Communication in Distributed Systems

11 Blockchain

Dr.-Ing. Michael Rademacher

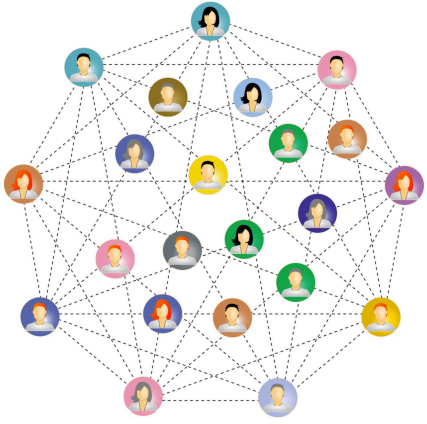
2021-06-15

Blockchain Overview

A major problem with blockchains

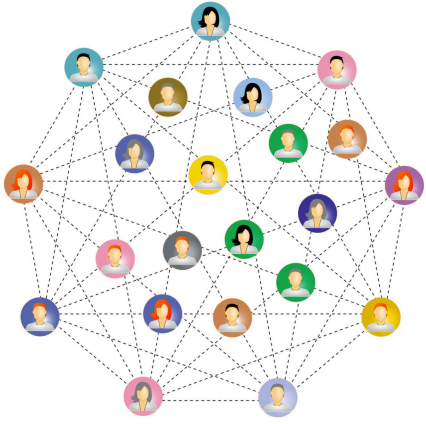
This Lecture: No guide for trading strategies of cryptocurrencies.

Definition



- A **blockchain** is a network based on a distributed transaction database for a tamper-proof storage of linear records
- The stored data is protected against unauthorized manipulation by **cryptography**, **decentralization** and **game theory**
- The innovation lies in the clever combination of these research areas and led for the first time to an efficient solution of the **Double-Spending-Problem**

Definition



- Blockchains make it possible to **dispense intermediate instances** and significantly reduce trust problems for transactions
- They offer very good protection against manipulation and are therefore highly **resistant to censorship**
- These properties lead to different possible **application**
- However, the overhead a blockchain is very high compared to a centralized database. The possible application should be questioned critically

Double-Spending-Problem

Definition:

The possibility to propagate a transaction (digital value transfer) multiple times on a decentralized network.

- Problem: Duplicates can cause a digital token to be transferred more than once
- Solution: Find a chronological **consensus** in a decentralized way so that no participant can manipulate it selfishly
- Central solution: Classic database (SEPA, Paypal)
- Decentralized solution: Blockchain

The blockchain led for the first time to the solution of the double-spending problem in decentralized systems.

Classification

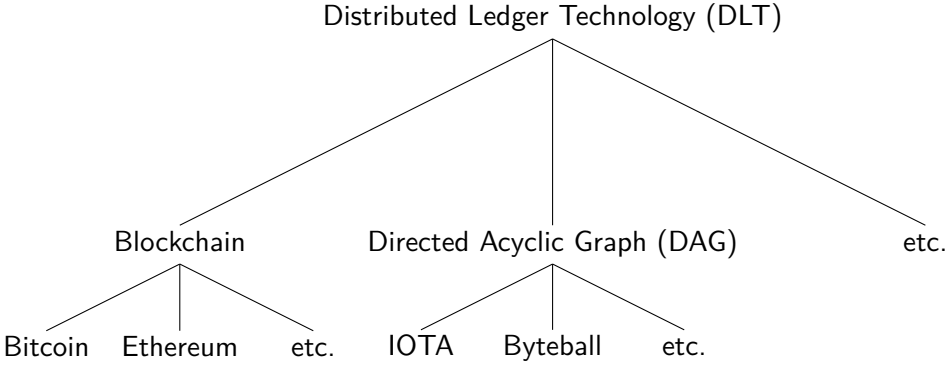
A Blockchain can be classified under the term Distributed Ledger Technology (DLT).

- A ledger is redundantly managed by different parties using multiple copies
- New transactions are transferred to all copies
- **The distribution of copies is a known and solved problem**
- **The challenge and the goal is to establish a consensus of the copies**

A blockchain is an innovative approach to implement a distributed ledger.

Every blockchain is a DLT, but not every DLT is a blockchain.

Classification



Models

Blockchains can be categorized into 3 different models [12]:

- **Public**
- **Private**
- **Federated**

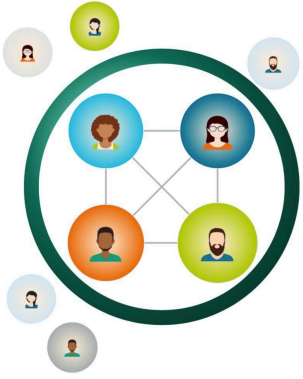
These models differ greatly in their degree of decentralization and the consensus algorithm used.

The term blockchain is highly controversial and debated for private and federated ledgers.

Public Blockchains

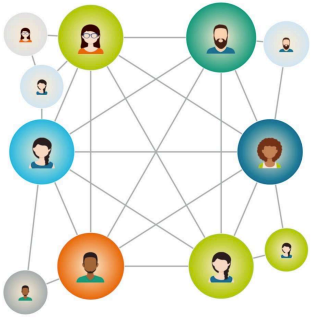
- Publicly accessible network
- Transactions are transparent and anonymous/pseudonymous
- **Anyone** can read, write and validate transactions
- Highest protection against tampering:
  - Cryptography
  - Decentralization
  - Game theory
- No central management
  - Therefore **no trust necessary**
- Complex consensus building with high computing power
  - Therefore mostly slow and poorly scalable
- Dimensions: Internet

Private Blockchains



- Closed network
- Transactions are private
- Special authorization needed to read, write and validate transactions
- Low protection against tampering:
  - Cryptography
  - Hardly any decentralization
  - No game theory necessary since network participants are all known
- Central management
  - Therefore **trust necessary**
- Trivial consensus building
  - Therefore mostly fast and easily scalable
- Dimensions: Intranet (private LAN/WAN)

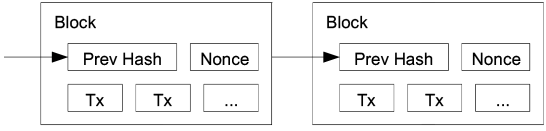
Federated Blockchains



- Hybrid solution
- Semi-public network
- Transactions are mostly transparent
- Special authorization needed to read, write or validate transactions
- Low protection against tampering:
  - Cryptography
  - Low decentralization
  - Low game theory
- Decentralized management by a consortium
  - Therefore **trust necessary**
- Trivial consensus building by a consortium
  - Therefore mostly fast and easily scalable

Important building blocks of blockchains

Cryptographic hash functions



[11]

Usage of cryptographic hash functions in Blockchains:

- Data can be stored in units of blocks
  - Enables the concept of a hashed list
  - Data blocks have fixed chronological order
  - Previous data blocks cannot be manipulated unnoticed
- Consensus mechanism
  - Basis of the so-called Proof of work (PoW) Hashcash Puzzle

Public Key Cryptography

$$f_{oneway}(k) = p$$

Private Key k: 

- Basis for generating a key pair
- Secret, non-public key

Public Key p: 

- Is irreversibly derived from the private Key
- Public, not secret key

Digital signatures

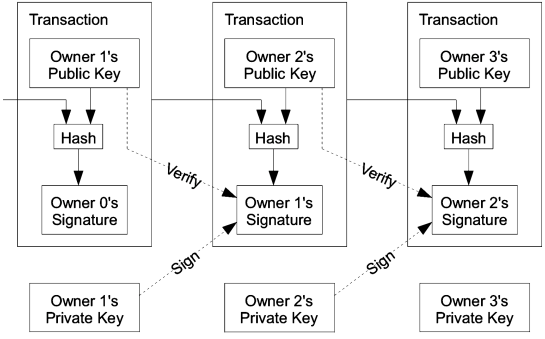
$$f_{sign}(m, k) = sig$$

$$f_{verify}(sig, p)$$

- Are supposed to emulate properties of physical signatures
- Three protection goals are fulfilled:
  1. Integrity
  2. Authenticity
  3. Liability
- Are generated by a signature scheme of the **sender**

Digital signatures

Transaction from owner to owner+1.
owwner signs the public key of owner+1



"We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin."[11]

Usage of digital signatures in Blockchains:

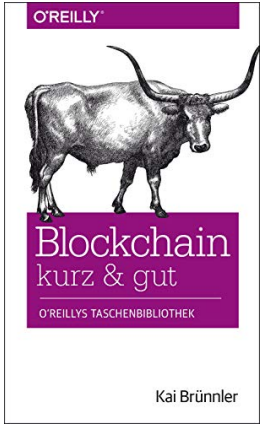
- Full transaction security
- Transactions are:
  - Not manipulated (integrity)
  - Authorized (authenticity)
  - Not deniable (liability)
- **digital ownership through private keys**
- **no private key, no ownership**

From a centralized Bank to a blockchain

Methodology

Methodology for the rest of theses slides: Piece by Piece derivation of a functional Blockchain starting with current online banking.

The methodology is inspired by the following book [6]:



The author's summary of blockchains [10]:

BRSU Communication Report Nr. 1
ISBN: 978-3-96043-081-0, Digital Object Identifier: 10.18418/978-3-96043-081-0

Technical Fundamentals of Blockchain Systems

Oliver Kattwinkel[1], Michael Rademacher[2]

Abstract
This work provides a short but technical introduction to the main building blocks of a blockchain. It argues that a blockchain is not a revolutionary technology but rather a clever combination of three fields: cryptography, decentralization and game theory. In addition, it summaries the differences between a public, private and federate blockchain model and the two prominent consensus mechanism Proof-of-Work (POW) and Proof-of-Stake (POS).

Keywords
Blockchain — Cryptography — Proof-of-Work — Proof-of-Stake

[1] *Kleenecode GmbH, Sankt Augustin, Germany*
[2] *Department of Computer Science, University of Applied Sciences Bonn-Rhein-Sieg, Sankt Augustin, Germany*
oliver.kattwinkel@kleenecode.com, michael.rademacher@inf.h-brs.de

01: Bank-protocol

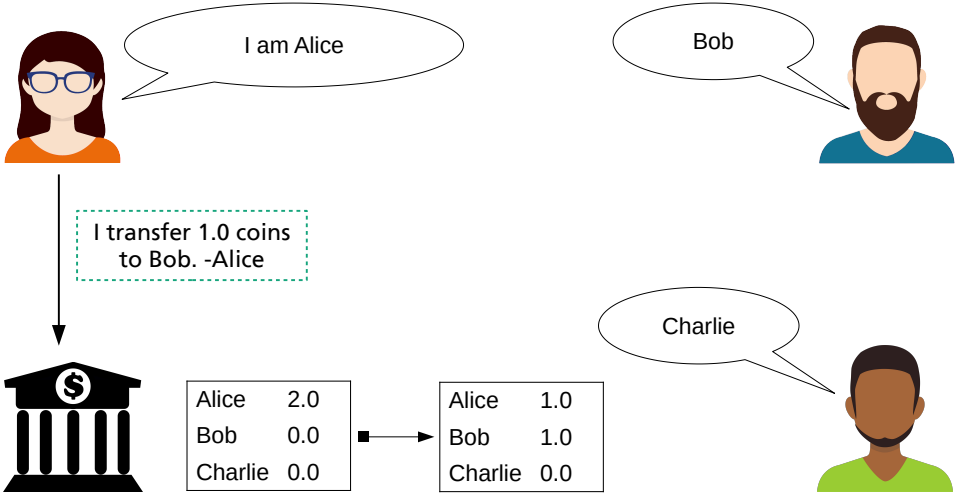
Initial situation: Current online banking

- A bank functions as a central administration
- Digital value transfer of a Fiat currency
- Access through credentials
  - Username and password
  - Digital signatures

Rules for this protocol:

- The bank manages credit balances of all participants in a central credit database
- To transfer credits, participants send signed transactions to the bank
- The bank accepts only valid transactions
- The bank updates balances according to accepted transactions
- All participants request their current credit via the bank

01: Bank-protocol



01: Bank-protocol

Problem:

- By managing all data the bank has great centralized power
- Participants dependent on the security of the bank
- As intermediary, the bank has more rights than any other participant in this system
  - Censorship through rejection of transactions
  - Inflation through generation of new credit
  - Manipulation by changing credit balances

The Five/Nine Hack in the TV Series Mr. Robot [4]. Destroy financial records of the largest bank in the USA.

Solution:

- No bank, no single intermediary, no centralized power
- Who manages the credit of the participants?
- **Each participant manages each credit!**

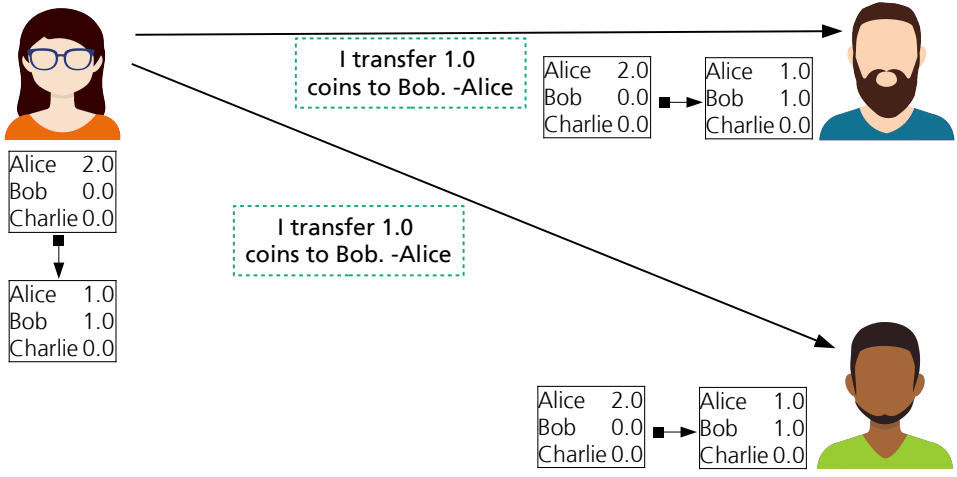
02: P2P-protocol

Transiation from a hierarchical bank protocol to a flat P2P-protocol

Rules:

- Each participant manages each credit of all participants in their own credit database
- To transfer credits, participants send signed transactions to all participants
- Each participant accepts only valid transactions
- Each participant updates all balances according to accepted transactions

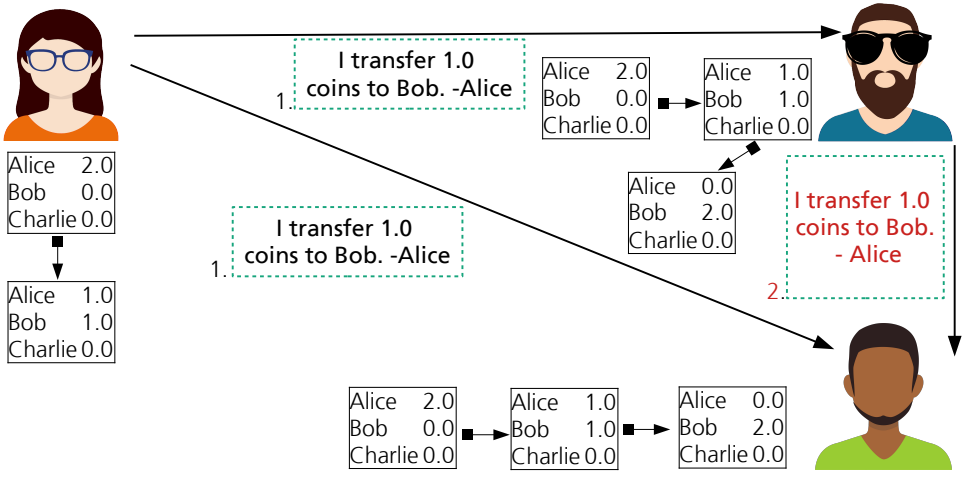
02: P2P-protocol



Problem:

- Each participant can manipulate their own database “as they wish”
- Manipulation of other databases through so-called replay attacks
- Replay attack:
  - Attacker can resend received transactions
  - Recipients verify authenticity only by the signature
  - All participants (except the victim) will accept the transaction
- Consensus (all participants agree on state of the database) is not assured

02: P2P-protocol replay attack



Thank you for your attention.
Are there any questions left?

Room K331
Rathausallee 10
Technopark
Sankt Augustin

michael.rademacher@h-brs.de
www.mc-lab.de
https://michael-rademacher.net

References I

[1] Cost of a 51% attack for different cryptocurrencies | crypto51.
https://www.crypto51.app/.
(Accessed on 06/14/2021).

[2] Cryptopunks.
https://www.larvalabs.com/cryptopunks.
(Accessed on 06/14/2021).

[3] Ethereum (eth) blockchain explorer.
https://etherscan.io/.
(Accessed on 06/14/2021).

[4] Mr. robot - wikipedia.
https://en.wikipedia.org/wiki/Mr._Robot.
(Accessed on 06/15/2021).

[5] Borchers, D.
Digitaler corona-impfpass: Ibm, ubirch und fünf blockchains | heise online.
https://www.heise.de/news/Digitaler-Corona-Impfpass-IBM-Ubirch-und-fuenf-Blockchains-5076161.html.
(Accessed on 06/14/2021).

References II

[6] Bruennler, K.
Blockchain kurz und gut.
O'Reilly, Sebastopol, 2018.

[7] Chen, R.
What is defi? an introduction to decentralized finance – openzeppelin blog.
https://blog.openzeppelin.com/what-is-defi/, 2020.
(Accessed on 06/14/2021).

[8] Compound Labs, I.
Compound.
https://compound.finance/, 2021.
(Accessed on 06/14/2021).

[9] Froelich, P.
'cryptopunk' nft sells for $11.8 million at sotheby's.
https://nypost.com/2021/06/12/cryptopunk-nft-sells-for-11-8-million-at-sothebys/.
(Accessed on 06/14/2021).

[10] Kattwinkel, O., and Rademacher, M.
Technical fundamentals of blockchain systems.
BRSU Communication Report (2020).

References III

[11] Nakamoto, S.
Bitcoin: a peer-to-peer electronic cash system, oct. 2008.
URL http://www. bitcoin. org/bitcoin. pdf.(cited on pp. 15 and 87) (2017).

[12] Voshmgir, S.
Types of blockchains & dlts (distributed ledger technologies).
https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/.
(Accessed on 06/14/2021).