Aula 012 - Bitcoin

Pagamentos

Prof. Rogério Aparecido Gonçalves[1]
rogerioag@utfpr.edu.br

[1]Universidade Tecnológica Federal do Paraná (UTFPR)
Departamento de Computação (DACOM)
Campo Mourão - Paraná - Brasil

Programa de Pós Graduação em Ciência da Computação
Mestrado em Ciência da Computação
PPGCC17 - Tópicos em Redes de Computadores e Cibersegurança

Agenda i

Introdução

Objetivos

- Apresentação de uma Visão Geral sobre rede **Bitcoin** e pagamentos.

Bitcoin

Bloco Genesis i

Bloco Genesis

O Bloco Genesis ou bloco $\#0$ foi *hardcoded* (codificado) por suas características especiais: ele é o único que não aponta para nenhum bloco anterior. No seu *hash* foi encriptado o bloco junto com a mensagem *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"*, manchete do jornal naquele dia. Além de servir como prova datada, a manchete escolhida representa justamente uma crítica ao sistema bancário.

Bloco Genesis ii

THE TIMES

Max 5C, min -5C | Saturday January 3 2009 timesonline.co.uk No 69523 | £1.50

Eat Out from £5

More than 900 great restaurants, including four **Gordon Ramsay** favourites from £15

Start collecting tokens today Pullout Inside

Israel prepares to send tanks and troops into Gaza

Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes News, page 3

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", The Times has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed gurantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1989 levels

Business, page 47

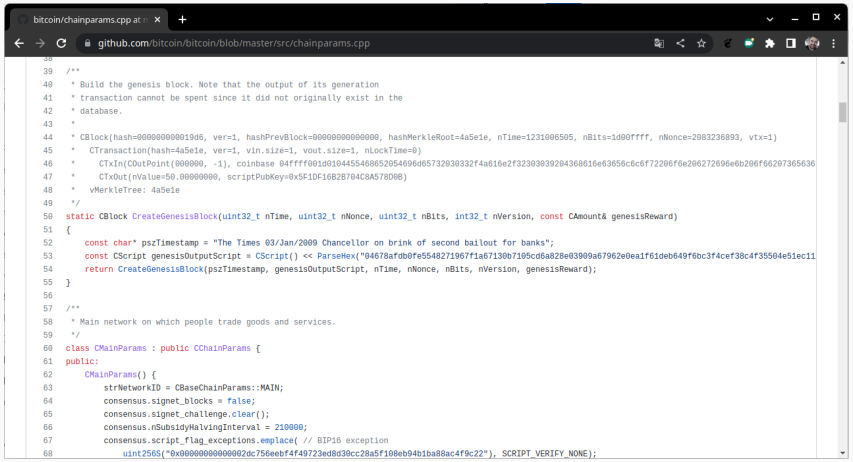
Michael Sheen Frost, Nixon and me
Magazine

Working mums So that's how she does it
Body&Soul

Detox in style The best spas on the planet
Travel

Salmon Rushdie I Won't Marry Again
Pages 22, 23

Giant Killing? Guide to the FA Cup Third Round
Sport




```
/**
 * Build the genesis block. Note that the output of its generation
 * transaction cannot be spent since it did not originally exist in the
 * database.
 *
 * CBlock(hash=000000000019d6, ver=1, hashPrevBlock=00000000000000, hashMerkleRoot=4a5e1e, nTime=1231006505, nBits=1d00ffff, nNonce=2083236893, vtx=1)
 *   CTransaction(hash=4a5e1e, ver=1, vin.size=1, vout.size=1, nLockTime=0)
 *     CTxIn(COutPoint(000000, -1), coinbase 04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c6c6f72206f6e206272696e6b206f66207365636
 *     CTxOut(nValue=50.00000000, scriptPubKey=0x5F1DF16B2B704C8A578D0B)
 *   vMerkleTree: 4a5e1e
 */
static CBlock CreateGenesisBlock(uint32_t nTime, uint32_t nNonce, uint32_t nBits, int32_t nVersion, const CAmount& genesisReward)
{
    const char* pszTimestamp = "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks";
    const CScript genesisOutputScript = CScript() << ParseHex("04678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec11
    return CreateGenesisBlock(pszTimestamp, genesisOutputScript, nTime, nNonce, nBits, nVersion, genesisReward);
}

/**
 * Main network on which people trade goods and services.
 */
class CMainParams : public CChainParams {
public:
    CMainParams() {
        strNetworkID = CBaseChainParams::MAIN;
        consensus.signet_blocks = false;
        consensus.signet_challenge.clear();
        consensus.nSubsidyHalvingInterval = 210000;
        consensus.script_flag_exceptions.emplace( // BIP16 exception
            uint256S("0x00000000000002dc756eebf4f49723ed8d30cc28a5f108eb94b1ba88ac4f9c22"), SCRIPT_VERIFY_NONE);
```

Fonte: https://github.com/bitcoin/bitcoin/blob/master/src/chainparams.cpp

Bloco Genesis iii

```
/**
 * Build the genesis block. Note that the output of its generation
 * transaction cannot be spent since it did not originally exist in the
 * database.
 *
 * CBlock(hash=000000000019d6, ver=1, hashPrevBlock=00000000000000, hashMerkleRoot=4a5e1e, nTime=1231006505, nB
 *   CTransaction(hash=4a5e1e, ver=1, vin.size=1, vout.size=1, nLockTime=0)
 *     CTxIn(COutPoint(000000, -1), coinbase 04ffff001d0104455468652054696d65732030332f4a616e2f3230303920436861
 *     CTxOut(nValue=50.00000000, scriptPubKey=0x5F1DF16B2B704C8A578D0B)
 *   vMerkleTree: 4a5e1e
 */
static CBlock CreateGenesisBlock(uint32_t nTime, uint32_t nNonce, uint32_t nBits, int32_t nVersion,
const CAmount& genesisReward)
{
  const char* pszTimestamp = "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks";
  const CScript genesisOutputScript = CScript() << ParseHex("04678afdb0fe5548271967f1a67130b7105cd6a828e03909a6
  return CreateGenesisBlock(pszTimestamp, genesisOutputScript, nTime, nNonce, nBits, nVersion, genesisReward);
}
```

A carteira de Satoshi i

- Carteira: `1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa`

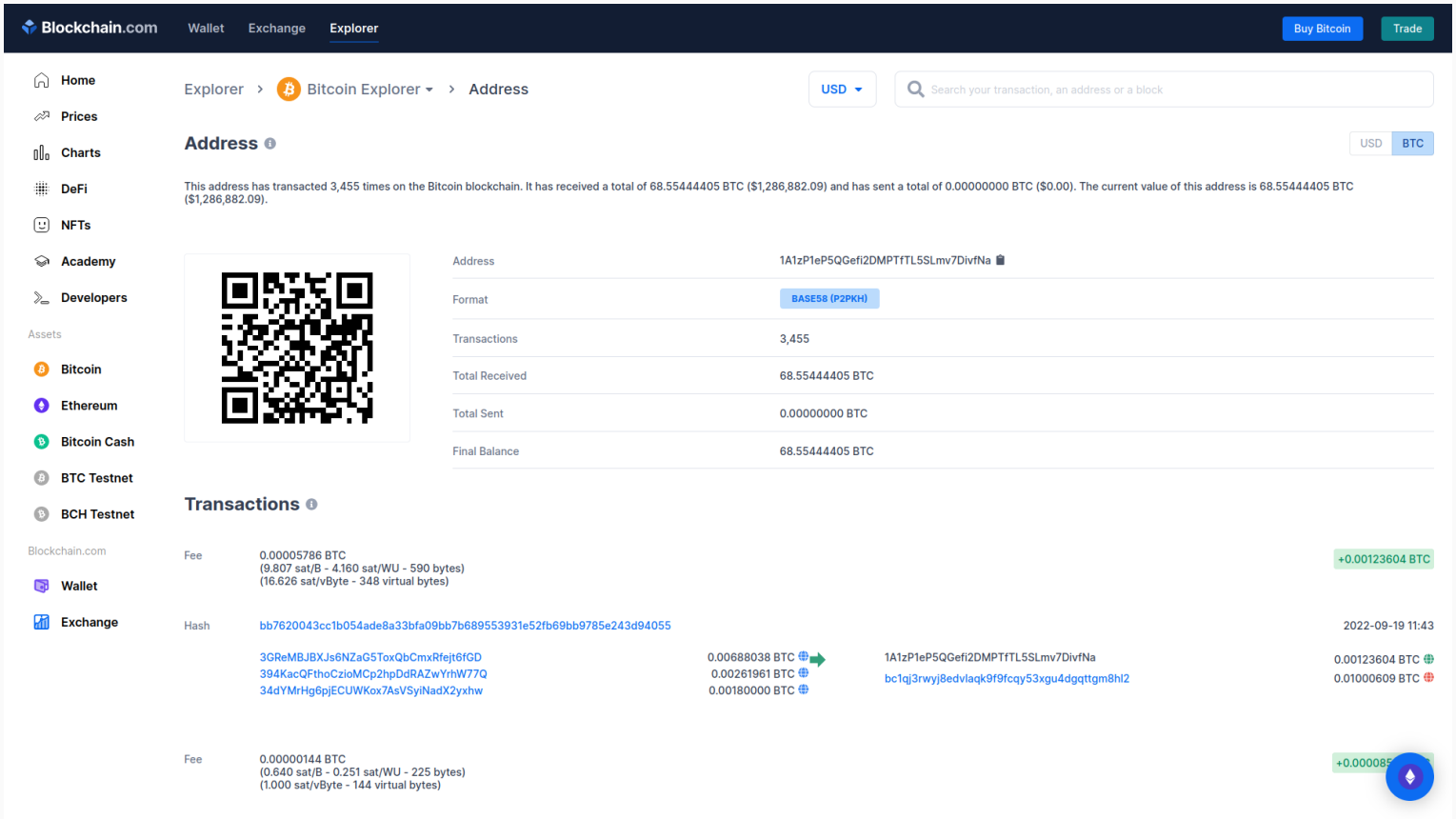


Figura 1: 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

A carteira de Satoshi ii

- Essa primeira transação foi incluída no **bloco #0**, sob o *hash* 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b.

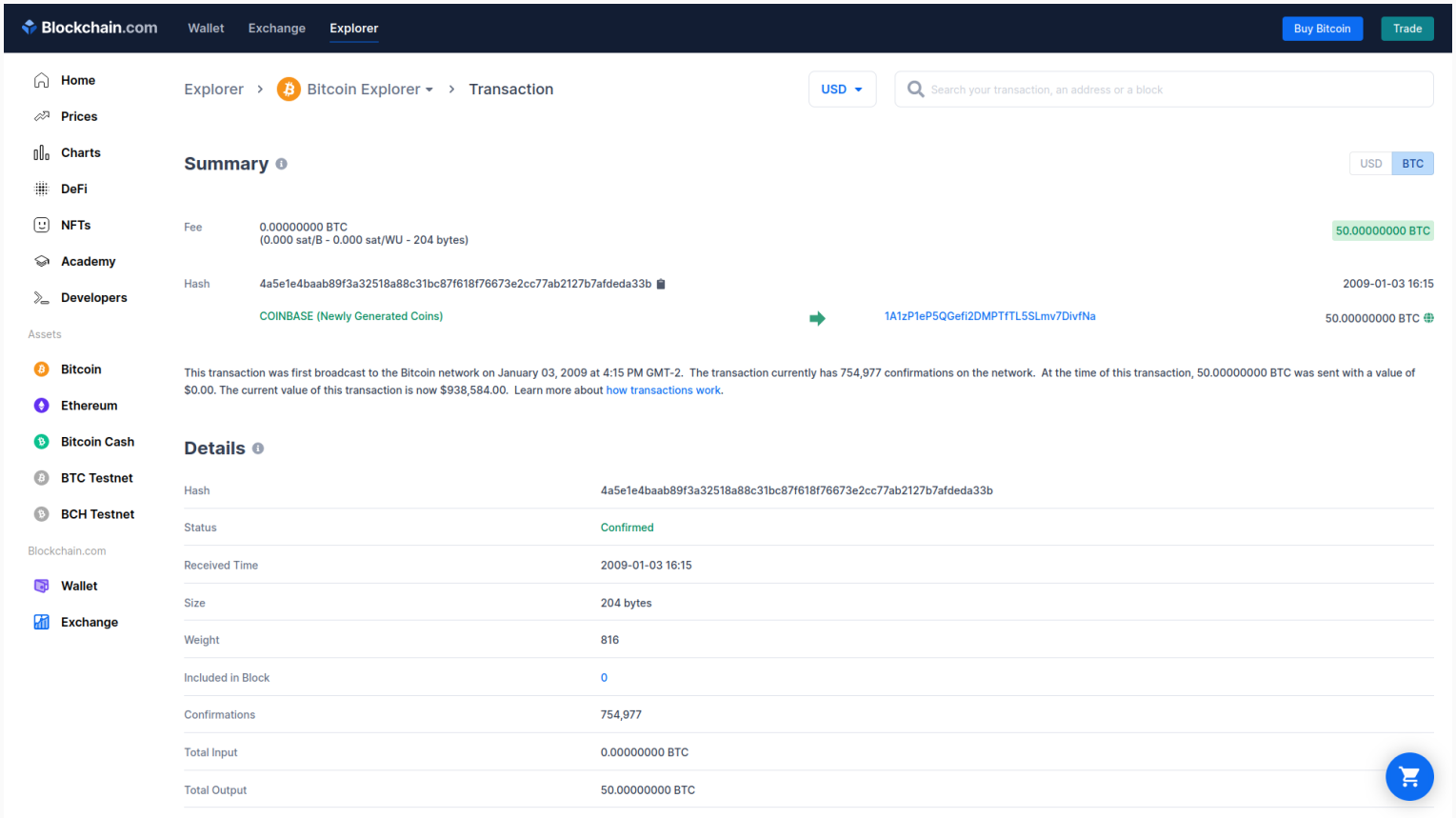


Figura 2: 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

A carteira de Satoshi iii

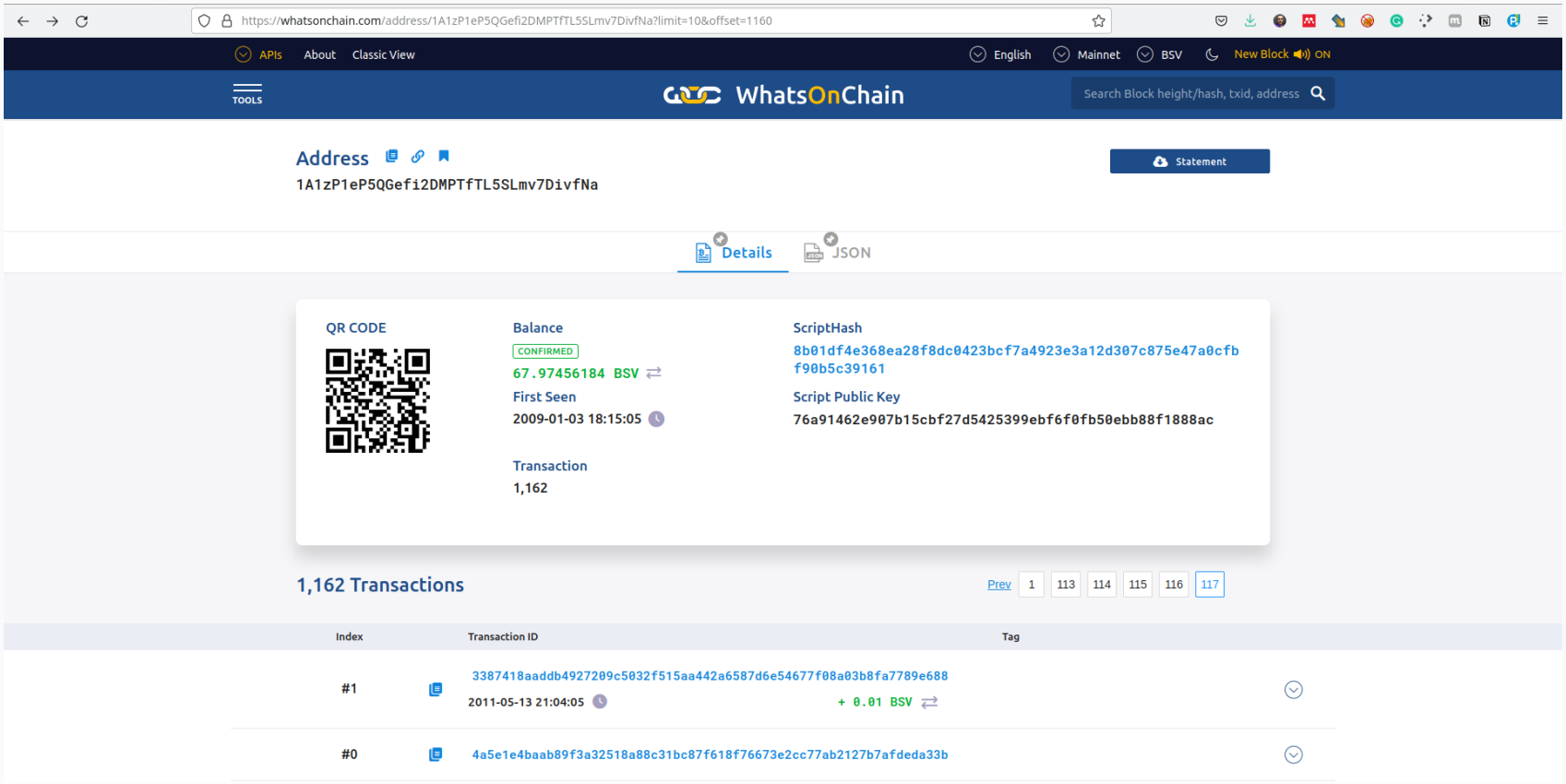


Figura 3: 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

A carteira de Satoshi iv

- Detalhes da Transação:

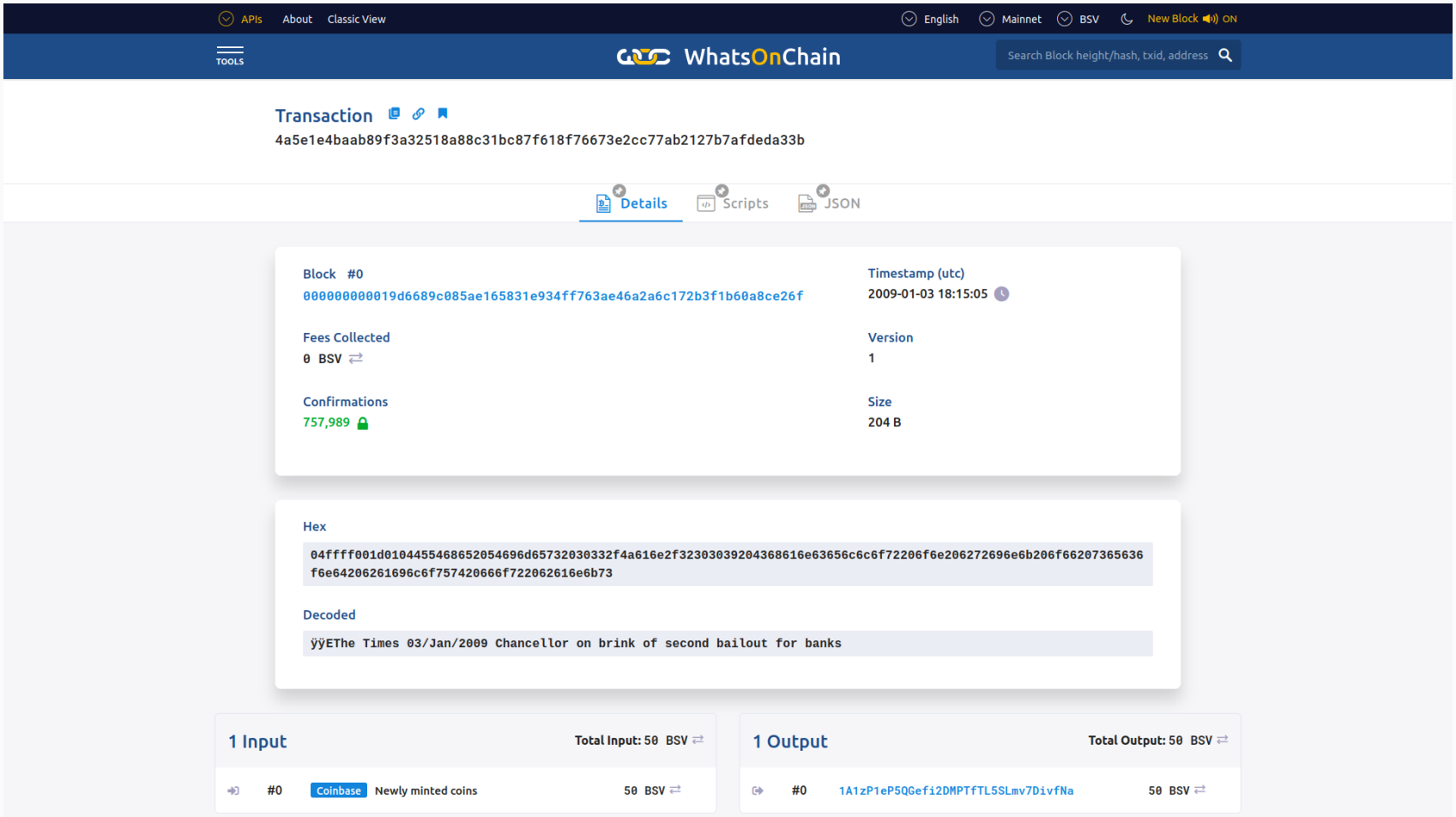
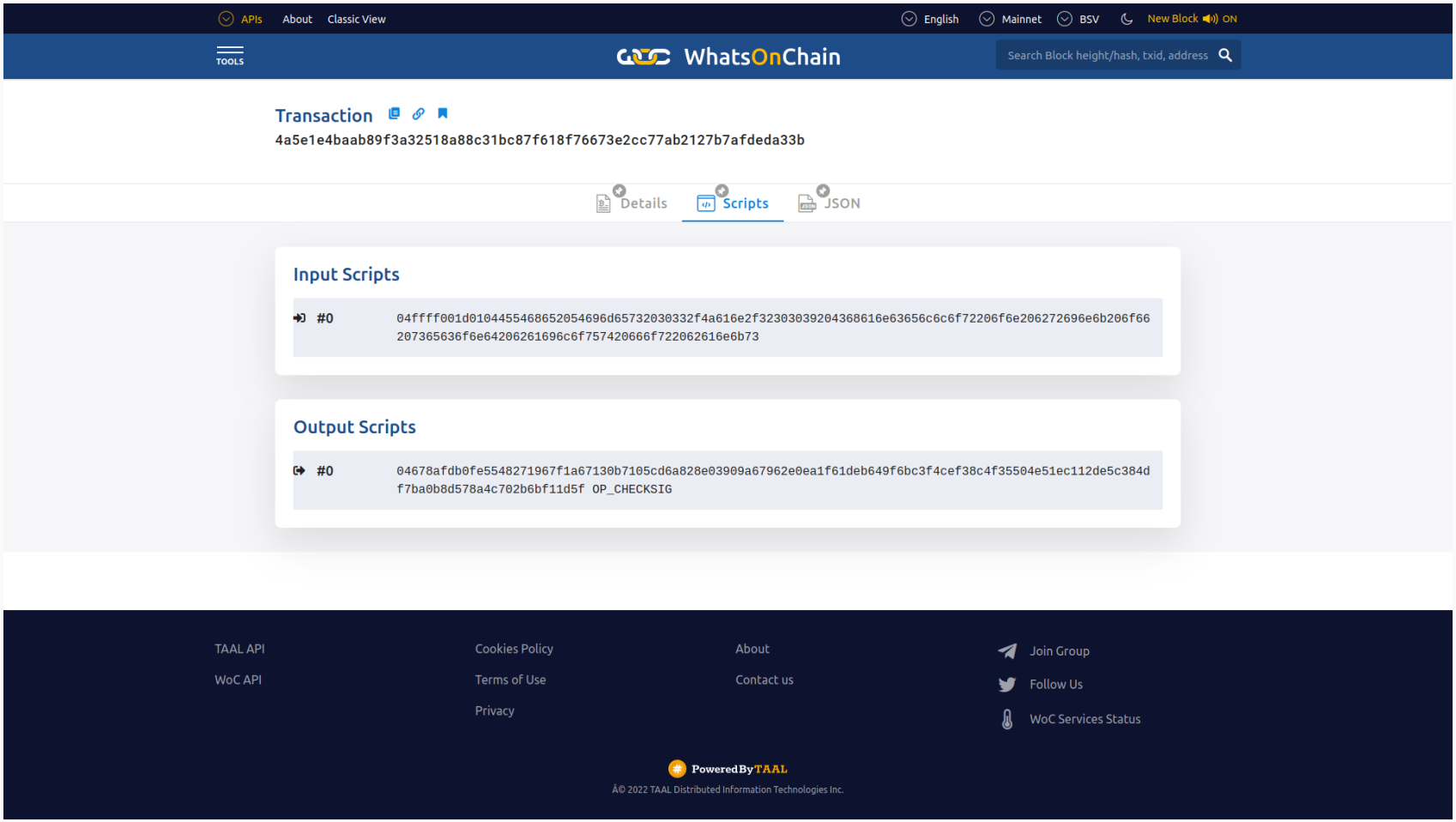


Figura 4: 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

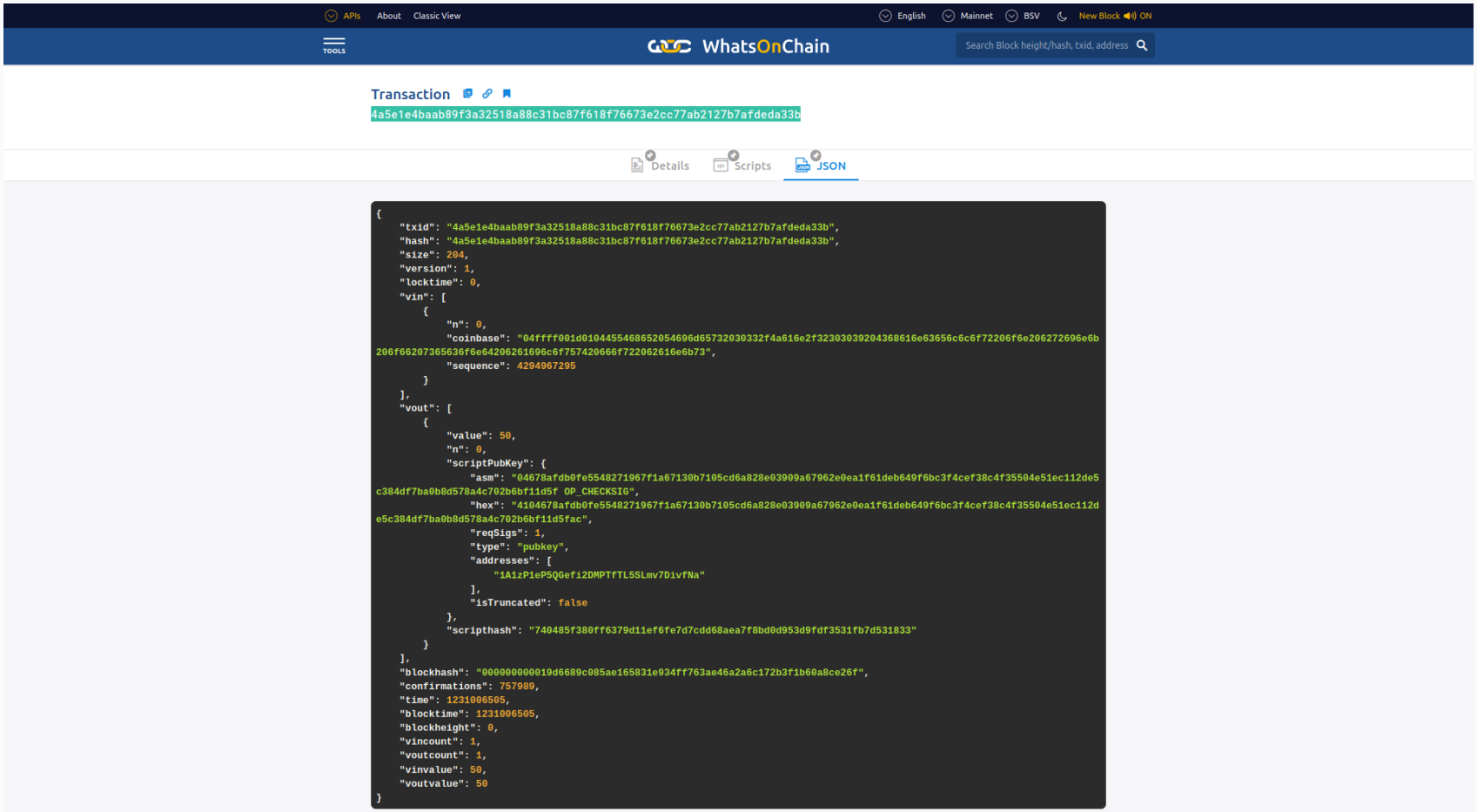
A carteira de Satoshi v

- Scripts



A carteira de Satoshi vi

- JSON



Transferência Inaugural i

A transferência inaugural de Bitcoin foi feita em 12 de Janeiro de 2009 para *Hal Finney*, primeiro a fazer *download* do software e minerar o bloco 170 com 50 BTCs de Satoshi. Finney foi escolhido em homenagem ao seu importante trabalho de criptografia *proof-of-work*.

Transferência Inaugural ii

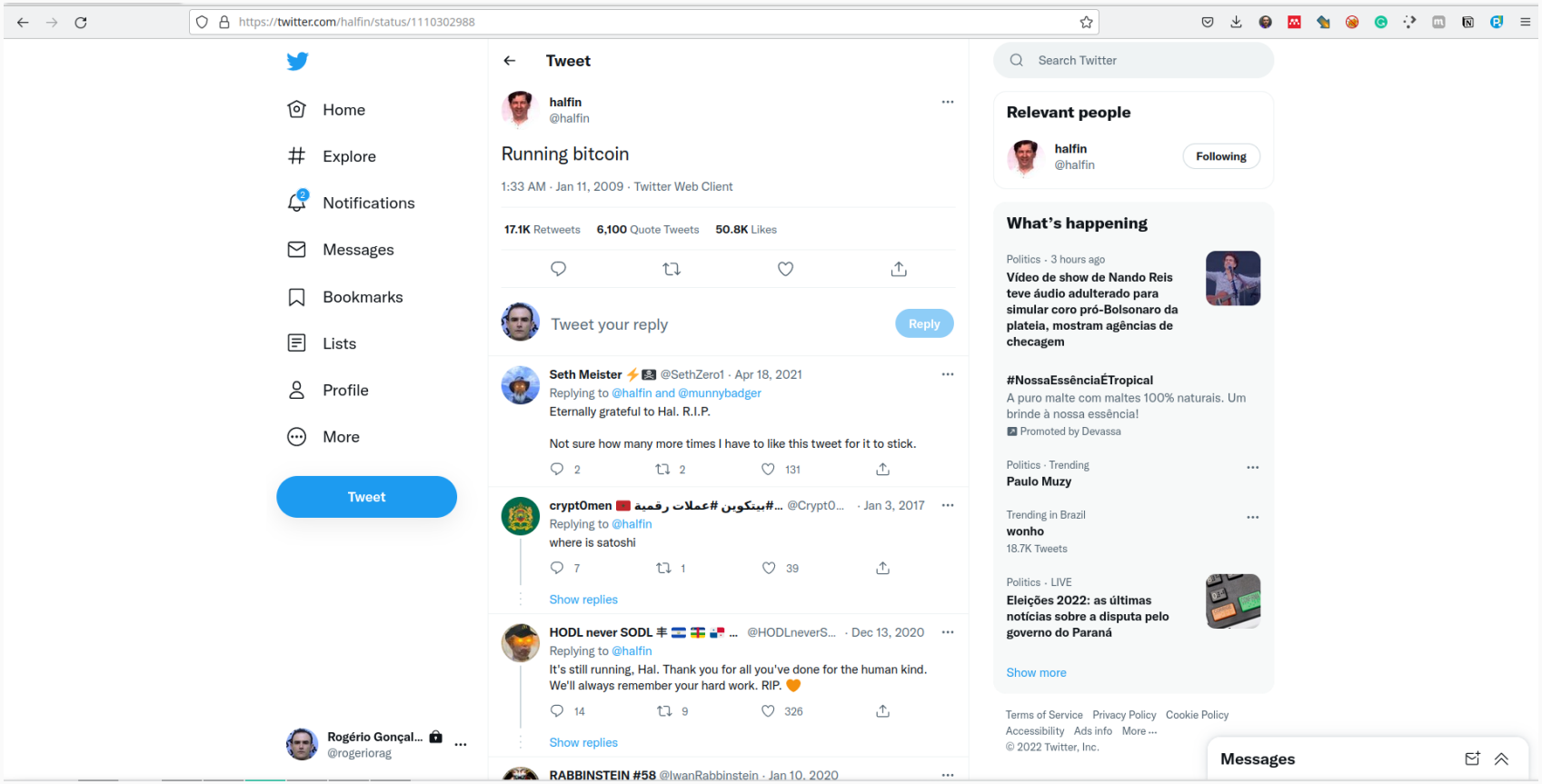


Figura 5: Tuíte de Hal Finney comunicando o início de suas atividades com Bitcoin

Transferência Inaugural iii

- Eles ficaram minerando sozinhos até 2010, quando foi divulgado em um grupo de nerds de tecnologia.
- Dentro deste grupo, *Laszlo Hanyecz* fez a primeira oferta pública para trocar 10.000 BTCs por duas pizzas da Domino's. A oferta ficou no ar por 4 dias, quando finalmente foi aceita por *Jercos* (Jeremy Sturdivant), um garoto de 18 anos na época.
- Então, o dia 22 de maio de 2010, a encomenda foi feita e a transação, realizado. *Laszlo* publicou no fórum a mensagem: *"Só para avisar que acabei de comprar uma pizza com 10.000 Bitcoins. Obrigado, Jercos!"*. Esse dia ficou conhecido e comemorado até hoje como `Pizza Day` (Dia da Pizza).

Transferência Inaugural iv

- A partir desse momento, *Bitcoin* passou a ser aceito como meio de pagamento por parte dos membros da comunidade em seus estágios iniciais. Desde então, lojas *on line* e físicas começaram a cogitar a possibilidade da criptografia operar fora de suas fronteiras, tornando-se, efetivamente, dinheiro.

Rede Bitcoin

Tipos de Nós da Rede i

- Tipos de Nós
  - Nós completos (Full nodes): quatro funções (wallet, mineração, armazenamento blockchain e nó de roteamento de rede).
  - SPV (Simple Payment Verification): clientes mais leves, funcionam como *wallets* e tem funções de roteamente de rede.
- Pool protocols
  - *Stratum*

Rede Bitcoin i

- Uma rede Bitcoin é identificada por um número mágico. Esses números mágicos são usados para indicar a rede de origem da mensagem.

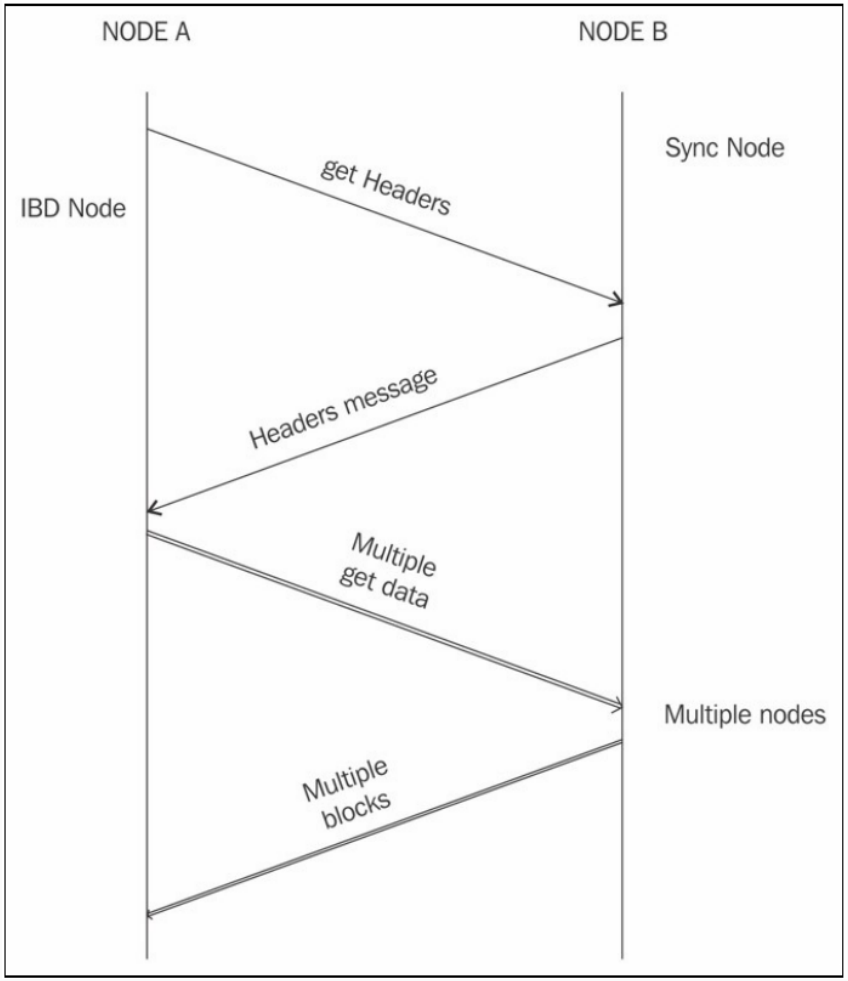
Network	*Magic value (in hex)*
main	`0xD9B4BEF9`
testnet	`0xDAB5BFFA`
testnet3	`0x0709110B`

Protocolo de mensagens i

- São 27 tipos de mensagens de protocolo. As mais comuns:

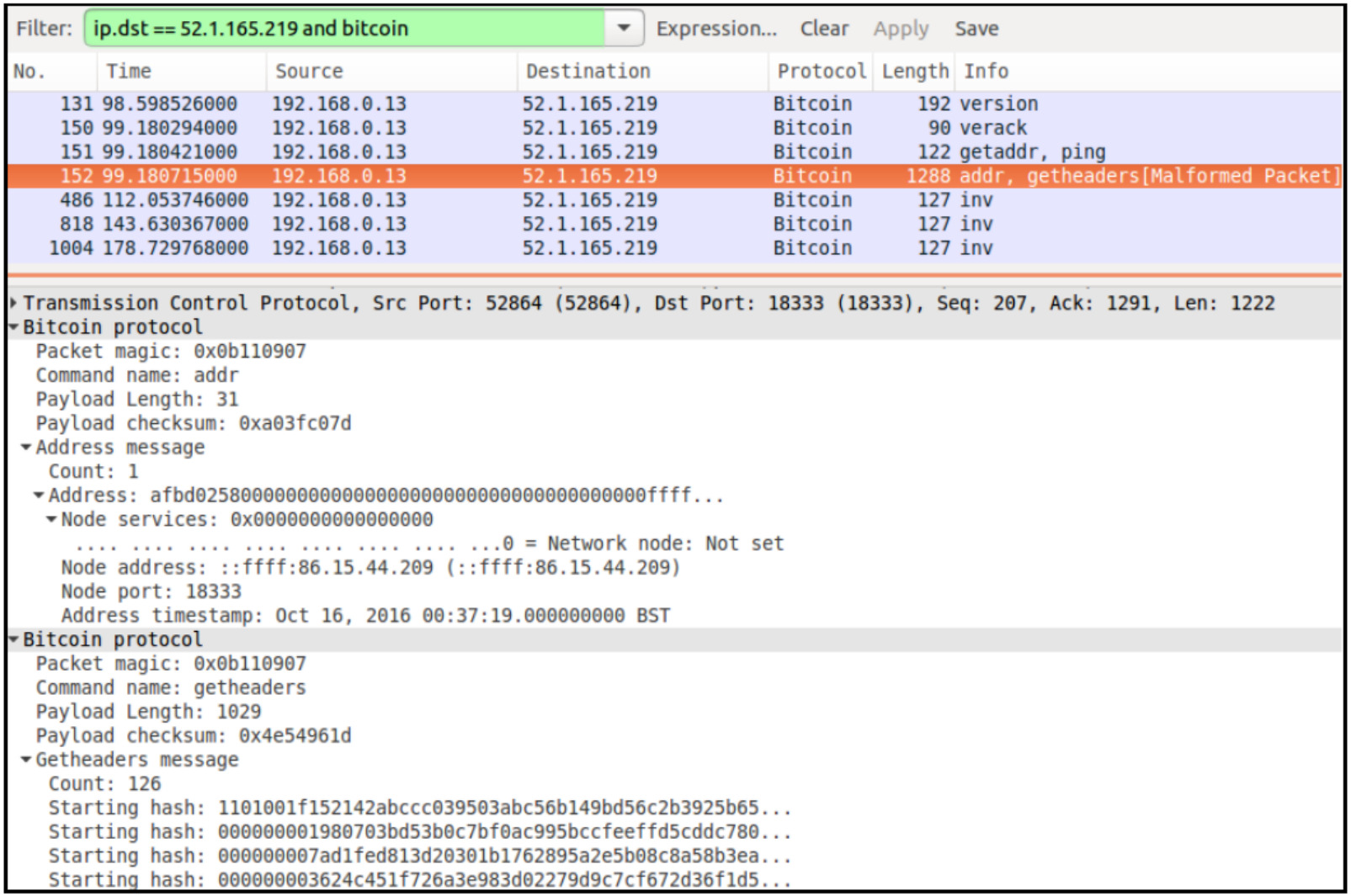
- Version
- Verack
- Inv
- Getdata
- Getblocks
- Getheaders
- Tx
- Block
- Headers
- Getaddr
- Addr
- Ping
- Pong

Processo de sincronização de blocos entre dois nós em uma rede *Bitcoin*.

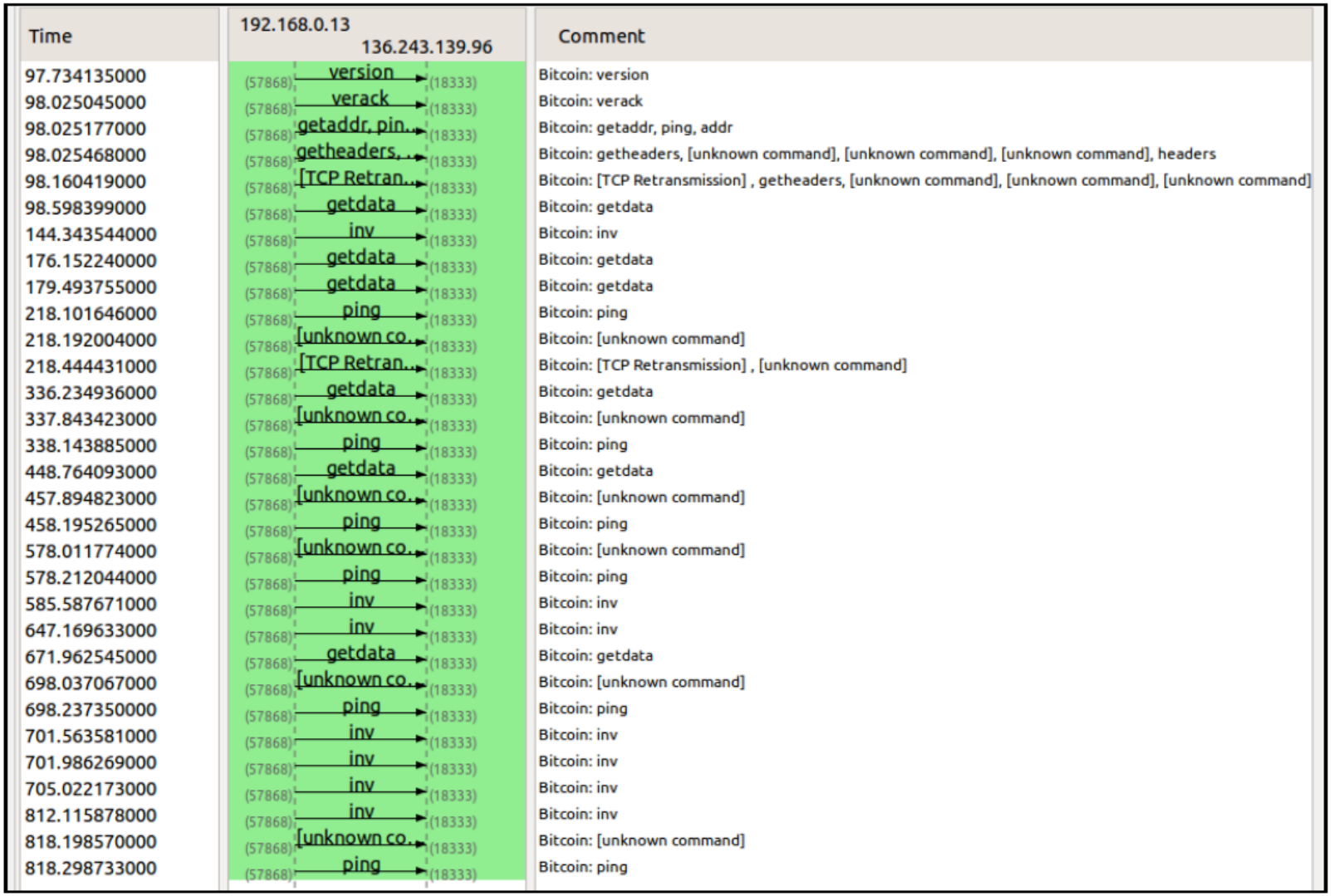


Protocolo de mensagens ii

- Captura das mensagens com `Wireshark`:



Protocolo de mensagens iii



Time	192.168.0.13 → 136.243.139.96	Comment
97.734135000	(57868) version (18333)	Bitcoin: version
98.025045000	(57868) verack (18333)	Bitcoin: verack
98.025177000	(57868) getaddr, pin.. (18333)	Bitcoin: getaddr, ping, addr
98.025468000	(57868) getheaders, .. (18333)	Bitcoin: getheaders, [unknown command], [unknown command], [unknown command], headers
98.160419000	(57868) [TCP Retran.. (18333)	Bitcoin: [TCP Retransmission] , getheaders, [unknown command], [unknown command], [unknown command]
98.598399000	(57868) getdata (18333)	Bitcoin: getdata
144.343544000	(57868) inv (18333)	Bitcoin: inv
176.152240000	(57868) getdata (18333)	Bitcoin: getdata
179.493755000	(57868) getdata (18333)	Bitcoin: getdata
218.101646000	(57868) ping (18333)	Bitcoin: ping
218.192004000	(57868) [unknown co.. (18333)	Bitcoin: [unknown command]
218.444431000	(57868) [TCP Retran.. (18333)	Bitcoin: [TCP Retransmission] , [unknown command]
336.234936000	(57868) getdata (18333)	Bitcoin: getdata
337.843423000	(57868) [unknown co.. (18333)	Bitcoin: [unknown command]
338.143885000	(57868) ping (18333)	Bitcoin: ping
448.764093000	(57868) getdata (18333)	Bitcoin: getdata
457.894823000	(57868) [unknown co.. (18333)	Bitcoin: [unknown command]
458.195265000	(57868) ping (18333)	Bitcoin: ping
578.011774000	(57868) [unknown co.. (18333)	Bitcoin: [unknown command]
578.212044000	(57868) ping (18333)	Bitcoin: ping
585.587671000	(57868) inv (18333)	Bitcoin: inv
647.169633000	(57868) inv (18333)	Bitcoin: inv
671.962545000	(57868) getdata (18333)	Bitcoin: getdata
698.037067000	(57868) [unknown co.. (18333)	Bitcoin: [unknown command]
698.237350000	(57868) ping (18333)	Bitcoin: ping
701.563581000	(57868) inv (18333)	Bitcoin: inv
701.986269000	(57868) inv (18333)	Bitcoin: inv
705.022173000	(57868) inv (18333)	Bitcoin: inv
812.115878000	(57868) inv (18333)	Bitcoin: inv
818.198570000	(57868) [unknown co.. (18333)	Bitcoin: [unknown command]
818.298733000	(57868) ping (18333)	Bitcoin: ping

Protocolo de mensagens iv

- Quando um nó *Bitcoin core* inicia, primeiro, ele descobre todos os seus pares da rede. Isto é alcançado consultando os *DNS seeds* que estão *hardcoded* no código do cliente *Bitcoin core* e que são mantidos peloa comunidade *Bitcoin*.
- O protocolo `Bitcoin` funciona sobre o TCP porta 8333 por padrão na rede principal e 18333 para a `testnet`.

Protocolo de mensagens v

- Os endereços de DNS no arquivo `chainparams.cpp`:

```
// Pieter Wuille, only supports x1, x5, x9, and xd
vSeeds.emplace_back("seed.bitcoin.sipa.be");
// Matt Corallo, only supports x9
vSeeds.emplace_back("dnsseed.bluematt.me");
// Luke Dashjr
vSeeds.emplace_back("dnsseed.bitcoin.dashjr.org");
// Christian Decker, supports x1 - xf
vSeeds.emplace_back("seed.bitcoinstats.com");
// Jonas Schnelli, only supports x1, x5, x9, and xd
vSeeds.emplace_back("seed.bitcoin.jonasschnelli.ch");
// Peter Todd, only supports x1, x5, x9, and xd
vSeeds.emplace_back("seed.btc.petertodd.org");
```

Bloom filters i

Bloom filters são usados para filtrar as transações relevantes para clientes *Bitcoin*.

- `fnv`, `murmur` e `Jenkins` são funções *hash* comumente usadas em *bloom filters*.
- Usados em clientes *Bitcoin SPV*.
- *Bitcoin Improvement Proposal 37*, implementada no *Bitcoin* como `BIP37`, introduziu três novos tipos de mensagem: `filterload`, `filteradd` e `filterclear`.

Wallets

Wallets i

- *Non-deterministic wallets*
- *Deterministic wallets*
- *Hierarchical deterministic wallets*
- *Brain wallets*
- *Paper wallets*
- *Hardware wallets*
- *Online wallets*
- *Mobile wallets*

Pagamentos com Bitcoin i

- Bitcoin pode ser aceito como pagamento usando várias técnicas.
- O Bitcoin não é reconhecido como moeda legal em muitas jurisdições, mas está sendo cada vez mais aceito como método de pagamento por muitos comerciantes online e sites de comércio eletrônico.

Indicação de aceitação de pagamentos em Bitcoin.

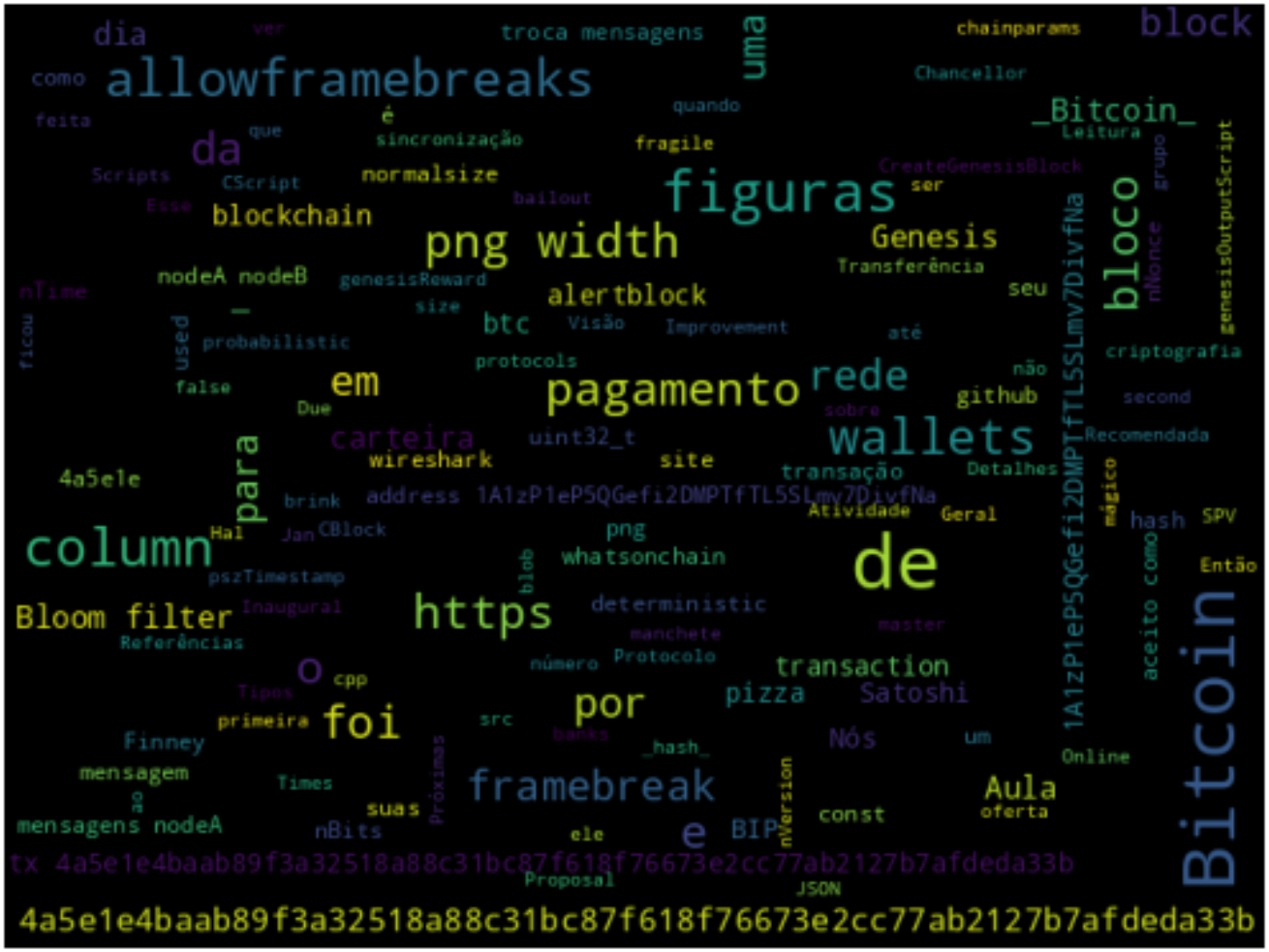
Inovação em Bitcoin i

- Bitcoin Improvement Proposals (BIPs)
  - Standard BIP
  - Process BIP
  - Informational BIP
- Advanced protocols
  - SegWit
  - Bitcoin Cash
  - Bitcoin Unlimited
  - Bitcoin Gold

Atividade

- Instalar o *Bitcoin client* e executar experimentos nele.

Word Cloud


dia
ver
troca mensagens
uma
chainparams
block
como
allowframebreaks
Chancellor
quando
Bitcoin
Leitura
feita
que
é
sincronização
fragile
da
Scripts
CScript
normalsize
CreateGenesisBlock
ser
figuras
grupo
genesisOutputScript
Esse
bailout
blockchain
png width
Genesis
bloco
nTime
nodeA nodeB
genesisReward
Transferência
seu
nNonce
alertblock
size
btc
Visão
Improvement
até
criptografia
ficou
used
probabilistic
protocols
em
pagamento
rede
não
false
Due
github
second
sobre
wallets
Recomendada
carteira
uint32_t
wireshark
site
transação
Detalhes
4a5e1e
para
brink
address 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa
Atividade
Geral
hash
SPV
Hal
Jan
CBlock
png
mágico
column
de
whatsonchain
aceito como
Então
pszTimestamp
blob
Bitcoin
Bloom filter
Inaugural
https
deterministic
Referências
manchete
master
O
cpp
número
Protocolo
transaction
Tipos
por
pizza
Satoshi
primeira
foi
src
banks
hash
Nós
um
Finney
mensagem
Times
framebreak
Online
Aula
ao
suas
próximas
nVersion
const
oferta
mensagens nodeA
nBits
ele
e
BIP
tx 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
Proposal
JSON
4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Leitura Recomendada

Leitura Recomendada

Capítulo 6: Bitcoin Network and Payments

Livro: IMRAN BASHIR. Mastering Blockchain : Distributed Ledger Technology, Decentralization, and Smart Contracts Explained, 2nd Edition.

Próximas Aulas

Próximas Aulas

- Pagamentos com *Bitcoin*.

Referências

Referências i

Imran, Bashir. 2018. *Mastering Blockchain : Distributed Ledger Technology, Decentralization, and Smart Contracts Explained, 2nd Edition.* Packt Publishing. https://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=1789486&lang=pt-br&site=eds-live&scope=site.