# Blockchain and Cryptocurrencies

## Chapter 0: Money

Prof. Dr. Peter Thiemann

Albert-Ludwigs-Universität Freiburg, Germany

SS 2020

# Contents

Based on the book chapter by Aleksander Berentsen

# Money

## Life in a Community

- daily granting of favors w/o immediate return
- informal accounting
- balancing / consensus by social means

# Money

## Life in a Community

- daily granting of favors w/o immediate return
- informal accounting
- balancing / consensus by social means

## Problem: Scalability

- ok with small groups
- difficult with large groups
- impossible for exchanges between unrelated persons

# Money as Memory

## Money

- formalizes the accounting
- keeps track of global favor-granting
- is memory

# Contents

Based on the book chapter by Aleksander Berentsen

# What is a Payment System?

## Payment System

- representation of money
- creation of money
- transfer of ownership

# Examples of Payment Systems

## Cash

- physical representation
  $\Rightarrow$ ownership obvious, anonymous, hard to tamper with
- drawbacks
  - physical proximity
  - storage and transportation of large values impractical

# Examples of Payment Systems

## Cash

- physical representation
  $\Rightarrow$ ownership obvious, anonymous, hard to tamper with
- drawbacks
  - physical proximity
  - storage and transportation of large values impractical

## Electronic Payment Systems

- mainly digital representation
- physical tokens (credit cards, debit cards, mobile phones) required for authentication
- book money
- centralized agencies keep track of balance

# Examples of Payment Systems II

## Blockchain-Based Payment Systems

- no physical representation — like credit card etc.
- algorithmic creation
- decentralized global consensus about account balances

# Contents

Based on the book chapter by Aleksander Berentsen

# Emergence of a Monetary Unit

- social process
- emerges from widely used / commonly accepted bartering good
- examples: basic foods, decorative objects (rocks, metal, animals, teeth, shells, feathers, . . . )

# Contents

Based on the book chapter by Aleksander Berentsen

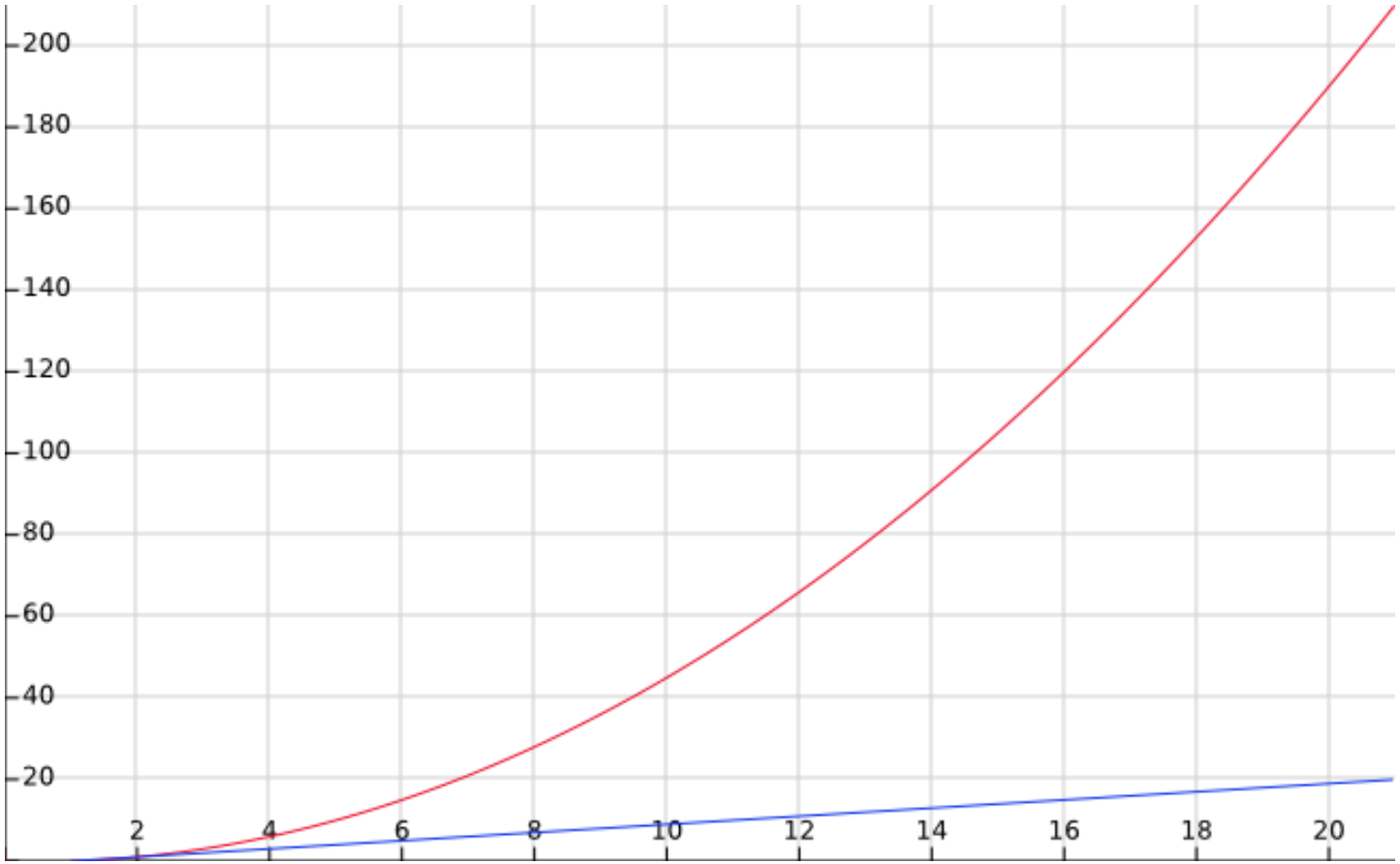
# Functions of a Monetary Unit

- means of exchange
- unit of accounting
- value storage

# Means of Exchange

- w/o money: only direct exchange of good and services
- impractical
  - multi-party exchanges
  - number of exchange pairs is quadratic
- w/ money
  - **buy**: goods for money
  - **sell**: money for goods

# Number of Exchange Pairs




- x-axis: # goods
- y-axis: # exchange pairs
- red: direct exchange
- blue: via money

# Unit of Accounting

- uniform, comparable valuation of goods and services
- market transparency
- lower transaction cost

# Value Storage

- possibility to save
- prepare for larger investments

## exchange good vs value storage

- exchange good $\Rightarrow$ value storage
- value storage $\overset{?}{\Rightarrow}$ exchange good

# Contents

Based on the book chapter by Aleksander Berentsen

# Fundamental Properties

- durability
- transferability
- divisibility
- homgeneity
- verifiability
- stability
- scarcity

# Fundamental Properties I

## Durability

- requirement for exchange goods and value storage
- rules out perishable items

# Fundamental Properties I

## Durability

- requirement for exchange goods and value storage
- rules out perishable items

## Transferability

- easy to change ownership (exchange)
- easy to convert to liquidity (value storage)

# Fundamental Properties I

## Durability

- requirement for exchange goods and value storage
- rules out perishable items

## Transferability

- easy to change ownership (exchange)
- easy to convert to liquidity (value storage)

## Divisibility

- valuation of arbitrary goods and services (exchange)
- alt: sufficiently small unit available

# Fundamental Properties II

## Homogeneity

- items interchangeable
- no individual valuation needed
- counter example: wine

# Fundamental Properties II

## Homogeneity

- items interchangeable
- no individual valuation needed
- counter example: wine

## Verifiability

- authenticity can be checked
- fakes easy to spot

# Fundamental Properties II

## Homogeneity

- items interchangeable
- no individual valuation needed
- counter example: wine

## Verifiability

- authenticity can be checked
- fakes easy to spot

## Stability of Value

- no regional or seasonal change
- stable relation of demand vs supply

# Fundamental Properties III

## Scarcity

- limited availability
- if unlimited: why trade
- if no trade: no value stored

# Contents

Based on the book chapter by Aleksander Berentsen

# Monetary Equivalent

**Where does monetary value come from?**

# Monetary Equivalent

**Where does monetary value come from?**

## Market Value of Unit

fundamental value

\+ payment promise

\+ speculation

# Monetary Equivalent

**Where does monetary value come from?**

## Market Value of Unit

fundamental value

\+ payment promise

\+ speculation

Each monetary unit combines one or more of these values

# The Value of Money

## Fundamental Value

- material value of object
- benefit from using or owning

# The Value of Money

## Fundamental Value

- material value of object
- benefit from using or owning

## Payment Promise

- not connected to the carrier / object
- based on trust in issuer

# The Value of Money

## Fundamental Value

- material value of object
- benefit from using or owning

## Payment Promise

- not connected to the carrier / object
- based on trust in issuer

## Premium for Liquidity/Speculation

- useability of object (what can I buy for it)
- demand for the object

# Examples

Non 0 material value

## Commodity Money

- fundamental value (+ speculation)
- fundamental value is lower bound of market value
- examples: shells, rings, jewellery, fur, metal (gold coins), cattle, basic foods, ...

never fall to 0.

# Examples

## Commodity Money

- fundamental value (+ speculation)
- fundamental value is lower bound of market value
- examples: shells, rings, jewellery, fur, metal (gold coins), cattle, basic foods, ...

## Credit Money

- traditional IOU
- arbitrary form
- market value depends on default risk
- (consider Euro Bonds)

# Excursion

## Origin of paper money

- originally payment promises backed by, e.g., a gold reserve
- exchangeable for a given amount of gold
- "The first known banknote was first developed in China during the Tang and Song dynasties, starting in the 7th century. Its roots were in merchant receipts of deposit during the Tang dynasty (618–907), as merchants and wholesalers desired to avoid the heavy bulk of copper coinage in large commercial transactions."
  https://en.wikipedia.org/wiki/Banknote


https://en.wikipedia.org/wiki/Gold_standard#/media/File:Us-gold-certificate-1922.jpg

# Fiat Money

- created "ex nihilo", named after the biblical "fiat lux"
- ("fiat" latin for "let there be")
- **no** fundamental value
- **no** payment promise
- value entirely based on expectation
  $\Rightarrow$ **not** bounded
- most currencies today are like that
- value maintained by central bank (obligated by law)
- legal tender
- introduced from the 1970es, before that currencies were backed by gold reserves (e.g., https://en.wikipedia.org/wiki/Fort_Knox)

# Contents

Based on the book chapter by Aleksander Berentsen

# Monetary Control Structures

- creation of money
- representation
- transaction processing

# Creation of Money

- limitation / scarcity required
- two modes of creation

## Competitive Creation

- everybody can create
- limit: production cost $<$ market value

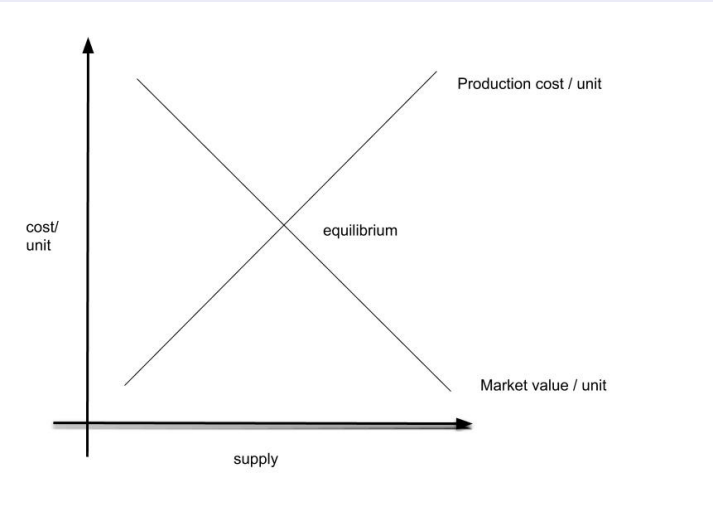
## Monopolized Creation

- restricted to (government) agencies

# Competitive Creation

## Scenario 1 (Gold Mining)

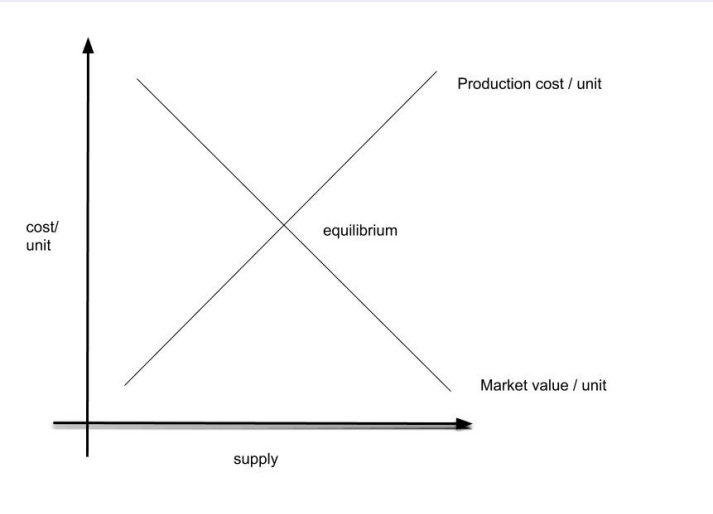
- increasing the money supply lowers the market value of a unit
- manufacturing a unit requires resources that become scarce



# Competitive Creation

## Scenario 1 (Gold Mining)

- increasing the money supply lowers the market value of a unit
- manufacturing a unit requires resources that become scarce




## Scenario 2: Constant low manufacturing cost

- unbounded manufacturing until market value $= 0$
- reality, but undesirable . . . , hence monopolize

# Monopolized Creation

- artificially limited
- government agency (e.g., central bank)
- manufacturing cost way below market value
- positive value created by restriction and law (legal tender)

# Excursion: Cost of the Euro

| coin | value/EUR |
|---|---|
| 1 Cent | 0.01 |
| 2 Cent | 0.01 |
| 5 Cent | 0.02 |
| 10 Cent | 0.02 |
| 20 Cent | 0.03 |
| 50 Cent | 0.04 |
| 1 Euro | 0.10 |
| 2 Euro | 0.13 |

| bank note | value/EUR |
|---|---|
| 5 Euro | 0.07 |
| 10 Euro | 0.09 |
| 20 Euro | 0.16 |
| 50 Euro | 0.16 |
| 100 Euro | 0.16 |
| 200 Euro | 0.16 |

# Creation by Banks

## Central Bank

The central bank creates money by loaning to corporate banks.
Temporary loans help regulate the money supply.

# Creation by Banks

## Central Bank

The central bank creates money by loaning to corporate banks.
Temporary loans help regulate the money supply.

## Requirement

- Trust in central bank / government
- otherwise: inflation, e.g., to shrink national debt

# Creation by Banks

## Central Bank

The central bank creates money by loaning to corporate banks.
Temporary loans help regulate the money supply.

## Requirement

- Trust in central bank / government
- otherwise: inflation, e.g., to shrink national debt

## Corporate Banks

- can create money by lending "deposit currency" (to private customers and businesses) that is not backed by legal tender
- (only a fraction needs to be backed by law)

$\Rightarrow$ if all customers withdraws legal tender according to their balance, the bank goes bankrupt

# Representation of Money

## Physical representation

- control of object = ownership of value
- easy to use / transfer
- no trust / infrastructure needed

## Disadvantages of physical representation

- bound to location — problematic for digital goods
- transportation — cost for managing and counting cash
- integrity — fake resistance by design; more expensive to manufacture
- divisibility — fixed denominations

# Virtual Representation

## From a note of ECB

A virtual currency ... is a digital representation of a value, which is not issued by a central bank or a public agency and which is not bound to a real currency, but which is nevertheless accepted as a means of payment by natural or legal entities and can be transmitted, stored, and traded electronically.

# Virtual Representation

## From a note of ECB

A virtual currency ... is a digital representation of a value, which is not issued by a central bank or a public agency and which is not bound to a real currency, but which is nevertheless accepted as a means of payment by natural or legal entities and can be transmitted, stored, and traded electronically.

## Naive digital bank note

- represented as a "cash file"
- unique ownership, e.g., by cryptographic certificate

$\Rightarrow$ no registry needed

- **but** unlimited copying possible

# On the Need for Registries

- explicit or implicit
- implicit registries
  - work for small communities
  - consensus by exhaustive communication
  - punishment by, e.g., exclusion / social pressure

# Excursion: Rai Stones

By Eric Guinther - English Wikipedia, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=161923

# Contents

Based on the book chapter by Aleksander Berentsen

# Transaction Processing

## Conditions for TP

**Capability** transactions can be started and value can be transferred

**Legitimacy** transaction can only be initiated by the owner

**Consensus** a process exists to determine the current balance of all accounts at all times

# Transaction Processing II

## TP for Physical Money

No issues

# Transaction Processing II

## TP for Physical Money

No issues

## TP for Virtual Money

- registries are needed
- for decentralized registries, how do we deal with malicious parties
- standard: centralized trusted registries
- risk of corruption, both internal and external (hackers)
- dilemma:
  - virtual money is more efficient
  - but the centralized registry is a single vulnerable point of control
- remained unsolved until the advent of Bitcoin in 2008

# Thanks!