15. Cryptocurrencies

15.1 Demands on cryptocurrencies

- Decentralized Network
  - No trusted authority needed
  - Everybody may validate
  - Partial attacks keeps the system flowing
- Anonymous and transparent
  - Each account should be anonymous
  - Every transaction is (in principal) known to everyone
- Small transaction fees
- Non-~~red~~ repudiable
  - No transactions may be cancelled

15.2 Mining

Cryptocurrencies are mined by verification of a part of the blockchain.
⇒ leads to a race for the same block
The first verifier with >50% confirmations wins the race
Other verifications will lead to „orphaned blocks"

15.3 Block of Transactions Managed by eWallets

- Everybody needs to have at least a cryptocurrency address
- Usually, user register via an eWallet
- There are many different providers for many different operating systems.

Tasks of the e Wallets:

- Issuing of the cryptocurrency addresses
- Administration of cryptocurrency accounts
- Management of cryptocurrency buying and selling transactions
- Connecting the cryptocurrency address to some credit card or bank account
- Authenticating the wallet owners by providing a signature of the transaction (by wallet owner)
- Publishing the block of transactions including all transaction of that user

Remarks:

- Some companies are accepting cryptocurrencies
- For transactions the cryptocurrency address (and the e Wallet) of the receiver needs to be known
- If it is handled like that, anonymity is violated
- Blocks are in principal issued to everybody in the cryptocurrency network, e.g., BitCoin.

  Merkle trees are used to introduce some hierarchy:
  - partial knowledge is sufficient (for verification)
  - avoids costly storage of the blockchain.

15.4 Blockchain

No security against fraud as double or invalid transactions in a block. Trust will be given by verification and confirmation by > 50% of the network. To corrupt the system more than 50% of the network corrupted. This is infeasible. To outpower cryptocurrency in 2017 you need to be able to calculate more than

- 3.500.000 TH/s (Bitcoin)
- 12.5 TH/s (Ethereum)

TH/s ≙ Tera hashes per second

The verification process should not be too easy. Hence,

- a difficulty target
- a nonce

are introduced.

The difficulty target might say how many leading zeros the hash value of the block shall. This aim may be reached by finding a suitable nonce

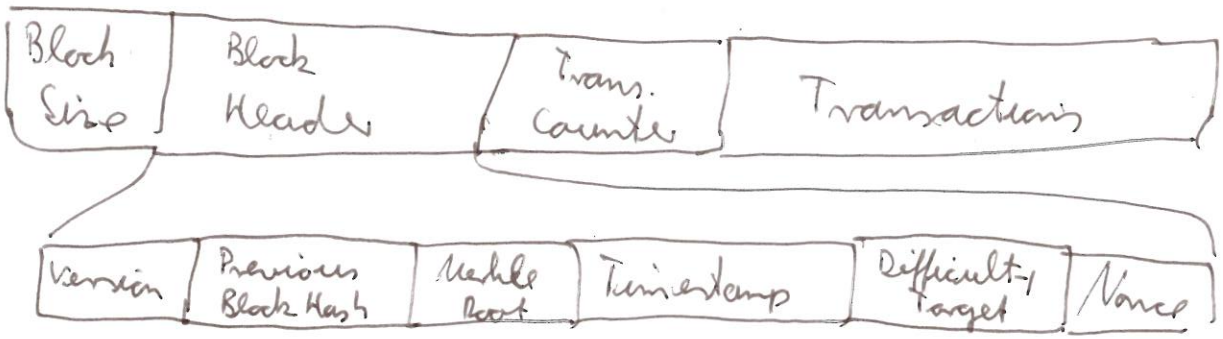
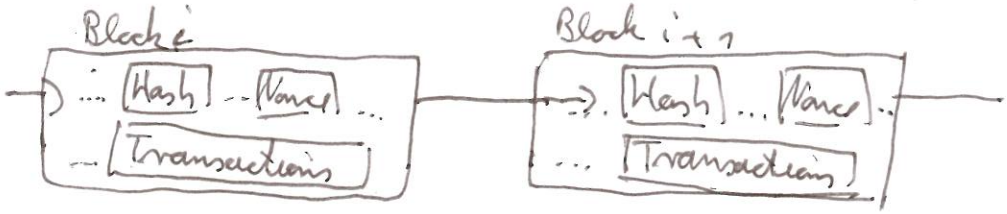


Fig. BitCoin Block Structure



The verification should include the following:

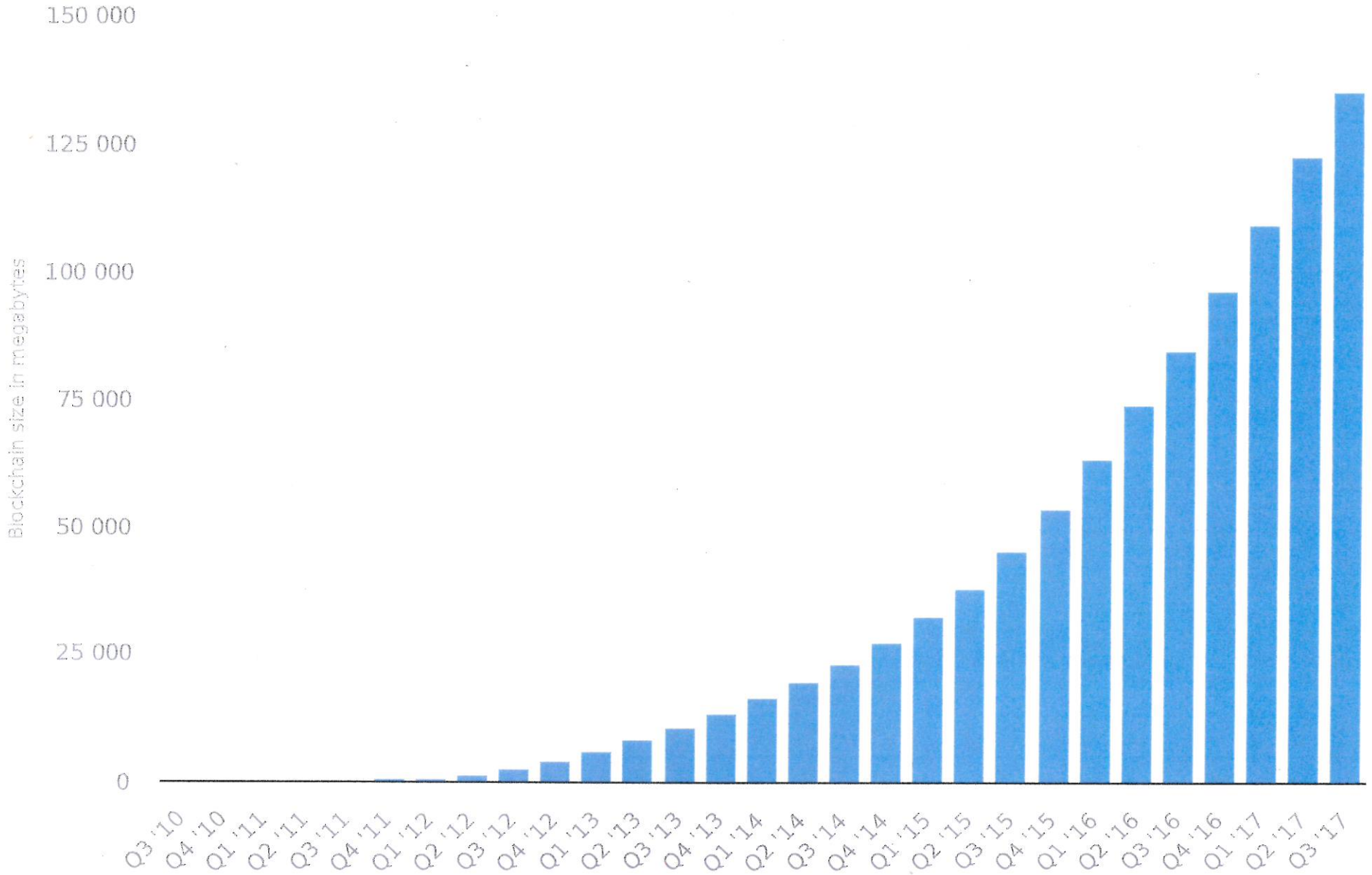
- Checking the integrity of all transactions of the block
- Checking authenticity
- Taking the current blockchain, particularly the hash of the last block
- Finding a nonce fulfilling the difficulty target
- Extending the chosen blockchain by the newly verified block

Confirmation is given by using this blockchain for another verification.

15.5 Remarks

- Paying sth immediately with cryptocurrency is problematic as verification may takes some time, approx. 10 minutes in 2017 for BitCoin. However, new concept as smart contracts are introduced
- The value of cryptocurrency is highly volatile, as on a stock market, but more volatile.
- It is important to keep the rewards of mining in relation to the (financial) effort by changing the reward and/or the difficulty of verification. Otherwise it will suffer from inflation.

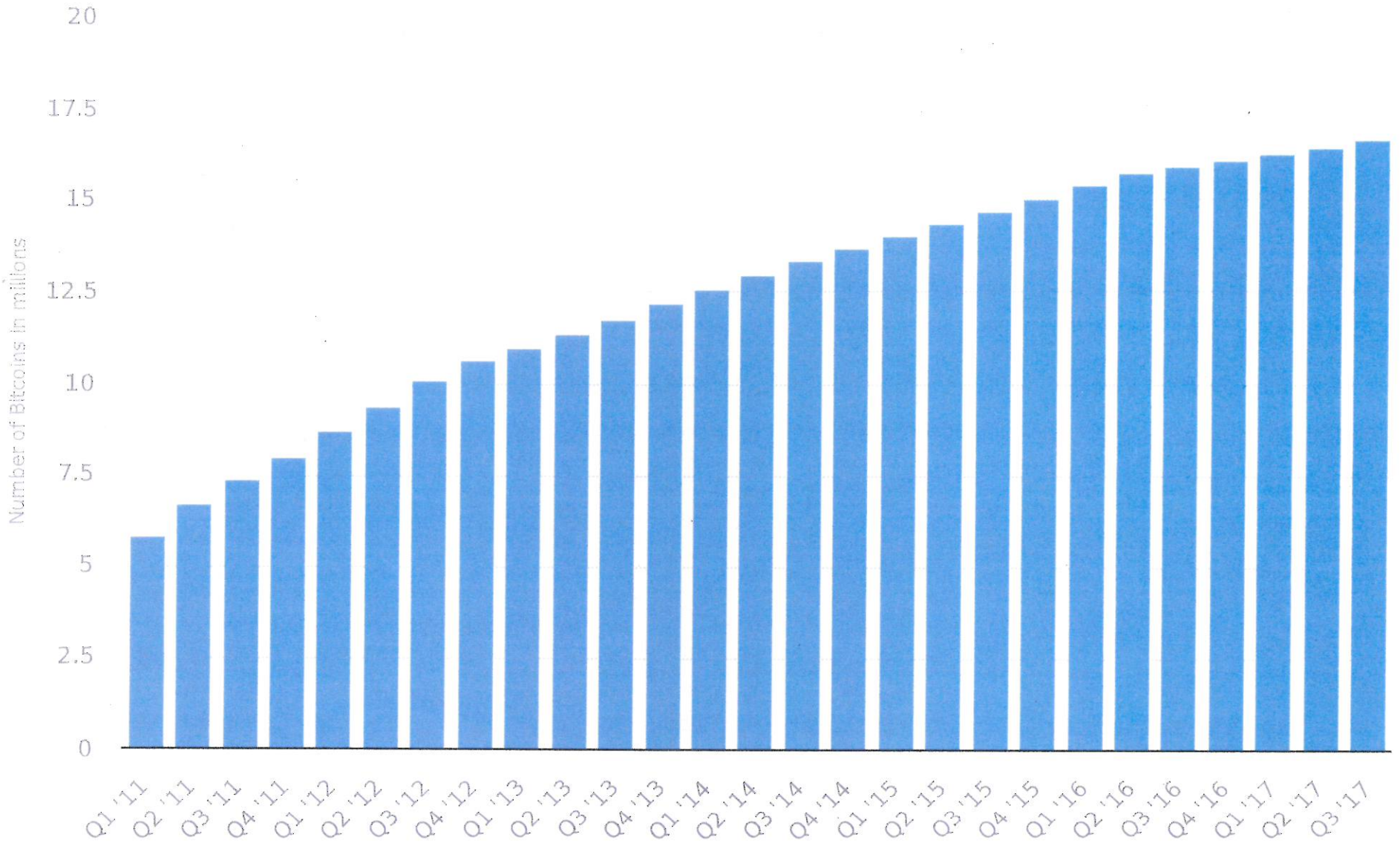
Size of the Bitcoin blockchain from 2010 to 2017, by quarter (in megabytes)



Source
Blockchain

Additional Information:
Worldwide; Blockchain; 2010 to 2017

Number of Bitcoins in circulation worldwide from 1st quarter 2011 to 3rd quarter 2017 (in millions)



Source
Blockchain

Additional Information:
Worldwide; Blockchain; Q1 2011 to Q3 2017