Social Payment: Flattr and Bitcoin

Tim Krämer

Universität Hamburg
Fachbereich Informatik
KunterBuntesSeminar

05. Juli 2011

general


Tim Krämer (7kraemer@inf...)


the talk will be filmed and (hopefully) published at (lecture2go).


please aks your questions directly!


download slides and sources here: (mafiasi.de/KBS).


This sheets are licensed under a CC-BY-SA 3.0

outline

reminder: what is money?

Micropayment

Bitcoins

Debate - Bitcoin: opportunities / risks

reminder: what is money?

- past: paper notes are convertible into pre-set, fixed quantities of gold (Gold standard).
- today: Fiat money (*lat.* ***fiat*** "let it be done")

Where's the need of Flattr and such?

- minimum stake: costs for processing the payments often exceed the actual value of a payment
- internet-donations, crowd-funding, ...
- paid-content: music, news, games, ...

how Flattr works:

- Flattr-Button: ”flattr” anything with just one click
- Flattr-Account: receive / send money
- monthly amount: money to spend, set individually by user
- $\frac{\text{amount}}{\text{clicks}}$ = money per click on flattr-button

try it now =)


Flattr
KunterBuntesSeminar - eMoney: Bitcoin und Flattr
By TieKei
What is this?
Flattr is a social micropayment service enabling you to support things you like with an easy click, join at flattr.com
To flattr this use one of the apps at flattr.com/offline or go to:
flattr.com/t/336536

there are more...

- Kachingle (USA)
- Paypal donate-button
- Bitcoin
- probably more...

What are Bitcoins?

- What is a bank?

What are Bitcoins?

- What is a bank?
- electronic *currency* (currency of the Bitcoin system)
- just a number associated with a Bitcoin Address
- a distributed bank, kind of
- traceable
- chain of transactions

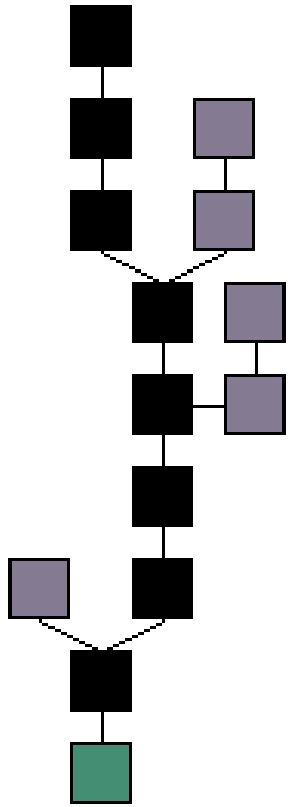
What is a transaction?

1. Bob sends his public key to Alice.
2. Alice adds Bob's public key along with the amount she wants to transfer, to the transaction.
3. Alice signs the transaction with her secret private key.

- $\rightarrow$ preventing stealing!
- similar to PGP

What about double-spending?

- Alice cannot replicate the coin and use it in more than one transaction:
- transaction forwarded to all other clients.
- record of all transactions saved in a growing chain of blocks.
- To be accepted in the chain, transaction blocks must be valid.
- when multiple valid continuations to this chain appear, only the longest is accepted.
- making a block is (mathematically) hard



Anonymity

- Each balance is associated with a public-private key pair
- the money "belongs" to whoever has the private key and can sign transactions with it
- A Bitcoin adress corresponds to a public key:
  - e.g.: 15VjRaDX9zpbA8LVnbrCAFzrVzN7ixHNsC
- you can have many of these adresses
  - each with its own balance

creation of coins - ”mining”

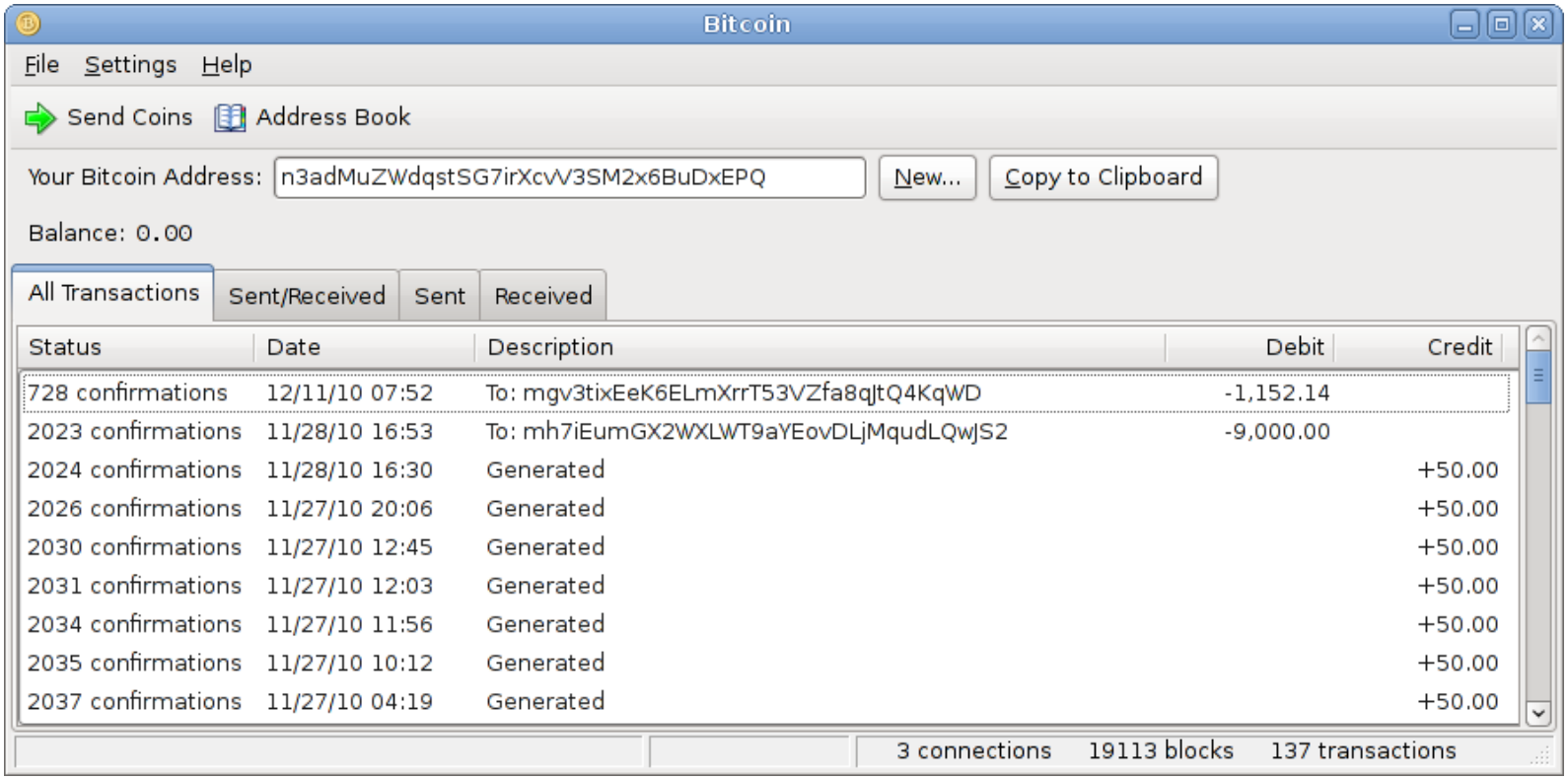
- a transaction is valid if it is included in the block-chain
- making a block is (mathematically) hard
- every computer that generates a block gains 50 BTC as a incentive for the calculation
  - the reward will be reduced to half every 4 years
- another way to get a reward: transaction fees
  - chosen, and paid, by the person who sends the money
- $\rightarrow$ minimum transaction fee required for transactions

technical details

- distributed network
- nodes connected via TCP/IP
- broadcast transactions
- distributed database (P2P)
- nodes join/leave at any time
- request any info that they miss

using bitcoin

- Bitcoin client = wallet = network node



- or online wallet at `mybitcoin.com`

merchants / services

buy stuff for BTC

- server hosting
- books
- music
- coffee
- clothing
- ...

questions?

see also: www.bitcoin.org

Debate - Bitcoin: opportunities / risks

- regulation
- acceptance
- deflation?
- bugs, hacks, attacks
- ...

Thanks!

Thank you for your interest! =)