



OST

Eastern Switzerland
University of Applied Sciences

Blockchain (BlCh)

DeFi Introduction*

Thomas Bocek (*slides partially based on Christian Killer's slides)

28.10.2021

Centralized Finance (CeFi)

- Centralized finance (CeFi) originally from ancient **Mesopotamia**
- Since then, wide range of goods and assets as currency [[link](#)].
 - Cattle, cacao and coffee beans, or cowrie shells, salt, precious metals
 - Gold has enjoyed near universal global acceptance as a 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](#)]








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

Decentralized Finance (DeFi) - Key Features

- Currency either carries intrinsic value (e.g., land, shares) or created by a centralized entity (**reserve bank**) (fiat currency) [**SNB**]
 - Government is backing the financial value of a currency (regulated, trusted)
- Blockchain's (BC) key innovations is the transfer and trade of financial assets without trusted intermediaries.
 - Decentralized Finance (DeFi) specializes in advancing financial technologies and services on top of smart contract enabled ledgers.
- CeFi vs. DeFi – 3 distinct features
 - 1) Transparency
 - Public rules and protocols [**sushiswap**]
 - Avoid private agreements, back-deals and centralization
 - 2) Control
 - DeFi gives control to its users. No-one should censor, move or destroy the users' assets
 - 3) Accessibility [**unbanked**] [**but...**]
 - Anyone with a computer, internet connection and know-how can use or create DeFi products

High Risk, High Reward?

- Financial gain in DeFi also presents a significant contrast to CeFi.
 - In the years 2020 and 2021, DeFi offered higher annual percentage yields (APY) than CeFi
 - **CeFi interest rates**
 - **DeFi interest rates**
- DeFi enables “similar” traditional financial products
 - DeFi also enables novel financial primitives, such as **flash loans [hack]** or **yield farming**

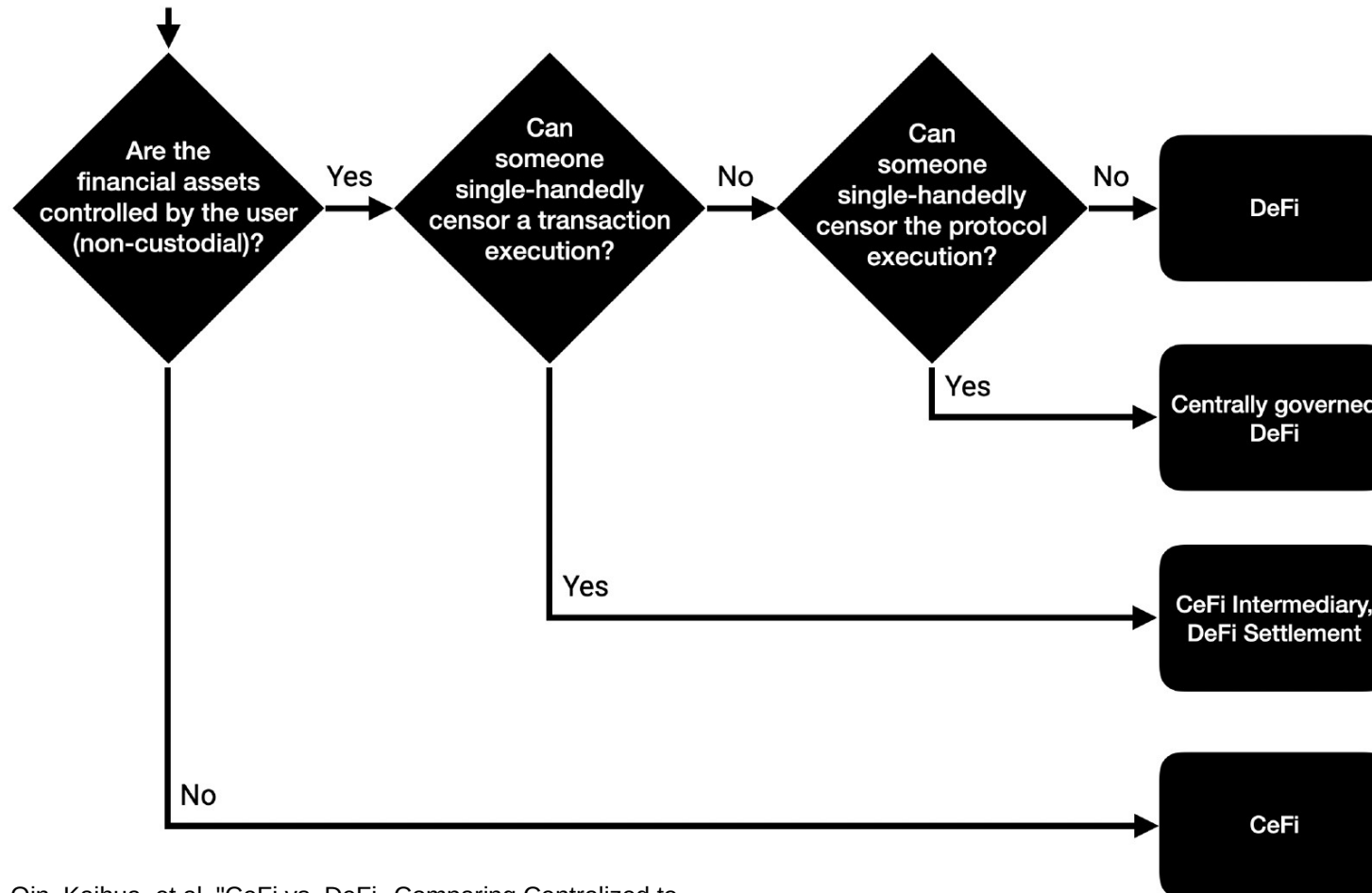
 BUSD 1 ibBUSD = 1.0708 BUSD	Lending APR: 10.35% Staking APR : 1.38% Total APR: 11.73% Total APY ⓘ: 12.44%	206.17M BUSD	131.73M BUSD	63.89%
 USDT 1 ibUSDT = 1.0266 USDT	Lending APR: 9.81% Staking APR : 1.76% Total APR: 11.56% Total APY ⓘ: 12.26%	117.95M USDT	71.4M USDT	60.53%
 TUSD 1 ibTUSD = 1.0057 TUSD	Lending APR: 0.921% Staking APR : 1.98% Total APR: 2.9% Total APY ⓘ: 2.94%	59.56M TUSD	11M TUSD	18.47%
 BTCB 1 ibBTCB = 1.0043 BTCB	Lending APR: 0.377% Staking APR : 1.16% Total APR: 1.54% Total APY ⓘ: 1.55%	2.75k BTCB	325.09 BTCB	11.82%
 ETH 1 ibETH = 1.0121 ETH	Lending APR: 0.830% Staking APR : 0.632% Total APR: 1.46% Total APY ⓘ: 1.47%	55.81k ETH	9.79k ETH	17.53%

<https://app.alpacafinance.org/lend>

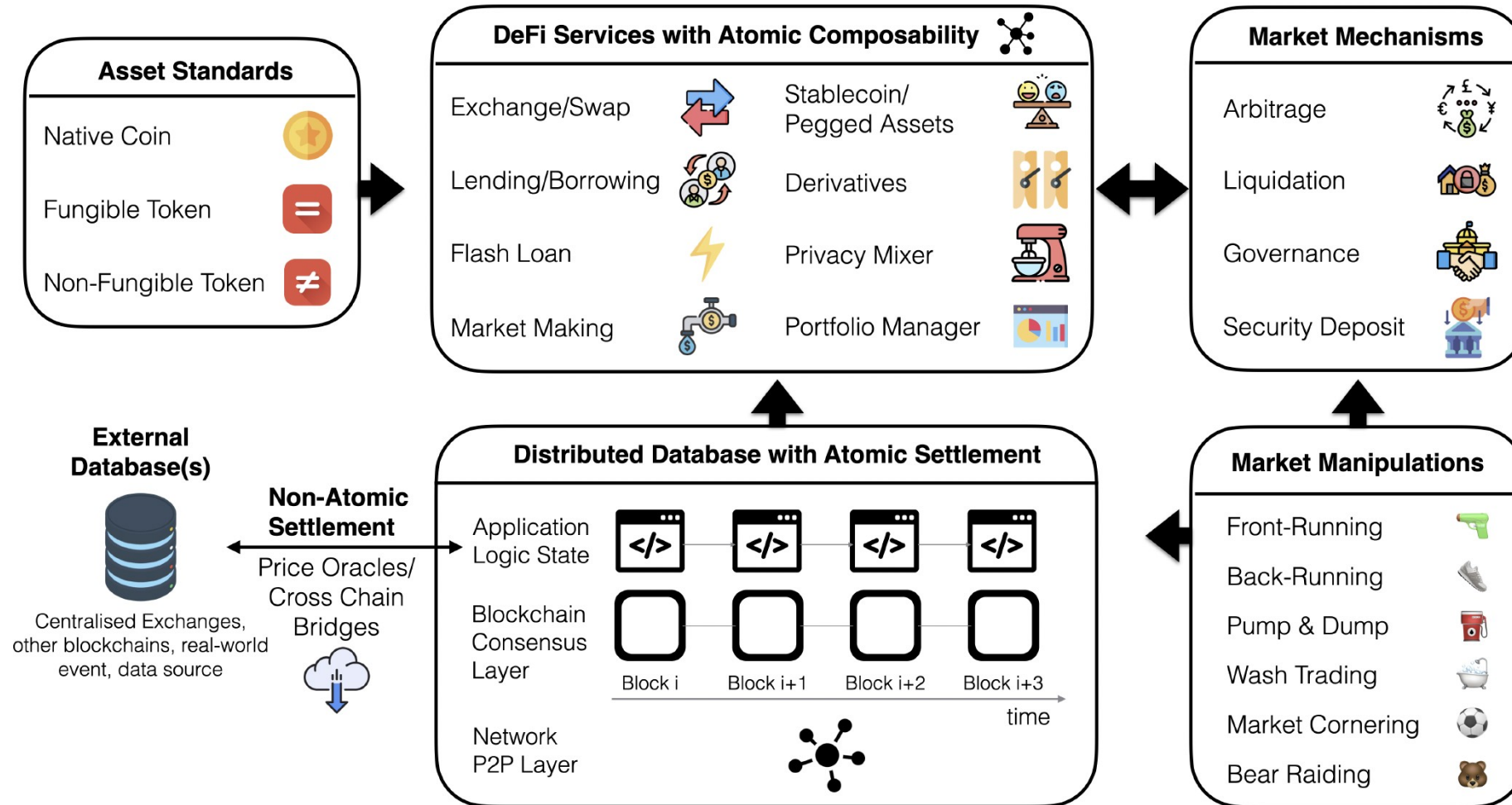


DeFi Decision Tree

- The boundaries of DeFi and CeFi not clear cut



High-Level Systematization of DeFi



Key DeFi Properties

1) Public Verifiability

- While the DeFi app may not be fully open-sourced, the execution and bytecode must be publicly verifiable on a BC
 - **Verify and Publish Source Code**

2) Custody

- DeFi allows its users to control their assets at any time (no need to wait for the bank to open). Technical risks are with the user, with CeFi, is mostly with the bank (USP)

3) Privacy: DeFi is present on non-privacy preserving smart contract blockchains (e.g., not on **Monero**).

- BCs offer pseudoanonymity, but no real anonymity
 - **deanonymization / clustering of transaction data**
- Centralized exchanges with KYC/AML practices are often the only viable route to convert between fiat and cryptocurrency assets
 - Can be queried by law enforcement

Key DeFi Properties

4) Atomicity: A BC transaction supports sequential actions, which can combine multiple financial operations.

- Flash loan example
- This combination can be enforced to be atomic
- While this programmable atomicity property mostly absent from CeFi, (likely costly and slow) legal agreements could enforce atomicity in CeFi as well.

5) Execution Order Malleability: Users on permissionless blockchains typically share publicly the transactions

- No centralized entity ordering transaction execution, peers can perform transaction fee bidding contests to steer the transaction execution order. [frontrunning]
 - Such order malleability was shown to result in various market manipulation strategies, which are widely used on BCs nowadays [generalized-frontrunning]
- In CeFi: regulatory bodies impose strict rules on financial institutions and services as in how transaction ordering must be enforced

Key DeFi Properties

6) Transaction Costs: Transaction fees in DeFi and blockchains in general are essential for the prevention of spam [38k for a tx]

- In CeFi, financial institutions can opt to offer transaction services at **no cost** (or are mandated by governments to offer certain services for free) because of the ability to rely on KYC/AML verifications of their clients

7) Anonymous Development and Deployment: Many DeFi projects are developed and maintained by anonymous teams

8) Non-stop Market Hours: It is rare for CeFi markets to operate without downtime.

- New York Stock Exchange & Nasdaq Stock Exchange business hours are Monday to Friday from 9:30 a.m. to 4 p.m. Eastern Time.
 - Many DeFi markets are open 24/7 (unless hacked or in maintenance mode)
- DeFi has no pre- or post-market trading
- System outages at CeFi stock happened (e.g., **GameStop** short squeeze event)

Regulations

- Regulatory uncertainty (e.g., does a software programmer hold liability to do KYC/AML for an application or code he/she provides to the public?)

A) Censoring (Temporarily) Transactions

- Miners can decide to temporarily censor transactions
- Nodes in lightning may simply refuse a transaction (forcing the user to fall-back to on-chain payment channels)

B) Blacklists, Fungibility and Destruction of Assets

- Once a service provider is KYC/AML regulated, the freezing and confiscation of financial assets may be requested

- **USDT** and USDC have blacklists

- USDT: 449 Accounts blacklisted so far, 43.97M USDT were destroyed

```
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.

Future? (opinion)

- Will DeFi replace CeFi?
 - Financial system still requires trust
 - Fully decentralized mortgage ~difficult
 - Safe custody of assets (e.g., not losing private key)
 - Thus, banks still required, but DeFi will change traditional banking
- DeFi could become the underlying infrastructure of future banks, whereas traditional finance / custody adapt

https://en.wikipedia.org/wiki/File:Paradeplatz_2015.jpg

