Bitcoin

Onde saber mais

- Mastering Bitcoin, Andreas M. Antonopoulos, ebook na Amazon (9,00), eventualmente na internet: tradução em português.
- Bitcoin para programadores, Marco Agner, na internet
- Bitcoin: um sistema de dinheiro eletrônico P2P, Satoshi Nakamoto, na internet

As grandes idéias:

- Computação abundante: o limite é o custo do Kwh. Mas já há alternativas
  - Ethereum: O participante adquire moeda e a põe num fundo. Troca prova de trabalho por prova de participação.
  - Peercoin: procedimento similar. Mote: moeda sustentável.
- Abaixo a entidade central: surge o blockchain
- Norton: não importa... não é o bastante
- Criptografia assimétrica é a espinha dorsal
- Solução brilhante para o Problema dos Generais Bizantinos
- Matemática, matemática e ... matemática

O que é o Bitcoin?

- conjunto de conceitos
- conjunto de tecnologias
- ecossistema de dinheiro digital
- software de código aberto
- transações transferem bitcoin de A para B
- a posse se dá pelo conhecimento da senha privada
- roda na arquitetura P2P: não há autoridade central
- bitcoins criados por "mineração"
- Limite de 21.000.000 de bitcoins em 2.140
- 1 satoshi $= \frac{1}{100.000.000}$ de bitcoin

Mineração

- É um bom nome ? – não
- qualquer um pode minerar
- Prova de processamento: disputa computacional
- A solução é facilmente atribuível e remunerada por 50 bitcoins
- A plataforma se ajusta para 1 bloco minerado a cada 10 minutos
- A prova fica mais ou menos difícil em função do poder computacional alocado à mineração
- A cada 4 anos: taxa de mineração cai à metade
- Quem vence a disputa da mineração também pode ser remunerado pelas transações

Moedas digitais

- O dinheiro é bom (não é falsificado ?)
- Ninguém vai reclamar de que o dinheiro é teu e não meu ? (duplo gasto)
- no modelo convencional: segurança do papel moeda, e quem tem o papel tem a propriedade.
- TE resolve-se pela compensação de todas as transações
- antes do Bitcoin, as moedas digitais sofriam na mão do BC (e temiam os hackers)

Bitcoin

- Rede P2P descentralizada rodando protocolo Bitcoin
- Registro público de transações (a blockchain)
- Emissão de moeda de maneira matemática, descentralizada e determinística
- Verificação descentralizada de transações

A história

- gestado na primeira década do século XXI
- 2008: Bitcoin: a P2P Electronic Cash System (S. Nakamoto)
- a rede surge em 2009
- abril 2011: Satoshi Nakamoto se afasta
- em 2014: valor da rede 10.000.000.000 US$
- Hoje: há problemas – 1 bloco de 1MB a cada 10 minutos é pouco. Surge a starvation

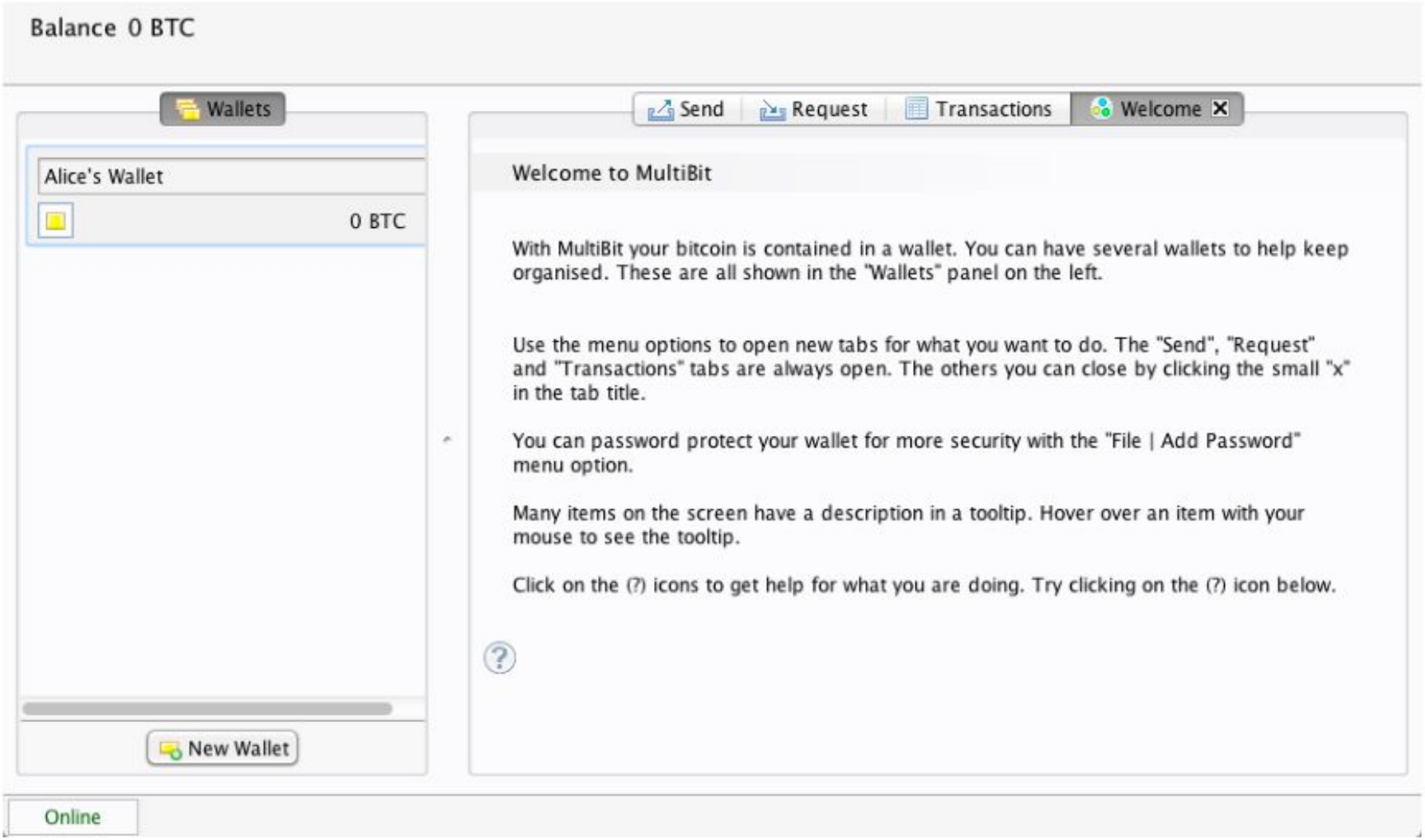
O que se pode fazer

- Varejo de baixo valor: moeda convencional
- Varejo de alto valor
- Contratos internacionais
- Redes amplas de Doações
- Mau uso: drogas, contrabando, armas, etc etc
- Mau uso bem comum: investimento de risco (pirâmides, fraude...)

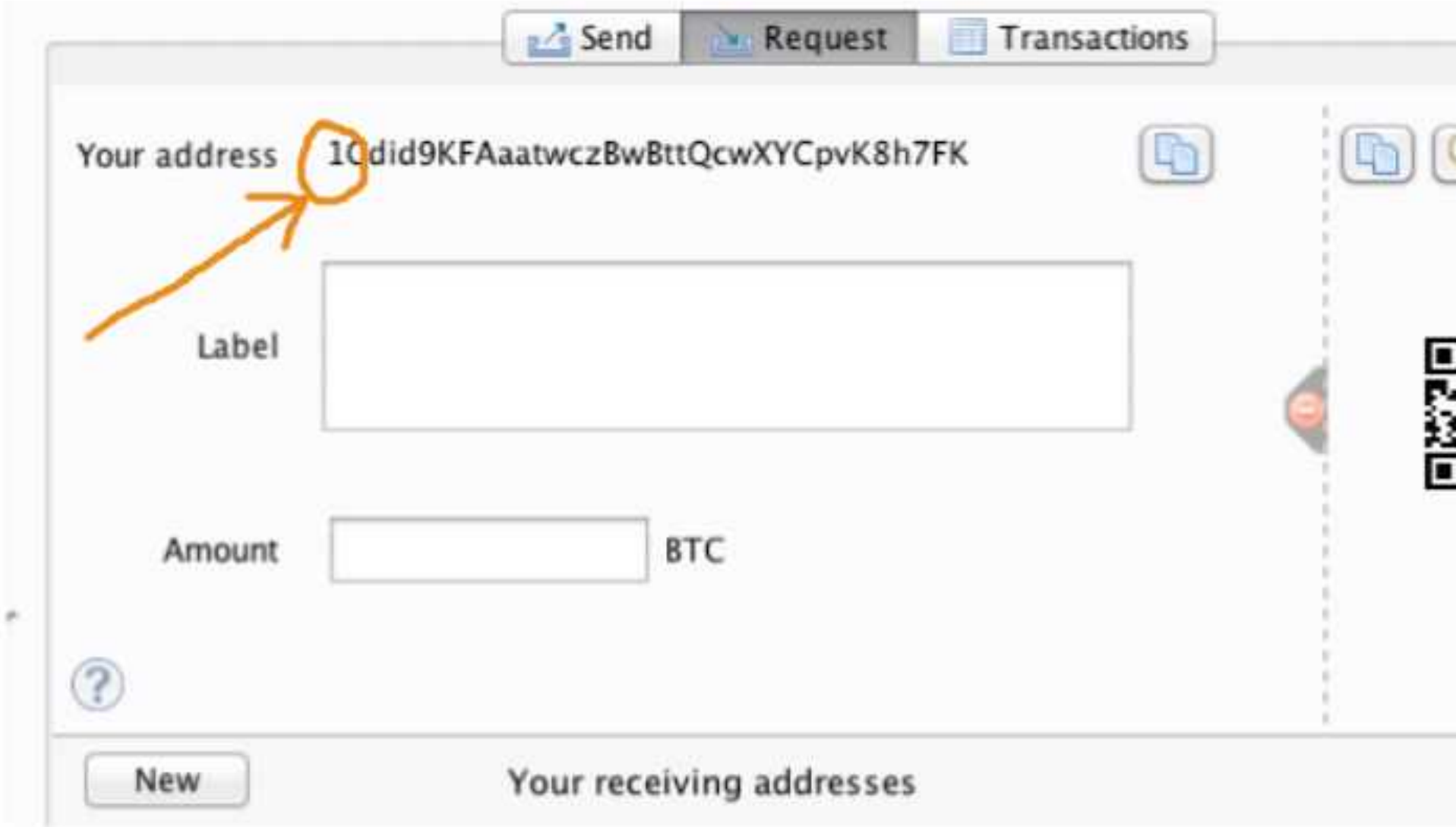
Como começar

- Ache um micro com acesso à Internet e:
  - cliente completo: armazena o histórico de todas as transações da rede desde 2009, gerencia carteiras de usuários e pode lançar transações (win, Mac e Linux)
  - cliente compacto: armazena a carteira do usuário mas depende de terceiros para acessar as transações e a rede Bitcoin
  - cliente web: armazena a carteira em um servidor de terceiros
- Para começar:
  - Gere uma senha privada e calcule a pública
  - compre alguns bitcoins (ou satoshis) que serão transferidos para o teu endereço público
  - Quando quiser gastar, deve provar a posse da moeda (pela apresentação da senha privada)
- A transação existe quando entra no blockchain: com 6 blocos adiante há um consenso de que a transação é irreversível
- Riscos: alguém roubar tua senha privada. Você perder a senha privada.

O cliente Multibit



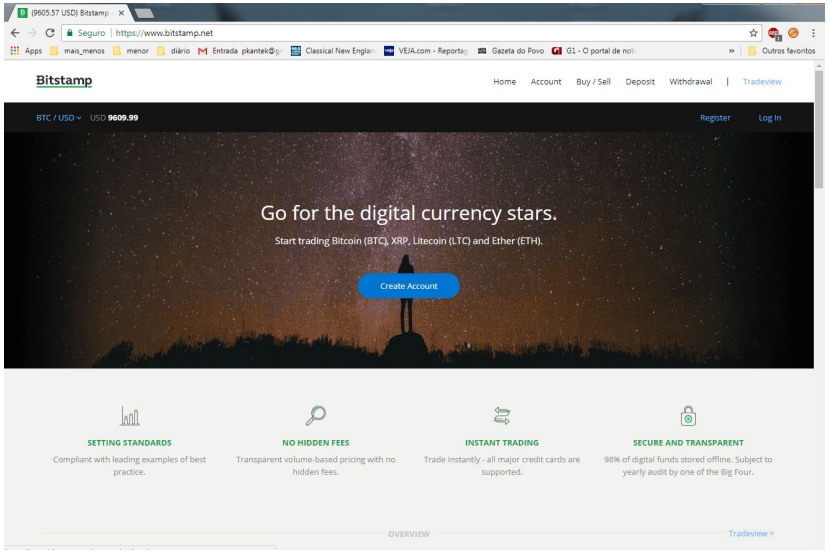
Endereço para receber

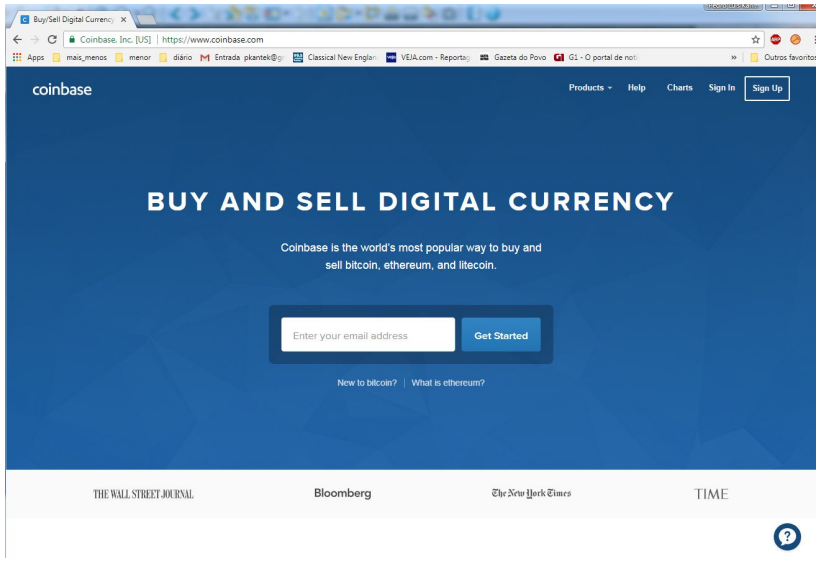


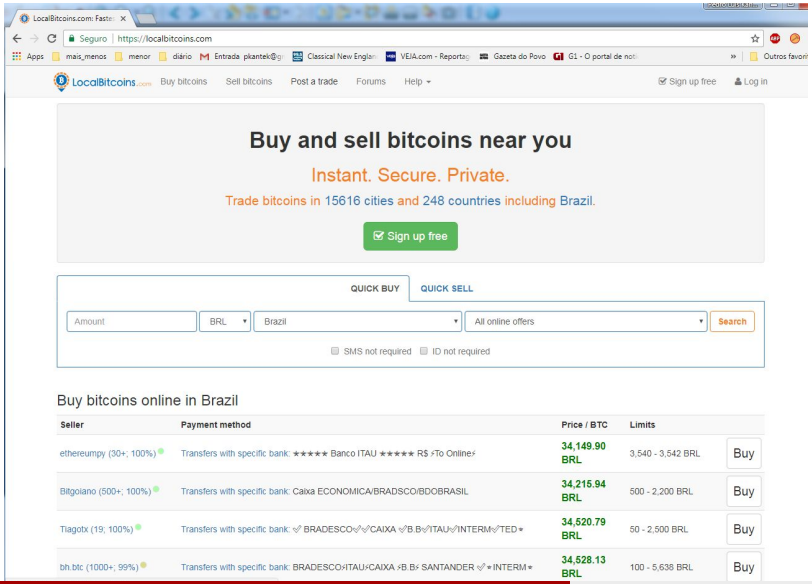
Onde ?

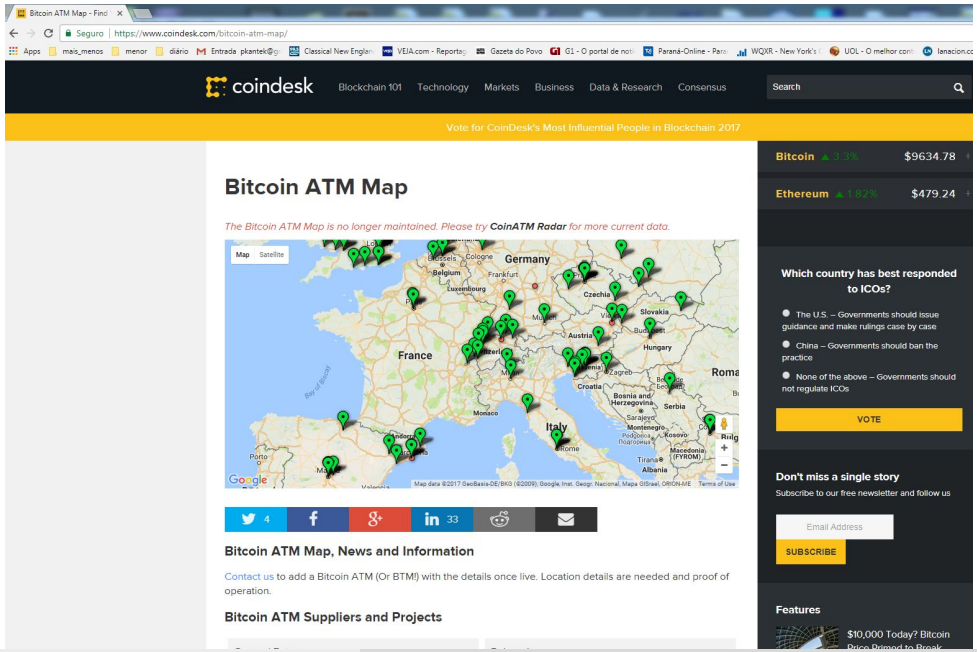
- bitstamp (https://www.bitstamp.net/)
- coinbase (https://www.coinbase.com/)
- mercado livre (https://www.mercadolivre.com.br/) ou
  - compre de um amigo que tenha bitcoins
  - serviço de classificados localbitcoins (https://localbitcoins.com/)
  - venda algo em bitcoins (programação ? web ? ...)
  - use um caixa eletronico: coindesk (https://www.coindesk.com/bitcoin-atm-map/)

Onde ?

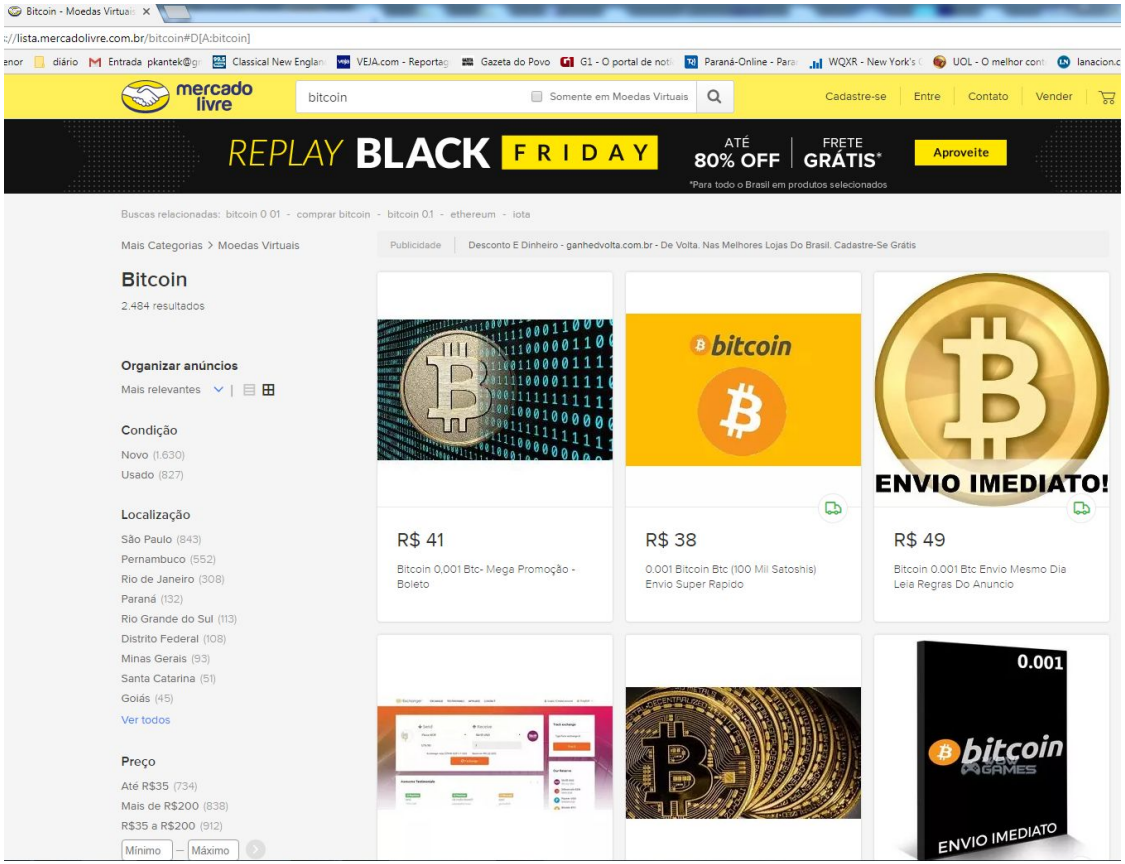

Bitstamp
Home
Account
Buy / Sell
Deposit
Withdrawal
Tradeview
BTC / USD
USD 9609.99
Register
Log In
Go for the digital currency stars.
Start trading Bitcoin (BTC), XRP, Litecoin (LTC) and Ether (ETH).
Create Account
SETTING STANDARDS
Compliant with leading examples of best practice.
NO HIDDEN FEES
Transparent volume-based pricing with no hidden fees.
INSTANT TRADING
Trade instantly - all major credit cards are supported.
SECURE AND TRANSPARENT
98% of digital funds stored offline. Subject to yearly audit by one of the Big Four.
OVERVIEW
Tradeview >


coinbase
Products
Help
Charts
Sign In
Sign Up
BUY AND SELL DIGITAL CURRENCY
Coinbase is the world's most popular way to buy and sell bitcoin, ethereum, and litecoin.
Enter your email address
Get Started
New to bitcoin?
What is ethereum?
THE WALL STREET JOURNAL
Bloomberg
The New York Times
TIME


LocalBitcoins
Buy bitcoins
Sell bitcoins
Post a trade
Forums
Help
Sign up free
Log in
Buy and sell bitcoins near you
Instant. Secure. Private.
Trade bitcoins in 15616 cities and 248 countries including Brazil.
Sign up free
QUICK BUY
QUICK SELL
Amount
BRL
Brazil
All online offers
Search
SMS not required
ID not required
Buy bitcoins online in Brazil
Seller
Payment method
Price / BTC
Limits
ethereumpy (30+; 100%)
Transfers with specific bank: Banco ITAU R$ To Online
34,149.90 BRL
3,540 - 3,542 BRL
Buy
Bitgoiano (500+; 100%)
Transfers with specific bank: Caixa ECONOMICA/BRADSCO/BDOBRASIL
34,215.94 BRL
500 - 2,200 BRL
Buy
Tiagotx (19; 100%)
Transfers with specific bank: BRADESCO/CAIXA B.B/ITAU/INTERM/TED
34,520.79 BRL
50 - 2,500 BRL
Buy
bh.btc (1000+; 99%)
Transfers with specific bank: BRADESCO ITAU CAIXA B.B SANTANDER INTERM
34,528.13 BRL
100 - 5,638 BRL
Buy


coindesk
Blockchain 101
Technology
Markets
Business
Data & Research
Consensus
Search
Vote for CoinDesk's Most Influential People in Blockchain 2017
Bitcoin ATM Map
The Bitcoin ATM Map is no longer maintained. Please try CoinATM Radar for more current data.
Germany
France
Italy
Bitcoin $9634.78
Ethereum $479.24
Which country has best responded to ICOs?
The U.S. – Governments should issue guidance and make rulings case by case
China – Governments should ban the practice
None of the above – Governments should not regulate ICOs
VOTE
Don't miss a single story
Subscribe to our free newsletter and follow us
Email Address
SUBSCRIBE
Features
Bitcoin ATM Map, News and Information
Contact us to add a Bitcoin ATM (Or BTM!) with the details once live. Location details are needed and proof of operation.
Bitcoin ATM Suppliers and Projects

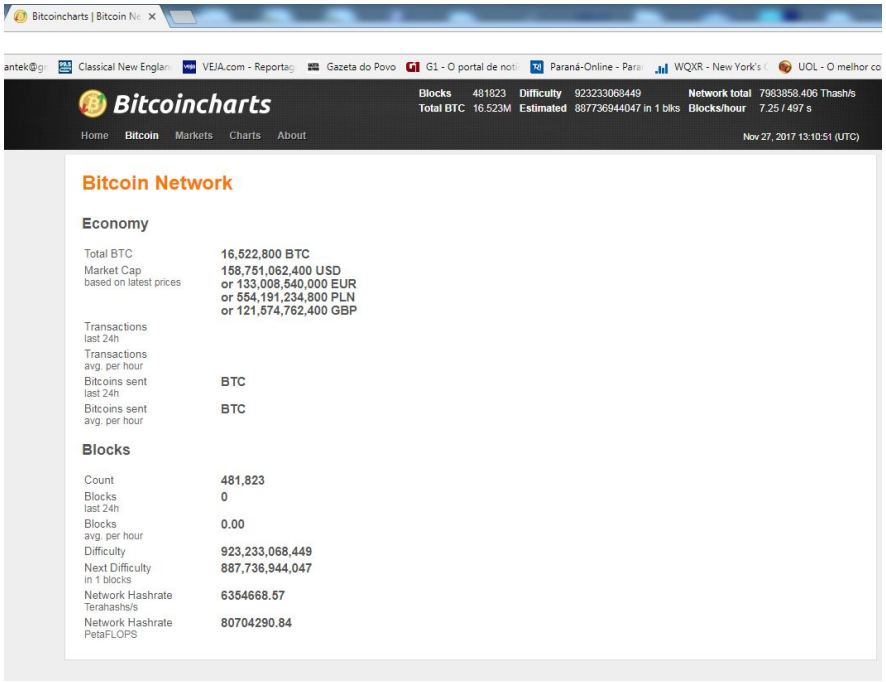
Onde - 2

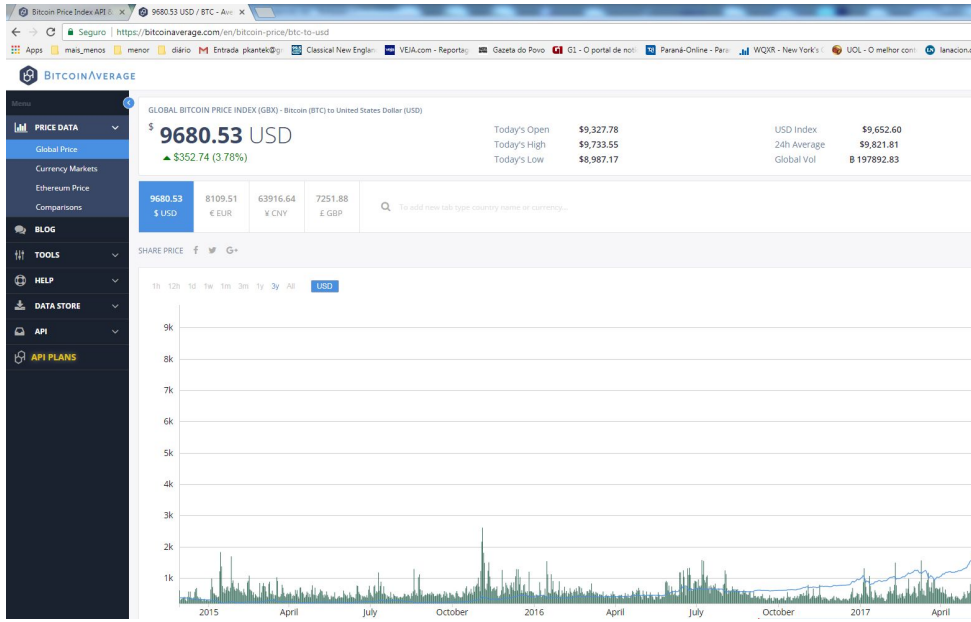

Bitcoin - Moedas Virtuais
mercado livre
bitcoin
Somente em Moedas Virtuais
Cadastre-se
Entre
Contato
Vender
REPLAY BLACK FRIDAY
ATÉ 80% OFF
FRETE GRÁTIS*
Aproveite
*Para todo o Brasil em produtos selecionados
Buscas relacionadas: bitcoin 0.01 - comprar bitcoin - bitcoin 0.1 - ethereum - iota
Mais Categorias > Moedas Virtuais
Publicidade
Desconto E Dinheiro - ganhedvolta.com.br - De Volta. Nas Melhores Lojas Do Brasil. Cadastre-Se Grátis
Bitcoin
2.484 resultados
Organizar anúncios
Mais relevantes
Condição
Novo (1.630)
Usado (827)
Localização
São Paulo (843)
Pernambuco (552)
Rio de Janeiro (308)
Paraná (132)
Rio Grande do Sul (113)
Distrito Federal (108)
Minas Gerais (93)
Santa Catarina (51)
Goiás (45)
Ver todos
Preço
Até R$35 (734)
Mais de R$200 (838)
R$35 a R$200 (912)
Mínimo
Máximo
bitcoin
ENVIO IMEDIATO!
R$ 41
Bitcoin 0,001 Btc- Mega Promoção - Boleto
R$ 38
0.001 Bitcoin Btc (100 Mil Satoshis) Envio Super Rapido
R$ 49
Bitcoin 0,001 Btc Envio Mesmo Dia Leia Regras Do Anuncio
0.001
bitcoin
ENVIO IMEDIATO

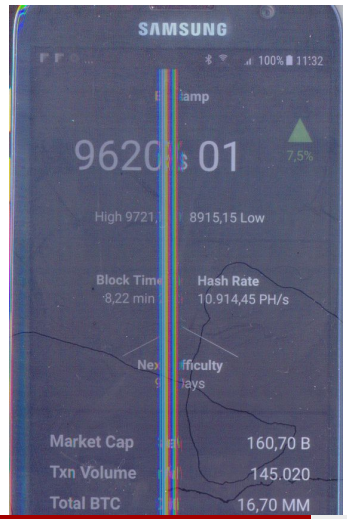
Quanto ?

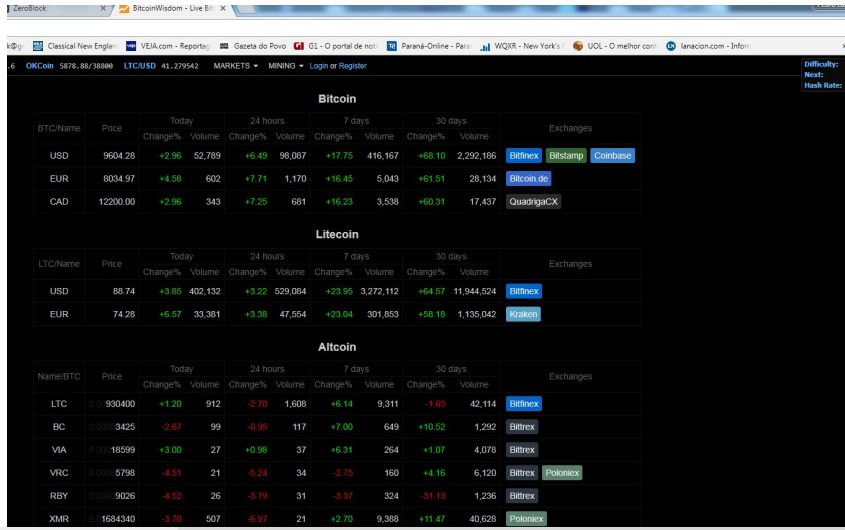
- bitcoin charts (https://bitcoincharts.com/bitcoin/)
- bitcoin average (https://bitcoinaverage.com/en/bitcoin-price/btc-to-usd)
- zero block (aplicativo para mobile: lojas)
- bitcoin wisdom (https://bitcoinwisdom.com/)

Quanto ?


Bitcoincharts
Blocks 481823 Difficulty 923233068449 Network total 7983858.406 Thash/s
Total BTC 16.523M Estimated 887736944047 in 1 blks Blocks/hour 7.25 / 497 s
Home Bitcoin Markets Charts About
Nov 27, 2017 13:10:51 (UTC)
Bitcoin Network
Economy
Total BTC 16,522,800 BTC
Market Cap 158,751,062,400 USD
based on latest prices or 133,008,540,000 EUR
or 554,191,234,800 PLN
or 121,574,762,400 GBP
Transactions last 24h
Transactions avg. per hour
Bitcoins sent last 24h BTC
Bitcoins sent avg. per hour BTC
Blocks
Count 481,823
Blocks last 24h 0
Blocks avg. per hour 0.00
Difficulty 923,233,068,449
Next Difficulty in 1 blocks 887,736,944,047
Network Hashrate Terahashs/s 6354668.57
Network Hashrate PetaFLOPS 80704290.84

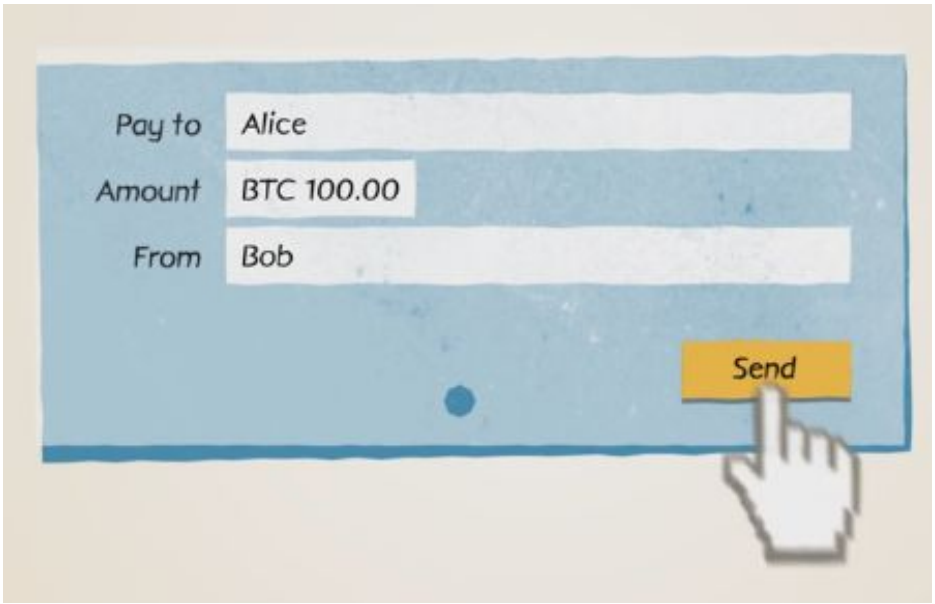

BITCOINAVERAGE
PRICE DATA
Global Price
Currency Markets
Ethereum Price
Comparisons
BLOG
TOOLS
HELP
DATA STORE
API
API PLANS
GLOBAL BITCOIN PRICE INDEX (GBX) - Bitcoin (BTC) to United States Dollar (USD)
$ 9680.53 USD
▲ $352.74 (3.78%)
Today's Open $9,327.78
Today's High $9,733.55
Today's Low $8,987.17
USD Index $9,652.60
24h Average $9,821.81
Global Vol Ƀ 197892.83
9680.53 $ USD
8109.51 € EUR
63916.64 ¥ CNY
7251.88 £ GBP
2015 April July October 2016 April July October 2017 April


SAMSUNG
Market Cap 160,70 B
Txn Volume 145.020
Total BTC 16,70 MM


Bitcoin
Litecoin
Altcoin
Exchanges
Bitfinex
Bitstamp
Coinbase
Bitcoin.de
QuadrigaCX
Kraken
Bittrex
Poloniex

A transação

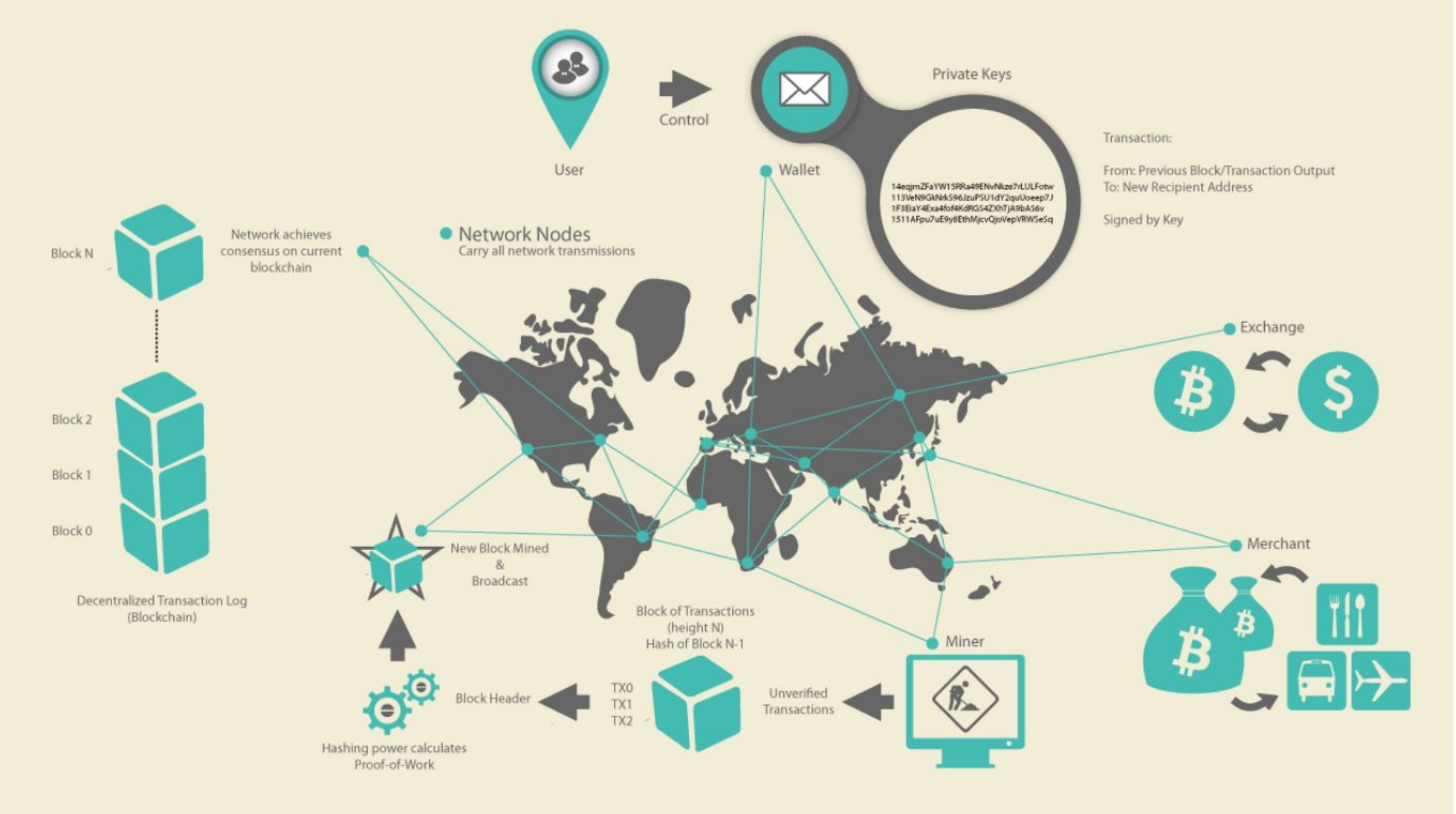
em qualquer aplicativo (por exemplo em https://www.blockchain.com/)



Confirmações

- Durante um tempo: o endereço de Alice mostra a transação de Bob como “transação não confirmada”.
- Quando for escolhida por um minerador vencedor, ela será incluída no blockchain.
- Após 6 blocos ela “ganha” o status de irreversível

Visão global do Bitcoin



Comprando uma xícara de café em bitcoin

O aplicativo do ponto de venda pode consultar a cotação e montar um QRCODE como

Código QR de solicitação de pagamento (Dica: Tente escanear esse código!)

O código QR de solicitação de pagamento codifica a seguinte URL, definida em BIP0021:

```
bitcoin:1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA?
amount=0.015&
label=Bob%27s%20Cafe&
message=Compra%20no%20Bob%27s%20Cafe

Componentes da URL

Um endereço bitcoin: "1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA"
Valor do pagamento (amount): "0.015"
Um rótulo para o endereço do destinatário (label): "Bob's Cafe"
Uma descrição para o pagamento (message): "Compra no Bob's Cafe"
```

Uma transação Bitcoin

Conceito: uma informação dirigida à rede de que o dono de uma certa quantidade de BTC transfere-os para outro dono.
Transações são linhas em um registro contábil de dupla entrada: [1] No Bitcoin:
Uma ou mais entradas (inputs) e uma ou mais saídas (outputs)
Pode OU não haver coincidência de valor. Se a entrada $>$ saída, a diferença é paga ao minerador que incluir esta transação no bloco, para furar a fila de transações. A longo prazo, esta vai ser a remuneração do minerador.

[1] No I Congresso Brasileiro de Contabilidade realizado em 1924, foram aprovadas quatro fórmulas de escrituração baseadas no método das partidas dobradas:

- 1ª fórmula um débito para cada crédito
- 2ª fórmula um débito e vários créditos
- 3ª fórmula vários débitos e um crédito
- 4ª fórmula vários débitos e vários créditos

Uma transação como registro contábil de dupla entrada

Transaction as Double-Entry Bookkeeping

Inputs	Value	Outputs	Value
Input 1	0.10 BTC	Output 1	0.10 BTC
Input 2	0.20 BTC	Output 2	0.20 BTC
Input 3	0.10 BTC	Output 3	0.20 BTC
Input 4	0.15 BTC		
Total Inputs:	0.55 BTC	Total Outputs:	0.50 BTC

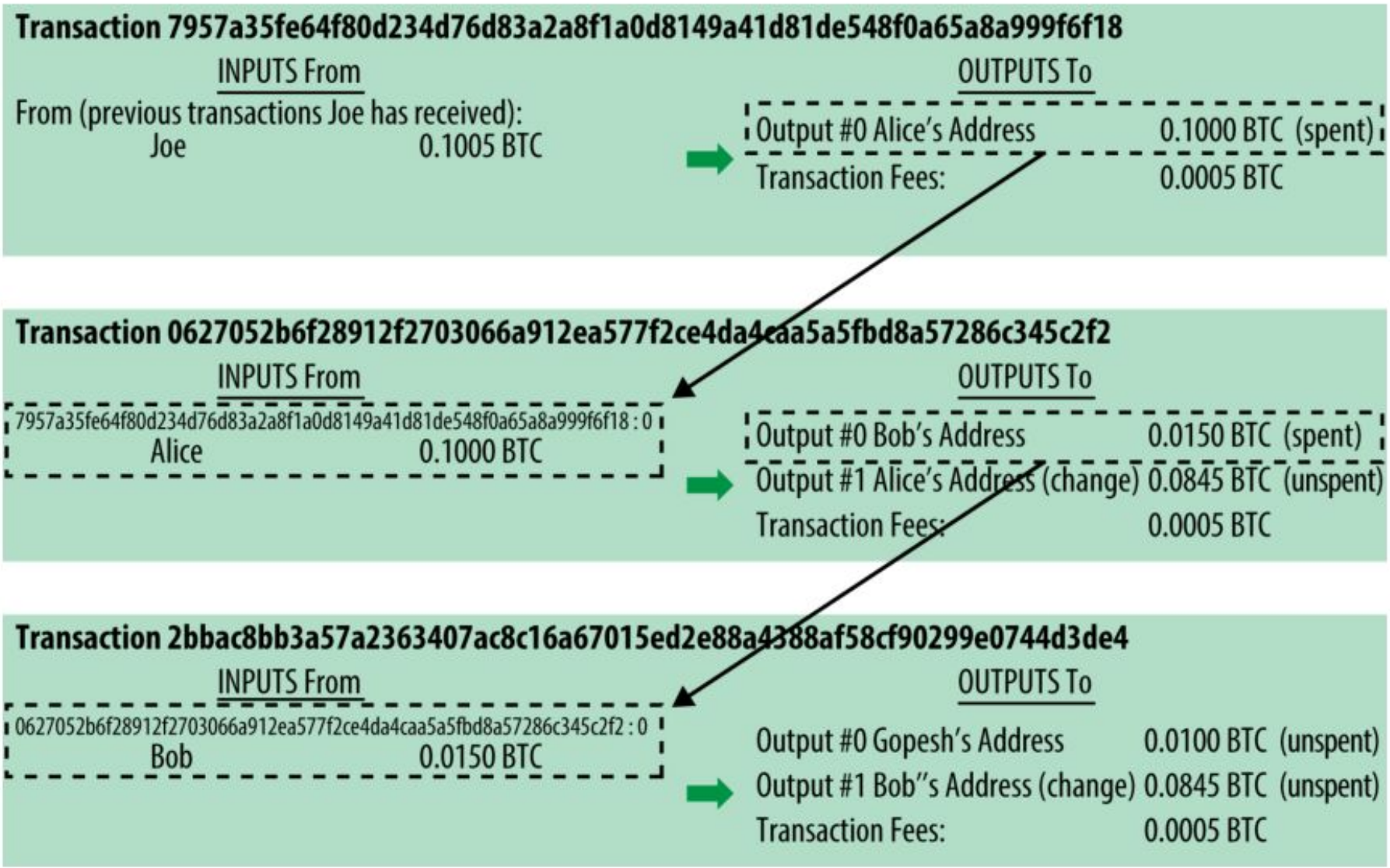
	Inputs	*0.55 BTC*
-	*Outputs*	*0.50 BTC*
	Difference	*0.05 BTC (implied transaction fee)*

Prova de posse

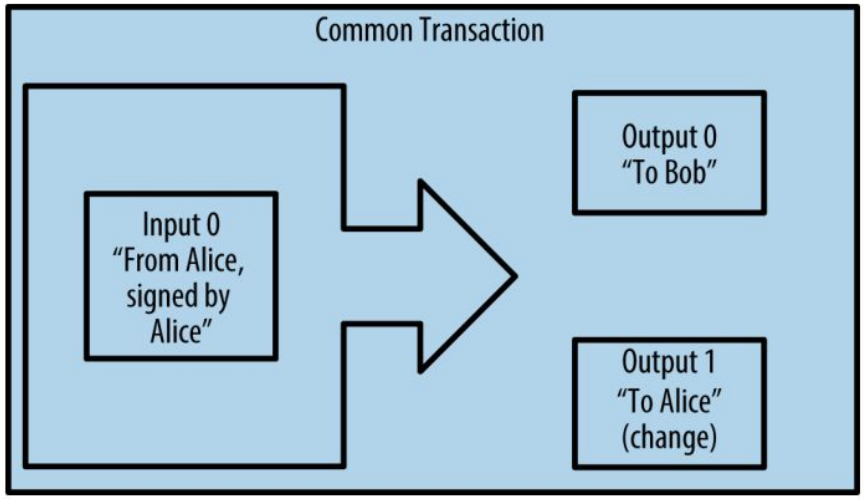
Cada entrada na transação que é transferida precisa uma prova de posse (assinatura digital do dono antigo). Pode ser validada facilmente por qualquer um. No Bitcoin, *gastar* é assinar uma transação de transferência para um novo endereço Bitcoin.

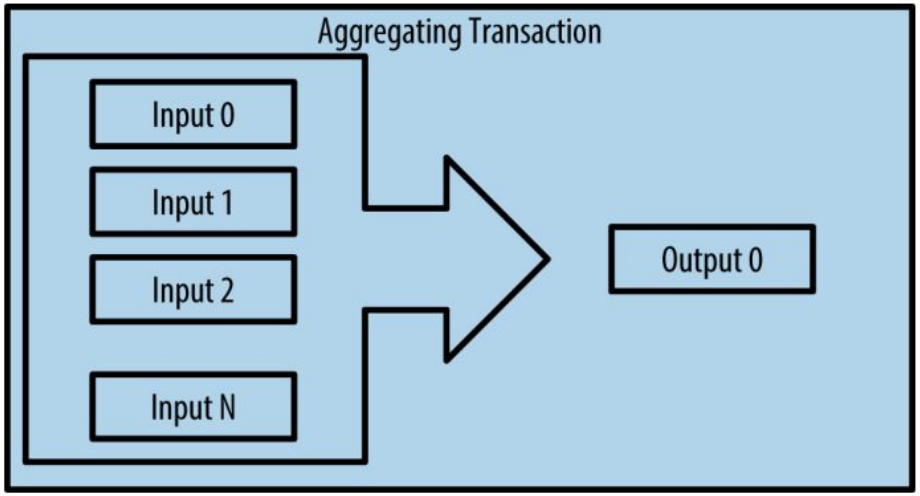
Esta transferência associa um valor ao novo dono através de um *script de travamento*. Este exige uma assinatura ou outra forma de validação (através de um script de destravamento) para este valor ser usado como entrada em uma transação futura. veja o exemplo
to spend = gastar (pret. e pp = spent)

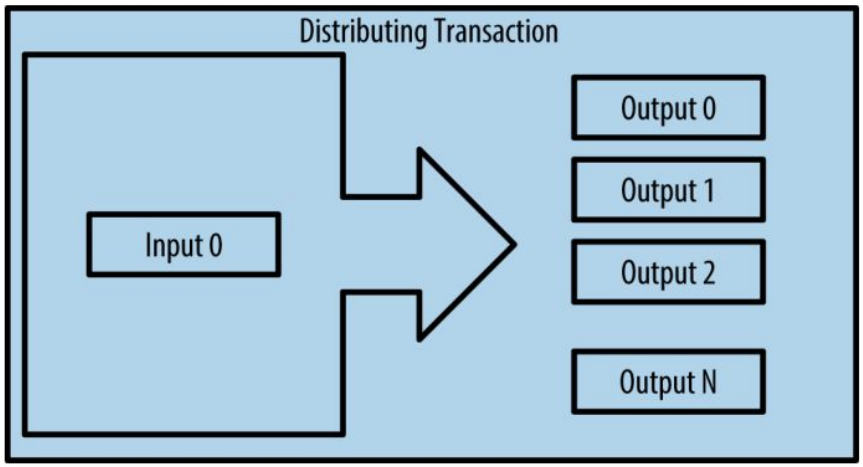
Uma cadeia de transações



Tipos de transação







Construindo uma transação

O aplicativo de carteira tem toda a lógica. Ele guarda num BD trancado os fundos (os inputs) daquela carteira. Pode ser feito offline (preencher um cheque). Se o cliente é completo ele valida todas as transações que chegam.
A saída é um script que aliena um valor. Este valor só pode ser resgatado se uma solução for apresentada ao script. Script pode ser: *pagar este output a quem apresentar uma assinatua para a chave do endereço público do credor*.
Havendo mais fundos que o gasto, a transação conterá um retorno na forma de troco. A transação pode ser vista usando um explorador de blockchain (web) como em

Uma transação no blockchain

Transaction View information about a bitcoin transaction

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK (0.1 BTC - Output)

1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA - (Unspent) 0.015 BTC

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK - (Unspent) 0.0845 BTC

97 Confirmations | 0.0995 BTC

Summary	
Size	258 (bytes)
Received Time	2013-12-27 23:03:05
Included In Blocks	277316 (2013-12-27 23:11:54 +9 minutes)

Inputs and Outputs	
Total Input	0.1 BTC
Total Output	0.0995 BTC
Fees	0.0005 BTC
Estimated BTC Transacted	0.015 BTC

Transmissão

- A transação é transmitida à rede P2P (não importa como)
- Quem recebe, valida e passa adiante.
- O credor pode receber a transação ANTES dela ser incluída no blockchain.
- A decisão de acatar ou aguardar é opção dele.
- Esperando 10 minutos: entra no BC (essa a idéia...)
- Esperando 60 minutos: considerada irreversível (idem)

Mineração

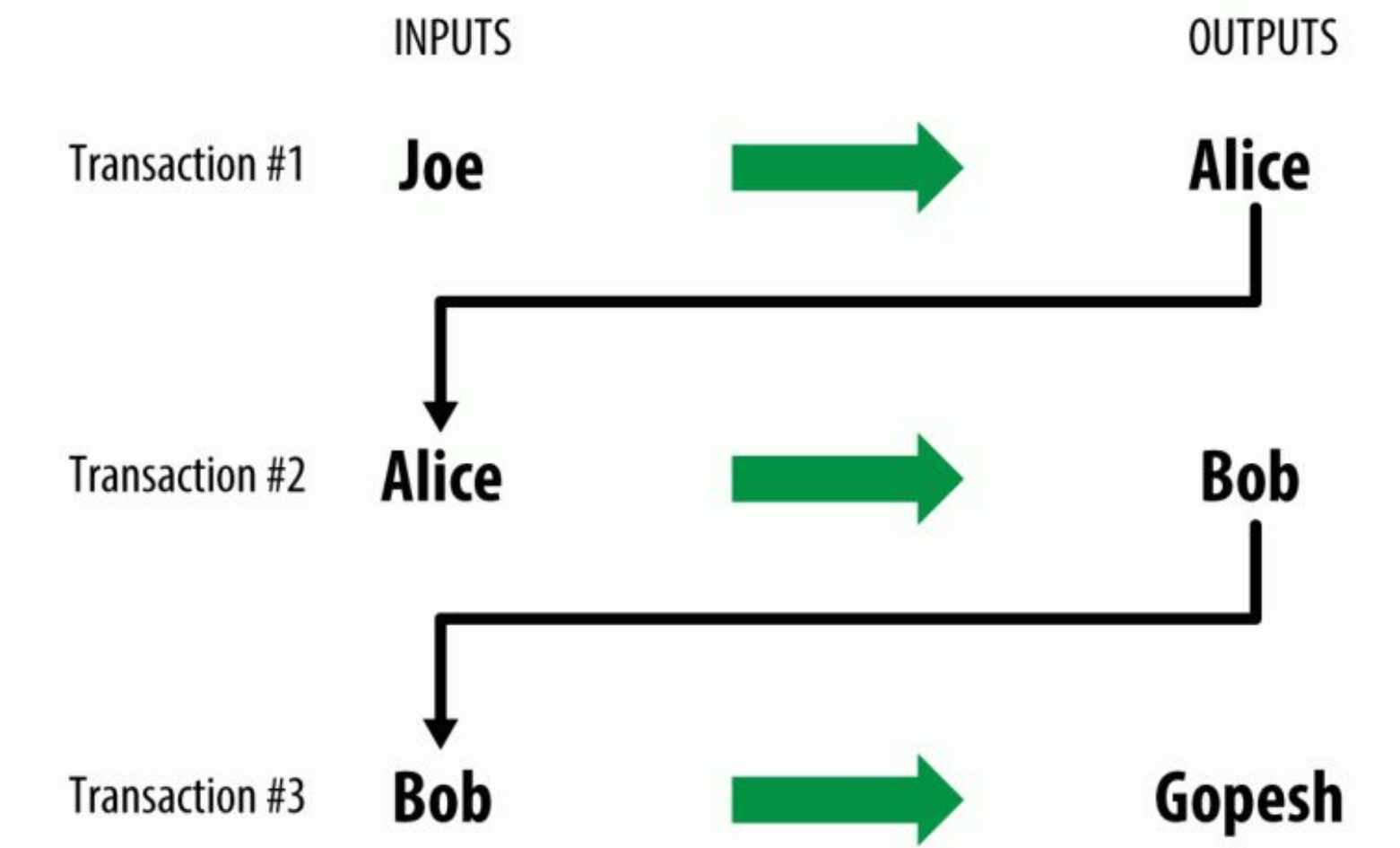
- A transação foi propagada
- os mineradores em ação vão capturá-la
- montar um bloco candidato e começar a mineração
- em 10 minutos (aproximadamente) alguém vai ter sucesso
- será remunerado pelo esforço (e pela competição) com moedas novas
- de quebra a transação (a primeira) será oficializada
- compromisso: a transação só será oficializada se enorme poder computacional for investido
- assimetria do hash: difícil achar, facil comprovar

Poder de mineração da rede bitcoin

Terahash/seg:

$2^{40} = 11.784.926 \times 1.099.511.627.776$ *hash/segundo* $(1\,TH \cong 10^{12})$

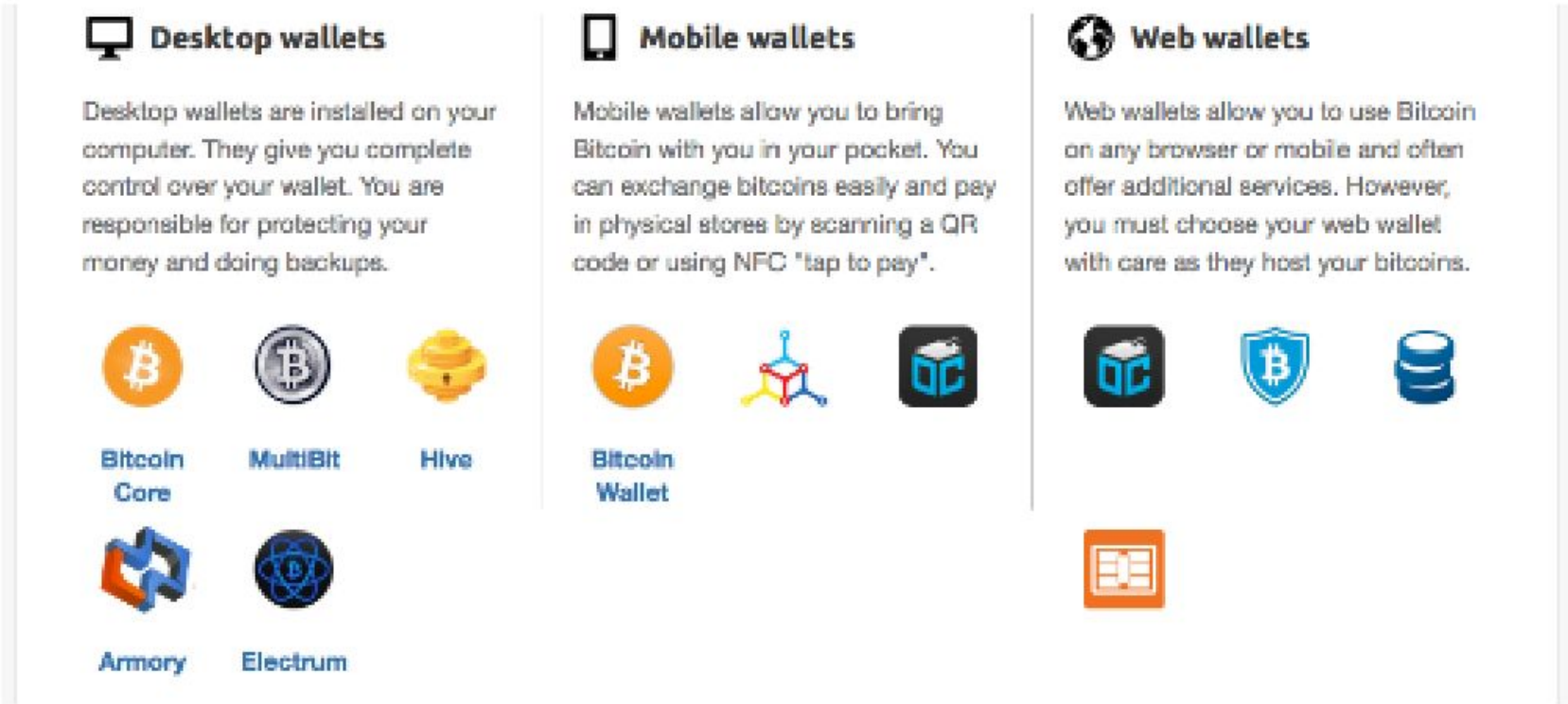
Gastando


INPUTS
OUTPUTS
Transaction #1
Joe
Alice
Transaction #2
Alice
Bob
Transaction #3
Bob
Gopesh

O cliente bitcoin

- em http://www.bitcoin.org pode baixar o *bitcoin core* o cliente referência em bitcoin (conhecido como cliente satoshi).
- Na primeira vez vai baixar a blockchain (150GB em finais de 2017)
- Quando acabar: *fora de sincronia* $\rightarrow$ *sincronizado*
- Para desenvolvedores: baixar o código fonte no github como um ZIP
- o cliente bitcoin core implementa uma interface JSON-RPC (protocolo de chamada de procedimento JSON)

Clientes disponíveis



Alguns comandos bitcoin RPC disponíveis

```
$ bitcoin-cli help
addmultisigaddress nrequired ["key",...] (
addnode "node" "add|remove|onetry"
backupwallet "destination"
createmultisig nrequired ["key",...]
createrawtransaction [{"txid":"id","vout":
decoderawtransaction "hexstring"
decodescript "hex"
dumpprivkey "bitcoinaddress"
dumpwallet "filename"
getaccount "bitcoinaddress"
getaccountaddress "account"
getaddednodeinfo dns ( "node" )
getaddressesbyaccount "account"
```

```
getbalance ( "account" minconf )
getbestblockhash
getblock "hash" ( verbose )
getblockchaininfo
getblockcount
getblockhash index
getblocktemplate ( "jsonrequestobject" )
getconnectioncount
getdifficulty
getgenerate
gethashespersec
getinfo
getmininginfo
getnettotals
getnetworkhashps ( blocks height )
getnetworkinfo
getnewaddress ( "account" )
getpeerinfo
getrawchangeaddress
```

```
getrawtransaction "txid" ( verbose )
getreceivedbyaccount "account" ( minconf )
getreceivedbyaddress "bitcoinaddress" ( minconf )
gettransaction "txid"
gettxout "txid" n ( includemempool )
gettxoutsetinfo
getunconfirmedbalance
getwalletinfo
getwork ( "data" )
help ( "command" )
importprivkey "bitcoinprivkey" ( "label" rescan )
importwallet "filename"
keypoolrefill ( newsize )
listaccounts ( minconf )
listaddressgroupings
listlockunspent
listreceivedbyaccount ( minconf includeempty )
listreceivedbyaddress ( minconf includeempty )
listsinceblock ( "blockhash" target-confirmations
listtransactions ( "account" count from )
listunspent ( minconf maxconf  ["address",...] )
```

```
setaccount "bitcoinaddress" "account"
setgenerate generate ( genproclimit )
settxfee amount
signmessage "bitcoinaddress" "message"
signrawtransaction "hexstring" (
[{"txid":"id","vout":n,"scriptPubKey":"hex"
["privatekey1",...] sighashtype )
stop
submitblock "hexdata" ( "jsonparametersobje
validateaddress "bitcoinaddress"
verifychain ( checklevel numblocks )
verifymessage "bitcoinaddress" "signature"
walletlock
walletpassphrase "passphrase" timeout
walletpassphrasechange "oldpassphrase" "new
```

Informações on line sobre Bitcoin

Existem inúmeras maneiras:

- Instalar uma carteira em nodo completo e usar comandos RPC bitcoin
- Instalar uma carteira simplificada e usar utilitários (python) ku e tx
- Consultar https://www.blockchain.com/
- Consultar https://live.blockcypher.com/
- Consultar https://www.blocktrail.com/BTC
- Consultar https://bitaps.com/ ($\leftarrow$ animada !)

Chaves, endereços, carteiras

A posse do bitcoin é estabelecida através de chaves digitais.
Uma chave é um conjunto de 2 números de mais de 70 dígitos.
Um deles é público, está em inúmeros lugares e é usado pelos outros para pagar coisas a você.
O outro é privado, e deve estar muito bem guardado:

- se alguém o roubar, ele passará a ser o dono do dinheiro
- se você o perder, o dinheiro estará perdido
- não há certificado de posse exceto este número
- não importa onde este número está: pendrive, computador, papel, cérebro de alguém

O público é facilmente calculado a partir do privado. A inversa não é verdadeira. Logo **O número privado é a única coisa a ser protegida**.
Uma analogia: a chave pública é o número da conta. A privada é a assinatura.

Um caso real

veja Jerusalém Tiririca Amarelas Ao Vivo – Vídeos Prêmio Veja-se TVEJA Revista V

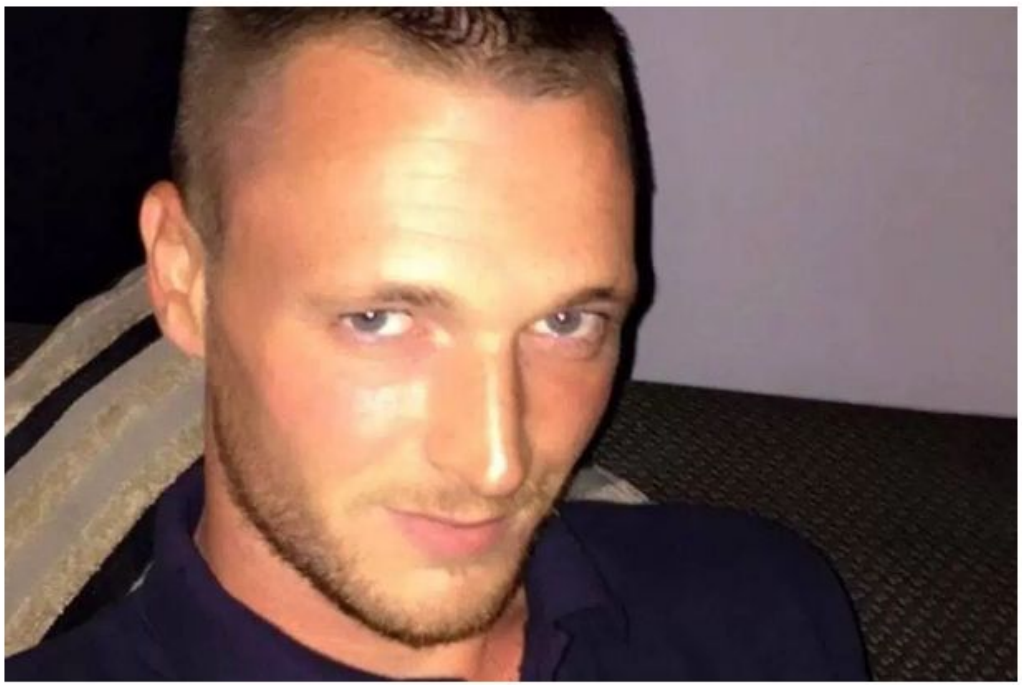
Economia

Britânico quer escavar lixão para reaver R$ 276 mi em bitcoins

Técnico em informática jogou fora, por engano, parte de computador em que estavam armazenadas suas moedas virtuais

Por **Da redação**

5 dez 2017, 16h58 - Publicado em 5 dez 2017, 13h04



Wallet

- wallet = carteira. Guarda as chaves
- a wallet nunca vai para a rede.
- Independe do protocolo, geradas e gerenciadas pelo software bitcoin, sem qualquer referência a blockchain ou acesso à internet.
- As chaves são a base de interessantes propriedades da bitcoin:
  - confiança descentralizada
  - controle do ambiente
  - atestação de posse
  - modelo de segurança por prova criptográfica

Transação bitcoin

Envolve três partes: recebimento do endereço destinatário, criação da transação, transmissão da transação
Gerada em algum computador no mundo (ligado ou não à rede bitcoin)
No local de **pagamento à**: endereço bitcoin (que é uma impressão digital da chave pública do destinatário)
Pode ser um usuário ou um script (um programa: logo absolutamente flexível)

criptografia

- Capítulo interessante da história da humanidade (O livro dos códigos de Simon Singh)
- Historicamente interessou a exércitos e amantes
- Antes do computador: Cifra de Cesar, Viginere, Playfair, ADFGVX,...
- Enigma e Código navajo
- Simétrica: uma senha lá e cá.
- A distribuição e gestão de senhas tendia a ser um problema incontrolável. Imagine a Internet...

Enigma

The imitation Game, filme de 2016

Navajo


NAVAJO INDIAN CODE TALKERS
U.S.M.C.
USED THEIR NATIVE LANGUAGE SKILLS TO
DIRECT U.S. MARINE CORPS ARTILLERY
FIRE DURING WWII IN PACIFIC AREA
JAPANESE COULD NOT BREAK CODE
THUS THESE EARLY AMERICANS
EXEMPLIFIED THE SPIRIT OF AMERICA'S
FIGHTING MEN
UNITED STATES MARINE CORPS
SPONSORED BY
DISABLED VETERANS
SOUTH MARION D.A.V. #85

Criptografia assimétrica

- 2 chaves: o que criptografa com uma, decriptografa com a outra e vice-versa
- Saber uma não implica descobrir a outra.
- Esconde-se a privada e publica-se a pública
- 2 processos

  Criptografia: $A \to B$: A criptografa com a pública de B e manda. Só B consegue ler.

  Certificação: $A \to x$: A criptografa com a sua privada. Todos podem ler, mas foi A que mandou.

Criptografia assimétrica

- o problema de distribuição de chaves crescia
- os mais visionários descobriram que a troca de chaves não era um axioma
- Whitfield Diffie e Martin Hellman (EUA) e James Ellis (Inglaterra) - a sacada: o receptor interfere na emissão
- Matemática de mão simples:
  - funções e funções inversas (p. ex: dobro e metade)
  - funções sem inversa: 10%3=x (x=1), mas x%3=1 (x pode ser 10, 13, 16, ... ∞)

RSA

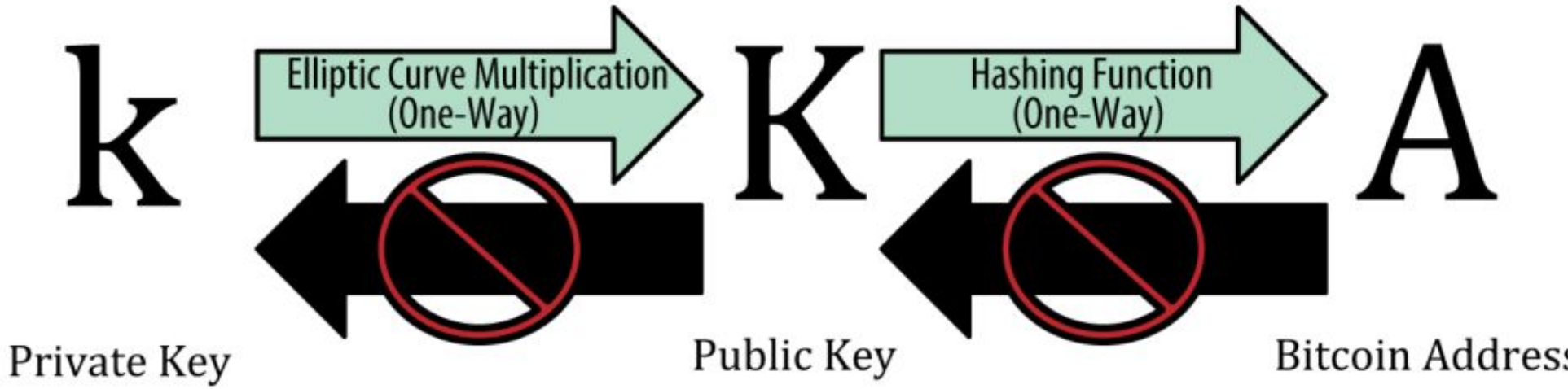
- Rivest, Shamir e Adleman
- criptografia na internet hoje

Para escolher a chave pública faz-se
n = produto de dois primos quaisquer p e q
c = qualquer número c que seja primo relativo a f = (p-1)x(q-1).
A chave pública é (c,n)
Para escolher a chave secreta
n = idem acima
d = qualquer desde que (c x d) mod f =(p-1)x(q-1) seja igual a 1.
A chave secreta é (d,n)
Para encriptar m (m tem que ser menor do que n)
$m^c mod\ n = y$
Para decriptar
$m = y^d mod\ n$

Criptografia no Bitcoin

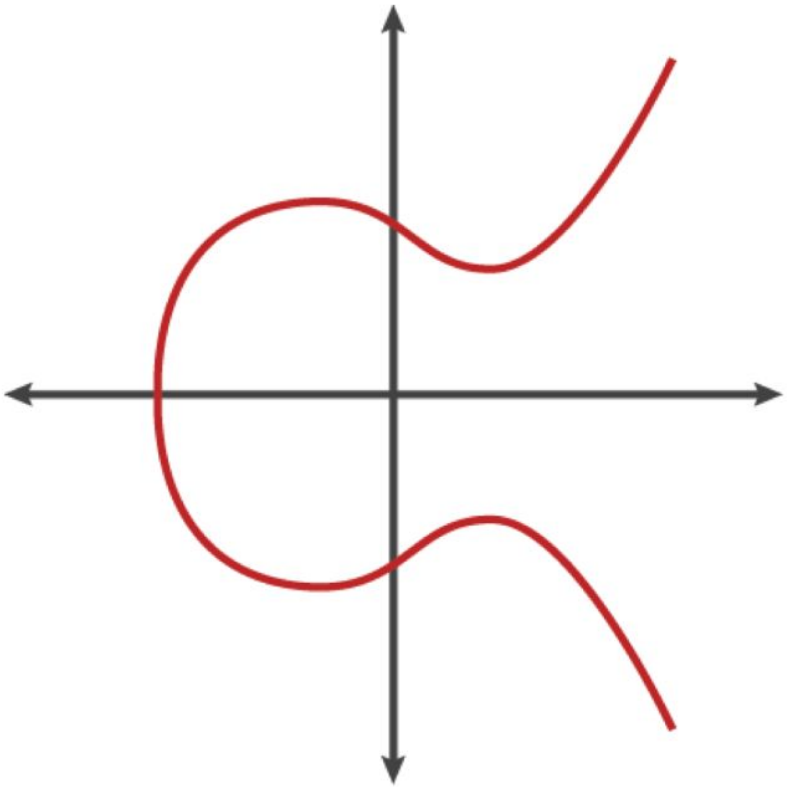
- Sai a exponenciação (RSA) entram as curvas elípticas (Lisbeth Salander, vol4)
- Papel importante na matemática moderna: Conjectura Tanayama-Shimura
- Último Teorema de Fermat: Andrew Willies, 1994
- Chave privada: um número de 256 bits escolhido ao acaso:
  - jogue 256 moedas: cara=0, coroa=1
  - Chame um software garantido com acesso a entropia ou aleatoriedade seguros
  - $2^{256} \approx 10^{77}$
- a chave pública é facilmente (!) calculada, fazendo uma multiplicação na curva elíptica
- a pública (K) funciona como gerador de seu endereço de pagamento
- a privada (k) garante que você é o dono da pública, permitindo gerar a assinatura que garante a posse dos bitcoins

Em termos gráficos



Na prática: fonte aleatória de qualquer tamanho $\rightarrow$ hash disso $\rightarrow$ 256 bits

Curva elíptica



- curva específica
- conjunto de constantes matemáticas
- definidas pelo padrão secp256k1
- definido pelo NIST
- função $y^2 = (x^3 + 7)\ mod\ p$
- $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$ um primo bem grande

Matemática elíptica

- Existe um ponto, chamado *ponto no infinito* que corresponde ao papel do zero na adição (elemento neutro).
- Existe um operador *passe* que funciona como a adição. Dados dois pontos P_1 e P_2 na curva, $P_3 = P_1 + P_2$ também na curva. Geometricamente P_3 é obtido ao passar uma reta entre P_1 e P_2. Ela cruza a curva em um ponto $P_x = (x, y)$. Refletindo P_x, obtem-se $P_3 = (x, -y)$.
- A multiplicação é definida por adições sucessivas: Para P_x na curva, $kP = P + P + P...$ (k vezes)

Algumas funções reais: (em python)

```
p=2**256 - 2**32 - 977
def inverse(x,p):
  inv1 = 1
  inv2 = 0
  while p != 1 and p!=0:
    inv1, inv2 = inv2, inv1 - inv2 *(x//p)
    x,p = p,x%p
  return inv2
def double_point(point,p):
  (x,y)=point
  if y==0:
    return None
  slope=3*pow(x,2,p)*inverse(2*y,p)
  xsum=pow(slope,2,p)-2*x
  ysum=slope*(x-xsum)-y
  return(xsum%p,ysum%p)
```

Mais

```
def add_point(p1,p2,p):
  (x1,y1)=p1
  (x2,y2)=p2
  if x1==x2:
    return double_point(p1,p)
  slope=(y1-y2)*inverse(x1-x2,p)
  xsum=pow(slope,2,p)-(x1+x2)
  ysum=slope*(x1-xsum)-y1
  return(xsum%p,ysum%p)
def point_mul(point,a,b):
  scale=point
  acc=None
```

```
while a:
  if a&1:
    if acc is None:
      acc=scale
    else:
      acc=add_point(acc,scale
  scale=double_point(scale,p)
  a>>=1
return acc
```

Agora: geração das coisas, passo-a-passo

```
Carregar as funções inverse, double_point,
                    add_point e mul_point
Carregar as constantes
p=2**256 - 2**32 - 977
g_x = 0x79BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959
       F2815B16F81798
g_y = 0x483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C
       47D08FFB10D4B8
g = (g_x,g_y)

Carregar os modulos:
import codecs
import hashlib
from base58 import b58encode
```

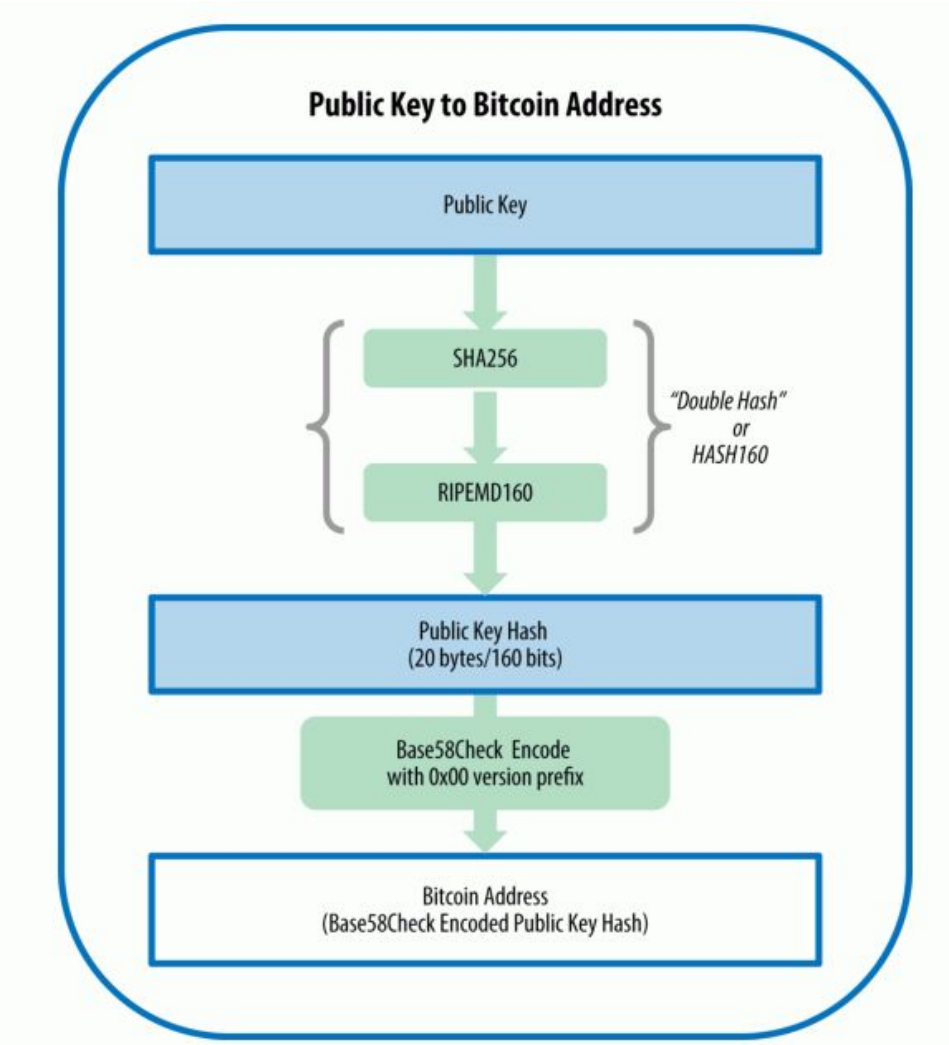
Tudo começa com a chave privada

```
k = 0x123456....abcdef # o número que você quiser....
K_x, K_y = point_mul(g,k,p)
print(K_x, K_y)
K = "04"+format(K_x,'x')+format(K_y,'x')
print(K)
K_bytes=codecs.decode(K.encode('utf-8'),'hex')
K_256=hashlib.sha256(K_bytes)
print(K_256.hexdigest())
K_ripe=hashlib.new('ripemd160')
K_ripe.update(K_256.digest())
print(K_ripe.hexdigest())
```

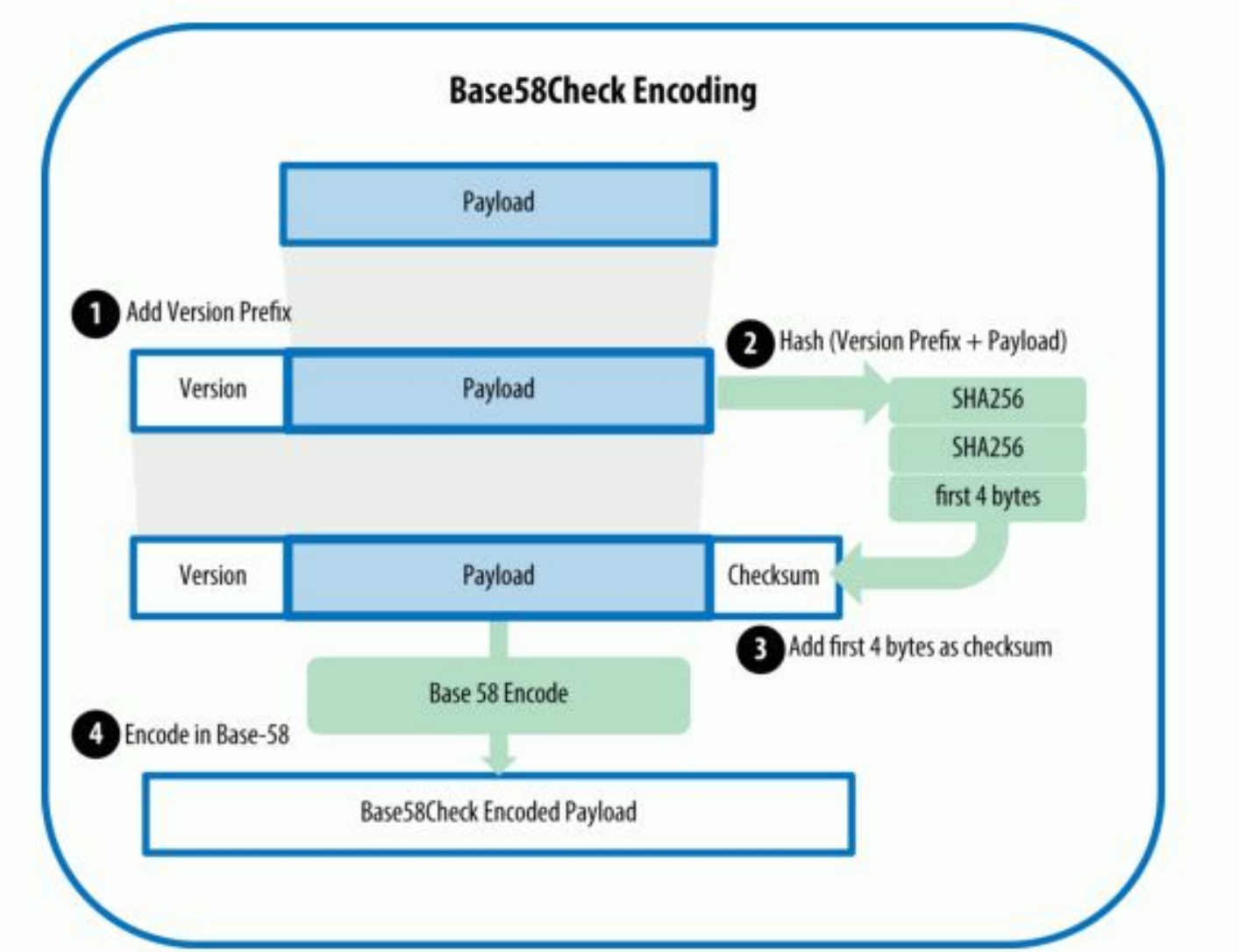
Mais

```
K_raw='00'+K_ripe.hexdigest()
print(K_raw) # endereço bitcoin, puro e em hexadecimal
K_rawbytes=codecs.decode(K_raw.encode('utf-8'),'hex')
print(K_rawbytes)
K_shasha=hashlib.sha256(hashlib.sha256(K_rawbytes).digest())
checksum=K_shasha.hexdigest()[:8]
print(checksum)
K_quase=K_raw+checksum
K_quasebytes=codecs.decode(K_quase.encode('utf-8'),'hex')
K_enfim=b58encode(K_quasebytes)
print(K_enfim)
```

Em termos gráficos



Em termos gráficos base58



Prefixos de versão

Tipo	Prefixo de versão (hex)	Base58 prefixo de resultado
Endereço Bitcoin	0x00	1
Endereço Pay-to-Script-Hash	0x05	3
Endereço Bitcoin Testnet	0x6F	m ou n
Chave Privada WIF	0x80	5, K ou L
Chave Privada Criptogr. em BIP38	0x0142	6P
Chave Pública Estendida em BIP32	0x0488B21E	xpub