



OST

Eastern Switzerland
University of Applied Sciences

Blockchain (BlCh)

Tokens, Stablecoins, NFTs

Thomas Bocek

02.10.2026

Learning Goals

- Lecture 5
 - Knowledge
 - Difference between fungible and non-fungible tokens
 - How stablecoins are backed, and why some failed
 - Application
 - Choose the right token type for a use case
 - Design token metadata and URIs
 - Know the ERC-20 pitfalls before using a token (CT: x402 with stablecoins)

Fungible vs. Non-Fungible

- **Explanation:** “Fungible tokens or assets are divisible and non-unique. For instance, fiat currencies like the dollar are fungible: A \$1 bill in New York City has the same value as a \$1 bill in Miami. A fungible token can also be a cryptocurrency like Bitcoin: 1 BTC is worth 1 BTC, no matter where it is issued.”
- 3 characteristics
 - Interchangeability
 - With other tokens of the same type
 - Divisibility
 - Into smaller units
 - Standardization
 - High degree of standardization and uniformity
- Non-fungible: every token unique, not divisible (ERC-721)
- Native vs. non-native
 - Native tokens: Built into blockchain protocol (Bitcoin, Ether)
 - Used directly for transaction fees / pays gas
 - Core part of blockchain infrastructure
 - Non-native tokens: Created via smart contracts (USDC, USDT, OST token)
 - Require smart contract interaction / needs gas
 - Unless: EIP-3009 (last lecture), ERC-4337 paymaster (CT HS2025)

Cryptocurrencies and Token Types

- Cryptocurrencies are fungible tokens
 - Digital currency not reliant on a central authority
 - CBDC is digital currency backed by central authority
 - “In contrast to cryptocurrencies, a central bank digital currency would be centrally controlled”
- 6 conditions (by Jan Lansky)
 - 1) The system does not require a central authority, distributed achieve consensus on its state.
 - 2) The system keeps an overview of cryptocurrency units and their ownership.
 - 3) The system defines whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the circumstances of their origin and how to determine the ownership of these new units.
 - 4) Ownership of cryptocurrency units can be proved exclusively cryptographically.
 - 5) The system allows transactions to be performed in which ownership of the cryptographic units is changed. A transaction statement can only be issued by an entity proving the current ownership of these units.
 - 6) If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them.
- Exchange cryptocurrencies
 - Decentralized exchanges (DEX) – same chain/cross chain, centralized exchanges (CEX)

Fungible Tokens: Applications and Regulatory Context

- Many types of tokens
 - Stablecoins
 - Pegged to [fiat money](#), e.g., USDC, XCHF
 - Gas for smart contracts
 - Use to execute smart contracts
 - Altcoins
 - Non mainstream coins (aka sh*tcoins), definition is vague
- Swiss [DLT law](#), since 01.08.2021
 - Licence for DLT trading facilities
 - Electronic registers
- [Finma](#) categorization (payment, utility and asset tokens):
 - Payment Tokens: Pure cryptocurrencies (no securities regulation)
 - Utility Tokens: Access to services (lighter regulation if genuine utility)
 - Asset Tokens: Represent real assets (full securities regulation applies)
 - Prospectus requirement
 - No-Action Letter: couple of months, provides regulatory clarity

FT / Tokens / ERC-20

- ERC-20

- Token contract keeps track of fungible tokens
- Can be used as vault for NFTs

- Optional (highly recommended)

- `function name() public view returns (string)`
- `function symbol() public view returns (string)`
- `function decimals() public view returns (uint8)`

- Events

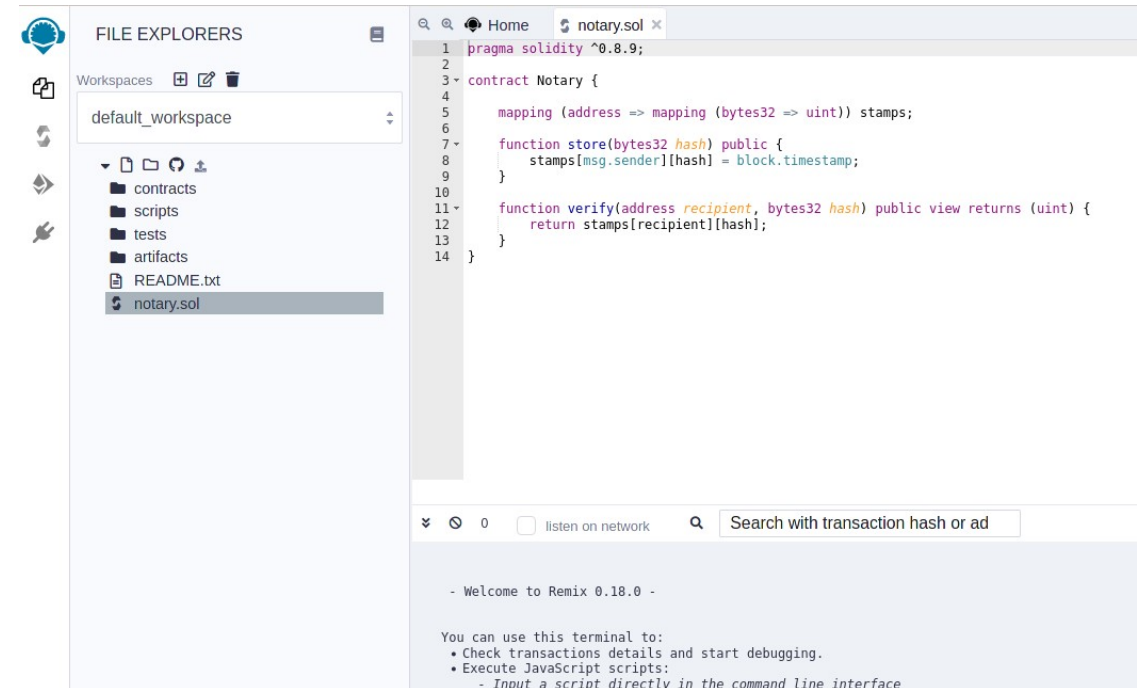
- `event Transfer(address indexed _from, address indexed _to, uint256 _value)`
- `event Approval(address indexed _owner, address indexed _spender, uint256 _value)`

- Mandatory

- `function totalSupply() public view returns (uint256)`
- `function balanceOf(address _owner) public view returns (uint256 balance)`
- `function transfer(address _to, uint256 _value) public returns (bool success)`
 - Direct token transfer from your address
- `function transferFrom(address _from, address _to, uint256 _value) public returns (bool success)`
 - Allows third party (e.g., DEX) to transfer tokens on your behalf after approval
- `function approve(address _spender, uint256 _value) public returns (bool success)`
 - Grants permission for transferFrom operations
- `function allowance(address _owner, address _spender) public view returns (uint256 remaining)`

ERC-20 Implementation

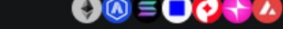
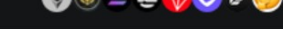
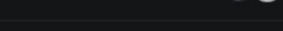
- [OpenZeppelin](#) – many default contracts, very good source
 - Let's implement a simple ERC20 and deploy on testnet
 - [Remix IDE](#)
- Pitfalls: Two transactions: approve, then transferFrom
 - User needs ETH, twice
- Signature instead of approve
 - EIP-2612 permit: signed allowance
 - EIP-3009 transferWithAuthorization: signed transfer (USDC, USDT0 → x402)
 - Permit2 (Uniswap): one approve, then signatures for every token
- Not every "ERC-20" is ERC-20
 - USDT (Ethereum, 2017): transfer returns nothing → OpenZeppelin SafeERC20
 - Decimals: 1 USDC = 10^6 , 1 ETH = 10^{18}



Introduction to Stablecoins

- “Stablecoins are cryptocurrencies where the price is designed to be pegged to a reference asset.” [\[link\]](#)
- Collateralization: how to back the stablecoin
 - Fiat money (USD, EUR)
 - Asset-backed (e.g., gold)
 - Crypto-Collateralized
 - Crypto asset backed stablecoins (decentralization)
 - Algorithmic stablecoins (probably don’t work)

- Reasons for stablecoins
 - Cryptocurrencies have high volatility
 - Payment in “real world” still with fiat
- Market Cap [\[link\]](#)

1	 Tether (USDT)	 +122	\$183.778b
2	 USD Coin (USDC)	 +149	\$74.134b
3	 Sky Dollar (USDS)		\$6.689b
4	 Ethena USDe (USDe)	 +23	\$4.866b
5	 Dai (DAI)	 +41	\$4.784b
6	 World Liberty Financial USD (US...)		\$4.432b
7	 Global Dollar (USDG)		\$3.089b
8	 PayPal USD (PYUSD)	 +11	\$2.738b
9	 Circle USYC (USYC)		ⓘ \$2.404b
10	 Ripple USD (RLUSD)	 (x)	\$2.4b

History of Stablecoins

- Early Days of Stablecoins (2014-2017)
 - 2014: Tether (USDT) launched as first major stablecoin, 1:1 peg to the US dollar
 - 2015-2017: USDT gains traction, offering traders a “safe harbor” from volatility
- Growth and Evolution (2018-2019)
 - 2017-2018: USDT raises questions about transparency and reserve audits
 - 2018: MakerDAO launches DAI, first major decentralized, crypto-collateralized stablecoin. DAI gains popularity in the DeFi space
 - 2019: Facebook announces Libra, global stablecoin backed by basket of fiat currencies.
- Stablecoins in DeFi and Algorithmic Experiments (2020-2021)
 - 2020: Stablecoins gain popularity due to DeFi. USDC, DAI, BUSD gain significant market share
 - 2021: UST emerges as prominent algorithmic stablecoin. Rapid adoption but collapses in 2022 → major crisis in crypto market
- Recent Developments (2022-Present)
 - 2022: Collapse of UST shows risks of algorithmic stablecoins.
 - 2023: Increased regulatory pressure from global entities, EU and U.S. (e.g., [MiCA](#)) → improve transparency and compliance.
 - 2025: [GENIUS Act](#), first US stablecoin law
 - 2025: Swiss FinIA consultation, CHF stablecoin licence

Stablecoins Gone Wrong (1/2)

- Successful: USDT/USDC/DAI
- Epic fail: [Terra/UST](#)
 - Algorithmic: UST ↔ LUNA
 - UST < 1\$: burn 1 UST, mint 1\$ of LUNA
 - UST > 1\$: burn 1\$ of LUNA, mint 1 UST
 - Anchor Protocol: ~20% yield on UST
- May 2022: withdrawals → depeg → death spiral
 - Burn UST, mint LUNA → LUNA price collapses → no backing
 - ~40b USD lost
- Co-founder and CEO: [Do Kwon](#)
 - Arrested in Montenegro 03/2023
 - Handed over to the US 12/2024, pleaded guilty 08/2025
 - 15 years prison (12/2025)

Stablecoins Gone Wrong (2/2)

- Fail: [Binance](#) stopped BUSD
 - Collaboration with Paxos
 - [Paxos](#) ordered by the New York Department of Financial Services (NYDFS) to stop issuing BUSD
 - SEC threatened Paxos with legal action, claiming BUSD might be an unregistered security
 - Paxos / Binance halted BUSD, but without any loss of funds
- Role of [Changpeng Zhao](#) - not related to BUSD
- Fail: [Facebook/Libre/Diem](#)
 - Rise of L1 blockchains: Aptos und Sui
 - Common origins and shared codebase
 - Regulatory resistance and collapse of diem
 - Global opposition
 - International resistance
 - Outcome
 - Meta ultimately abandoned the Diem project
 - Continuation of Diem's Legacy
 - Aptos, Sui (mainnet), Linera (devnet)

Stablecoins in Switzerland

- Today: no own rules
 - Issuer owes you CHF → deposits → banking licence or bank guarantee
 - Fintech licence: max. CHF 100m, rarely used
- FinIA reform (consultation Oct 2025)
 - New licence "payment instrument institution"
 - 1:1 backed, redeemable at par, client funds separate, no interest
 - Not before 2027
- XCHF (Bitcoin Suisse, 2018)
 - Backed by CHF at a bank, issuer owes you 1 CHF
 - Stopped 2024
- ZCHF (Frankencoin, 2023) [[link](#)]
 - Backed by crypto, no issuer → no banking licence needed
 - Peg holds as long as **collateral** > ZCHF and weak positions are liquidated in time
 - But: nobody owes you 1 CHF, no redemption, but no value lost while the peg holds
 - ~31m CHF vs. ~305b USD whole market

Stablecoins

- Why would anyone use a stablecoin besides less volatility?
 - Borrowing / Lending with Stablecoins
 - Higher yield on stablecoins than on ETH
- Vault / liquidation
 - Collateral below threshold → auction
 - Debt + penalty covered, debt burned, rest to vault owner
 - Maker: 90 liquidation auctions between 8 and 12 May [\[link\]](#)
- PSM (Peg Stability Module): DAI/USDS ↔ USDC 1:1
 - Stabilizes the peg
 - But: DAI depends on USDC → March 2023 USDC depeg (SVB), DAI followed
 - Risk: every stablecoin is only as good as its collateral
- Stablecoin risks?
 - See UST

NFT

- Non-fungible token

▶ **fungible** *adj.* [LAW]

erplatzbar

- Unique token on a public blockchain
 - Guarantees that a digital asset is unique and not interchangeable
 - Can be any digital data that can be hashed (only hash is stored on-chain)
 - With NFT: proof of ownership (you can copy the digital data, but the ownership remains)
- NFT market place [OpenSea](#) - open to everyone, for any NFT



CryptoPunk #7523, sold for 11.8m USD [\[link\]](#)

NFT

- Also big players: [NBA](#)
- Market Evolution
 - 2021: Biggest NFT sale so far: Beeple sold for ~\$70m, [Everydays: the First 5000 Days](#)
 - Current: Post-boom consolidation
 - Shift from speculation to utility (tickets, gaming, authentication)
 - B.20 token case study
 - NFT (also Beeples) stored in B.20 vault, where artists are also participating – [conflict of interest?](#)
 - B.20 went up to 25\$, now down to [0.05\\$](#)
- Collectible media (football, basketball players), eg., video, Jack Dorsey sold first twitter post for [\\$2.9m](#)
- Tickets, every entry ticket is unique, keep ticket after events, fee for artist on reselling NFT ticket
- Artists [sell music](#) as NFT
- Memes: e.g., [disaster girl](#), [nyan cat](#)
- Fashion: add NFT token to make clothes unique ([sneakers](#))
- Source code: [Tim Berners Lee](#), \$5.4m
- No NFTs
 - Fan Tokens are not NFTs, e.g., PSG, FCB, [YB](#)
 - NFT items in [games](#), e.g., [CS:GO skins](#) (traded decentrally, but not an NFT)



Connect

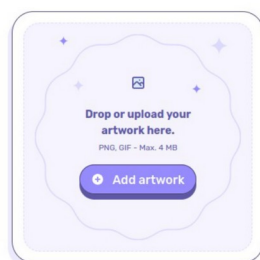
Make your memories live forever.

After minting, POAPs unlock a variety of experiences. From group chats to discounts, paint parties and more, POAPs keep the good times alive.

ERC-721

- Non-Fungible Token Standard
 - June 2018 - [ERC721](#) accepted as final
 - “There is either one NFT or there are none”
- Pros
 - P2P trading without intermediaries
 - Operates 24/7 on decentralized marketplaces (e.g., OpenSea)
 - Ownership history on-chain

Let's create your POAP.



Recommended for optimal performance:
500x500px, rounded shape, less than 200KB
Animated pngs are not supported. Use of gif format recommended.

POAP title *

Blockchain Lecture 23.10.2023

29/150

POAP description *

Embark on a transformative journey into the intricate world of blockchain with our distinguished lecturer, Thomas [Boczek](#). This [POAP](#) commemorates an enlightening session at [OST](#), where attendees delved deep into the ever-evolving landscape of decentralized systems, smart contracts, and the future of a [trustless](#) economy.

What makes this [POAP](#) special? It's not just a digital badge—it's a symbol of your passion for blockchain technology and your commitment to being at the forefront of digital innovation.

909/1500

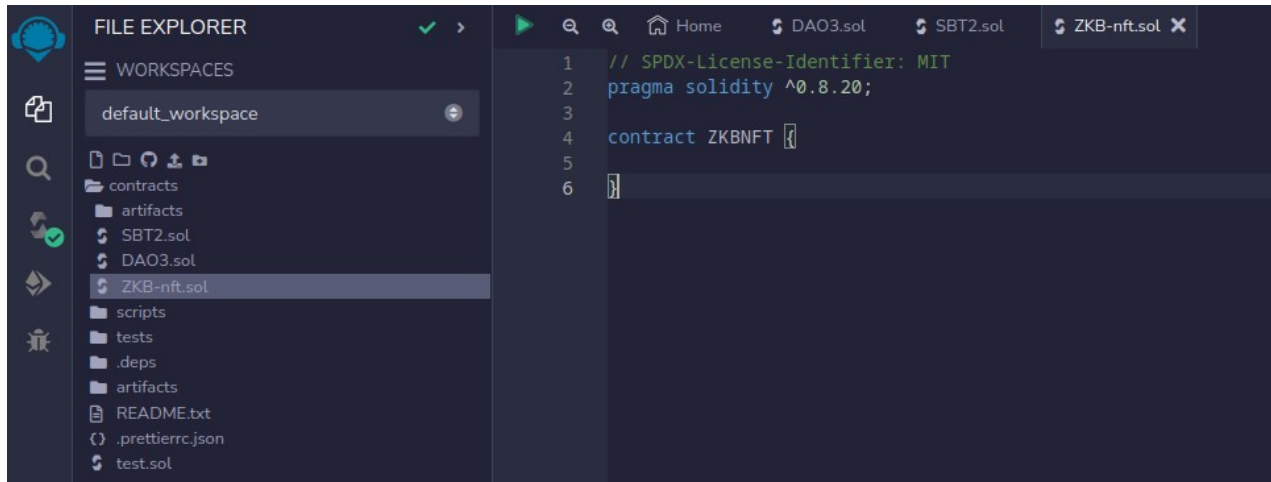
Website

[https:// dsi.lost.ch/lect/hs23/](https://dsi.lost.ch/lect/hs23/)

- Cons
 - More functions than ERC-20, more to get wrong
 - NFT ownership $\neq$ copyright
 - Rights stay with the creator unless explicitly transferred
 - Metadata usually off-chain
 - URL dies $\rightarrow$ NFT points to nothing
- [POAP](#) Event at OST [2023](#)
 - POAP shut down 08/2026: ~7.6m badges, no business model [\[link\]](#)
 - Good news: NFTs remain on-chain, metadata still online

NFT Implementation – Mandatory Interfaces und Events

- On Ethereum, [OpenZeppelin](#) has many standard implemented, for IDE [Remix](#) is a good choice
- Let's implement and deploy an NFT
- Metamask
 - Crypto wallet and gateway to blockchain apps, available as a browser extension



- We'll use that to connect the browser to the Ethereum network

Extensions

- Optional Enumaration - discoverable
 - `function totalSupply() external view returns (uint256);`
 - `function tokenByIndex(uint256 _index) external view returns (uint256);`
 - `function tokenOfOwnerByIndex(address _owner, uint256 _index) external view returns (uint256);`
- Mandatory ERC-165
 - `function supportsInterface(bytes4 interfaceID) external view returns (bool);`
 - `balanceOf(address) → 0x70a08231`
- Optional ERC721TokenReceiver
- Optional ERC721Metadata
- OpenSea
 - More metadata [here](#)
- ERC 1155
 - Supports fungible and non-fungible tokens in a single contract, reducing deployment costs and simplifying asset management
 - Enables batch transfers of multiple tokens in one transaction, ideal for mass distributions (e.g., game items)
 - But: complexity