



Bitcoin, Blockchain e o pagamento na era digital

EDSON BRUSQUE E RAFAEL NOGUEROL

Temas

A história do dinheiro

Edson Brusque

Bitcoin e Blockchain

Rafael Noguerol

Quem somos ?

- ▶ Edson Brusque – Graduado em engenharia elétrica pela FURB e mestrando em Digital Currency pela University of Nicosia, fundador da Bruschi Amps e grande entusiasta de economia e moedas digitais, tendo organizado alguns eventos em Blumenau como o Bitcoin Day
- ▶ Rafael Noguerol – Estudante de Engenharia de Controle e Automação na UFSC, entusiasta de Bitcoin e Blockchain desde 2013, atualmente trabalha na mais recente Exchange de Bitcoin do Brasil a Walltime (<https://walltime.info>) de Campinas/SP





APRESENTAÇÃO BRUSQUE

A história do dinheiro

Bitcoin e Blockchain

- ▶ Como funciona o Blockchain ?

"O blockchain fará pelos negócios o que a internet fez pela comunicação" - IBM



Blockchain na mídia



Blockchain e Bitcoin representarão 10 por cento do PIB global até 2027

28 MAR 2017 13h33



Conferência internacional em SP destaca o potencial do Blockchain

iMasters - 23 de mar de 2017

Conferência internacional em SP destaca o potencial do Blockchain ... Links, primeira conferência internacional sobre Blockchain no Brasil.



Tecnologia

Brasil ainda vive o hype do Blockchain

Estamos dois passos atrás os países mais avançados, que já começam a realizar as primeiras provas de conceito da tecnologia para além da área financeira. Mas isso pode ser uma vantagem

FOLHA DE S.PAULO
País pode usar blockchain contra crise de confiança da carne



Ronny Santos/Folhapress

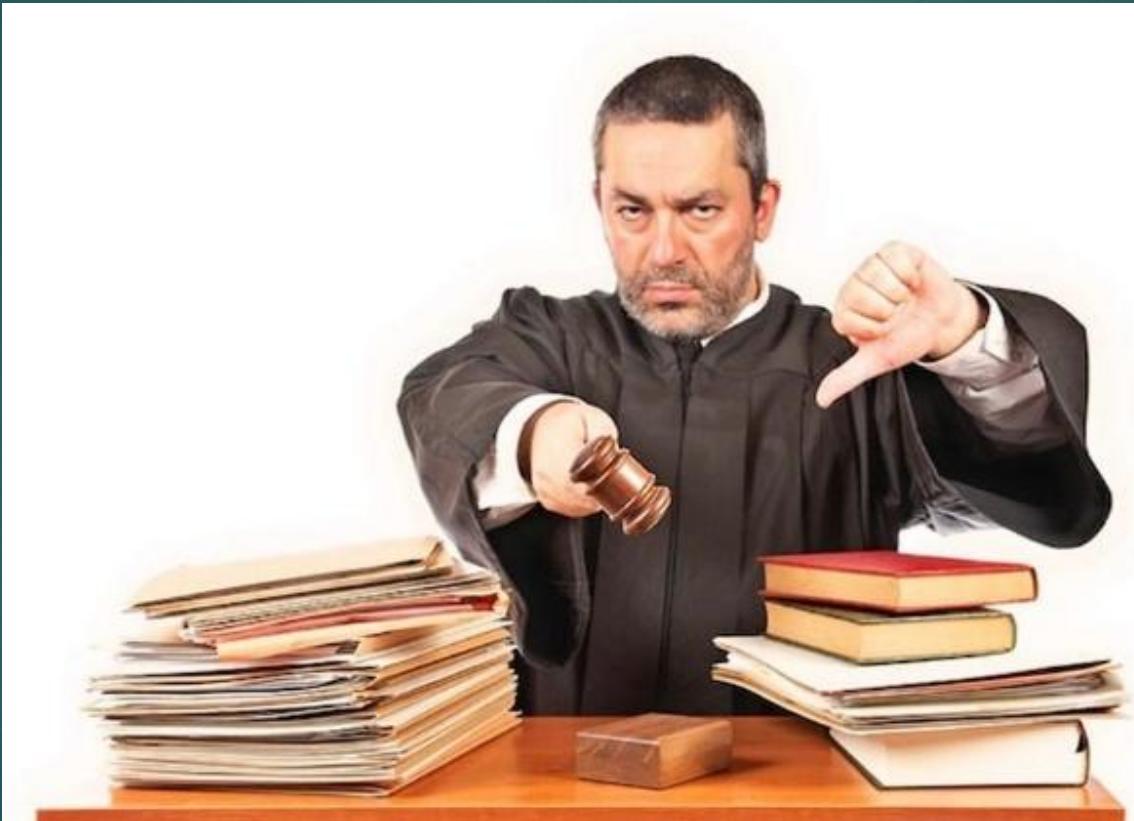
Analogias

- ▶ Blockchain -> Maçã
- ▶ Bitcoin -> Metal precioso

Maçã – Transação P2P



Vamos olhar de perto o que aconteceu



Continuando...



Voltando para as maçãs

De repente eu digo: **tenho uma maçã digital aqui.**

Toma, vou te dar minha **maçã digital** te transferindo
ela por WhatsApp ou por Telegram.

Agora as coisas estão **ficando interessantes...**

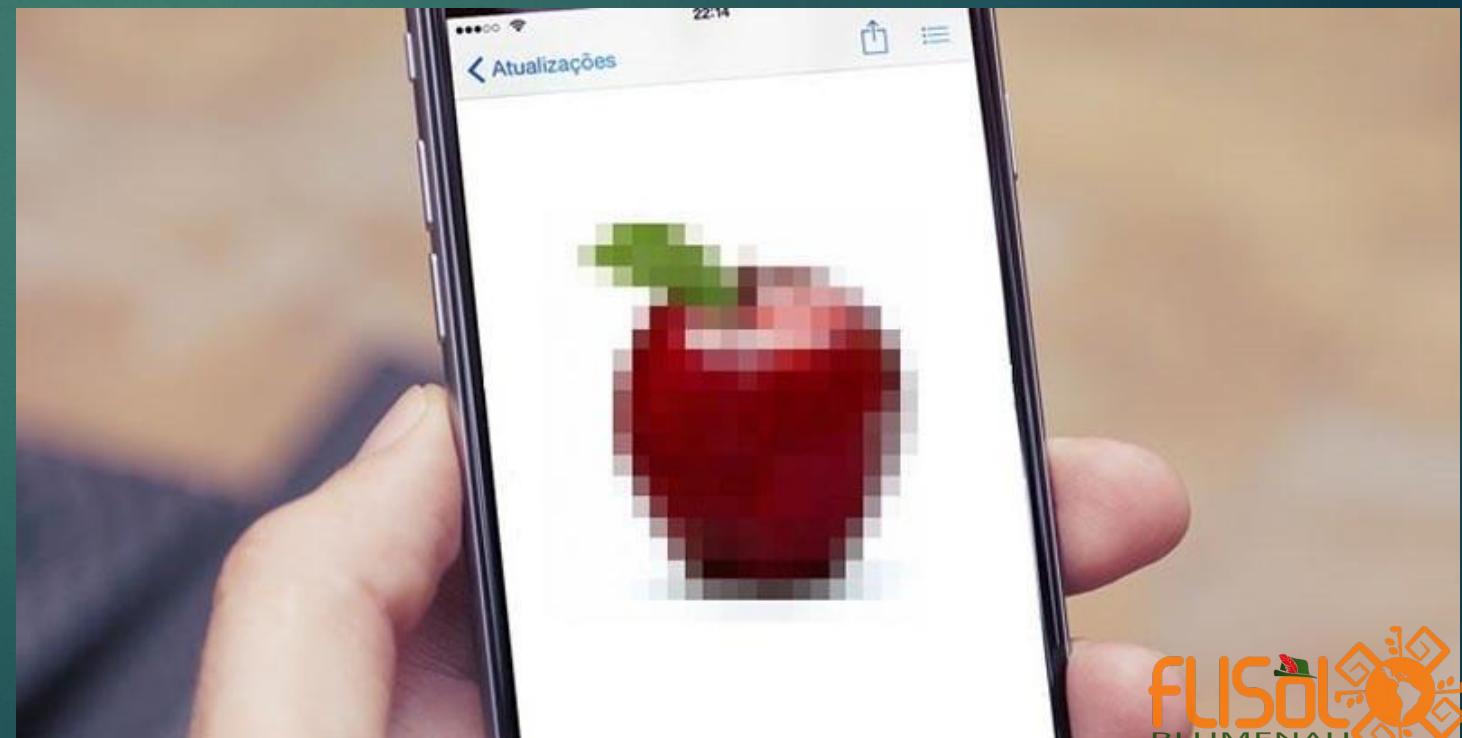
Maçã digital

Como você sabe se aquela maçã *digital* que costumava ser minha, agora é só sua?

Pense nisso por um segundo.

...

É meio complicado, certo?



Maçã digital



- maçã - Copia (2)
- maçã - Copia (3)
- maçã - Copia (4)
- maçã - Copia (5)
- maçã - Copia (6)
- maçã - Copia (7)
- maçã - Copia (8)
- maçã - Copia (9)
- maçã - Copia (10)
- maçã - Copia (11)
- maçã - Copia (12)
- maçã - Copia (13)
- maçã - Copia (14)
- maçã - Copia (15)
- maçã - Copia (16)
- maçã - Copia (17)
- maçã - Copia (18)
- maçã - Copia (19)
- maçã
- maçã

Maçã digital

Transferir maçãs *digitais* não é nada parecido com transferir maçãs *físicas*.

...

Maçãs digitais podem ser copiadas.

Maçã digital

Há um problema com a transferência
de tudo o que é digital.

Mandar algo digital na internet
não é como estarmos sentados
aqui transferindo maçãs físicas.

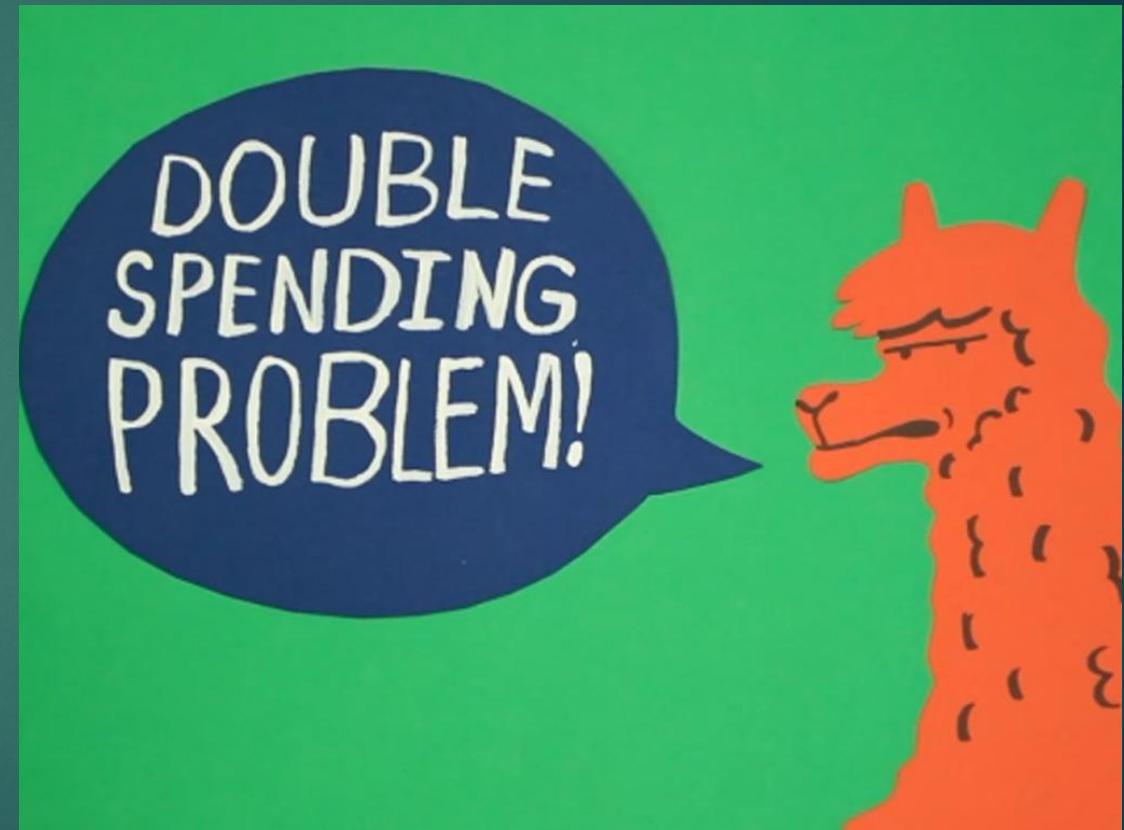
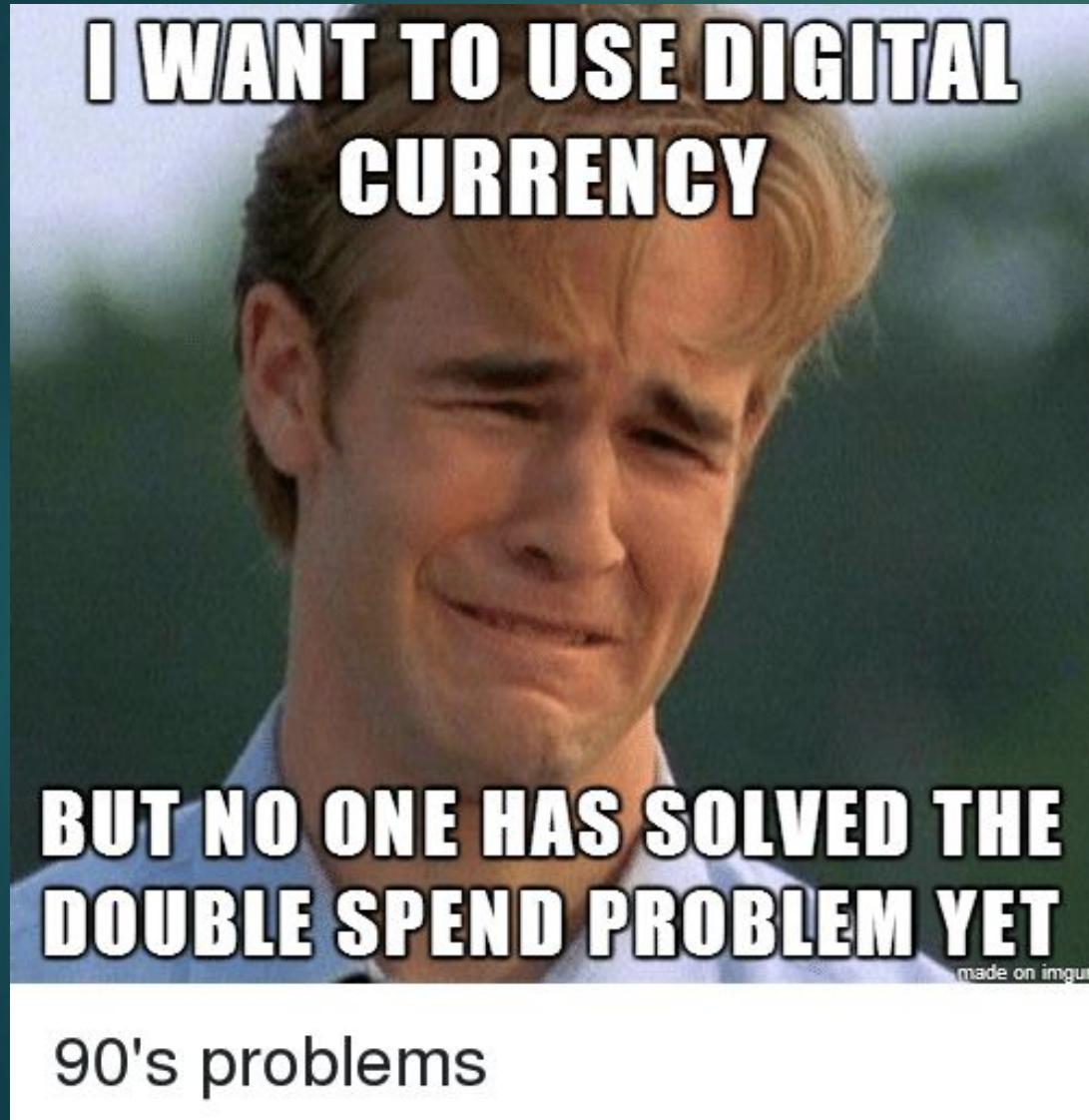
O que acontece se essas pessoas que estão na internet criam várias maçãs digitais e distribuem elas?

Você não vê problema nisso?

Mas e se isso fosse feito com o seu dinheiro?

Afinal, como posso mandar minha
maçã digital para você, e você ter
a certeza de que eu não copiei ela
ou passei para outra pessoa?

Problema do Gasto Duplo



Maçã digital

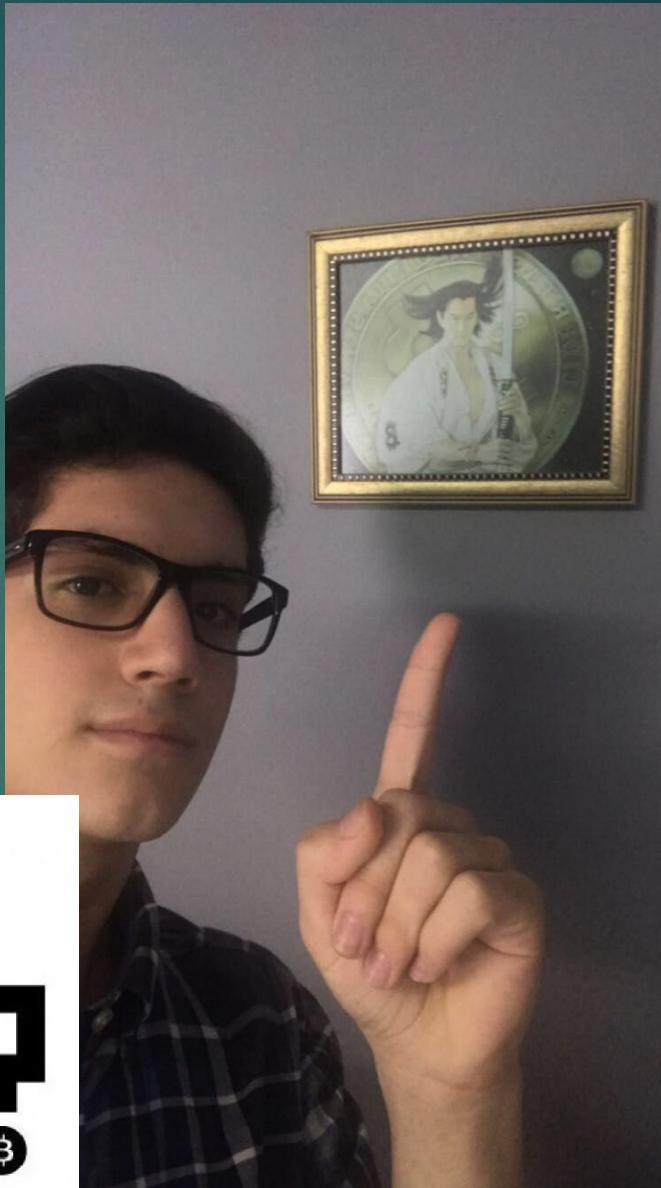
Será que existe alguma maneira de **pararem**
de replicar as nossas maçãs digitais?

Satoshi Nakamoto

Bitcoin: A Peer-to-Peer Electronic Cash System

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

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not co-attacking the network, they'll generate the longest chain and outpace attacks. The network itself requires minimal structure. Messages are broadcast on a peer-to-peer basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.



Livros-razão digitais

A solução genial.

Talvez a **transferência dessas maçãs digitais precisem ser monitoradas** em um grande livro-razão para que ninguém copie e distribua elas.



Livros-razão digitais

Necessitam basicamente de um lugar onde você possa rastrear todas as transações das maçãs de uma pessoas para a outra, como em um livro contábil.

Livros-razão digitais

Esse livro não precisa ter alguém para cuidar dele. Todos
são capazes de cuidar com seus computadores
conectados a internet a qualquer minuto.

...



Explicando como funciona a solução genial

- ▶ O que aconteceria se nós dêssemos esse livro-razão para **todos**?



Explicando como funciona a solução genial

- Você não pode enganá-las.

Explicando como funciona a solução genial

- ▶ Ele não é controlado por uma pessoa
- ▶ As regras do sistema já foram definidas no início.

O sistema que eu expliquei já existe.



BLOCKCHAIN



- ▶ Então, você viu o que aconteceu?
- ▶ O que a contabilidade pública digital permitiu?

É open source (código aberto) lembra?

- O número total de maçãs foi definida na contabilidade pública no início.

Eu sei o **número exato de quantas maçãs que existem dentro desse sistema**, e eu sei que elas são limitados (escassas).

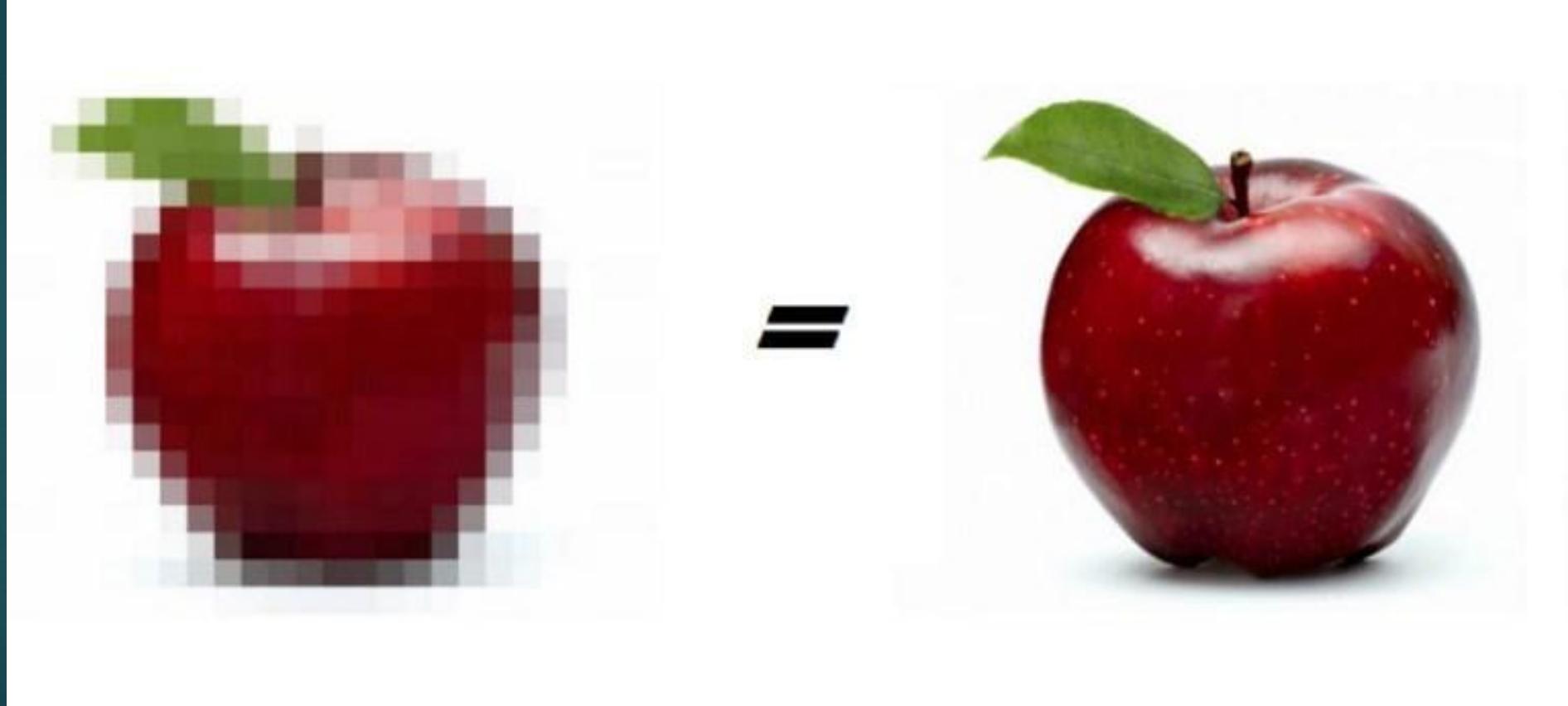
Quando eu fazer uma troca agora
eu sei que a **maçã** deixou de estar
sob minha posse e agora é
totalmente sua.

Porque é um **livro público**, eu não
vou precisar de um juiz para
certificar de que eu não vou
enganar as pessoas, ou fazer
cópias extras de maçãs para mim,
ou enviar maçãs duas vezes, ou três
vezes, etc...

Eu vou simplificar um pouco...

- ▶ A troca de algo digital é agora apenas como a troca de algo físico.
- ▶ Não há possibilidade de fazer cópias ou fraudes.
- ▶ Agora, temos tanta certeza que transferência online é semelhante a certeza de ver um objeto físico deixar de ser meu e passar a ser seu.
- ▶ E, assim como antes, a troca envolveu apenas duas pessoas.

Em outras palavras, agora a
maçã *digital* se comporta como
uma maçã *física*.



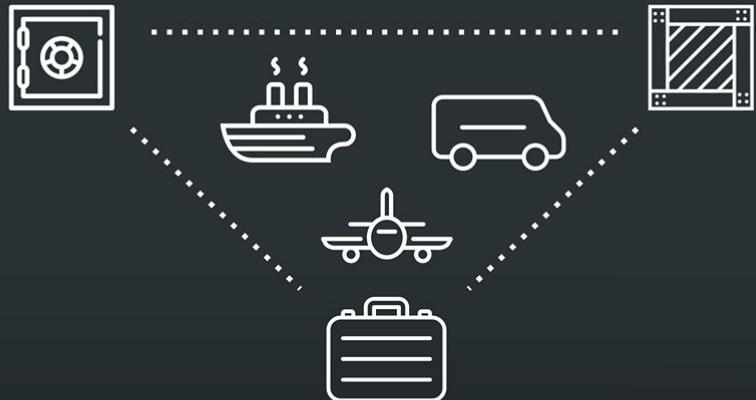
Mas você sabe o que mais é legal? **Essa maçã é digital !**

- ▶ **Agora podemos transferir milhares de maçãs** como: 1.000 maçãs, ou 1 milhão de maçãs, ou até mesmo um valor reduzido, como 0,0000001 maçãs.
- ▶ **Eu posso enviá-las com alguns cliques nos botões digitais do meu Smartphone**, e ainda **posso colocá-las no seu bolso digital...**
- ▶ **Posso até fazer outras coisas digitais** e não chamá-las mais de maçãs digitais! **Oras bolas, é digital.**

Bitcoin como metal precioso



*ouro, prata
e outros metais.*



bitcoin



Bitcoin como um metal.



Walltime
<https://walltime.info>

O que é bitcoin?

- ▶ Uma das analogias mais interessantes sobre o bitcoin é a de que ele é um metal.
- ▶ Um metal que, assim como o ouro e outros metais preciosos, é muito escasso e bastante divisível. Só pode ter 21 milhões de unidades no máximo, sendo que cada unidade pode ser dividida em até 100 milhões de vezes.

O que é bitcoin

- ▶ Diferente do ouro e outros metais, ele é bem feio.
- ▶ Quase **invisível**.
- ▶ Pouco **palpável**.
- ▶ Meio esquisito.
- ▶ Ele é **tele transportável**.
- ▶ Em **qualquer lugar do mundo em que a Internet possa chegar**, o bitcoin poderá chegar.
- ▶ Pode assumir uma forma física.

O que é Bitcoin?

- ▶ Parece coisa de filme, não? Uma mistura de The Matrix e Tron.
- ▶ Pois é, o futuro chegou e o bitcoin está mudando completamente a forma como a riqueza mundial é armazenada e transportada.

Então, isso é ótimo!

Como devemos tratar o valor
dessas “maçãs digitais”(bitcoin)?

Elas são bastante úteis, não são?

Valor

Bem, um monte de pessoas estão
discutindo sobre isso agora...

Previsões para o preço do Bitcoin (em dólar)



Valor

- ▶ É realmente difícil compreender porque algo digital como **1 unidade de bitcoin** vale cerca de **R\$ 34.000,00** no dia de hoje.
- ▶ O Bitcoin supera em grande vantagem o dinheiro estatal

Ouro X Fiat Money X Bitcoin

Traits of Money	Gold	Fiat (US Dollar)	Crypto (Bitcoin)
Fungible (<i>Interchangeable</i>)	High	High	High
Non-Consumable	High	High	High
Portability	Moderate	High	High
Durable	High	Moderate	High
Highly Divisible	Moderate	Moderate	High
Secure (<i>Cannot be counterfeited</i>)	Moderate	Moderate	High
Easily Transactable	Low	High	High
Scarce (<i>Predictable Supply</i>)	Moderate	Low	High
Sovereign (<i>Government Issued</i>)	Low	High	Low
Decentralized	Low	Low	High
Smart (<i>Programmable</i>)	Low	Low	High

Valor

- ▶ **Ouro digital**
- ▶ **Moeda**
- ▶ **Utopia**
- ▶ **Já mudou o mundo**
- ▶ **Moda passageira**

- ▶ O fato é que ela existe e tenho minha própria opinião sobre. Mas essa é uma história para outro dia.

- ▶ **Pronto**, agora você já sabe mais sobre **Bitcoin** do que a maioria.



Joseph Young
@iamjosephyoung

Follow

Deutsche Bank recorded a profit of \$146 million in 2018 Q1, according to CNBC and Reuters. First shared by
@alistairmilne

Binance recorded a profit of \$200 million in 2018 Q1.

Cryptocurrency exchanges are beating the world's biggest banks in profitability. Insane.

3:34 AM - 26 Apr 2018

1,408 Retweets 3,007 Likes



94 1.4K 3.0K



Armin van Bitcoin ⚡
@ArminVanBitcoin

Banks will disappear.
Governments will fall.
Corruption will vanish.
Crime will drop.
Wars will end.

...

#Bitcoin will remain.

5:12 AM - 24 Apr 2018

223 Retweets 1,074 Likes



94 223 1.1K

AGE 25-34

39% of users are young adults

MALE

Over 90% identify as Male

NON-RELIGIOUS

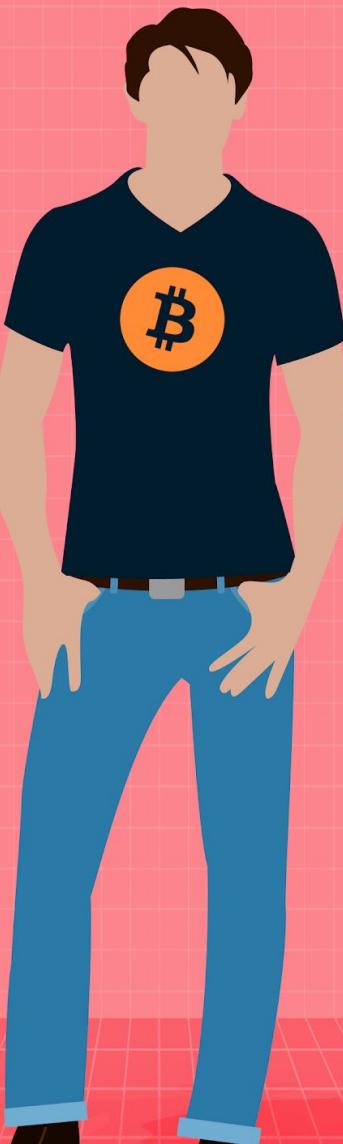
61% of Bitcoin users do not consider themselves to be actively religious

MARRIED

56% of users are either married or in a relationship

LIBERTARIAN

37% consider themselves Libertarian, or anarcho-capitalist



AMERICAN

53% are from either North or South America

\$50-100k

23.9% have a yearly household income of \$50 - 100k per year

EMPLOYED

Over 43% have full-time employment

GENEROUS

77% spend coins as gifts, donations, and for purchasing legal goods

Cost of a 51% attack

\$4,835,548,302

Hardware cost only, at cheapest rate

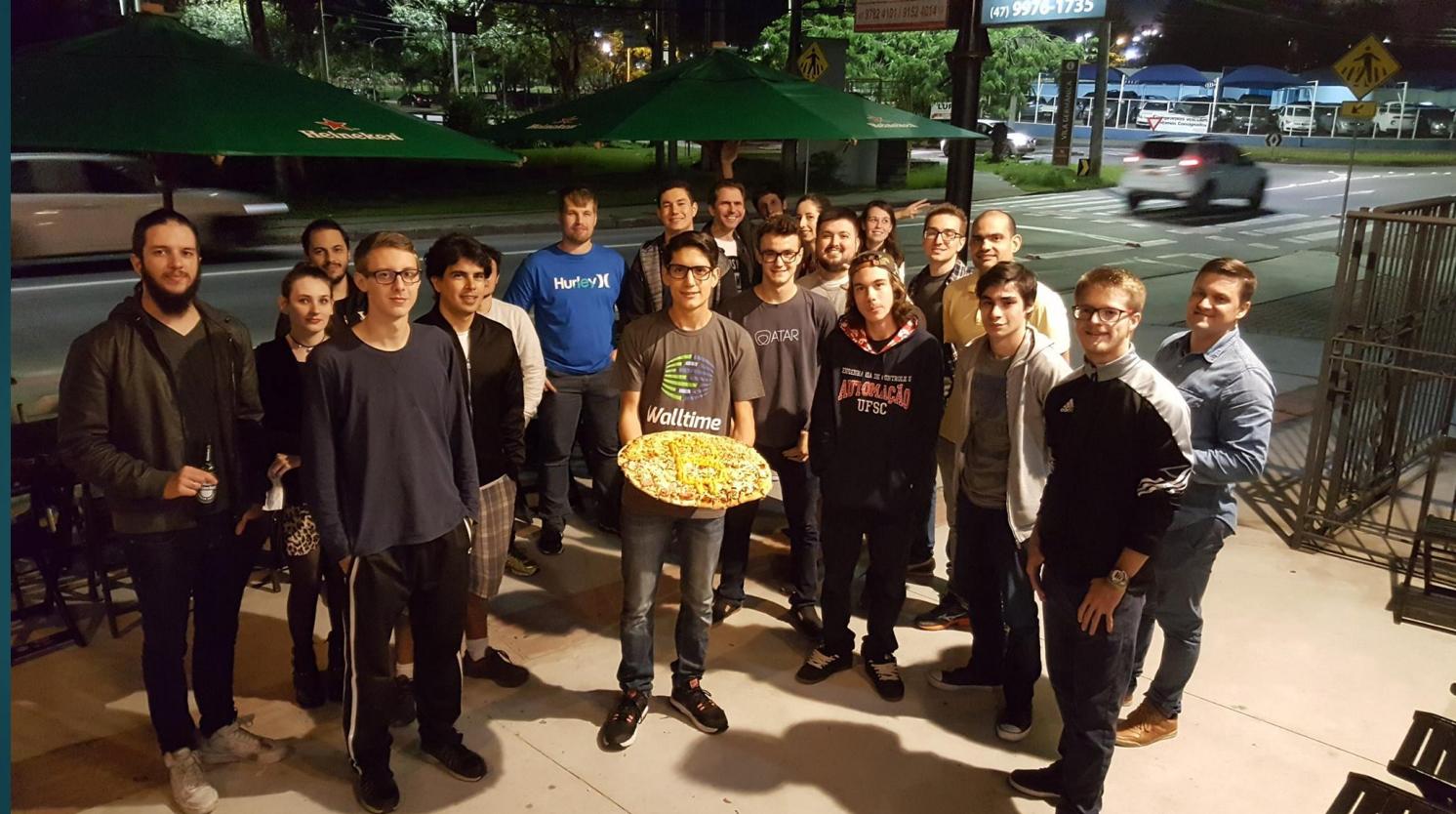
The attack would consume 66,488,789 kWh per day (3,324,439\$ per day)



Happy Bitcoin Pizza Day!

MAY 22

Bitcoin Pizza Day Blumenau



No dia 21 de Maio de 2010, Laszlo Hanyecz postou no Fórum BitcoinTalk que gostaria de comprar pizzas e pagar em bitcoin...



Essa transação ficou marcada na história do bitcoin como a primeira compra de produto físico utilizando a criptomoeda.

Naquela época, 10000 bitcoins valiam cerca de **41 dólares**, hoje, 05 de junho de 2017, esse valor chega a mais de **25 milhões de dólares**.

Opendime



Paper Wallet



Walltime

+

Software Livre

Bitcoin Paranoid

Walltime Finanças

★★★★★ 3.400



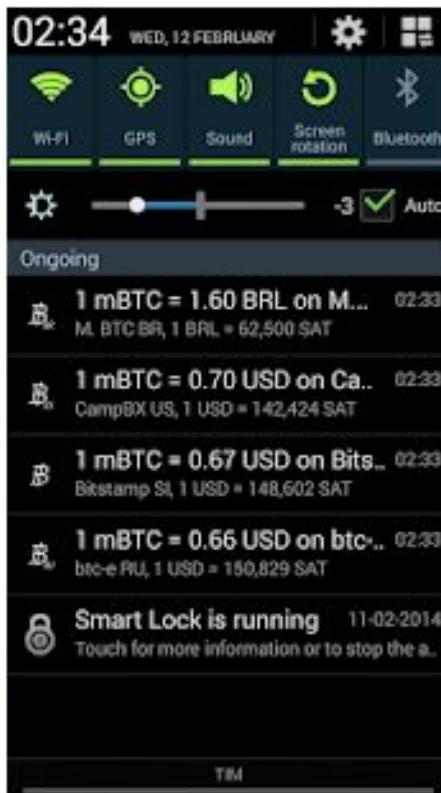
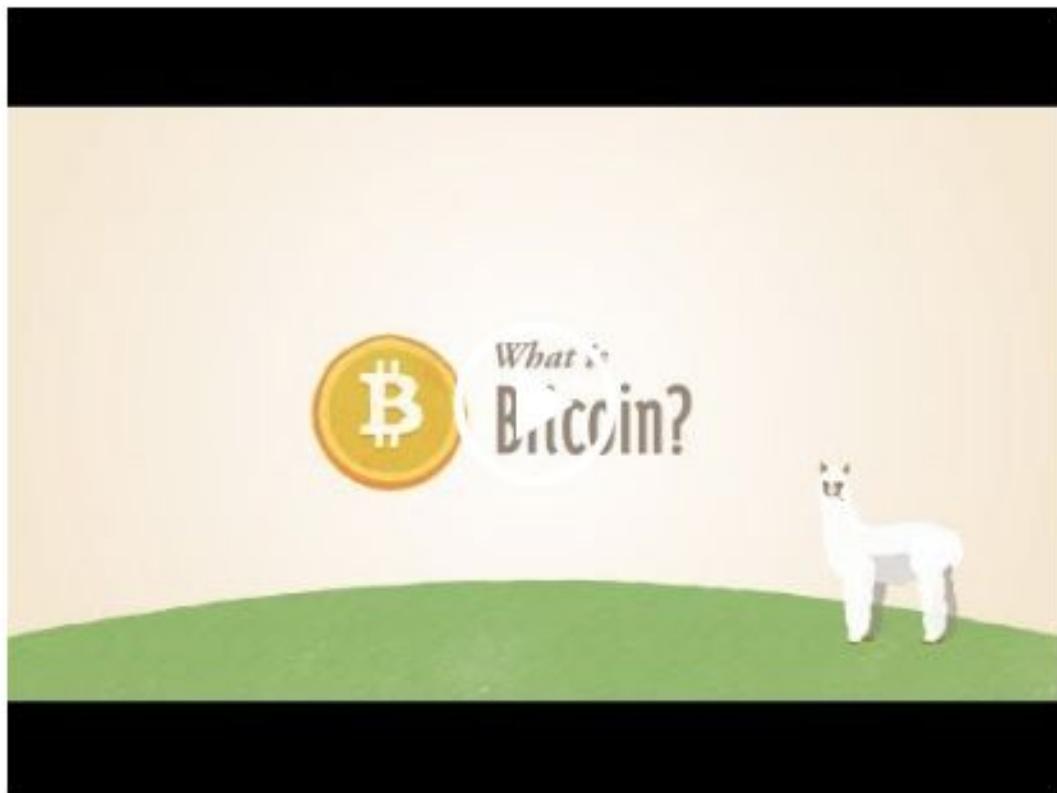
L

⚠ Você não possui dispositivos.



Adicionar à lista de desejos

Instalar





Thunderbird®



Cachet



Walltime

Joined Jul 2017

ABOUT WALLTIME

<https://walltime.info> is a a brazilian
digital assets exchange and other

Creators 1

PATRON OF



Matrix.org

is creating the future of open...

404 patrons \$4,057 per month

We are hiring!

<https://walltime.info/jobs.html>



Walltime

Sorteio da Cold Wallet Walltime



Carteira offline de acrílico BIP-38

