Elements of DeFi

https://web3.princeton.edu/elements-of-defi/

Professor Pramod Viswanath

Princeton University

Lecture 15

Stablecoins

Last Lecture: Wrapped tokens and bridges

- Importing data from other blockchains
  - Wrapped tokens
- General bridge architecture
  - Design space
  - Desired properties
- Bridge designs
- Blockchain interoperability not via bridges

This lecture: Stablecoins

- Fiat-pegged, centralized:
  - USDC, USDT – stay pegged to dollar because of centralized backing
- Fiat-pegged, decentralized:
  - DAI and incentives around it – stay pegged to dollar because of decentralized borrow/lending incentive mechanism
- Algorithmic stablecoins:
  - BasisCash, Terra-Luna – stay pegged to dollar because of decentralized algorithmic mechanism
- Reserve coins:
  - OHM – backing instead of pegging, monetary policy reactive to market volatility

History

- The US Dollar was initially backed by a fixed amount of gold – so that value of the currency is tied to a real-world asset
- Backing was relaxed after the Great Depression - 1930s
- Enabled the Fed to react to periods of stress by controlling inflation rates
- Today, US Dollar derives value purely from trust in the Fed
- Fiat currency system with a monetary policy

“Fiat” currencies in DeFi

- Currencies like BTC, ETH not tied to any other currency/commodity
- Leads to high volatility of the currency’s value in terms of “real world assets”
- No assurance that if the currency starts losing value, users have assets to fall back on
- Minting and burning of tokens follows a fixed schedule and does not react to economic situation - Fiat currency system without a monetary policy

Need for better alternatives

- Need to create currencies so that transaction tracked on-chain, but value derived from other assets

- Option 1: Derive value from trust in the Fed – peg to USD
  - Stable coins – most of this lecture

- Option 2: Derive value by backing from a bucket of assets + minting, burning happens according to a decentralized monetary policy
  - Reserve coins – still many open questions

Centralized stable coins

- Simplest solution: Derive value from trust in Fed + back every minted coin by exactly 1 USD
- Regulated centralized entity does book-keeping – maintain 1:1 backing
- Uses USD reserves to earn interest

Name	Market Cap
Tether USDT	$69,364,670,280
USD Coin USDC	$42,159,943,903
Binance USD BUSD	$22,549,289,118

Comparison with TradFi

Traditional Currencies

- Transfer funds using wires, ACH, credit cards etc can can take up to several days
- Transaction fees for wires, credit card fees (~2-3%) passed on to consumer
- Purchase protection can reverse transactions in the case of fraud
- ATM acts as a bridge between TradFi cash system and TradFi digital system
- Well regulated

Fiat-backed stablecoins

- Transaction settlement within minutes
- Generally lower transaction fees
- Transactions are irreversible (no protection against fraud once the transaction goes through)
- Acts as a bridge between TradFi digital system and Web3 system
- Seem well regulated

Centralized stable coins

- However, trust needs to be placed in the centralized entity – that they invest backing responsibly
- Need to decentralize the pegging to USD

Balances

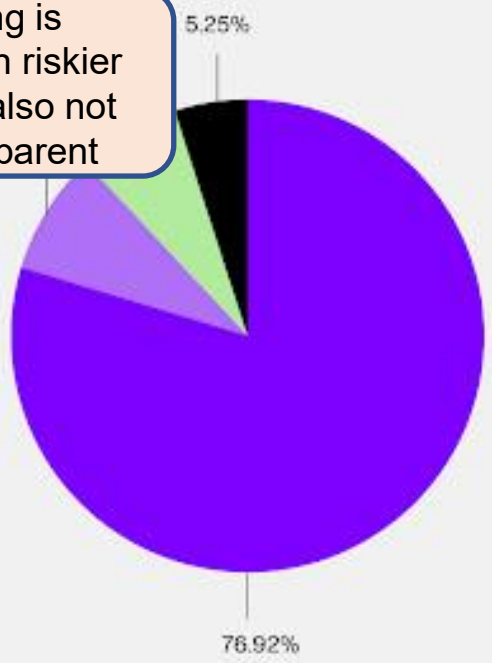
USDC's backing is considered to be in safe assets, Circle has been compliant with regulations and transparent

USDC in circulation	$44.0B
USDC reserves [2]	$44.2B
Cash	$8.5B
Short-duration U.S. Treasuries	$35.7B

Tether's Reserves Breakdown

Data collected from June, 2022

USDT's backing is considered to be in riskier assets, Tether is also not completely transparent



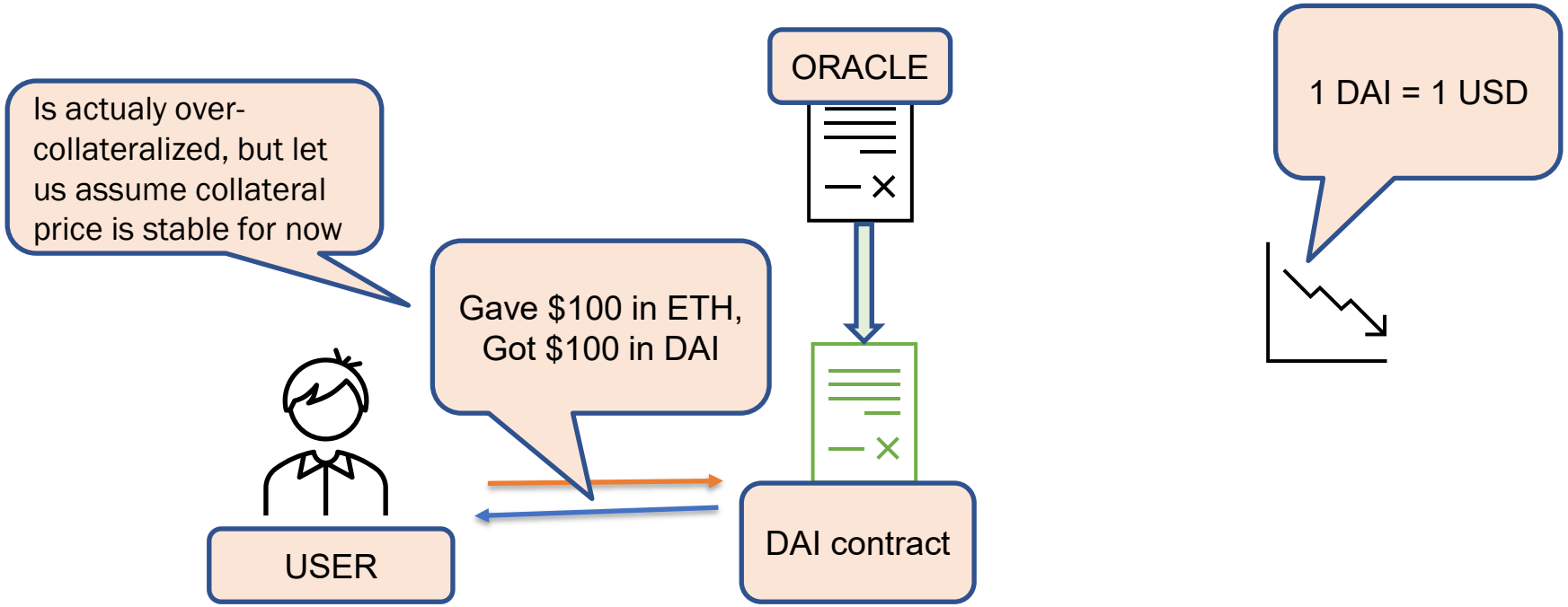
- 79.62% Cash & Cash Equivalents & Other Short-Term Deposits & Commercial Paper
- 8.36% Other Investments (Including Digital Tokens)
- 6.77% Secured Loans (None to affiliated entities)
- 5.25% Corporate Bonds, Funds & Precious Metals

Collateralized Stablecoins

- Value kept pegged to USD via a borrow/lending mechanism
- Tokens are minted using collateral that is posted to a contract
- Tokens are burnt when returned to a contract and collateral withdrawn
- Key Idea:
  - When peg is above $1, users should be incentivized to mint tokens
  - When peg is below $1, users should be incentivized to burn tokens

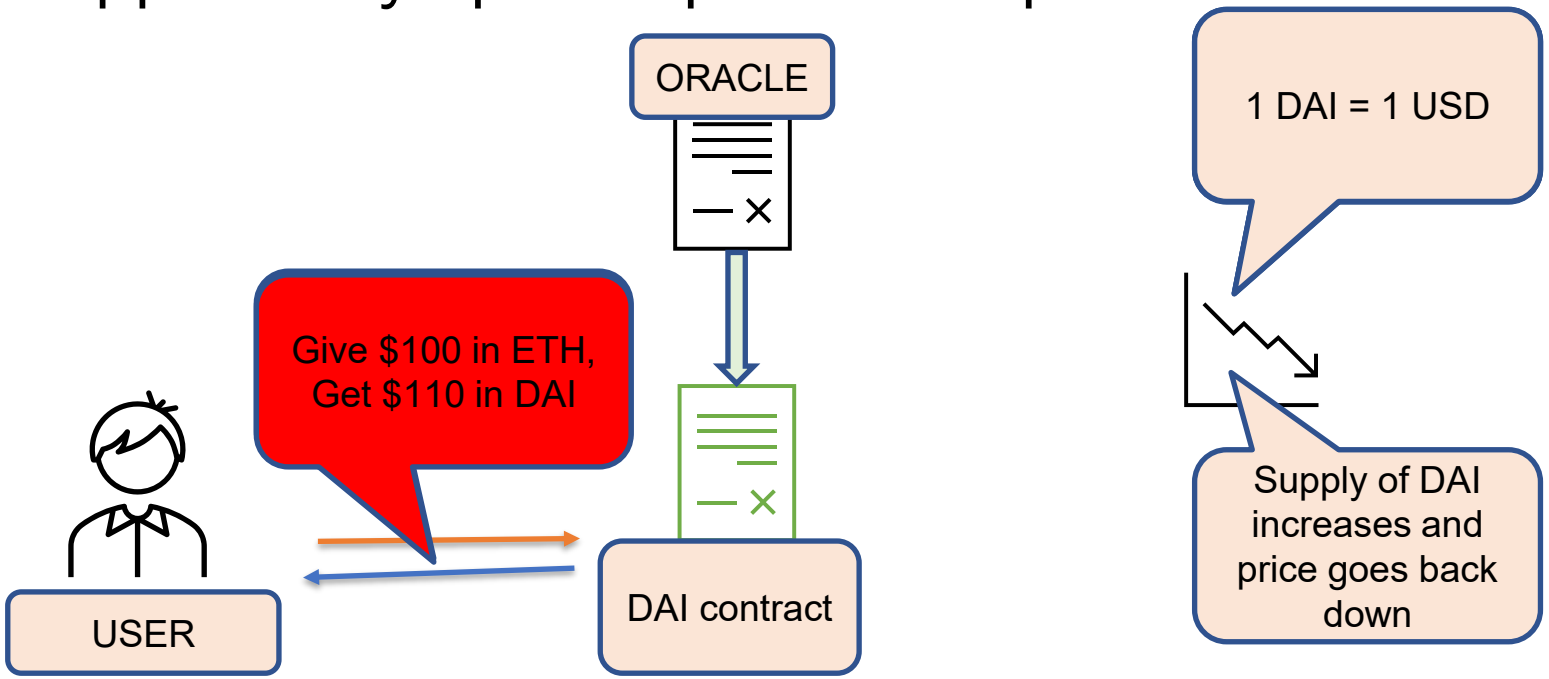
DAI: USD stablecoin on Ethereum

- DAI uses the borrow/lending method to peg
- User deposits collateral – can be ETH, BTC, USDC, etc.
- Value of collateral in USD is minted as DAI



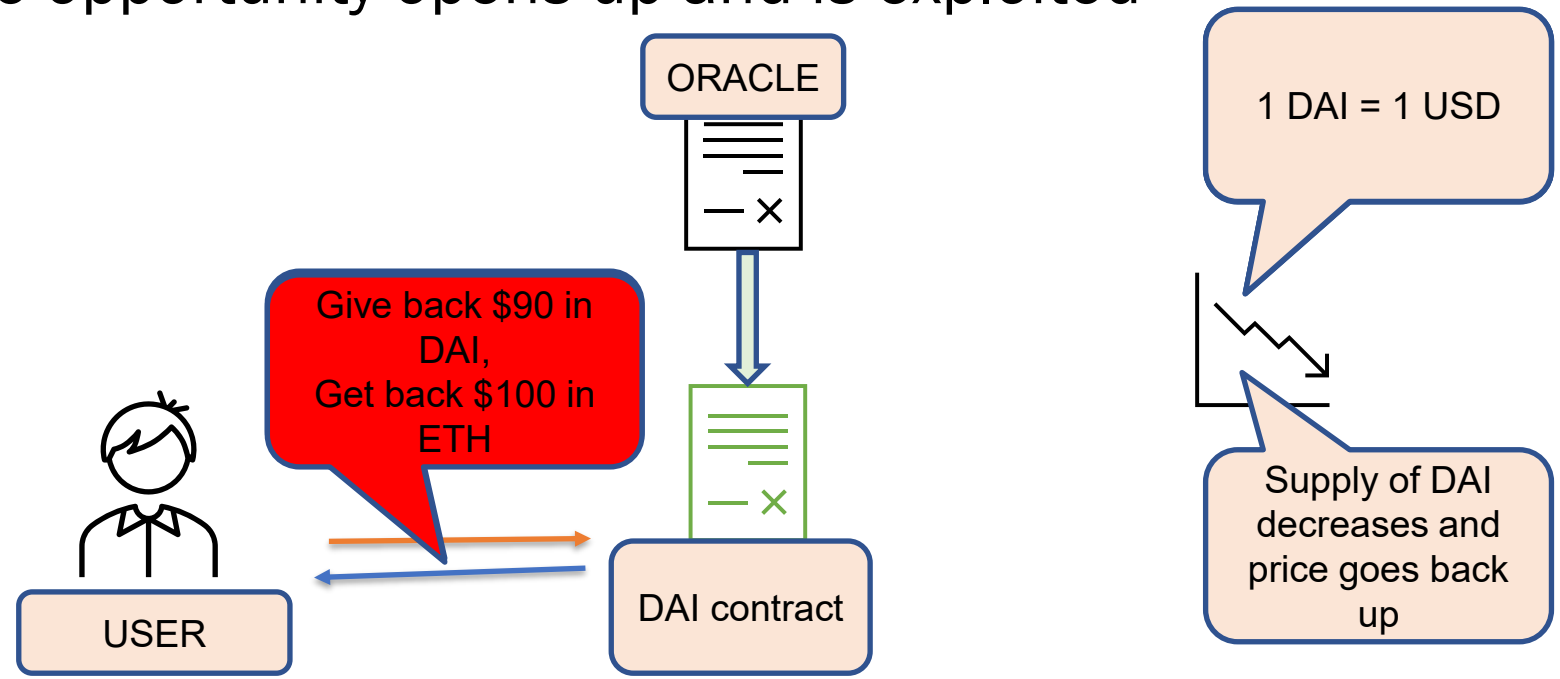
DAI: USD stablecoin on Ethereum

- What happens when 1 DAI = 1.1 USD?
- User incentivized to mint more DAI and sell on the market
- This is because value of collateral in USD is minted as DAI
- Arbitrage opportunity opens up and is exploited



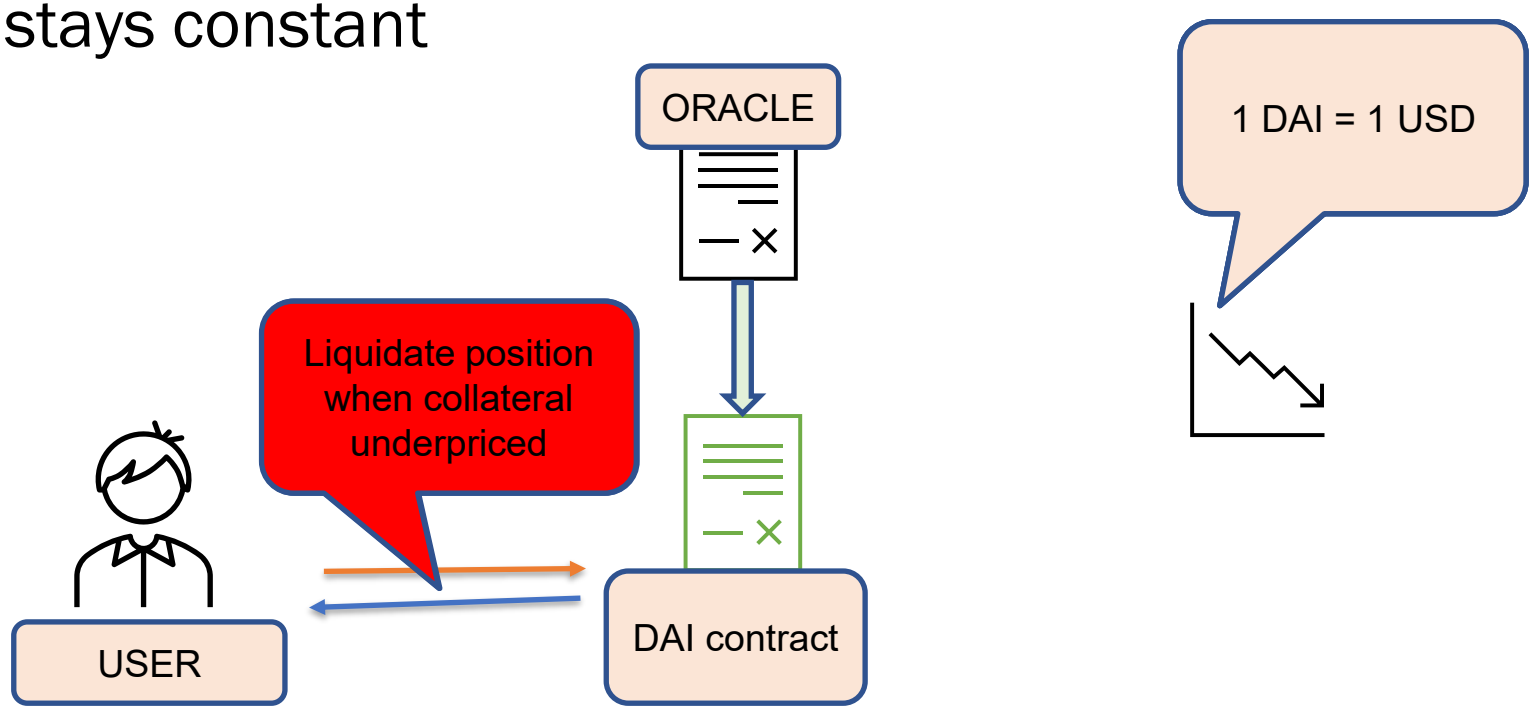
DAI: USD stablecoin on Ethereum

- What happens when 1 DAI = 0.9 USD?
- User incentivized to “burn” DAI by buying it on the market
- This is because it is now cheaper to pay back the loan than when you took it
- Arbitrage opportunity opens up and is exploited



DAI: USD stablecoin on Ethereum

- DAI follows over collateralization in its implementation
- Liquidation mechanism is similar to a lending protocol – except liquidations are automatic
- Oracle helps track prices of collateral, ensures the USD value of backing stays constant

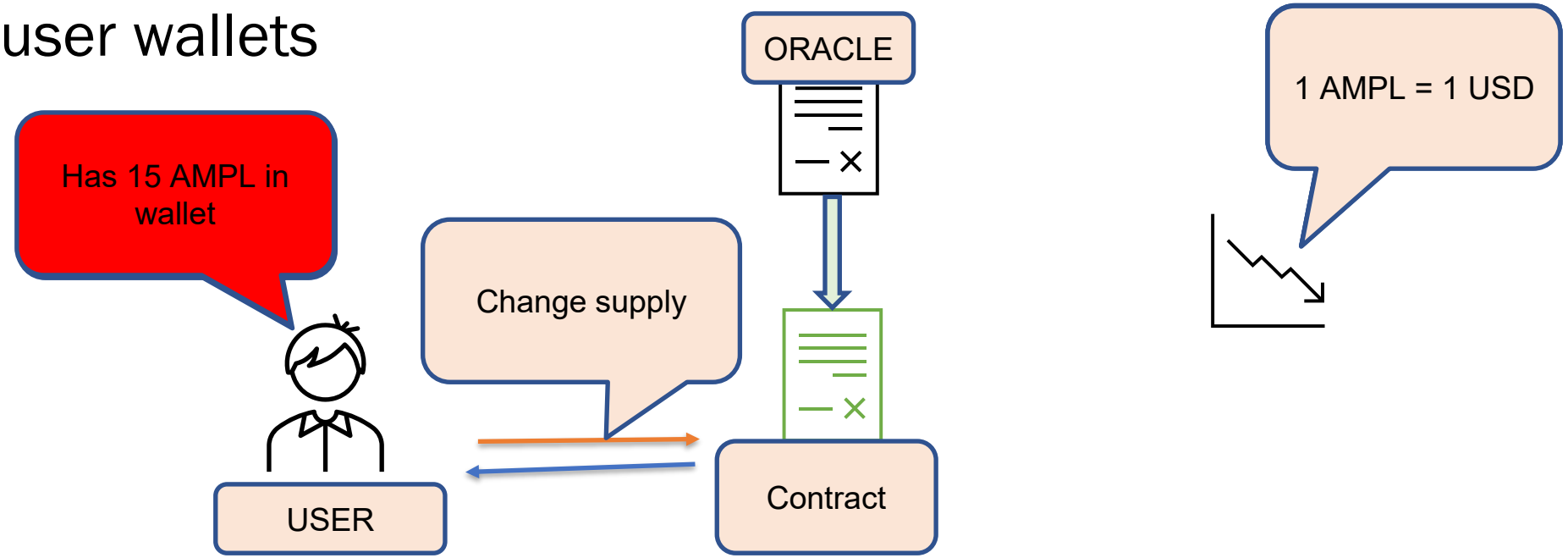


Algorithmic Stablecoins

- Algorithmic stablecoins mint/burn tokens directly in response to prices instead of relying on arbitrage incentives
- Does not involve over-collateralization and is hence more capital efficient
- However, such mechanisms have proved to be unstable: Basis Cash, Terra-Luna Crash
- Depegging risk is higher than in collateralized – and users have no assets to fall back on if a crash happens

Algorithmic Stablecoins: Rebasing

- Follows the simplest way to achieve price stability
- If oracle says price above peg, directly increase token supply in user wallets
- If oracle says price below peg, directly decrease token supply in user wallets

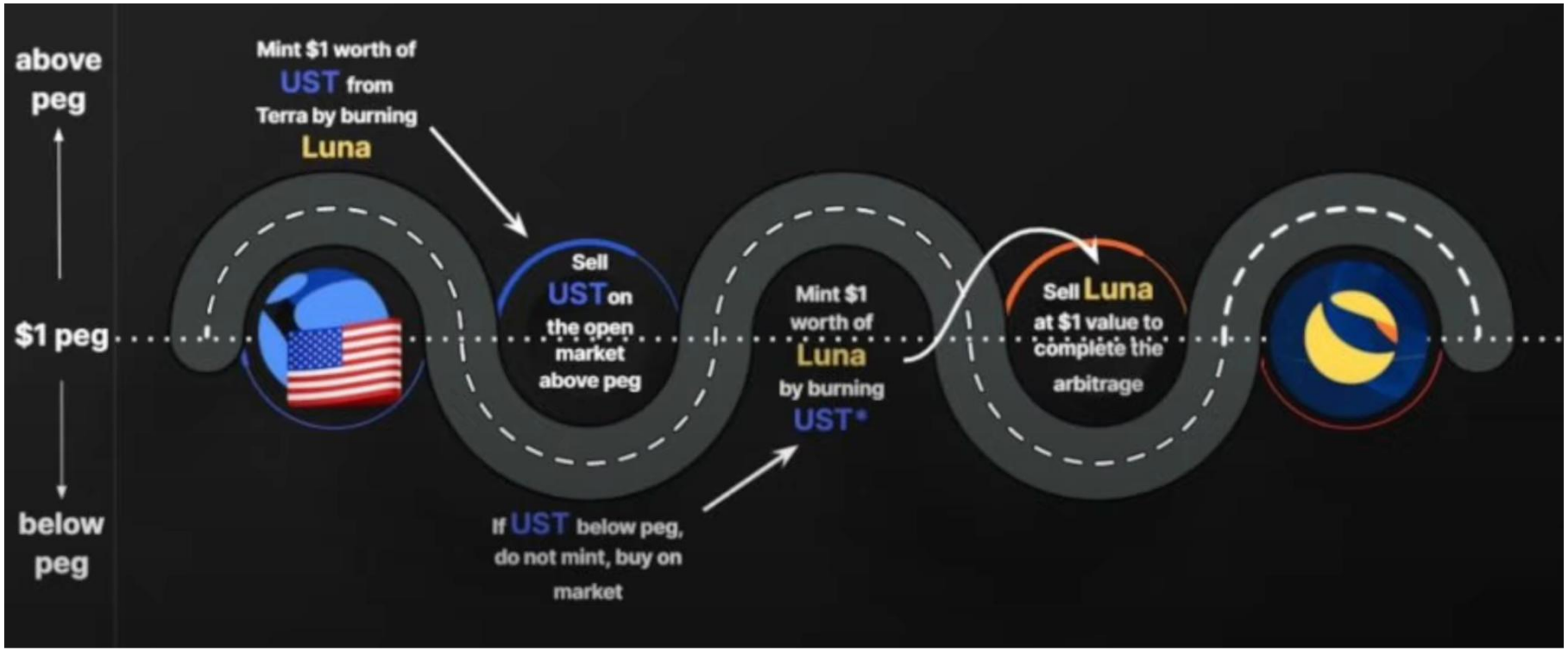


Algorithmic Stablecoins: Seigniorage

- Seigniorage stablecoins involve a pair of tokens, one of whose price is to be kept at a peg.
- When price goes below peg, bonds are sold in exchange for tokens, which are then burnt. This decreases token supply.
- Bonds are redeemed when price goes above the peg. This mints tokens, increasing its supply.

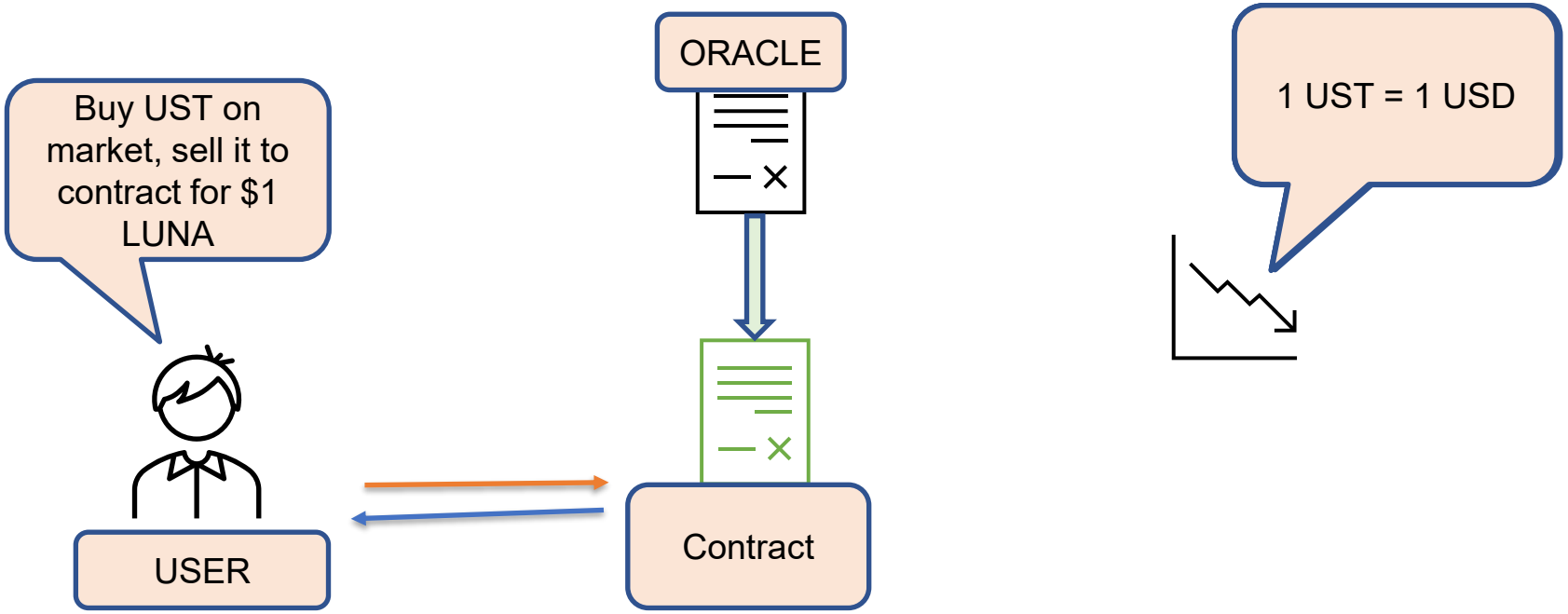
Algorithmic Stablecoins: Seigniorage

- E.g. Terra-Luna stablecoin pair – UST(Terra) was the stablecoin and Luna was the bond.



Algorithmic Stablecoins: Seigniorage

- How does this work? What keeps the peg?
- Key Idea: Smart Contract always allows $1 worth of bond to be exchanged for the stablecoin, no matter what its value on market.



Algorithmic Stablecoins: Depegging

- However, neither coin is backed by any other asset.
- What if users lose faith in the protocol itself?
- This leads to both tokens being sold on the open market rather than back to smart contract to be minted or burnt.
- That UST and LUNA lose value at the same time.
- This mints more LUNA, devaluing it even more.
- Both end up crashing – called a "death spiral"
- This indeed happened – UST lost its peg in May 2022

Reserve coins

- Coins are backed by assets instead being pegged to an asset
- Guarantee : User can exchange at least $1 of asset for each token – thus value of coin is lower bounded
- Uses bond mechanisms from seigniorage stablecoins to reduce volatility – not to keep a peg
- E.g. OHM – Olympus protocol
- Open problems :
  - Optimal Bonding mechanism
  - Optimal Monetary policy

LECTURE ENDS