O LIVRO MAIS SIMPLES SOBRE  *JÁ ESCRITO*

Keysa Luna

* dar a pílula laranja (orangepillar)* to orange-pill: (verbo)
/ tu' ȯr-inj-'pil/
: o ato de explicar o bitcoin de tal maneira que um pre-coiner entenda e se torne um bitcoinheiro!

1 bitcoin = 100.000.000 satoshis

O Livro Mais Simples Sobre Bitcoin Já Escrito

Capa e design interiores por Keysa Luna
Foto da capa por Vallota do Pixabay.com
Tradução e edição para o português feita por Mercado Satoshi www.mercadosatoshi.com.br Twitter: @mercadosatoshi Nost: @mercadosatoshi
Publicado de forma Independente

ÍNDICE

para todas as nossas crianças

agradecimentos à Satoshi e aos cypherpunks

Eu amo a vida simples,
Eu amo a natureza, Eu amo ficar descalça,
Eu amo conversas profundas que despertam a criatividade, conexão e inspiração.
Eu amo a liberdade.

E, Eu amo o Bitcoin.

Amor é uma grande palavra, mas o bitcoin é digno de um grande amor.

Sua existência é um ponto de luz brilhante neste momento tão desafiador da existência humana.

Escrevi este livro na esperança de tornar o bitcoin e as razões pelas quais precisamos dele, mais acessíveis a mais pessoas.

Este livro é um ponto de partida para o que eu, e muitos outros, descobrimos ser uma toca de coelho fenomenalmente infinita, bela e transformadora!

Que você tome essa pílula laranja, que você seja livre,
e que sua jornada seja muito enriquecedora!

- **Observação:** Tudo o que é apresentado neste pequeno livro está aberto à debates, discussões, atualizações e correções!

- Como tudo na vida, há vários pontos de vista sobre o bitcoin, seu futuro e todos os seus vários aspectos.

- Comentários empolgados são transmitidos 24 horas por dia, 7 dias por semana no Twitter, que oscilam entre confundir e esclarecer! E, ainda assim, é um recurso inestimável (até que uma plataforma melhor e descentralizada seja amplamente adotada) para interagir com pessoas que já estão há muito tempo na toca do coelho...

- Todo esse ecossistema é um desdobramento emergente, popular, confuso e fascinante! É, de longe, o maior experimento global já realizado, com pessoas de todas as raças, religiões, classes e convicções se engajando juntas, sem permissão, para descobrir um novo caminho a seguir.

- Se você se sentir inspirado por esse movimento, é muito provável que caia na toca do coelho com gente!

- Um brinde às mentes e corações abertos ao longo do caminho...

    - Lembre-se: Não confie, Verifique *(Don't Trust, Verify)*

- E sempre faça sua pesquisa por conta própria! *(DYOR Do Your Own Research!*

Desenvolvi um novo sistema de dinheiro eletrônico P2P de código aberto chamado Bitcoin. Ele é totalmente descentralizado, sem servidor central ou partes confiáveis, porque tudo se baseia em prova de criptografia em vez de confiança. Experimente-o ou dê uma olhada nas capturas de tela e no documento de design:

Baixe Bitcoin v0.1 em http://www.bitcoin.org

~ Satoshi Nakamoto 11-02-2009 22:27:00 UTC
Publicado em metzdowd.com, uma das primeiras listas de discussão sobre criptografia

POR QUE NÓS PRECISAMOS DO bitcoin ?

NÓS PRECISAMOS DO bitcoin PORQUE O DINHEIRO ESTÁ EM COLAPSO

A raiz do problema com a moeda convencional é toda a confiança necessária para que ela funcione. O banco central deve ser confiável para não desvalorizar a moeda, mas a história das moedas fiduciárias está cheia de violações dessa confiança. Os bancos devem ser confiáveis para guardar nosso dinheiro e transferi-lo eletronicamente, mas eles o emprestam em ondas de bolhas de crédito com apenas uma fração na reserva. Temos que confiar neles nossa privacidade, confiar neles para não permitir que ladrões de identidade suguem nossas contas.

~ Satoshi Nakamoto 11-02-2009

- O sistema de moeda fiduciária está em colapso (sempre esteve).
- Ele não é sustentável (nunca foi).
- Não há como consertá-lo (nunca haverá).

- A maioria das pessoas ainda acredita que o dinheiro é lastreado no Ouro.

- Mas não é.

- Ele não é lastreado em ouro desde 1971, quando o presidente Nixon retirou unilateralmente o mundo do padrão ouro (o Choque Nixon).

- Consulte **oqueaconteceuem1971.com** para ter uma ideia clara dos danos causados por esse fato.

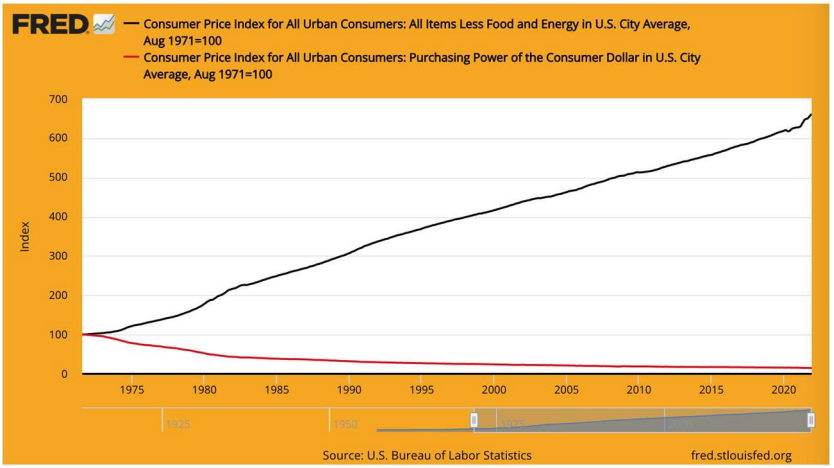


Gráfico mostrando a inflação do CPI (linha preta) versus o poder de compra do dólar (linha vermelha) desde 1971.

- **Fato Curioso:** O WEF foi criado em 1971.

Fiduciário FIAT: (substantivo) /ˈfiːˌæt/

: uma ordem autoritária ou arbitrária: DECRETO
: uma determinação autoritária: DITAR
:um comando ou ato de vontade que cria algo sem ou como se não houvesse esforço adicional

~ merriam-webster.com/dictionary

FIAT: do latim fieri "ser feito, vir a existir"

- Fiat é um dinheiro que tem valor apenas porque o governo diz que tem.
- Portanto, as pessoas têm de acreditar que sim.
- **Mesmo que não acreditem que a moeda fiduciária tenha valor, por lei são obrigados a usá-la e a aceitá-la como pagamento de bens e serviços.**
- **O dinheiro fiduciário é impresso/criado do nada.**
- Atualmente, 3% de todos os dólares são impressos como dinheiro em espécie.
- Os outros 97% são criados por bancos que inserem números em um computador (não estou brincando!), quando emitem empréstimos.

Custa apenas alguns centavos para a Casa da Moeda Americana gravar e imprimir uma nota de US$ 100
~ Barry Eichengreen, Economista Americano

***Scott Pelley, do programa '60 Minutes' da NBC**: É justo dizer que você simplesmente inundou o sistema com dinheiro?*
***Presidente do Fed, Jerome Powell:** Sim. Nós o fizemos. Essa é outra maneira de pensar sobre isso. Nós o fizemos.*
***Pelley**: De onde ele (o dinheiro) vem? Vocês simplesmente o imprimem?*
***Powell**: Nós o imprimimos digitalmente. Portanto, como um banco central, temos a capacidade de criar dinheiro digitalmente. E fazemos isso comprando títulos do Tesouro ou outros títulos garantidos pelo governo. E isso de fato aumenta a oferta de moeda. Também imprimimos moeda de fato e a distribuímos por meio dos bancos do Federal Reserve.*

~ Entrevista'60 Minutes' da CNBC, 17 de maio de 2020
Dois meses após o início do lockdown da C*vid-19

Realmente não há limites para o que podemos fazer com esses programas de empréstimo que temos.
~ Presidente do Fed, Jerome Powell

Sim, há uma quantidade infinita de dinheiro no Federal Reserve. Faremos o que for necessário para garantir que haja dinheiro suficiente no sistema bancário.
~ Neel Kashkari, Presidente do Fed de Minneapolis

O "nós" aqui são cinco pessoas votando em mudanças na política monetária dentro do sistema do Federal Reserve durante as reuniões do FOMC. 5 de 330.000.000. Isso é tudo o que é necessário para mudar a política monetária dos EUA.
~ @MartyBent, fundador da TFTC.io

CITAÇÕES NOTÁVEIS

O banco se beneficia de juros sobre todo o dinheiro
que ele cria a partir do nada.
~ William Paterson, 1694, fundador do Banco de Inglaterra

Todas as perplexidades, confusões e aflições nos Estados Unidos
decorrem, não dos defeitos da Constituição ou da Confederação,
não da falta de honra ou virtude,
mas sim da ignorância absoluta
da natureza da moeda, do crédito e da circulação.
~ John Adams
2° Presidente dos Estados Unidos, 1735-1826

Acredito que as instituições bancárias são mais
perigosas para as nossas liberdades do que os exércitos
permanentes.
Já criaram uma aristocracia monetária
que colocou o governo em desacordo.
O poder de emissão deve ser retirado aos bancos e devolvido ao
povo a quem pertence.
~ Thomas Jefferson
3° Presidente dos Estados Unidos, 1801-1809

Enquanto nos vangloriávamos de nossos nobres feitos, tivemos o
cuidado de ocultar o fato desagradável de que, por meio de um
sistema monetário iníquo, nacionalizamos um sistema de opressão
que, embora mais refinado,
não é menos cruel do que
o antigo sistema de escravidão de bens móveis.
~Horace Greeley (1811-1872)
Congressista dos EUA e fundador do The New York Tribune

Quem controla o volume de dinheiro em qualquer país é o senhor absoluto de toda a indústria e comércio...
Quando você perceber que todo o sistema é facilmente controlado, de uma forma ou de outra, por alguns homens poderosos no topo, não será preciso dizer como períodos de inflação e depressão se originam.
~ James A. Garfield,
20° Presidente dos EUA, março a setembro de 1881
Assassinado em 1881

Atualmente, existe um poder descontrolado nas mãos de um grupo de homens para fazer dólares a partir do nada.
~ Thomas W. Lawson, Frenzied Finance, 1905

Eu era tão reservado - de fato, tão furtivo - quanto qualquer conspirador. Sabíamos que a descoberta simplesmente não deveria acontecer, caso contrário, todo o nosso tempo e esforço seriam desperdiçados. Se fosse revelado que nosso grupo específico havia se reunido e redigido um projeto de lei bancária, esse projeto não teria nenhuma chance de ser aprovado pelo Congresso.
~ Frank A.Vanderlip
Presidente do National City Bank de New York
(precursor do Citi Bank)
~ Escrevendo em 1935 sobre a reunião secreta que ocorreu em Jekyll Island em 1910, para redigir o projeto de lei que foi aprovado como Federal Reserve Act em 1913.

Essa lei (do Federal Reserve) estabelece o mais gigantesco trust do mundo. Quando o presidente (Woodrow Wilson) assinar o projeto de lei, o governo invisível do Poder Monetário será legalizado... O pior crime legislativo de todos os tempos é perpetrado por esse projeto de lei bancário e monetário.
~ Charles A. Lindbergh, Sr. (1859-1924)

Sou um homem muito infeliz. Sem querer, arruinei meu país. Uma grande nação industrial é controlada por seu sistema de crédito. Nosso sistema de crédito é concentrado. Portanto, o crescimento da nação e todas as nossas atividades estão nas mãos de poucos homens. Acabamos nos tornando um dos governos mais mal-governados, um dos mais completamente controlados e dominados do mundo civilizado. Não mais um governo de livre opinião, não mais um governo por convicção e pelo voto da maioria, mas um governo pela opinião e pela coação de um pequeno grupo de homens dominantes.

~ Woodrow Wilson,
28° Presidente dos Estados Unidos, 1913-1921
6 anos após a aprovação do Federal Reserve Act de 1913.

A verdade real da questão é, como você e eu sabemos, que um elemento financeiro nos grandes centros é o dono do governo dos EUA desde os dias de Andrew Jackson.

~ Franklin D. Roosevelt, 32° presidente dos EUA
em uma carta escrita em 21 de novembro de 1933 ao Coronel E. Mandell House

Ela [a depressão] não foi acidental. Foi uma ocorrência cuidadosamente planejada.... Os banqueiros internacionais procuraram criar uma condição de desespero aqui para que pudessem emergir como os governantes de todos nós.

~Louis T. McFadden, congressista (assassinado em 1936) Graham
Presidente do Comitê Bancário e de Moeda da Câmara

Toda vez que um banco faz um empréstimo, é criado um novo crédito bancário - novos depósitos - dinheiro novo em folha.

~ Graham F.Towers
Gov. do Central Bank do Canada, 1934-55

Se não houvesse dívidas em nosso sistema monetário,
não haveria dinheiro algum.
~ Marriner Eccles, 1941, Gov. do Fed

Ainda não encontrei ninguém que pudesse, por meio do uso da lógica e da razão, justificar o empréstimo do governo federal para o uso de seu próprio dinheiro...
Acredito que chegará o momento em que as pessoas exigirão que isso seja mudado. Acredito que chegará o momento neste país em que eles realmente culparão você, eu e todos os outros ligados ao Congresso
por ficarmos de braços cruzados e permitirmos um sistema tão idiota continue.

~Wright Patman, congressista democrata de 1928 a 1976, presidente do Comitê de Bancos e Moedas de 1963 a 1975

Quando você ou eu emitimos um cheque, deve haver fundos suficientes em nossa conta para cobrir o cheque, mas quando o Federal Reserve emite um cheque, não há nenhum depósito bancário sobre o qual esse cheque seja sacado. Quando o Federal Reserve emite um cheque, ele está criando dinheiro.
~ Banco da Reserva Federal de Boston
"Putting It Simply", 1984

- O Fed é o banco central "independente" dos EUA. Ele foi criado em 1913 com a aprovação da Lei da Reserva Federal.
- **Ele tem uma estrutura única, parte privada e parte governamental.**
- Supõe-se que seja uma entidade politicamente independente e não partidária dentro do governo.
- Embora o Conselho de Governadores do Fed seja nomeado pelo Presidente e confirmado pelo Congresso, **as decisões do Fed não precisam ser ratificadas por ninguém. Sim, é confuso!**

Ele é composto por:

- O Conselho de Governadores do Federal Reserve
- 12 Bancos do Federal Reserve
- O Comitê Federal de Mercados Abertos (FOMC), que é o órgão responsável pela política monetária.

O Fed é responsável por:

- Supervisionar a política monetária dos EUA, promovendo emprego e preços estáveis.
- Regulamentar e supervisionar instituições bancárias e financeiras.
- Prestar serviços de pagamento a instituições financeiras.
- Promover a proteção ao consumidor e o desenvolvimento comunitário.

O presidente do Federal Reserve também se encarrega de:

- Presidir o Comitê Federal de Mercado Aberto (FOMC), que decide sobre a direção da política monetária dos política monetária dos EUA (por exemplo: QE, aumento das taxas de juros)
- É membro do Fundo Monetário Internacional, o FMI
- É membro do Bank for International Settlements, o BIS (Banco de Compensações Internacionais).
- É o ministro das finanças do G-7
- É o ministro das finanças do G-20

É **muito** poder para uma só pessoa!

- **Banco de reservas fracionárias:** Até março de 2020, os bancos eram obrigados a manter uma reserva de 10% e podiam emprestar 90%.

- **A partir de março de 2020, não há exigência de reserva, permitindo que os bancos emitam empréstimos ilimitados (!!!).**

- Um empréstimo é dinheiro baseado em dívida, e você precisa pagar juros sobre o empréstimo.

- **Fato curioso 1:** O dinheiro para pagar os juros do empréstimo NÃO é criado pelos bancos.

- **Fato curioso 2:** Este NUNCA é criado.

- **Fato curioso 3:** NÃO HÁ DINHEIRO SUFICIENTE no mundo para pagar todos os empréstimos + os juros devidos sobre esses empréstimos.

- **Fato curioso 4:** Nunca haverá!

- Pode-se dizer que, **até 1971, o dólar era lastreado em ouro e, desde 1974, é lastreado em petróleo e, por padrão, nas Forças Armadas dos EUA.**

- **Em 1974, os EUA e a Arábia Saudita firmaram acordos bilaterais para fixar o preço de venda do petróleo em dólares americanos.**

- Desde então, a maioria das vendas globais de petróleo tem sido liquidada em dólares americanos.

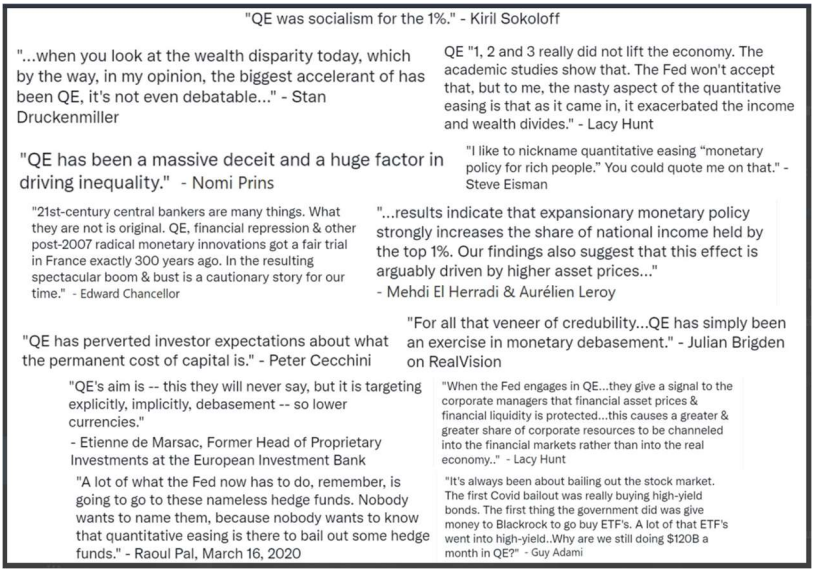
- Isso contribuiu muito para que o dólar se tornasse a moeda mais forte do mundo.

- **Assim, ele foi artificialmente sustentado,** mesmo em épocas em que normalmente teria enfrentado dificuldades.

- Enquanto eu escrevia este texto, as coisas estavam se deteriorando rapidamente, pois a invasão russa na Ucrânia estava esquentando, e a Rússia e a China estavam fazendo acordos de petróleo em rublo/yuan, deixando de usar o dólar.

- É muito provável que esse possa ser o início do fim do petrodólar. Resta saber o que acontecerá em seguida...

- **O Quantitative Easing é considerado uma "política monetária não convencional" usada pelos bancos centrais para "estimular a economia", por meio da qual o Fed compra títulos do governo e outros títulos públicos.**
- Ela foi usada pela primeira vez pelo Japão entre 2001 e 2006. Depois disso, os EUA, o Reino Unido e a zona do euro usaram o QE durante a crise financeira de 2008.
- Desde então, a única vez que os EUA não tiveram um programa de QE foi entre 2014 e 2019.
- Como visto abaixo, **os críticos afirmam que o QE beneficia principalmente os já ricos.**



Créditos: @RudyHavenstein no Twitter

- **Em toda a natureza, há ciclos, fluxos e refluxos naturais, expansões e contrações.**

- Isso **contribui para o equilíbrio e a sustentabilidade geral, ao longo do tempo, de todo o sistema interconectado,** de toda a vida na Terra.

- **O sistema de moeda fiduciária, baseado em dívidas, ignora a sabedoria dos ciclos naturais** e, em vez disso, baseia-se e depende 100% de sua sobrevivência em um crescimento sem precedentes e não mitigado para continuar pagando suas dívidas.

- Na natureza, isso é um câncer.

- Na "economia", essa trajetória antinatural é ainda mais apoiada pelo governo, que socorre bancos e grandes empresas falidas, em vez de permitir que elas se desfaçam e sejam recicladas em algo novo, algo mais saudável.

- **A miopia de socorrer empresas falidas está colocando toda a economia em risco.** Em essência, está apenas chutando a lata pela estrada, e a inevitável turbulência que está por vir provavelmente será muito, muito mais intensa do que se fosse permitido que os ciclos naturais se desenrolassem.

- **Estamos em dívida com Satoshi Nakamoto e com os cypherpunks antes e depois dele**, por terem a visão, a previsão, a determinação e a habilidade de fornecer um bote salva-vidas para nos levar a novas praias.

- Quando percebermos a dádiva que isso representa, caberá a nós embarcar, com o coração cheio e a mente limpa, para fazer a viagem e construir um novo mundo com o Dinheiro da Paz.

- **O Bitcoin conserta o dinheiro, cabe a nós consertar o resto. E, para deixar claro, ao consertar o dinheiro, MUITAS outras coisas serão consertadas, por padrão.**

- A principal delas é que a guerra cinética em larga escala, iniciada pelo governo, não será mais lucrativa ou possível sem o apoio das pessoas.

- Além disso, haverá naturalmente menos consumo, juntamente com uma mudança para bens e serviços de valor real, mercados livres, poupança real e desmonetização de moradias e imóveis, que nunca foram feitos para serem monetizados.

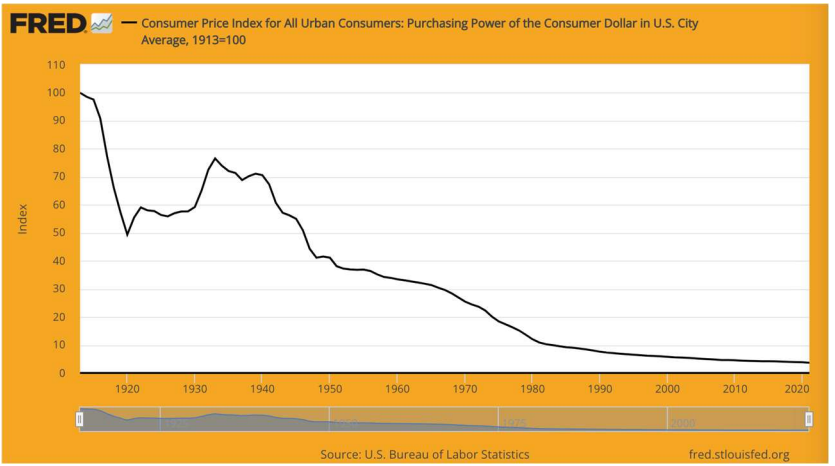


Gráfico que mostra o declínio do poder de compra do dólar desde a a formação do Federal Reserve em 1913. A taxa de inflação acumulada desde 1913 é de cerca de 2.525,4%. Todas as moedas fiduciárias dos bancos centrais estão seguindo uma taxa de declínio semelhante.

- **Quanto mais dinheiro é criado do nada, mais o dinheiro perde valor.**

- Isso é chamado de **inflação**.

- A inflação é um **roubo de tempo**, literalmente. O valor do seu tempo é roubado quando você o economiza em uma moeda que é inflacionada e manipulada.

- A inflação também é um **imposto oculto**.

- Esse roubo de tempo e esse imposto também afetam as moedas fiduciárias de todos os outros países, já que todas elas estão atreladas ao dólar americano,

que tem sido a moeda de reserva mundial desde o acordo de Bretton Woods em 1944.

- **Nos EUA, uma taxa de inflação anual de 2% está prevista no mandato do Federal Reserve.**

- Isso significa que **você tem a GARANTIA de poder comprar 2% MENOS** com a mesma nota de US$ 20 a cada ano.

- **Em fevereiro de 2022, a taxa de inflação anual foi de 7,9%** (muito mais do que 2%), o que significa que você perdeu 7,9% do seu poder de compra no ano passado.

- Em outras palavras, isso significa que, em média, o preço das coisas subiu 7,9%.

- Portanto, se uma cesta de mantimentos custou US$ 50 em 2021, a mesma cesta custou US$ 53,95 em 2022.

- **Se a inflação fosse medida com precisão, como era feito até o início da década de 1980, ela estaria, na verdade, mais próxima de 15% agora em 2022, e sua cesta de compras custaria US$ 57,50.**

- **Quando analisada por categoria, é possível ver que a inflação é, na verdade, muito pior do que 7,9% em muitas categorias no último ano:**

- Energia - 25.6%
- Gasolina - 38%
- Veículos novos - 12.4%
- Carros e caminhões usados. - 41.2
- Alimentos - 7.9% (o maior desde Julho de 1981)

Inflação média nos últimos 50 anos nos EUA:

Custo Médio	1971	2021	% Increase
Salário	$9,400	$53,400	469%
Residência	$23,400	$408,000	1,643%
Galão de Gasolina	$0.36	$3.60	1,000%
Carro Novo	$3,400	$39,000	1,047%
Diploma Universitário	$1,400	$26,000	1,757%
Cesta Básica	$20	$133	565%
Eletricidade/kWh	$0.02	$0.14	600%

História real:

~ Uma casa foi comprada em 1976 por US$ 58.000.

~ Ao contabilizar a inflação "oficial", esse valor seria de US$ 279.000 em dólares de 2022.

~ Em 2022, a mesma casa foi recentemente avaliada em US$ 2,09 milhões.

~ Pondere isso...

- **À medida que a inflação aumenta, suas economias (se você tiver a sorte de ter economias) perdem valor.**

- Com o tempo, elas perdem MUITO valor.

- Se você começasse a poupar US$ 100/mês hoje, com a melhor taxa de juros disponível de 0,05%:
  - Em 30 anos, você teria economizado US$ 84.019.

- Quando ajustado para a inflação de 2% exigida pelo FED:
  - Em 30 anos, sua poupança teria um **poder de compra efetivo** de apenas US$ 46.384.

- Ajustando pela inflação "real" de 7% de hoje:
  - Suas economias no valor de US$ 84.019 teriam o poder de compra de apenas US$ 11.037 em 30 anos!

- **De fato, isso significa que ~seis de cada sete horas de seu trabalho foram roubadas = *Roubo de tempo.***

Outra maneira de ver isso é a seguinte:

- Em 1971, o custo de uma casa = 2,5 vezes o salário médio anual.
- Em 2021, o custo de uma casa = 8 vezes o salário médio anual.

- Em 1971, um carro novo custava cerca de 1/3 de um salário médio.
- Em 2021, um carro novo custa quase 2/3 de um salário médio.

Acredito que agora esteja
claro que inflação
não
trabalha a seu favor.

Observação: todos esses números são médias e variam de acordo com muitos fatores. O que importa é que a inflação disparou e não mostra sinais de desaceleração, graças à contínua impressão de dinheiro. A inflação é um imposto oculto e um roubo de tempo de nosso trabalho e produção reais.

Dinheiro de verdade resolve isso.

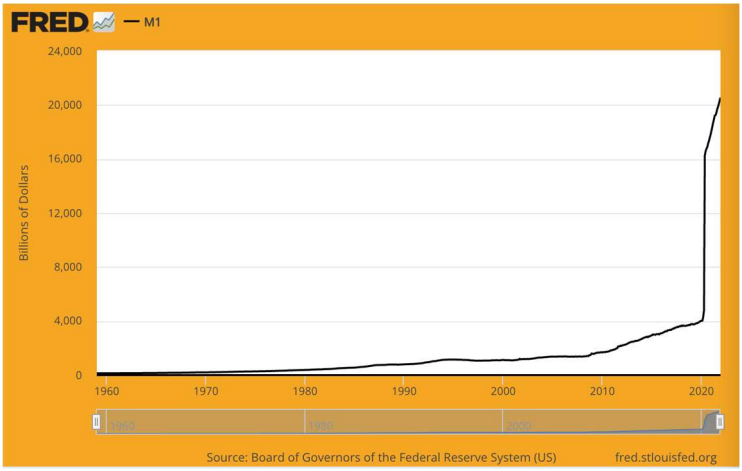
Bitcoin é dinheiro de verdade.

NÓS PRECISAMOS DO bitcoin PARA SUBSTITUIR A ECONOMIA CENTRALIZADA, MANIPULADA E BASEADA EM DIVÍDAS

Acredito que nunca mais teremos um bom dinheiro antes de tirá-lo das mãos do governo, ou seja, não podemos tirá-lo violentamente das mãos do governo, tudo o que podemos fazer é, de alguma forma, introduzir algo que eles não possam impedir.

~ Friedrich Hayek

~ Economista austríaco, filósofo e autor



Graph Gráfico mostrando o aumento da oferta monetária M1 de US$ 4 trilhões para mais de US$20 trilhões desde março de 2020!

- **Exploda sua mente aqui:** https://usdebtclock.org/

- **45% de todos os dólares americanos existentes foram impressos nos últimos 21 meses, de abril de 2020 a janeiro de 2022!**

- Ou seja, impressos do nada, lembra-se?

- O dinheiro fiduciário é controlado centralmente pelo Estado, e a oferta é facilmente manipulada.

- **Foram necessários 205 anos para que a dívida nacional dos EUA chegasse a US$ 1 trilhão. (1776 > 1981)**

- Foram necessários apenas **mais 31 anos para** que a dívida nacional dos EUA **chegasse a US$ 30 trilhões!** (1981 > 2022)

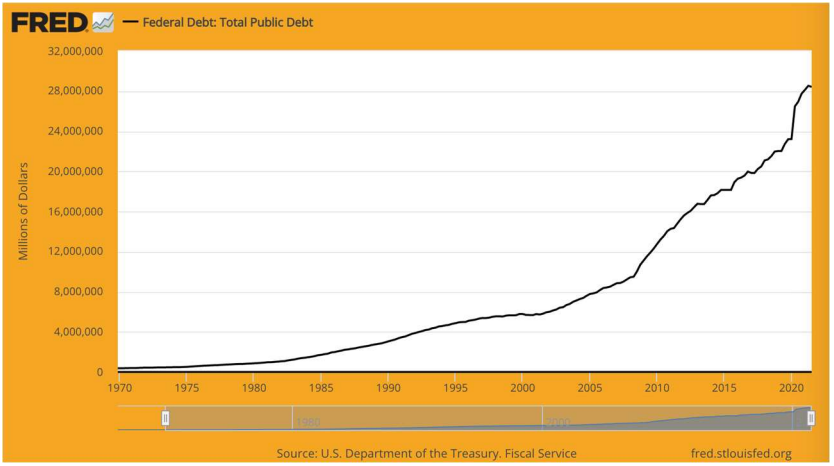


Gráfico mostrando a Dívida Pública Total 1970-2021 nos EUA.

A dívida global, medida pelo Institute of International Finance, agora totaliza US$ 303 TRILHÕES. Este é o nosso planeta com base em dívidas fiduciárias. A propósito, o PIB global é de apenas US$ 84 trilhões.

~ Nik Bhatia, Autor de "Layered Money", 2021

- **Para referência:**

Se você tiver:	**Você pode gastar $1/minuto**	
$1 Milhão	por 11 dias	= 11 dias
$1 Bilhão	por 11,680 dias	= 32 anos
$1 Trilhão	por 11,680,000 dias	= 32,000 anos

- Estamos todos à mercê daqueles que têm o poder de decidir quando imprimir mais e quais taxas de juros cobrar.

- **Se o Fed aumentar as taxas de juros, conseguir um empréstimo para comprar uma casa ou um carro se tornará subitamente mais caro, o que reduzirá os gastos, levando à estagflação**

- **Se eles mantiverem as taxas artificialmente baixas, entraremos em um período de depressão**

- **Permitir que o banco central crie o "clima" financeiro tira nossa liberdade de deixar o mercado decidir o que tem valor e o que não tem.**

- Além disso, **quando eles socorrem os bancos e as empresas, eles sustentam artificialmente a economia.** É apenas uma questão de tempo até que o castelo de cartas caia.

- O argumento original para a existência de um banco central era a necessidade de haver um emprestador de última instância quando a economia oscilasse.

Isso fez com que o banco central se tornasse um governante de primeira instância, com poder incomparável, não eleito e, em última instância, autoritário.

Todo dinheiro é político, exceto o Bitcoin. Moedas fiduciárias, instrumentos bancários, créditos de fintech, outras criptomoedas e até mesmo o ouro são todos controlados por governos, corporações ou pequenos grupos. Ter uma exceção se mostrará muito útil à medida que nos aproximamos do futuro.

~ Alex Gladstein @gladstein
Diretor de estratégia da Human Rights Foundation

O Bitcoin conecta 8 bilhões de pessoas, conecta cem milhões de empresas, sincroniza o mundo entre jurisdições políticas, devolve a racionalidade a todo o sistema financeiro e devolve a liberdade e os direitos de propriedade a toda a raça humana.

~Michael Saylor, CEO da Microstrategy

NÓS PRECISAMOS DO bitcoin PARA BANCARIZAR OS DESBANCARIZADOS

Para 953 milhões de pessoas em 20 países com moedas enfraquecidas, o Bitcoin representa algo maior do que um ativo de tesouraria. Para elas, é mais como uma arca de energia criptografada para escapar do dilúvio.

~ Michael Saylor
CEO da Microstrategy

- **Aproximadamente 30% dos adultos no mundo não têm conta bancária, cerca de 1,9 bilhão de pessoas!**

- **Isso significa que eles não têm acesso a serviços bancários e não podem usar caixas eletrônicos, cartões de débito, cartões de crédito ou cheques.**

- **Além disso, não podem obter empréstimos para iniciar um negócio, comprar um carro ou uma casa etc.**

- **Enviar e receber dinheiro, ou descontar cheques, é caro.**

- Elas precisam usar serviços de transferência de dinheiro e de desconto de cheques, como a Western Union, que cobram taxas altas e levam tempo para serem processados.

- É **extremamente caro para as pessoas que enviam dinheiro para suas famílias** em outros países (remessas), que podem custar até 10%.

- É **caro e demorado para as pessoas que recebem remessas,** pois elas precisam pagar pelo transporte e ir até o escritório de transferência de dinheiro, muitas vezes longe de onde moram, para receber o dinheiro que o membro da família enviou.

- Muitas vezes, não é seguro para eles se deslocarem até esses escritórios.

- O Bitcoin, por meio da Lightning Network, oferece uma solução instantânea para esses problemas!

#bitcoin conserta isso

Quando uma tecnologia que dá poder às pessoas foi freada?

~Jeff Booth
Autor de: O Preço do Amanhã (The Price of Tomorrow)

NÓS PRECISAMOS DO bitcoin PARA AJUDAR AS PESSOAS A ESCAPAR DA TIRANIA E DO COLAPSDO DA MOEDA.

- Como vimos, nos últimos meses, mesmo em 2022, os governos podem e de fato congelam as contas bancárias daqueles com quem não concordam.

- **Isso mostra que, em essência, seu dinheiro no banco nada mais é do que um IOU que pode ser roubado de você a qualquer momento.**

- Além disso, quando a inflação é desenfreada, como estamos vendo atualmente na Venezuela, Sudão, Líbano, Síria, Argentina, Zimbábue, Turquia e outros países, as poupanças das pessoas são vaporizadas, às vezes da noite para o dia, e não há nada que elas possam fazer a respeito.

- Para as pessoas que passam por qualquer uma das situações acima, **o bitcoin se torna uma solução real e imediata para um problema que, de outra forma, seria insustentável.**

- **Considerando que tanto a tirania quanto a inflação estão aumentando em muitos lugares, seria sensato se proteger contra elas comprando bitcoin agora.**

- Você deve ter ouvido falar que **os bancos centrais estão começando a criar CBDCs, Moedas Digitais de Banco Central**. Em maio de 2020, 35 países estavam explorando essa opção.

- No momento em que este artigo foi escrito, em fevereiro de 2022, 87 países estavam ativamente procurando, ou já haviam lançado uma CBDC.

- Nos EUA, ele é chamado de Projeto Hamilton.

- **As CBDCs são muito semelhantes ao dinheiro eletrônico que você vê em sua conta bancária on-line, exceto que, por serem *nativamente digitais*, são *programáveis* e *100% controláveis*.**

> *A principal diferença com os CBDCs é que os bancos centrais teriam* ***controle absoluto*****.**
>
> ~Agustin Carstens
> GM, BIS - Bank for International Settlements (Banco de Compensações Internacionais)
> (O banco de todos os bancos)

- **Isso significa que o governo pode programar uma data de vencimento para o seu dinheiro, forçando-o a gastá-lo antes que ele expire.**

- **Ele também pode programar outras coisas,** como permitir que o dinheiro seja gasto somente em determinadas lojas, sites ou jurisdições, e não em outras.

- **Eles podem vinculá-lo a:** sua pontuação de crédito, sua ficha de saúde, ID digital e outras pontuações sociais.

- **Depois disso, eles podem programar quaisquer restrições que considerem adequadas,** com base em sua pontuação específica em uma área, ou em sua "pontuação geral", ou no que eles consideram que a "economia" precisa.

- Além disso, eles poderão monitorar tudo o que você faz com seu dinheiro.

Não sabemos quem está usando uma nota de US$ 100 hoje e não sabemos quem está usando uma nota de 1.000 pesos hoje. A principal diferença com o CBDC é que ***o banco central terá controle absoluto sobre as regras e regulamentos que determinarão o uso dessa expressão de responsabilidade do banco central, e também teremos a tecnologia para impor isso.***

~Agustin Carstens
GM, BIS - Bank for International Settlements (Banco de Compensações Internacionais)

- **Observação:** Dizer "**essa expressão de responsabilidade do banco central**" implica que seu valor, sua força vital, armazenada como dinheiro, é na verdade "propriedade" do banco central. (Hum, não!)

- **O Bitcoin arranca, pela raiz, o maior problema que enfrentamos: a mentira das moedas Fiat.**

- Essa é a mentira da moeda fiduciária corrompida, da usura e de tudo o que vem com ela para roubar seu tempo e, ao mesmo tempo, enriquecer enormemente as pessoas mais próximas de quem imprimi o dinheiro. (conhecido como Efeito Cantillon).

- **A mentira da moeda fiduciária** é como uma **erva daninha gigante e monstruosa** em seu jardim, sugando todos os nutrientes do solo, **matando** todo o micélio e **bloqueando** a luz do sol, de modo que as outras plantas não conseguem se desenvolver e estão lutando para sobreviver.

- De repente, quando essa erva daninha nociva e monstruosa da mentira da moeda fiduciária desaparece, a Verdade entra!

- Todas as plantas (**as pessoas**) podem começar a se recuperar
- O solo (**que é a criatividade das pessoas, bens e serviços reais**) pode se regenerar.
- O micélio (**que é a conexão autêntica entre as pessoas**) se regenerará.
- E a luz do sol (**força vital não mediada**) brilhará mais uma vez sobre todos nós!

- Isso não é uma piada. A hashtag **#bitcoinconsertaisso** é um meme recorrente no BT (Bitcoin Twitter), por um bom motivo.

- Embora isso possa parecer um tanto "grandioso", deixe-me explicar. Quando se considera a "forma como as coisas estão", mesmo antes de 2020, **qualquer pessoa poderia, e ainda pode, ver que "algo está muito errado".**

- Destruição desenfreada, degradação ambiental, famílias e comunidades divididas, perda de culturas, idiomas, tradições, aumento da pobreza, concentração maciça de riqueza nas mãos de (muito) poucos, consumo excessivo, dinheiro infinito apoiando políticos, falta de alimentos e água potável para milhões, obesidade e doenças autoimunes cada vez maiores, guerras aparentemente intermináveis...

- Poderíamos pensar que, com o crescimento exponencial de ONGs, organizações sem fins lucrativos, fundações de caridade e as chamadas instituições apoiadas pelo governo, esses problemas estariam se tornando menos graves.

- Em vez disso, **eles estão se tornando mais graves.**

bitcoin CONSERTA ISSO

INCLUSÃO FINANCEIRA

- **Com o bitcoin, todos têm acesso ao mesmo sistema financeiro, com as mesmas regras para todos.**

- Não há brechas, backdoors ou acordos especiais para ninguém.

- Todos têm a possibilidade de serem compensados pelo valor que fornecem com o mesmo dinheiro real, criado e mantido com as mesmas regras.

- **O Bitcoin é acessível a qualquer pessoa, em qualquer lugar, com uma conexão à Internet.**

AGREGANDO VALOR AO MUNDO

- **O Bitcoin incentiva as pessoas a agregarem valor real à comunidade e ao mercado, pois essa é a única maneira de ganhar mais dinheiro.**

- Se alguém estiver satisfeito com menos, ainda assim se beneficiará trabalhando por um salário justo e, **quando economizar, essa economia manterá seu valor ao longo do tempo.**

MEIO AMBIENTE

- A moeda sólida, com uma oferta limitada, cria uma dinâmica muito diferente da que vemos hoje.

- Em vez de um impulso imparável para consumir cada vez mais, em uma corrida para o fundo do poço para pagar taxas de juros crescentes sobre empréstimos e dívidas que, em última análise, nunca serão pagas, o **bitcoin oferece uma saída para um mundo em que se busca ter uma baixa preferência temporal**.

- **A destruição ambiental desenfreada é substituída por menos consumo, menos desperdício e uma abordagem ponderada da produção, em que o mercado decide o que tem valor real e, portanto, as coisas são feitas para durar.**

- Esse é um benefício real para as pessoas, plantas e animais!

GUERRAS

- O sistema de moeda fiduciária é o que torna possíveis e lucrativas as "guerras eternas". Como as pessoas, em sua maioria, não sabem como funcionam os gastos de guerra ou de onde vem o dinheiro para a guerra, há pouca ou nenhuma responsabilidade por parte do governo. As guerras podem se arrastar por anos em lugares remotos, sem nenhuma supervisão real.
- A partir do Vietnã, as guerras se tornaram "guerras de cartão de crédito" (h/t @AlexGladstein), uma vez que o governo toma dinheiro emprestado para financiar as guerras e depois toma mais dinheiro emprestado para pagar os juros dos empréstimos iniciais.
- **Em um padrão bitcoin, seria necessário que a população de um país estivesse disposta a ajudar a pagar por uma guerra. Provavelmente só o fariam se fosse absoluta e claramente necessário, para defender sua família e seu país, com um objetivo final em mente.**
- Como não haveria lucros indevidos a serem obtidos, as autoridades governamentais e as empresas não seriam incentivadas a promover ou se envolver em guerras como uma opção viável.
- **Em vez disso, os esforços aumentariam muito para encontrar maneiras de chegar a resoluções pacíficas e de baixo custo.**

PREFERÊNCIA TEMPORAL

- A alta preferência temporal leva à destruição pessoal, social e ambiental. Quando nosso dinheiro está perdendo valor a cada dia, somos "forçados" a gastá-lo o mais rápido possível, antes que perca mais valor. Quando nosso tempo é desvalorizado por uma moeda fiduciária em constante inflação, perdemos a conexão com o valor do nosso tempo.

- Isso leva à desconexão e a uma corrente subterrânea de estresse.

- As tentativas de aliviar o estresse e encontrar significado são distorcidas e se transformam em distrações, como o consumo excessivo de drogas, álcool, compras, pornografia, fast food, déficit de atenção, dependência de telas/mídias sociais etc.

- **Por outro lado, o dinheiro de verdade, que mantém seu valor ao longo do tempo e mede adequadamente nossas contribuições por meio de nosso trabalho, leva a uma baixa preferência temporal, a uma qualidade de vida atenciosa, com relacionamentos significativos, menos consumo, conexões mais profundas, conversas mais profundas e maior criatividade.**

O QUE É bitcoin ?

"Escrever uma descrição para essa coisa para o público em geral é muito difícil. Não há nada com que relacioná-la."

~ Satoshi Nakamoto 05-07-2010

A circulação total será de 21.000.000 de moedas. Elas serão distribuídas aos nós da rede(mineradores) quando eles criarem blocos, com a quantidade cortada pela metade a cada 4 anos. Primeiros 4 anos: 10.500.000 moedas próximos 4 anos: 5.250.000 moedas próximos 4 anos: 2.625.000 moedas próximos 4 anos: 1.312.500 moedas etc... Quando isso se esgotar, o sistema poderá suportar taxas de transação, se necessário. Ele se baseia na concorrência de mercado aberto, e provavelmente sempre haverá nós dispostos a processar transações gratuitamente.

~ Satoshi Nakamoto 01-09-2009

- **O Bitcoin é dinheiro da liberdade...** no sentido de que tem o potencial de nos libertar da manipulação abrangente e do controle do sistema bancário central.

- **No bitcoin, as regras monetárias são as mesmas para TODOS, EM TODOS OS LUGARES.**

- O Bitcoin é inclusivo, no sentido de que qualquer pessoa com uma conexão à Internet pode participar da rede e precisa seguir as mesmas regras.

bitcoin é:

- **DESCENTRALIZADO**
- **VERDADEIRAMENTE ESCASSO**
- **RESISTENTE À CENSURA**
- **UM LIVRO RAZÃO DISTRIBUÍDO**
- **INCORRUPTÍVEL**
- NÃO NECESSITA DE PERMISSÃO
- AUDITÁVEL
- TRANSPARENTE
- IMUTÁVEL
- SEM FRONTEIRAS
- DIFÍCIL DE SER FALSIFICADO
- PSEUDÔNIMO
- SEM FRICÇÃO
- SEM TERCEIROS DE CONFIANÇA
- DE PESSOA PARA PESSOA (P2P)

Esse grupo de cinco propriedades propriedades distinguem o bitcoin de **todas** as outras criptomoedas!

- **O Bitcoin é descentralizado.**
- **Ele é executado em milhares de nós em todo o mundo, por milhares de pessoas que não se conhecem.**
- Nenhuma pessoa, governo ou empresa pode controlá-lo.
- Você também pode administrar um nó, é fácil ;)
- Ao administrar seu próprio nó, você ajuda a proteger a rede e, ao mesmo tempo, tem a capacidade de verificar suas próprias transações.

Não confie. Verifique.

- **O Bitcoin (‘B’ maiúsculo)** é uma rede monetária.

- **bitcoin (letra ‘b’ minúscula),** é a moeda ou ativo monetário emitido e executado na rede Bitcoin.

O Bitcoin é o grande incentivador.

A genialidade de Satoshi foi tal que, no bitcoin, pela primeira vez, tanto os bons quanto os maus atores são incentivados a seguir as regras.

"O incentivo pode ajudar a encorajar os os nós a permanecerem honestos. Se um invasor ganancioso conseguir montar mais CPU proof-of-worker do que todos os nós honestos, ele terá que escolher entre usá-la para fraudar as pessoas, roubando seus pagamentos, ou usá-la para gerar novas moedas. Ele deve achar mais lucrativo seguir as regras, regras essas que o favorecem com mais moedas novas do que todos os outros juntos, do que minar o sistema e a validade de sua própria validade de sua própria riqueza."

~ Satoshi Nakamoto 31-10-2008

- **O Bitcoin é o primeiro *dinheiro digitalmente nativo*.**
- Ao contrário de sua conta corrente on-line, que é apenas uma forma fiduciária digital do banco central.
- O Bitcoin é uma moeda digital **descentralizada**.
- O Bitcoin não tem **autoridade central**.
- A Bitcoin é **apátrida**.
- Considere as implicações...

O Bitcoin é uma moeda digital descentralizada que permite pagamentos instantâneos a qualquer pessoa, em qualquer lugar do mundo. O Bitcoin usa tecnologia ponto a ponto para operar sem autoridade central: o gerenciamento de transações e a emissão de dinheiro são realizados coletivamente pela rede.

~ Bitcoin Wiki
en.bitcoin.it

- O Bitcoin é o dinheiro mágico da Internet.
- Não, é sério, o **Bitcoin é a forma como vamos consertar o mundo.**
- Sério? Sim.

- **O Bitcoin é uma forma de transferir valor**
- seja o valor que for
- de forma segura
- instantaneamente (via Lightning Network)
- entre duas partes
- a qualquer momento
- 24/7
- em qualquer lugar
- sim, em qualquer lugar
- pense sobre isso.

> *Com a moeda eletrônica baseada em prova criptográfica, sem a necessidade de confiar em um terceiro intermediário, o dinheiro pode ser seguro e as transações sem esforço.*
>
> ~ Satoshi Nakamoto 11-02-2009

O Bitcoin é (quase) sem custo para ser movimentado, com certeza. Eu sei com 100% de certeza o que estou recebendo.

~ Michael Saylor CEO da Microstrategy

- Você pode enviar US$ 1,13, ou 46c ou 359 sats ou 500.000.000 sats ou US$ 1 milhão para qualquer pessoa, em qualquer lugar, a qualquer momento... instantaneamente e quase de graça, por meio da Lightning Network, criada com base no Bitcoin.

- **E ninguém pode impedi-lo.**

- Você pode fazer isso com ouro, prata, USD/GBP/EUR/YEN/CYK/ZAR ou qualquer outra moeda fiduciária do banco central? (Não)

- **O Bitcoin é histórico**. Esta é a primeira vez na história que um sistema monetário verdadeiramente descentralizado, resistente à censura, imutável, sem fronteiras, sem permissões e incorruptível com um limite máximo absoluto (21 milhões de moedas) criado.

- O Bitcoin é **tão importante para descentralizar o poder e aumentar a inclusão financeira** quanto a invenção da prensa tipográfica e, posteriormente, da World Wide Web, **foi para descentralizar e aumentar o acesso à informação**.

Muitas pessoas descartam automaticamente a moeda eletrônica como uma causa perdida por causa de todas as empresas que faliram desde a década de 1990.
Espero que seja óbvio que foi apenas a natureza de controle centralizado desses sistemas que as condenou.
Acho que esta é a primeira vez que estamos experimentando um sistema descentralizado e não baseado em confiança.

~ Satoshi Nakamoto 15-02-2009

- **O Bitcoin é um livro-razão distribuído, descentralizado, transparente e imutável.**

- Isso significa simplesmente que é uma maneira pela qual qualquer pessoa no mundo pode ver quem possui o quê, a qualquer momento, e isso não pode ser alterado.

- Só que o "quem" não é um nome, é um endereço composto de números e letras.

- Um exemplo de um endereço de bitcoin:

  `bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf5mdq`

- **Portanto, o Bitcoin é pseudônimo.**

Bitcoin é

- um emissor imparcial de ativos
- uma reserva de valor
- um meio de troca
- e em breve será uma unidade de conta
- ***bem como***
- ***o meio de troca.***

É o emissor, o ouro, o dinheiro, o cartão de débito E o paypal, o banco, venmo, cashapp, western union

TUDO EM UM SÓ!

- **O Bitcoin é um detentor de registros que usa matemática e ciência da computação, em vez de banqueiros, contadores e contabilistas.**

- Ele elimina os intermediários, bancos, governos, taxas de cheque especial, taxas de conta corrente, horário de atendimento limitado, possibilidade de censura, contas congeladas, manipulação da oferta de moeda, taxas de juros, FMI, WEF, prédios físicos, caixas eletrônicos, cheques, corrupção, usura, petrodólar, eurodólar, senhoriagem bancária, títulos, ações, banco de reserva fracionária, visa, mastercard, amex, western union, BIS, dias de espera para que sua transferência eletrônica seja concluída.

- **Em vez de ter alguém entre você e a pessoa cuja mão você quer apertar, você pode simplesmente apertar a mão dela diretamente.**
- **Não há necessidade de pedir permissão para enviar seu próprio dinheiro!**

- Agora você pode fazer isso como, quando e onde quiser, instantaneamente, com a liquidação final ocorrendo imediatamente!

Simplificando...

- **Bitcoin é uma propriedade digital que ninguém pode tirar de você.**

- Possuir bitcoin significa ter o direito de enviar valores de um endereço específico que você controla com sua chave privada para QUALQUER outro endereço que você escolher.

> *O bitcoin é um direito de propriedade que independe do monopólio da violência.*
>
> ~ Robert Breedlove @breedlove22

- **E podemos reaproveitar dezenas de milhares de prédios bancários de tijolo e argamassa em todo o mundo para transformá-los em centros comunitários, bibliotecas, salas de concerto, estúdios de artistas e qualquer outra coisa que possamos imaginar para enriquecer e animar nossas comunidades!**

- **O Bitcoin é um evento único em uma espécie.**

- **A descoberta do Bitcoin, há 14 anos, está para a liberdade e soberania financeira humana, como a descoberta do fogo foi para o florescimento humano há mais de 500.000 anos e a prensa de impressão estava para a descentralização do acesso ao conhecimento humano há quase 900 anos.**

- Bitcoin é escolha.

- O Bitcoin **gera soberania.**

- **O Bitcoin é uma verdadeira reserva de valor.**

- Ele armazena seu recurso mais precioso, seu tempo, de forma que você possa acessá-lo novamente mais tarde.

> *O Bitcoin é como um canal de energia de alta largura de banda para o seu eu futuro... você pode trabalhar hoje e o Bitcoin congelará sua energia para uso posterior.*
>
> ~ Robert Breedlove

> *A raiz do dinheiro é o tempo*
> *E a raiz do tempo é o valor*
>
> ~ Guy Swann

- **O Bitcoin é uma cadeia de tempo,** literalmente.

- Você pode medir o tempo em blocos, já que um bloco é extraído a cada ~10 minutos.

- **Nosso tempo é nosso recurso mais escasso e precioso.**

- **Ele é literalmente nossa força vital.**

- **O Dinheiro de Verdade nos permite armazenar nosso tempo!**

- É a maneira de reconhecermos o tempo que 'gastamos'.

- Nós **Trocamos nosso tempo por dinheiro, que é simplesmente um registro de nosso tempo e esforço.**

- É mágica essa **capacidade de preservar nosso tempo de forma que tenhamos 'acesso' a ele mais tarde na vida, quando não pudermos mais trabalhar como antes.**

- **Quando a inflação ocorre, ela rouba de nós o valor do nosso tempo.**

- O Bitcoin é uma **reserva de valor.**
- O Bitcoin é um **meio de troca.**
- Um dia, o Bitcoin **será uma unidade de conta.**
- Um dia, o Bitcoin **será *A unidade de conta*.**

- **O Bitcoin é escasso.**
- Ele tem um limite máximo de 21.000.000 de moedas.
- Nunca haverá mais.
- O código é a lei aqui. *

* Embora seja "tecnicamente" possível alterar o código, a genialidade de Satoshi impede que isso aconteça, pois aumentar (inflar) a oferta só serviria para diminuir o valor de todas as moedas em circulação. Portanto, isso incentiva todos a concordarem implicitamente em manter o limite máximo de 21.000.000 de moedas.

- **O Bitcoin é infinitamente divisível.**
- Atualmente, ele é divisível até a oitava casa decimal: 1,00000000
- Há 100.000.000 satoshis em 1 bitcoin.
- 1 satoshi = ₿ 0,00000001
- Você pode comprar sats (satoshis) em qualquer valor.

- **O Bitcoin é o dinheiro mais sólido e sonante que já conhecemos.**

- É ainda mais sólido do que o ouro, já que o ouro não é facilmente divisível ou portátil, tem baixa velocidade (move-se lentamente) e não é facilmente verificável.

- **O Bitcoin tem as propriedades monetárias superiores de qualquer ativo já conhecido.**

Propriedades do dinheiro	Bitcoin	Ouro	Fiat
Verificavelmente Escasso	✓	✗	✗
Facilmente Transportável	✓	✗	✗
Verificável instantaneamente	✓	✗	✓
Facilmente Divisível	✓	✗	✓
Durável ao Longo do Tempo	✓	✓	✗
Fungível em Qualquer Lugar	✓	✓	✗
Resistente à Censura	✓	✗	✗
Difícil de falsificar	✓	✓	✗
Altamente Veloz	✓	✗	✓

O Bitcoin é o antídoto.

A tentativa de "estabilizar" a economia com resgates, impressão de dinheiro, QE e manipulação da taxa de juros é como mantê-la em um suporte de vida artificial.

Essa "máquina" só pode continuar por um certo tempo, antes de se tornar cada vez mais cara de manter e cada vez menos sustentável, levando a um sério colapso.

O Bitcoin conserta isso.

O Bitcoin é um dinheiro melhor.

- **O Bitcoin é antifrágil.**
- E se torna ainda mais a cada tentativa de ataque, a cada proibição governamental, a cada tentativa de FUD (medo, incerteza, dúvida) da mídia convencional.
- O Bitcoin nunca foi hackeado*.
- Embora muitos tenham tentado.

* Embora você possa ter ouvido falar de hacks, foram as corretoras que foram hackeadas.

Lembre-se: Se não são suas chaves, não são suas moedas
>> Sempre retire seus sats para sua **própria carteira**.
E o **melhor** é comprar peer-to-peer >> A Bisq funciona.
Vale 1000% a pena gastar tempo para aprender como!

- **O Bitcoin é uma combinação de:**
  - criptografia
  - matemática
  - networking/redes
  - teoria dos jogos
  - incentivos econômicos...
- **... que trabalham juntos para criar confiança em um ambiente descentralizado e sem confiança para dar suporte a uma moeda digital segura.**

- **Bitcoin é uma toca de coelho muito, muito profunda,** que faz com que você questione quase tudo o que achava que sabia ;)

- Bitcoin é autônomo.

- **Bitcoin simplesmente é.**

- **O Bitcoin é uma relação simbiótica** entre: humanos <-> uma solução perfeita para transferir e armazenar tempo/valor.

- Os seres humanos precisam do Bitcoin, o bitcoin precisa dos seres humanos.

- **O Bitcoin é a solução para o problema dos Generais Bizantinos.**

- Esse era considerado um problema sem solução na ciência da computação.

- Esse problema surge em sistemas descentralizados, nos quais se acreditava ser impossível provar que a mensagem enviada = mensagem recebida, já que o "homem no meio" poderia ser um mau ator e falsificar a mensagem.

- Em outras palavras, parecia impossível formar um consenso entre uma rede de computadores distribuídos e independentes.

- Ao usar o registro de data e hora junto com o livro-razão distribuído criptograficamente seguro, Satoshi resolveu esse problema.

- Sua solução é conhecida como **consenso Nakamoto**.

- **O Bitcoin é a solução para o problema do gasto duplo.**

- Isso significa que, quando você envia bitcoin, o destinatário pode ter certeza de que você realmente possui o bitcoin que enviou e que, depois de enviá-lo, você não poderá gastar essas moedas novamente enviando-as para outra pessoa (gasto duplo).

- É como se eu lhe desse uma laranja.

- Uma vez que ela sai de minhas mãos e está em suas mãos, eu não tenho mais a laranja para dar a outra pessoa.

> ... os gastos duplos nunca são aceitos no pool de transações, portanto, cada nó é testemunha de qual transação viu primeiro trabalhando para colocá-la em um bloco
>
> ~ Satoshi Nakamoto 09-12-2010

- **O Bitcoin é um ativo ao portador,** como dinheiro ou ouro, mantido diretamente pelo portador (proprietário).

- **Isso significa que, uma vez enviado (dado), ele vai diretamente para o novo portador (proprietário), sem a necessidade de um intermediário (banco) para processar a transação.**

- **Bitcoin é P2P (peer-to-peer).**
- O Bitcoin é resistente à censura.
- **Isso significa que ninguém tem o poder de atrasar ou impedir que uma transação chegue ao novo portador.**
- O Bitcoin flui livremente.
- Não precisa de guardiões.

Bitcoin é sem terceiros de confiança.

> *A raiz do problema da moeda convencional é toda a confiança necessária para que ela funcione. É preciso confiar que o banco central não vai desvalorizar a moeda, mas a história das moedas fiduciárias está repleta de violações dessa confiança.*

~ Satoshi Nakamoto sobre a importância da natureza de não necessitar de terceiros confiança no Bitcoin.

- **Bitcoin é código.**

- **Código é discurso.**

- Surpreenda-se aqui: Dê uma olhada em: **github.com/bitcoin**

- Clique para ver o código, as solicitações de pull, as revisões, os commits, dos incríveis desenvolvedores que estão trabalhando, mantendo e aprimorando a criação que é o bitcoin.

- **O Bitcoin é a Internet do dinheiro.**

- Quando se para considerar que tudo o mais está se tornando/se tornou digital, inclusive:

- música
- livros
- bancos
- filmes
- educação
- fotos
- ligações telefônicas
- mapas
- e a lista continua... para o bem e para o mal...
- … então se vê como é realmente um passo lógico para o dinheiro seguir.

(**MAS** precisamos de BITCOIN, **NÃO** de CBDCs!)

- O Bitcoin é **TUDO** a seguir
- Um **livro-razão descentralizado e distribuído**
- E um **sistema de pagamento**
- E o próprio **valor sendo transferido.**

- Fora do bitcoin, a **criação de dinheiro** (emissão) e a **contabilidade** (manutenção do controle do dinheiro recebido/gasto) **são centralizadas** e incluem as seguintes camadas separadas:

  - **Emissão de dinheiro** pelo Banco Central
  - **O tipo de dinheiro** que está sendo negociado (ouro, prata/USD/EUR/YEN/ZAR etc.)
  - **A quantidade** de dinheiro que está sendo negociada
  - **O registro da conta,** seja ele escrito ou digital
  - **As partes de confiança** que inserem os números nos livros contábeis
  - **As partes confiáveis** que mantêm os livros físicos seguros ou que mantêm os bancos de dados de computador
  - **As equipes de segurança especializadas** que trabalham para evitar a invasão dos bancos de dados

- Com o bitcoin, **todas essas camadas são dobradas em uma só!**

- Embora isso possa parecer mais centralizado, a genialidade de Satoshi fez com que o oposto fosse verdadeiro.

- Ele é 100% descentralizado!

- **O Bitcoin NÃO tem nenhum ponto de falha central.**
- **A única maneira de tudo ser reunido em um só e ser descentralizado é que o registro distribuído é mantido por um grupo voluntário, mundial e ad-hoc (destinado a este fim), de pessoas que voluntariamente mineram e/ou operam nós completos.**
- Além disso, os incentivos da rede **encorajam todos a seguir as regras.**
- Você pode se juntar a nós!

O Bitcoin é
uma revolução pacífica

Bitcoin é Esperança

COMO O bitcoin FUNCIONA?

Regras sem Regradores

tic-toc/
/próximo bloco

Criptografia (substantivo) / kɾip.tɔ.gɾɐ.fˈi.ɐ/

: cifragem e decifragem de mensagens em código secreto ou cifra
: a codificação e decodificação computadorizada de informações

~ Dicionário Merriam Webster

Hashing (verbo) /ˈhæʃɪŋ/

: um método de criptografia
: o processo de usar um algoritmo matemático contra dados para produzir um valor numérico (um hash digest) que é representativo desses dados.

~ crsc.nist.gov

Lembre-se:
O ecossistema do bitcoin inclui >>
bitcoin: o ativo monetário digital
Bitcoin: a **rede de pagamento** de mineradores e nós

1 bitcoin = 100.000.000 satoshis (sats)
(**Você pode comprar sats, uma fração de um bitcoin**)

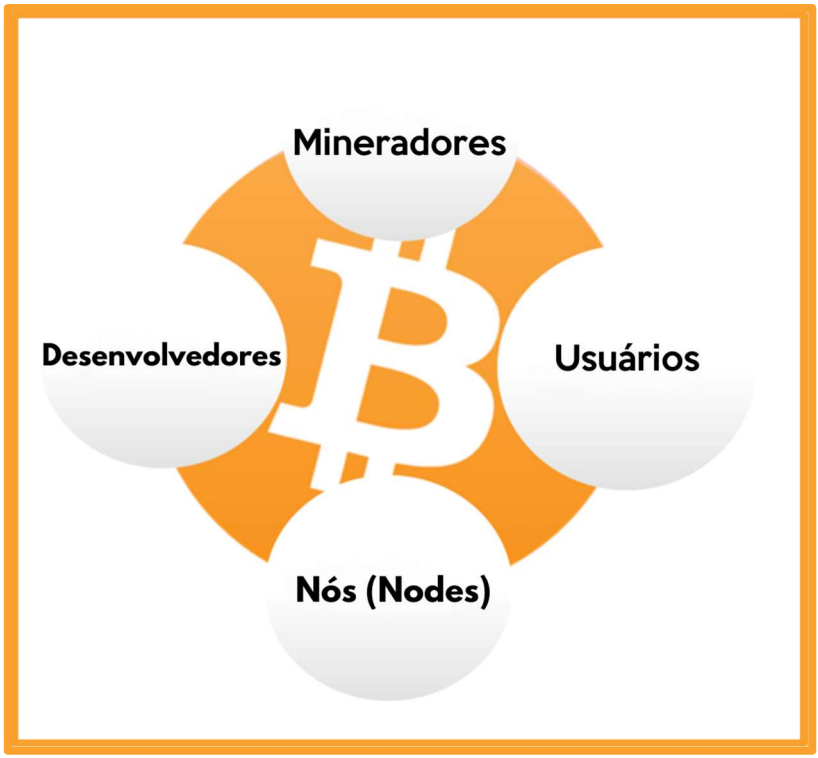
- O Bitcoin usa **prova de trabalho, criptografia de chave pública** e **rede ponto-a-ponto** para processar e verificar pagamentos em um livro-razão global, distribuído e on-line.

Definimos uma moeda eletrônica como uma cadeia de assinaturas digitais. Cada proprietário transfere a moeda para o próximo assinando digitalmente um hash da transação anterior e a chave pública do próximo proprietário e adicionando-os ao final da moeda. Um beneficiário pode verificar as assinaturas para verificar a cadeia de propriedade.

~ Satoshi Nakamoto
Bitcoin White Paper, Parte.2, 2008
Descrevendo como uma transação de bitcoin funciona no livro-razão distribuído

O ECOSSISTEMA DO BITCOIN...

consiste em Mineradores, Nós, Usuários e Desenvolvedores
todos trabalhando de forma independente, e simultaneamente,
para animar o que é o BITCOIN!



MINERADORES

- **Nós (Nodes) especializados (computadores) que "mineram" os blocos** que se tornam parte do blockchain do bitcoin.
- Ao fazer isso, eles **confirmam as transações verificadas feitas pelos usuários, cunham novos bitcoins e protegem toda a rede.**

USUÁRIOS

- **Você e eu. Todos nós. As pessoas. Reconhecendo e apreciando o valor fornecido,** fazendo transações, dando e recebendo esse dinheiro energético.
- **Armazenando nossa energia** para uso posterior, conforme necessário.

NÓS (NODES)

- **Os nós formam uma rede descentralizada, global e voluntária de milhares de computadores,** grandes e pequenos, cada um **executando independentemente a blockchain do bitcoin, verificando transações (evitando assim gastos duplos), e ajudando a proteger o sistema.**

DESENVOLVEDORES (DEVS)

- **Codificadores, programadores, autores digitais e videntes que trabalham para manter e dimensionar a rede, melhorar a segurança, a privacidade e a interface do usuário,** traduzindo o código em linguagem e recursos visuais que o restante de nós possa compreender e utilizar.

UMA TRANSAÇÃO DE BITCOIN:

Ali quer enviar um bitcoin para Benji:

1. Ali **abre o aplicativo de carteira de bitcoin** em seu telephone e clica em **"Send" (Enviar)**.

2. Benji **abre seu aplicativo de carteira** e **clica em "Receive" (Receber)**.

3. **Se eles estiverem juntos**: Ali escaneia o código QR no aplicativo da carteira no telefone de Benji.

4. **Se eles não estiverem juntos**: Ali copia e cola o endereço enviado por Benji para ela no campo de endereço em sua carteira.

5. Ali **digita a quantia a ser enviada** e clica em **"Send" (Envia)**.

6. **Alguns segundos depois,** Benji verá a quantia pendente em sua carteira.

7. Se o envio tiver sido feito pelo Lightning, ele será confirmado quase que instantaneamente, e é quase gratuito.

8. Se tiver sido enviada "on-chain" (na cadeia principal do Bitcoin), ela inclui uma pequena taxa e geralmente leva cerca de 10 minutos para ser confirmada. Pode demorar mais, dependendo do tráfego.

UMA TRANSAÇÃO DE BITCOIN POR TRÁS DA CENA:
(Seguem as definições dos termos)

1. Quando Ali envia esses sats para Benji, a **transação** de de pagamento é **transmitida** para a rede.
2. **A transação é verificada pelos nós** que garantem que Ali realmente tem o bitcoin para enviar e que ele não foi gasto anteriormente (para evitar o gastos duplo).
3. Depois de verificada por um nó, ela **aguarda no mempool** com as transações de outras pessoas.
4. As transações no mempool **são adicionadas em um bloco ao blockchain** quando um minerador encontra um nonce que satisfaça o **algoritmo de dificuldade**.
4. **Cada bloco tem um registro de data e hora.**
5. Isso **cria imutabilidade e ajuda a proteger o ajuste do algoritmo de dificuldade de ser manipulado**.
6. **Cada bloco representa uma confirmação** para as transações incluídas nele.
7. À medida que os blocos são criados e adicionados, aproximadamente a cada dez minutos, a imutabilidade da blockchain aumenta.

***TRANSAÇÃO* ~ Envio/recebimento de bitcoin**

- Uma transferência de valor na forma de satoshis, de um portador de bitcoin para outro.

***NÓ (NODE)* ~ Uma "agência" do "banco" bitcoin. Qualquer pessoa pode administrar um nó.**

- Os nós, juntamente com os mineiros (nós especializados), os utilizadores e os programadores, formam a rede Bitcoin peer-to-peer.
- Imagine **cada nó completo como um livro-razão que contém os saldos de cada chave privada.**
- Eles Interagem e chegam a um consenso (concordam) entre si, aceitando e validando transações de outros nós, juntamente com blocos dos mineradores, e depois transmitem-nos a outros nós.
- Os nós são geridos por um grupo *ad-hoc* de milhares de voluntários em todo o mundo. Um nó completo é aquele que validou independentemente toda a cadeia de blocos Bitcoin, desde o Bloco Génesis extraído por Satoshi em 2009. Atualmente, demora cerca de 2-3 dias e ~390GB de espaço.
- Quanto mais nós ativos existirem, mais distribuída e, por conseguinte, mais resistente se torna toda a rede.
- Existem **atualmente mais de 15 000 nós completos e acessíveis em todo o mundo e muito mais nós inacessíveis.**
- Todos os nós participantes são iguais.

- ***BROADCAST*** **~ Informa à rede que você está enviando bitcoin para alguém.**

  - Quando clica em "Enviar", a sua carteira assina a transação com a sua chave privada e permite que todos os outros nós saibam da sua intenção de transferir valor para que a possam validar.

- ***MEMPOOL*** **~ Uma sala de espera para transações**

  - Esta é a "sala de espera" onde as transações validadas são enviadas para serem recolhidas por um minerador e adicionadas a um bloco.

- ***BLOCO*** **~ Uma "página" no livro-razão do Bitcoin**

  - O livro-razão distribuído da Bitcoin é composto por "blocos" digitais. Cada bloco contém transações de bitcoin verificadas que mantêm o livro-razão global preciso e atualizado. Também contêm o nonce, um carimbo de data/hora e um hash do bloco anterior, que contribuem para a imutabilidade da cadeia de blocos de bitcoin.

- ***BLOCKCHAIN*** **~ O livro razão completo Bitcoin**

  - A cadeia de blocos de bitcoin é o livro-razão distribuído que contém todos os blocos e todas as transações de bitcoin já efetuadas desde que o bloco Genesis foi minerado por Satoshi em 2009.

MINERADOR **~ Um nó especializado que confirma transações e emite novos bitcoins.**

- Os mineradores de Bitcoin são computadores especializados. Eles dedicam muito poder de computacional (hashrate) numa loteria digital a fim de adivinhar um número que satisfaça o algoritmo de dificuldade atual, "minerando" assim um "bloco" (uma parte do livro-razão).
- Um bloco minerado é marcado com um carimbo de data e hora e adicionado à cadeia de blocos (também conhecida como timechain).

ALGORITMO DE DIFICULDADE **~ Um design especial e adaptável que ajuda a manter previsível a emissão de novas bitcoins.**

- Esta foi uma das soluções geniais de Satoshi para ajudar a proteger a emissão de bitcoin de ultrapassar a si própria, à medida que são desenvolvidos computadores mais avançados.
- Quanto mais mineradores ficam on-line, o número-alvo (nonce) na "loteria" fica menor e, portanto, mais difícil de ser encontrado.
- Quanto menos mineradores online, a "loteria" fica mais fácil.
- O algoritmo se **ajusta automaticamente a cada 2016 blocos** (aproximadamente a cada duas semanas), para garantir uma taxa previsível de fornecimento, em que um bloco é minerado aproximadamente a cada dez minutos.

NONCE **~ Um número aleatório de 32 bits**

- Um número aleatório de 32 bits que os mineradores adicionam ao final da lista de transações com hash, para tentar satisfazer o algoritmo de dificuldade para minerar um bloco.

- Quando um minerador encontra um nonce que está abaixo do número-alvo atual, ele minerou um bloco e pode adicioná-lo ao blockchain e reivindicar a recompensa.

TIMESTAMP **~ Marca o tempo**

- Todo bloco minerador tem um registro de data e hora adicionado a ele.
- Isso é para maior segurança, imutabilidade e para ajudar a estabelecer o ajuste de dificuldade.

IMUTABILIDADE **~ Não pode ser alterada.**

- Isso significa que o blockchain é "gravado em uma pedra digital".

PROVA DE TRABALHO (PoW) **~ Prova criptográfica de que foi feito um trabalho difícil para satisfazer um algoritmo.**

- Os mineradores usam o algoritmo PoW para provar que usaram muito poder computacional por meio de eletricidade (trabalho), a fim de obter consenso de forma descentralizada e evitar que agentes corruptos enviem spam para a rede.

CRIPTOGRAFIA DE CHAVE PÚBLICA **~ Um processo que cria as chaves digitais para acessar seus bitcoins**

- Esse é um sistema em que duas chaves são criadas por meio de um algoritmo criptográfico.
- **Uma chave é pública** - Como o número da sua conta bancária, que você pode fornecer às pessoas para que enviem bitcoins para você em troca de mercadorias, presentes ou serviços.
- **A outra chave é privada** – Você tem somente uma cópia e a usa para desbloquear sua conta e acessar seu bitcoin, assim como uma senha desbloqueia sua conta bancária on-line.

REDE PONTO A PONTO (P2P) **~ Uma rede descentralizada sem intermediários**

- Os Nós completos (pares) mantêm de forma colaborativa uma rede ponto a ponto para validação de blocos e transações. Nesse tipo de rede, cada nó é capaz de solicitar/fornecer dados de/para seus pares. Não há gatekeepers.

REDE LIGHTNING ~ **Uma rede criada com base no bitcoin, que possibilita o envio/recebimento de sats muito rápido e quase de graça.**

- A Lightning é uma solução de escalonamento de camada 2. Isso significa que ele fornece uma maneira de escalonar o bitcoin, dando-lhe o potencial de processar milhões de transações por segundo (TPS).

CARTEIRA **~ Uma "carteira" é um aplicativo de software que contém as chaves criptográficas para acessar seu bitcoin.**

- Pode estar em um telefone, computador ou em um pequeno dispositivo de hardware separado.
- Uma carteira de bitcoin seria mais precisamente chamada de dispositivo de assinatura. Seu bitcoin nunca sai de fato do blockchain, o livro-razão digital.
- Quando você quiser enviar ou gastar seu bitcoin, a carteira assinará e transmitirá a transação para a rede, para que possa ser verificada e adicionada a um bloco no blockchain.

DESENVOLVEDORES **~ Programadores de computador**

- Cypherpunks/programadores que mantêm a rede, melhoram a segurança, verificam bugs, enviam solicitações pull (para novas atualizações ou recursos), revisam solicitações pull, auditam o código.

- ***CHAVE PÚBLICA*** **~ Como um número de conta bancária para receber bitcoin.**

- Você pode fornecê-la para que as pessoas lhe enviem bitcoin, assim como você forneceria o número da sua conta para que alguém lhe enviasse moeda fiduciária.

- ***CHAVE PRIVADA*** **~ Para proteger, acessar e enviar bitcoin, como a chave de um cofre de segurança.**

- Uma chave privada de bitcoin é uma sequência secreta de números e letras que permite que você envie/gaste seu bitcoin.
- Somente você tem uma cópia. ****É muito importante mantê-la muito segura e protegida, pois qualquer pessoa que obtiver uma cópia poderá gastar seu bitcoin.** **

- ***LIVRO-RAZÃO DISTRIBUÍDO (LEDGER)*** **~ Um livro-razão mantido por todos que desejam ajudar a mantê-lo.**

- Em vez de um livro-razão controlado centralmente e invisível para o público, como um livro-razão mantido por um banco, o Bitcoin é um livro-razão transparente, aberto, descentralizado e visível para qualquer pessoa, a qualquer momento.
- Os endereços são cadeias de letras e números, sem nomes.
- Embora pseudônimo, é possível rastrear transações, especialmente se o bitcoin foi comprado em uma corretora centralizada com KYC.
- É preciso confiar que os bancos estão mantendo seus registros honestamente.
- A rede Bitcoin, por outro lado, é confiável e qualquer pessoa pode auditá-la a qualquer momento.

- O Bitcoin é "minerado" por computadores potentes e especialmente projetados em todo o mundo, chamados ASICS.

Um minerador de Bitcoin Antminer S9 ASIC

- **Os mineradores dedicam poder de computação, também conhecido como hashrate, por meio de eletricidade para a rede,** para adicionar blocos ao blockchain do Bitcoin.

- Esses computadores funcionam 24 horas por dia, geralmente em grupos de poucos, até algumas centenas ou milhares de outro computadores.

- **Basicamente, eles estão realizando participando de uma loteria. Quando um deles adivinha uma resposta** (o nonce) que satisfaz o algoritmo de dificuldade**, ele pode adicionar o próximo bloco à cadeia de tempo (timechain).**

- **Tudo isso é a prova de trabalho (PoW) necessária para gerar novos bitcoins.**

RECOMPENSA DO BLOCO DE BITCOIN

- **Por seu trabalho, eles recebem:**

  - **Uma recompensa na forma de bitcoins recém-criados.**
  - **Todas as taxas das transações verificadas incluídas nesse bloco.**

- **Quando você envia bitcoin para alguém, essa transação inclui uma taxa** e precisa ser verificada por um minerador e, em seguida, incluída em um bloco.
- A **recompensa do bloco de bitcoin** é cortada pela metade a cada quatro anos.
- **Atualmente, é de 6,25 bitcoins** por bloco minerado.
- **A próxima "redução pela metade" (Halving) ocorrerá em 2024,** quando a recompensa do bloco cairá para 3,125 bitcoins por bloco minerado.
- Como mencionado anteriormente**, isso mantém a emissão estável.**
- **No ano de 2140, a último satoshi será minerado.**
- Depois disso, os mineradores receberão apenas as taxas das transações que verificarem em cada bloco.

Em algumas décadas, quando a recompensa ficar muito pequena, a taxa de transação se tornará a principal compensação para os nós (mineradores).

~Satoshi Nakamoto

- **Os mineradores sempre serão necessários para verificar as transações, mantendo assim a rede segura.**
- Está ficando mais fácil para qualquer pessoa minerar em casa.
- Embora seja preciso estar ciente de que há custos envolvidos e que a lucratividade é baixa para os mineradores domésticos, essa é uma maneira poderosa de ajudar a proteger e manter a rede descentralizada.

- Os mineradores duram alguns anos. Atualmente, há muitos Antminer S9, por exemplo, que estão funcionando há mais de 6 anos.
- Quando os mineradores são aposentados, eles podem ser **facilmente desmontados e reciclados**.
- **Muitas inovações fascinantes estão acontecendo, com pessoas usando as mineradoras para aquecer suas casas, saunas e até banheiras de hidromassagem!**

SOBRE A REDE LIGHTNING

- **Os blocos do Bitcoin são intencionalmente pequenos*** (1 MB cada), o que faz com que a cadeia principal de bitcoin consiga processar cerca de 7 transações por segundo (TPS).

- A Visa processa cerca de 4.000 TPS.

- Além disso, **geralmente leva no mínimo 10 minutos para que a primeira confirmação seja feita em uma transação da cadeia principal** (já que um bloco é minerado a cada 10 minutos).

- Isso não é prático se você estiver em uma loja e quiser fazer um pagamento rápido de suas mercadorias.

Detalhe importante:** O motivo pelo qual os blocos são pequenos é manter **o blockchain pequeno o suficiente para que qualquer pessoa possa executar seu próprio nó em casa,** o que **ajuda a manter a rede descentralizada. Satoshi percebeu a importância disso ↓

> *Os usuários de Bitcoin podem se tornar cada vez mais tirânicos em relação à limitação do tamanho da cadeia para que seja fácil para muitos usuários e dispositivos pequenos.*
>
> ~ Satoshi Nakamoto, 10-12-2010

- **LEIA**: "A Guerra dos Blocos" de Jonathan Bier

- Entre, a **Lightning Network (LN), uma solução de escalonamento de bitcoin de camada 2.**
- **"Camada 2"** significa **que ela é construída sobre o bitcoin.**
- "**Solução de Escalonamento**" significa que ela permite que a rede:
  - **Aumente enormemente a velocidade de processamento.**
  - **Aumente enormemente o número de transações que pode processar por segundo.**
  - **Torne possíveis os micro pagamentos.**

- A Lightning Network pode ser (mais ou menos) pensada como uma conta que você mantém com alguns amigos no bar.

- Todos mantêm o controle de quem deve o quê (como um canal da Lightning Network) e, no final da noite, seu grupo acerta a conta com o barman ("a cadeia principal").

- **Os canais Lightning podem permanecer abertos por dias, semanas ou meses antes de serem "liquidados" na cadeia principal.**

- **Os blocos do Bitcoin são intencionalmente pequenos*** (1 MB cada), o que faz com que a cadeia principal de bitcoin consiga processar cerca de 7 transações por segundo (TPS).

- A Visa processa cerca de 4.000 TPS.

- Além disso, **geralmente leva no mínimo 10 minutos para que a primeira confirmação seja feita em uma transação da cadeia principal** (já que um bloco é minerado a cada 10 minutos).

- Isso não é prático se você estiver em uma loja e quiser fazer um pagamento rápido de suas mercadorias.

Detalhe importante:** O motivo pelo qual os blocos são pequenos é manter **o blockchain pequeno o suficiente para que qualquer pessoa possa executar seu próprio nó em casa,** o que **ajuda a manter a rede descentralizada. Satoshi percebeu a importância disso ↓

> *Os usuários de Bitcoin podem se tornar cada vez mais tirânicos em relação à limitação do tamanho da cadeia para que seja fácil para muitos usuários e dispositivos pequenos.*
>
> ~ Satoshi Nakamoto, 10-12-2010

➢ **LEIA**: "A Guerra dos Blocos" de Jonathan Bier

- Entre, a **Lightning Network (LN), uma solução de escalonamento de bitcoin de camada 2.**
- **"Camada 2"** significa **que ela é construída sobre o bitcoin.**
- "**Solução de Escalonamento**" significa que ela permite que a rede:
  - **Aumente enormemente a velocidade de processamento.**
  - **Aumente enormemente o número de transações que pode processar por segundo.**
  - **Torne possíveis os micro pagamentos.**

- A Lightning Network pode ser (mais ou menos) pensada como uma conta que você mantém com alguns amigos no bar.

- Todos mantêm o controle de quem deve o quê (como um canal da Lightning Network) e, no final da noite, seu grupo acerta a conta com o barman ("a cadeia principal").

- **Os canais Lightning podem permanecer abertos por dias, semanas ou meses antes de serem "liquidados" na cadeia principal.**

BENEFÍCIOS DA  *:*

- ***VOLUME*** ~ O volume de transações por segundo é, em essência, ilimitado, pois inúmeros canais podem ser abertos ao mesmo tempo, cada um mantendo sua própria "conta".

- ***MICROPAGAMENTOS*** ~ Você pode enviar apenas 1 satoshi (atualmente US$ 0,0003).

- ***VELOCIDADE*** ~ Geralmente, leva de um milissegundo a alguns segundos para receber um pagamento.

- ***PRIVACIDADE*** ~ As transações não são armazenadas no blockchain aberto e público do bitcoin. De certa forma, ela é ainda mais privada do que o dinheiro, pois com o Lightning, nem mesmo a outra parte sabe necessariamente quem você é, já que seu pagamento "salta" por diferentes canais para chegar ao destinatário. Para ser claro, não estou dizendo que é 100% impossível de ser descoberto, apenas muito mais do que com pagamentos na cadeia principal do bitcoin. Seria necessário muito tempo e energia para estabelecer com certeza quem estava fazendo pagamentos a quem, e nem sempre seria possível fazer isso.

➢ **Desfrute de uma incrível visualização** da Lightning Network em: lnrouter.app/graph

O Bitcoin em si não pode ser dimensionado para que todas as transações financeiras do mundo sejam transmitidas a todos e incluídas no blockchain. É preciso haver um nível secundário de sistemas de pagamento que seja mais leve e mais eficiente.

~ Hal Finney, 30-12-2010
Antigo cypherpunk & a
segunda pessoas rodar o Bitcoin

Pense nisso da seguinte forma:

- Bitcoin: **Conta poupança** ~ Transações mais lentas para quantias maiores.
- **Conta corrente** ~ Transações muito rápidas para quantias menores.

O Bitcoin aprimorado pelo Lightning pode ser visto tanto como um produto (propriedade digital) quanto como um serviço (rede monetária aberta). A capacidade de transferir energia monetária através do tempo e do espaço sem a intervenção do governo ou de bancos convencionais é extremamente valiosa para a humanidade.

~ Michael Saylor @saylor
CEO Microstrategy

COMO bitcoinIZAR

Bitcoinizar - To Bitcoin: (verbo) /tuːˈbɪtkɔɪn/

Proponho que bitcoinizar (to bitcoin) seja um verbo que englobe a plenitude da participação no ecossistema bitcoin/Bitcoin.

Bem, agora que você já deve ter tomado a pílula laranja e está pronto para se tornar seu próprio banco, participando do primeiro dinheiro livre e do mundo! aí vem a parte divertida!

- É aqui que está a mudança realmente épica para se tornar financeiramente autossuficiente, e pode levar tempo para entender completamente o que isso significa.

- **É necessário um pouco de intenção e dedicação para entender como fazer isso da maneira mais segura possível.**

- Com o objetivo de manter este livro como "o livro sobre bitcoin mais simples já escrito", apresentarei um esboço aqui e, no final, oferecerei recursos para você mergulhar, que são muito mais profundos do que o escopo desta cartilha.

HODL: (verbo) /ho'dill/

:manter seus bitcoins
: não vender

(de uma postagem de 2013 no bitcointalk.org, em que o autor da postagem afirmou estar bêbado e escreveu "HOLD" incorretamente - Pesquise no Google, vale a pena ler ☺)

Embora a rede ainda esteja crescendo, há muito valor nos milhões de hodlers globais de última alternativa.

- **O Bitcoin entra no mercado quando os mineradores vendem alguns dos bitcoins que recebem como recompensa** para pagar seus custos operacionais.

- **Você pode adquirir bitcoin comprando em uma plataforma de negociação ponto a ponto (P2P), aceitando-o como pagamento por bens ou serviços que você oferece, como um presente ou minerando-o. (Em último análise, não é recomendado usar uma corretora).**

- Ao recebê-lo, você está tecnicamente recebendo as chaves privadas com as quais pode acessar seu bitcoin.

- **O bitcoin em si, nunca sai do blockchain.**

- Você pode adquirir bitcoin de forma anônima ou com verificação de identidade (KYC - Know Your Customer).

- O KYC é exigido por lei para cumprir as leis de combate à lavagem de dinheiro (AML) ao comprar em corretoras.

- **Como o bitcoin é dinheiro da liberdade, recomendo fortemente a compra de bitcoin sem KYC.**
- **Isso preserva seu direito à privacidade no futuro.**

Sem verificação de Identidade Non-KYC >> De forma anônima

Como Comprar Bitcoin sem KYC (Anonimamente):

RECOMENDADO

1. Selecione um app de carteira somente Bitcoin.
2. Escolher um método. (veja abaixo).
3. Compre, receba ou minere bitcoin.
4. Saque os bitcoins para sua carteira.
5. HODL

- **Compre no Bisq ou no HodlHodl.** Dê uma olhada em bisq.wiki para saber como comprar. Pode levar um pouco de tempo para aprender a usar a plataforma, mas vale muuuuito a pena! Fique livre de KYC!

- **Compre em um caixa eletrônico de bitcoin** >> Verifique antes de usar, pois alguns exigem identificação. Outros pedem apenas um nome e número (você pode usar um número de telefone temporário).

- **Compre um voucher da Azteco.** Visite azte.co

- **Ganhe pelo seu trabalho.** ~ Peça para ser pago em Bitcoin. Ofereça desconto para pagamentos em Bitcoin.

- **Compre pessoalmente em encontros Bitcoin (meet-ups)**
- **Minere** ~ Está cada vez mais fácil minerar em casa, você pode participar de um pool de mineração, mas (faça sua própria pesquisa) para ficar livre de KYC.

Como Comprar Bitcoin com KYC (verificando a identidade):

NÃO RECOMENDADO

1. Selecione um app de carteira Bitcoin Only.
2. Escolha uma corretora para comprar Bitcoin
3. Crie uma conta.
4. Selecione (vincule) um método de pagamento.
5. Atenda aos requisitos de KYC (Identificação).
6. Compre Bitcoin.
7. Saque para sua própria carteira.
8.HODL.

KYC >> Verificação de Identidade Obrigatória

- **Esteja ciente de que seu bitcoin estará para sempre vinculado à sua identidade** se você o comprar dessa forma.

- Se você optar por esse método, recomendo que encontre uma ***corretora de bitcoin*** com boa reputação.

- ***Verifique se que a corretora permita que você retire seu bitcoin para sua própria carteira!***

- **Por lei as Corretoras são obrigadas a exigir a identificação do usuário (KYC).**

- Elas solicitam **seu nome completo, endereço, número de documentos, e-mail, número de telefone e, muitas vezes, uma foto sua segurando seu documento de identidade.**

- **Confirme se a corretora tem suporte telefônico e por e-mail** para atendimento ao cliente.

- Peça orientação sobre como enviar o bitcoin que está na corretora para sua própria carteira, assim você estará auto custodiando seus bitcoins = **manter suas próprias chaves.**

> - **Isso NÃO apaga o fato de que você comprou bitcoin deles... nunca.**
> - **As transações são rastreáveis na blockchain e, em muitos países, você é responsável pela tributação ao gastar seu bitcoin.**

- **Evite comprar por meio do Venmo e do Paypal, pois atualmente não é possível retirar seus sats para sua própria carteira de auto custódia.**

- Como se diz no BT (bitcoin twitter):
  "**No keys, No cheese**" **(Sem chaves, sem queijo)** ou
  "**Se não for suas chaves, Não é seu Bitcoin.** "

- Isso significa que, enquanto um serviço centralizado detiver as chaves privadas do seu bitcoin, existe a possibilidade de que a plataforma seja invadida ou que eles sofram captura regulatória e você perca seu bitcoin.

- Isso aconteceu com o ouro em 1933... **O presidente Roosevelt emitiu a Ordem Executiva 6102, que exigia que todos os cidadãos dos EUA entregassem a maior parte de seu ouro em troca de notas bancárias.**
- O ouro foi avaliado em US$ 20,67/onça. No ano seguinte, o governo aumentou o preço do ouro para US$ 35/onça com o Gold Reserve Act de 1934, desvalorizando efetivamente as notas que as pessoas haviam recebido, já que o valor das notas nunca subiu com o preço inflacionado do ouro.

POSTMASTER: PLEASE POST IN A CONSPICUOUS PLACE.—JAMES A. FARLEY, Postmaster General

UNDER EXECUTIVE ORDER OF THE PRESIDENT

Issued April 5, 1933

all persons are required to deliver

ON OR BEFORE MAY 1, 1933

all GOLD COIN, GOLD BULLION, AND GOLD CERTIFICATES now owned by them to a Federal Reserve Bank, branch or agency, or to any member bank of the Federal Reserve System.

Executive Order

FORBIDDING THE HOARDING OF GOLD COIN, GOLD BULLION AND GOLD CERTIFICATES.

For Further Information Consult Your Local Bank

GOLD CERTIFICATES may be identified by the words "GOLD CERTIFICATE" appearing thereon. The serial number and the Treasury seal on the face of a GOLD CERTIFICATE are printed in YELLOW. Be careful not to confuse GOLD CERTIFICATES with other issues which are redeemable in gold but which are not GOLD CERTIFICATES. Federal Reserve Notes and United States Notes are "redeemable in gold" but are not "GOLD CERTIFICATES" and are not required to be surrendered

Special attention is directed to the exceptions allowed under Section 2 of the Executive Order

CRIMINAL PENALTIES FOR VIOLATION OF EXECUTIVE ORDER $10,000 fine or 10 years imprisonment, or both, as provided in Section 9 of the order

Secretary of the Treasury.

- **Demorou até 1975, 42 anos para que o EO6102 fosse revogado.**

- Embora isso seja improvável, não é impossível. Neste momento, temos pouca ideia de como os órgãos reguladores responderão ao bitcoin à medida que ele continua a ganhar popularidade e a ser adotado de forma mais ampla.

- Até o momento, a recepção tem sido mista. No entanto, por enquanto, parece que muitos entendem, ou talvez apenas aceitem, que o bitcoin não pode ser detido em última instância.

- Vários políticos estão começando a se manifestar a favor do bitcoin como parte de sua plataforma. Há também alguns que são contra.

- **Em última análise, seria do interesse de todos os governos adotá-lo e adicioná-lo a seus balanços patrimoniais, como uma proteção contra suas moedas fiduciárias que se inflacionam rapidamente e se desvalorizam.**

- El Salvador está muito à frente neste ponto, tendo tornado a moeda uma forma de curso legal em 2021

- É empolgante ver qual será o próximo país!

- Depois de dar o passo que mudou sua vida ao comprar seu primeiro bitcoin ₿ (parabéns!), você precisa decidir como **armazená-lo com segurança.**

- **Ser seu próprio banco é uma forma poderosa de soberania individual.**
- E isso **precisa ser levado a sério!**

- *** Por favor DYOR > Do Your Own Research < (Faça sua própria pesquisa) além das minhas recomendações básicas aqui***

- **O ecossistema do bitcoin está evoluindo a cada minuto.**

- O Twitter é um bom lugar para ficar por dentro dos últimos desenvolvimentos (até que um aplicativo melhor e descentralizado ganhe força).

CONFIRA ESTES SITES PARA OBTER TUTORIAIS:

- BTC Sessions no You Tube
- Bitcoiner.guide
- Armantheparman.com

CARTEIRAS SOMENTE BITCOIN (BITCOIN-ONLY)

- É melhor armazenar o Bitcoin em sua própria carteira
  - **custódia própria**
  - **não custodial**
  - **carteira somente para bitcoin**

- Uma "carteira" é, na verdade, um software que é um dispositivo de assinatura. Ela contém suas chaves privadas, que são usadas para assinar uma transação que você envia (transmissão).

CARTEIRA QUENTE (HOT WALLET)

- **Esse é um aplicativo de carteira de bitcoin on-line, que você baixa no seu telefone ou computador.**
- É melhor usado para quantias menores, para gastos diários.

CARTEIRA FRIA (COLD WALLET)

- **É uma carteira off-line.** Também conhecida como carteira de hardware.
- É um dispositivo de hardware separado no qual você armazena suas chaves. É como um cofre de segurança.

> - **Por Favor DYOR (faça sua própria pesquisa) Compare os recursos e as vantagens e desvantagens entre as carteiras**

- Embora ambas funcionem bem, geralmente é recomendável usar uma carteira fria quando você tiver mais de US$ 500-1000 em bitcoins, pois ela é mais segura.
- ***APP DE CARTEIRAS QUENTE (HOT WALLET APPS) - Não-Custodial***
  Muun Wallet, Blue Wallet, Samourai Wallet (Somente para Android), Sparrow Wallet, Green Wallet, Phoenix Wallet

- ***CARTEIRAS FRIAS (COLD STORAGE WALLETS)***
  Cold Card, Trezor, Passport, Keystone, Blockstream Jade, Seed Signer, Bitbox,

- **SEMPRE** compre sua carteira fria (hardware wallet) **diretamente do fabricante**, para ter certeza de que ela não foi adulterada.

- **Siga o BTC Sessions no YouTube** para obter excelentes tutoriais sobre a configuração da carteira (e muito mais).

- Ao configurar sua carteira, certifique-se de **anotar a Seed Phrase de 12 ou 24 palavras em um papel.**
- ***Mantenha-a off-line. Nunca faça uma captura de tela dela.***
- **ARMAZENE A SEED PHRASE COM MUITA SEGURANÇA.**
- **ARMAZENE A SEED PHRASE COM MUITA SEGURANÇA.**
- **MUITA, MUITA SEGURANÇA!**

- **Muitas empresas fabricam placas de metal para gravar as seeds de por meio de perfuração e assim aumentar a proteção contra fogo/água.**

- Se você perder o acesso à sua carteira quente ou fria, poderá restaurá-la com a frase-semente e recuperar seus fundos.

- Isso pode ser feito em qualquer carteira que suporte o mesmo tipo de seed-phrase BIP39 (12/24 palavras).

- A prática recomendada seria armazenar o caminho de derivação de sua carteira, além de sua seed.

- **Lembre-se: *Qualquer pessoa que tenha a seed tem acesso ao seu bitcoin!***

SOBRE PRIVACIDADE

- A privacidade ao **comprar (sem KYC), proteger, armazenar e gastar** bitcoin está se tornando cada vez mais importante, especialmente em decorrência dos recentes eventos com contas bancárias sendo apreendidas/congeladas.

- Além disso, **a privacidade digital geral é fundamental se você deseja obter soberania on-line e se proteger de vigilância e fraude indevidas.**

- Abaixo estão alguns serviços atuais voltados para a privacidade. Está além do escopo deste livro se aprofundar em cada um dos serviços a seguir, portanto, fique atento e siga as contas que menciono abaixo no Twitter para obter atualizações.

> *A privacidade é necessária para uma sociedade aberta na era eletrônica. Privacidade não é sigilo. Um assunto privado é algo que não se quer que o mundo inteiro saiba, mas um assunto secreto é algo que não se quer que ninguém saiba. Privacidade é o poder de se revelar seletivamente, revelar a si mesmo ao mundo.*
>
> ~Eric Hughes, "O Manifesto Cypherpunk"

GUIAS DE PRIVACIDADE

- Bitcoiner.guide @BitcoinQ_A
- Econoalchemist.com @econoalchemist
- Sethforprivacy.com @sethforprivacy
- diverter.hostyourown.tools @Diverter_NoKYC
- Citadeldispatch.com @ODELL
- KYCnot.me
- Lopp.net @lopp > Click Resources > Privacy
- Privacytools.io
- Enegnei.github.io
- Restoreprivacy.com @ResPrivacy
- Keepitsimplebitcoin.com @KISBitcoin
- @SovrnBitcoiner
- K3tan.com @_k3tan

VPN (rede virtual privada para ocultar seu ISP)

- Mullvad.net - Pague com bitcoin

APLICATIVOS DE AUTENTICAÇÃO DE DOIS FATORES

- Authy
- Google Authenticator
- Yubi Key

NAVEGADORES COM FOCO EM PRIVACIDADE

- TOR
- Firefox
- Brave

APLICATIVO DE "NOTAS" CRIPTOGRAFADAS

- StandardNotes.com

MECANISMOS DE PESQUISA COM FOCO EM PRIVACIDADE

- Duck Duck Go
- Brave
- Startpage
- Qwant

APLICATIVOS DE MENSAGENS COM FOCO EM PRIVACIDADE

- Signal
- Session
- Element

RODANDO SEU PRÓPRIO NODE

- Bitcoin Core
- Ronin Dojo
- Run Citadel
- Raspi Blitz
- Umbrel – Se você rodar apenas o node bitcoin.

SERVÇOS DE MIXING

- Coinjoin
- Paymarket
- Coinswap

CELULARES/SERVIÇOS DE USO ÚNICO

- Run Calyx OS no Android Pixel
- Text Verified

PAGAMENTOS PRIVADOS

- Pay with Moon
- Bitrefill
- Paxful

RECEBIMENTO PRIVADO

- PayNym

MÍDIA SOCIAL DESCENTRALIZADA

- Nostr
- Mastodon
- Zion (taxa mensal, será adicionado o bitcoin como opção de pagamento)

> *A possibilidade de ser anônimo ou pseudônimo depende de você não revelar nenhuma informação de identificação sobre si mesmo em relação aos endereços de bitcoin que usa. Se você publicar seu endereço de bitcoin na Web, associará esse endereço e todas as transações com ele ao nome com o qual o publicou. Se você postou com um nome que não associou à sua identidade real, então você ainda é um pseudônimo.*
>
> ~ Satoshi Nakamoto 25-11-2009

> Para maior privacidade, é melhor usar endereços de bitcoin apenas uma vez. Você pode mudar de endereço quantas vezes quiser.
>
> ~Satoshi Nakamoto 25-11-2009

DESMISTIFICANDO O bitcoinFUD

(Fear Uncertainty Doubt - Medo, Incerteza, Dúvida)

- Abaixo estão alguns argumentos comuns contra o bitcoin, ou medos sobre ele.
- Esses argumentos são, em grande parte, infundados, resultantes de ignorância ou talvez de um entendimento incompleto.
- Apresento aqui breves refutações para cada um deles e no final, você encontrará indicações de leituras mais aprofundados que refutam todo os FUDs. (Fear Uncertainty Doubt - Medo, Incerteza, Dúvida)

O BITCOIN USA MUITA ENERGIA

> *O calor do seu computador não é desperdiçado se você precisar aquecer sua casa... O custo é igual se você gerar o calor com seu computador.*
>
> ~ Satoshi Nakamoto 09-08-2010

> *Em um primeiro momento, a produção de uma mercadoria simplesmente porque ela é cara parece um desperdício. No entanto, a mercadoria de custo incalculável agrega valor repetidamente ao permitir transferências benéficas de riqueza. Mais do custo é recuperado toda vez que uma transação se torna possível ou menos dispendiosa.*
> *O custo, inicialmente um desperdício total, é amortizado em muitas transações.*
>
> ~ Nick Szabo Cypherpunk

- **O "excesso" de energia é uma proposta de valor que deve considerar como valorizamos a finalidade do uso da energia.**

- **Se considerarmos que as luzes de Natal nos EUA usam tanta eletricidade quanto toda a rede Bitcoin**, talvez possamos ver que tudo isso é relativo!

- Usar energia, mesmo muita energia, para garantir o dinheiro mais difícil e resistente à censura que a humanidade já conheceu, vale 1000% a pena!

- Ao comparar o uso de energia do bitcoin com o usado pelo sistema legado, também precisamos considerar a "pilha completa" de ambos os lados:

Ecossistema do Bitcoin	**Sistema Legado Fiat**
Mineradoras ASIC	BIS (Banco de Compensações Internacionais)
Nós (Nodes)	Bancos Centrais
Carteiras de Hardware	Bancos Nacionais/Regionais Banks
Aplicativos de Carteiras	Complexo Industrial Militar
	Backup de Dados de Bancos
	Impressão de Dinheiro Físico
	Aplicativos de Banco On-line
	Rede de Caixas Eletrônicos

- Ao usar o bitcoin, acabaremos reduzindo o uso de energia em várias outras áreas, principalmente por não precisarmos mais do Complexo Industrial Militar para proteger o petrodólar.

O bitcoin é um direito de propriedade que é independente do monopólio da violência.
~ @breedlove

- Além disso, o consumismo desenfreado, necessário para manter o sistema baseado em dívidas, será reduzido com o tempo, já que o **dinheiro de verdade incentiva naturalmente gastos e economias prudentes** (já que suas economias realmente manterão seu valor, um conceito que não experimentamos desde que saímos do padrão ouro).

- **Por último, e mais importante, a mineração de bitcoin já está reduzindo a poluição ao capturar o gás natural queimado e usá-lo para alimentar as mineradoras.** Como as mineradoras buscam baixos custos de eletricidade, é provável que esse também seja o maior impulsionador da energia renovável de baixo custo, já que os incentivos são compatíveis.

- Nic Carter, Ethan Buchman, Troy Cross, NYDIG, no vídeo "This Machine Greens" de Swan Bitcoin no YouTube e um excelente episódio do programa "What is Money" (WiM161) com B.Quittem **contém informações detalhadas** sobre Bitcoin e Energia.

O BITCOIN É UM ESQUEMA PONZI

O Bitcoin não é um esquema Ponzi:

- Os investidores antigos não recebem nenhum dinheiro dos novos investidores.
- Ao comprar bitcoin, ninguém está prometendo um retorno sobre seu investimento.
- Não há equipe de liderança ou de promoções.
- Não houve pré-mineração.
- **Leia:** 'Why Bitcoin is Not a Ponzi' (Porque o Bitcoin não é um Ponzi) de Lyn Alden para saber mais.

O BITCOIN É MUITO LENTO

Embora a camada de base do Bitcoin seja lenta, a **Lightning Network de segunda camada construída sobre a camada de base é... rápida como um raio!**

A rede do Bitcoin pode processar cerca de 7 transações por segundo (TPS).

A rede Visa afirma que pode processar até 24.000 TPS, embora 4.000 TPS esteja mais próximo do uso real.

A Lightning Network, uma solução de segunda camada criada com base no Bitcoin, tem a capacidade de processar milhões de transações por segundo!

OS GOVERNOS PODERIAM PROIBIR O BITCOIN

- Alguns governos já tentaram, como a China, a Índia e a Nigéria, por exemplo. Em todos os casos, o uso do bitcoin aumentou rapidamente entre a população do país em questão.

- **Não há como os governos realmente "banirem" o bitcoin**, pois ele é, por sua natureza, sem permissão e resistente à censura. É código e código é discurso.

- Dito isso, os governos podem dificultar a compra e a venda de bitcoins e transformá-los em moeda fiduciária. Eles também podem tributá-la como uma commodity, como fazem nos EUA.

- **Em última análise, não será favorável a eles tentar bani-la, já que o bitcoin é inevitável e eles estão começando a perceber isso.** Eles seriam muito mais inteligentes se o adicionassem ao balanço patrimonial de seus países como uma proteção contra a inflação de suas moedas fiduciárias.

> *Os governos são bons em cortar a cabeça de redes controladas centralmente, como o Napster, mas as redes P2P puras, como Gnutella e Tor, parecem estar se mantendo.*
>
> ~ Satoshi Nakamoto

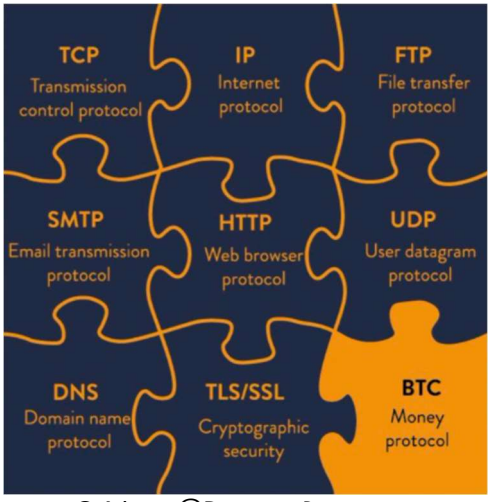
- **Excelente artigo:** O governo pode deter o Bitcoin? por Alex Gladstein, CSO da Human Rights Foundation

- **Mais como "tecnologia de ponta"**, com relação à escassez digital, descentralização e solução do problema de gasto duplo e do problema dos generais bizantinos. Uma vez descoberta, ela não pode ser redescoberta.

- **Uma vez que a roda foi inventada, ela nunca mais poderá ser reinventada.**

- O protocolo TCP/IP, no qual a Internet é executada, tem sido o padrão para todas as redes de computadores desde 1983. É provável que continue sendo o padrão por um longo tempo.

- Quando uma solução perfeita, uma tecnologia de camada de base é descoberta e funciona de forma ideal, ela pode durar centenas ou milhares de anos.



Créditos: @DecouvreBitcoin

O BITCOIN É USADO POR CRIMINOSOS

- **O mesmo acontece com o dólar e todas as outras moedas fiduciárias do mundo.** Embora essas atividades me entristeçam muito, é simplesmente incorreto atribuí-las ao próprio bitcoin. **O Bitcoin é uma ferramenta, assim como uma faca, e cabe a cada um de nós decidir como usá-la.**

- Observação: Como o blockchain do Bitcoin é auditável, ele é, na verdade, uma péssima opção para atividades criminosas.

A COMPUTAÇÃO QUÂNTICA PODE QUEBRAR O BITCOIN

- Embora essa seja uma possibilidade para um dia no futuro, **os desenvolvedores já estão trabalhando em soluções para criptografia pós-quântica**. Elas seriam implementadas quando necessário.

- O Bitcoin é apenas um dos inúmeros aplicativos on-line que dependem do hashing SHA-256 para segurança. Até mesmo os militares o utilizam, portanto, há um enorme incentivo além da comunidade bitcoin para desenvolver novos protocolos de criptografia.

- Além disso, se o SHA-256 for quebrado, teremos muito mais com que nos preocupar além do bitcoin.

O BITCOIN NÃO TEM VALOR REAL

"O valor dos bitcoins é impulsionado por sua escassez obrigatória"

~ Fidelity Digital Assets

- **A raridade é o valor. Todo dinheiro, em todos os tempos, foi valorizado porque tinha alguma medida de escassez.**

- Além disso, foi respaldado pela crença de que manteria seu valor, de modo que poderia ser trocado no futuro por outra coisa de valor.

- À medida que a rede Bitcoin cresce, respaldada pelas propriedades monetárias superiores que ela incorpora, o efeito de rede cresce exponencialmente.

- Quanto maior o efeito de rede, mais valor ele oferece, como um ativo escasso. O valor é um reflexo da demanda e, à medida que a demanda aumenta, o valor aumenta.

- É verdade que algumas pessoas têm muito mais do que outras. **Ao liberar o protocolo abertamente, Satoshi permitiu que ele circulasse livremente, e aqueles que entenderam o potencial que ele tinha mineraram ou compraram antecipadamente. Essa foi a maneira mais justa e orgânica possível de apresentá-lo ao mundo.**

- Com o tempo, quando o mundo estiver hiperbitcoinizado, ou seja, quando estivermos vivendo em um padrão bitcoin, aqueles que tiverem mais dinheiro naturalmente o gastarão na economia.

- Mesmo que em um determinado momento não seja mais possível comprar com moeda fiduciária, as pessoas serão pagas por seu trabalho em bitcoin. O fato de sermos pagos com dinheiro realmente sólido nos permitirá ter economias reais que não serão degradadas com o tempo pela inflação.

- Embora sempre haja pessoas com mais riqueza e outras com menos, devido a um grande número de fatores, **o padrão bitcoin tornará permeável a membrana entre as classes de riqueza**, como diz Aleks Svetsi. Isso permitirá que a mobilidade ascendente e descendente seja muito, muito mais fluida do que é hoje.

- **Tendo nascido e nadado toda a nossa vida em um mundo fiduciário, é quase impossível imaginar e compreender plenamente as implicações de ter um dinheiro que não pode ser degradado ou manipulado!**

- **Isso é normal durante a fase de descoberta de preços de um novo ativo monetário.** Não há outra maneira de o crescimento acontecer quando ele é orgânico e emergente (em oposição a um crescimento de cima para baixo e ordenado).
- Além disso, neste estágio da existência humana, com mudanças exponenciais ocorrendo em todas as esferas, faz sentido que algo tão revolucionário como o bitcoin sofra oscilações violentas.
- Embora aqueles de nós que estão no fundo da toca do coelho o vejam como o futuro, atualmente apenas cerca de 1-2% da população global possui bitcoin. Isso o torna vulnerável a uma imensa volatilidade.
- À medida que amadurecer e a adoção aumentar, a volatilidade diminuirá e, por fim, ela se estabilizará e se tornará uma unidade de conta.

> *Tenho certeza de que em 20 anos haverá um volume muito grande de transações ou nenhum volume.*
>
> ~ Satoshi Nakamoto 14-02-2010

VOCÊ NÃO PODE TOCAR EM UM BITCOIN

- **Isso é um recurso, não um bug.** O próprio fato de o bitcoin não ser físico é justamente o que o torna inconfiscável!

O BITCOIN PODE SER HACKEADO

- Nos 14 anos desde que foi lançado, ele nunca foi hackeado.

- No entanto, houve invasões em corretoras, portanto, recomendo enfaticamente que você transfira seu bitcoin para sua própria carteira de custódia o mais rápido possível.

- Estima-se que para quebrar a criptografia SHA-256 (que o bitcoin usa) em 24 horas, um computador quântico precisaria de 13.000.000 de qubits físicos. No momento, o recorde atual de qubits mantido pela IBM é de apenas 127 qubits.

- Supõe-se amplamente que um método de criptografia quântico seguro será desenvolvido bem antes de ser necessário.

> *O fato de ser de código aberto significa que qualquer pessoa pode revisar o código de forma independente. Se fosse de código fechado, ninguém poderia verificar a segurança. Acho que é essencial que um programa dessa natureza tenha código-fonte aberto.*
>
> *~Satoshi Nakamoto 10-12-2009*

MAIS SOBRE COMO DESMASCARAR FUDS AQUI:

- Endthefud.org
- Bitcoinmythbusters.org
- Casebitcoin.com
- Safehodl.github.io/failure/
- Lopp.net - Misconceptions

O Bitcoin é fundamentalmente diferente de qualquer outro ativo digital. Nenhum outro ativo digital tem probabilidade de melhorar o bitcoin como bem monetário porque o bitcoin é o dinheiro digital mais seguro, descentralizado e sólido (em relação a outros ativos digitais) e qualquer "melhoria" necessariamente enfrentará compensações.

Relatório de Ativos Digitais da Fidelity, 'Bitcoin First', janeiro de 2022
Chris Kuiper, CFA, Diretor de Pesquisa
Jack Neureuter, analista de pesquisa

- **Eu vejo o hodling (manter) bitcoin como ter uma conta poupança de longo prazo.**
- O preço diário não importa, pois espera-se que ele seja volátil (suba e desça) por alguns anos ainda.

- Como mencionei anteriormente, isso é normal para um novo ativo em fase de descoberta de preço.

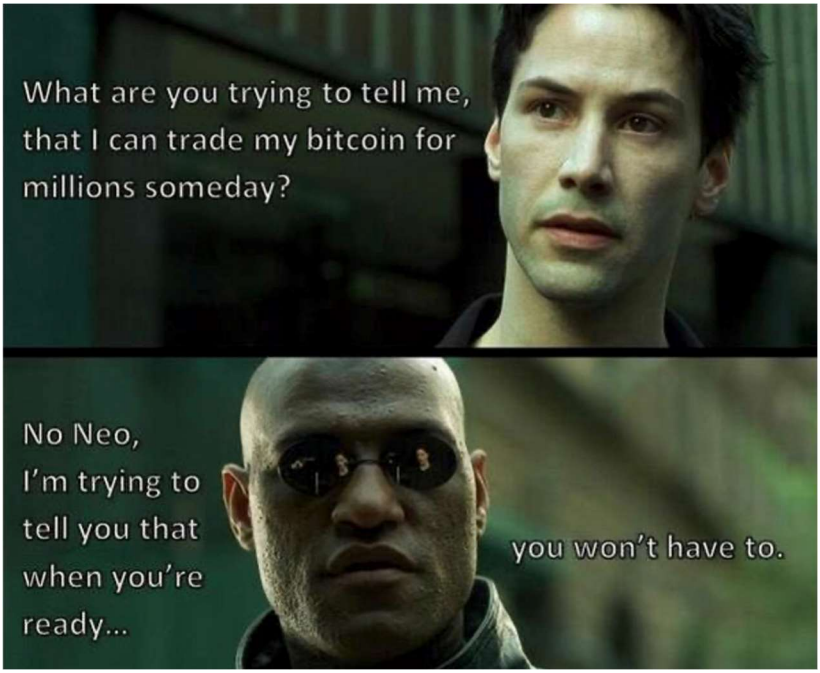
- Se você der um zoom no gráfico de preços do BTC/USD, verá que ele aumentou +31.296% desde 2009, com uma média de ~200% ao ano.

- As oscilações de preço refletem vários artigos de notícias, atualizações regulatórias, demanda do mercado, medo e entusiasmo. É uma montanha-russa!

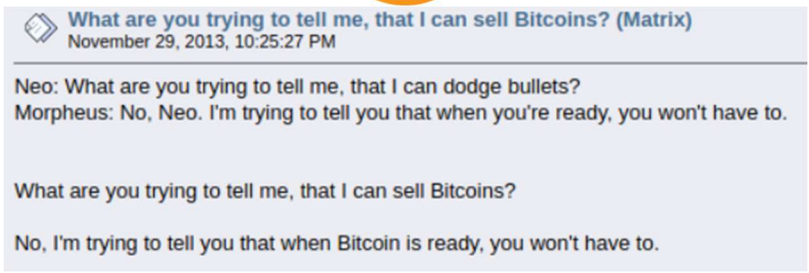
- **Quanto mais tempo você acumula, mais aprende e entende os fundamentos e mais percebe as profundas implicações de ter dinheiro sólido, menos o preço importa.**

- **No final, o "preço" não terá importância alguma, pois o bitcoin será a unidade de conta.**

- Dito isso, devo acrescentar esta isenção de responsabilidade: a recomendação geral é investir apenas o que você "pode se dar ao luxo de perder", já que, obviamente, não há garantias.



Neo: O que você está tentando me dizer? Que eu posso ganhar milhões negociando com meus bitcoins?
Morpheus: Não, Neo, o que estou tentando dizer é que quando você estiver pronto você não precisará fazer isso.
-The Matrix.



Fonte original do bitcointalkforum.org para um dos memes mais clássicos sobre bitcoin de todos os tempos.

ENQUANTO ISSO, FALEMOS SOBRE IMPOSTOS

>> Isenção de responsabilidade: este **não** é um conselho financeiro ou tributário!

- No código tributário dos EUA, o bitcoin é atualmente visto como uma commodity, portanto, há possíveis implicações tributárias se você o vender de volta em moeda fiduciária ou mesmo se comprar algo com seu bitcoin.

- Se o preço caiu antes de você vender/gastar, você pode alegar uma perda.

- Se o preço subiu, você deve declarar um ganho de capital e pagar entre 10 e 30% de CGT (imposto sobre ganhos de capital).

- O valor depende de vários fatores, como por quanto tempo você o manteve antes de vendê-lo ou gastá-lo e em qual faixa de imposto você se enquadra.

- Se você planeja vender ou gastar bitcoin, especialmente quantias maiores, pode considerar a possibilidade de consultar um profissional da área tributária.

- Se você simplesmente comprar e mantiver, atualmente não terá nenhum evento tributável relacionado à bitcoin.

- E se você comprar sem KYC...

POR QUE SOMENTE bitcoin?

Das mais de 20.000 (sim, 20.000!) criptomoedas existentes, o bitcoin é a ***única*** que é:

- **VERDADEIRAMENTE descentralizada**
- Com um **livro-razão VERDADEIRAMENTE distribuído**
- Com uma oferta **VERDADEIRAMENTE limitada**
- Um **livro-razão VERDADEIRAMENTE imutável**
- Um **efeito de rede** construído ao longo de 14 anos
- E uma **política monetária que não pode ser manipulada!**

- **Todas as outras criptomoedas têm um grupo pequeno e centralizado que controla o fornecimento e/ou tem o poder de alterar o protocolo da camada de base (política monetária).**

- **Isso é exatamente como o sistema bancário central fiduciário que vemos hoje.**

- Um poder centralizado como esse favorece a manipulação e a corrupção.

- Veja o golpe da pump/dump de altcoin descrito na página seguinte.
- Veja também:
- Podcast de Stephan Livera Pod (SLP306) with Guy Swann
- Uma lista de altcoin/defi rug-pulls (puxadas de tapete): **https://rekt.news/leaderboard**

- Infelizmente, isso é real e acontece diariamente com "criptos/tokens" que não o bitcoin.

- Há várias iterações, mas um dos tipos mais comuns é o seguinte:

Criação de Tokens: Um novo token de criptografia é criado (isso é muito mais fácil do que parece!)

Website: Geralmente, um site brilhante e sofisticado é criado para fazer com que o token pareça legítimo.

Influenciadores Pagos: Promovem-no nas mídias sociais.

Grupos Pagos de Informações Privilegiadas: As informações são enviadas aos líderes de algumas das centenas de grupos de "negociação" ou "investimento", onde as pessoas pagam taxas mensais ou anuais para obter "informações privilegiadas".

Pré Lançamento: Os influenciadores pagos e os líderes de grupos pagos compram primeiro, pelo preço mais baixo.

Lançamento: O token é "lançado" por esses influenciadores/líderes de grupo, que dizem a seus seguidores: "Rápido, compre agora!"

Pump: O preço sobe rapidamente à medida que seus seguidores se esforçam para comprar logo.

O rápido aumento do preço atrai as pessoas comuns a comprar, na esperança de fazer fortuna.

- O que, por sua vez, tem o efeito de aumentar ainda mais o preço.

- **Dump:** Essa parte triste geralmente acontece rapidamente. Em um determinado momento, os líderes do grupo pago vendem seus tokens, "no topo". Em seguida, eles dizem a seus seguidores para venderem.

- Como muitas pessoas vendem ao mesmo tempo e a liquidez geralmente é baixa por se tratar de uma moeda nova, o preço cai rapidamente.

- **Pânico:** A queda de preço causa pânico entre o público em geral, que não tem ideia dessas artimanhas secretas, e eles começam a vender em pânico.

- **Bag Holders:** O final dessa triste história é que aqueles que ficaram "segurando a sacola" (bag holders) provavelmente ficarão segurando suas sacolas para sempre

- Sem qualquer valor real ou fundamentos, a maioria desses tokens nunca recuperará um preço de mercado.

- **Fique com o bitcoin.**
- **Seja supervigilante quanto à sua segurança cibernética!**
- **Faça sua própria pesquisa** e **proteja seu bitcoin** com o máximo cuidado.

- **NUNCA forneça suas seeds a ninguém a quem você não daria a chave de seu estoque de ouro!**

- **NUNCA clique em nenhum link** em seu e-mail que solicite a confirmação de detalhes da conta de qualquer tipo. **Em vez disso, vá diretamente ao site oficial** e verifique se há algum aviso exigindo alguma ação.
- **ESTEJA CIENTE** de que há inúmeras imitações de contas com grande número de seguidores nas mídias sociais. Se um influenciador enviar uma DM aleatória para você, provavelmente é um golpe.
- **EVITE todos os golpes que aparecem nas contas de mídia social,** prometendo dobrar seu bitcoin se você enviar algum para eles! Não está acontecendo!
- **EVITE esses mesmos golpes de "dobrar sua criptografia" no** You Tube.
- **TENHA CERTEZA** do endereço para o qual está enviando bitcoin, pois as transações são irreversíveis.

O Bitcoin foi projetado para minerar *6* blocos por hora >> um bloco a cada ~10 minutos.

- 24 horas em um dia
  2+4=*6*

- Isso resulta em 144 blocos por dia
  1+4+4=*9*

- 52560 blocos por ano
  5+2+5+6+0=18
  1+8=*9*

- 52704 blocos por ano bissexto
  5+2+7+0+4=18
  1+8=*9*

- 21 milhões de moedas:
  2 + 1 + 0 + 0 + 0 + 0 + 0 + 0 = *3*

- 33 Halvings:
  3 + 3 = *6*

- A dificuldade é ajustada a cada 2016 blocos:
  2 + 0 + 1 + 6 = *9*

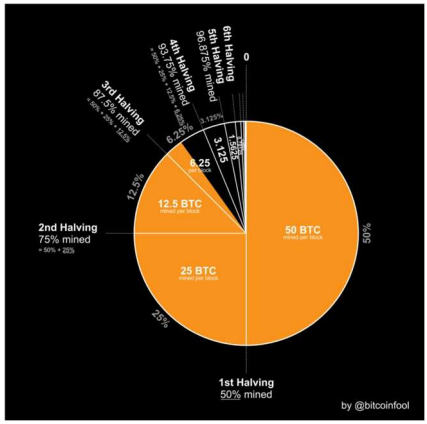
~ Baseado no Tweet de @level39

- A redução pela metade da recompensa do bloco ocorre a cada 210.000 blocos (a cada quatro anos)
  2 + 1 + 0 + 0 + 0 + 0 = *3*

"Se você conhecesse a magnificência do 3, 6 e 9, teria a chave do universo."
~ Nikola Tesla

RECOMPENSA DO BLOCO = % DO FORNECIMENTO

- A recompensa do bloco (número de bitcoins recompensados para cada novo bloco minerado) representa a porcentagem do suprimento total que será minerado durante essa época.
- Por exemplo, a recompensa de bloco atual entre 2020 e 2024 é de 6,25 bitcoins.
- Nesses mesmos quatro anos, 6,25% dos 21 milhões de bitcoins serão minerados.
- Satoshi, você continua surpreendendo.



Créditos: @bitcoinfool

A cada quatro anos, as recompensas do bitcoin são reduzidas pela metade para cada bloco minerado. Uma Recompensa por Época tem um período de quatro anos.

- **Recompensa época 1**: 2009-2012
= (50 bitcoin * 210.000 blocos) = 10.500,000 bitcoin
1+0+5+0+0+0+0+0 = *6*
- **Recompensa época 2**: 2012-2016
= (25 * 210.000) = 5.250,000 bitcoin
5+2+5+0+0+0+0 = 12
1+2 = *3*
- **Recompensa época 3**: 2016-2020
= (12,5 * 210.000) = 2.625,000 bitcoin
2+6+2+5+0+0+0 = 15
1+5 = *6*
- **Recompensa época 4:** 2020-2024
= (6,25 * 210.000) = 1.312,500 bitcoin
1+3+1+2+5+0+0 = 12
1+2 = *3*
- **Recompensa época 5:** 2024-2028
= (3,125 * 210.000) = 656.250 bitcoin
6+5+6+2+5+0 = 24
2+4 = *6*
- **Recompensa época 6:** 2028-2032
= (1.5625 * 210,000) = 328.125 bitcoin
3+2+8+1+2+5 = 21
2+1 = *3*
- **Recompensa época 7: 2032-2036**
= (0.78125*210,000) = 164.062.5 bitcoin
1+6+4+0+6+2+5 = 24
2+4 = *6*

ANIVERSÁRIO DE SATOSHI

- **5 de Abril de 1975** é a data que Satoshi declarou ser seu aniversário.
- Embora não possamos saber se essa foi de fato sua verdadeira data de nascimento, ela é muito interessante.
- **O dia 5 de abril** (1933) foi o dia em que a Ordem Executiva 6102 foi assinada pelo presidente dos Estados Unidos, Franklin D. Roosevelt, "proibindo o acúmulo de moedas de ouro, barras de ouro e certificados de ouro no território continental dos Estados Unidos.
- **1975** foi o ano em que a EO 6102 foi finalmente revogada, e os cidadãos norte-americanos puderam novamente possuir mais de 5 onças de ouro, mais de quatro décadas depois.

UM PALÍNDROMO A NUMERIC PALINDROME 6102-2016

- ***6102*** foi o número da Ordem Executiva mencionada acima.
- ***2016*** é o número de blocos minerados durante cada ajuste de dificuldade (aproximadamente 2 semanas).

➢ Em ambos os exemplos acima, pode-se postular que Satoshi estava usando números para indicar uma reversão, um desdobramento do dano infligido pelo excesso do governo.

- O dia 22 de maio é conhecido como o Bitcoin Pizza Day. Esse foi o dia em que um homem, chamado Laszlo Hanyecz, anunciou no bitcointalkforum.org que havia conseguido trocar 10.000 bitcoins por pizza! Naquela época, o valor era de cerca de US$ 40.
- Nos preços atuais, isso equivaleria a US$ 420.000.000 ☺
- Esse foi um marco para o bitcoin, pois foi o primeiro caso conhecido de alguém trocando bitcoin por um bem ou serviço. Que longo caminho percorrido!

laszlo
Full Member

Activity: 199
Merit: 1014

Re: Pizza for bitcoins?
May 21, 2010, 09:33:45 PM

I just think it would be interesting if I could say that I paid for a pizza in bitcoins

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

laszlo
Full Member

Activity: 199
Merit: 1014

Re: Pizza for bitcoins?
May 22, 2010, 07:17:26 PM
Merited by vizique (10), paxmao (10), vapourminer (1), Searing (1), BitcoinFX (1), 600watt (1), Toxic2040 (1), xtraelv (1), Spray. (1), TotSamiy (1), Aricoin (1), dektox (1)

I just want to report that I successfully traded 10,000 bitcoins for pizza.

Pictures: http://heliacal.net/~solar/bitcoin/pizza/

Thanks jercos!

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

sirius
Bitcoiner
Sr. Member

Activity: 429

Re: Pizza for bitcoins?
May 22, 2010, 10:10:25 PM
Merited by Aricoin (1)

Congratulations laszlo, a great milestone reached

5184x3456 (1/60) f/5.6 f(35)=78mm (flash)
2010-05-22 15:01:22 -0400

Download: IMG_0985.jpg

5184x3456 (1/60) f/5.6 f(35)=78mm (flash)
2010-05-22 15:01:29 -0400

Download: IMG_0986.jpg

CALENDÁRIO DE DIAS NOTÁVEIS DO BITCOIN

18-08-2008 ~ O nome de domínio bitcoin.org foi registrado.
(2+0+0+8+0+8+1+8 = 27, 2+7 = *9*)
31-10-2008 ~ Dia do White Paper do Bitcoin: O White Paper, intitulado "Bitcoin: A Peer-to-Peer Electronic Cash System" (Bitcoin: um sistema de dinheiro eletrônico ponto a ponto) foi publicado por um criptógrafo anônimo chamado Satoshi Nakamoto, na lista de discussão sobre criptografia em metzdowd.com
(2+0+0+8+1+0+3+1 = 15, 1+5 = *6*)
03-01-2009 ~ Aniversário do Bitcoin: A rede Bitcoin foi lançada, quando Satoshi extraiu o bloco Gênesis.
(2+0+0+9+0+1+0+3 = 15, 1+5 = *6*)
12-01-2009 ~ Ocorreu a primeira transação de bitcoin, quando Hal Finney recebeu dez bitcoins de Satoshi.
(2+0+0+9+0+1+1+2 = 15, 1+5 = *6*)
5 de Outubro de 2009 ~ Pela primeira vez, o Bitcoin tem um preço de mercado de US$ 0,001 por moeda.
22-05-2010 ~ Bitcoin Pizza Day: A primeira ocorrência conhecida de bitcoin sendo usado para comprar um bem ou serviço, quando Lazslo Hanyecz pagou 10.000 bitcoin por duas pizzas da Papa John's!
(2+0+1+0+5+2+2 = 12, 1+2 = *3*)
12-12-2010 ~ A última vez confirmada que Satoshi escreveu no fórum bitcointalk.org.
(2+0+1+0+1+2+1+2 = *9*)
8 de Fevereiro de 20122 ~ O Bitcoin atinge a paridade com o dólar americano pela primeira vez.
3 de Março de 2017 ~ O Bitcoin atinge a paridade com uma onça de ouro.
21 de Agosto de 2012 ~ 1° Dia do Infinito Bitcoin (Bitcoin Infinity Day) comemorado anualmente sugerido pelo meme de Knut Svanholm:
Tudo dividido por 21 milhões. $\frac{\infty}{21{,}000{,}000}$
07-09-2021 ~ El Salvador se torna o primeiro país a tornar o bitcoin moeda de curso legal.
(2+0+2+1+0+9+0+7 = 21, 2+1 = *3*)

Isso foi só o começo...

aqui estão mais

POR ONDE ENTRAR NA TOCA DO COELHO DO bitcoin

"Cada vez mais curioso! " disse Alice

FILMES

Você pode encontrar estes filmes no You Tube

FILMES SOBRE BITCOIN:

- The Great Reset and the Rise of Bitcoin (2022)
- Where Did Bitcoin Come From (2021)
- This Machine Greens (2021) About Bitcoin & Energy
- Bit X Bit: In Bitcoin We Trust (2018)
- Bitcoin Big Bang (2018) About the 2014 Mt Gox hack
- Magic Money: The Bitcoin Revolution (2017)
- Banking on Bitcoin (2016)
- Deep Web (2015) About Silk Road & Ross Ulbricht
- The Bitcoin Gospel (2015)
- Bitcoin: The End of Money as We Know It (2015)
- The Rise and Rise of Bitcoin (2014)
- Bitcoin in Uganda (2014)

FILMES SOBRE DE DINHEIRO FIDUCIÁRIO (SISTEMA FIAT):

- How is Money Created (2020)
- Hidden Secrets of Money Series - Mike Maloney ('13-'18)
- Who Controls All of our Money (2017)
- How the Economic Machine Works - Ray Dalio (2013)
- Inside Job (2010) - On events leading up to 2008 crash
- The Money Masters (1996)

LIVROS

SOBRE BITCOIN:

- **Layered Money** by Nik Batia
- **21 Lessons** by DerGigi
- **The Bullish Case for Bitcoin** by Vijay Boyapati
- **The Bitcoin Standard** by Saifedean Ammous
- **Bitcoin Clarity** by Kiara Bickers
- **Inventing Bitcoin** by Yan Pritzker
- **Independence Reimagined** & **Bitcoin: Sovereignty Through Mathematics** by Knut Svanholm
- **Check Your Financial Privilege** by Alex Gladstein
- **Hard Money You Can't F*ck With** by Jason A.Williams
- **Why Buy Bitcoin** by Andy Edstrom
- **Bitcoin Audible:** If you prefer listening to reading, Guy Swann, reads Bitcoin books and articles.

SOBRE O ATUA SISTEMA MONETÁRIO FIDUCIÁRIO BASEADO EM DÍVIDA:

- **The Price of Tomorrow** by Jeff Booth
- **The Sovereign Individual** by JD Davidson and Lord W Rees-Mogg (not only about money)

PODCASTS

Ouça no aplicativo Fountain, você e os apresentadores ganham sats por ouvir.

Se ainda não estiver no Fountain, encontre-os no Spotify e no iTunes.

- **Citadel Dispatch** with Matt Odell
- **BitBuyBit Podcast** with Max Buybit
- **Bitcoin Rapid Fire** with John Vallis
- **The "What is Money" Show** with Robert Breedlove
- **Stephan Livera Podcast**
- **This is Bitcoin Podcast** with Bitcoin Gandalf
- **Wake Up Podcast** with Aleks Svetski
- **Coin Stories** with Nat Brunell
- **The Bitcoin Standard Podcast** with Dr S. Ammous
- **Bitcoin Magazine Podcast**
- **The Bitcoin Matrix** with Cedric Youngelman
- **Bitcoin Fixes This** with Jimmy Song
- **Orange Pill Podcast** with Max Keiser and Stacy Herbert
- **What Bitcoin Did** with Peter McCormack

- **Bitcoin Audible** with Guy Swann reading books/articles

CURSOS GRATUITOS

- **Saylor Academy** - Bitcoin for Everybody: Free Course
- **Bitcoin Magazine** - 21 Days of Bitcoin Daily Lessons

WEBSITES

Cada um deles tem uma grande compilação de conteúdo:

- Nakamotoinstitute.org
- Bitcoinmagazine.com
- Bitcoin-only.com
- Bitcoin Wiki - En.bitcoin.it
- Lopp.net
- Casebitcoin.com
- Bitcoiner.guide
- Bitcoin.tv
- Learnmeabitcoin.com – Simples e ótima explicação técnica sobre btc!
- Hope.com
- Bitcoin-resources.com
- Myfirstbitcoin.io (disponível em espanhol)

Por dentro do coração pulsante do Bitcoin:

- github.com/bitcoin

CAIXAS ELETRÔNICOS DE BITCOIN

- **Coin ATM Finder** - coinatmfinder.com
- **Coin Radar** - coinatmradar.com

ARTIGOS

- Bitcoinmagazine.com - Excelente, novos artigos diariamente!
- Muitas contas do Twitter abaixo escrevem no Medium, Substack

BT ~ BITCOIN TWITTER

Alguns cypherpunks, gênios e selvagens para seguir!
Por meio dessas contas, você encontrará milhares de plebeus e
outros pensadores profundos,
todos em sua jornada.
A BT é, em grande parte, onde este experimento está crescendo,
desenrolando-se em tempo real, através do tempo e do espaço,
nos éteres do ciberespaço, conectado ao físico,
por meio de todos nós,
humanos,
compartilhando uma visão.
Há também os mais silenciosos, os desenvolvedores que trabalham
nos bastidores
sem os quais
nada disso seria possível.
Todos nós
juntos
soltos,
como o bitcoin foi entregue para nós,
uma bênção incomensurável.

OS TÓPICOS INCLUEM: Bitcoin, Prova de Trabalho, Privacidade, Filosofia, História Monetária, Código, Mineração de Bitcoin, Sociologia, Teoria dos Jogos, Economia Austríaca, Educação em Bitcoin, Rede Lightning, Ambiente Regulatório, Uso de Energia do Bitcoin, Desenvolvedores Principais, Comunidades Bitcoin, Futuro do Bitcoin.

Esteja ciente: Ter a casca grossa Twitter é importante e saiba que há muita paixão em defesa do bitcoin. Manter uma linha clara entre ela e todas as altcoins dá trabalho. Manter a clareza, a segurança e a pureza do único dinheiro verdadeiramente sólido que o mundo já conheceu é fundamental se quisermos ter uma chance de prosperar nestes tempos que estão chegando.

Adam Back - @adam3us
Allen Farrington - @allenf32
Anil - @anilsaidso
Arman the Parman - @parman_the
Bitcoin Gandalf - @BTCGandalf
Bitcoin Q+A - @BitcoinQ_A
BTC Sessions - @BTCsessions
BTC Times - @btc
Brandon Quittem - @Bquittem
D++ - @D_plus__plus
Dylan Le Clair - @DylanLeClair_
Gigi - @dergigi
Greg Foss - @FossGregfoss
Guy Swann - @TheGuySwann
Hugo Nguyen - @hugohanoi
Jameson Lopp - @lopp
Jeff Booth - @JeffBooth
Jimmy Song - @jimmysong
Knut Svanholm - @knutsvanholm
Luke Dash Jr - @LukeDashjr
Lyn Alden - @LynAldenContact
Marty Bent - @MartyBent
Matt Odell - @ODELL
Michael Saylor - @saylor
Natalie Brunell - @natbrunell
Nayib Bukele - @nayibbukele
Nick Szabo - @NickSzabo4
Nik Bhatia - @timevalueofbtc
Parker Lewis - @parkeralewis
Pleb Lab - @PlebLab
Preston Pysh - @PrestonPysh
Tomer Strolight - @TomerStrolight
Troy Cross - @thetrocro
Vijay Boyapati - @real_vijay

Obrigado a todos vocês por me ensinar todos os dias!

PROJETOS DA COMUNIDADE bitcoin

- **Abaixo estão alguns dos projetos de base em todo o mundo que estão trabalhando para criar uma economia circular e local com bitcoin**

- Siga os projetos no Twitter para saber mais ou para fazer doações:

- **Bitcoin Beach El Zonte** - El Salvador - @Bitcoinbeach

- **Bitcoin Ekasi** - Mossel Bay, South Africa - @BitcoinEkasi (Supports Surfer Kids NGO)

- **Bitcoin Beach Brazil** - Jericoacoara, Brazil - @BitcoinBeachBR

- **Bitcoin Jungle Costa Rica** - Dominical, CR - @BitcoinJungleCR

- **Bitcoin Venezuela** - Venezuela - @btcven

- **Bitcoin Smiles Dentistry** - El Salvador - @BitcoinSmiles

- **Saul M - El Salvador** - Chalatenango - @saulhodl

- **Apata Johnson - Nigeria** - @ApataJ

- **Bitcoin Lake** - Lake Atitlan - @LakeBitcoin

Agradecimentos a
Satoshi
e a todos os
orangepillados
sonhadores
videntes
magos cyphepunks
poetas da liberdade
guardiões da sabedoria
indivíduos soberanos
caçadores de último recurso
avançando sem medo
sozinhos e juntos
pela liberdade
Vires In Numeris!

O Bitcoin é realmente uma "coisa" bastante fascinante
Só que não é uma "coisa
No sentido de que você não pode tocá-lo
No entanto, ele está tocando milhões de pessoas
Em todo o mundo
Em breve, bilhões...
É verdade que
São bits e bytes digitais
Algoritmos e códigos
0's e 1's
E que se cada nó único
Nó de mineração, nó completo e nó de luz
Fossem de alguma forma
Destruídos
Ele não existiria mais
Da forma como o conhecemos
Seríamos capazes de percebê-lo.
No entanto, ele ainda "existiria
No sentido em que a física quântica
Ou a gravidade
Existe
Independentemente da percepção humana.
No sentido de que a matemática existia
Antes que os humanos a codificassem
Escolheram símbolos para representá-la...
A verdade
Não precisa de nós

POR QUE TODO O VALOR SE ACUMULARÁ NO BITCOIN

- Existem algumas teorias dos jogos interessantes que parecem convergir quando se trata de bitcoin, tornando cada vez mais certa a probabilidade de seu crescimento e aumento de valor ao longo do tempo.

PONTO DE SCHELLING

- Introduzido na década de 1960 pelo economista americano Thomas Schelling, o ponto de Schelling basicamente afirma que **as pessoas que não podem necessariamente se comunicarem umas com as outras ainda podem convergir em uma decisão ou curso de ação, especialmente quando uma solução convincente para um problema se apresenta** (-> bitcoin)

- Além disso, à medida que mais pessoas são atraídas para o ponto de Schelling, ele atrai cada vez mais pessoas (-> bitcoin)

EFEITO LINDY

- Em essência, o Efeito Lindy afirma **que quanto mais tempo uma ideia, uma tecnologia ou uma empresa estiver em vigor, maior será a probabilidade de ela perdurar.**

LEI DE METCALFE

- Popularizada por Robert Metcalfe, que inventou a Ethernet, entre outras coisas. A lei de Metcalfe afirma que uma **rede se torna proporcionalmente mais valiosa quanto mais usuários ela tiver**. A utilidade aumenta exponencialmente à medida que mais e mais usuários aderem, fortalecendo a Web.

É um banco de dados distribuído global, com acréscimos ao banco de dados por consentimento da maioria...

~ Satoshi Nakamoto 18-02-2009

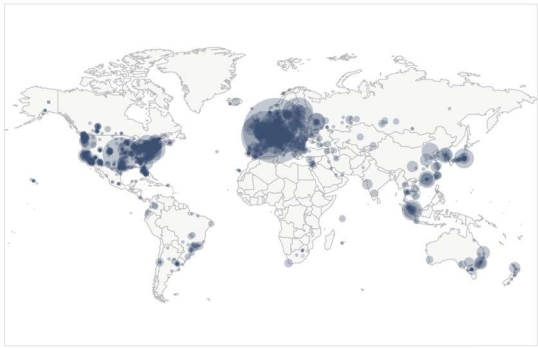
GLOBAL BITCOIN NODES DISTRIBUTION
Reachable nodes as of Sun Feb 6 17:46:46 2022 CST.

15147 NODES 24h 90d 1y

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	n/a	8108 (53.53%)
2	United States	1781 (11.76%)
3	Germany	1750 (11.55%)
4	France	540 (3.57%)
5	Netherlands	384 (2.54%)
6	Canada	288 (1.90%)
7	United Kingdom	231 (1.53%)
8	Finland	200 (1.32%)
9	Russian Federation	162 (1.07%)
10	Switzerland	120 (0.79%)

More (85) »



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

Distribuição global de nós de Bitcoin visíveis

O resultado é um sistema distribuído sem um único ponto de falha. Os usuários detêm as chaves criptográficas de seu próprio dinheiro e fazem transações diretamente entre si, com a ajuda da rede P2P para verificar se há gastos duplos.

~ Satoshi Nakamoto 11-02-2009

BITCOIN, COMUNICAÇÃO NÃO VIOLENTA & PERMACULTURA

Eu vejo o **Bitcoin**, trazido a nós por Satoshi Nakamoto, como sendo a camada de base para uma sociedade saudável no que diz respeito:

- **comunicação de valor**
- **transações e trocas**
- **armazenamento de nosso tempo/energia vital**

em um desdobramento emergente, orgânico e honesto.

Eu vejo a **Comunicação Não Violenta**, trazida a nós por Marshall Rosenberg PhD, como a camada de base para uma sociedade saudável no que diz respeito a:

- **comunicação de sentimentos e necessidades**
- **escuta profunda, empatia**
- **encontrar soluções cocriativas**

em um desdobramento emergente, orgânico e honesto.

Vejo a **Agricultura Natural e a Permacultura**, trazidas a nós por nossos ancestrais e, mais recentemente, por Masunobu Fukuoka e Bill Mollison, como sendo a camada de base para uma sociedade saudável no que diz respeito a:

- **comunicação com a terra**
- **cultivo de alimentos, cura do solo**
- **cuidado da natureza**

em um desdobramento emergente, orgânico e honesto.

Cada uma dessas tecnologias, uma matemática, que nos leva além da matemática, uma linguística, que nos leva além da linguagem, e uma biológica, que nos leva além da biologia, são baseadas na Verdade.

Cabe a nós fazer uso delas, vivê-las e permitir que elas nos guiem cada vez mais profundamente para o profundo potencial que sentimos formigando nas pontas de nossa percepção.

Que possamos encontrar a coragem, a força,
a sabedoria e a graça
para avançar sem medo
na jornada.

A privacidade é necessária para uma sociedade aberta na era eletrônica. Privacidade não é segredo. Um assunto particular é algo que não se quer que o mundo inteiro saiba, mas um assunto secreto é algo que não se quer que ninguém saiba. Privacidade é o poder de se revelar ao mundo de forma seletiva.

Se duas partes têm algum tipo de negociação, cada uma delas tem uma memória de sua interação. Cada parte pode falar sobre sua própria memória disso; como alguém poderia impedir isso? Poderíamos aprovar leis contra isso, mas a liberdade de expressão, ainda mais do que a privacidade, é fundamental para uma sociedade aberta; procuramos não restringir nenhuma expressão. Se muitas partes falam juntas em um mesmo fórum, cada uma pode falar com todas as outras e agregar conhecimento sobre indivíduos e outras partes. O poder das comunicações eletrônicas possibilitou esse tipo de discurso em grupo, e ele não desaparecerá simplesmente porque queremos que isso aconteça.

Como desejamos privacidade, devemos garantir que cada parte de uma transação tenha conhecimento apenas do que é diretamente necessário para essa transação. Como é possível falar sobre qualquer informação, devemos nos certificar de que revelaremos o mínimo possível. Na maioria dos casos, a identidade pessoal não é importante. Quando compro uma revista em uma loja e entrego o dinheiro ao funcionário, não há necessidade de saber quem eu sou.
Quando peço ao meu provedor de correio eletrônico para enviar e receber mensagens, ele não precisa saber com quem estou falando, o que estou dizendo ou o que os outros estão dizendo para mim; ele só precisa saber como enviar a mensagem e quanto devo em taxas. Quando minha identidade é revelada pelo mecanismo subjacente da transação, não tenho privacidade. Não posso me revelar de forma seletiva; devo sempre me revelar. Portanto, a privacidade em uma sociedade aberta exige sistemas de transações anônimas. Até agora, o dinheiro tem sido o principal sistema desse tipo. Um sistema de

transações anônimas não é um sistema de transações secretas. Um sistema anônimo permite que os indivíduos revelem sua identidade quando desejarem e somente quando desejarem; essa é a essência da privacidade.

A privacidade em uma sociedade aberta também exige criptografia. Se eu disser algo, quero que seja ouvido apenas por aqueles a quem me dirijo. Se o conteúdo de minha fala estiver disponível para o mundo, não terei privacidade. Criptografar é indicar o desejo de privacidade, e criptografar com criptografia fraca é indicar um desejo não muito grande de privacidade. Além disso, revelar a própria identidade com segurança quando o padrão é o anonimato requer a assinatura criptográfica. Não podemos esperar que governos, corporações ou outras organizações grandes e sem rosto nos concedam privacidade por sua beneficência.
É vantajoso para eles falar sobre nós, e devemos esperar que eles falem. Tentar impedir que falem é lutar contra as realidades da informação. A informação não quer apenas ser livre, ela anseia por ser livre. As informações se expandem para preencher o espaço de armazenamento disponível. A informação é a prima mais nova e mais forte do boato; a informação é mais ágil, tem mais olhos, sabe mais e entende menos do que o boato.

Precisamos defender nossa própria privacidade se quisermos ter alguma. Precisamos nos unir e criar sistemas que permitam a realização de transações anônimas. As pessoas têm defendido sua privacidade há séculos com sussurros, escuridão, envelopes, portas fechadas, apertos de mão secretos e mensageiros. As tecnologias do passado não permitiam uma privacidade forte, mas as tecnologias eletrônicas permitem.

Nós, os Cypherpunks, nos dedicamos a criar sistemas anônimos. Estamos defendendo nossa privacidade com criptografia, com sistemas de encaminhamento de correspondência anônima, com assinaturas digitais e com dinheiro eletrônico.

Os Cypherpunks escrevem códigos. Sabemos que alguém precisa escrever software para defender a privacidade e, como não conseguiremos privacidade a menos que todos nós o façamos,

nós o escreveremos. Publicamos nosso código para que nossos colegas Cypherpunks possam praticar e brincar com ele.

Nosso código é gratuito para ser usado por todos, em todo o mundo. Não nos importamos muito se você não aprova o software que escrevemos. Sabemos que o software não pode ser destruído e que um sistema amplamente disperso não pode ser desligado.

Os cypherpunks deploram as regulamentações sobre criptografia, pois a criptografia é fundamentalmente um ato privado. O ato de criptografar, de fato, remove as informações do domínio público. Mesmo as leis contra a criptografia alcançam apenas a fronteira de uma nação e o braço de sua violência.
A criptografia se espalhará inelutavelmente por todo o globo e, com ela, os sistemas de transações anônimas que ela possibilita.

Para que a privacidade seja disseminada, ela deve fazer parte de um contrato social. As pessoas devem se unir e implantar esses sistemas para o bem comum. A privacidade só se estende até o limite da cooperação de seus companheiros na sociedade. Nós, os Cypherpunks, buscamos suas dúvidas e preocupações e esperamos poder envolvê-los para que não nos enganemos. No entanto, não nos desviaremos de nosso curso porque alguns podem discordar de nossos objetivos.
Os Cypherpunks estão ativamente empenhados em tornar as redes mais seguras para a privacidade. Vamos prosseguir juntos em um ritmo acelerado.Em frente.
Eric Hughes <hughes@soda.berkeley.edu>
9 de Março de 1993

(A ênfase em **negrito** é coisa minha)

ALGUNS DOS PRIMEIROS CYPHERPUNKS

que podemos agradecer por contribuírem para o desenvolvimento do dinheiro digital ponto a ponto

- **Satoshi Nakamoto** - cypherpunk anônimo que apresentou o bitcoin ao mundo em 2009.
- **Nick Szabo** - Bit Gold 2005
- **Hal Finney** - Prova de Trabalho Reutilizável (RPoW) de 2004, autor do PGP 2.0. Segunda pessoa a executar o cliente bitcoin. Recebeu a primeira transação de bitcoin de 10 bitcoins de Satoshi Nakamoto
- **Wei Dai** - B-money 1998
- **Dr Adam Back** - HashCash 1997 - CEO da Blockstream
- **Douglas Jackson and Barry Downey** - E Gold 1996
- **John Gilmore**
- **Timothy C.May**
- **Eric Hughes**

Fundadores do movimento Cypherpunk e da lista de discussão em 1992.

- **Philip Zimmermann**: 1991 PGP 1.0, a criptografia de e-mail mais usada atualmente
- **David Chaum** - Ecash 1983 e DigiCash 1989

O White Paper do bitcoin

Apresentado ao mundo em metzdowd.com
31-10-2008

por Satoshi Nakamoto

Um cypherpunk pseudônimo, que se comunicou pela última vez com a comunidade cypherpunk no fórum bitcointalk.org em 10-12-2010.

Ao sair, ele permitiu que o Bitcoin fosse um verdadeiro experimento na natureza. Todos os que trabalham nele são voluntários em algum sentido <-> inspirados pelo potencial de libertar a humanidade dos grilhões de um sistema monetário manipulado e baseado em dívidas e, em vez disso, participar de uma rede global, sem terceiros de confiança, sem permissão, resistente à censura, verdadeiramente escassa, peer-to-peer, descentralizada de dinheiro e pagamentos monetários, que está inspirando uma ordem emergente a surgir das cinzas fiduciárias.

Todos somos Satoshi

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

~ Texto de uma manchete do The Times de Londres, gravada no bloco Bitcoin Genesis por Satoshi Nakamoto em 03-01-2009

Bitcoin: Um Sistema de Dinheiro Eletrónico Ponto-a-Ponto

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Translated in Portuguese from bitcoin.org/bitcoin.pdf
by @rhlinden

Sinopse. Uma versão puramente ponto-a-ponto de dinheiro eletrónico permitiria o envio de pagamentos interativos diretamente de um interveniente para outro sem passar por uma instituição financeira. Assinaturas digitais proporcionam parte da solução, mas os principais benefícios perdem-se se continuar a ser necessária uma terceira entidade de confiança para evitar gastos duplos. Propomos uma solução para o problema do gasto duplo usando uma rede ponto-a-ponto. A rede marca a hora nas transações codificando-as numa cadeia continua de provas-de-trabalho baseada em *hash*, formando um registo que não pode ser alterado sem refazer a prova-de-trabalho. A cadeia mais longa, não só serve de prova da sequência de acontecimentos testemunhados, mas prova que tem origem no grupo de maior capacidade de processamento. Desde que a maioria da capacidade de processamento seja controlada por nós que não estejam conjugados para atacar a rede, eles produzirão a cadeia mais longa e prevalecerão sobre atacantes. A própria rede necessita uma estrutura mínima. As mensagens são difundidas numa base do melhor esforço, e os nós podem abandonar e reintegrar a rede à vontade, aceitando a cadeia mais longa de provas-de-trabalho como prova do que aconteceu enquanto estiveram fora.

1. Introdução

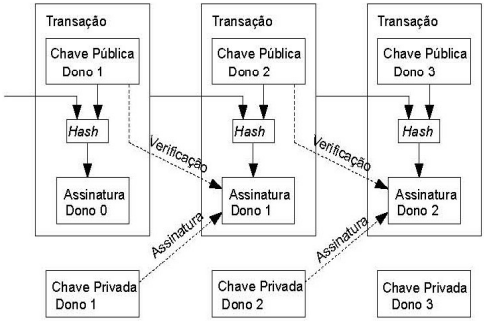
O comércio na Internet vem dependendo quase exclusivamente de instituições financeiras atuando como terceira parte de confiança para o processamento de pagamentos eletrónicos. Embora o sistema funcione suficientemente bem para a maioria das transações, continua a sofrer das fraquezas inerentes ao modelo baseado na confiança. Transações completamente irreversíveis não são possíveis, uma vez que as instituições financeiras não podem evitar a mediação de disputas. O custo da mediação aumenta os custos da transação, limitando o tamanho mínimo praticável e restringindo a possibilidade de pequenas transações casuais, e há um custo mais alargado na perda da capacidade de efetuar pagamentos irreversíveis de serviços irreversíveis. Com a possibilidade de reembolso, a necessidade de confiança aumenta. Os comerciantes devem ser cuidadosos com os seus clientes, exigindo mais informação que a de outra forma seria necessária. Uma certa percentagem de fraude é aceite como inevitável. Estes custos e incertezas do pagamento podem ser evitadas usando moeda física em pessoa, mas não existe mecanismo para fazer pagamentos sobre um canal de comunicações sem uma terceira parte de confiança.

O que é necessário é um sistema eletrónico de pagamento baseado em prova criptográfica e não em confiança, permitindo a duas partes interessadas transacionar diretamente sem a necessidade de uma terceira parte de confiança. Transações de reversão computacionalmente impraticável protegeriam os vendedores da fraude, e mecanismos de garantia podem ser facilmente implementados para proteger compradores. Neste trabalho, propomos uma solução para o problema do gasto duplo usando um servidor distribuído ponto-a-ponto de marcas

temporais para gerar prova computacional da ordem cronológica das transações. O sistema é seguro enquanto os nós honestos controlarem coletivamente mais capacidade de processamento que qualquer grupo coodenado de nós atacantes.

2. Transações

Definimos uma moeda eletrónica como uma cadeia de assinaturas digitais. Cada proprietário transfere a moeda para o próximo assinando digitalmente um *hash* da transação anterior e a chave pública do próximo proprietário e adicionando estas ao fim da moeda. Um recetor pode verificar as assinaturas para verificar a cadeia de propriedade.

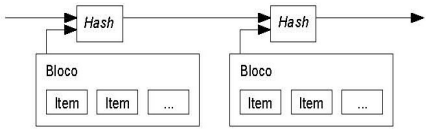


O problema obviamente é que o recetor não pode verificar se um dos proprietários anteriores não terá gasto duas vezes a mesma moeda. Uma solução comum é introduzir uma autoridade central de confiança, ou emissor, que verifique cada transação para gasto duplo. A cada transação, a moeda deveria retornar ao emissor que emitiria então uma nova moeda, e apenas as moedas emitidas diretamente pelo emissor teriam a garantia de não terem sido gastas duas vezes. O problema desta solução é que todo o sistema monetário dependeria da empresa encarregada do emissor, e cada transação teria que passar por ele, tal como um banco.

Precisamos de uma forma do recetor saber que os proprietários anteriores não assinaram nenhuma transação anteriormente. Para este propósito, a transação mais antiga é a transação que conta, pelo que não nos interessam tentativas posteriores de gasto duplo. A única forma de confirmar a falta de uma transação é ter conhecimento de todas as transações. No modelo baseado num emissor, o emissor conhecia todas as transações e saberia qual chegou primeiro. Para conseguir isso sem uma parte de confiança, as transações precisam ser anunciadas publicamente [1], e precisamos de um sistema em que os participantes acordem num único histórico da ordem em que elas foram recebidas. O recetor precisa da prova que na altura de cada transação, a maioria dos nós concordou que ela foi a primeira a ser recebida.

3. Servidor de Marca Temporal

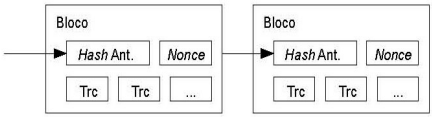
A solução que propomos começa com um servidor de marca temporal. Um servidor de marca temporal funciona usando um *hash* de um bloco de items a ser marcados temporalmente e publicando o *hash* amplamente, como num jornal ou um publicação na Usenet [2-5]. A marca temporal prova que os dados tiveram que existir nessa altura, evidentemente, para que tivessem sido incluídos no *hash*. Cada marca temporal inclui a marca temporal anterior no seu *hash*, formando uma corrente, com cada marca temporal reforçando a anterior.



4. Prova-de-Trabalho

Para implementar um servidor de marca temporal distribuído numa base ponto-a-ponto, precisamos usar um sistema de prova-de-trabalho similar ao de Adam Back Hashcash[6], em vez de um jornal ou publicação na Usenet. A prova-de-trabalho implica procurar um valor que quando codificado, por um algoritmo tal como SHA-256, o *hash* comece por um número de bits zero. O trabalho médio necessário é exponencial com o número de bits zero necessários e pode ser verificado executando um único *hash*.

Para a nossa rede de marcas temporais, implementamos a prova-de-trabalho incrementando um *nonce* no bloco até encontrar um valor que produza o *hash* do bloco com os bits zero necessários. Uma vez despendido o esforço de processamento para satisfazer a prova-de-trabalho, o bloco não pode ser modificado sem refazer o trabalho. Como os blocos seguintes são encadeados após, o trabalho para modificar o bloco inclui também refazer todos os blocos seguintes.



A prova-de-trabalho também resolve o problema de determinar a representatividade na tomada de decisão da maioria. Se a maioria fosse baseada em um-endereço-IP-um-voto, poderia ser subvertida por alguém capaz de reservar muitos IPs. Prova-de-trabalho é essencialmente um-processador-um-voto. A decisão da maioria é representada pela cadeia mais longa, que tem investido em si o maior esforço de prova-de-trabalho. Se a maioria da capacidade de processamento for controlada por nós honestos, a cadeia honesta crescerá mais rapidamente e ultrapassará qualquer cadeia concorrente. Para modificar um bloco anterior, um atacante teria que refazer a prova-de-trabalho desse bloco e de todos os blocos seguintes e ainda alcançar e ultrapassar o trabalho dos nós honestos. Vamos mostrar adiante que a probabilidade de um atacante lento alcançar os honestos diminui exponencialmente à medida blocos subsequentes são adicionados.

Para compensar a velocidade crescente do hardware e a variação de interesse em manter nós em execução ao longo do tempo, a dificuldade da prova-de-trabalho é determinada por uma média variável visando um número médio de blocos por hora. Se forem gerados muito rápido, a dificuldade aumenta.

5. Rede

Os passos para manter a rede são os seguintes:

1) Novas transações são difundidas para todos os nós.
2) Cada nó recolhe novas transações para um bloco.
3) Cada nó tenta encontrar uma prova-de-trabalho difícil para o seu bloco.
4) Quando um nó encontra uma prova-de-trabalho, difunde o bloco para todos os nós.

5) Os nós aceitam o bloco apenas se todas as transações neste são válidas e não foram ainda gastas.
6) Os nós expressam a aceitação do bloco criando o próximo bloco na cadeia, usando o hash do bloco aceite como o hash anterior.

Os nós consideram sempre a cadeia mais comprida como a correta e continuaram a tentar aumentá-la. Se dois nós difundirem versões diferentes do bloco seguinte simultaneamente, alguns nós poderão receber um ou o outro em primeiro lugar. Nesse caso, processam o primeiro recebido, mas guardam o outro ramo caso venha a ser maior. O desempate faz-se quando a próxima prova-de-trabalho for determinada e um ramo ficar maior; os nós que estavam a processar o outro ramo mudarão para o maior..

A difusão de novas transações não necessita chegar necessariamente a todos os nós. Desde que chegue a bastantes nós, eles acabarão por determinar um bloco. As difusões de blocos também toleram a perda de mensagens. Se um nó não receber um bloco, irá solicitá-lo quando receber o próximo bloco e constatar que faltou um.

6. Incentivo

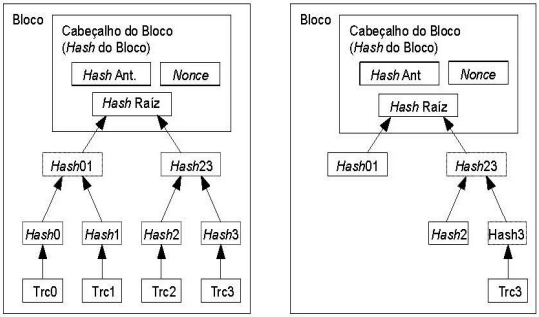
Por convenção, a primeira transação de um bloco é uma transação especial que inicía uma nova moeda de propriedade do criador desse bloco. Isto dá um incentivo para os nós suportarem a rede, e constitui uma forma de introduzir moedas em circulação uma vez que não há uma autoridade central que as emita. A constante adição de uma quantidade constante de novas moedas é semelhante a mineiros gastando recursos para adicionar ouro à circulação. No nosso caso, tempo de processamento e eletricidade investidos.

O incentivo também pode ser financiado por taxas sobre as transações. Se o valor de saída de uma transação for menor que o valor de entrada, a diferença é a taxa que é adicionada ao valor do incentivo do bloco que contem a transação. Depois de um determinado número de moedas entrar em circulação, o incentivo pode passar a ser exclusivamente constituído por taxas sobre a transação e completamente livre de inflação.

O incentivo pode encorajar os nós a permanecer honestos. Se um atacante ganancioso conseguir reunir maior capacidade de processamento que todos os nós honestos, terá ainda que escolher entre usá-la para enganar as pessoas roubando os seus pagamentos, ou usá-la para gerar novas moedas. Deverá achar mais rentável cumprir as regras, as mesmas que o favorecem com mais novas moedas que todos os restantes em conjunto, que comprometer o sistema e a validade da sua própria riqueza.

7. Recuperação do Espaço em Disco

Depois da última transação de uma moeda ter sido sobreposta por um número suficiente de blocos, as transações de despesa anterior podem ser descartadas para poupar espaço em disco. Para facilitar esse objetivo sem comprometer o *hash* do bloco, as transações são codificadas numa árvore Merkle [7][2][5], incluindo apenas a raiz no *hash* do bloco. Blocos antigos podem ser compactados removendo ramos da árvore. Os *hashes* interiores não necessitam ser mantidos.



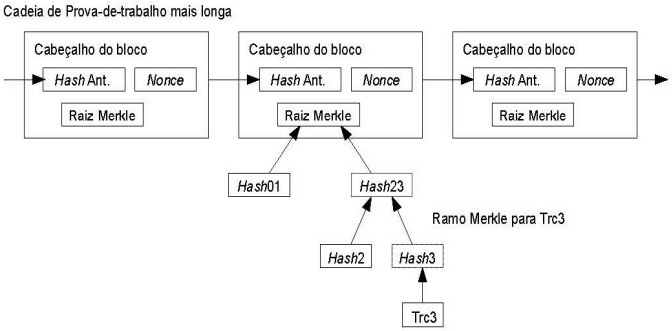
Transações *Hashed* numa árvore Merkle

Depois de remover Trc0-2 do Bloco

Um cabeçalho de bloco sem transações deverá ter cerca de 80 bytes. Se considerarmos blocos gerados a cada 10 minutos, 80 bytes * 6 * 24 * 365 = 4.2MB por ano. Com computadores a ser vendidos tipicamente com 2GB de RAM em 2008, e a Lei de Moore prevendo o crescimento de 1.2GB por ano, o armazenamento não deverá ser um problema mesmo que os blocos tenham que ser mantidos em memória.

8. Verificação de Pagamento Simplificada

É possível verificar pagamentos sem operar um nó de rede completo. O utilizador só necessita manter uma cópia dos cabeçalhos de bloco da cadeia de maior prova-de-trabalho, que pode obter questionando nós de rede até estar convencido que obteve a mais longa, e obter o ramo Merkle ligando a transação ao bloco com a marca temporal correspondente. Não pode confirmar a transação por si próprio, mas ao estabelecer uma relação com um ponto da cadeia, pode verificar que um nó da rede a aceitou, e blocos posteriores confirmam ainda que a rede a aceitou.

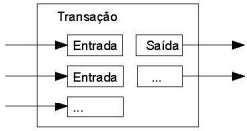


Assim a verificação é confiável desde que os nós honestos controlem a rede, mas é mais vulnerável se a rede for dominada por um atacante. Apesar dos nós da rede poderem verificar eles próprios transações, o método simplificado pode ser enganado por transações fabricadas de um atacante enquanto este puder continuar a dominar a rede. Uma estratégia para proteger contra isso seria aceitar alertas dos nós da rede quando estes detetam um bloco inválido, solicitando ao software do utilizador para descarregar o bloco e as transações sujeitas ao alerta para confirmar a inconsistência. Empresas que recebam pagamentos frequentes ainda vão querer provavelmente

operar os seus próprios nós para mais segurança independente e rápida verificação.

9. Combinando e dividindo valores

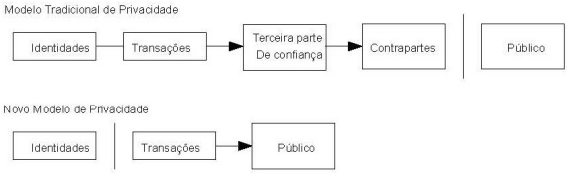
Embora fosse possível gerir moedas individualmente, seria trabalhoso fazer uma transação separada para cada cêntimo de uma transferência. Para permitir a divisão e combinação de valor, as transações contêm múltiplas entradas e saídas. Normalmente haverá uma entrada única de uma transação maior anterior ou múltiplas entradas combinando montantes inferiores, e no máximo duas saídas: uma para o pagamento, e uma devolvendo o troco, se houver, de volta para o remetente.



De notar que a dispersão, onde uma transação depende de múltiplas transações, e essas dependem de ainda mais, não representa um problema. Nunca há a necessidade de extrair uma cópia completamente independente da história de uma transação.

10. Privacidade

O modelo bancário tradicional obtém algum nível de privacidade limitando o acesso à informação às partes envolvidas e à terceira parte de confiança. A necessidade de anunciar todas as transações publicamente inviabiliza este método, mas a privacidade pode ainda ser mantida quebrando o fluxo de informação em outro ponto: mantendo as chaves públicas anónimas. O público pode ver que alguém está a enviar um montante a outra pessoa, mas sem informação que possa relacionar a transação a alguém. É similar ao nível de informação publicado pela bolsa de valores, onde data e montante dos negócios individuais, a "fita", é tornada pública, mas sem divulgar quais as partes.



Como proteção adicional, um novo par de chaves deverá ser usado para cada transação para evitar que sejam relacionados a um proprietário comum. Algum relacionamento é inevitável com transações de múltipla entrada, que revelam necessariamente que as entradas pertencem ao mesmo proprietário. O risco é que, se o proprietário de uma chave for revelado, o relacionamento pode revelar outras transações pertencentes ao mesmo proprietário.

11. Cálculos

Consideremos o cenário de um atacante tentar gerar uma cadeia alternativa mais rapidamente que a cadeia honesta. Mesmo que o consiga, não torna o sistema aberto a alterações arbitrárias, como

criar valor a partir do nada ou apropriar-se de dinheiro que nunca pertenceu ao atacante. Os nós não iram aceitar uma transação inválida como pagamento, e os nós honestos nunca aceitarão um bloco que a contenha. Um atacante só poderá tentar alterar uma das suas próprias transacções para recuperar dinheiro que tenha gasto recentemente.

A competição entre a cadeia honesta e a cadeia atacante pode ser caracterizada como Passeio Aleatório Binomial. O evento de sucesso será a cadeia honesta ser aumentada de um bloco, aumentando a sua liderança de +1, e o insucesso é a cadeia atacante ser aumentada de um bloco, reduzindo a diferença de -1.

A probabilidade de um atacante recuperar de um determinado deficit é semelhante ao problema da Ruína do Jogador. Imagine-se um jogador com crédito ilimitado iniciando com deficit jogando um número potencialmente infinito de jogadas para tentar atingir o equilíbrio. Podemos calcular a probabilidade de alguma vez atingir o equilíbrio, ou que um atacante alguma vez atingir a cadeia honesta, como se segue [8]:

p = probabilidade de um nó honesto encontrar o próximo bloco
q = probabilidade de um atacante encontrar o próximo bloco
q_z = probabilidade do atacante alguma vez recuperar de z blocos de atraso

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Se assumirmos que p > q, a probabilidade cai exponencialmente com o aumento do número de blocos que o atacante tem que recuperar. Com a probabilidade contra ele, se não fizer um avanço de sorte muito cedo, as probabilidades tornam-se minúsculas enquanto vai ficando para trás.

Consideremos agora quanto tempo o recetor de uma nova transação deverá esperar até ter suficiente certeza que o emissor não pode modificar a transação. Assumimos que o emissor é um atacante que pretende que o recetor acredite momentaneamente que lhe pagou, e após algum tempo reverterá o pagamento para ser reembolsado. O recetor será alertado quando isso acontecer, mas o emissor espera que seja demasiado tarde.

O recetor gera uma novo par de chaves e dá a chave pública ao emissor pouco tempo antes da assinatura. Isto impede o emissor de preparar uma cadeia de blocos antecipadamente, trabalhando nela continuamente até ter a sorte de se distanciar e efetuar a transação nesse momento. Assim que a transação for enviada, o emissor desonesto começará a trabalhar secretamente numa cadeia paralela contendo uma versão diferente desta transação.

O recetor aguarda até que a transação seja adicionada a um bloco e z blocos tenham sido ligados após este. Ele não sabe exatamente o progresso atingido pelo atacante, mas assumindo que o bloco honesto demorou a média esperada para cada bloco, o potencial progresso do atacante será uma distribuição Poisson com o valor esperado:

$$\lambda = z\frac{q}{p}$$

Para obter a probabilidade que o atacante poderá recuperar, multiplicamos a densidade do Poisson por cada progresso que poderíamos efetuar pela probabilidade de alinharmos desde esse ponto:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & if\ k \le z \\ 1 & if\ k > z \end{cases}$$

Reorganizando para evitar a cauda infinita da distribuição...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Convertendo para código C...

```
#include <math.h>
double ProbabilidadeSucessoAtacante(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Obtendo alguns resultados, podemos ver a redução exponencial da probabilidade com z.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Resolvendo para P menor que 0.1%...

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

12. Conclusão

Propusemos um sistema para transações eletrónicas sem depender da confiança. Começamos com a estrutura usual de moedas baseadas em assinaturas digitais, que proporcionam um grande controlo de posse, mas que é incompleta sem um meio de prevenir o gasto duplo. Para resolver este problema, propomos uma rede ponto-a-ponto usando uma prova-de-trabalho para fazer o registo histórico das transações que rapidamente se tornam de mudança impraticável para um atacante se os nós honestos controlarem a maioria da capacidade de processamento. A rede é robusta dada a sua simplicidade desestruturada. Os nós trabalham em simultâneo com pouca coordenação. Eles não necessitam ser identificados, uma vez que as mensagens não são encaminhadas para para uma localização particular e só precisam ser entregues numa base do melhor esforço. Os nós podem abandonar e retornar à rede à vontade, aceitando a cadeia de prova-de-trabalho como prova do que aconteceu enquanto estiveram ausentes. Votam com a sua capacidade de processamento, exprimindo a sua aceitação de blocos válidos trabalhando na sua extensão e rejeitando blocos inválidos rejeitando a sua evolução. Quaisquer regras ou incentivos podem ser obrigados com base neste mecanismo de consenso.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, e J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, Maio 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, num 2, páginas 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," *In Sequences II: Methods in Communication, Security and Computer Science*, páginas 329-334, 1993.

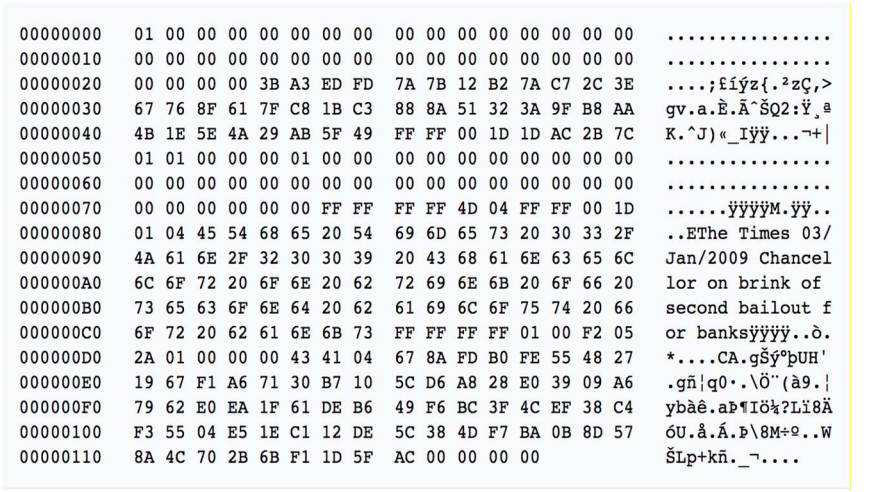
[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, páginas 28-35, Abril 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. *1980 Symposium on Security and Privacy*, IEEE Computer Society, páginas 122-133, Abril 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

Bloco Gênesis do Bitcoin ~ Versão Hexadecimal
03-01-2009



```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ŠLp+kñ._¬....
```

e assim,
uma nova era,
foi desencadeada

Profunda gratidão a Satoshi, aos cypherpunks do passado, presente e futuro, ao vórtice do Twitter do Bitcoin, aos maxis tóxicos, aos maxis não tóxicos, aos senhores e senhoras dos memes, aos crentes, aos cínicos, aos videntes...
e sempre,
minha amada família, amigos,
e Aquele que respira através de todos nós,
por sempre me acompanharem,
mais precioso do que qualquer coisa, até mesmo o bitcoin.

Confira outros assuntos em:
thesimplestbitcoinbook.net (em breve)

Fique à vontade para enviar comentários, perguntas, atualizações, feedback para:
TheSimplestBitcoinBook@protonmail.com

No entanto, não posso prometer que o farei em tempo hábil... talvez esteja descalça em uma montanha em algum lugar

Stack sats
Seja forte
Seja verdadeiro

lá no fim, o Amor

Bloco # 728922

Se você encontrou valor neste livro, considere a possibilidade de enviar uma doação para me apoiar, pois estou trabalhando para criar o próximo livro educacional sobre bitcoin!

Aqui estão alguns links para envio sats via lightning ou bitcoin:
Muito obrigada!