Why Bitcoin is not Bitcoin

by
Manuel Lains
Christian Lains

Presentation at FSCONS 2015
7-8 November, Göteborg, Sweden

Satoshi's Vision

- Satoshi Nakamoto (2008): Bitcoin: A Peer-to-Peer Electronic Cash System
- «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»
- «Commerce on the Internet [relies...] on third parties to process electronic payments»
- «What is needed is an electronic payment system based on cryptographic proof instead of trust allowing any two willing parties to transact directly with each other»

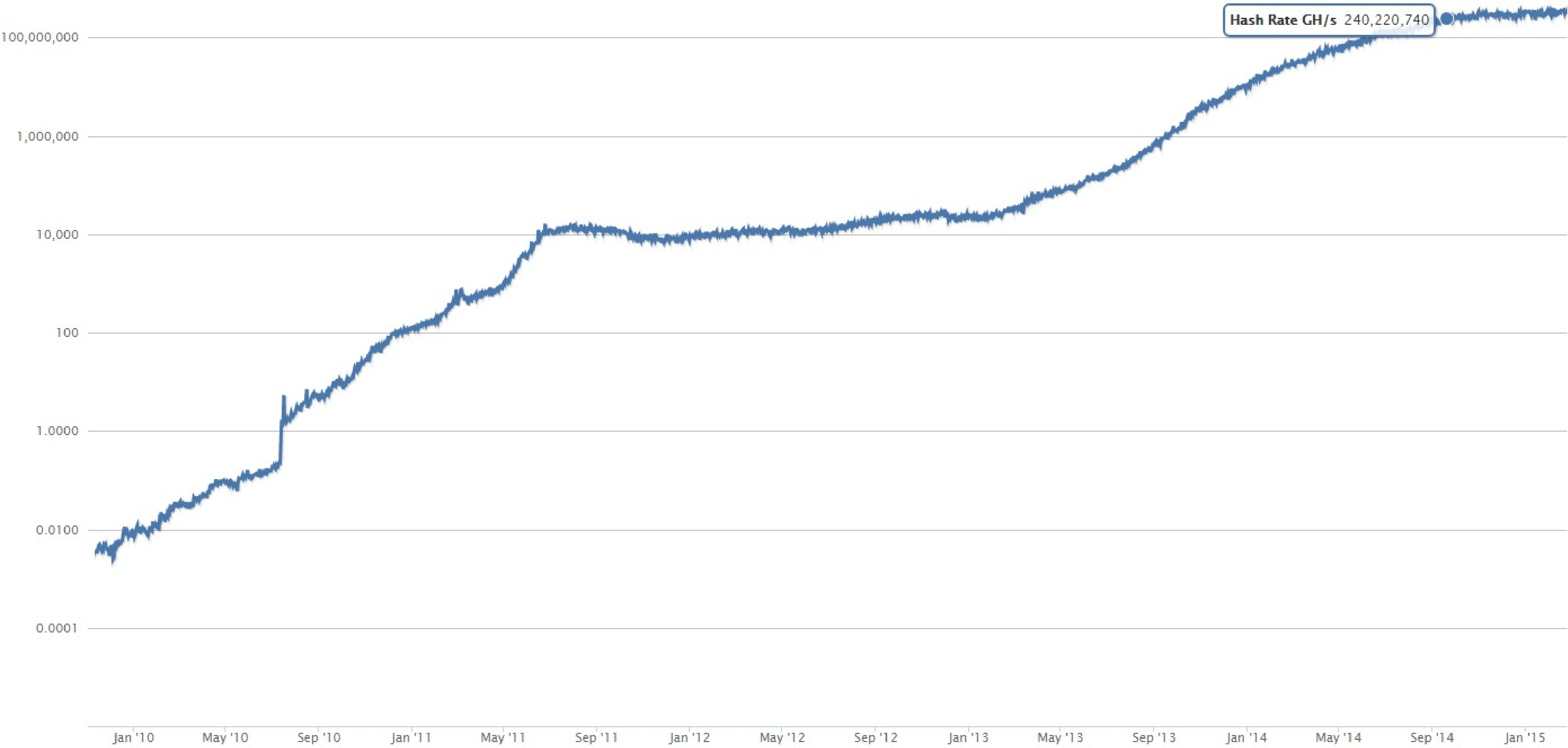
Creator of Bitcoin

Image: BitCrystals

Bitcoin Facts

- Open Source code first released in 2009
- Based on cryptography and P2P technology
- Solution to Decentralized Consensus Problem
- Proof-Of-Work «mining»
- Satoshi's idea: 1 CPU, 1 vote
- Enormous ASIC mining industry
- 2013: 1 exaFLOPS, 8 times faster than top 500 supercomputers. But single-purpose.

Bitcoin Network Hash Rate



The Cryptocurrency Evolution

- Decentralized innovation
- Namecoin (DNS)
- Litecoin ("Silver")
- Peercoin (POS)
- Dogecoin (memecoin)
- 1000s of cryptocurrencies
- Online Coin Generators

very currency wow much coin how money so crypto plz mine v rich
wow

The Cryptocurrency Revolution

- PC (1980s): decentralized computing
- Internet (2000s): decentralized information
- Cryptocurrencies (?): decentralized economy
- Unhindered P2P communication of value
- Liquid, efficient channeling of resources
- Empowering the Individual
- Transparency for big actors
- Privacy for small actors

The Future of Bitcoin

- Various Views
  - Single global currency
  - Global store of value (Gold)
  - Complementary to traditional currencies
  - Has some problems that might be hard to solve
  - Bitcoin is fundamentally flawed and will fail
  - We have to fight Bitcoin

Criticisms of Bitcoin

CAPITALISM IS EVIL.
MICHAEL MOORE
BREEN San Diego Union-Tribune 4-25 © 2009 Creators.com
SAID THE MULTIMILLIONAIRE FILMMAKER

Problems

- Scarcity
  - Early Adopters have too much power
  - Not enough bitcoins for everyone
- Integrity and Security
  - Miner Centralization
- Scalability and future growth
  - Transaction Volume Constraints
  - Block Size Debate
  - Economic Viability

Scarcity

Slices Of The 12 Million Bitcoin Pie

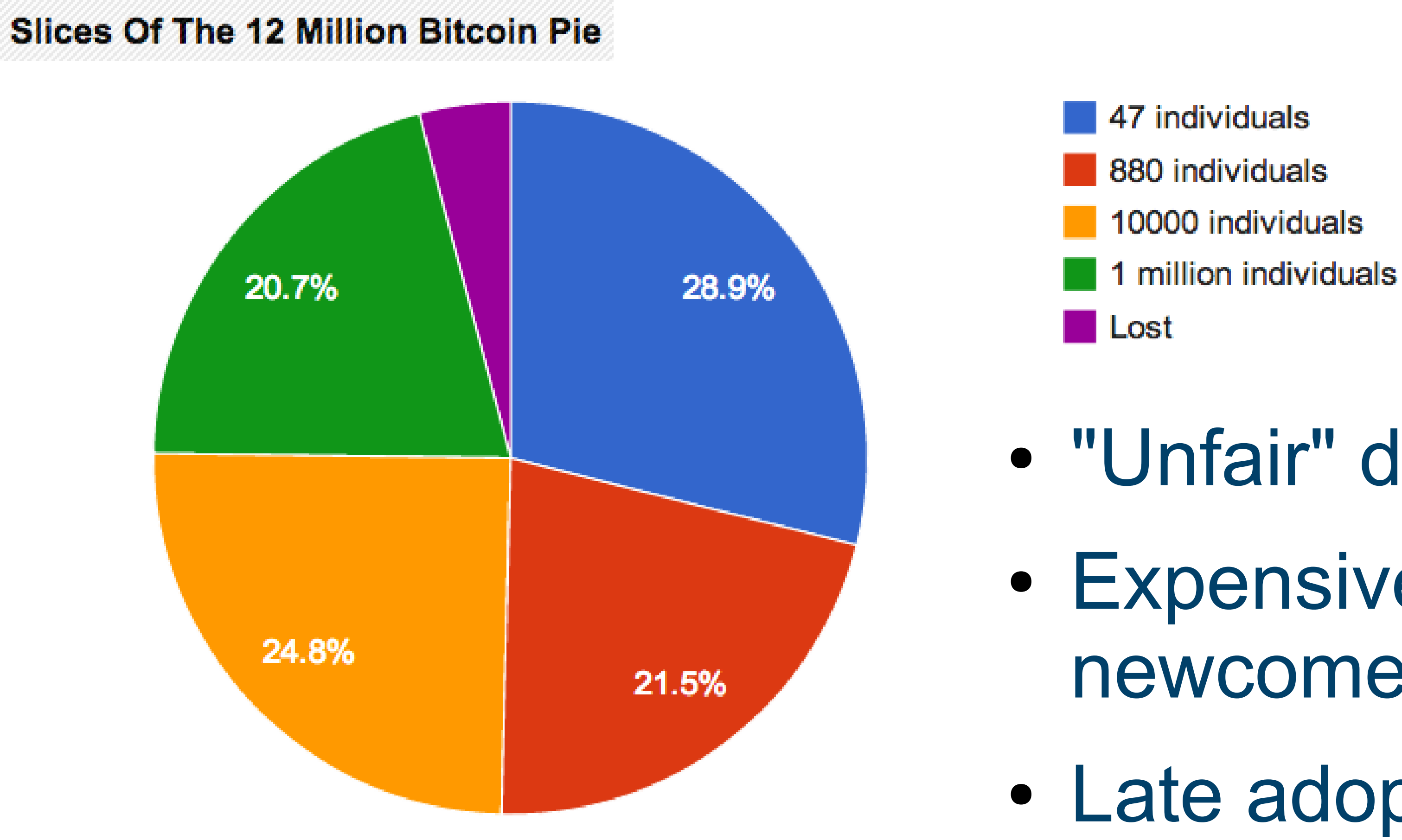


Chart: economonitor.com

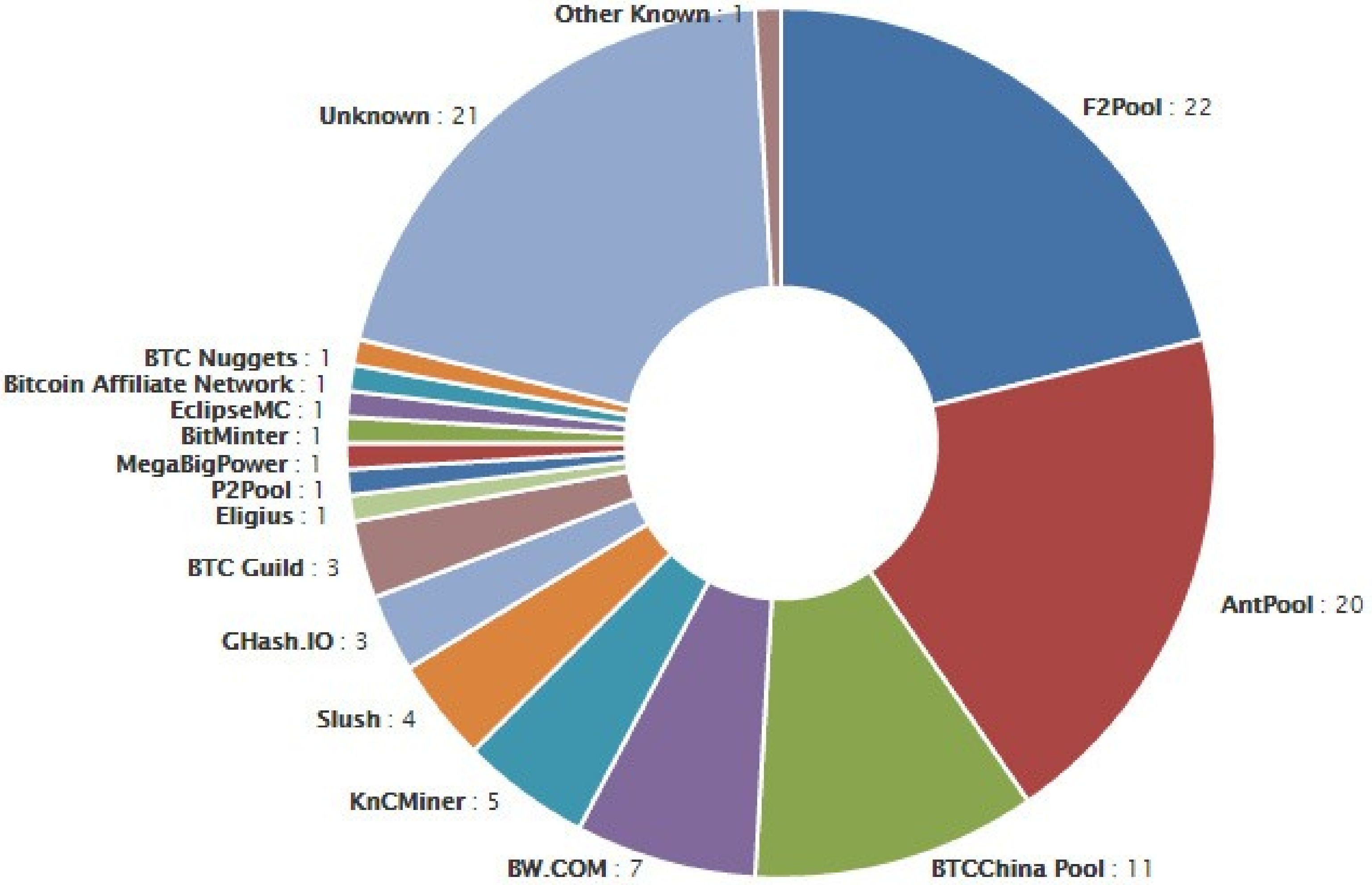
- "Unfair" distribution
- Expensive for newcomers
- Late adopters will be poor

Illusion of Scarcity

- One coin to rule them all
  - Network of currencies
  - Users flow to competitors when Bitcoin is too expensive
- Mining: 3600 BTC / day
  - 1,5 million USD sell pressure
  - Stable supply of bitcoins
  - Damping effect on spikes
  - Gives people time

I put $700 million into Bitcoin, and now I own the system!!!
Mmwahahaha!

Integrity and Security



Bitcoin Mining Distribution (cryptomining-blog.com)

Integrity and Security

- Mining community self-regulates
  - ghash.io
  - P2Pools
- Future ASICS will be dirt cheap
  - Electrical Heating
- Again, Bitcoin is not alone

SOMETHING SMELLS FISHY
AND IT CERTAINLY ISN'T FISH
Free image hosting by www.techpowerup.com

Scalability Concerns

- Bitcoin today: 1MB blocksize
  - Max 3-7 TPS (ensures low hardware requirements)
  - Not enough for global coverage
- Block Size Debate
  - Exposed Bitcoin centralization
  - Gavin Andresen/BIP101
    - 8 MB in 2016
    - Double every 2 years, up to 8 GB
  - BitcoinXT threat worked
- Economic Viability Concerns

Infinite Scalability

- Bitcoin is not only Bitcoin
- Scalability issues create demand
  - Litecoin: Supports 4x transactions
  - BitShares: Claims 100.000 TPS technology
  - Overlapping, but also complementary function
  - Microtransactions
  - Payment channels, Lightning Network
- Economic viability and exponential thinking
  - Value rises faster than block reward decreases

Liquid Economy

- Bitcoin is the Heart of the new Economy
  - Biggest and most important, yet replaceable
- Dynamic market
  - No artificial fences
  - Value flows easy
  - Become your own economic entity
  - Create your own ecosystem
  - True Voluntaryism

Money does grow on trees

Image: Glenn Batten

If banks can create money, why can't we?

Beyond Bitcoin

Beyond Bitcoin

- Three aspects of Bitcoin
  - as Blockchain
  - as Currency
  - as Ecosystem
- Blockchain applications
  - Bitcoin 1.0 (Currency)
  - Bitcoin 2.0 (Crypto Finance)
  - Bitcoin 3.0 (Beyond Finance)

Bitcoin 1.0 Example

- JoyStream
  - BitTorrent Client (P2P)
- Application of Bitcoin
  - Micropayments
  - Machine to machine payment
- Economics of torrenting
  - How to cooridnate supply and demand?
  - Enable users to sell uploads and buy downloads

Crypto-Finance (Bitcoin 2.0)

- Smart Contracts
  - General idea: Programmable money.
  - Agreements between parties posted to the blockchain for automated execution.
  - Analogy: Vending Machine.
- Decentralized Finance
  - Any online transaction of value can now be decentralized in a trustless manner without a controlling authority in the middle.

Crypto-Finance Applications

- Crowdfunding
- Microfinance
- Exchange Financial Instruments
  - Currencies / Tokens
  - Public / Private equities
  - Derivatives / Commodities
- Records of Trading/Spending/Loans

Crypto-Finance Examples

- BitShares
  - Exchange
  - Financial Instruments
- PeerTracks
  - Crowd-funding
  - Artist Shares

BitShares Decentralized Exchange

- The need for a Decentralized Exchange
  - Trade
    - Bitcoin and cryptocurrencies
    - Stocks, derivatives, smartcoins
  - The unbanked
    - Half of the of the world's population
    - More than one in four Americans
    - No access to trading financial instruments

PeerTracks

- Front End
  - Streaming, Download, Merchandize, ArtistCoin
- Back End
  - ArtistCoin/Token
    - BaseBall Card – Token
    - Token-Controlled Access
    - VIP pass
  - Crowd-funding with equity

PeerTracks Benefits

- Benefits from Smartcoins and IOUs
  - Transparent Transactions / Accounting
  - Programmable functions
- Benefits from ArtistCoins
  - Talent discovery
  - The case of Oculus

Beyond Finance (Bitcoin 3.0)

- Blockchain technology is a new and highly effective model of organizing activity in general, not just financial activities.
- The advent of blockchain technology enables decentralized consensus and decision-making on an unprecedented scale.

Bitcoin 3.0 Applications

- Decentralized (blockchain based) applications, communities, organizations and companies that go beyond crypto-finance.
  - Identification: Passport, voter registrations
  - Intangible assets: Patents, trademarks, copyrights.
  - Public records: Property titles, marriage certificates.
  - Attestation: Proof of existence, ownership.
  - Physical asset keys: Home, hotel rooms, rental cars

Examples of Bitcoin 3.0

- Augur / Truthcoin
  - Prediction Market
- Namecoin / DotP2P
  - Decentralized DNS
- Follow My Vote
  - E-Voting Solution

Augur / Truthcoin

- Prediction Market
  - Rewards users for correctly predicting events
- Wisdom of Crowds
  - Incentive to bet if you have information
  - Incentive to find information
- Decentralized
  - Judged by the crowd
  - Regulation and assassination markets

Namecoin / DotP2P

- Accessing a Website
  - Domain Name System (DNS)
    - Internet Corporation for Assigned Names and Numbers (ICANN)
  - Top-Level Domains
    - .com (USA)
    - .cn (China)
- Decentralized DNS
  - Namecoin
  - DotP2P

Follow My Vote

- Problem of E-Voting
  - How to vote remotely, while being able to verify your vote and keeping anonymity?
- Blockchain-based solution
  - Remote voting via internet
  - Get your voting token without revealing identity
  - Vote anonymously
  - Verify that the vote was registered as cast

BitSpace

- BitSpace.no
  - Group Focused on Cryptocurrency Applications
  - Building the Future with Blockchain technology
    - Follow My Vote
- BitGate
  - Gateway to the BitShares Exchange
  - Trade Cryptocurrencies, Equities, IOUs, Assets, Tokens, and SmartCoins