15. Cryptocurrencies

15.1 Demand on cryptocurrencies

- Decentralized Network
  - No trusted authority needed
  - Everybody may validate
  - Partial attack keeps the system flowing

- Transparency and Traceability
  - Each account should be anonymous
  - Every transaction is (in principal) known to everyone

- Small Transaction Fees
  - Non-refundable
  - No transactions may be cancelled

15.2 Mining

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

15.3 Blocks of Transactions Managed by E-Wallets

- Everybody needs to have at least a cryptocurrency address
- Usually, user requires via an E-Wallet
- There are many different providers for many different operating systems
Tasks of the e-Wallets:

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

Barnaby:

- 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 blockchain will be given by verifications and confirmed by >50% of the network. To corrupt the network more than >50% of the network corrupted, this is infeasible. To outpower crypto currency in 2017 you need to be able to calculate more than:

- 3,500,000 TH/s (Bitcoin)
- 12.5 TH/s (Gethcoin)

TH/s = Terahashes 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 should. This aim may be achieved by finding a suitable nonce.

![Diagram of Bitcoin Block Structure]

![Diagram of Two Blocks]
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 the blockchain for another verification.

15.5 Remarks

- Paying with immediately with cryptocurrency is problematic as verification may take some time (approx. 10 minutes in 2013 for Bitcoin). However, new concepts 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
© Statista 2017

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
© Statista 2017

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