Bitcoin, Blockchain & Pagamentos na Web

Diogo Cortiz

ceweb.br nic.br cgi.br

Bitcoin: A Peer-to-Peer Electronic Cash System

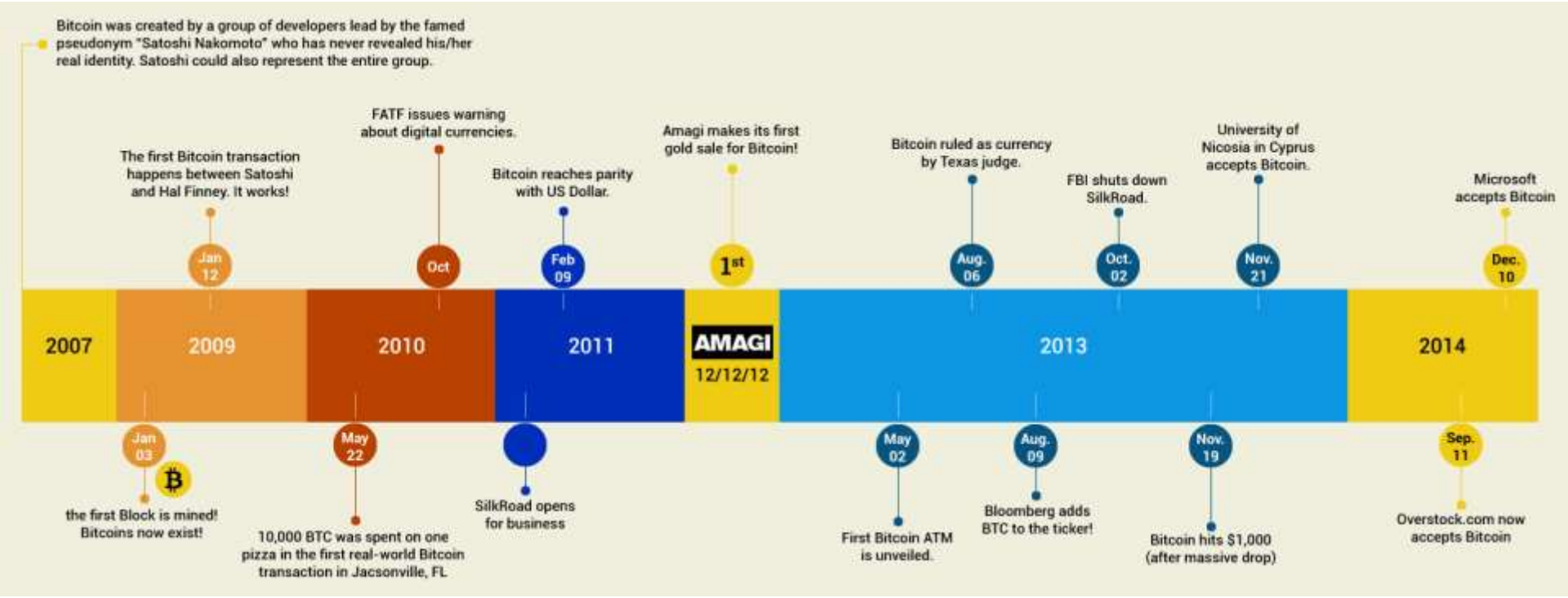
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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

Genesis Block - 03/01/2009



CoinDesk ✓
@coindesk

Follow

Freshly-delivered Papa John's pizza at the CoinDesk office - Happy #BitcoinPizzaDay everyone!

8:31 AM - 22 May 2014

32 23

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**.

- 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

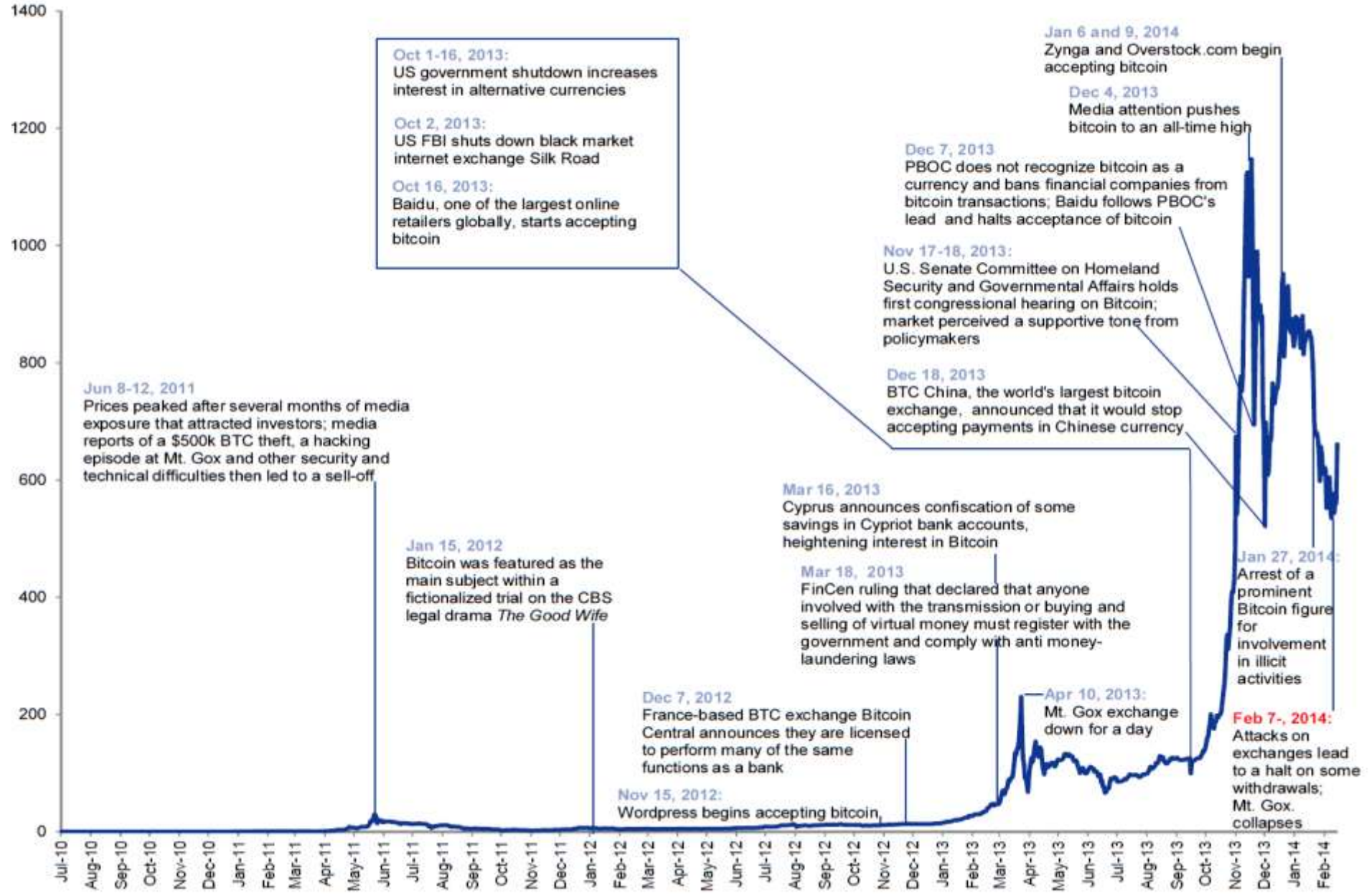
Dificuldade atual: ~286 milhões

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.

COINDESK BITCOIN PRICE INDEX, BTC/$



CERN Accelerating science

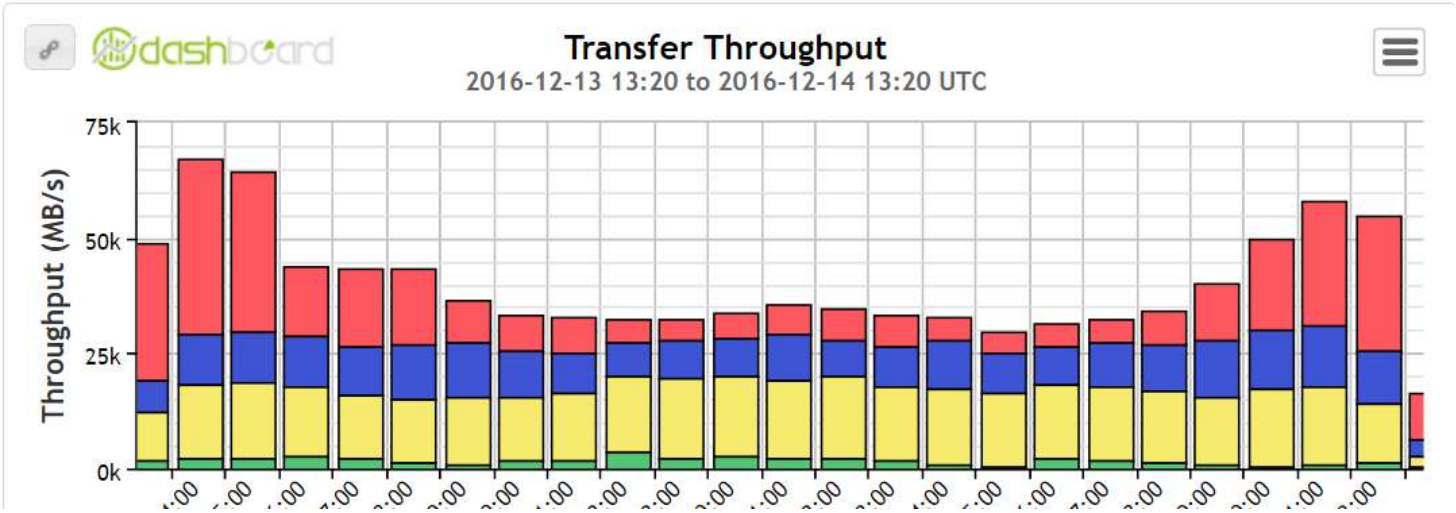
WLCG
Worldwide LHC Computing Grid

Home | Collaboration | Meetings | Grid Operations | Security | Tools | Docs & Ref | Getting Started

Home

Welcome to the Worldwide LHC Computing Grid

Last 24 hours



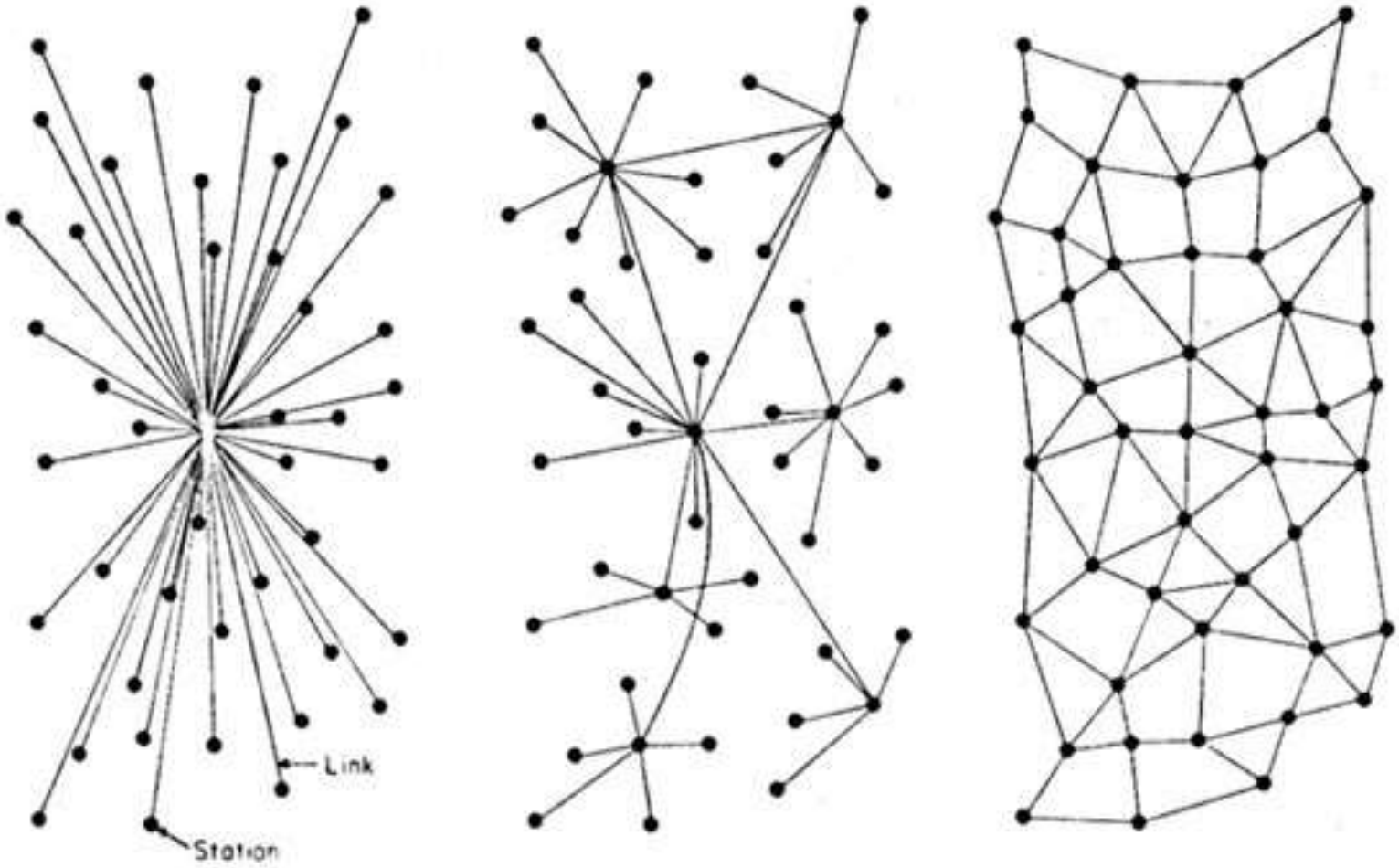
HOW DO BITCOINS WORK?

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

Bitcoin exchanges will trade between conventional currencies and Bitcoin, offering a way into the market for non-miners, 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-the-flesh enterprises, QR codes can be used to let customers pay quickly and easily



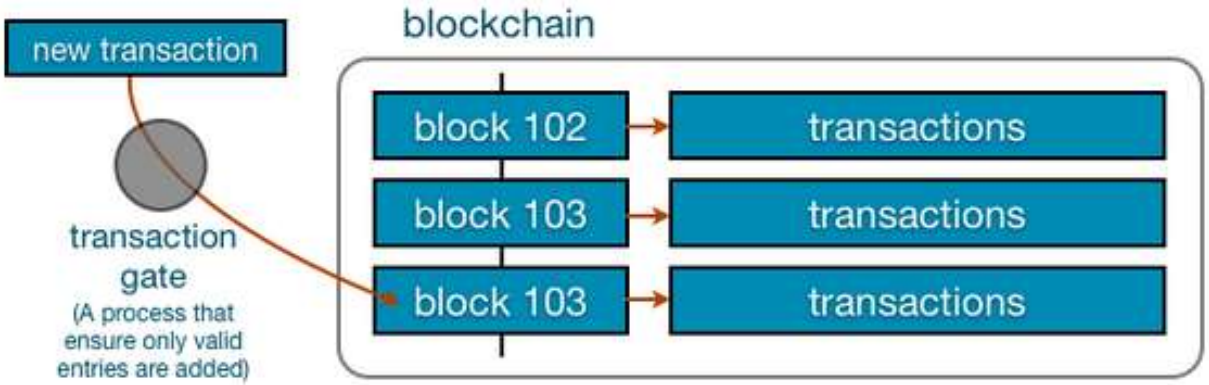
CENTRALIZED
(A)

DECENTRALIZED
(B)

DISTRIBUTED
(C)

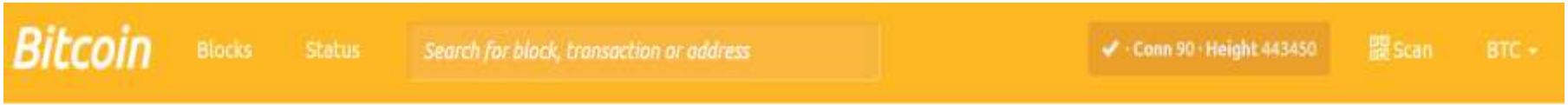
How blockchain works

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.

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



Block #443453

BlockHash 00000000000000002a45b850f67482aa503ba060782160d9d2f748ef51c582d

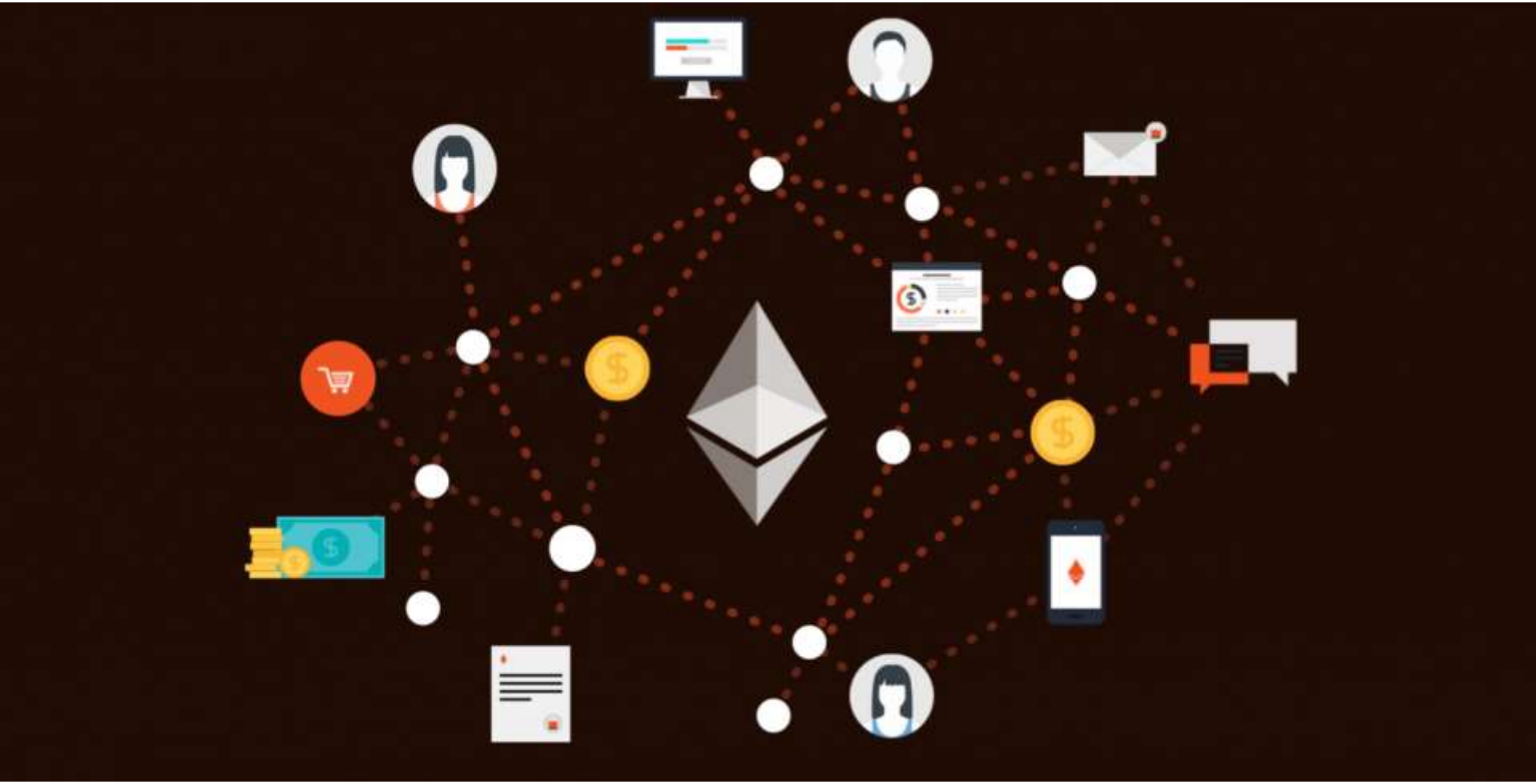
Summary

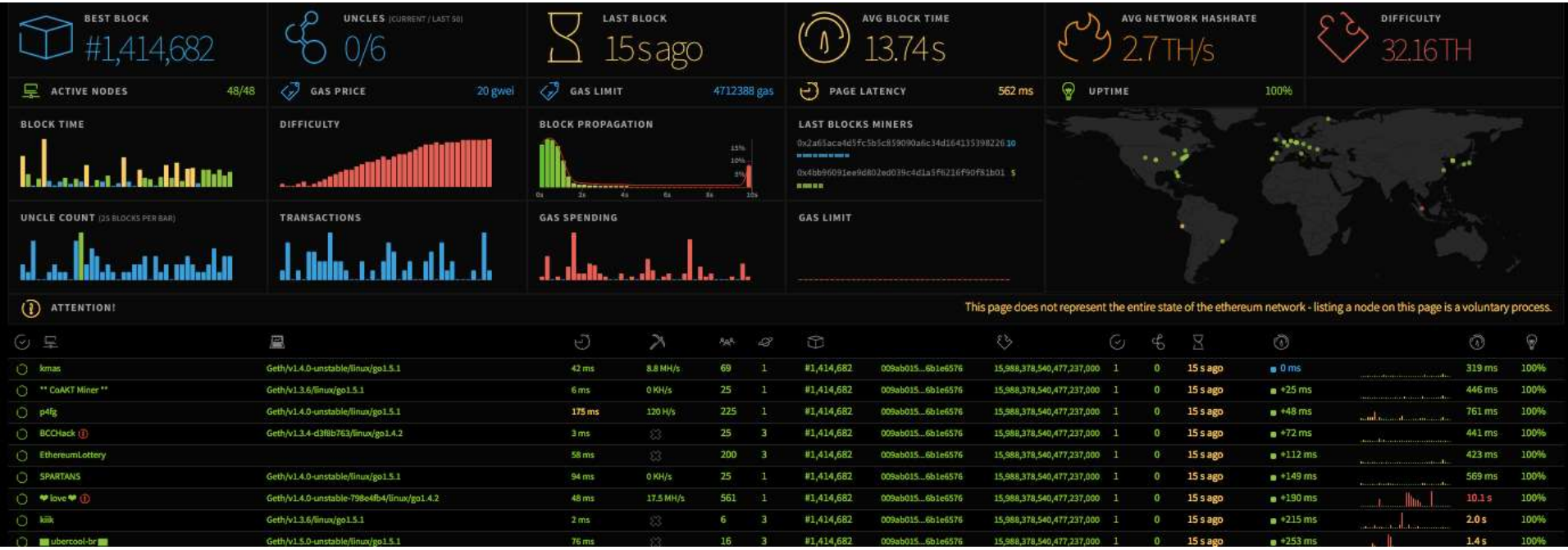
Number Of Transactions	2648	**Difficulty**	286765766820.5504
Height	443453 (Mainchain)	**Bits**	1803d589
Block Reward	12.5 BTC	**Size (bytes)**	998011
Timestamp	Dec 14, 2016 11:31:47 AM	**Version**	536870912
Mined by		**Nonce**	4276298796
Merkle Root	ac649f218984e6a25719cae320fb13...		

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





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

Rob Price

Jun. 17, 2016, 10:34 AM 26,229

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.