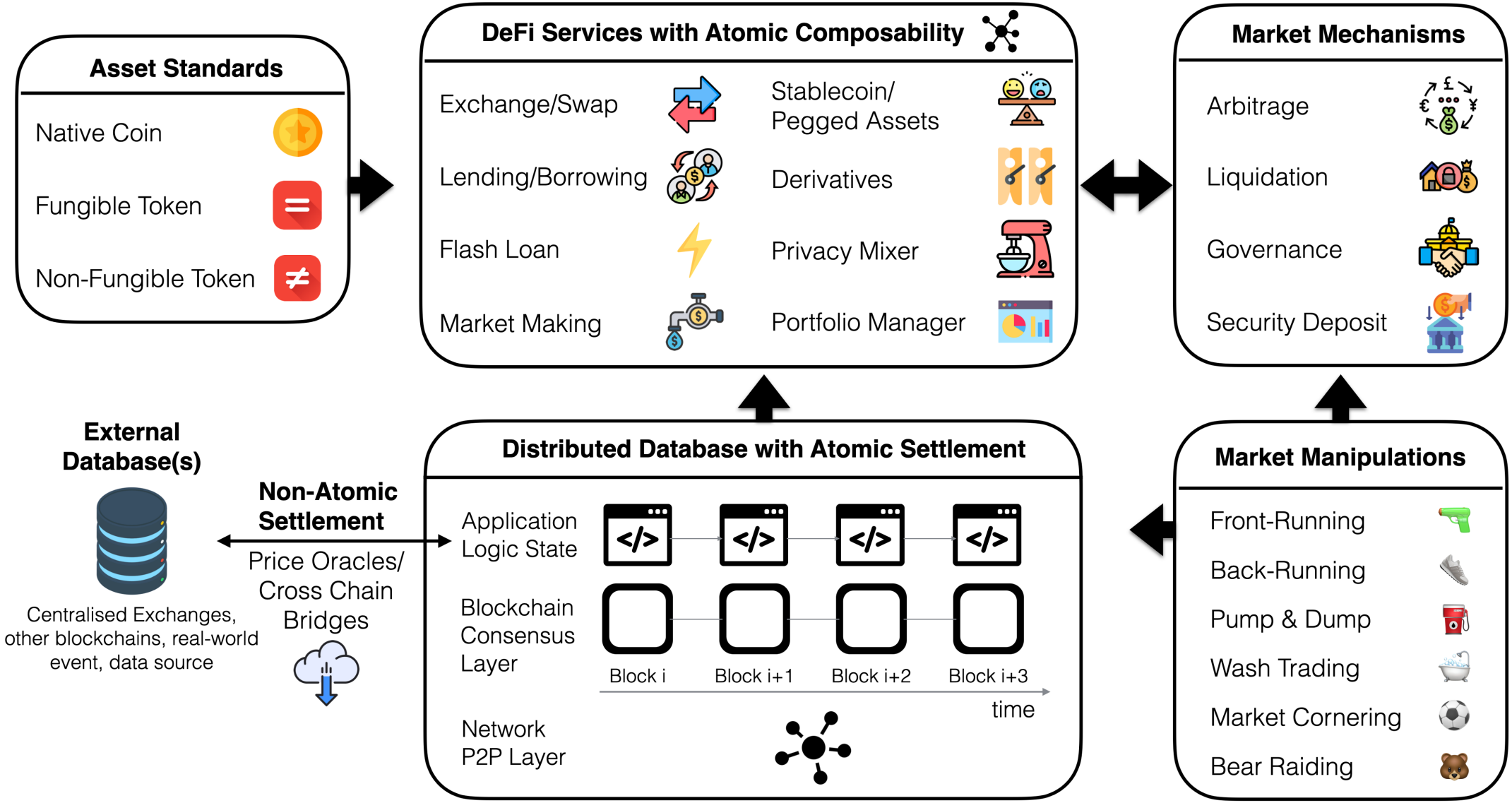
CeFi vs. DeFi

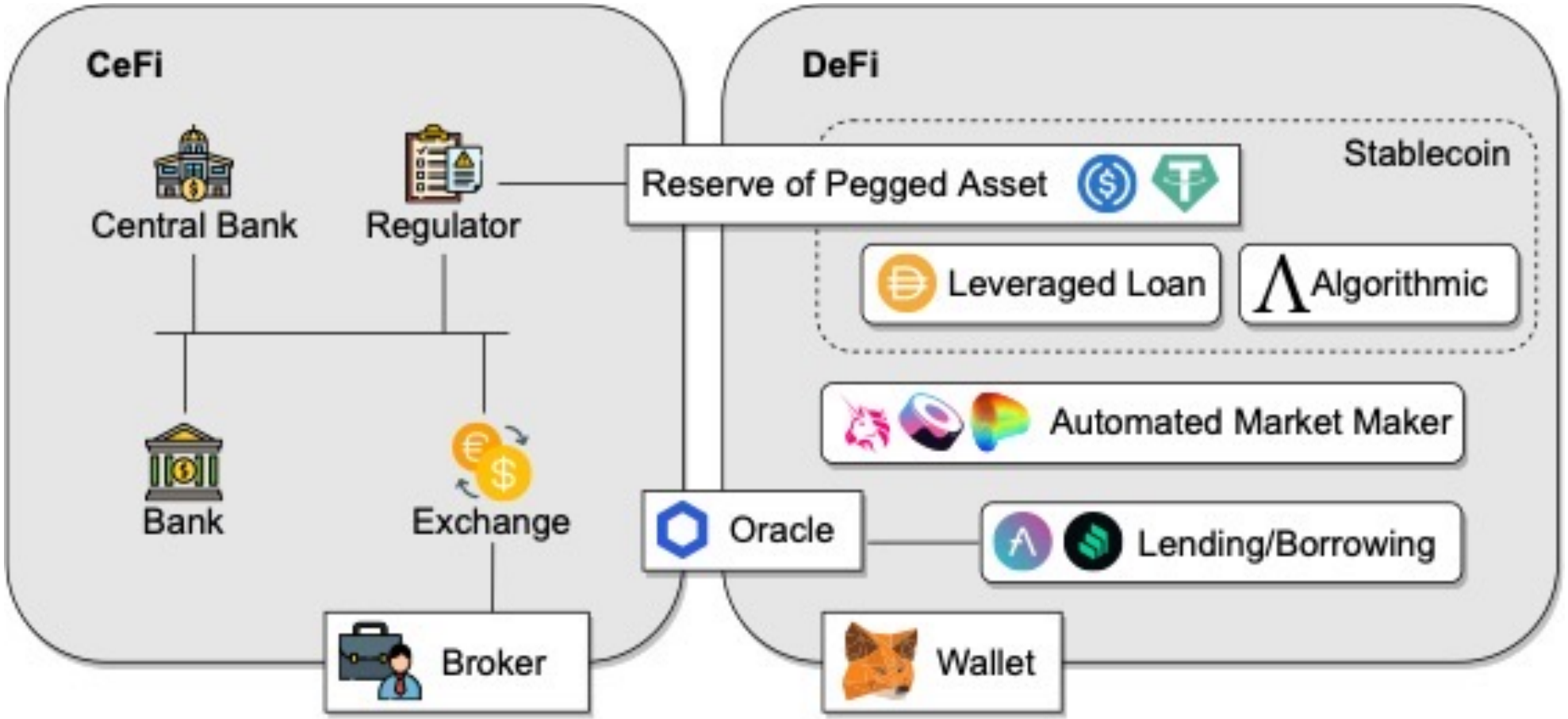
Comparing Centralized with Decentralized Finance

Instructor: Arthur Gervais

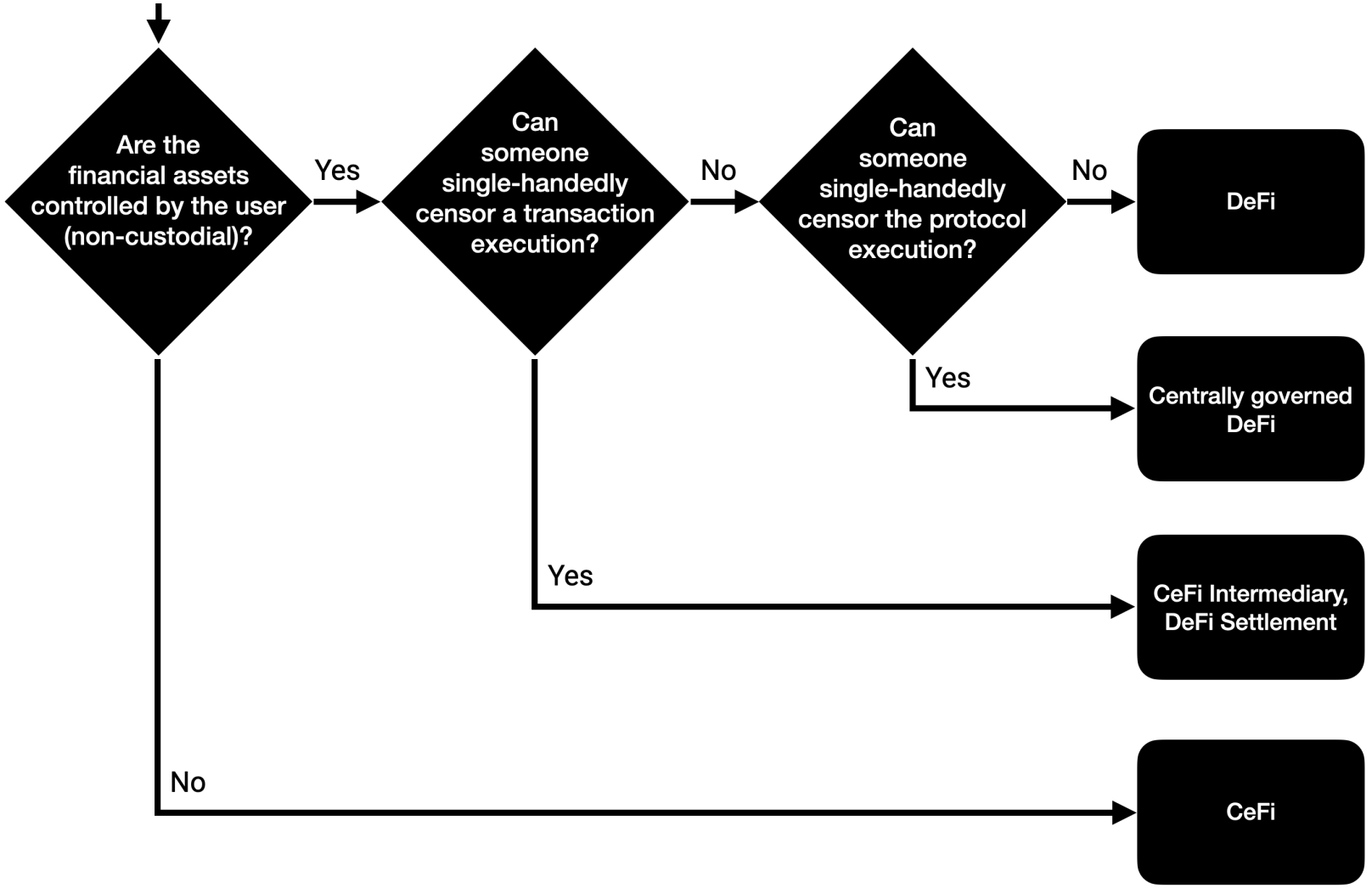
DeFi Stack


Asset Standards
Native Coin
Fungible Token
Non-Fungible Token
DeFi Services with Atomic Composability
Exchange/Swap
Stablecoin/
Pegged Assets
Lending/Borrowing
Derivatives
Flash Loan
Privacy Mixer
Market Making
Portfolio Manager
Market Mechanisms
Arbitrage
Liquidation
Governance
Security Deposit
External
Database(s)
Centralised Exchanges,
other blockchains, real-world
event, data source
Non-Atomic
Settlement
Price Oracles/
Cross Chain
Bridges
Distributed Database with Atomic Settlement
Application
Logic State
Blockchain
Consensus
Layer
Block i
Block i+1
Block i+2
Block i+3
time
Network
P2P Layer
Market Manipulations
Front-Running
Back-Running
Pump & Dump
Wash Trading
Market Cornering
Bear Raiding

High-Level Service Architecture of CeFi, DeFi

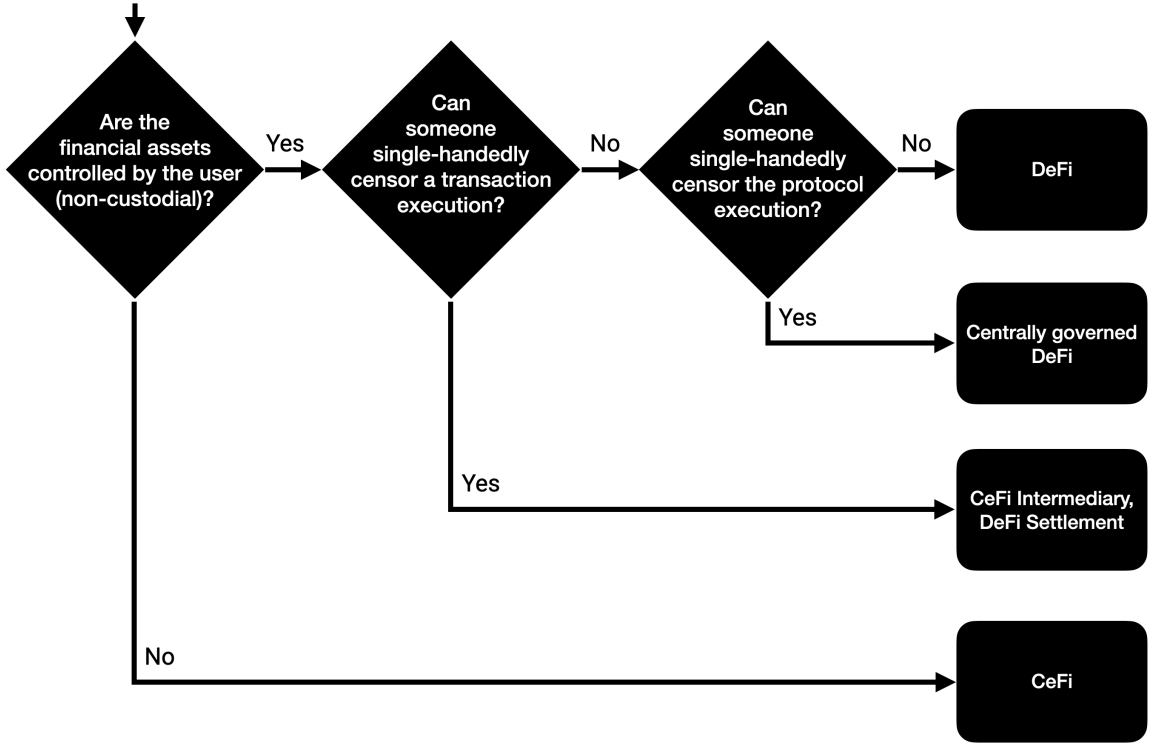


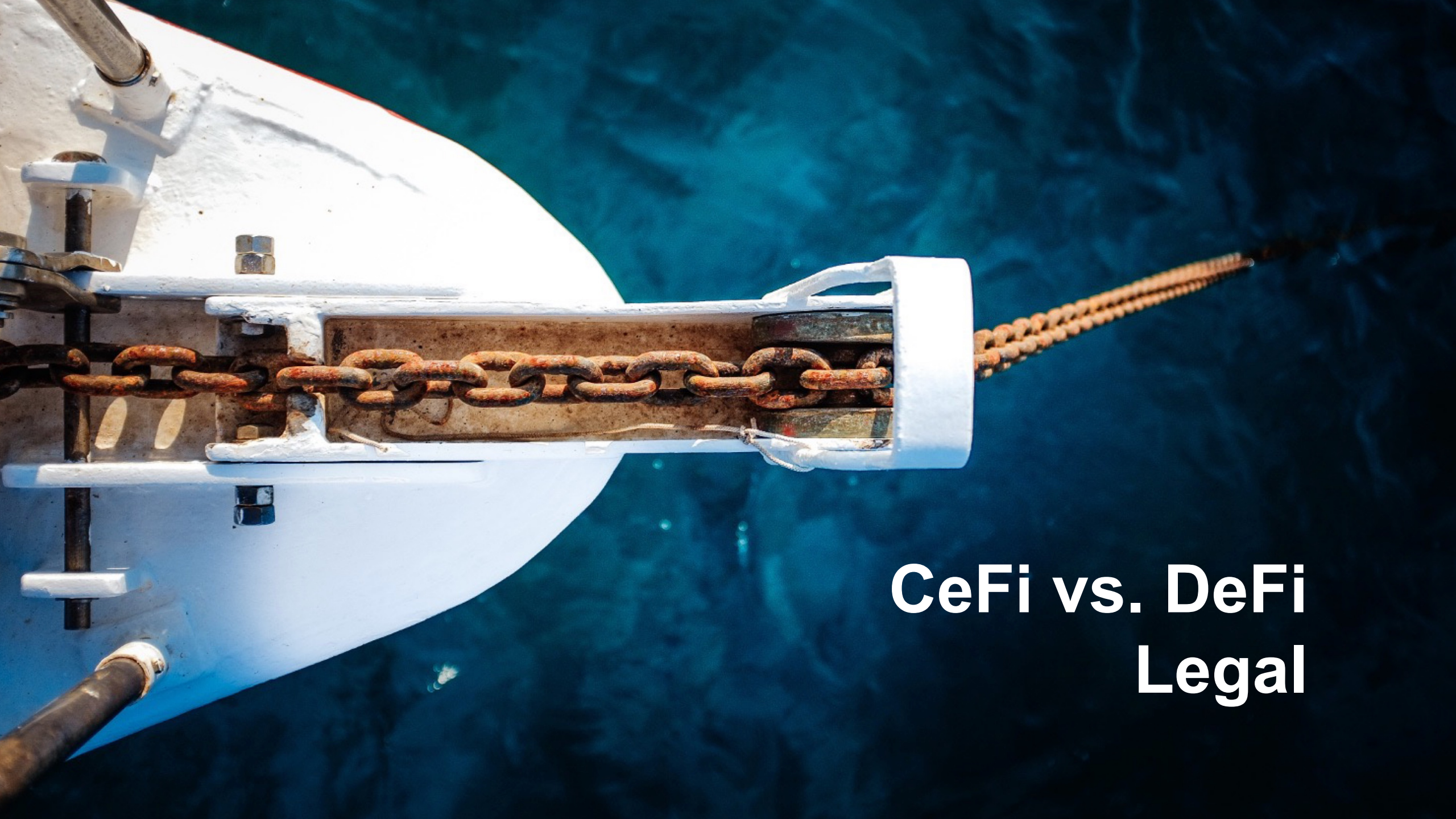
What is Decentralized Finance?



DeFi Properties

- Public Verifiability
- Custody
- Privacy
- Atomicity
- Execution Order Malleability
- Transaction Costs
- Non-stop Market Hours
- Anonymous Development and Deployment





CeFi vs. DeFi
Legal

DeFi On-boarding

- CeFi has strict on-boarding & continuous compliance rules
  - KYC (know your customer)
  - AML (anti-money laundering)
  - CFT (combat the financing of terrorism)

- On-boarding in DeFi
  - Either from CeFi
  - .. or P2P purchase of coins from people IRL

FAFT

- Financial Action Task Force
  - Sets global policy examples that countries can (and do) follow

- New FATF rules target software engineers
  - SW may be liable for engineering DeFi source code
  - .. even if operated by others
  - .. even if no further involvement

Transaction Censoring

- Miners can (temporarily) censor transactions
- Layer 2/Off-chain operator may be able to censor transactions

→ If an entity can single-handedly censor or intervene in a financial transaction, regulators may enforce KYC/AML requirements

Censoring Example: Stablecoins

- USDT and USDC have built-in code to:
  - Blacklist addresses
  - Destroy coins
- USDT blacklisted 449 accounts, destroyed nearly 44M USDT!
- USDC blacklisted 8 accounts

```
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 }
```

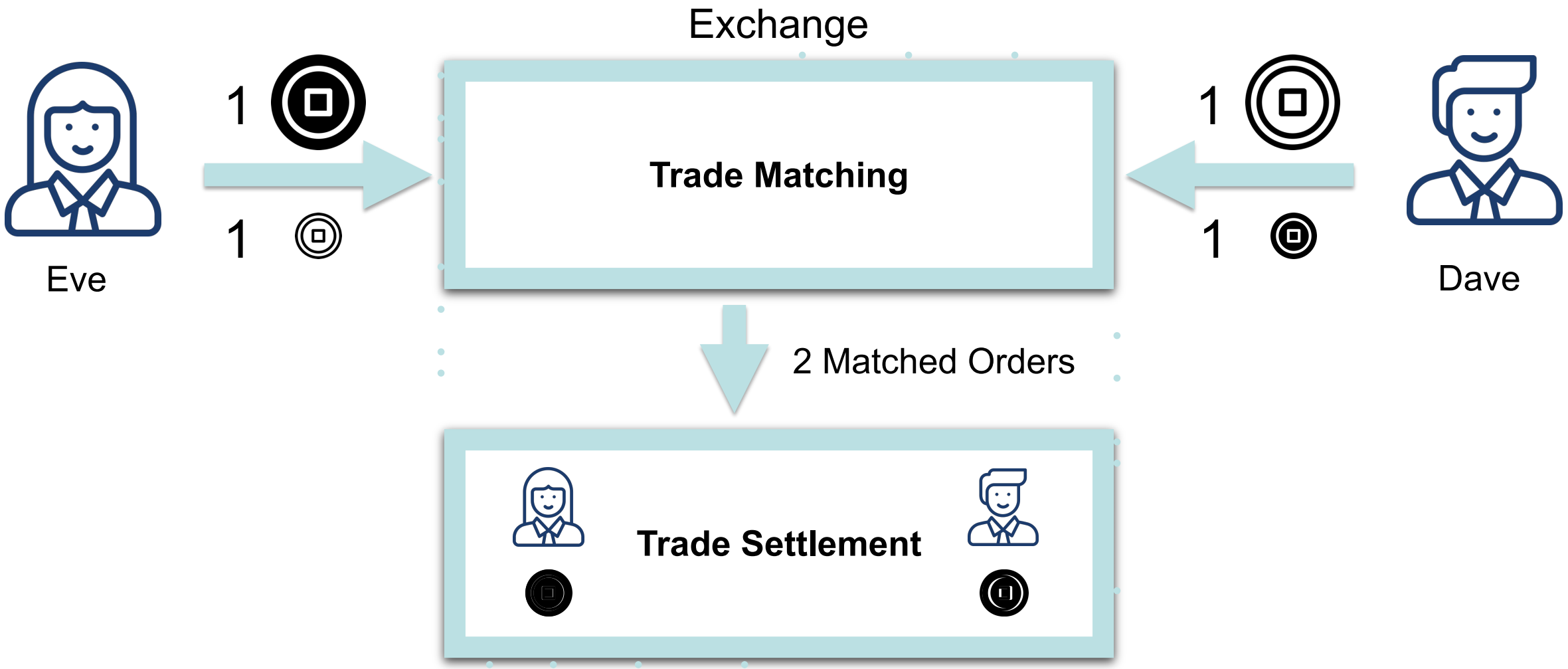
DeFi “Bank Run”

- Bank Run in CeFi
  - No money returned

- “Bank Run” in DeFi
  - A pool (e.g., Curve, Aave) **may get blacklisted**
  - First come, first served
  - Pool formula penalizes destabilizing a pool
  - Increasingly worse price for late-comers

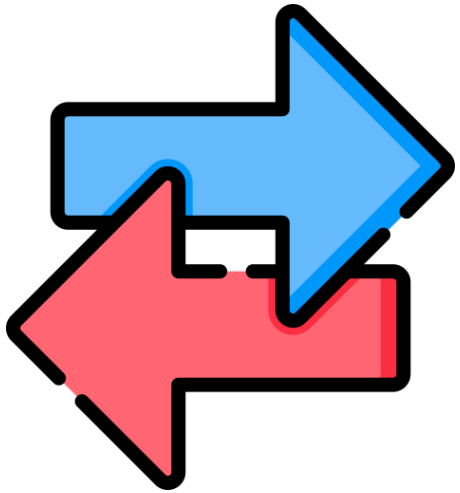
CeFi vs. DeFi Exchanges

Financial Asset Exchanges



Financial Asset Exchanges

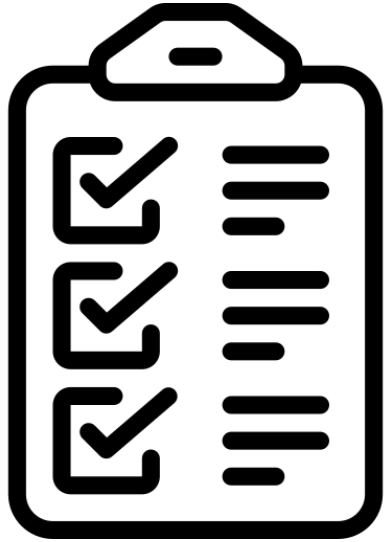
- Three core components
  - Price discovery
  - Algorithmic Trade Matching Engine
  - Trade Clearing System



- Various techniques to realize a DEX
  - On-chain smart contract only (DEX), e.g., Uniswap
  - Trusted Execution Environments (TEE)
  - Multi-Party Computation (MPC)
  - Layer-2/Rollup (off-chain)

Financial Instrument Listing

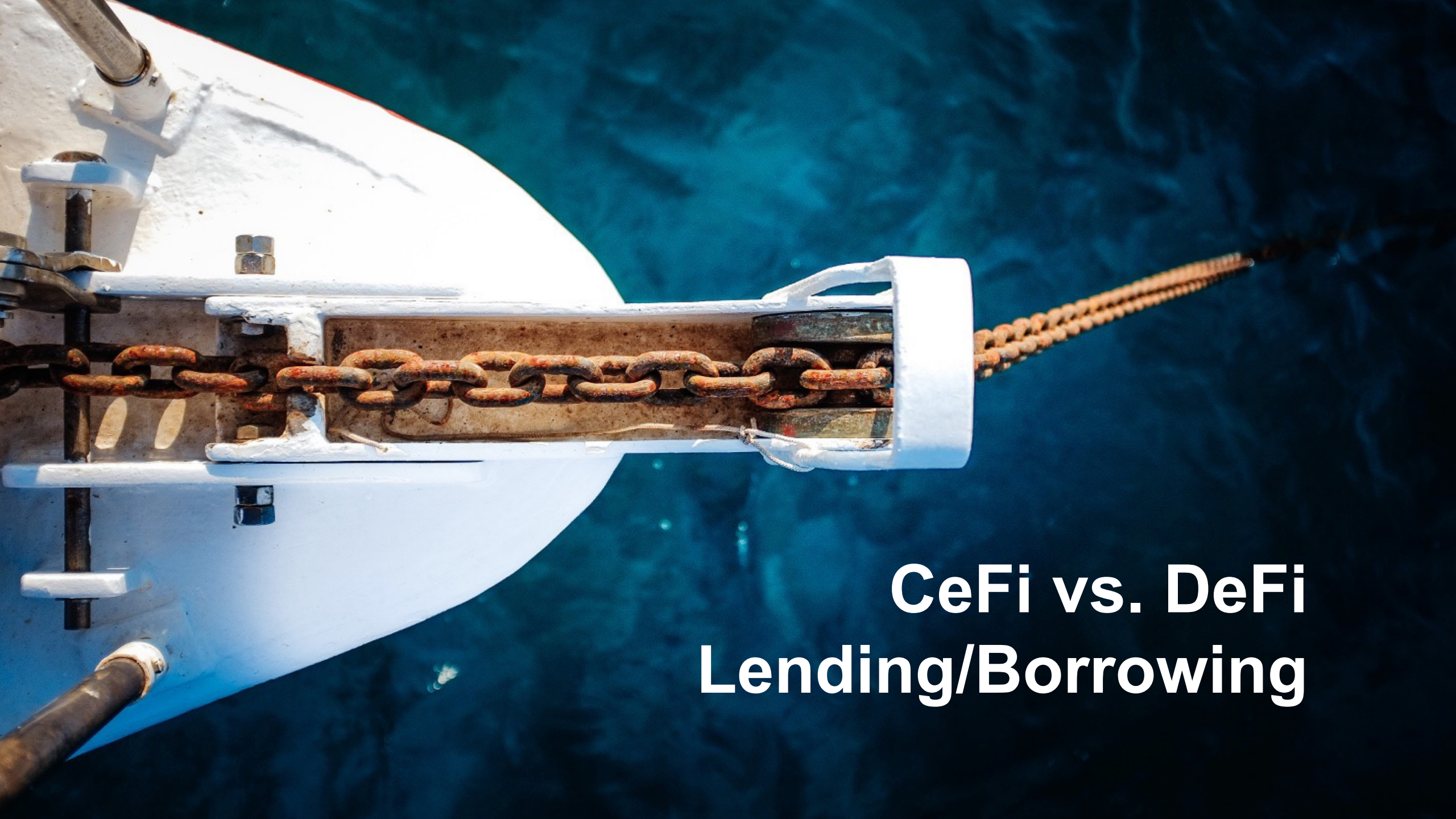
- CeFi asset listings are well regulated
  - Financial audits
  - Earnings report
  - Minimum working capital
- DeFi listing is currently unregulated
  - No binding legal requirements
  - Arbitrary accept/refuse from centralized EX
  - DEX listing can be permissionless → Uniswap



Arbitrage & High-Frequency Trading

- HTF strategies in CeFi and DeFi are similar
  - News-based trading
  - Social media/On-chain activity metrics
  - Trading volume reports, # holders, etc
  - Algorithmic market making
  - Network Latency matters! P2P network optimizations..

- Arbitrage Execution
  - DeFi allows for atomic transactions!
  - “Risk-free” arbitrage



CeFi vs. DeFi Lending/Borrowing

Lending & Borrowing

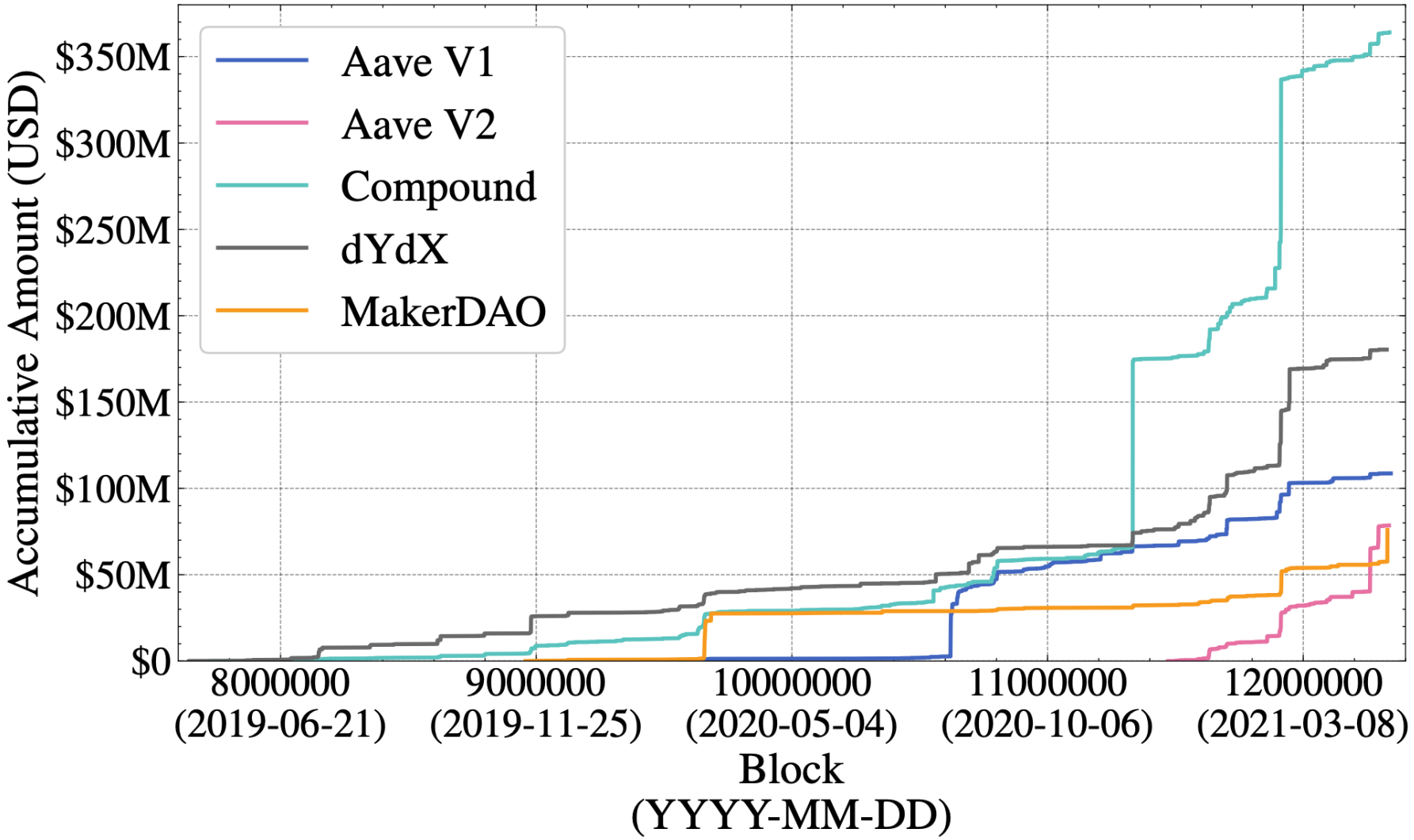
- Lending is critical in both CeFi and DeFi
  - CeFi measures credit "worthiness"
  - DeFi does not grant credits
- DeFi's over-collateralization
  - *Deposit/Collateralize* more than you borrow
  - Provides < 2x leverage (MakerDAO, Aave)
- DeFi's under-collateralization
  - Borrow for a specific purpose only, leverage >2x
  - Enforced by smart contracts (e.g., Alpha Homora)

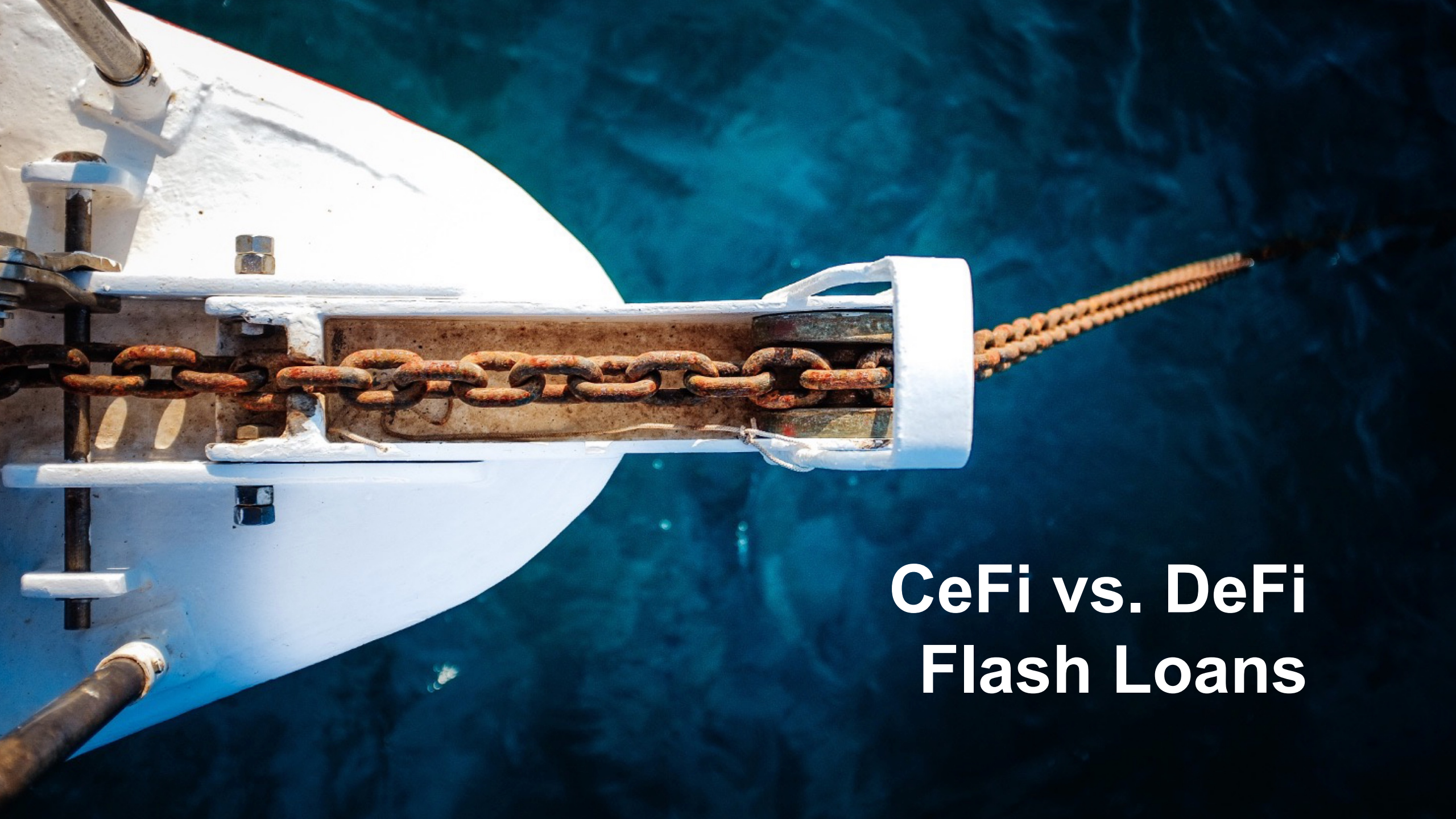
DeFi Liquidations

- Collateral == Security guarantee
- If (price(collateral) < 110%):
  - Collateral may become available for liquidation

- Liquidation == Selling collateral at a discount
  - Goal: secure the debt

Liquidation Statistics

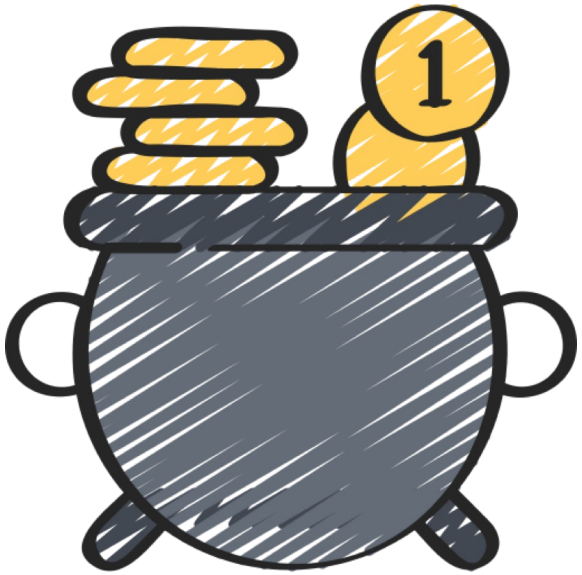




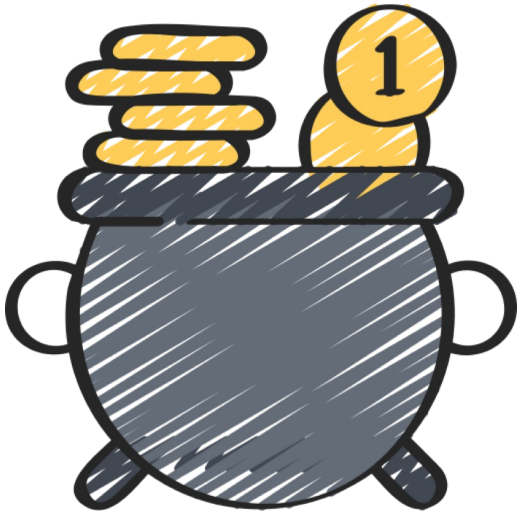
CeFi vs. DeFi Flash Loans

Flash Loans

- Blockchains enable *atomic* transactions
  - The actions within a transaction are *executed entirely in sequence*, or *fail collectively*
- Pools lend assets within one transaction
  - Under the condition that the assets
    - are paid back by the end of the transaction
    - plus interests on the lent amounts
  - Can grow to Billions of USD
    - without upfront costs (only transaction fees)
- Does not exist in CeFi!



Flash Loans

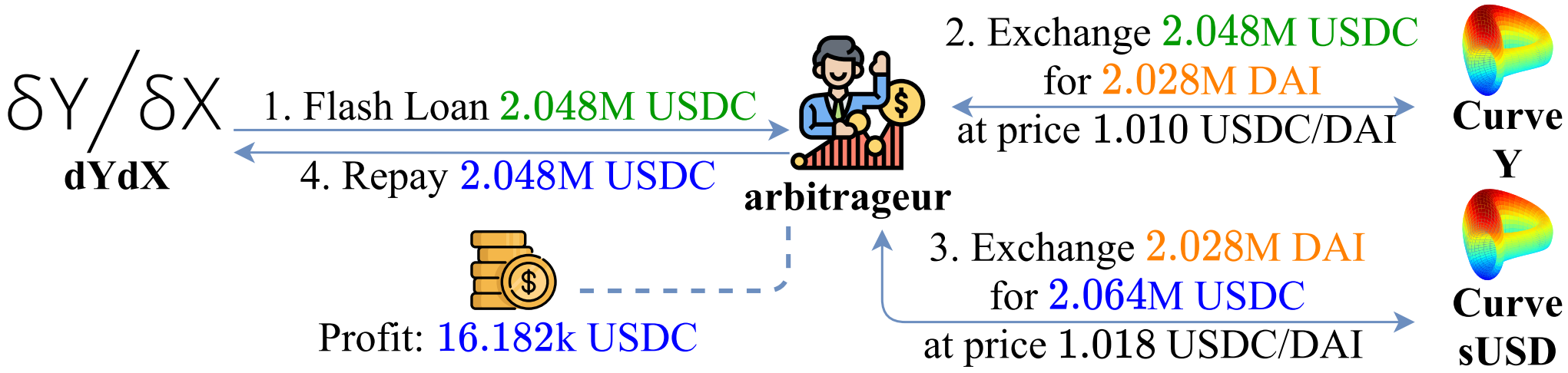


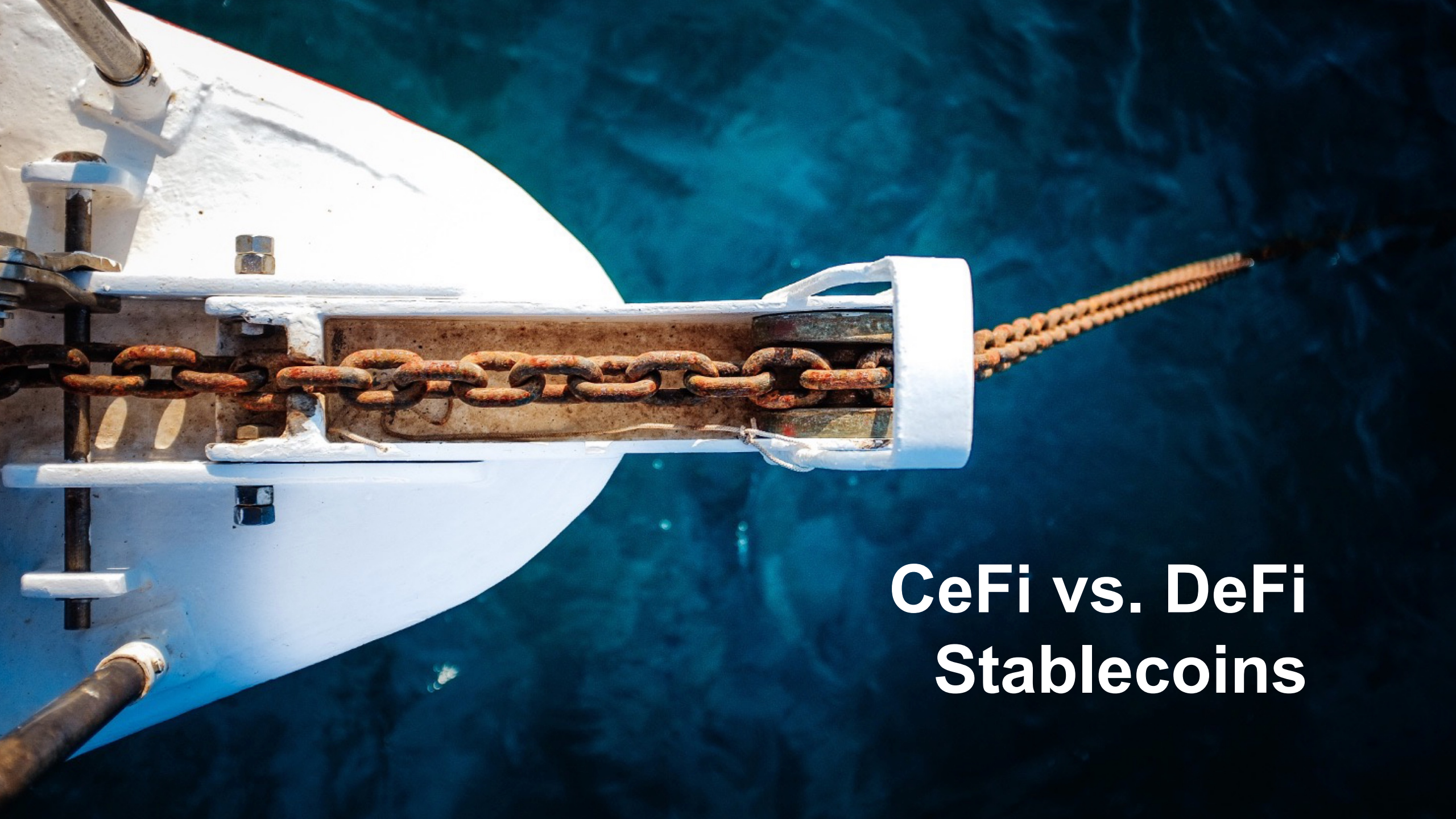
1. Take flash loan

2. go-Wild(loan);

3. Repay loan + interest

Flash Loan Example





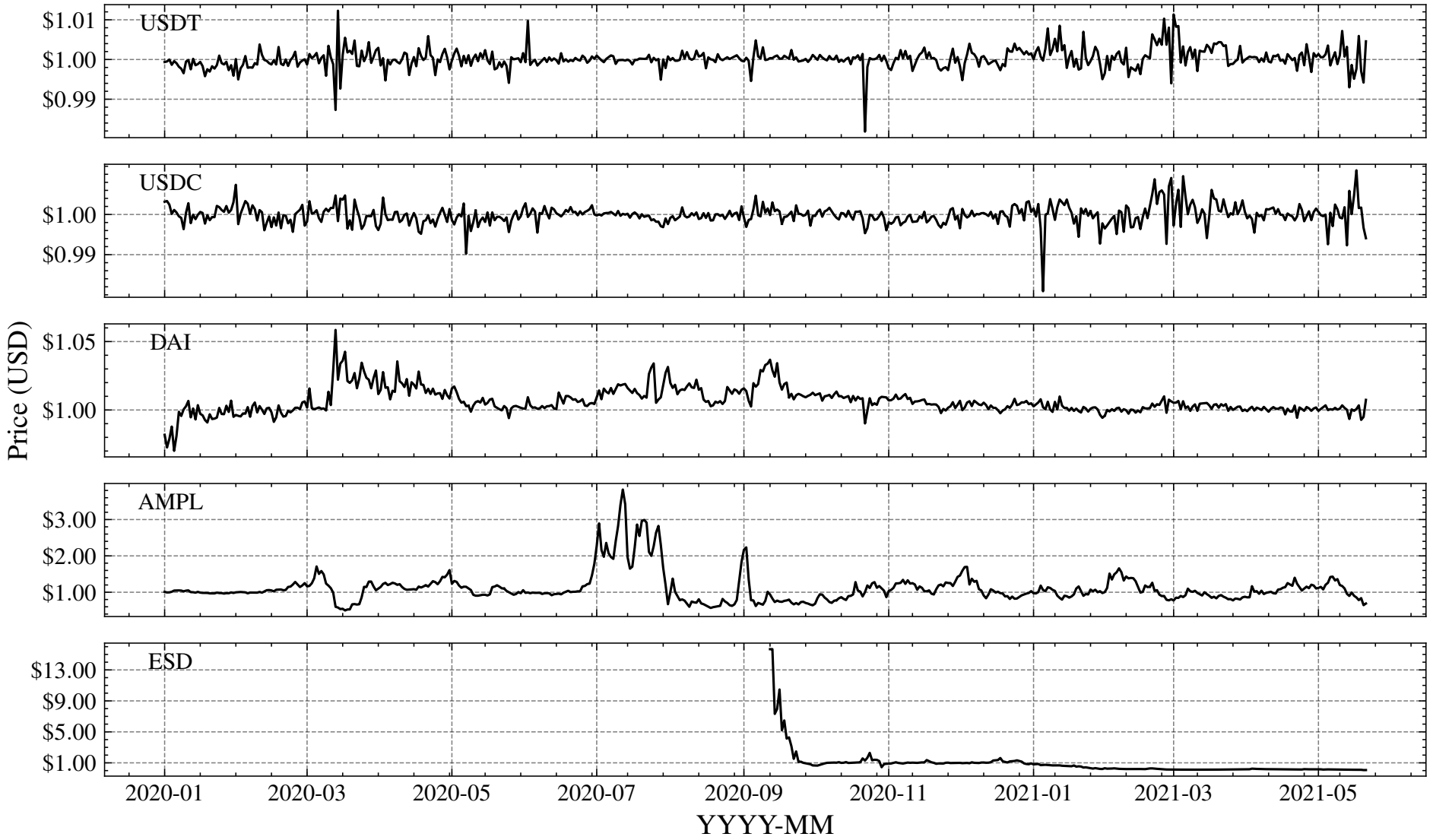
CeFi vs. DeFi Stablecoins

Stablecoin Models

- Various technical means to realize a stable coin
  - Reserve of Pegged Assets
  - Leveraged Loans
  - Algorithmic Supply Adjustments

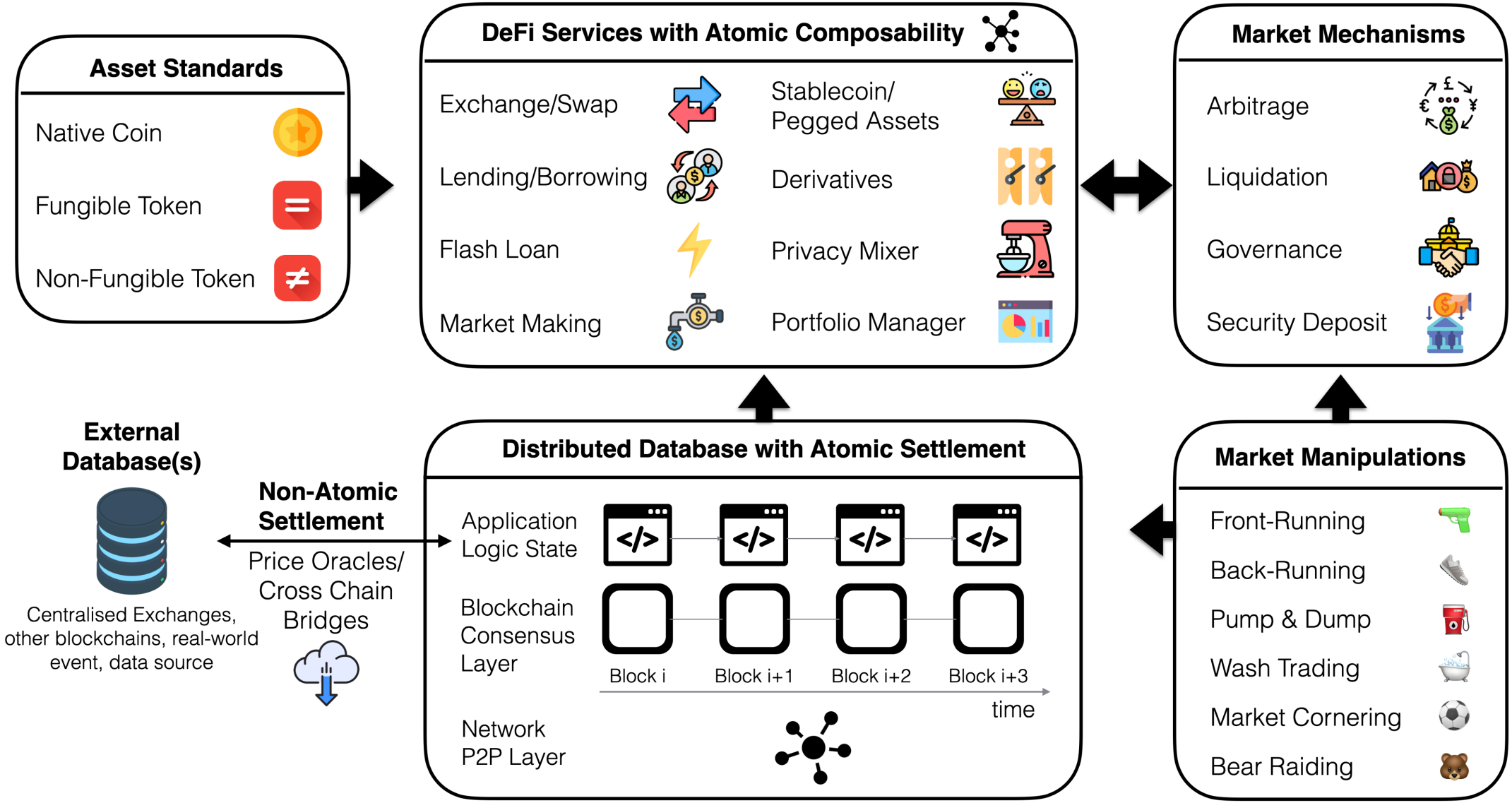
- Different degrees of centralization
  - USDT/USDC can censor assets
  - DAI is backed by over 50% USDT/USDC
  - Algorithmic stable coins are perceived as non-custodial (permissionless)

Stablecoin (In-)stability



CeFi vs. DeFi Security

DeFi Security - Issues on all Layers

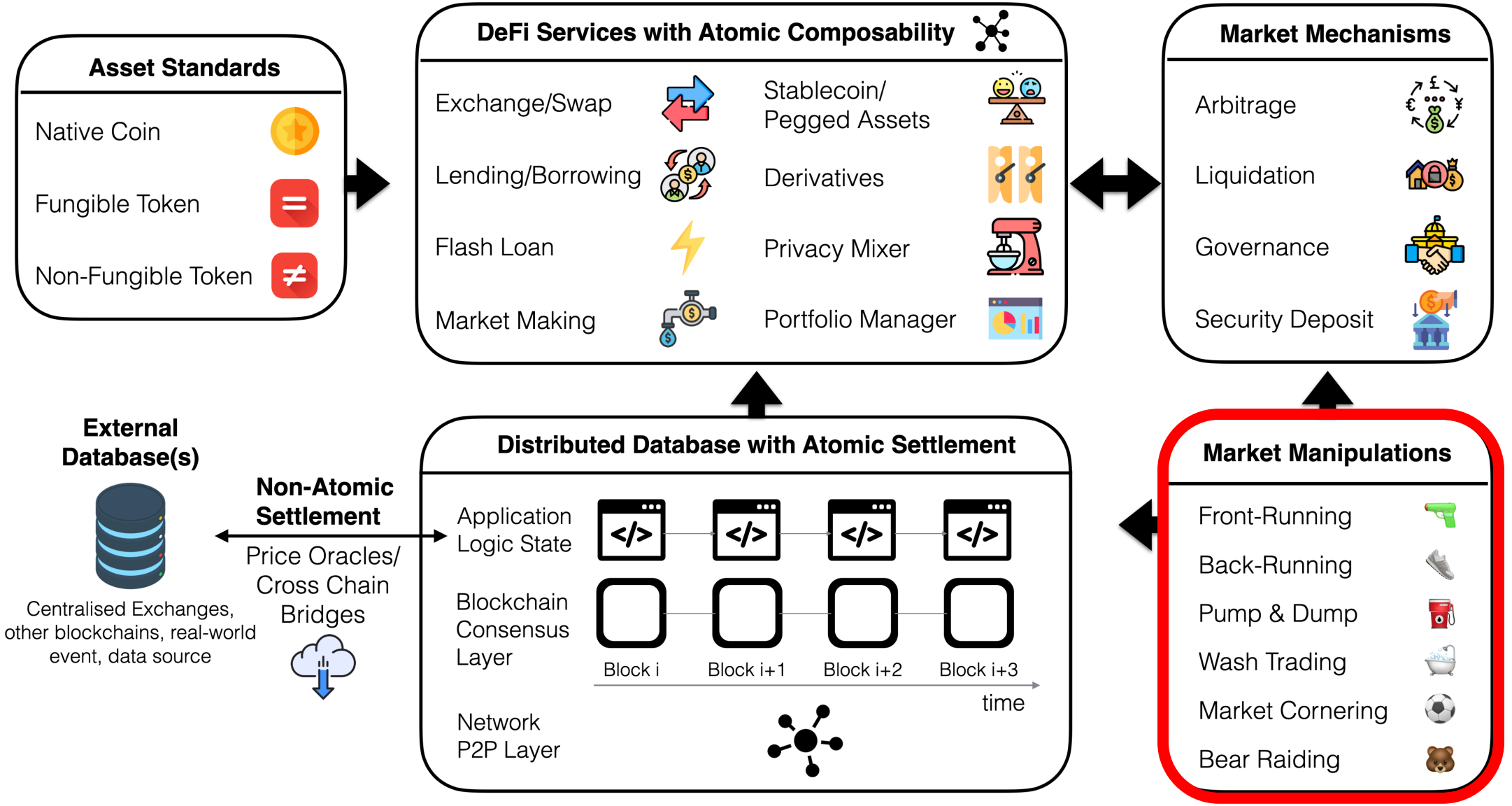


DeFi Security - Issues on all Layers

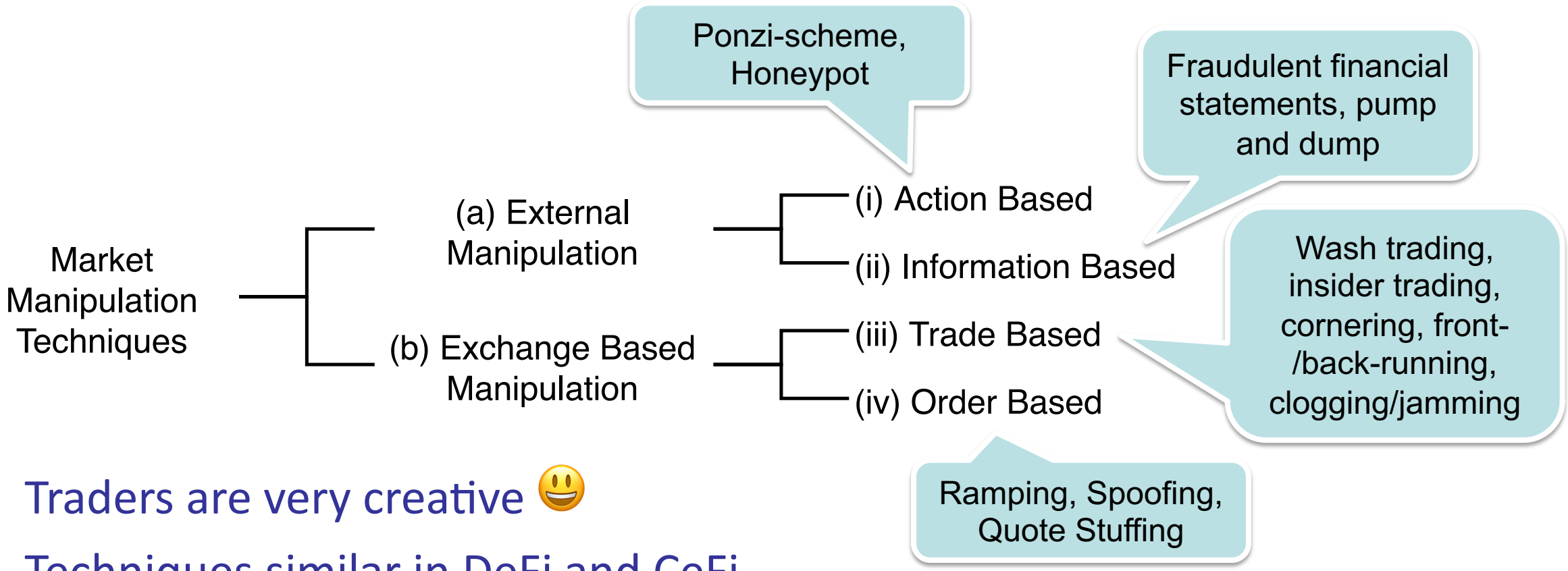
- Network attacks
  - Eclipse/Dos attacks
- Consensus attacks
  - 51% attacks/Double-spending/Selfish mining
- Smart Contract code bugs
  - Reentracy/Authorization/etc
- DeFi Protocol Composability attacks
  - Excessive arbitrage between pools, flash loans

CeFi vs. DeFi Market Manipulation

Market Manipulation



Market Manipulation



- Traders are very creative 😀
- Techniques similar in DeFi and CeFi
- DeFi is more transparent, attacks are transparently measurable

Pump and Dump in CeFi

- Coordinated in groups via Telegram/social media
- Exchanges collude in P&D activities.
- P&D grows trading volume by more than 10x
- Seemingly more prevalent in DeFi than in CeFi

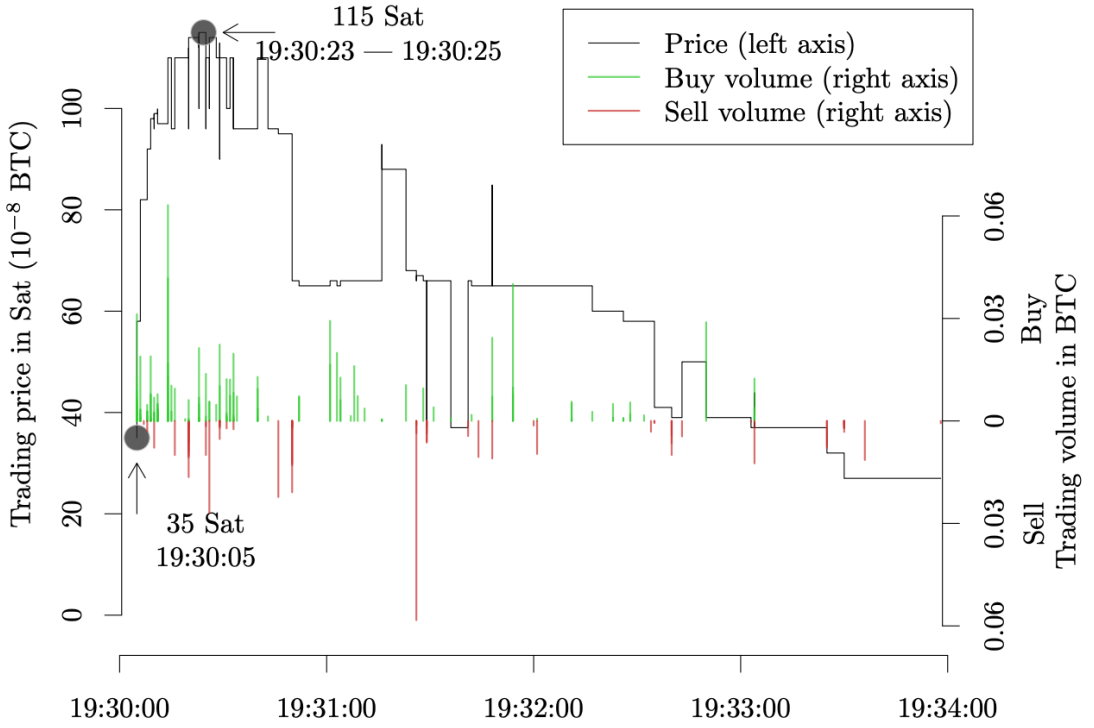


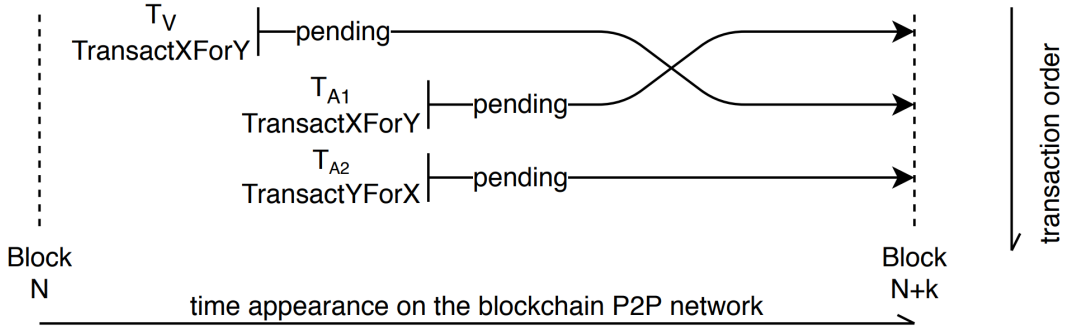
Figure 4: Tick-by-tick movement of the BVB/ BTC market during the first four minutes after the coin announcement.

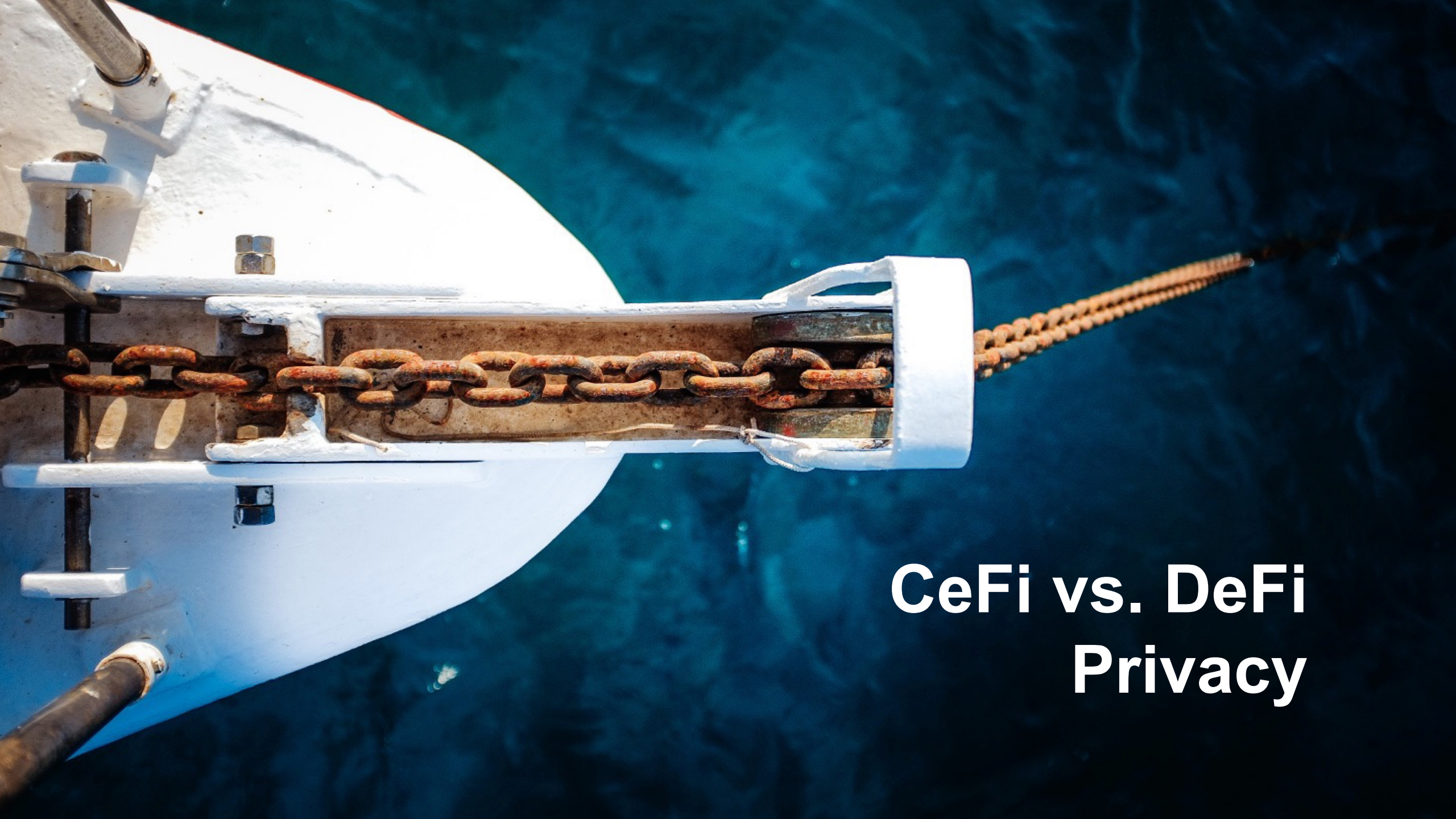
https://www.usenix.org/conference/usenixsecurity19/presentation/xu-jiahua

Front-running and Sandwich Attacks

1. Adversary ($\mathcal{A}$) observes a transaction $\mathcal{T}$ on the blockchain P2P network
2. $\mathcal{A}$ creates a transaction $\mathcal{T}2$ that pays a higher transaction fee (gas)
3. Miners mine transactions based on their paid fee, execute $\mathcal{T}2$ before $\mathcal{T}$
4. Same technique can be used to back-run a transaction

   → Sandwich attacks 🥪

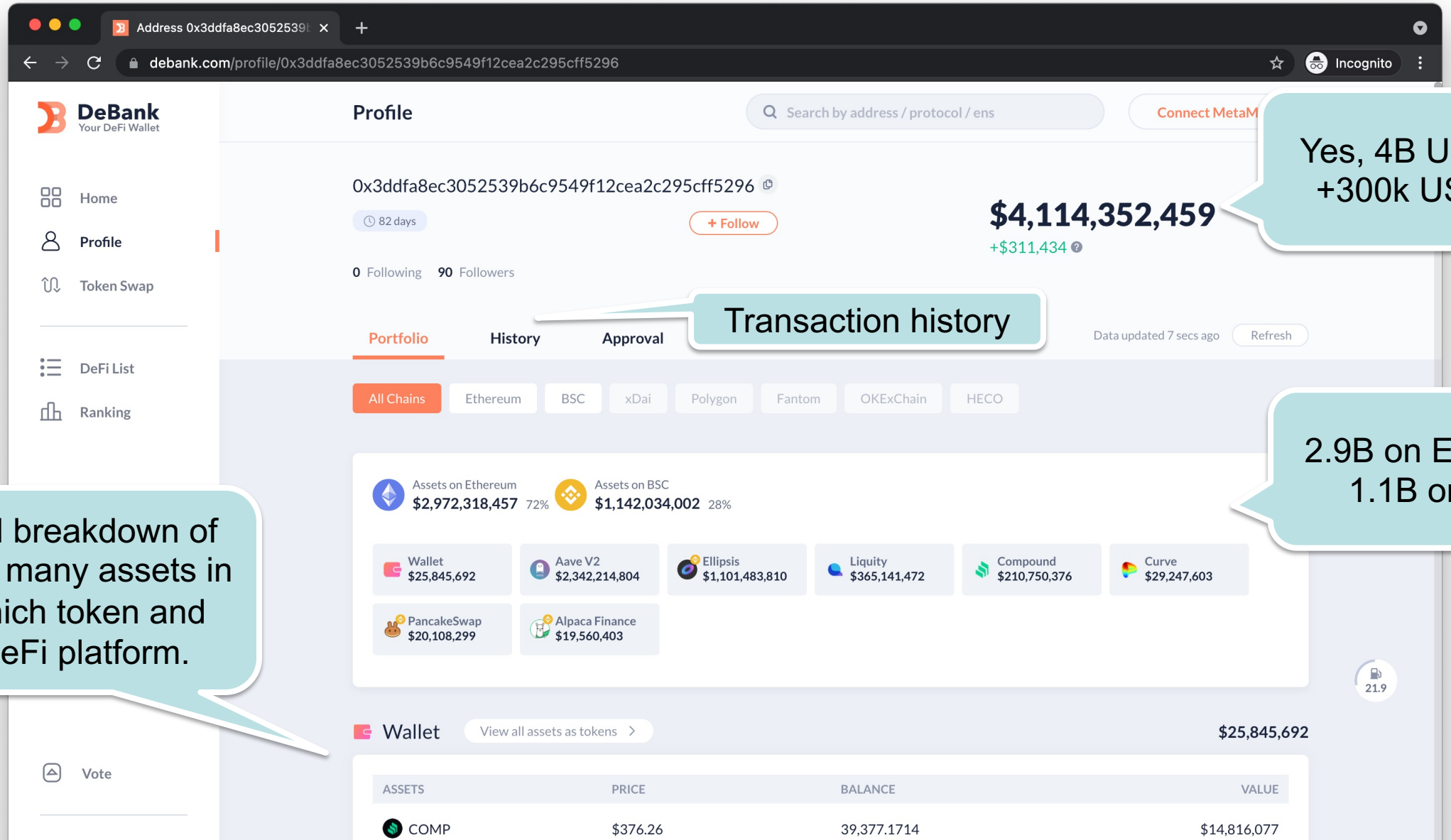



CeFi vs. DeFi
Privacy

Privacy in DeFi

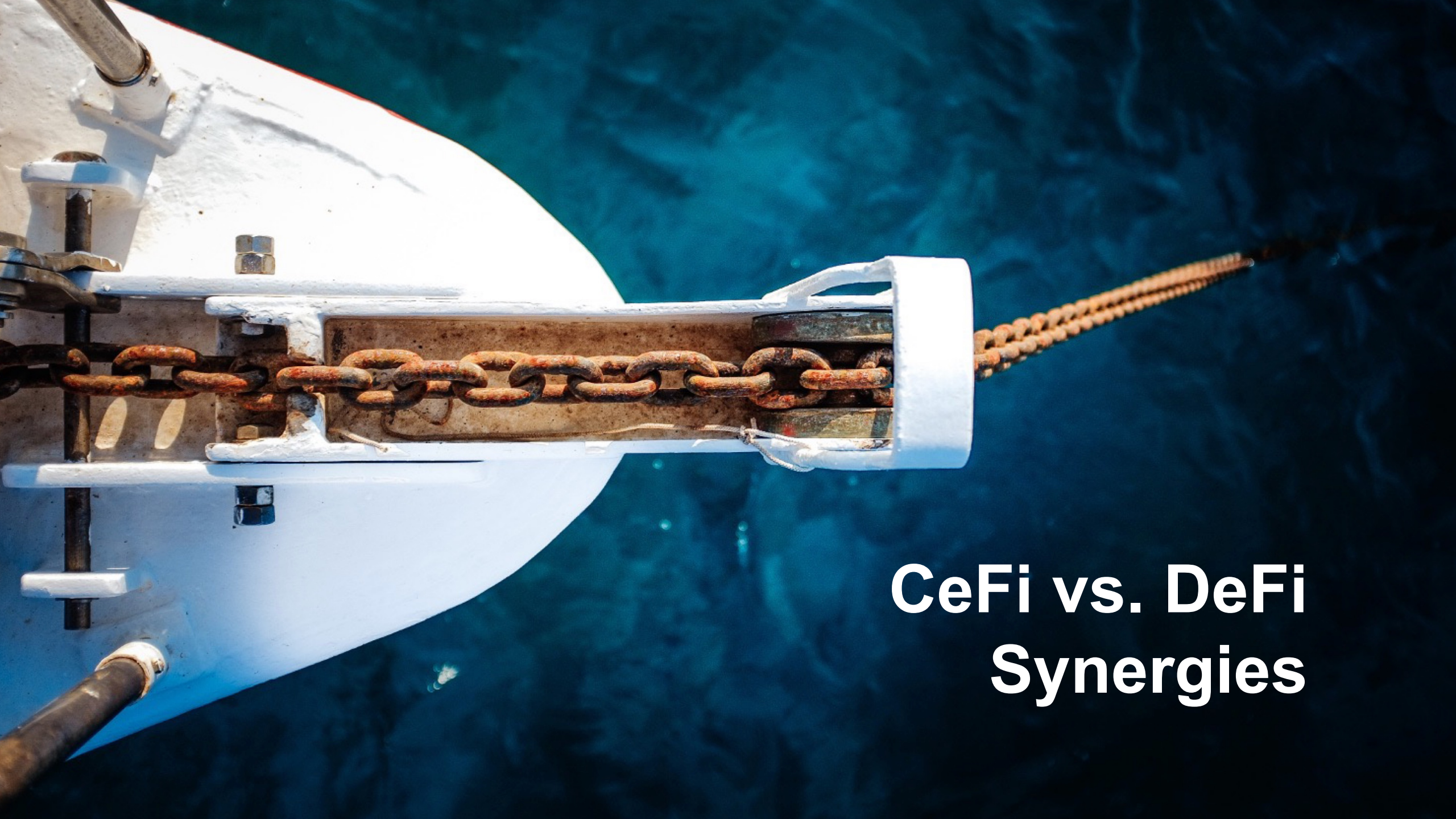
- Blockchains with DeFi are mostly pseudonymous, not anonymous.
- Balances, transactions, timestamps, amounts are all public.
- See the many super-wealthy DeFi accounts for yourself..

(Non-existent) Privacy in DeFi



Mixer

- Mixer try to break the linkability between blockchain addresses.
- Inspired from privacy-by-design blockchains (such as Zcash, Monero)
- *E.g., Tornado.Cash*

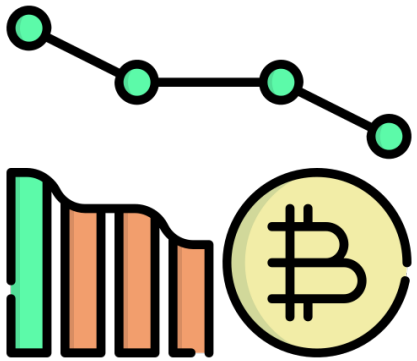


CeFi vs. DeFi Synergies

DeFi Price Collapses

- Multiple significant price declines in cryptocurrencies
  - -30% on the 12th of March 2020
  - -40% on the 19th of May 2021
- CeFi exchange services collapsed (e.g., Robinhood, Coinbase)
- Stock markets have circuit breakers to stop losses

- Yet, DeFi seems to “operate well”
- Transaction prices on blockchains spiked, a regular coin transfer costed over 100 USD



DeFi: An Innovative Addition to CeFi

- DeFi copies many concepts from CeFi
- But, DeFi also innovates
  - Automated Market Maker Exchanges instead of limit order books
  - Flash Loans
  - Over-collateralized Loans
  - Liquidation Mechanisms
  - Atomic Composability of DeFi
  - Liquidity Mining
- Hopefully this innovation feeds back to CeFi

DeFi and CeFi strengthen each other!