do Bitcoin, veja as referências que selecionei (Apêndice IV - Bibliografia Recomendada).

Bitcoin (e outros sistemas baseados em blockchain) estão revolucionando o mundo de diversas maneiras. Viveremos muitos anos de transição, mas é apenas uma questão de tempo para que muitas das formas de transações que existem hoje sejam substituídas. Porque todo mundo valoriza liberdade, segurança, autonomia, acesso, democracia e agilidade. Não tem volta.

Parabéns por dedicar seu tempo a um assunto tão importante!

Obrigado,

Dennis Zasnicoff

Apêndice I - Wallets

Wallets (carteiras) são aplicações online ou softwares instalados em computadores ou celulares que possuem as seguintes funções:

- Criar contas
  (não é necessário estar online);
- Transferir bitcoins
  (é necessário estar online para enviar a transação para a rede de usuários que fará a validação e inclusão no blockchain);
- Monitorar saldos, recebimentos e pagamentos
  (a carteira atualiza as informações toda vez que está online);

Toda vez que uma conta de Bitcoin é criada, dois números são gerados:

- Um endereço público (número da conta) que você irá compartilhar com o mundo para receber bitcoins, mesmo que não esteja online;
- Uma chave privada associada, que será utilizada para você poder gastar os bitcoins recebidos em sua conta.

Wallets também podem oferecer outras funcionalidades, algumas delas bem avançadas, que não são necessárias para a maioria das transações.

As chaves privadas (que nunca devem ser compartilhadas com ninguém) são códigos longos e impossíveis de se memorizar. Em pouco tempo, você poderá ter várias contas e chaves para administrar. A solução prática é encriptar (embaralhar, esconder) todas as chaves através de uma única senha mestra. Todo wallet que se preste tem essa opção. VOCÊ DEVERÁ ESCOLHER UMA SENHA MEMORÁVEL E, AO MESMO TEMPO, IMPOSSÍVEL DE SER DESCOBERTA.

Mesmo que o arquivo encriptado seja roubado, nunca poderá revelar as chaves sem o conhecimento da senha. Por outro lado, a senha permite acesso a todas chaves e portanto a todos seus bitcoins. É a informação mais importante que você deve controlar! Utilize uma frase longa, do tipo: “A grama do meu quintal mais parece o cabelo do caixa do super-mercado”. Mas não confie em sua memória. Escreva a senha em um papel e guarde-o em um local seguro.

O arquivo encriptado pode estar armazenado no software wallet (menos segurança) ou fora dele (mais segurança). De qualquer forma, lembre-se que este arquivo poderá ser perdido ou corrompido em algum momento - drives USB deixam de funcionar, discos de computadores e celulares podem quebrar - então a segunda preocupação é fazer um backup (uma cópia) desse arquivo e armazená-lo em outro local seguro.

Esse backup, por sua vez, também está sujeito a desaparecer com o tempo. Considere uma forma mais segura de recuperar as chaves, como aquela oferecida pelas chamadas carteiras determinísticas.

No final das contas, você deve se certificar de que:

- Possui uma senha mestra segura para esconder todas as suas chaves, onde quer que elas estejam armazenadas. Essa senha deve ser memorizada e será utilizada toda vez que desejar transferir bitcoins;
- Tem alguma forma confiável de recuperar as chaves caso elas sejam perdidas: um backup seguro (preferencialmente encriptado) ou uma frase determinística muito bem escondida.

Para maior segurança, as chaves não devem ser armazenadas no software wallet do computador ou do celular - mesmo que estejam encriptadas - mas sim em alguma forma de cold storage (armazenamento frio), desconectado da Internet, como um drive USB ou uma paper wallet.

São muitas as possibilidades de criação e armazenamento de chaves, não existe uma receita simples. A melhor dica aqui é você estudar as opções disponíveis, escolher o nível de segurança desejado e não pecar nos detalhes.

O wallet referência de mercado, que contém o código “original" do Bitcoin, com todas as normas do sistema, que é mantido pela comunidade e implementa de fato a rede mundial do Bitcoin, chama-se "Bitcoin Core”.

Bitcoin Core é utilizado pela maioria dos usuários que participam ativamente do ecossistema, fiscalizando as transações e adicionando confiabilidade ao Bitcoin. No entanto, não possui uma interface tão amigável, além de consumir muito disco, memória e processamento dos computadores dos usuários.

Idealmente, este deveria ser o wallet utilizado por todos, mas vou apresentar aqui outras opções, porque estamos sendo extremamente práticos. É melhor termos usuários participando e contribuindo com um pouco, do que não termos usuários.

Uma nota sobre código aberto: via de regra, quando você baixa um aplicativo da Internet, implicitamente você está confiando no desenvolvedor e nunca poderá dizer exatamente o que o software está executando. Exemplo, o wallet poderá criar chaves para suas contas e automaticamente enviá-las para outra pessoa, sem que você saiba. Quando o software possui código aberto, todo o seu funcionamento é transparente e existem maneiras de o usuário certificar-se de que baixou e está utilizando uma versão confiável. Nesse sentido, wallets que não possuem código aberto demandam necessariamente que o usuário confie no seu desenvolvedor.

Alguns dos wallets mais populares são:

SOFTWARE

Aplicativos para celulares, programas de computador ou extensões para navegadores:

- Armory - diversas funcionalidades, voltada para usuários avançados. Código aberto.
- Electrum - utiliza uma rede própria de servidores para confirmar transações e viabilizar carteiras “light”, que são rápidas e leves para o computador / celular. Suporta hardware wallets. Código aberto.
- Exodus - excelente interface de usuário, visual e informativa. Suporta várias moedas e corretagem entre elas no próprio software. Não possui código aberto.

- Jaxx - com suporte a várias cripto-moedas e boa interface de usuário, também pode ser instalado como uma extensão para Chrome. Apesar de o desenvolvedor disponibilizar partes do código para consulta, não podemos dizer que possui código aberto.
- Mycelium - App para celulares, oferece funcionalidades como trading, reputação e chat seguro. Suporta hardware wallets. Possui código aberto (no sentido de poder ser verificado).

ONLINE

Não recomendadas, pelo simples motivo de suas chaves serem criadas e armazenadas em um servidor que pode ser atacado. Para muitos usuários, no entanto, talvez seja mais seguro confiar em um terceiro do que em si próprio:

- blockchain.info
- Coinbase
- Xapo - oferece cartão / funcionalidade para sacar dinheiro em caixas-eletrônicos.

HARDWARE

Dispositivos que armazenam as chaves com mais segurança, teoricamente imunes a vírus. Funcionam juntamente com um software que realiza as transações, acessa o blockchain e monitora os saldos:

- Ledger Nano
- Trezor

SEGURANÇA AVANÇADA:

- BitKey - software baseado em Linux, executado a partir de um drive USB.
- Paper wallets - mecanismo para criação segura de chaves (offline) e armazenamento em papel.
- Copay - facilita a utilização de contas com multi-assinaturas que requerem a autorização de duas ou mais partes para que as moedas sejas gastas.

Apêndice II - Altcoins

"Altcoins" é o termo usado para todas as moedas virtuais que surgiram após o Bitcoin. Existem literalmente centenas delas. Muitas já desapareceram e estima-se que a maioria deverá sumir antes de conseguirem uma boa tração de mercado.

Bitcoin conseguiu sobreviver por nove anos por diversos motivos: foi a primeira moeda virtual baseada em blockchain, obteve, desde o início, grande apoio da comunidade (desenvolvedores, acadêmicos, analistas), atraiu a atenção do público e conseguiu construir um ecossistema de usuários e mineradores. Toda moeda que pretenda oferecer utilidade, segurança e confiabilidade, gerando valor para seus usuários, precisa conseguir se adaptar frente às ameaças e bugs de software. Sem um sólido ecossistema, uma moeda virtual não consegue sobreviver.

Por ser referência de mercado e possuir um grande número de usuários, Bitcoin tem a característica de ser conservador. Quando alterações no software são propostas, a comunidade analisa cuidadosamente os riscos e benefícios de longo prazo. Isso significa que algumas das melhorias desejadas pelos usuários demorem muito tempo, ou simplesmente nunca sejam adicionadas ao Bitcoin. Exemplos de possíveis melhorias no Bitcoin são: maior número de transações por segundo e menor tempo para confirmação de transações (hoje em torno de 10 minutos).

Altcoins surgem justamente como uma maneira de se oferecer funcionalidades que ainda não existem no Bitcoin, colocando-se no mercado como alternativas mais arrojadas e experimentais - portanto mais perigosas. Não bastasse o risco, nem sempre conseguem demonstrar um apelo forte para arrecadar um número suficiente de usuários. Muitas altcoins já conseguiram se estabelecer no mercado, mas todas elas, inevitavelmente, têm seu valor influenciado pelo valor do Bitcoin, que funciona como termômetro do mercado.

Algumas das mais populares são:

- Bitcoin Cash: Um hard fork do Bitcoin - ou uma alteração no software - que acabou dividindo o blockchain em dois. Pode ser considerado um "dissidente" do Bitcoin, oferecendo características distintas, como menor taxas de transações.

- Bitcoin Gold: Outro fork do Bitcoin, com o objetivo de descentralizar a mineração, aumentando as chances dos pequenos mineradores.
- Dash: oferece transações instantâneas, mas depende de servidores próprios (centralização).
- Dogecoin: uma moeda que pretende construir uma comunidade mais descontraída, é frequentemente utilizada como “gorjeta” (likes com valor) em redes sociais.
- Ethereum: a maior plataforma de Smart Contracts (contratos inteligentes), utilizada para transacionar diversos tipos de bens. Está associada a emissão de tokens (recompensas, milhagem, títulos de clubes, direitos de uso etc.), Organizações Autônomas Descentralizadas (DAOs), Aplicações Descentralizadas (DAPPs) e Initial Coin Offerings (ICOs).
- IOTA: desenvolvida para conectar negócios e facilitar a Internet das Coisas (IoT), baseia-se em DAG - uma alternativa aos blockchains tradicionais que busca não depender do poder computacional de mineradores.
- Litecoin: surgiu com a missão de acelerar a velocidade das transações e distribuir o poder de mineração. Conseguiu se estabelecer como uma das mais populares altcoins.
- Monero: tem a promessa de não ser rastreável: garante anonimidade aos usuários e impede a existência de moedas "sujas".
- Ripple: focado em instituições financeiras, é o blockchain mais utilizado por bancos com o pretexto de melhorar seus serviços.
- Steem: uma moeda-recompensa (token) voltada para geradores de conteúdos em redes sociais. Em muitos aspectos, é semelhante aos tokens criados no blockchain do Ethereum.
- Tether: uma tentativa de lastrear a cripto-moeda em moedas nacionais, como o dólar, em uma relação de uma para uma. Na prática, é uma representação virtual da moeda real, com os possíveis benefícios de um blockchain.
- Zcash: outra proposta de moeda com anonimidade, utiliza novos modelos criptográficos conhecidos como zero-knowledge proofs.

Apêndice III - Notícias e Publicações

- criptoBomba - Verdades (in)Convenientes
  criptobomba.com
- Bitcoin.org (Bitcoin Core)
  bitcoin.org/pt_BR/
- Bitcoin Magazine
  bitcoinmagazine.com/
- Bitcoin Wiki
  en.bitcoin.it/wiki/Main_Page
- Blockchain Alliance
  www.blockchainalliance.org/
- Blockchain Research Institute
  www.blockchainresearchinstitute.org/
- Coindesk
  www.coindesk.com/
- CoinJournal
  coinjournal.net/
- Cointelegraph
  cointelegraph.com/
- Crypto Stack
  cryptostack.xyz/
- Kyle Torpey's Daily Bitcoin Recap
  www.getrevue.co/profile/kyletorpey/
- The Blockchain Info
  www.theblockchaininfo.com/

Apêndice IV - Bibliografia Recomendada

- Bitcoin a Moeda na Era Digital
  2014
  por Fernando Ulrich
- Blockchain: Blueprint for a New Economy
  29 de Janeiro de 2015
  por Melanie Swan
- Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World
  10 de Maio de 2016
  por Don Tapscott, Alex Tapscott
- Código-fonte do Bitcoin
  github.com/bitcoin/bitcoin
- Mastering Bitcoin: Programming the Open Blockchain
  12 de Junho de 2017
  por Andreas M. Antonopoulos
- The Internet of Money
  05 de Setembro de 2016
  por Andreas M. Antonopoulos
- The Internet of Money (Volume II)
  01 de Dezembro de 2017
  por Andreas M. Antonopoulos

Apêndice V - Golpes Idiotas

Essas são mensagens reais, recebidas todos os dias na forma de e-mails, mensagens instantâneas e posts em redes sociais. Muitas delas são mal escritas e sugerem grupos internacionais que não falam nativamente a língua utilizada - típico de golpistas em alguns países do mundo. Outras vezes, são esquemas muito bem elaborados, com websites, PDFs e vídeos bem produzidos.

Seja como for, o idiota sempre garante segurança e lucratividade, utilizando-se de termos que parece não entender.

Exemplo em Inglês:

"Hello, how are you doing, have you ever invested or interested in bitcoin / binary trading? Well I'm an expert Bitcoin miner and Binary Option trader I Mine bitcoin with the aid of my antminer bitmain And I trade using the MetaTrader4 software.and This is 97% guaranteed... you will not lose your money..your investment capital is 100% safe so Theres nothing to worry about or be scared of.get back to me if you're interested. Thank you.”

Exemplo em Português:

"Boa tarde a paz do senhor gostaria de te apresentar uma oportunidade de negócio fantástico vou te mandar arquivos pq sei que vc é um empreendedor falando sobre investimento em uma moeda chamada bitcoin... É uma moeda criptografada… Os bancos usam o nosso dinheiro para investir em bitcoin… Dá uma olhada no que te mandei pq está no início de uma realidade do futuro breve acabar dinheiro de papel…Depois vc me diz oque achou…”

Quase sempre as mensagens são enviadas com um documento anexo. Um PDF que recebi recentemente é um bom exemplo. Não vou citar o nome da empresa.

Primeiro, explicam que existe uma nova forma de empreendedorismo, baseada em um modelo de afiliados (leia-se: pirâmide), com diversos níveis de comissão, que possuem nomes incríveis como Super-Tulipa-Ouro e Triplo-Diamante. O sistema deles é único, uma das maiores evoluções jamais vista no mundo dos negócios.

Na sequência, a famosa comparação da rentabilidade de cripto-moedas versus CDB e Poupança, seguida pela frase de impacto: “Se você tivesse investido $100 em Bitcoin, hoje teria milhões”.

Depois, uma tabela de ganhos, com as porcentagens garantidas - de acordo com o seu nível - e os prêmios para quem mudar de categoria: viagens, iPhones, cruzeiros, casas, carros de luxo. Para finalizar, o endereço da empresa, em algum lugar exótico do mundo, como NY, Dubai ou Suíça.

****

Primeira edição, v1.1, Outubro de 2018

zasnicoff.com - Treinamento e Consultoria

criptobomba.com - Verdades in(Convenientes) - Acompanhe criptoBomba para vídeos e discussões sobre Bitcoin, Blockchain e o Universo Cripto.

Capa: Dennis Zasnicoff

Foto: Satoko Nakamoshi