# Marker addresses: Adding identification information to Bitcoin transactions to leverage existing trust relationships

Jan Vornberger

Bitcoin Workshop & Tutorial
Braunschweig, September 20, 2012

# Agenda

1. Motivation
   - Goal: Fast transactions
   - Double Spending
   - Approaches
2. Marker addresses
   - Out-of-band vs. in-band
   - Mechanism
   - Advantages & disadvantages
3. Implementation
   - Green addresses
   - Patches for Bitcoin daemon
4. Conclusion

# Goal: Fast transactions

### Goal

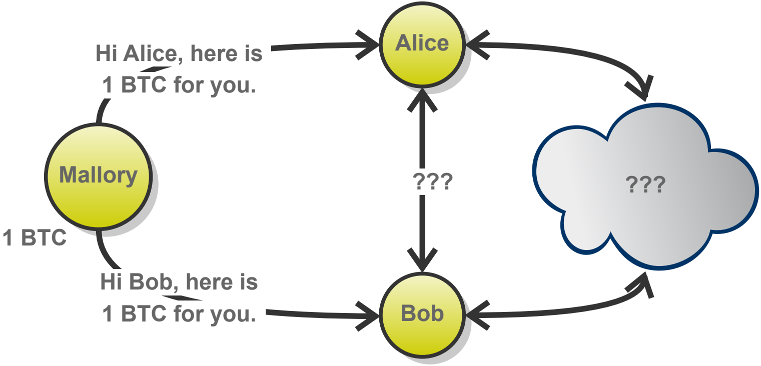
Fast transactions for time-critical applications.

### Challenge

The nature of the Bitcoin system makes it necessary to wait for a number of confirmations to be sure that a transaction has made it into the block chain.

If someone accepts a transaction with few or no confirmations, they risk becoming a victim of a double spend.

# Double Spending


Hi Alice, here is 1 BTC for you.
Alice
Mallory
???
???
1 BTC
Hi Bob, here is 1 BTC for you.
Bob

# Approach 1

## Approach 1

Do nothing and simply rely on zero confirmation transactions.

Problematic, as it opens up the possibility for fairly simple double spend attacks.

# Approach 2

## Approach 2

Closely monitor the Bitcoin network and use heuristics to quickly make a risk assessment.

A good deal safer, but still vulnerable to attacks involving colluding miners.

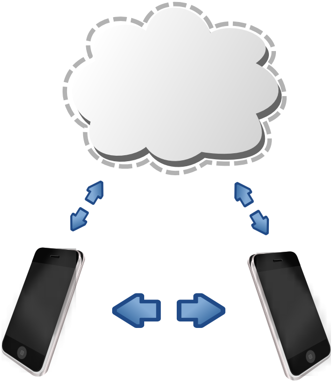
# Approach 3

## Approach 3

Double spending can only be performed by the original sender.
Therefore: Take trustworthiness of sender into account.

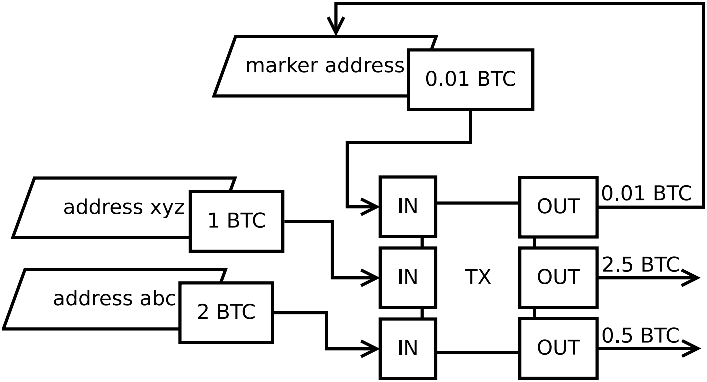
Limits the recipient to specific senders, but is in those cases then simple and safe.

# Out-of-band vs. in-band



Design decision: in-band

# Marker addresses: mechanism



# Advantages & disadvantages

## Advantages

- works everywhere where Bitcoin works today: behind firewalls, without a static ip or domain name
- backwards compatible

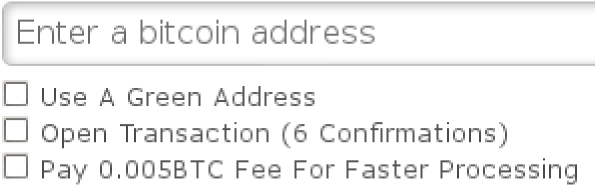
## Disadvantages

- negative effects on privacy
- increases transaction size and thus requires more space in the blockchain as well
- new challenge: deal with trust relationships of numerous senders

# Green addresses

First appeared as an optional feature of Instawallet in July 2011 (only sending): The site created a total of 12000 transactions of this type, until Paymium took over operation of the site in March 2012 and changed the backend which currently does not provide the feature anymore.

Since October 2011 Mt.Gox offers a green address option on the withdrawal page:

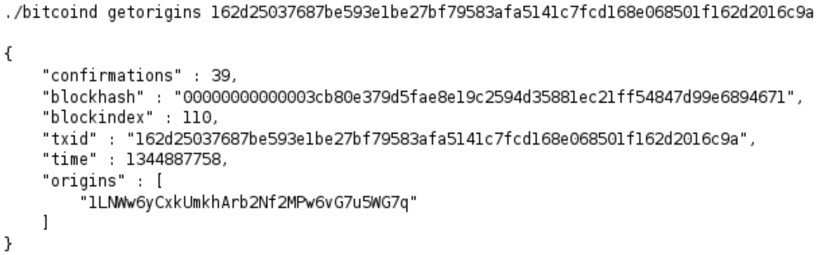


Enter a bitcoin address

□ Use A Green Address
□ Open Transaction (6 Confirmations)
□ Pay 0.005BTC Fee For Faster Processing

# Patches for Bitcoin daemon

“getorigins” RPC method:



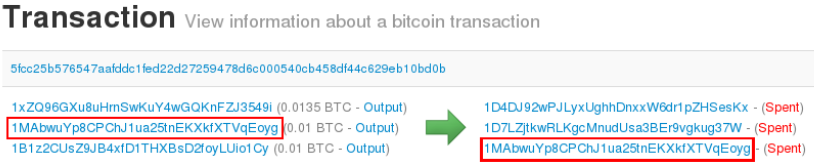
```
./bitcoind getorigins 162d25037687be593e1be27bf79583afa5141c7fcd168e068501f162d2016c9a

{
    "confirmations" : 39,
    "blockhash" : "00000000000003cb80e379d5fae8e19c2594d35881ec21ff54847d99e6894671",
    "blockindex" : 110,
    "txid" : "162d25037687be593e1be27bf79583afa5141c7fcd168e068501f162d2016c9a",
    "time" : 1344887758,
    "origins" : [
        "1LNWw6yCxkUmkhArb2Nf2MPw6vG7u5WG7q"
    ]
}
```

https://github.com/javgh/bitcoin/tree/bw-getorigins

# Patches für Bitcoin Daemon

Sending is still a bit hacky: Marker address to be used for outgoing transactions is hardcoded in the source code.



**Transaction** View information about a bitcoin transaction

5fcc25b576547aafddc1fed22d27259478d6c000540cb458df44c629eb10bd0b

1xZQ96GXu8uHrnSwKuY4wGQKnFZJ3549i (0.0135 BTC - Output)
1MAbwuYp8CPChJ1ua25tnEKXkfXTVqEoyg (0.01 BTC - Output)
1B1z2CUsZ9JB4xfD1THXBsD2foyLUio1Cy (0.01 BTC - Output)

1D4DJ92wPJLyxUghhDnxxW6dr1pZHSesKx - (Spent)
1D7LZjtkwRLKgcMnudUsa3BEr9vgkug37W - (Spent)
1MAbwuYp8CPChJ1ua25tnEKXkfXTVqEoyg - (Spent)

https://github.com/javgh/bitcoin/tree/bw-markeraddress

# Conclusion

## Marker addresses

Allow a sender to identify himself to a recipient using an in-band mechanism. Can be used as a basis for fast transactions between trusted parties.

Thanks for your attention!