Lehrstuhl Netzarchitekturen und Netzdienste
Institut für Informatik
TU München

Electronic Cash, BitCoin

Dr. Heiko Niedermayer

Electronic Cash / Payment Systems

- Desire
  - Directly exchange money between peers without exchanging coins, banknotes, or doing traditional bank transfers

- Basic idea
  - User can transfer real-world money into a virtual representation
  - € ←→ virtual €
    - Can either be based on discrete coins or accounts with a balance

- Money Creation
  - Banks exchange real-world money into electronic money and vice versa

Money Exchange

- Money exchange
  - Double-Spending
    - Basic problem of all electronic cash: how to prevent that a peer spends the same coin twice?
  - Online: Peer1 → Bank → Peer2
    - Bank envolved to check that coin was not already spent by Peer1
    - Usually enhanced with some anonymization
      - E.g. Blinding in DigiCash (Blind Signatures), ~1990s
  - Online: Peer1 → Bank1 → Bank2 → Peer2
    - Transfer money between accounts at the banks, here money not on user computer
  - Offline: Peer1 → Peer2
    - No bank envolved in transfer, via local or global connectivity
      - E.g. FairCASH
    - Usually secured with trusted hardware (smartcard, TPM), hardware protects against user, unencrypted coins never leave the secure environment

Virtual Currencies

Virtual Currency vs Electronic Cash

- Instead of virtual representations of real-world money, e.g. € or US-$, generate a new currency.
- Coins are then not in €, but in abstract units of the virtual currency
  - Exchange between € and virtual currency not directly part of the system
  - Service to exchange may exist and operate with changing exchange rates

  → Value of a coin not constant!

Virtual Currency Concepts

- b-money
- BitCoin

b-money

- b-money (W. Dai, "b-money,“ http://www.weidai.com/bmoney.txt, 1998)
  - Basis for BitCoin concept
- Assumption
  - Unjammable (anonymous) broadcast channel
  - Each user has Public / Private Key Pair
  - No join / leave
- Money / Account
  - Each user (= Public Key) has an account, the balance is managed by all nodes in the network

b-money

- Money Creation
  - Dig for your money! Network provides a list of hard computational problems.
  - Solving a yet unsolved problem, makes you create new money. The reward may vary depending of the difficulty of the problem.
  - Broadcast to network:
    „Me, A, solved the problem…. . Here is solution:….“ signed withK_A
  - All nodes verify the statement and if the problem was yet unsolved, then add a certain amount of units of money to A‘s account

- Money Exchange
  - A broadcasts to network: „Me, A, transfers x units of money to B. “ signed with K_A
  - All nodes will update the accounts of A and B if A has more than x units of money in his account.

BitCoin

BitCoin

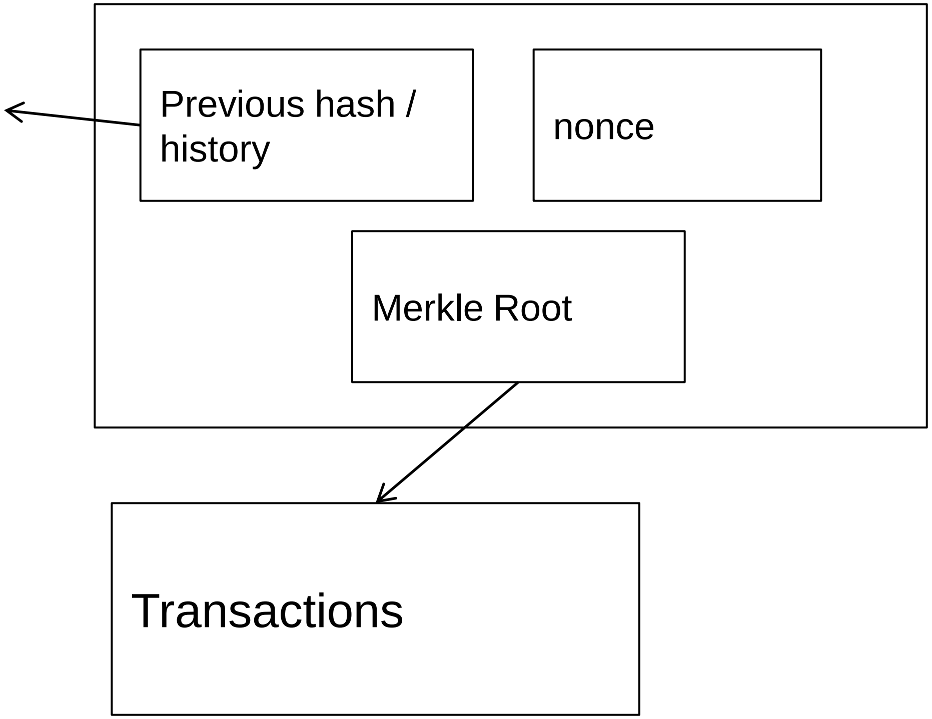
- Adaption of b-money idea
- Broadcasts realized via IRC

Money Creation

- Coins and transactions are managed in a large data structure.
  - Like a transaction log file.
- To generate new coins, a participant needs to find a hash inversion based on current state
  - Transactions are thus ACKed by new coins added on the basis of this state.
  - Transaction costs can be set. Sum of transaction costs of new transactions is additional reward.

BitCoin – Block / Hash Solution / Merkle Root

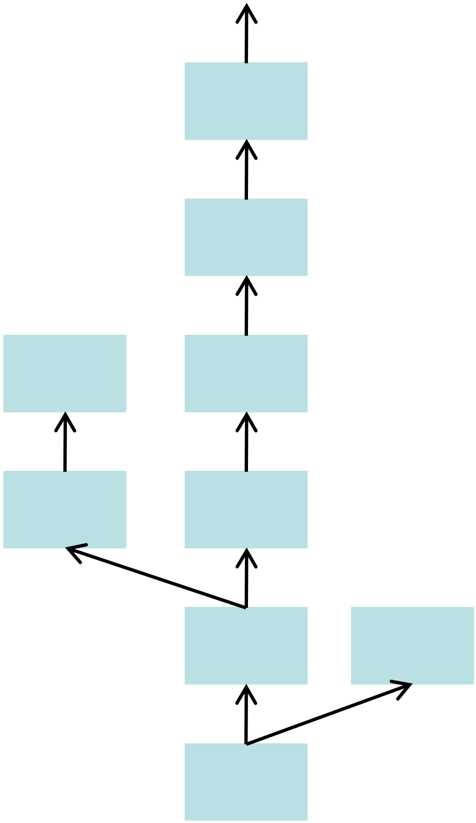
- A block is a large history data structure and one block is signed per approx. 10 min (when a hash inversion was found)
  - This signature then finalizes a block and its transactions.



Goal: find nonce so that hash has k leading zeros.
k is parameter to change over time.

BitCoin chain

- In the long run, the idea is that there is one chain.
- However, parallel reports of a new solution compete for some time.
  - The longer chain wins.



Deflation / Attacks

- Coins limited to 21 million
  - Converges to 21 million due to reduced reward, in the end transaction signatures should be rewarded by transaction cost chosen freely by the entity doing the transaction
- New coins are harder to compute, reward reduced → deflation (coins increase in value over time)
  - Unlike most currencies today where inflation is common (value of a monetary unit is reduced over time)
- Real value of coins depends on system popularity and security

- Attacks
  - Account password at exchange point hacked
  - Coins stolen from computer
  - Stock exchange-like exchange between US-$ and BitCoin misused
  - …

Helpful Links

- Satoshi Nakamoto: “Bitcoin: A Peer-to-Peer Electronic Cash System” www.**bitcoin**.org/**bitcoin.pdf**
- W. Dai, "b-money,“ http://www.weidai.com/bmoney.txt

- In German:
  - CCC Chaos Radio Express on BitCoin (30.06.2011)
    http://chaosradio.ccc.de/cr169.html
    (easy-to-understand introduction in a 2h podcast, not purely scientific)