Smart Contracts and Blockchain Technology

Lecture 1. Introduction and overview

Christian Ewerhart

University of Zurich

Fall 2022

Welcome!!!

This lecture is embedded into a broader study program

Smart Contracts and Blockchain Technology

- Lecture with integrated exercises (6 ECTS)[1]
- Seminar (3 ECTS)

Written thesis in collaboration with Blockchain Presence

- BA thesis (18 ECTS)
- MA thesis (30 ETCS)
- Individual learning unit (6 ECTS)

[1] The course is offered the first time this fall. If successful, it will be offered regularly in the fall term.

Schedule

Lecture (Wednesday 8:00 a.m. - 9:45 a.m.)

- Prof. Dr. Christian Ewerhart
- 80 percent of the final grade[2]

Tutorial (Friday 12:15 p.m. - 13:45 p.m.)[3]

- Haoyuan Zeng (ZGSE)
- 20 percent of the final grade[4]

---

[2] The final exam takes place at 8 a.m. on January 11, 2023. Since access to the internet needs to be prohibited, the sustainability principle implies that the exam will be held in a closed-book format.

[3] The tutorial starts this week!

[4] Solutions of selected problems should be handed in via OLAT and Mumbai blockchain, as detailed in the problem sets.

Economics of blockchain (1)

Trust and consensus

In many realms of economic reality, **trust** or a **reliable third party** is needed to reach a certain goal.

Examples:

- Payments (banks and central banks)
- Real estate transactions (notaries)
- Elections (public authorities)

Blockchain technology provides a way to replace such institutions by a decentralized **consensus protocol**.

Economics of blockchain (2)

Public blockchains

The **blockchain** itself...

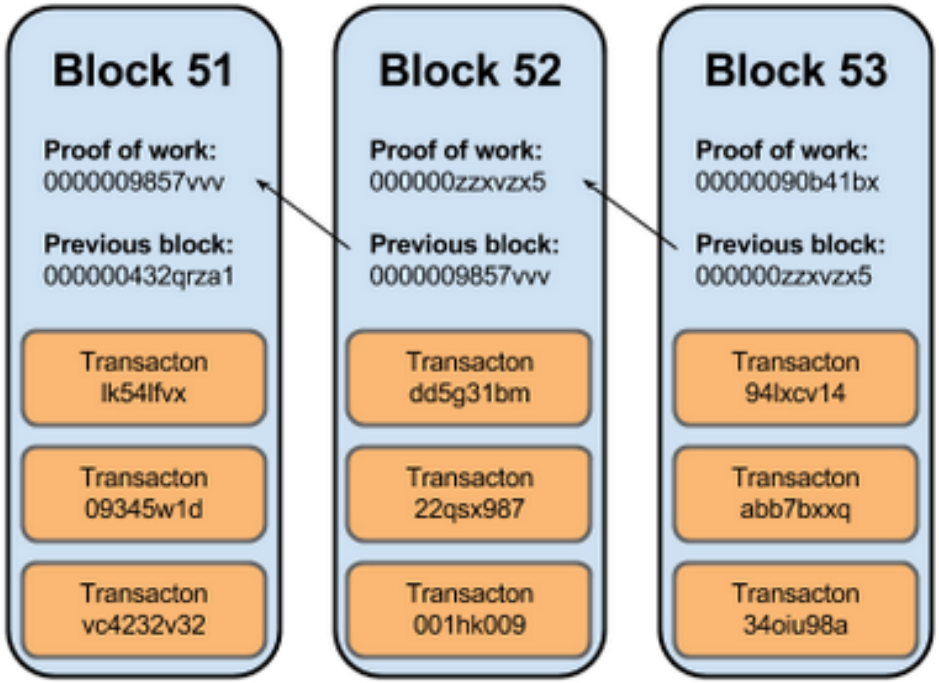
- ...consists of a heap of **blocks** (essentially linear and starting from a "genesis block"),...

...that is maintained as a **public and distributed database** (or "ledger") in a peer-to-peer network.

Economics of blockchain (3)

Blocks and transactions

In the bitcoin blockchain, each **block** consists of a list of **transactions** plus a header.



New blocks are added to the blockchain using the **proof-of-work** validation protocol.

Economics of blockchain (4)

Incentives for miners

Every new block creates a **reward**, consisting of

- a block subsidy, and
- transaction fees.

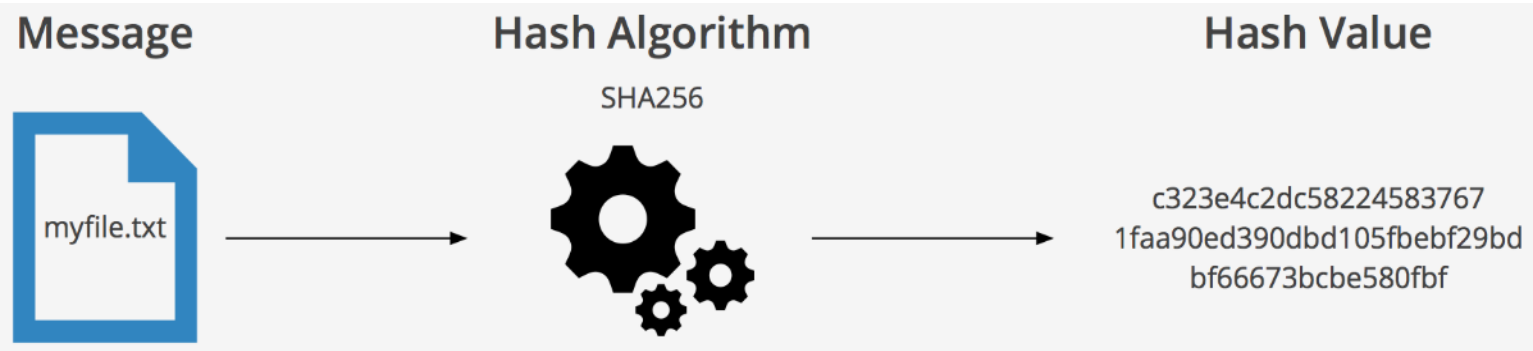
Each **miner** tries to add a block to the blockchain that distributes the reward in his own interest ("coinbase transaction")!

However, to get consensus for his block, the miner has to present the solution to a **difficult computational problem** (or "crypto puzzle").

Economics of blockchain (5)

Understanding the miner's problem

The **SHA256** algorithm takes any text message and transforms it into a 64-digit hexadecimal string.



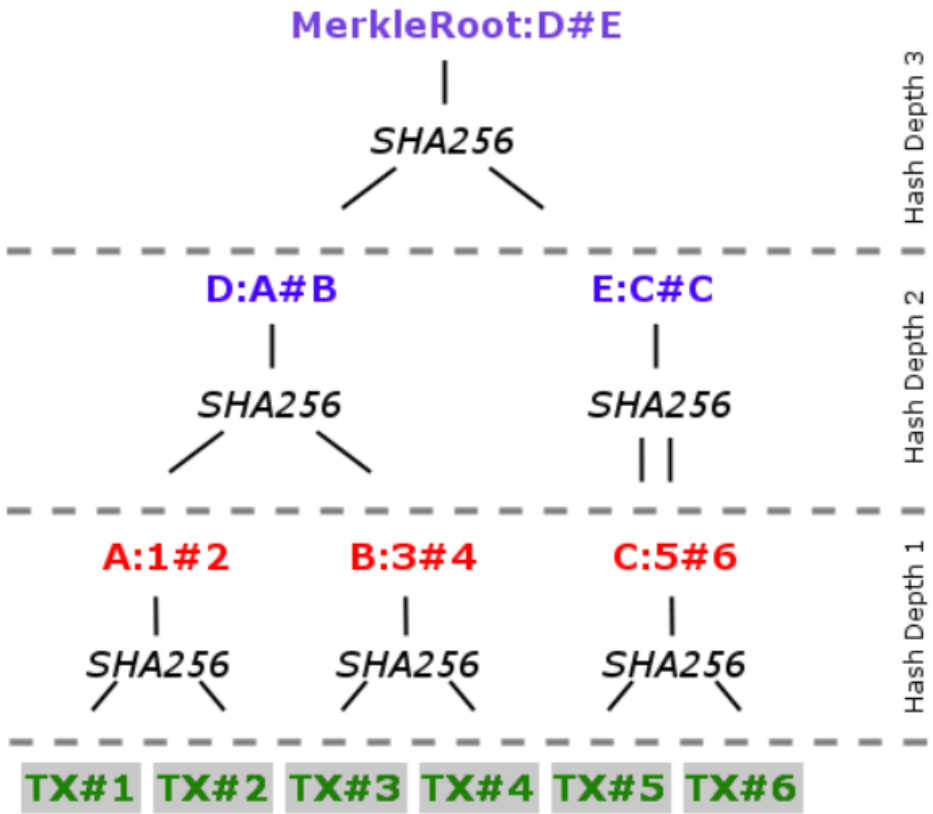
The algorithm is **deterministic** and computationally **non-invertible**.

Economics of blockchain (6)

Merkle root

SHA256 -> hexadecimal code with 64 digits

The transactions of a block are condensed, using iterated SHA256 hashes, into a single **Merkle root**.



Economics of blockchain (7)

Block header

The Merkle root is a component of the **block header**.

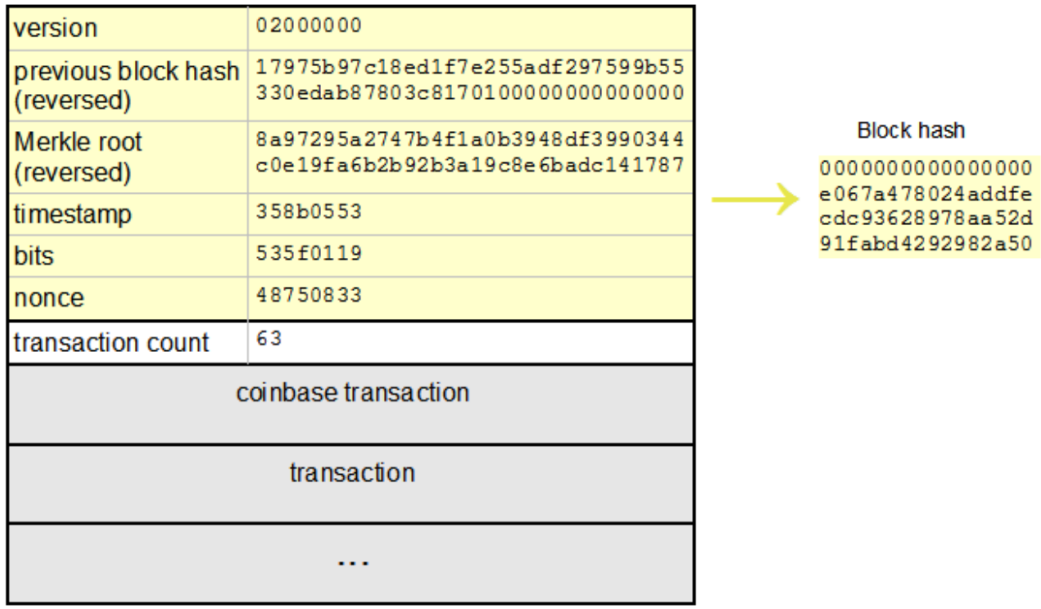
Size	Field	Description
4 bytes	Version	The Bitcoin Version Number
32 bytes	Previous Block Hash	The previous block header hash
32 bytes	Merkle Root	A hash of the root of the merkle tree of this block's transactions
4 bytes	Timestamp	The timestamp of the block in UNIX.
4 bytes	Difficulty Target	The difficulty target for the block.
4 bytes	Nonce	The counter used by miners to generate a correct hash.

The **block hash** is determined by hashing the block header through SHA256 (twice).

Economics of blockchain (8)

Nonce

To solve the cryptopuzzle, the miner changes the **nonce** many times, until the block hash is below a certain threshold.



That threshold (corresponding to the difficulty level) is dynamically adjusted so as to have a new block in regular time intervals.

Economics of blockchain (9)

Block time

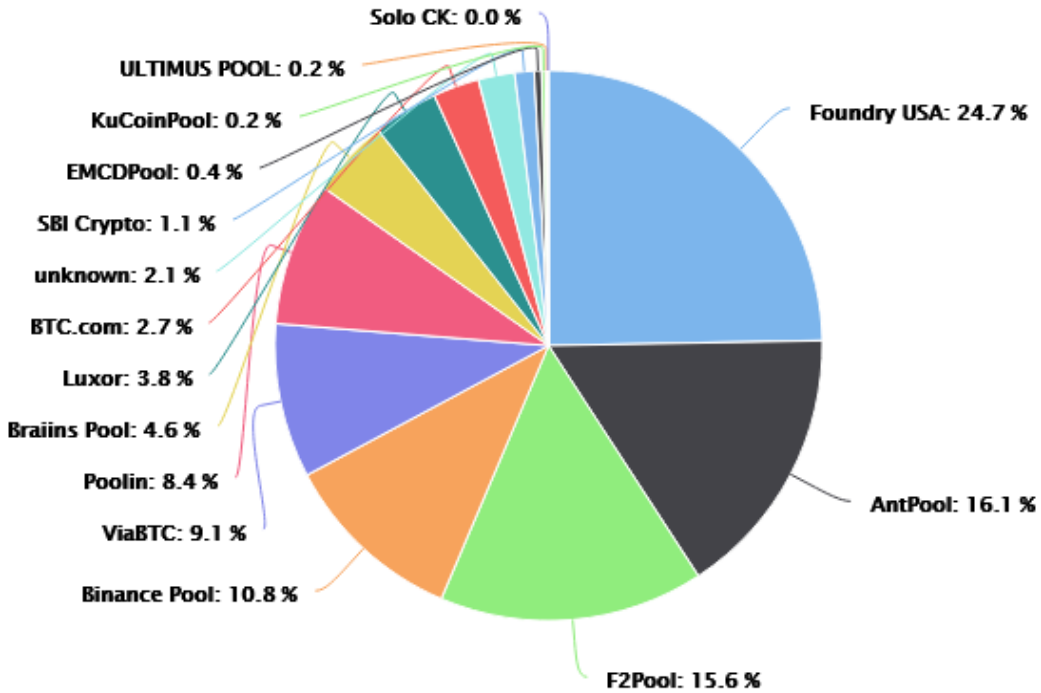
Height	Age	Transactions	Mined by	Size
541912	16 minutes ago	2331	SlushPool	959888
541911	20 minutes ago	2895		917302
541910	31 minutes ago	1754	AntMiner	922638

The **block time** is the average time it takes for the network to generate one extra block in the blockchain. The block time for Bitcoin is about 10 minutes. The blocktime for Ethereum is approximately 15 seconds.

Economics of blockchain (10)

Bitcoin mining pools

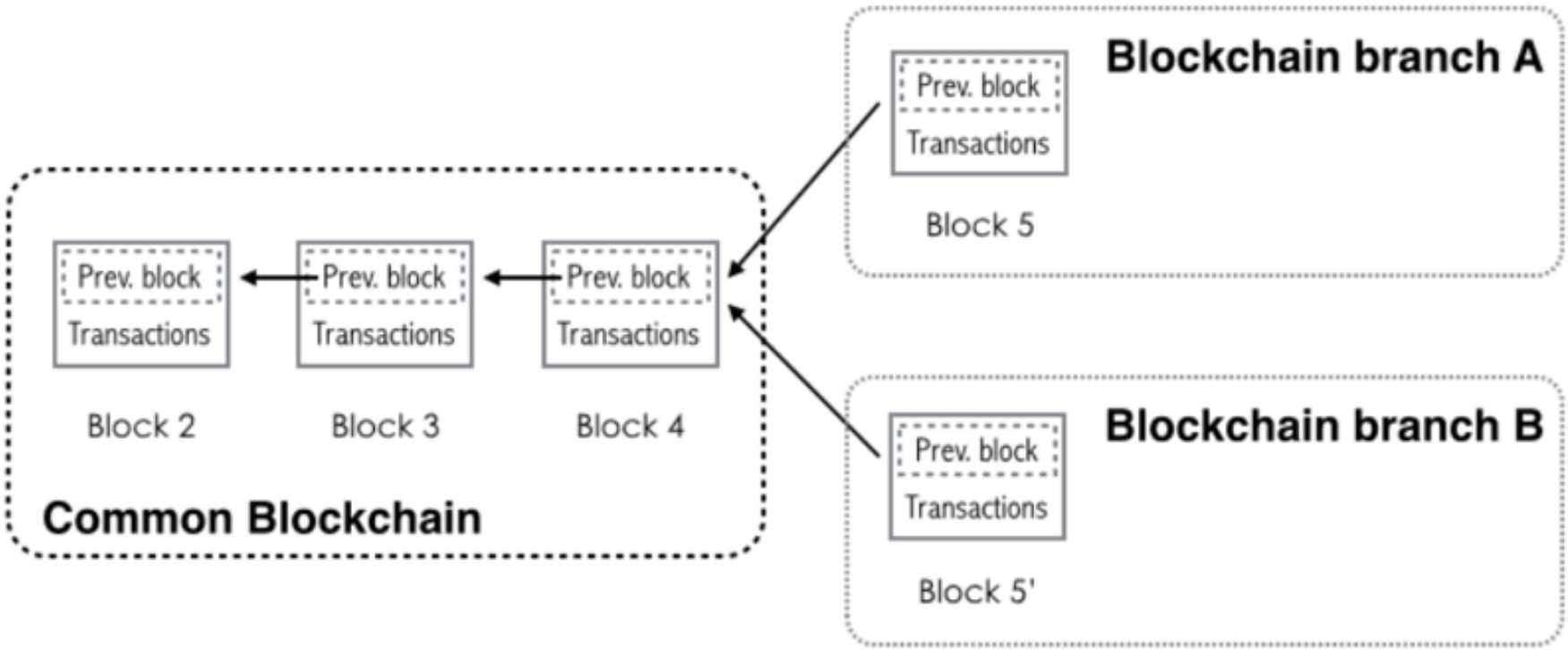
Mining power distribution as of August-September 2022:[5]



[5] Source: BTC.com

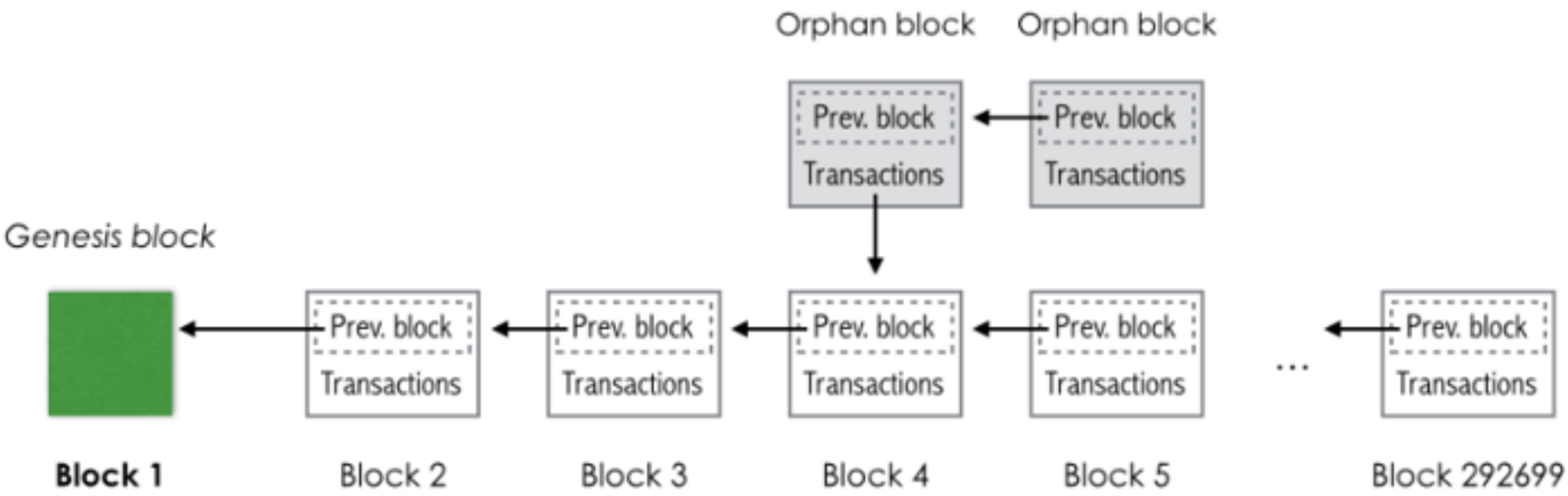
Economics of blockchain (11)

Forking



Economics of blockchain (12)

Orphan blocks



Economics of blockchain (13)

Some figures

Bitcoin market cap in USD since February 2013:[6]

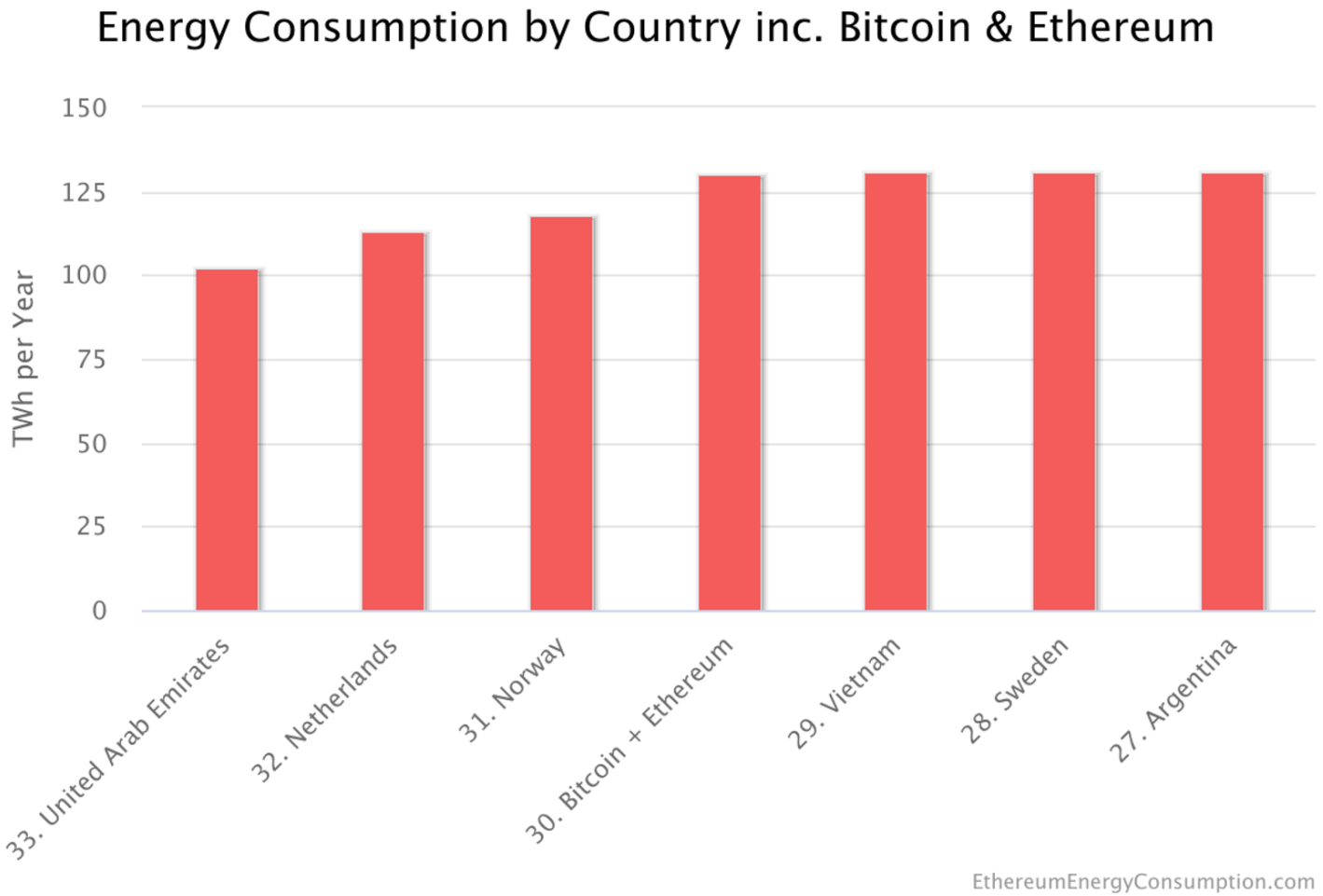
Hypes in December 2017 and December 2021...

Compare: UBS Group $58B, CS Group $13B

[6] Source: coinmarketcap.com

Economics of blockchain (14)

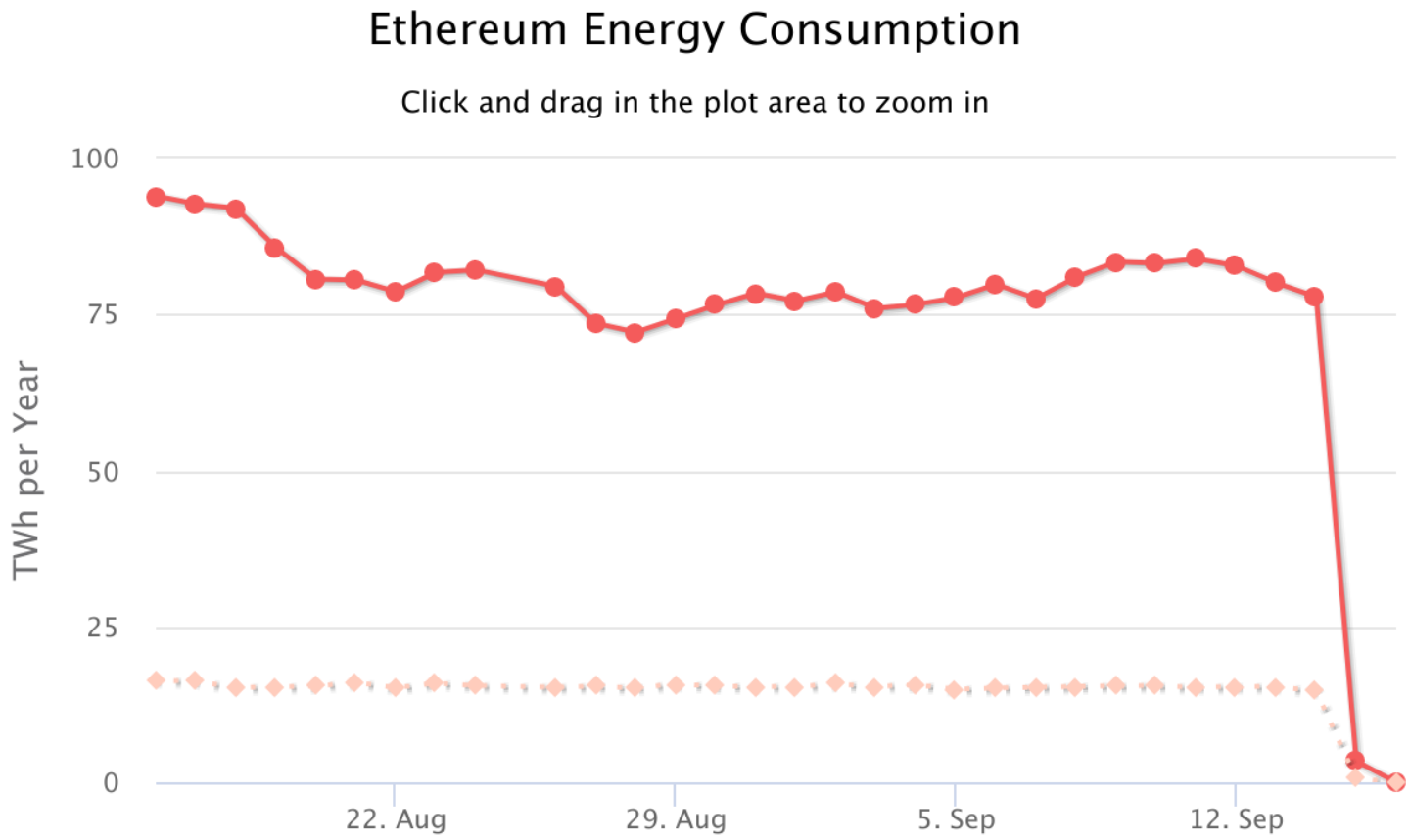
Energy consumption



Economics of blockchain (15)

Ethereum's move from proof-of-work to proof-of-stake

Ethereum's merge might have lowered the world's energy consumption by 0.2 percent[7]



[7] Source: Vitalik Buterin, EthereumEnergyConsumption.com

Economics of blockchain (16)

Smart contracts and blockchain oracles

Smart contracts is software that is stored and executed on a blockchain; usually, they govern transfers in cryptocurrencies.

Almost all smart contract applications require input from the real world. This input is received from so-called **blockchain oracles**, such as Chainlink, Band Protocol, API3, etc.

Economics of blockchain (17)

History of blockchain technology

2008 Bitcoin, the first decentralized blockchain, was launched under the acronym Satoshi Nakamoto.[8]

2015 Ethereum, the first decentralized smart contract platform, was conceptualized and launched by Vitalik Buterin and Gavin Wood, in particular.[9]

[8] See the Bitcoin Whitepaper. It is not known who hides their identity behind the acronym.

[9] See the excellent monograph *Mastering Ethereum*, by Andreas M. Antonopoulos and Gavin Wood. To access this document, you need to sign up at Github first.

Economics of blockchain (18)

The double-spending problem

Imagine you wish to create a protocol that allows to transfer value electronically (by email, say).

Suppose you do not want to make use of a bank (maybe because society went through a financial crisis that led to a lot of inequality).

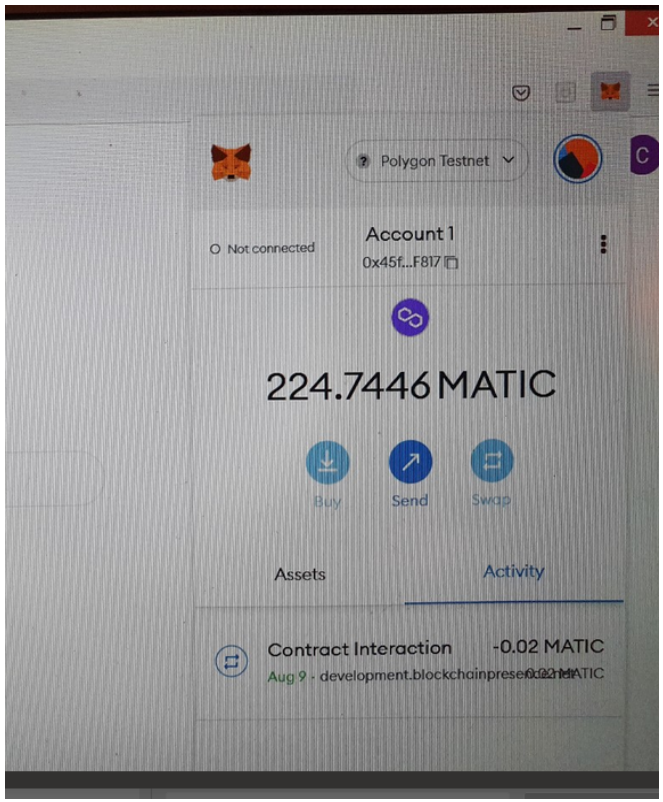
Then, your major problem would be the so-called **double-spending problem**: How do you make sure that the same amount is not used twice?

Blockchain technology solves this problem.

Economics of blockchain (19)

Wallets

The simplest way to open a wallet is using the browser plug-in Metamask.



Economics of blockchain (20)

The blockchain trilemma

Public blockchains suffer from the so-called **blockchain trilemma**:

- Decentralization
- Security
- Scalability

Overview

Main topics of the lecture:

I. Mining and consensus formation (4 lectures)
II. Cryptographic underpinnings (2 lectures)
III. Smart contract programming (4-5 lectures)
IV. Decentralized finance (2-3 lectures)

Next week, we will start with part I (Mining and consensus formation).

Some final points

If possible, bring a laptop or tablet to the next tutorial.

Thanks for the attention and and see you next week!

Smart Contracts and Blockchain Technology

Lecture 2. The mining game

Christian Ewerhart

University of Zurich

Fall 2022

Introduction and overview

Last lecture: Introduction to the topic

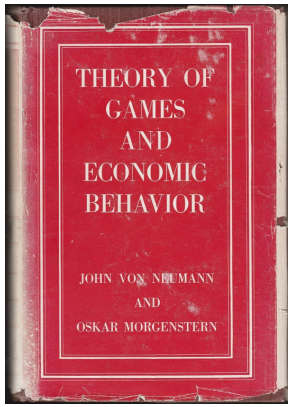
This lecture:

- We plan to have about four lectures on the game-theoretic analysis of
  - mining and
  - consensus formation.
- *Today:* The mining game with homogenous costs

Bitcoin mining as a contest (1)

The game-theoretic approach

Game theory has existed for more than a century by now. Its breakthrough to mainstream economics is often associated with the appearance of the monograph by John von Neumann and Oskar Morgenstern (1945).



Bitcoin mining as a contest (2)

Non-cooperative games

In a **non-cooperative game**, a finite number of players independently and simultaneously choose strategies, which has payoff implications for all of them.

An **equilibrium concept**, such as Nash equilibrium, is applied to make specific predictions.

Examples:

- Cournot model (quantity competition)
- Bertrand model (price competition)

Bitcoin mining as a contest (3)

Non-cooperative games

We will model blockchain mining as a game. As an equilibrium concept, we use the **Cournot-Nash equilibrium**.[1]

This means that each player **correctly anticipates** the strategies chosen by her opponents, and chooses an optimal response.

Optimality means here that each player **maximizes her expected payoffs** given equilibrium expectations.

[1] Nash equilibrium was initially defined for games with finitely many strategies for each player (Nash, 1950, 1951). The Cournot-Nash equilibrium is a generalization in which players may choose strategies from a continuous strategy set (e.g., from an interval).

Bitcoin mining as a contest (4)

Posing a difficult mathematical problem

Suppose that, in regular time intervals, the crypto protocol formulates a new **mathematical problem**, and organizes a competition between anybody interested to participate.

The **reward** for solving the puzzle is denoted by $R > 0$.

In reality, the reward is denominated in crypto (e.g., bitcoin) and may be composed of several components:

- block reward
- transaction fees
- additional rewards (e.g., so-called uncle rewards in Ethereum)

Bitcoin mining as a contest (5)

Miners

Users participating in the competition are called **miners**. Each miner $i \in \{1, 2\}$ decides about her computational power $h_i \geq 0$ (the "hash rate").

The computations are assumed to create a **continuous flow of costs** $C(h_i)$, say within a fixed time interval of length $T > 0$.

We assume that miner i's **cost function** is given by $C(h_i) = c_i \cdot h_i$, where $c_i > 0$ is miner i's constant marginal cost to produce a unit of computational power.

Bitcoin mining as a contest (6)

Discussion of the assumptions on the cost functions

In reality, miners' investment decisions are more complicated for various reasons.

We impose the following **assumptions**:

- Fixed-cost investments (set-up of hardware and software) are depreciated using the straight-line method.
- Costs of computational power stand for operational variable costs (such as energy consumption and maintenance).
- Costs are expressed in bitcoin (rather than in fiat currency).

Bitcoin mining as a contest (7)

The case of homogeneous costs

For simplicity, we start with the case of two **ex-ante identical** miners.

Thus, we assume that:

- $n = 2$, and
- $c_1 = c_2 \equiv c$ (**homogeneous costs**).

Bitcoin mining as a contest (8)

Excursus: Poisson process

The Poisson process is one of the stochastic processes most commonly used in economics (and many other fields).

Key properties:

- Process in continuous time $t \geq 0$
- Counting process (starting at zero, constant almost everywhere, upward jumps by one at random times)
- Memoryless (delay does not make the "discovery" in the next instant more or less likely)

The Poisson process may be considered as the limit of discrete-time search processes as the time interval $\Delta t > 0$ between two consecutive experiments goes to zero, where the probability of a discovery $p \approx \lambda \cdot \Delta t$ is asymptotically linear in Δt.

Bitcoin mining as a contest (9)

The distribution of the time of discovery

Denote by $\widetilde{t}$ the **time of the discovery**. This is a random variable.

Let

$$F(t) = \text{prob}\{\widetilde{t} \leq t\} \tag{1}$$

be the **cumulative distribution function** of the probability law that is followed by $\widetilde{t}$.

The **instantaneous probability** of a discovery is

$$f(t) = \lim_{\Delta t \to 0} \frac{F(t + \Delta t) - F(t)}{\Delta t} = F'(t). \tag{2}$$

Bitcoin mining as a contest (10)

Relationship to the exponential distribution

As the process is memoryless, the instantaneous probability of a discovery, conditional on not having discovered the solution before, is constant:

$$\frac{f(t)}{1 - F(t)} = \lambda, \tag{3}$$

for some $\lambda > 0$.

Solving the ordinary differential equation (3) leads to

$$F(t) = 1 - \exp(-\lambda t), \tag{4}$$

$$f(t) = \lambda \exp(-\lambda t). \tag{5}$$

Thus, $\widetilde{t}$ is **exponentially distributed** with parameter λ.

Bitcoin mining as a contest (11)

Expected waiting time

The expected waiting time is defined as

$$E[\widetilde{t}] = \int_0^\infty f(t)tdt. \tag{6}$$

Lemma 1. *The* **expected waiting time** *for the discovery is*

$$E[\widetilde{t}] = \frac{1}{\lambda}. \tag{7}$$

Bitcoin mining as a contest (12)

Proof of the lemma

We use the **integration-by-parts** formula

$$\int_a^b u'(t)v(t)dt = u(t)v(t)|_a^b - \int_a^b u(t)v'(t)dt, \tag{8}$$

with functions

$$u(t) = -\exp(-\lambda t) \tag{9}$$
$$v(t) = t. \tag{10}$$

Then,

$$\int_0^\infty \lambda \exp(-\lambda t)tdt = \int_0^\infty \exp(-\lambda t)dt = \frac{1}{\lambda}, \tag{11}$$

as has been claimed. $\square$

Bitcoin mining as a contest (13)

Waiting time for an individual miner

We assume that solving the puzzle (by try and error) follows a Poisson process with parameter

$$\lambda_i = \frac{h_i}{d}, \tag{12}$$

where d is the **difficulty of the puzzle**.

Let $\widetilde{t}_i$ be miner i's **waiting time** for solving the puzzle. Then, $\widetilde{t}_i$ is an exponentially distributed random variable with parameter λ_i.

Moreover, the **expected waiting time for miner** i is

$$E[\widetilde{t}_i] = \frac{1}{\lambda_i} = \frac{d}{h_i}. \tag{13}$$

Bitcoin mining as a contest (14)

Waiting time for the market

The time of the first solution in the market is $\widetilde{t} = \min(\widetilde{t}_1, \widetilde{t}_2)$.

Let's assume that individual waiting times $\widetilde{t}_1$ and $\widetilde{t}_2$ are stochastically independent.

Then, $\widetilde{t}$ is likewise exponentially distributed because, for any $t \geq 0$,

$$\begin{aligned} \text{prob}\{\widetilde{t} \leq t\} &= 1 - (1 - F_1(t))(1 - F_2(t)) && (14) \\ &= 1 - \exp(-\lambda_1 t)\exp(-\lambda_2 t) && (15) \\ &= 1 - \exp(-(\lambda_1 + \lambda_2)t). && (16) \end{aligned}$$

Bitcoin mining as a contest (15)

Parameters

For the computation above, the parameter of the exponential distribution underlying $E[\widetilde{t}]$ has the parameter $\lambda = h/d$, where $h = h_1 + h_2$.

Moreover, the **expected waiting time for the market** is

$$E[\widetilde{t}] = \frac{1}{\lambda} = \frac{d}{h}. \tag{17}$$

Note: The parameter d is adjusted by the protocol such that $E[\widetilde{t}] = T$ (e.g., in the case of bitcoin, $T = 10$ minutes).

Bitcoin mining as a contest (16)

Two-stage game

Stage 1. Miners simultaneously and independently choose hash rates h_1 and h_2.

Stage 2. The protocol endogenously adjusts the difficulty level d such that

$$\frac{d}{h} = 10 \text{ minutes.} \tag{18}$$

Therefore, **miner i's profit** in any time interval of expected length T starting after the discovery of the previous block is

$$\Pi_i(h_1, h_2) = \begin{cases} R - c \cdot h_i & \text{if } i \text{ is first to solve the puzzle} \\ -c \cdot h_i & \text{if } i \text{ is not first to solve the puzzle.} \end{cases} \tag{19}$$

Bitcoin mining as a contest (17)

Property of the Poisson process

The probability for miner 1 to solve the problem is given as

$$
\begin{aligned}
p_1 &= \int_0^\infty f_1(t)(1 - F_2(t))dt && (20)\\
&= \int_0^\infty \lambda_1 \exp(-\lambda_1 t) \exp(-\lambda_2 t)dt && (21)\\
&= \lambda_1 \int_0^\infty \exp(-(\lambda_1 + \lambda_2)t)dt && (22)\\
&= \frac{\lambda_1}{\lambda_1 + \lambda_2}. && (23)
\end{aligned}
$$

Lemma 2. *Miner 1's probability of winning equals*

$$p_1 = \frac{\lambda_1}{\lambda_1 + \lambda_2}. \quad (24)$$

Bitcoin mining as a contest (18)

Contest success function

Note that

$$\frac{\lambda_1}{\lambda_1 + \lambda_2} = \frac{h_1/d}{h_1/d + h_2/d} = \frac{h_1}{h_1 + h_2}. \tag{25}$$

Therefore, regardless of d, the ratios

$$p_1 = \frac{h_1}{h_1 + h_2} \tag{26}$$

$$p_2 = \frac{h_2}{h_1 + h_2} \tag{27}$$

represent the probabilities that miners 1 and 2, respectively, will be first in solving the puzzle.

Bitcoin mining as a contest (19)

The miner's profit

Therefore, **miner i's expected profit** is

$$E[\Pi_i] = \frac{h_i}{h_1 + h_2} R - c_i h_i \qquad (i \in \{1, 2\}), \tag{28}$$

where the ratio is interpreted as zero if $h_1 = h_2 = 0$.

Bitcoin mining as a contest (20)

Exploiting first-order conditions

Maximization of miner 1's expected profit with respect to h_1 leads to the **first-order condition**

$$\frac{Rh_2}{(h_1 + h_2)^2} = c. \tag{29}$$

We focus on symmetric equilibria. Thus,

$$h_1 = h_2. \tag{30}$$

Then

$$\frac{R}{4h_1} = c \tag{31}$$

$$\Rightarrow \quad h_1^* = h_2^* = \frac{R}{4c}. \tag{32}$$

Bitcoin mining as a contest (21)

Nash equilibrium

Proposition 1. *The unique Nash equilibrium of the mining game with homogeneous costs is given by*

$$h_1^* = h_2^* = \frac{R}{4c}. \tag{33}$$

Comparative statics: The hash power (energy consumption, CO_2 footprint)

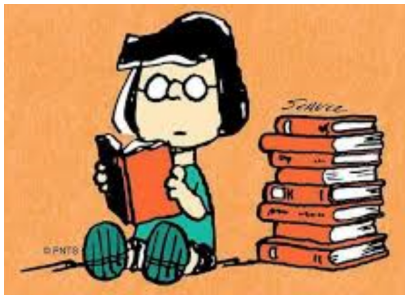
- increases strictly in the reward R,
- declines with marginal costs of mining c (i.e., Pigouvian taxation would be desirable).

Bitcoin mining as a contest (22)

Bibliographic notes

This lecture is based on the recent **game-theoretic literature on blockchain economics**. This literature studies the **economic incentives and competitive behavior** of blockchain users.

Our model of bitcoin mining follows **Dimitri (2017)**.



Houy (2016) considered a similar model, allowing for endogenous block size.

Bitcoin mining as a contest (23)

References

Dimitri, N. (2017), Bitcoin mining as a contest, *Ledger* **2**, 31-37.

Houy, N. (2016), The Bitcoin mining game, *Ledger* **1**, 53-68.

Nash, J. (1950). Equilibrium points in *n*-person games. *Proceedings of the National Academy of Sciences* **36**, 48-49.

Nash, J. (1951). Non-cooperative games, *Annals of Mathematics* **54**, 286-295.

von Neumann, J., Morgenstern, O. (1945). *Theory of Games and Economic Behavior*.