All your Bitcoin are belong to us

Introduction to digital currency

Amichay Peretz Klopshtock
dc9723, 18.12.12

What is bitcoin?

- Decentralized digital CryptoCurrency:
  - P2P currency system
  - Based on public key cryptography
  - Free as in freedom
  - No Central authority

How does it work?

- Alice send Bob Bitcoins
- The transaction is confirmed by miners in the network, and small fee is paid to the miners
- Bob give Alice what she bought
- The miners do the math to cryptographically confirm the legitimacy of the deal, and the first miner to solve the problem gets 25 BTC as a reward

Advantages

- Low fees
- Global
- Easy to use
- No inflation
- Secure
- Anonymous
- Independent
- Free as in freedom

Disadvantages

- Wallets can be lost or stolen
- Not widely accepted
- No physical form
- No valuation guarantee

Weaknesses

- Botnet mining
- Speculants
- Hacking:
  - DDoS
  - Stealing of wallets
  - Hacking into large trading websites

History

- 1.11.2008 - Idea first published by Satoshi Nakamoto on Cryptography Mailing list

- 3.1.2009 - Foundation of the network:
  - Release of the first open-source Bitcoin client
  - Issuance of the first Bitcoins - "The genesis block"

- 2010 - Early trading with Bitcoins:
  - 10K BTC for two pizzas
  - David Forster's alpaca socks

History

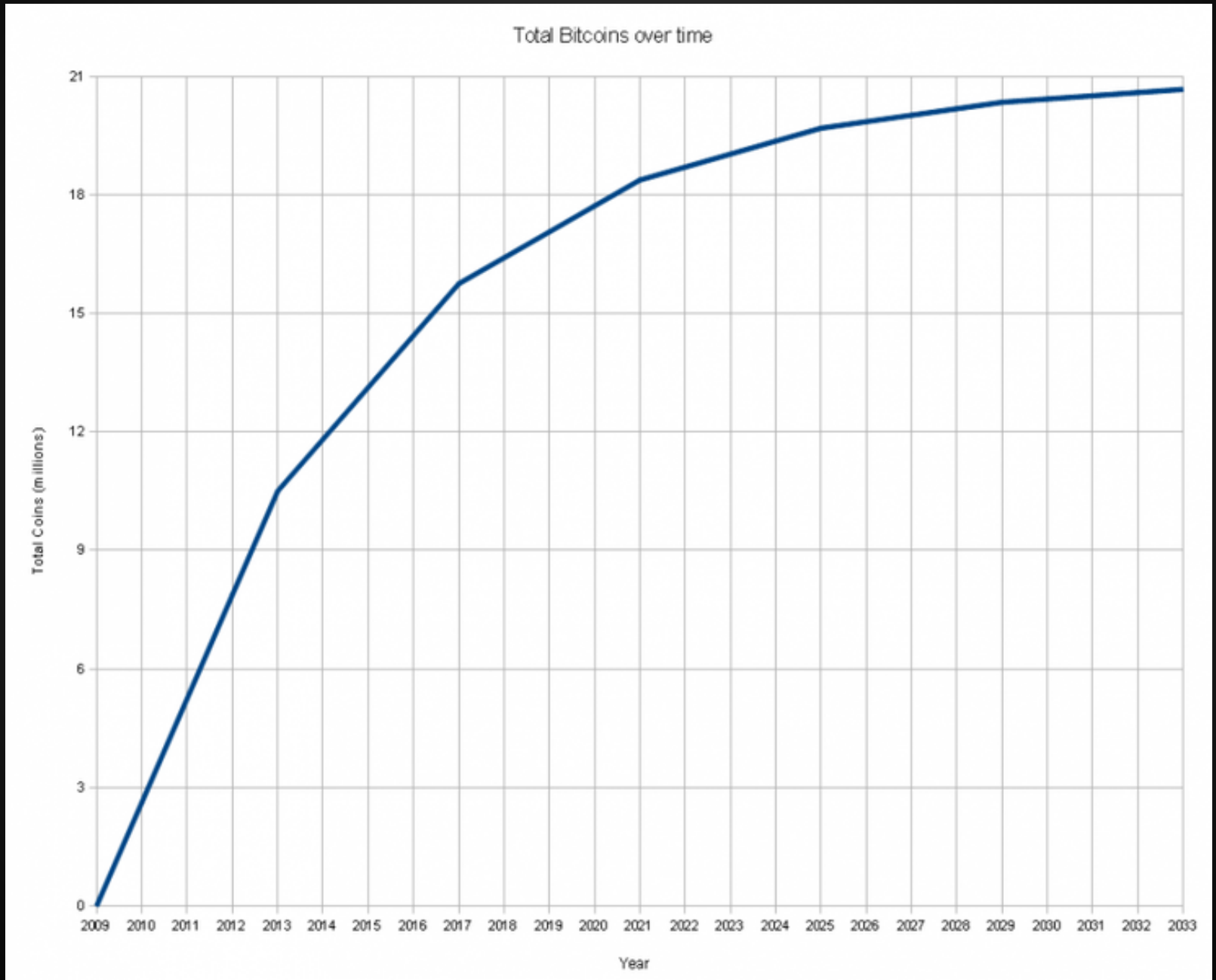
- 15.2.2011 - First car sale for Bitcoins
- 8.6.2011 - Highest value - over 31.9 USD/BTC
- 19.6.2011 - Mt. Gox being hacked
- 28.11.2012 - First halving day
- 6.12.2012 - Bitcoin-Central get licensed as bank in europe

Some data

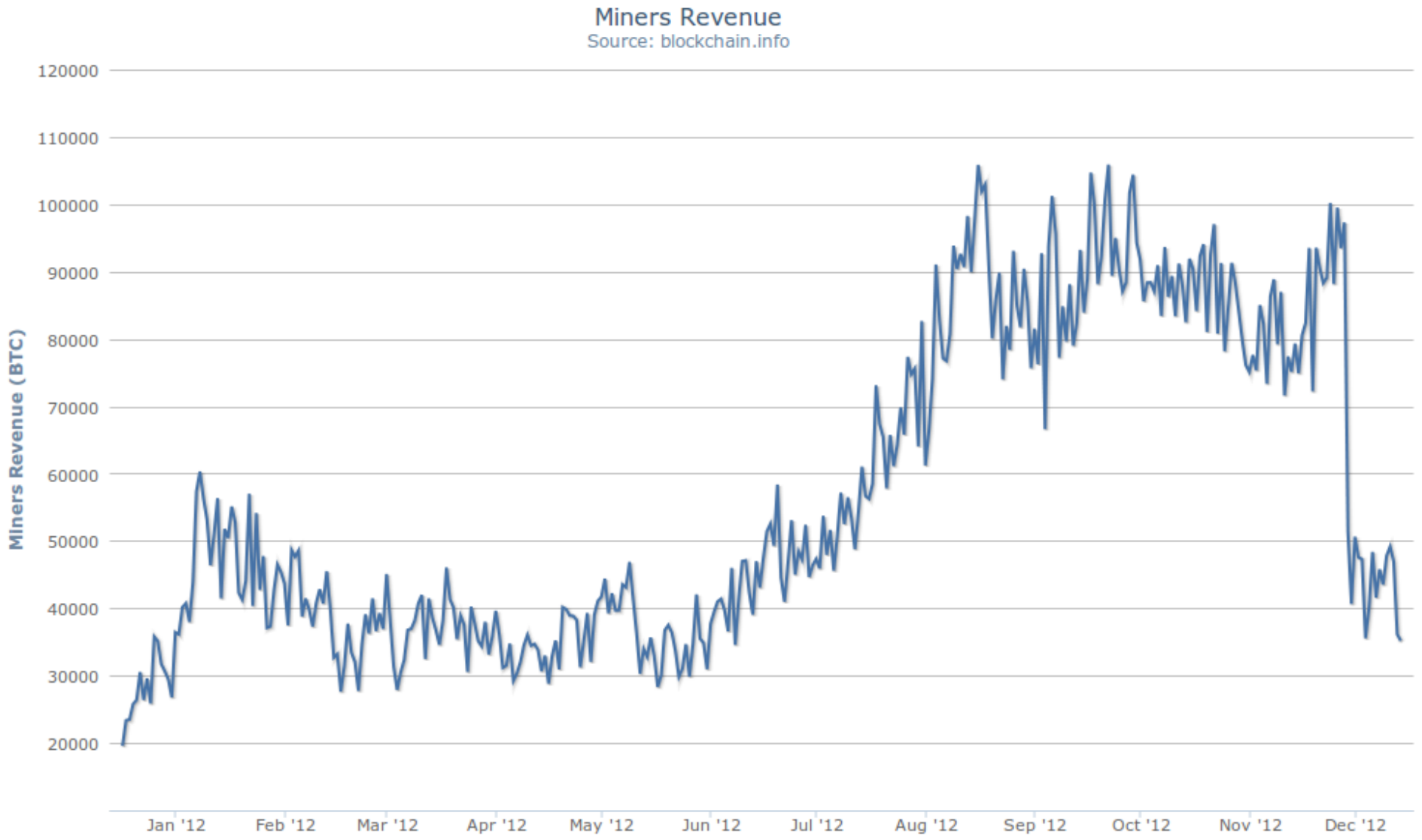
- Total BTC: 10,557,600 BTC
- Market capitalization:
  - 144,850,000 USD
  - 550,285,000 NIS
- BTC value: ~13.5 USD, or ~55 NIS
- Bitcoins send (avg. per hour): 74,602.56 BTC

All data as of 15.12.12, 20:00

Total Bitcoins over time



Miners revenue - One year



BTC value in USD - One year

BTC value in USD - from the beginning

Mining hardware

- CPU's
- GPU
- SuperComputers
- Pool mining
- Botnet mining
- Special mining hardware?

Bitcoin mining is becoming more difficult over time!

Physical Bitcoins

- Include a real usable bitcoin under a hologram
- *"Vires in numeris" == "Strength in numbers"*

Future

- Bitcoin mining will become more difficult:
  - Special mining hardware?
  - Botnet mining?
  - Pool mining?
- Legality issues?
- Centralization?
  - Bitcoin banks?
  - Online wallets?
- Public opinion?
- Number of users?
- Bitcoin value?
- Security?

Questions?

Resources

- Bitcoin: A Peer-to-Peer Electronic Cash System, by Satoshi Nakamoto
  - Hebrew translation by Meni Rosenfeld
- Wikipedia
- The Israeli bitcoin community
- cryptography@metzdowd.com mailing list
- Security now, episode 287: Bitcoin CryptoCurrency
- Charts from blockchain.info

- Bitcoin - כסף דיגיטלי ב-P2P, ד"ר אריק פרידמן, Digital Whisper 24
- עושים היסטוריה, פרק 98: על ההיסטוריה של האינפלציה
- אמצעי תשלום מקובל: המטבע הווירטואלי ביטקוין קיבל רישיון בנק, TheMarker, 9.12.12
- ביטקוין, בקרוב גם בארנק הווירטואלי שלכם?, הארץ, 11.12.12