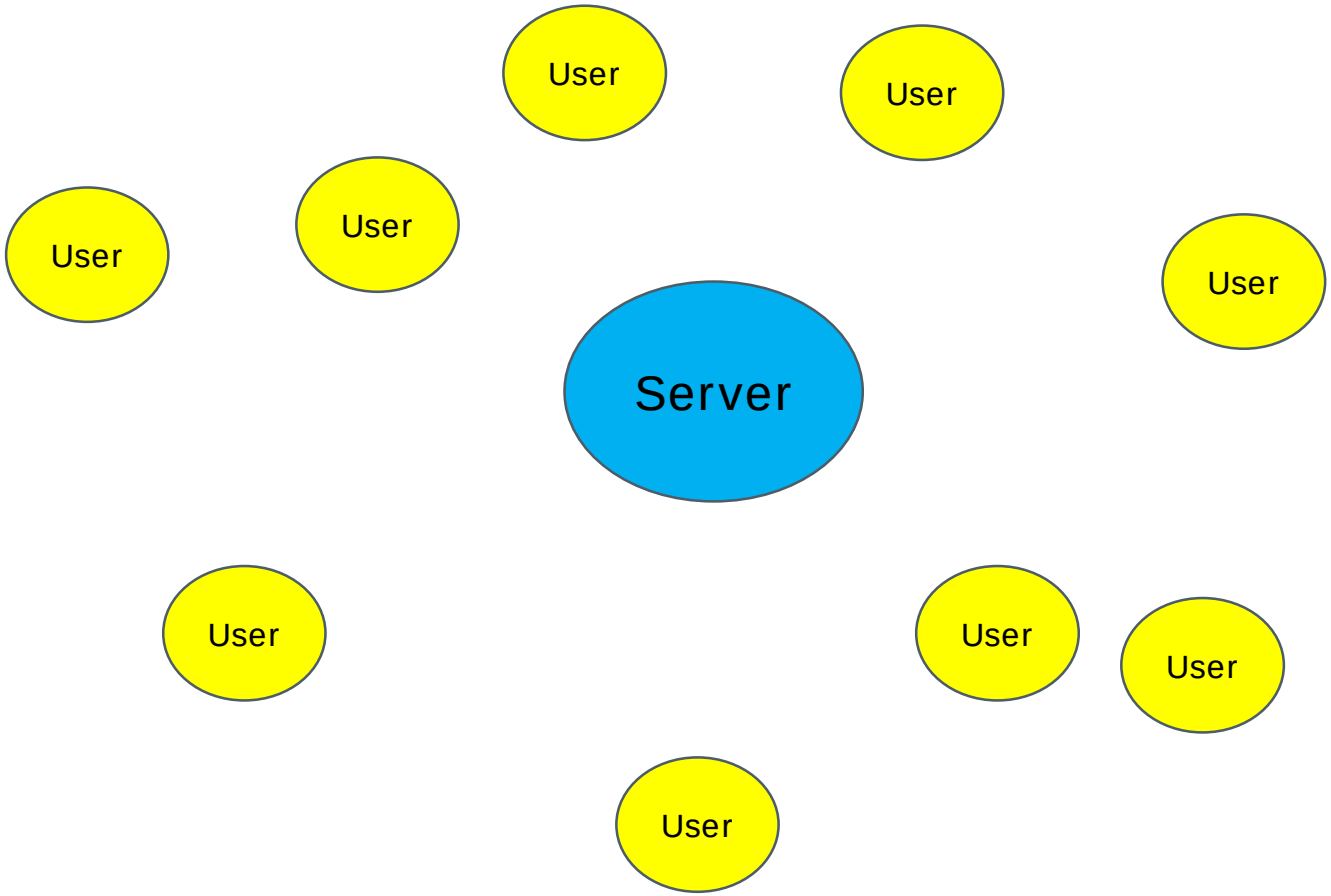
Blockchain und Kryptowährungen

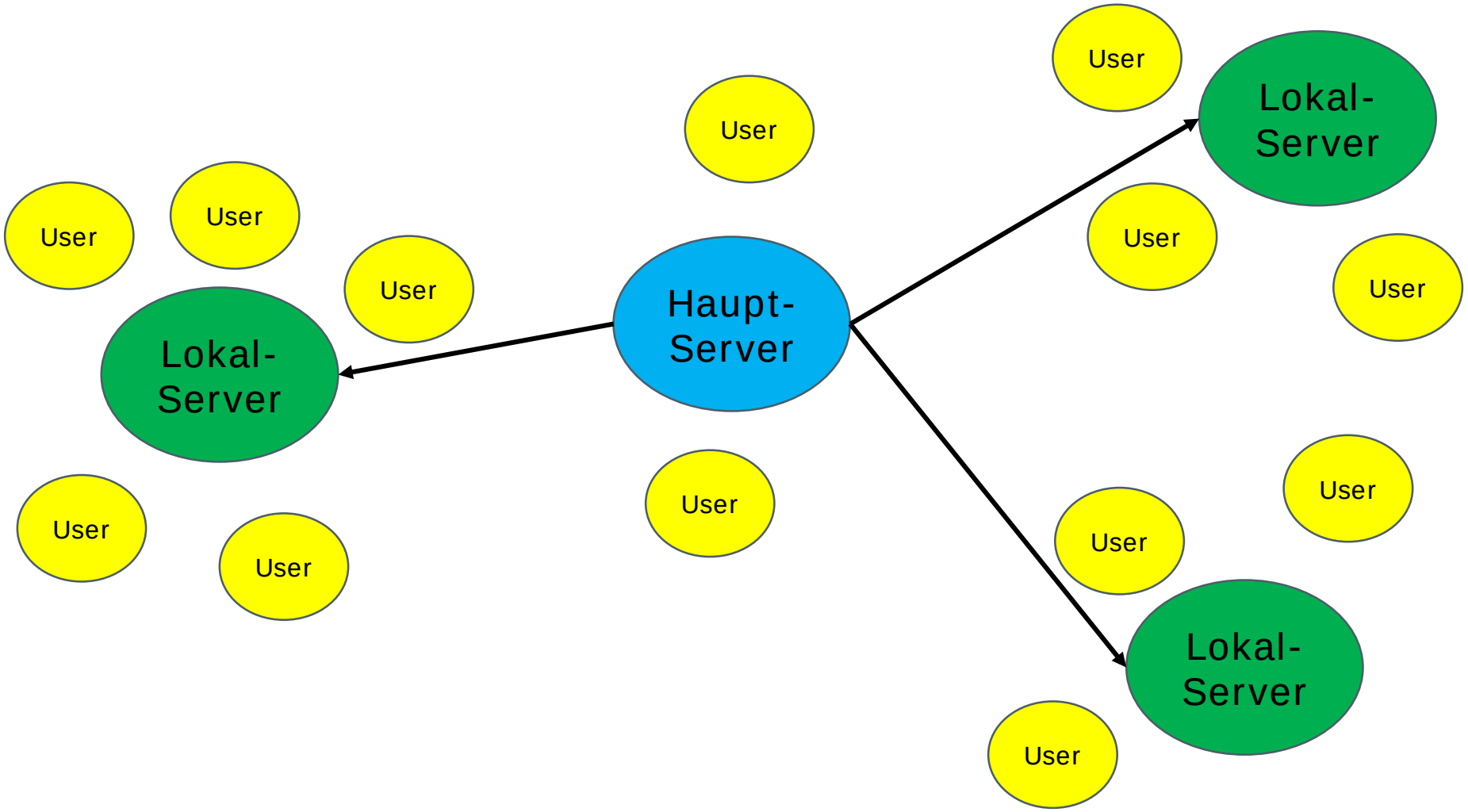
Mag. Philipp H. Bohrn

24.5.2018

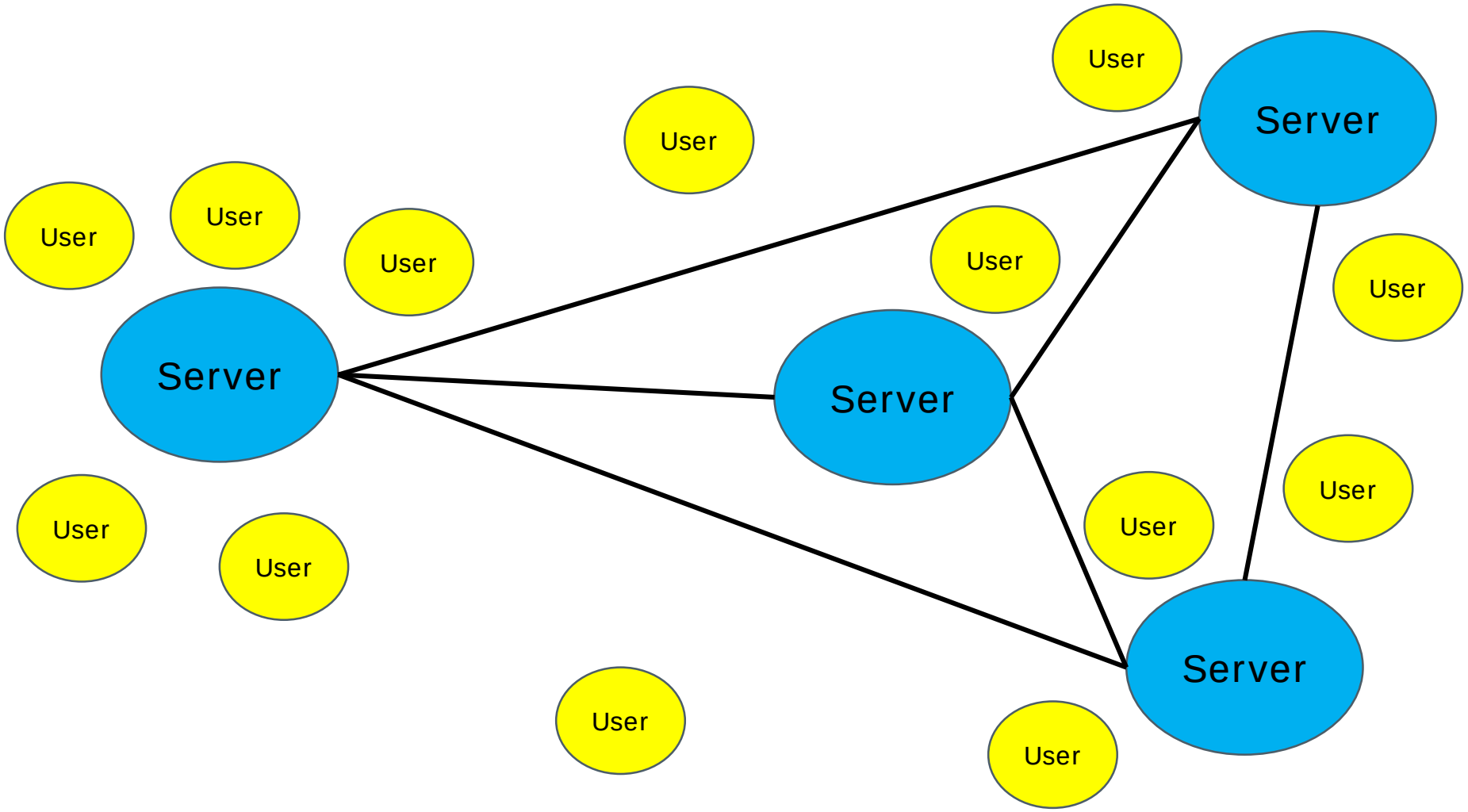
Zentralisiert



Verteilt (Distributed)



Dezentralisiert (Blockchain)



Vergleich

Dezentralisiert

- Ineffizient
- Schwer zu managen
- Teilweise langsam

Verteilt

- Vertrauen notwendig
- Potentielle Sicherheitsprobleme

Eigenschaften von Blockchains

- Transparenz
- Erreichbarkeit
- Finalität
- Sicherheit
- Keine zentrale Verwaltung/Entscheidungsstelle

Mögliche Anwendungsbereiche

- Firmenbuch?
- Herstellungsnachweise?
- Kryptowährungen
- Smart Contracts

Kryptowährungen - Die Rollen

- Nutzer zum Geldtransfer
- Investor?
- „Mining“-Betreiber
- Händler

Kryptowährungen – Mining

- Warum Mining
  - Durchführung von Transaktionen
  - Sicherung des Netzwerkes
- Wie verdienen „Mining“-Betreiber Geld?
  - Transaktionskosten
  - Neue Blocks durch steigende „Coins“
- Kosten für Mining
  - Technische Anschaffungen
  - Strom

Kryptowährungen - Die Brieftasche (Wallet)

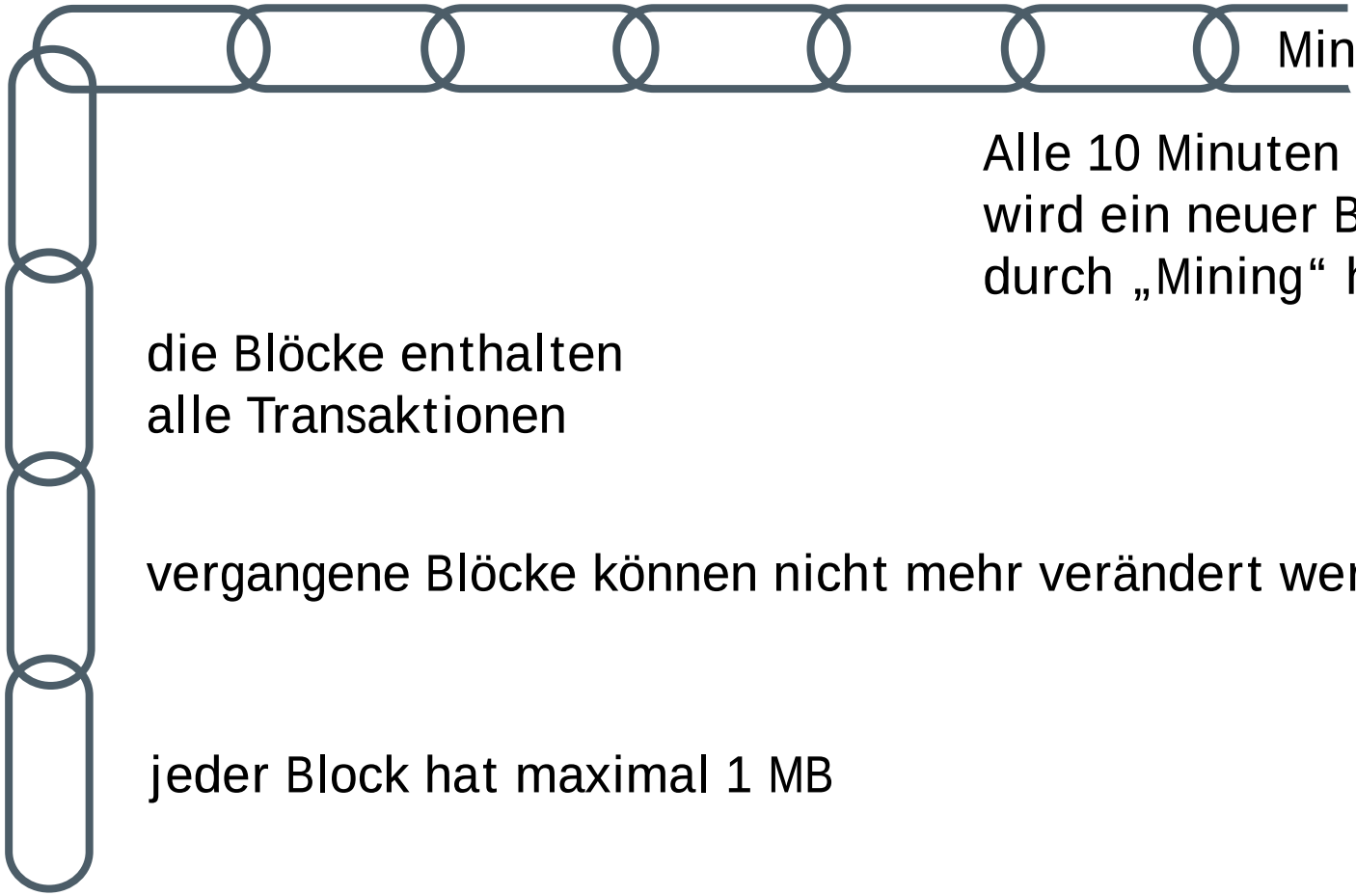
- Funktionen
  - Hält die Privaten Schlüssel „private keys“ und nutzt diese, um die eigenen Transaktionen zu verschlüsseln.
  - Kalkuliert die Kosten der Transaktion.
  - Kalkuliert die noch nicht ausgegebenen Transaktionen, daher den „Kontostand“.

- Problemstellungen
  - Wenn der Zugang weg ist oder von einem anderen eine Transaktion durchgeführt wurde, gibt es keine Sicherheitsbarrieren.

Kryptowährungen – Ablauf

- Der Nutzer erhält (durch Kauf oder Mining) Transaktionsvolumen (häufig Coins gennant).
- Der Nutzer beauftragt eine Transaktion.
- „mempool“: Nachdem eine Transaktion vom Nutzer freigegeben wurde kommt diese in den „mempool“. Durch Mining wird die Transaktion in die Blockchain aufgenommen und damit sichergestellt.

Kryptowährungen - Beispiel Bitcoin



Alle 10 Minuten
wird ein neuer Block
durch „Mining“ hinzugefügt.

die Blöcke enthalten
alle Transaktionen

vergangene Blöcke können nicht mehr verändert werden

jeder Block hat maximal 1 MB

Fragen