

AFINAL,  
BITCOIN  
É UMA MOEDA OU UM ATIVO?

Evandro Pires da Silva

<evandro@evandropires.com.br>

<https://www.linkedin.com/in/epiresdasilva/>

# SOBRE ESSA APRESENTAÇÃO

How to navigate:

- space bar: next slide
- n: next, p: previous
- f: full screen
- esc: overview
- arrow keys: directional moves
- s: speaker's view with notes

Open source: [fork me on github!](#)

# SOBRE O AUTOR

- Programador desde os 12 anos ( aprendi com Clipper :D ).
- Trabalho com Java desde 2005.
- Arquiteto de Sistemas e Empreendedor/Intraempreendedor.
- Amo trabalhar com TI, é exatamente o que gosto de fazer.
- Estudando blockchain e cripto moedas desde 2018.

# AGENDA

- O que é dinheiro/moeda.
- O que são bitcoins e o que é blockchain.
- Como criptografia e rede distribuída são utilizadas no bitcoin.
- Bitcoin pelo mundo
- Momento de Reflexão!

# DINHEIRO / MOEDA



# RESUMO DA HISTÓRIA DAS MOEDAS

- Troca/Escambo
- Metais raros, minerais.
- Moedas de Ouro/Prata/Bronze.
- Adoção do Gold Standard (1821-1900).
- Nota de banco (passível de conversão em ouro).
- Reserva fracionária.
- "Fiat Money" (fim do Gold Standard, Richard Nixon em 1971).

# FUNÇÕES DO DINHEIRO

*"As principais funções do dinheiro são descritas como:*

- *um meio de troca;*
- *uma unidade de conta;*
- *uma reserva de valor; Qualquer item ou registro verificável que atenda a essas funções pode ser considerado como dinheiro."*

*(Wikipedia)*

# PROPRIEDADES DO DINHEIRO

- Fungibilidade: suas unidades individuais devem ser capazes de substituição mútua.
- Durabilidade: capaz de suportar o uso repetido.
- Portabilidade: facilmente carregado e transportada.
- Divisibilidade: pode ser dividido em pequenos incrementos que podem ser trocados por bens de valores variados.
- Conhecibilidade: seu valor deve ser facilmente identificado.
- Estabilidade de valor: seu valor não deve flutuar.

# BITCOIN

- Criptografia.
- Rede distribuída.
- Teoria de jogos.
- Teoria econômica.

# O QUE É BITCOIN?

*"First decentralized digital currency."*

*(bitcoin.org)*

*"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."*

*(Satoshi Nakamoto - the bitcoin whitepaper)*

# RESUMO DA HISTÓRIA DO BITCOIN



# O QUE HÁ DE NOVO?

- Resolve o problema de "gastos duplos".
- Descentralizado.
- Confiável: sem instituições financeiras, governos ...
- Resistente à censura.

# O QUE HÁ DE NOVO?

- Resiliente e seguro.
- Sem permissão
  - Instantâneo
  - Banco de baixo custo para todos
  - 24/7, 365 dias/ano.
- Globalizado, sem fronteiras.

# O QUE HÁ DE NOVO?

Bitcoin é

- Ativo.
- Escasso.
  - Emissão imita a extração de ouro.
- Divisível.
- Durável.

# O QUE HÁ DE NOVO?

A primeira vez na história, temos um ativo digital que pode ser transferido, mas não pode ser duplicado.

Ouro 2.0?

# BITCOIN VS FIAT MONEY VS OURO

Funções	Ouro	FIAT Money	Bitcoin
Meio de troca	OK	OK	OK
Unidade de conta	OK	OK	OK
Reserva de valor	OK	OK	OK

# BITCOIN VS FIAT MONEY VS OURO #2

Propriedades	Ouro	FIAT Money	Bitcoin
Fungibilidade	+	++	+++
Durabilidade	++	+	++
Portabilidade	-	+	++
Divisibilidade	+	++	+++
Conhecibilidade	-	+	++
Estabilidade	++	+	-

# BITCOIN VS FIAT MONEY VS OURO #3

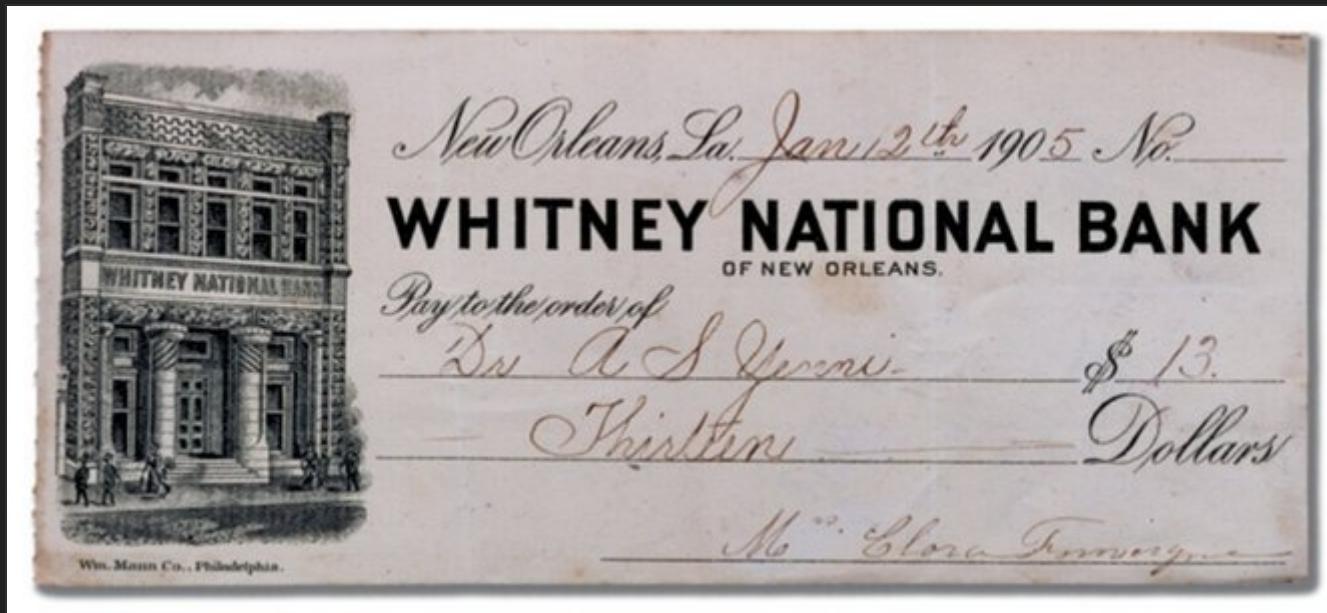
Características	Ouro	FIAT Money	Bitcoin
Valor intrínseco	None	None	None
Segurança	Química	Papel e tinta	Criptografia
Emissão	Disponibilidade	Discricionário	Algorítmico
Adoção	Voluntário	Legal	Voluntário



# O PROTOCOLO BITCOIN

# TRANSAÇÃO

A transação contém basicamente a mesma informação que um cheque.



A assinatura digital permite que qualquer um verifique a transação imediatamente e com segurança.

# TRANSAÇÃO

Alice envia \$2 para Bob e assina a transação:

De	Para	Valor	Assinatura
Alice	Bob	\$2	101110111

A transação é transmitida para todos os nós da rede do bitcoin e depois de alguns segundos todos os nós tem uma cópia dele na mempool.

# TRANSAÇÃO BITCOIN

Aqui é como uma transação real se parece no [blockchain.info](#) website.

26668946106e70a56e60077f59c70693d6e978eb5b95b6b85b95f0de01861de1	(Fee: 0.00224774 BTC - 151.06 sat/WU - 604.23 sat/B - Size: 372 bytes) 2018-04-03 15:46:50	
12XF17pwVT3KrNs2Dkz5yUBN7orv6urFhv (0.08410364 BTC - <a href="#">Output</a> ) 12TtJCm9B4evWebcqTPSSgqk4R1sLm7S2V (0.00150014 BTC - <a href="#">Output</a> )	→ 19gWsg7VHfRKW9bvwbpk7c9dFsMdm5g5WG - (Unspent) 18R6pdwgCWiFkTm5dRSJJ921BTLVkfDGsQ - (Unspent)	0.07356038 BTC 0.00979566 BTC
		0.08335604 BTC
3634e4f652dbc431230dc15e99c6ece7bb109a428ea72106eda2af91a1ec9b76	(Fee: 0.00203138 BTC - 150.7 sat/WU - 602.78 sat/B - Size: 337 bytes) 2018-04-03 15:46:13	
14bzxjpVfcgyzXRLbZentmbNn3G6tH39A (0.221 BTC - <a href="#">Output</a> ) 184FAc551vjZNzMES636kCPVdUdo1LPEQt (0.00211314 BTC - <a href="#">Output</a> )	→ 3Bny46amjyDcdTA3WQi2Kw6n2KGJwg55fY - (Unspent)	0.22108176 BTC
		0.22108176 BTC
fe64239cc6882d7e56e8ca3efa631db778b82a98ec21f9d56f4a9d37407159e5	(Fee: 0.001187 BTC - 131.89 sat/WU - 527.56 sat/B - Size: 225 bytes) 2018-04-03 15:47:13	
1F47A9BMP8c6ESwQjGoGzPsgf3efraoseU (0.10528809 BTC - <a href="#">Output</a> )	→ 1AirRFzz8FdDVuZt37hb5VZeJ8jQsyhGLS - (Unspent) 1FF4eYEXShkaQHda9BocH4DzCZPgE5WXUN - (Unspent)	0.00249976 BTC 0.10160133 BTC
		0.10410109 BTC

# O LIVRO

O Livro contém todas as transações desde o início.

De	Para	Valor	Assinatura
-	Alice	\$10	010101110
-	Bob	\$5	101110110
-	Charlie	\$3	111010110
Alice	Bob	\$2	101110111
Bob	Charlie	\$1	010001001

# LIVRO DESCENTRALIZADO

Todo nó tem uma cópia total da blockchain, tornando um livro descentralizado.



# ENDEREÇO BITCOIN

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



Load & Verify

**Bitcoin Address**  
1BapCVnUC7oWAiv1sadWaweoRpRVhqqPOR  
*bitcoin bitcoin bitcoin bitcoin bitcoin bitcoin bit*



**Private Key**  
L4ndrPHgbPzQ3cLF8ZZc192NNnptysXPAj2ddkxJtDykgMiECWQ



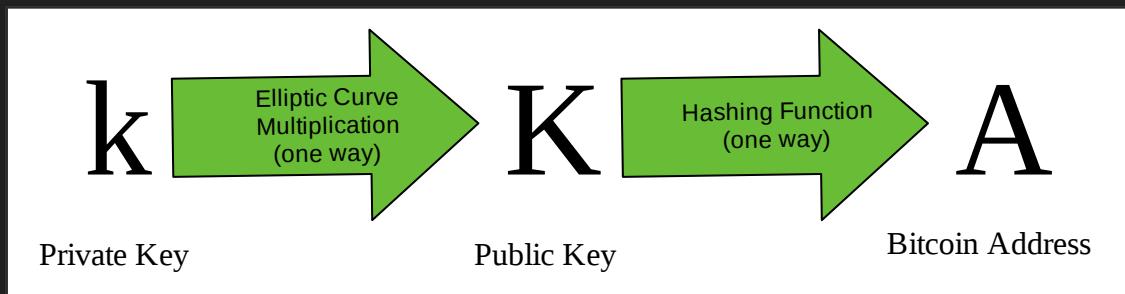
Spend



Gerado por [bitaddress.org](https://bitaddress.org).

# ENDEREÇO BITCOIN

- A chave privada é (um número randômico  $<2^{256}$ ) usado para assinar transações de gastos.
- O endereço bitcoin representa os beneficiários; ele é obtido por um algoritmo de hash e é representado na Base 58, contém um dígito de versão e uma soma de verificação.



# BLOCO

O Bloco contém transações e um cabeçalho de informação.

Quando o hash apropriado é calculado, o bloco pode ser anexado ao blockchain.

A photograph of a woman with long dark hair standing in the doorway of a luxury handbag store. She is wearing a light-colored coat over a dark top. The store's interior is visible through the glass doors, showing shelves filled with various colored handbags (red, orange, yellow, green, blue) and a wooden floor. The lighting is warm and focused on the products.

UTILIZANDO O  
BITCOIN

# CASOS DE USO

- Remessa internacional.
- Reserva de valor.
- Pagamentos online.
- Caridade/Doação.
- Mineração.

# WALLETS

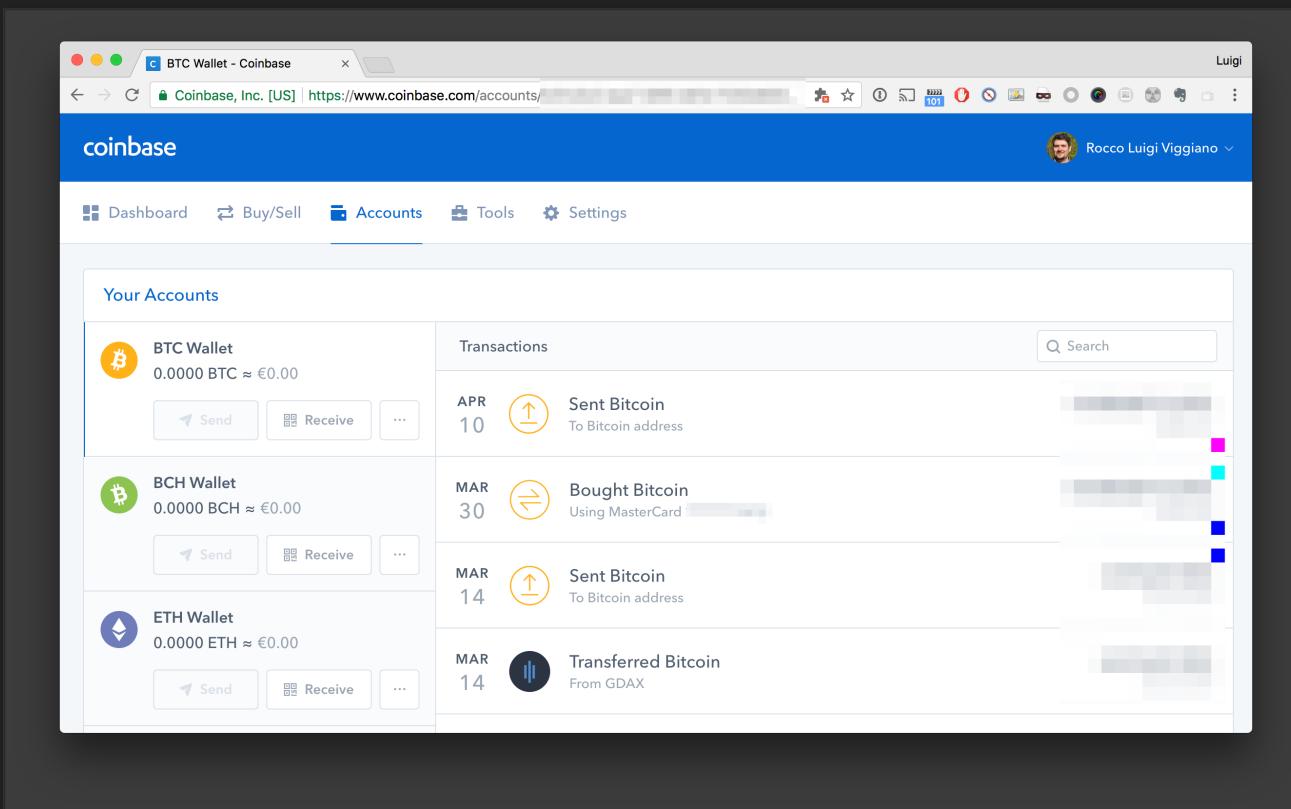
## HOT STORAGE

- Web Wallets.
- Software Wallets:
  - Mobile Wallets.
  - Desktop Wallets.

## COLD STORAGE

- Paper Wallets.
- Hardware Wallets.

# WEB WALLETS



# WEB WALLETS

## PROS

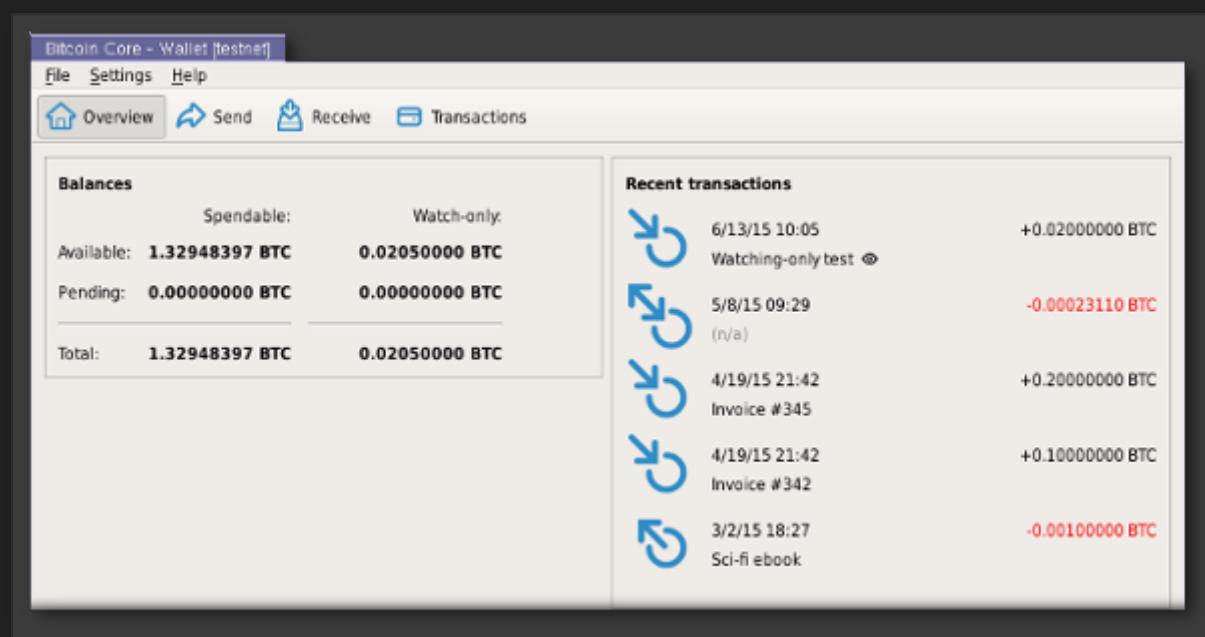
- Fácil de usar.
- Acessível de qualquer dispositivo.
- Geralmente vinculado a serviços de troca.

## CONS

- Chaves privadas estão no servidor de outra pessoa.
- Propenso a hackers.
- O gerenciamento de websites pode suspender e controlar sua conta.
- Você confia na segurança de outra pessoa.

TIP: Sempre use 2FA.

# SOFTWARE WALLETS



# SOFTWARE WALLETS

## PROS

- Mais seguro do que os web wallets.
- Você tem o controle sobre seu dinheiro.
- Fácil para o uso diário e prático de transportar.
- Você pode fazer backup sozinho.

## CONS

- Vulnerável a malwares, vírus e hackers.
- O dispositivo pode ser perdido ou roubado ou incorrer em uma falha de hardware.

# PAPER WALLETS



# PAPER WALLETS

## PROS

- Mais seguro que software wallets e web wallets.
- Sempre off-line (quando corretamente manipulado) não pode ser hackeado.
- Fácil backup.

## CONS

- Eles podem ficar danificados com o tempo, a água, o fogo...
- Eles podem ser roubados.
- Eles precisam ser gerados offline; algum conhecimento técnico é necessário.

# HARDWARE WALLETS



# HARDWARE WALLETS

## PROS

- Mais seguro.
- Pode ser feito backup.
- Protegido por senha.
- Risco mínimo para hacking.

## CONS

- Custo.
- Não é muito fácil para o uso diário.

# TERMOS COMUNS

# BITCOIN NO MUNDO

# BANCO CENTRAL DO BRASIL

"estas (moedas virtuais) não são emitidas nem garantidas por qualquer autoridade monetária, por isso não têm garantia de conversão para moedas soberanas, e tampouco são lastreadas em ativo real de qualquer espécie, ficando todo o risco com os detentores. Seu valor decorre exclusivamente da confiança conferida pelos indivíduos ao seu emissor"

Veja: [Comunicado nº 31.379, de 16/11/2017.](#)

# BANCO CENTRAL PORTUGUÊS

*"(...) as moedas virtuais não são seguras. As entidades que emitem e comercializam moedas virtuais não são reguladas nem supervisionadas por qualquer autoridade do sistema financeiro, nacional ou europeia" Comunicado do Banco de Portugal*

Veja: Bitcoin: a moeda digital que está a desafiar o dinheiro tradicional.

# ESTCOIN: CRIPTOMOEDA DA ESTÔNIA

*"An ICO within the e-Residency ecosystem would create a strong incentive alignment between e-residents and this fund, and beyond the economic aspect makes the e-residents feel like more of a community since there are more things they can do together." Vitalik Buterin, Ethereum founder and a supporter of the Estcoin Project*

Veja: Estonia Considers Issuing ‘Estcoin’ in First Ever Government-Backed ICO e e-Residency

# MOMENTO DE REFLEXÃO

# PONTO DE VISTA DO G20

"We acknowledge that technological innovation, including that underlying crypto-assets, has the potential to improve the efficiency and inclusiveness of the financial system and the economy more broadly. Cryptoassets do, however, raise issues with respect to consumer and investor protection, market integrity, tax evasion, money laundering and terrorist financing (...)"

Veja: Communiqué 19-20 March 2018, Buenos Aires, Argentina.

# CUSTO PARA MINERAÇÃO

# FINANCIAMENTO DE TERRORISMO

"AS the Bitcoin price soars, grotesque terror network ISIS has been using the cryptocurrency to fund its reign of terror."

Veja: Bitcoin WARNING: ISIS using cryptocurrency to fund reign of terror as Bitcoin price soars.

# REFERENCES

- Demo:
  - Anders Brownworth: Blockchain demo.
- Books:
  - Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System.
  - A. M. Antonopoulos: Mastering Bitcoin.
  - Gianmaria Allisiardi: Bitcoin Per Tutti.

# REFERENCES

- Online courses:
  - **Bitcoin and Cryptocurrency Technologies.**
- Movies:
  - Christopher Cannucciari: Banking on Bitcoin.
  - Nicholas Mross: The Rise and Rise of Bitcoin.
  - Bitcoin: The End of Money as We Know It.
- Youtube:
  - Andreas M. Antonopoulos.
  - Marco Ducci.
  - Ferdinando M. Ametrano.

**FIM**

**OBRIGADO PELA ATENÇÃO!**

**DÚVIDAS?**