E333 Blockchain and Cryptocurrencies – A Hands-On Lecture

Lecture 5

Ethereum and Smart Contracts

Christian Manger
University of Tübingen
Winter Semester 2026/27

What Is Ethereum?

What Is Ethereum?

Bitcoin

- Trustless validation and distributed storage of **transaction data**
- Its scripting language is deliberately limited

Ethereum

- Trustless validation and distributed storage **and processing** of data and logic
- Anyone can upload a program that everybody can use

A "world computer"

Ethereum is one shared computer that nobody owns: decentralized, censorship-resistant and paid for by its users. Launched in 2015, its native coin is **ether** (ETH).

Ether in Numbers

	Ether (ETH)	Bitcoin (BTC)
Price	ca. 1,800 USD	ca. 64,600 USD
Coins in circulation	ca. 122 million	ca. 20 million
Market capitalization	ca. 220 billion USD	ca. 1,300 billion USD
Maximum supply	none	21 million

- Ether is the second-largest cryptocurrency after Bitcoin
- Prices change quickly: check coingecko.com for today's numbers

Source: CoinGecko, 15 November 2026, rounded

Ethereum and Bitcoin Compared

	Bitcoin	**Ethereum**
Built-in coin	bitcoin (BTC)	ether (ETH)
Chain of blocks	linked by hashes	linked by hashes
Access	public and permissionless	public and permissionless
Consensus	proof of work	proof of stake (since 2022)
Block time	about 10 minutes	12 seconds
Bookkeeping	UTXOs	accounts
Programs	simple scripts	general smart contracts

The Merge

In September 2022, Ethereum switched from **proof of work** to **proof of stake**:

- Validators lock (“stake”) 32 ETH
- A random validator proposes the next block, others check and vote
- Validators who cheat lose part of their stake (“slashing”)
- Energy use fell by more than 99.9 %

More on proof of stake in Lecture 9.

Discussion

- Is proof of stake less “democratic” than proof of work?
- Do a few large staking providers control too much?
- But proof of work needs expensive, specialized hardware

Smart Contracts

A **smart contract** is a program that lives on the blockchain:

- Its code is stored in the chain and copied to every node
- Every node runs it in the same environment, the **Ethereum Virtual Machine** (EVM)
- It is started by a transaction, often one that also sends coins or tokens
- Once deployed, nobody can secretly change it

EVM chains

Many other chains run the same EVM, for example Polygon. Your MetaMask address works on all of them.

Not really "smart"

A smart contract does exactly what its code says, including its bugs.

Smart Contracts in Action

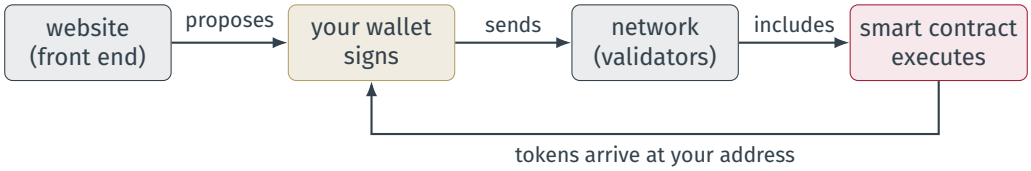
Decentralized Exchanges

- A **decentralized exchange** (DEX) lets you swap one token for another
- There is no company in between: a smart contract holds the tokens and sets the price
- The price comes from an **automated market maker** (Lecture 7)
- The largest DEX is **Uniswap**. It runs on Ethereum and on many EVM chains, including Polygon

The website is not the exchange

app.uniswap.org is only a front end. It prepares a transaction, your wallet signs it, and the smart contract on the chain executes it.

What Happens When You Swap



Read before you sign

The website can propose any transaction, including one that empties your wallet. Check what your wallet shows you: the network, the amount and what you allow the contract to do.

Your First Swap

Swap 0.2 POL for USDC

1. Type app.uniswap.org yourself (no links from search ads or messages)
2. Connect MetaMask and choose the **Polygon** network
3. Sell 0.2 POL, buy **USDC**
4. Check the token: native USDC on Polygon ends in `...3359`
5. Look at the quote: price, fee and minimum amount you will receive
6. Confirm in MetaMask and wait a few seconds

Keep at least 4 POL: you need them for Lecture 6.

Find Your Swap on the Chain

On polygonscan.com

1. Search for your address
2. Open your swap transaction
3. Find: the contract you interacted with, the tokens that moved, the gas used and the fee in POL

Question

Your transaction went to a contract, but the USDC came from somewhere else. Why?

Question

If USDC does not show up in MetaMask, why is it still yours?

NFTs Use Smart Contracts

- An NFT collection is a smart contract that records who owns which token
- Example: **Twin Tigers**, the Azuki jacket NFT on Ethereum: token 1 = jacket not yet redeemed, token 2 = redeemed
- On etherscan.io, the tab “Contract” shows its source code
- Anyone can read the code and call functions such as `balanceOf(address, 1)`

Look it up

Open the Twin Tigers contract on etherscan.io and find the function `redeemJacketToken` in `Tiger.sol`. What happens to your token when you redeem a jacket?

See the jacket on opensea.io. More on NFTs in Lecture 10.

Accounts

Two Types of Accounts

	Externally owned account (EOA)	**Contract account**
Controlled by	a private key	its code
Has code	no (except with EIP-7702, see below)	yes
Can start a transaction	yes	no, only react to one
Example	your MetaMask address	Uniswap, Twin Tigers, USDC

- Both have an address starting with `0x` and a balance in ETH
- Whoever has the private key of an EOA can do anything with it, everybody else nothing

The Nonce Again

- Every Ethereum account counts its transactions: 0, 1, 2, …
- Each transaction must carry the next number, called the **nonce**
- This prevents the same signed transaction from being sent twice
- It is the sequence number you know from NeckarCoin and from Lecture 4

Same word, different thing

In Bitcoin mining (Lecture 3), the nonce was the number miners change to find a valid hash. On Ethereum, the nonce of an account is a counter.

Smart Accounts

The problem

- An EOA has one key and no rules: lose it and everything is gone
- You always need ETH for gas

Account abstraction

- **ERC-4337** (2023): wallets that are smart contracts
- **EIP-7702** (2025): an existing EOA can use smart contract code

What smart accounts can do

- Log in with a fingerprint or passkey
- Recover access through friends or a second device
- Spending limits
- Several actions in one transaction
- Someone else pays the gas

Gas

Gas

- Bitcoin: the fee depends on the size of a transaction
- Ethereum: the fee depends on the **computation** a transaction needs
- Every step of the EVM costs **gas**: simple steps little, storing data a lot
- Gas is paid in ETH (on Polygon: in POL)

Transaction	Gas
Send ETH	21,000
Swap on a DEX	ca. 150,000
Deploy a token	ca. 1,000,000+

Why gas?

A program could run forever. Gas puts a price on every step, so every transaction ends and nobody can block the world computer for free.

How Gas Works

When you send a transaction, your wallet sets

- a **gas limit**: the most gas you allow it to use
- a **gas price**: what you pay per unit of gas, in gwei (1 gwei $= 10^{-9}$ ETH)

$$\text{fee} = \text{gas used} \times \text{gas price}$$

Example

Sending ETH at 0.3 gwei: $21{,}000 \times 0.3$ gwei $= 6{,}300$ gwei $= 0.0000063$ ETH, about 1 cent.

- If the gas runs out, the transaction fails, but the gas used is still paid
- Current prices: etherscan.io/gastracker, polygonscan.com/gastracker

How Many Transactions Fit in a Block?

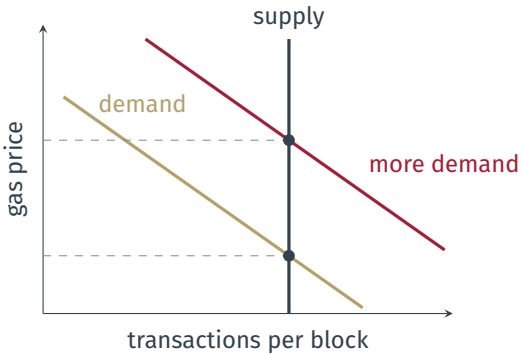
- A new block every **12 seconds**
- Each block may use at most **60 million gas** (the gas limit, raised from 30 million in 2025)
- An average transaction uses about 95,000 gas

at most: $\dfrac{60{,}000{,}000 \text{ gas}}{95{,}000 \text{ gas per tx}} \approx 630 \text{ tx per block} \quad \Rightarrow \quad \dfrac{630}{12 \text{ s}} \approx 50 \text{ tx per second}$

In reality

On average, blocks are only half full: EIP-1559 steers them towards half the gas limit (more on this soon). In one hour on 16 November 2026: about 330 transactions per block, or 27 per second – Visa handles thousands.

Gas Wars



- The space in a block is fixed: supply is **inelastic**
- If demand rises, only the price can adjust
- In 2021, popular NFT sales pushed single fees above 100 USD

Today

Higher gas limits and layer 2 chains have made fees on Ethereum very low. Polygon is even cheaper.

EIP-1559 and the Supply of Ether

EIP-1559: Burning Fees

- Introduced in August 2021 by the **London** hard fork
- Hard fork: all nodes must update their software to stay in the network
- EIP stands for Ethereum Improvement Proposal

The fee has two parts

- **Base fee**: set by the protocol and **burned**
- **Priority fee** (tip): goes to the validator

The base fee adjusts

- Target: half of the gas limit
- Block fuller than target: base fee rises by up to 12.5 %
- Block emptier: base fee falls

Why burn?

Fees become predictable, and every user's fee benefits all holders of ETH: burned coins reduce the supply.

“Ultrasound Money”?

- New ETH is created as a reward for validators
- Burned ETH is destroyed
- After the Merge, issuance fell sharply. In busy times, more ETH was burned than created
- From 2022 to early 2024, the supply even **fell**, from about 120.5 to about 120 million

The story

Fans called ether “ultrasound money”: not only limited like Bitcoin (“sound money”), but shrinking. See ultrasound.money.

Why the Burn Collapsed

- In March 2024, the **Dencun** upgrade made data for layer 2 chains much cheaper (“blobs”)
- Much activity moved to layer 2 chains
- Less demand for block space ⇒ low base fee ⇒ little burned
- In 2026, the burn offsets only about 2 % of new issuance

Time	Supply (ETH)
Merge, Sept. 2022	ca. 120.5 million
Low, early 2024	ca. 120.0 million
November 2026	ca. 122.4 million

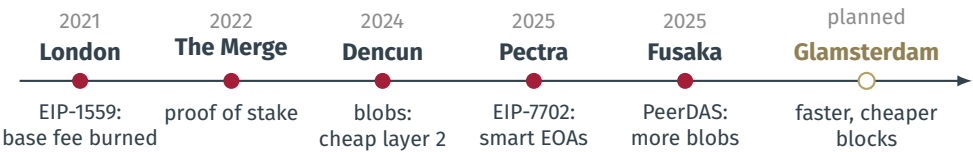
Discussion

The supply now grows by roughly 0.8 % per year. Is cheap block space good or bad for holders of ETH?

Source: ultrasound.money, etherscan.io, CoinGecko; rounded, estimates differ

How Ethereum Changes

Ethereum Upgrades



- Upgrades are hard forks: developers propose, node operators decide to install
- Each upgrade is first tested on test networks such as Sepolia

What Comes Next: Glamsterdam

- **Enshrined proposer-builder separation** (ePBS): building a block and proposing it become separate roles in the protocol
- **Block-level access lists**: a block says in advance which accounts it touches, so nodes can process transactions in parallel
- Goal: higher gas limits, more transactions, lower fees

Status (15 November 2026)

Live on the test network Sepolia since October 2026. A date for the main network has not been set yet.

Summary

Summary

Concept	Key idea
Smart contract	Program on the blockchain, run by every node in the EVM
DEX	Smart contract that swaps tokens, the website is only a front end
Accounts	EOAs (private key) and contract accounts (code), each with a nonce
Gas	Price for computation, fee $=$ gas used $\times$ gas price
EIP-1559	Base fee is burned, priority fee goes to the validator
Supply of ether	No cap, currently growing slowly, burn depends on demand

Next Week

Lecture 6: Create Your Own Token

- What is a token standard (ERC-20)?
- We write and deploy our own token
- We trade it on a DEX

Please prepare

Bring a computer (not a smartphone) with MetaMask and keep at least 4 POL in your wallet.