The Problem that the Blockchain Solves

Kai Brünnler

Research Institute for Security in the Information Society
Bern University of Applied Sciences

Bitcoin

What is Bitcoin?

- An open-source software
- A peer-to-peer network
- A payment network
- A currency

Bitcoin

What is Bitcoin?

- An open-source software
- A peer-to-peer network
- A *decentralized* payment network
  Like cash, unlike Paypal
- A *decentralized* currency
  Like gold, unlike the US Dollar

Bitcoin

What is Bitcoin?

- An open-source software
- A peer-to-peer network
- A *decentralized* payment network
  Like cash, unlike Paypal
- A *decentralized* currency
  Like gold, unlike the US Dollar

BankCoin

Alice

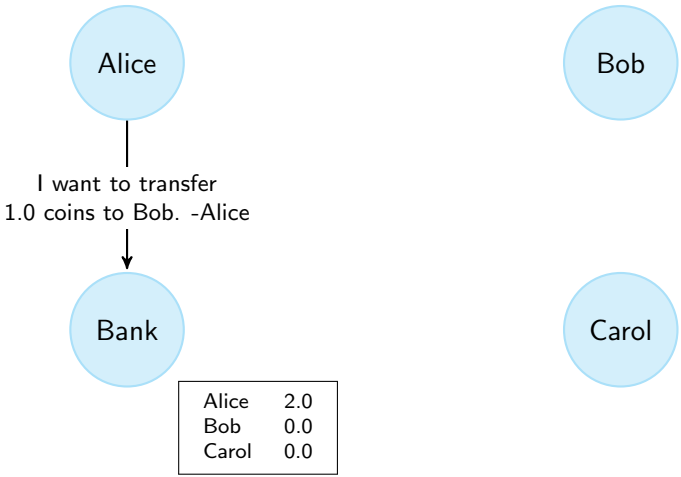
Bob

Bank

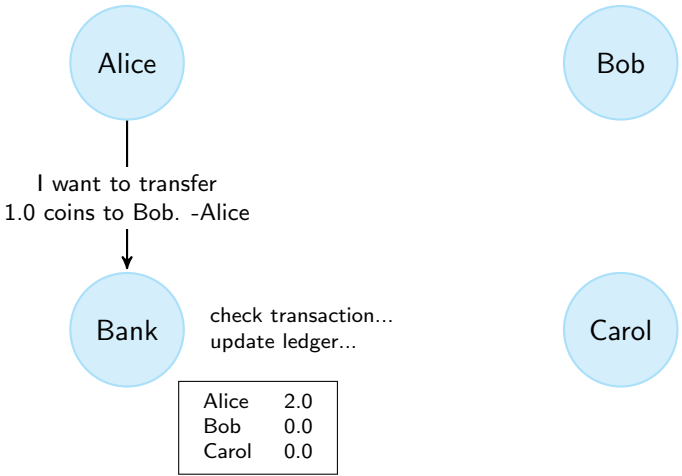
Carol

Alice	2.0
Bob	0.0
Carol	0.0

BankCoin


Alice
Bob
I want to transfer
1.0 coins to Bob. -Alice
Bank
Carol
Alice 2.0
Bob 0.0
Carol 0.0

BankCoin


Alice
Bob
I want to transfer
1.0 coins to Bob. -Alice
Bank
check transaction...
update ledger...
Carol
Alice 2.0
Bob 0.0
Carol 0.0

BankCoin

Alice

Bob

Bank

Carol

Alice	1.0
Bob	1.0
Carol	0.0

BankCoin

BankCoin Rules

- The bank has the ledger
- The bank accepts all valid transactions it receives and updates its ledger
- Everybody sends transactions to the bank

Problem

- The bank can censor transactions, create money, etc.
- Can we design a protocol without a central intermediary?
- In such a protocol, who would maintain the ledger?

NaiveCoin

Alice

Alice	2.0
Bob	0.0
Carol	0.0

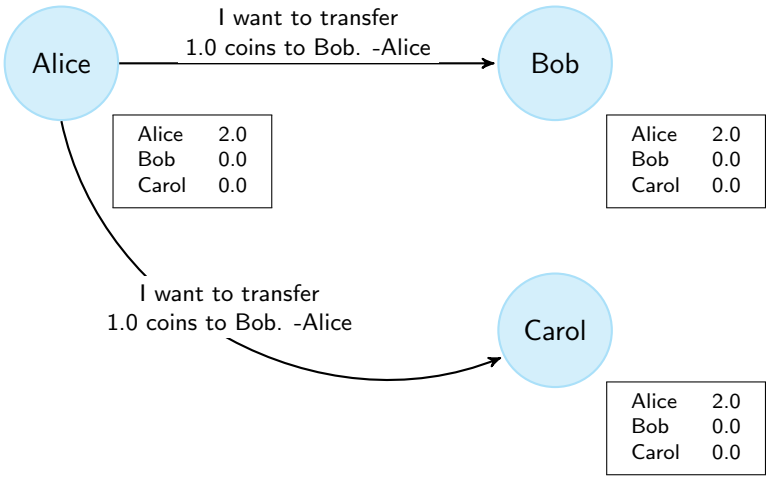
Bob

Alice	2.0
Bob	0.0
Carol	0.0

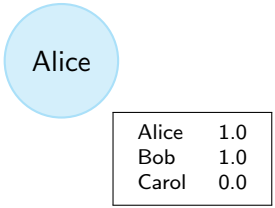
Carol

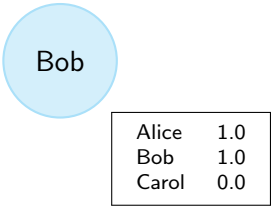
Alice	2.0
Bob	0.0
Carol	0.0

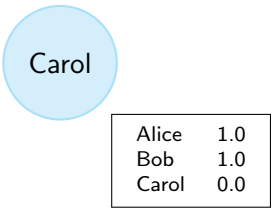
NaiveCoin


Alice
I want to transfer
1.0 coins to Bob. -Alice
Bob
Alice 2.0
Bob 0.0
Carol 0.0
Alice 2.0
Bob 0.0
Carol 0.0
I want to transfer
1.0 coins to Bob. -Alice
Carol
Alice 2.0
Bob 0.0
Carol 0.0

NaiveCoin


Alice
Alice 1.0
Bob 1.0
Carol 0.0


Bob
Alice 1.0
Bob 1.0
Carol 0.0


Carol
Alice 1.0
Bob 1.0
Carol 0.0

NaiveCoin

NaiveCoin Rules

- Each node has a copy of the ledger
- Each node accepts all valid transactions it receives and updates its ledger
- Each node broadcasts its transactions to all nodes

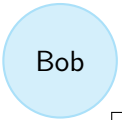
Problem solved

- No more bank!

New Problem

- The Double Spending Problem

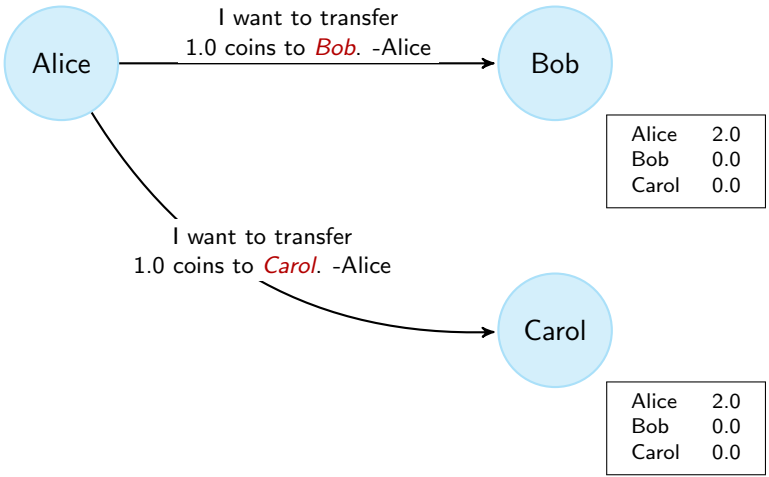
The Double Spending Attack



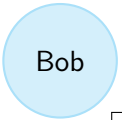
Alice	2.0
Bob	0.0
Carol	0.0

Alice	2.0
Bob	0.0
Carol	0.0

The Double Spending Attack



The Double Spending Attack



Alice	1.0
Bob	1.0
Carol	0.0

Alice	1.0
Bob	0.0
Carol	1.0

The Double Spending Attack

- Both Bob and Carol think they have been payed
- Bob will have trouble when he later tries to pay Carol
- The network is not in *consensus* anymore

- The problem of how to avoid this attack is the famous *double spending problem*
- This problem has only recently been solved by Satoshi Nakamoto in the Bitcoin whitepaper

Book

Kai Brünnler. Blockchain kurz & gut.
O'Reilly, 2018.

You can download a draft here.