Have a Snack,
Pay with Bitcoin

Tobias Bamert

Distributed Computing, TIK, ETH Zürich
Vending Machine
Vending Machine
Vending Machine
Vending Machine

bitcoin Wallet

Freitag, 27. September 13
Advantages

- Funds directly transferred to merchant
- Centralized
- Small transaction fees
Confirmation Time

- Transactions instantly visible
- Confirmed at irregular intervals
- Approximately 10 minutes
Fast Payment

- Trust unconfirmed transaction
- Hedge against loss
Double Spend

Attacker

Merchant
Double Spend

Attacker

Merchant

\[ T_v \]
Double Spend

Attacker

\[ T_a \]

Merchant

\[ T_v \]
Double Spend
Double Spend

$T_v$ $T_a$
Double Spend

\[ T_v \quad T_a \]
Double Spend

$T_v \quad T_a$
Double Spend

$T_v$  $T_a$
Countermeasures
Countermeasures

- Connect to many nodes
- No incoming connections
- No transaction relay
Evaluation

- Attacker and merchant
- Double spend attempts
- Random release points
Evaluation

\[ T_v \]

\[ T_a \]
Evaluation

Time until detection

- Average time
- Median time
- 95 percentile
- 99 percentile

Node sample size

Time [s]
Evaluation

Time until detection

- **Average time**
- **Median time**
- **95 percentile**
- **99 percentile**

Node sample size

Time [s]
Successful Double Spend

\[ P_{ds} = P_{fTv} \cap P_{nd} \cap P_{cTa} \]
Successful Double Spend

1. Merchant sees $T_v$ first

$$P_{ds} = P_{fT_v} \cap P_{nd} \cap P_{cTa}$$
Successful Double Spend

1. Merchant sees $T_v$ first
2. Only sees one transaction

$$P_{ds} = P_{fT_v} \cap P_{nd} \cap P_{cT\alpha}$$
Successful Double Spend

1. Merchant sees $T_v$ first
2. Only sees one transaction
3. $T_a$ is later confirmed

$$P_{ds} = P_{fT_v} \cap P_{nd} \cap P_{cT_a}$$
Evaluation

$P_{ds} = 0.088\%$
One loss in 1000 purchases
Select product

bitcoin Wallet
Display QR tag

bitcoin Wallet

Freitag, 27. September 13
Send Bitcoins

Listen for Announcements

bitcoin Wallet
OK!
Thank you!
Questions?

Tobias Bamert
Christian Decker
Lennart Elsen
Roger Wattenhofer
Samuel Welten