Smart Contracts and Blockchain Technology

Lecture 1. Introduction and overview

Christian Ewerhart

University of Zurich

Fall 2022

Copyright © 2022, Christian Ewerhart.

All rights reserved.

Without permission of the author, it is not allowed to distribute this script or parts of it.

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...

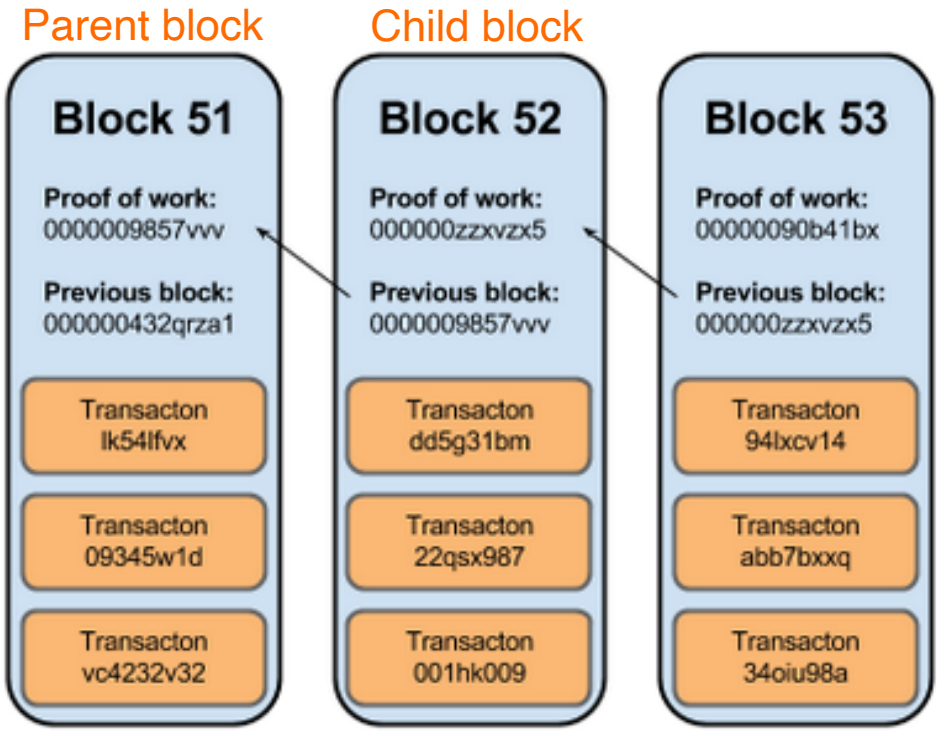
- ...consists of a heap of **blocks** (essentially linear and starting from a "genesis block"),...

...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").

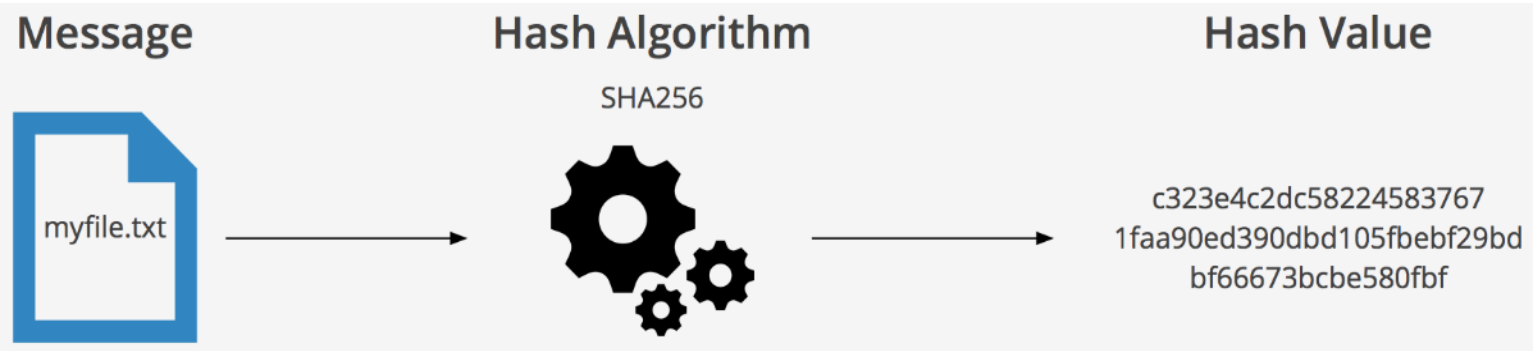
Economics of blockchain (5)

Understanding the miner's problem

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

Hexadecimal numers:
- digits -> 0, 1, 2, 3, 4, …, a, b, c, d, …

0x = prefix for a hexadecimal number
-> 0xb = 11



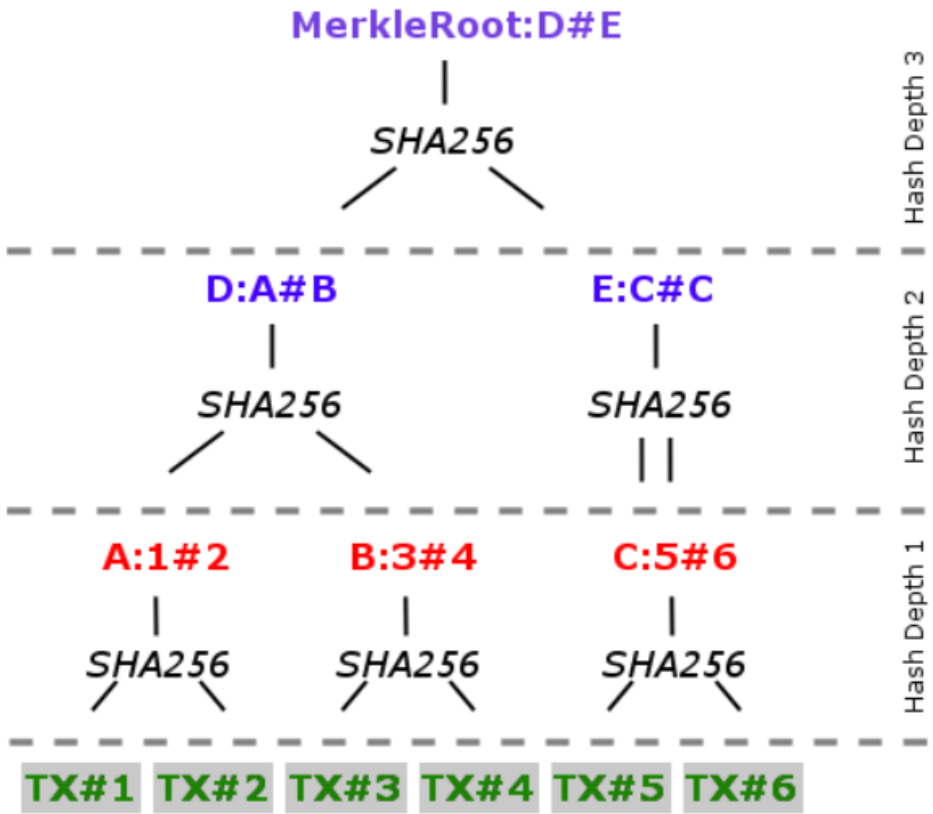
The algorithm is **deterministic** and computationally **non-invertible**.

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**.

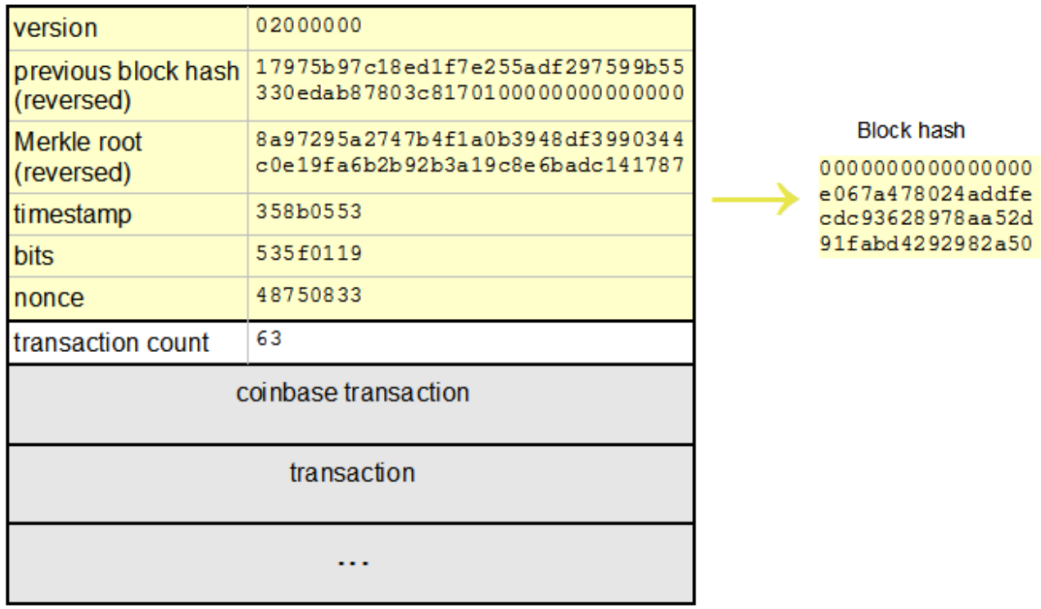
Size	Field	Description
4 bytes	Version	The Bitcoin Version Number
32 bytes	Previous Block Hash	The previous block header hash
32 bytes	Merkle Root	A hash of the root of the merkle tree of this block's transactions
4 bytes	Timestamp	The timestamp of the block in UNIX.
4 bytes	Difficulty Target	The difficulty 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

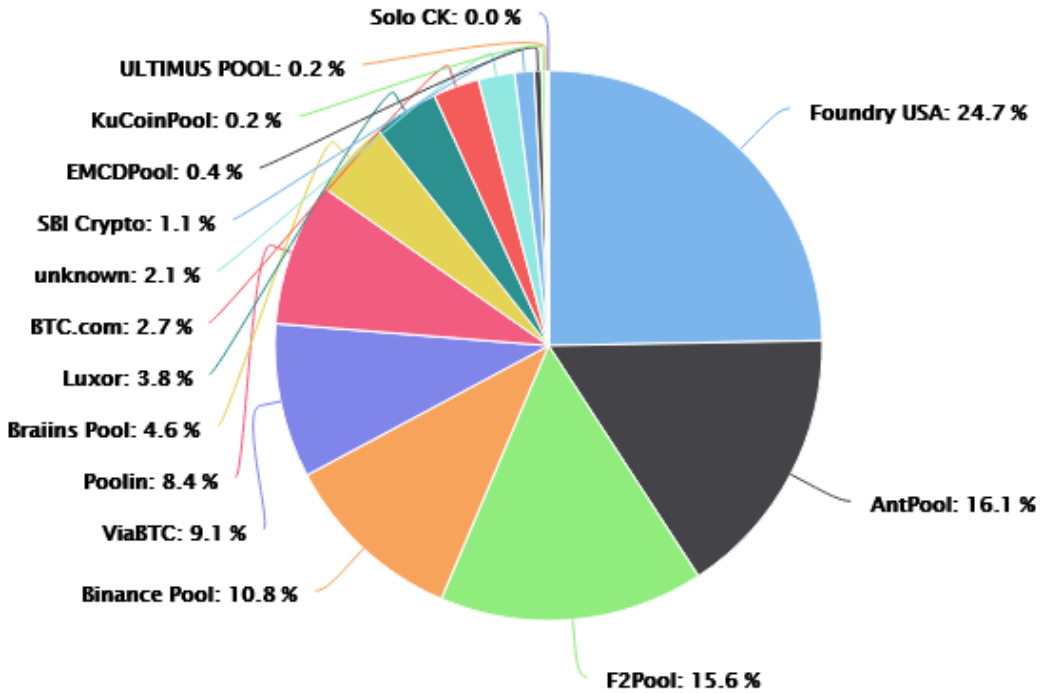
Height	Age	Transactions	Mined by	Size
541912	16 minutes ago	2331	SlushPool	959888
541911	20 minutes ago	2895		917302
541910	31 minutes ago	1754	AntMiner	922638

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

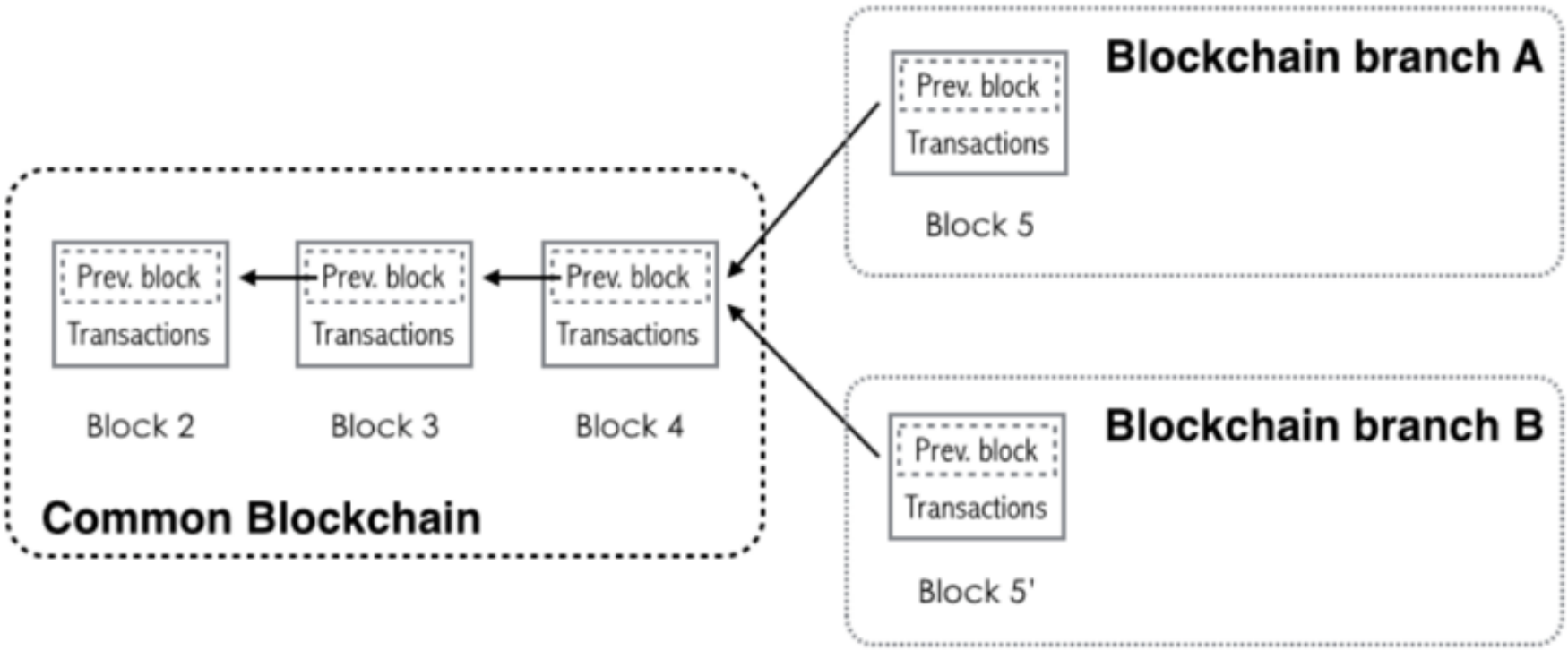
Mining power distribution as of August-September 2022:[5]



[5] Source: BTC.com

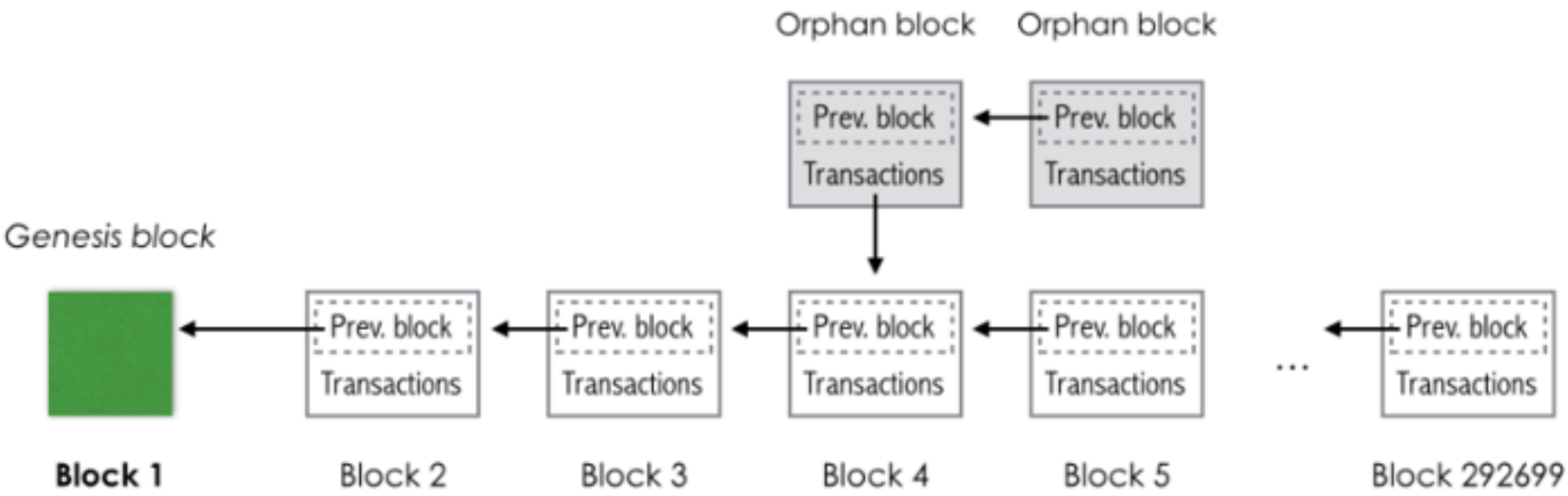
Economics of blockchain (11)

Forking



Economics of blockchain (12)

Orphan blocks



Economics of blockchain (13)

Some figures

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

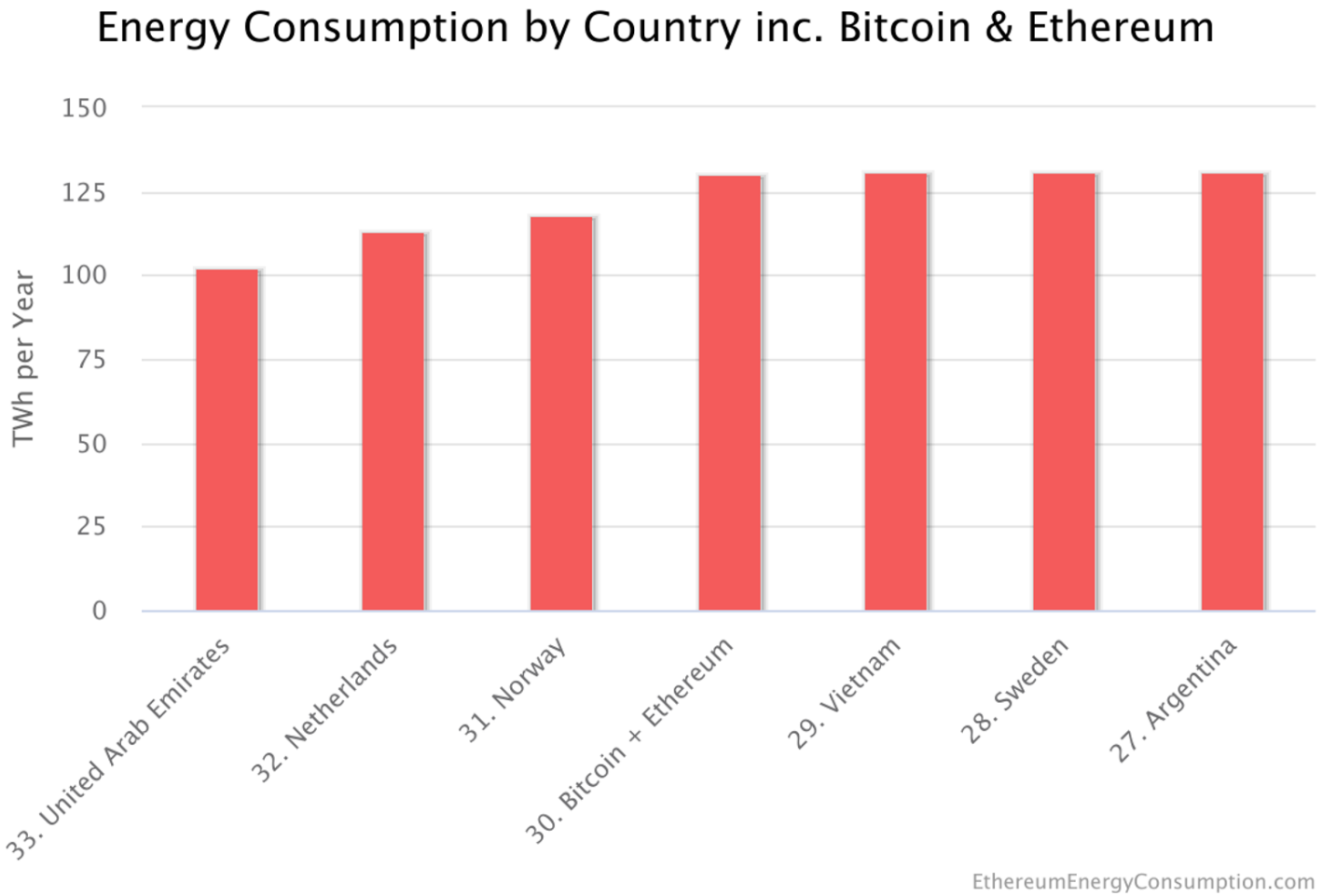
Hypes in December 2017 and December 2021...

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

[6] Source: coinmarketcap.com

Economics of blockchain (14)

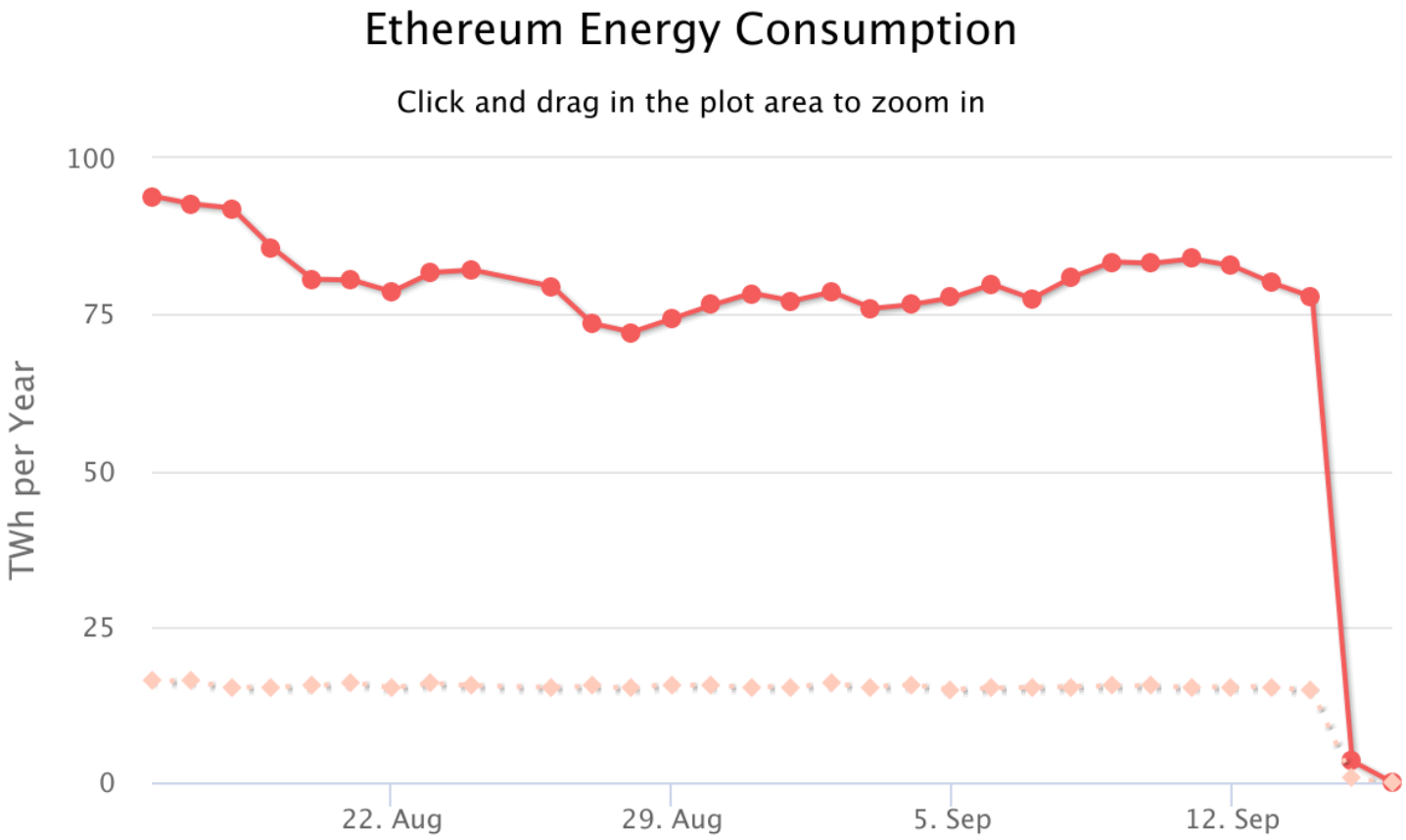
Energy consumption



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).

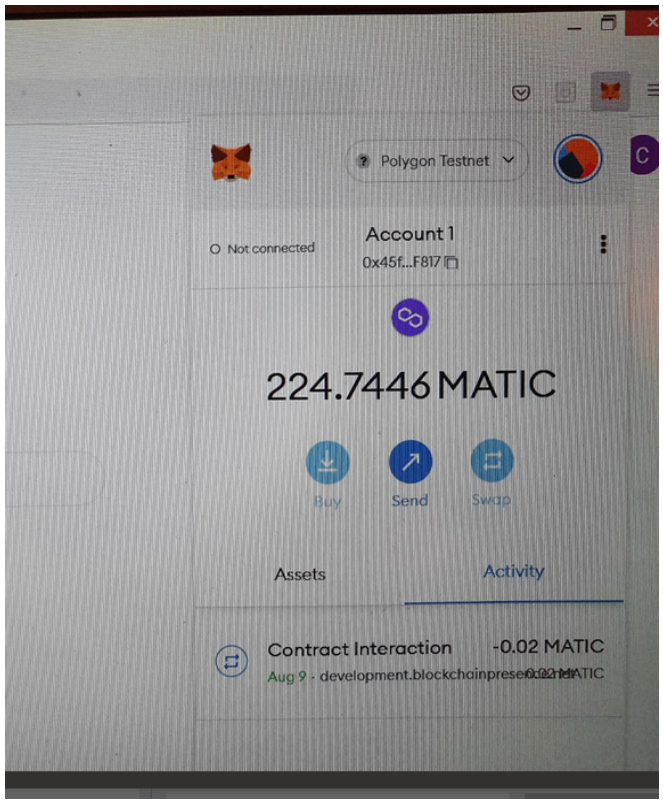
Then, your major problem would be the so-called **double-spending problem**: How do you make sure that the same amount is not used twice?

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!