Introduction to Bitcoin II

The digital currency of the future

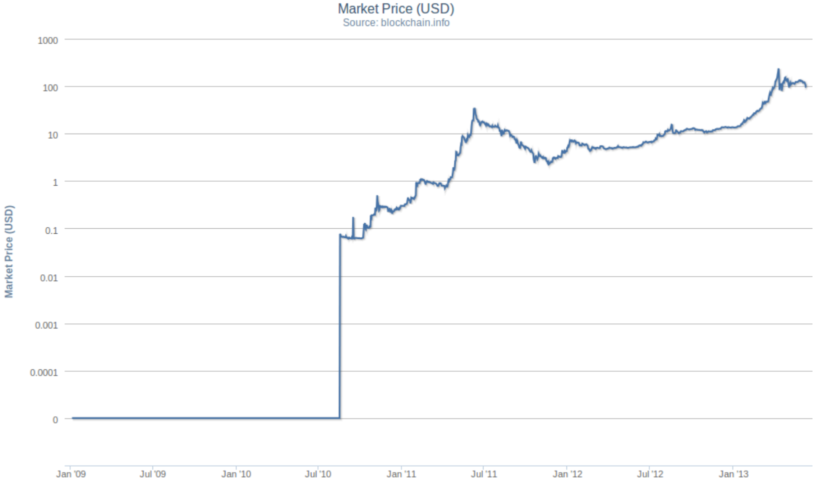
M. Sala[1] A. Tomasi[1] R. Aragona[1]

[1]University of Trento
Department of Mathematics

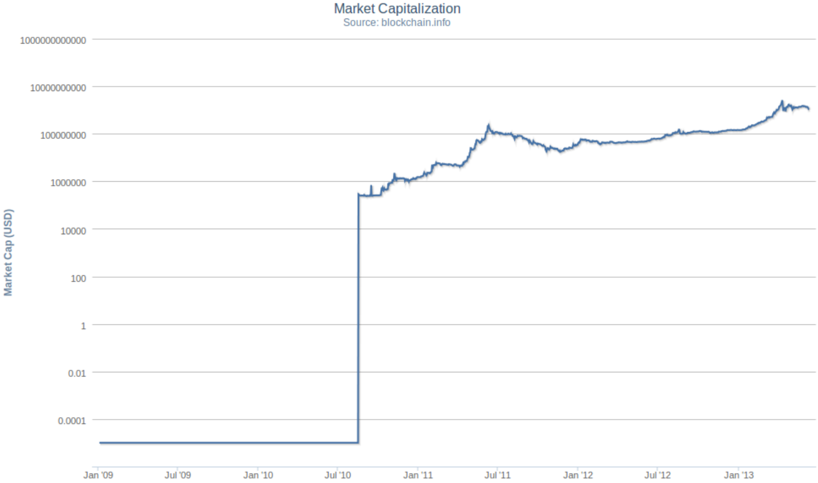
June 10, 2013

UNIVERSITÀ DEGLI STUDI DI TRENTO
Dipartimento di Matematica

Exponential growth: market price

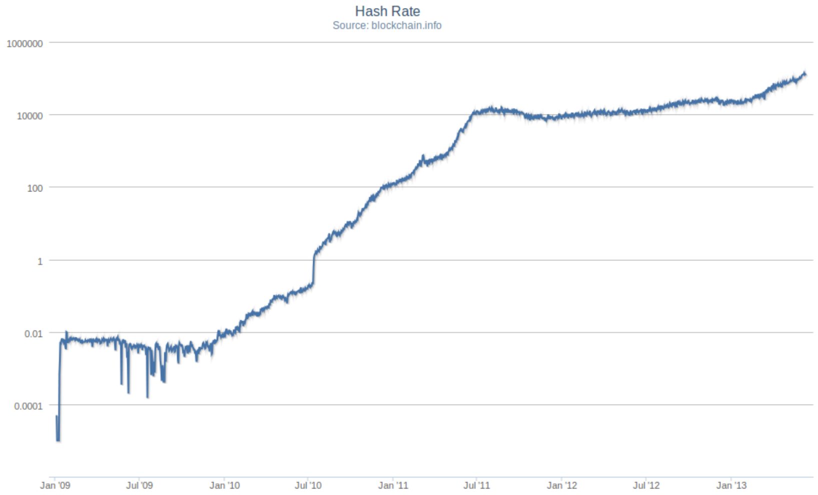


Exponential growth: market capitalisation


Market Capitalization

Source: blockchain.info

Exponential growth**?**: hash rate



e-Wallet

- An e-Wallet is where someone keeps his bitcoins.
- However an e-Wallet does not exist.
- An e-Wallet is actually only the private key of the person who holds bitcoins.

e-Wallet

Anyone obtaining your private key (i.e. your e-Wallet), can spend all your bitcoins.

Private-key storing

Nowadays there are two main methods for storing the private key:

- in a server
- in user's mobile
- (or in both)

Storing in a server

- If you store your private key in a server, for you it is the same as having an online-banking account.
- So also the security is the same: it is necessary to protect user's login, password, etc.
- This includes the use of cryptography to protect the connection between your computer and the server.

Storing in mobile

- If you store your e-Wallet in your smartphone it is only necessary to protect your key.
- For example, it is not necessary to protect the communication between your smartphone and the Bitcoin Network, since all transactions have to be signed by your private key.

Storing in mobile

So to have an e-Wallet on your smartphone, you need only to

- install an e-Wallet APP,
- store the key within the key-chain/key-store.

Storing in mobile

It is fundamental that the kernel is not modified, that is,

- an Android rooting, or
- an iOS jailbreaking

have not been performed.

Authentication

One problem remains: you must authenticate with your APP.

You might use different methods

- No method (who has your phone is you),
- Username and password (or PIN),
- Some biometric features that your smartphone can detect.