OST
Eastern Switzerland
University of Applied Sciences

Blockchain (BlCh)

DeFi

Thomas Bocek

11.10.2025

Learning Goals

- Lecture 7
  - Knowledge
    - Explain the fundamental differences between TradFi, CeFi, and DeFi
    - Understand key DeFi properties: transparency, custody, atomicity, and regulatory challenges

Traditional / Centralized Finance (TradFi/CeFi)

- Traditional / Centralized finance (TradFi/CeFi) originally from ancient Mesopotamia
  - TradFi: Traditional banking (fiat, regulated banks)
  - CeFi: Blockchain trading with centralized entities (Binance, Kraken)
- Since then, many goods and assets as currency [link]
  - Cattle, cacao and coffee beans, shells, salt, precious metals
    - Gold standard era: universal acceptance as store of value
    - Fiat currencies (USD, CHF).
      - fiat („Es sei getan! Es geschehe! Es werde!“)

- “Clay tokens, described by some scholars as the world's first money, found in Susa, Iran have been dated to 3300 B.C.” [history]

- Evolution of money continues today [link]

Image Source: https://factsanddetails.com/world/cat56/sub363/item1514.html

OST

CeFi vs. DeFi - Key Features

- Traditional Finance: Centralized trust model
  - Currency backed by governments (fiat) or intrinsic value (assets)
  - Intermediaries manage and control financial transactions
  - Example: Swiss National Bank (SNB) guarantees CHF value
- DeFi: Trustless financial infrastructure
  - Blockchain enables transfer without trusted intermediaries
  - Smart contracts execute automatically, no third parties needed
  - Financial services built on transparency and code

- CeFi vs. DeFi – 3 key differences

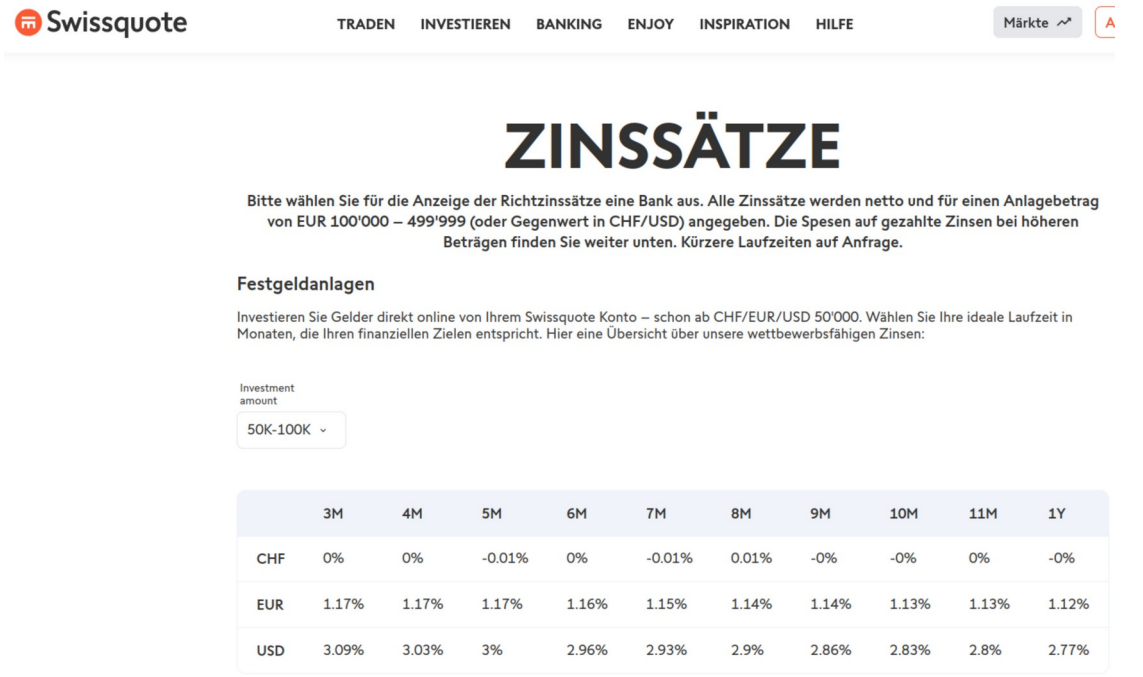
1) Transparency
   - DeFi: Public rules and protocols (e.g., Uniswap)
   - CeFi: Private agreements, closed systems
   - Anyone can verify smart contract code
2) Control
   - DeFi: Users control their own assets (non-custodial)
   - CeFi: Intermediaries hold assets (custodial)
   - No entity can freeze, censor, or confiscate in true DeFi
3) Accessibility
   - DeFi: Permissionless access with internet + wallet
   - Enables "unbanked" population (1.4B globally)
   - Reality: "First-World Problem" - requires technical knowledge, stable internet, and understanding of risks
   - Bridging accessibility gap: ongoing challenge

OST

High Risk, High Reward?

- DeFi Summer (2020-2021)
  - Token-incentivized pools: 100,000%+ APY (double investment in ~8 hours!)
  - Stablecoin pools: 100-999% APY
  - Reality: Unsustainable "death spirals" when farmers dumped tokens
- Why so high?
  - Token emission rewards + low liquidity + speculation frenzy
  - Floating rates tied to token price
- Today (2024-2025)
  - Aave USDT: ~2% APY vs. US Treasury: ~4-5%
  - Sustainable yields: 8-12% (down from triple digits)
- DeFi Innovation: Flash Loans
  - Borrow millions without collateral (repay in same tx)
  - Risk: yEarn hack $11M via flash loan exploit
  - Lesson: 100,000% APY = 100,000% risk

2025: https://www.swissquote.com/de-ch/private/trade/products/securities/money-markets



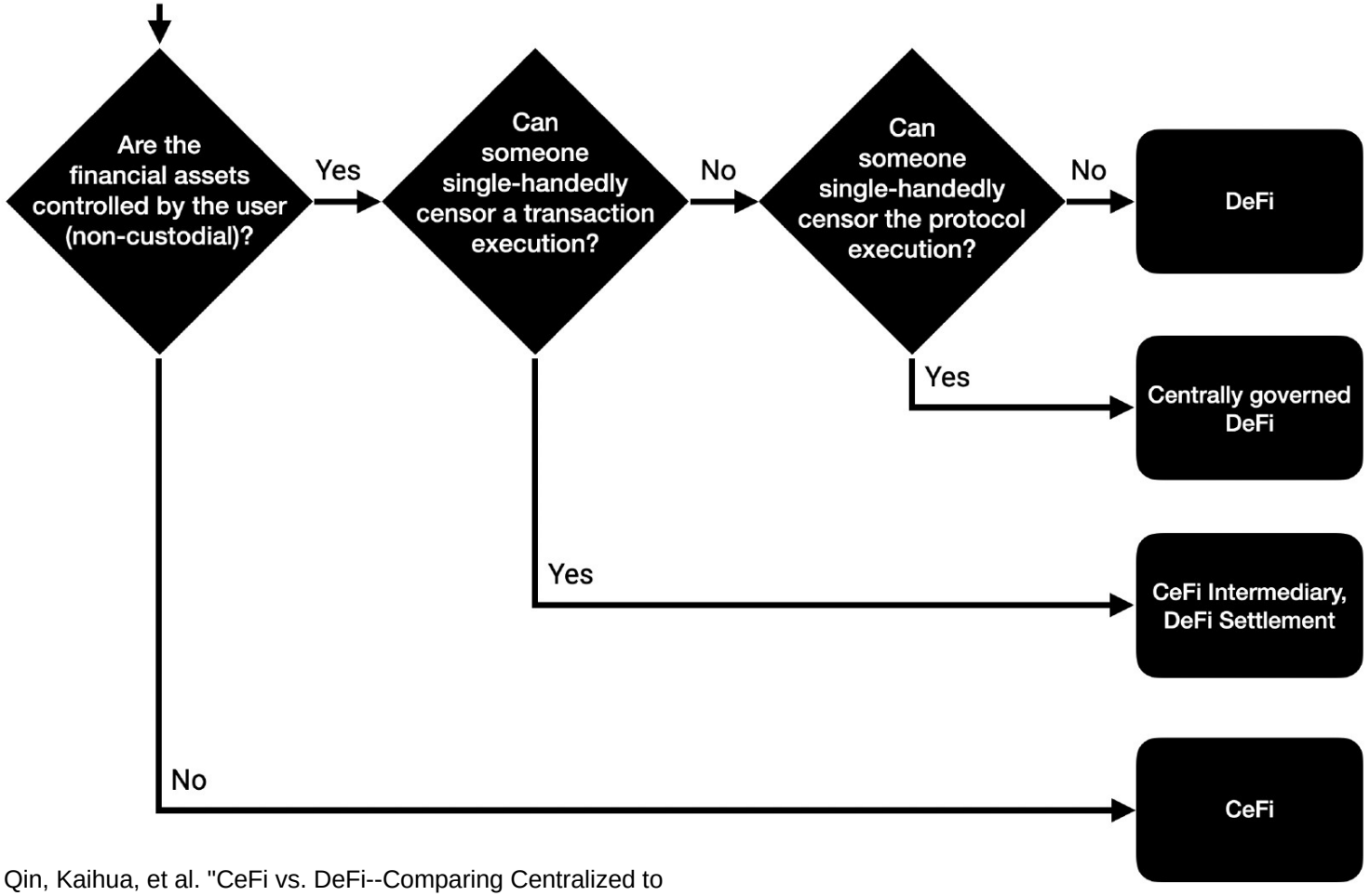
	3M	4M	5M	6M	7M	8M	9M	10M	11M	1Y
CHF	0%	0%	-0.01%	0%	-0.01%	0.01%	-0%	-0%	0%	-0%
EUR	1.17%	1.17%	1.17%	1.16%	1.15%	1.14%	1.14%	1.13%	1.13%	1.12%
USD	3.09%	3.03%	3%	2.96%	2.93%	2.9%	2.86%	2.83%	2.8%	2.77%

Asset	Total supplied	Supply APY	Total borrowed	Borrow APY, variable
USD Coin USDC	1.50B $1.50B	4.22%	1.31B $1.31B	5.38%
Tether USDT	1.69B $1.69B	4.02%	1.44B $1.44B	5.25%
Dai Stablecoin DAI	119.89M $119.86M	3.83%	109.79M $109.76M	5.63%
Rocket Pool Protocol RPL	570.99K $5.86M	3.82%	378.99K $3.89M	7.31%
Curve.Fi USD Stablecoin crvUSD	700.70K $699.83K	3.54%	525.33K $524.68K	5.29%
PayPal USD PYUSD	11.03M $11.02M	3.49%	8.71M $8.71M	5.58%
LUSD Stablecoin LUSD	3.96M $3.96M	3.45%	3.11M $3.11M	5.55%
Frax FRAX Isolated	798.25K $795.95K	2.80%	599.88K $598.15K	4.70%

2024: https://app.aave.com/markets/?marketName=proto_mainnet_v3

DeFi Decision Tree

- The boundaries of DeFi and CeFi not clear cut

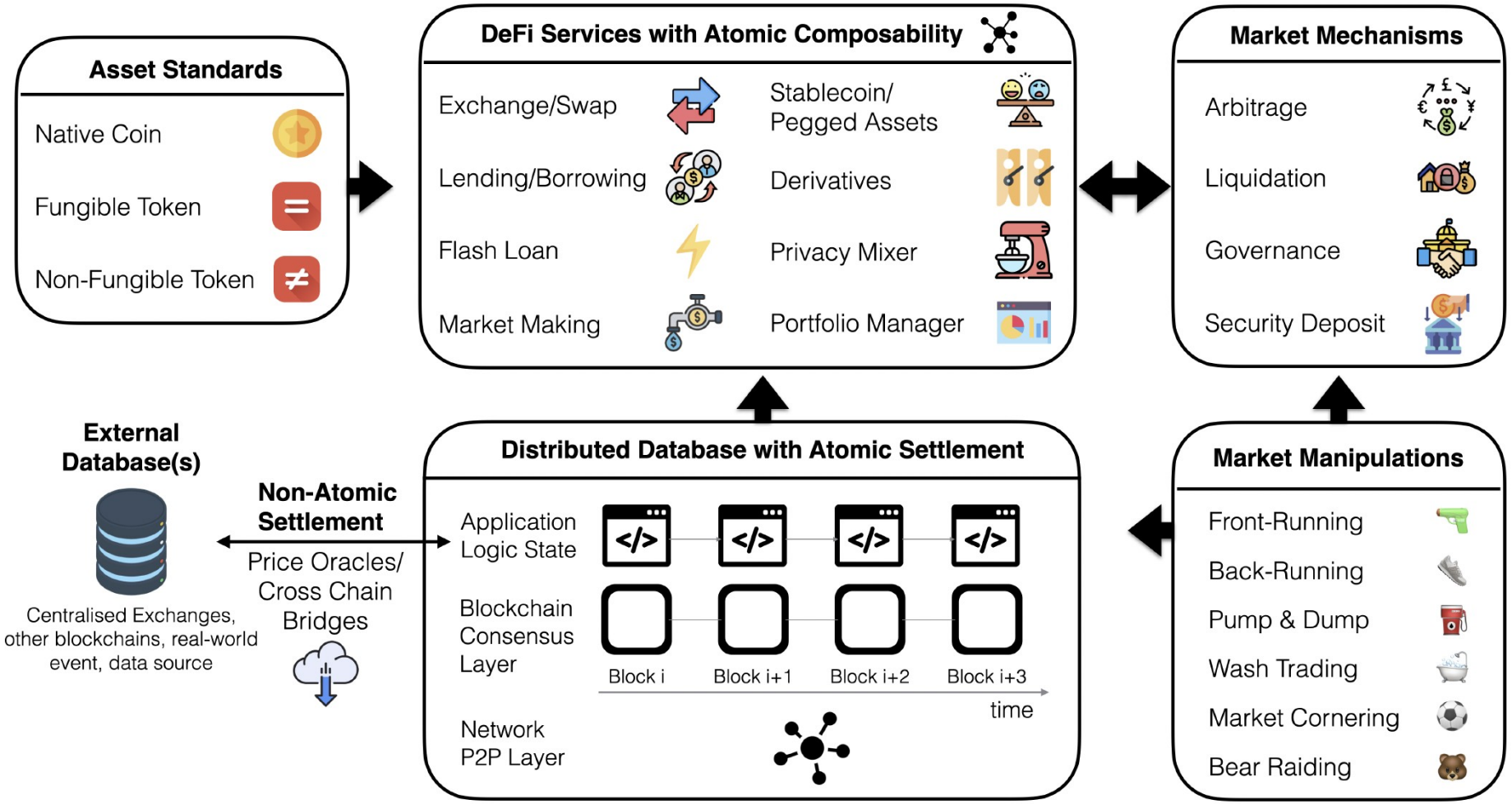


Qin, Kaihua, et al. "CeFi vs. DeFi--Comparing Centralized to Decentralized Finance." arXiv preprint arXiv:2106.08157 (2021). [link]

OST

Bear raid
Cornering the market

High-Level Systematization of DeFi



Qin, Kaihua, et al. "CeFi vs. DeFi--Comparing Centralized to Decentralized Finance." arXiv preprint arXiv:2106.08157 (2021). [link]

OST

Key DeFi Properties (1/3)

- Public Verifiability
  - Bytecode and execution publicly verifiable on blockchain
  - Anyone can audit smart contract code
  - Etherscan: "Verify and Publish Source Code"
  - Transparency builds trust, but doesn't guarantee security
- Custody (User Control)
  - DeFi: Users control their own assets (non-custodial)
  - CeFi: Bank/institution controls assets (custodial)
  - Unique Selling Point (USP): "Be your own bank"
  - BUT: User bears technical risks (smart contract bugs, lost keys)
  - No deposit insurance, no customer service

- Privacy: Pseudonymous, Not Anonymous
  - Public blockchains: All transactions visible
  - Addresses are pseudonymous (not linked to real identity)
  - BUT: Deanonymization possible through:

    → Transaction clustering (linking addresses)

    → KYC/AML at centralized exchanges (fiat on/off-ramps)

    → Blockchain analysis (Chainalysis, Elliptic)
  - Privacy coins (Monero): True anonymity, but rare in DeFi

OST

Key DeFi Properties (2/3)

- Atomicity: All-or-Nothing Transactions
  - Multiple operations in one transaction
  - Either all succeed, or all fail (rollback)
  - Example: Flash loan - borrow, trade, arbitrage, repay (all atomic)
  - CeFi equivalent: Costly legal agreements with slow settlement
- Execution Order Malleability (Transaction Ordering)
  - No central authority controls transaction order
  - Permissionless blockchains: Public mempool (pending transactions)
  - Validators/miners choose which transactions to include
  - Users bid with higher gas fees for priority
- MEV: Miner/Maximal Extractable Value
  - Frontrunning: Execute before victim's transaction
  - Backrunning: Execute after victim's transaction
  - Sandwich attack: Execute before AND after (profit from price impact)
  - Flashbots: ~$1.8B+ extracted since 2020
- CeFi Comparison
  - Strict regulatory rules on transaction ordering
  - FIFO, price-time priority enforced
  - Frontrunning is illegal in traditional markets

OST

Key DeFi Properties (3/3)

- Transaction Costs: Spam Prevention
  - DeFi: Every transaction costs gas fees
  - Essential to prevent network spam and Sybil attacks
  - Typical costs on Ethereum: ~$1 depending on network congestion
  - CeFi: can offer free transactions (cross-subsidized by fees, minimums, or interest margins)
- Anonymous Development & Deployment
  - Many DeFi projects developed by pseudonymous/anonymous teams
  - Examples: SushiSwap (Chef Nomi)
  - Risk: No legal recourse if project fails or rug pulls
  - Trade-off: Censorship resistance vs. accountability
- Non-Stop Market Hours (24/7/365)
  - TradFi: NYSE/NASDAQ Mon-Fri 9:30am-4pm ET
  - DeFi: Always open, no weekends, no holidays
  - Exception: Protocol maintenance or hacks
  - Example: GameStop short squeeze (Jan 2021)

    → Robinhood halted trading, sparking outrage

    → DeFi protocols continued operating without interruption

OST

Regulations - The Grey Zone

- DeFi Developer Liability (KYC/AML)?
  - Legal frameworks vary by jurisdiction (US, EU, Switzerland, etc.)
- Asset Freezing/Blacklists
  - Centralized stablecoins (USDT/USDC) freeze funds via built-in blacklists (e.g., $1.5B+ frozen).
  - Tension: Compliance vs. Decentralization ideal
- Recent Regulatory Actions (2023-2025)
  - Tornado Cash sanctions (US OFAC, Aug 2022)
  - EU MiCA regulation (Markets in Crypto-Assets, 2024)
  - Switzerland: DLT Act providing legal clarity
- Future: Hybrid Models?

```
1  function transfer(address _to, uint _value) public
       whenNotPaused {
2    require(!isBlackListed[msg.sender]);
3    if (deprecated) {
4      return UpgradedStandardToken(upgradedAddress).
           transferByLegacy(msg.sender, _to, _value);
5    } else {
6      return super.transfer(_to, _value);
7    }
8  }
9  function addBlackList (address _evilUser) public
       onlyOwner {
10   isBlackListed[_evilUser] = true;
11   AddedBlackList(_evilUser);
12 }
13 function destroyBlackFunds (address _blackListedUser)
       public onlyOwner {
14   require(isBlackListed[_blackListedUser]);
15   uint dirtyFunds = balanceOf(_blackListedUser);
16   balances[_blackListedUser] = 0;
17   _totalSupply -= dirtyFunds;
18   DestroyedBlackFunds(_blackListedUser, dirtyFunds);
19 }
```

Listing 1: USDT code blacklist functionality.

OST