

Bitcoin, Blockchain & Pagamentos na Web

Diogo Cortiz



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 cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort 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.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as

սսսսս



Genesis Block - 03/01/2009

սսսսս



uuuuu

ഒ



Naquela época, 10000 bitcoins valiam cerca de **41 dólares,** hoje, 22 de maio de 2016, esse valor chega a mais de **4,5 milhões de** dólares.

սսսսս

- Block Height: 171
- Transaction Count: 2
- Difficulty: 1
- Created at: 2014-12-16T21:40:15Z
- Reward: 50 BTC
- Total Sent: 10 BTC
- Size: 490 bytes
- TX HASH (generation): b1fea52486ce0c62bb442b530a3f0132b826c74e473d1f2c220bfa78111c5082
- TX HASH (sent to Hal): f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16

Dificuldade atual: ~286 milhões

սսսսս

Bitcoin Block Reward Halving Countdown



Reward-Drop ETA date: 02 Jul 2020 01:01:19

The Bitcoin block mining reward halves every 210,000 blocks, the coin reward will decrease from 12 to 6 coins.

սսսսս



COINDESK BITCOIN PRICE INDEX, BTC/\$



Jan 6 and 9, 2014

Zynga and Overstock.com begin accepting bitcoin

Dec 4, 2013

Media attention pushes bitcoin to an all-time high

PBOC does not recognize bitcoin as a currency and bans financial companies from bitcoin transactions; Baidu follows PBOC's lead and halts acceptance of bitcoin

U.S. Senate Committee on Homeland Security and Governmental Affairs holds first congressional hearing on Bitcoin; market perceived a supportive tone from

BTC China, the world's largest bitcoin exchange, announced that it would stop accepting payments in Chinese currency,

uuuuu

involved with the transmission or buying and selling of virtual money must register with the government and comply with anti money-

-Apr 10, 2013:

Mt. Gox exchange down for a day

Jun-13

Jul-1

Aug-13 Sep-13 Oct-13

cemed'ni uic'ni câi'ni

Bitcoin figure for involvement in illicit activities

Nov-13

Dec-13 lan-14

Feb 7-, 2014:

Jan 27, 201

Arrest of a

prominent

Attacks on exchanges lead to a halt on some withdrawals; Mt. Gox. collapses



Home

Welcome to the Worldwide LHC Computing Grid

Last 24 hours

ര



uuuuu

HOW DO BITCOINS WORK?



'Miners' create Bitcoins by using computers to solve mathematical functions. The same process also verifies previous transactions

WORLDWIDE, DECENTRALISED PEER-TO-PEER NETWORK



Bitcoin exchanges will trade between conventional currencies and Bitcoin, offering a way into the market for nonminers, as well as a way to cash out

₿

Users download a Bitcoin 'wallet' that works a little like an email address, providing a way to store and receive currency. Bitcoins can be transferred from one wallet to another using a web browser or a phone app Businesses create a wallet in the same way as an individual user, typically using a website button to enable a Bitcoin payment. For in-thefiesh enterprises, QR codes can be used to let customers pay quickly and easily

սսսսս





Ó

บบบบบบ

How blockchain works

A blockchain is a database shared by every participant in a given system. The blockchain stores the complete transaction history of a cryptocurrency or other record keeping system.



Transactions aren't recognized until they are added to the blockchain. Tampering is immediately evident, and the blockchain is safe as record because everyone has a copy. The source of discrepancies is also immediately obvious.

սսսսս

cewebbr nicbr cgibr

From http://zdnet.com/blog/hinchcliffe on whet by Dion Hinchcliffe

Bitcoin

Status Search for b

Search for block, transaction or addres

Conn 90 Height 4434

躍Scan

Block #443453

BlockHash 00000000000000002a45b850F67482aa503ba060782160d9d2f748eF51c582d 🕅

Summary

Number Of Transactions	2648
Height	443453 (Mainchain)
Block Reward	12.5 BTC
Timestamp	Dec 14, 2016 11:31:47 AM
Mined by	
Merkle Root	ac649f218984e6a25719cae320fb13

b

Difficulty	286765766820.5504
Bits	1803d589
Size (bytes)	998011
Version	536870912
Nonce	4276298796

սսսսս



นบบบับ

How China Took Center Stage in Bitcoin's Civil War

点击查看本文中文版 Read in Chinese

By NATHANIEL POPPER JUNE 29, 2016



սսսսս



սսսմս

പ

везт вlocк #1,414,682	UNCLES (CURRENT / LAST SO)		ьоск S ago	1		AVG BLOCK TIME 13.74S			3	^{ig netw}	iork hashrat H/S	re E	DIFFICULTY 32,16TH		
💂 ACTIVE NODES 48/48	GAS PRICE 20 gwei	🦪 GAS LIMIT		471238	l gas	PAGE L	ATENCY	562 ms 💮 🛛	эртіме			100%			
BLOCK TIME			D N 62	194 194 6 1			MINERS 555:859090a&c34d1641353 802ed039c4d1a5F8216F9DF			•••			S.v.s	1	
		GAS SPENDING	.	l.		GAS LIMIT					7				
							Thi	s page does not repres	ent the e	ntire sta	te of the ethered	um network - listir	ng a node on this pag	e is a voluntary	y process.
© ₽	8	Ð	X	84 ⁸		(\mathbf{i})		₿.		¢	R	۲		۲	Ŷ
) kmas	Geth/v1.4.0-unstable/linux/go1.5.1	42 ms	8.8 MH/s	69		#1,414,682	009ab0156b1e6576	15,988,378,540,477,237,0	00 1		15 s ago	🗉 0 ms		319 ms	100%
CoAKT Miner**	Geth/v1.3.6/Enux/go1.5.1	6 ms	0 KH/s	25		#1,414,682	009ab0156b1e6576	15,988,378,540,477,237,0	00 I		15 s ago	∎ +25 ms		446 ms	100%
O p4fg	Geth/v1.4.0-unstable/linux/go1.5.1	175 ms	120 H/s	225		#1,414,682	009ab0156b1e6576	15,988,378,540,477,237,0	00 1		15 s ago	+48 ms		1000	100%
O BCCHack ()	Geth/v1.3.4-d3f8b763/linux/go1.4.2	3 ms		25		#1,414,682	009ab0156b1e6576	15,988,378,540,477,237,0	10 1		15 s ago	+72 ms		441 ms	100%
C EthereumLottery		58 ms		200		#1,414,682	009ab0156b1e6576	15,988,378,540,477,237,0	00 1		15 s ago	+112 ms		423 ms	100%
O SPARTANS	Geth/v1.4.0-unstable/linux/go1.5.1	94 ms	0 KH/s	25		#1,414,682	009ab0156b1e6576	15,988,378,540,477,237,0	00.1		15 s ago	■ +149 ms		569 ms	100%
O 🕈 lave 🎔 🕕	Geth/v1.4.0-unstable-798e4fb4/linux/go1.4.2	48 ms	17.5 MH/s	561		#1,414,682	009ab0156b1e6576	15,988,378,540,477,237,0	00 1		15 s ago	■ +190 ms	i llin l	10.1 5	100%
O kiik	Geth/v1.3.6/linux/go1.5.1	2 ms				#1,414,682	009ab0156b1e6576	15,988,378,540,477,237,0	00 1		15 s ago	∎ +215 ms	an a	2.0 s	100%
🔿 📷 ubercool-br 📷	Geth/v1.5.0-unstable/linux/go1.5.1														

นนนนั้น

틀





Digital currency Ethereum is cratering because of a \$50 million hack



սսսոս

The value of the digital currency Ethereum has dropped dramatically amid an apparent huge attack targeting an



WEB PAYMENTS AT W3C

Making Payments Easy on the Web



Payment is an essential element of trade and commerce, and "digital interactions are expected to influence 64 cents of every dollar spent in retail stores by the end of 2015. However, behind these impressive numbers, the payment landscape is quickly changing, and new challenges are appearing. For instance, the average shopping cart abandonment rate is 69% across all devices, and even higher on mobile. A variety of factors are limiting the potential of ecommerce, from the high level fraud related to credit card payments, to the fragmentation of payment solutions available on the Web but not available on all merchant sites or on all devices.

At the same time, there is a growing interest from businesses to find alternatives to business models based on advertisement. These alternatives include e.g. in-app payments, or micropayments that are today challenging due to a variety of factors such as heterogeneity and number of payment options to support, or the inability for existing payment systems to cope with very small payments.

սսսմա