Decentralized Finance I

Ronghui Gu

Fall 2025

Columbia University

Course website: https://verigu.github.io/6998Fall2025/

-1 NO Financial Advice!!!

0 Guest Lecture Next Week by YZI Labs (Binance Labs)

1 Stablecoins

What is a Stablecoin?

A cryptocurrency designed to trade at a fixed price

- Lives as a digital token on a blockchain
- Minimizes price volatility with respect to a stable fiat currency or asset

Why Stablecoins?

- Get the good part of Bitcoin (convenience, programmability, and/or censorship-resistance), without the price volatility
- Integrate real-world currencies into on-chain decentralized applications
  - Prediction markets, e.g., Polymarket
  - Decentralized exchange, e.g., Uniswap, PancakeSwap
  - Borrowing and lending, e.g., Aave

Types of Stablecoins

	Centralized	Decentralized
Collateralized	Custodian stablecoins	Synthetic stablecoins
Un(der)collateralized	Central bank digital currency (CBDC)	Under-collateralized stablecoins

Types of Stablecoins

	Centralized	Decentralized
Collateralized	Custodian stablecoins	Synthetic stablecoins
Un(der)collateralized	Central bank digital currency (CBDC)	Under-collateralized stablecoins

Custodian Stablecoins

- **Examples**: USDC, USDT, Paxos
- **Backing**:
  - dollars or “cash” in a custodian account
- **Peg mechanisms**: issuance and redemption
- **Risks**: counterparty risk, regulatory risk, operational risk

Custodian Stablecoins

- **Examples**: USDC, USDT, Paxos
- **Backing**:
  - dollars or “cash” in a custodian account
- **Peg mechanisms**: issuance and redemption
- **Risks**: counterparty risk, regulatory risk, opera

Custodian Stablecoins

- **Examples**: USDC, USDT, Paxos
- **Backing**:
  - dollars or “cash” in a custodian account
- **Peg mechanisms**: issuance and redemption
- **Risks**: counterparty risk, regulatory risk, operat

```
/**
 * @dev Function to mint tokens
 * @param _to The address that will receive the minted tokens.
 * @param _amount The amount of tokens to mint. Must be less than or equal
 * to the minterAllowance of the caller.
 * @return A boolean that indicates if the operation was successful.
 */
function mint(address _to, uint256 _amount)
    external
    whenNotPaused
    onlyMinters
    notBlacklisted(msg.sender)
    notBlacklisted(_to)
    returns (bool)
{
    require(_to != address(0), "FiatToken: mint to the zero address");
    require(_amount > 0, "FiatToken: mint amount not greater than 0");

    uint256 mintingAllowedAmount = minterAllowed[msg.sender];
    require(
        _amount <= mintingAllowedAmount,
        "FiatToken: mint amount exceeds minterAllowance"
    );

    totalSupply_ = totalSupply_.add(_amount);
    balances[_to] = balances[_to].add(_amount);
    minterAllowed[msg.sender] = mintingAllowedAmount.sub(_amount);
    emit Mint(msg.sender, _to, _amount);
    emit Transfer(address(0), _to, _amount);
    return true;
}
```

Custodian Stablecoins

- **Examples**: USDC, USDT, Paxos
- **Backing**:
  - dollars or “cash” in a custodian account
- **Peg mechanisms**: issuance and redemption
- **Risks**: counterparty risk, regulatory risk, opera

TECH

Stablecoin USDC nearly regains $1 peg after Circle says $3.3 billion held with SVB will be available

PUBLISHED MON, MAR 13 2023•7:11 AM EDT

Arjun Kharpal
@ARJUNKHARPAL

WATCH LIVE

KEY POINTS

- Circle, which issues USD Coin (USDC), said that the $3.3 billion it held with the now-collapsed Silicon Valley Bank will be “fully available” on Monday when U.S. banks open.
- After SVB’s collapse, USDC lost its $1 peg, falling as low as 86 cents on Saturday.
- The broader cryptocurrency market rallied Monday as regulators stepped in.
- Bitcoin jumped as much as 10%, rallying above $22,000.

Custodian Stablecoins

- **Examples**: USDC, USDT, Paxos
- **Backing**:
  - dollars or “cash” in a custodian account
- **Peg mechanisms**: issuance and redemption
- **Risks**: counterparty risk, regulatory risk, opera

Bitcoin.com News

News Learning Center Newsletters Advertise

NEWS BYTES
by Bitcoin.com

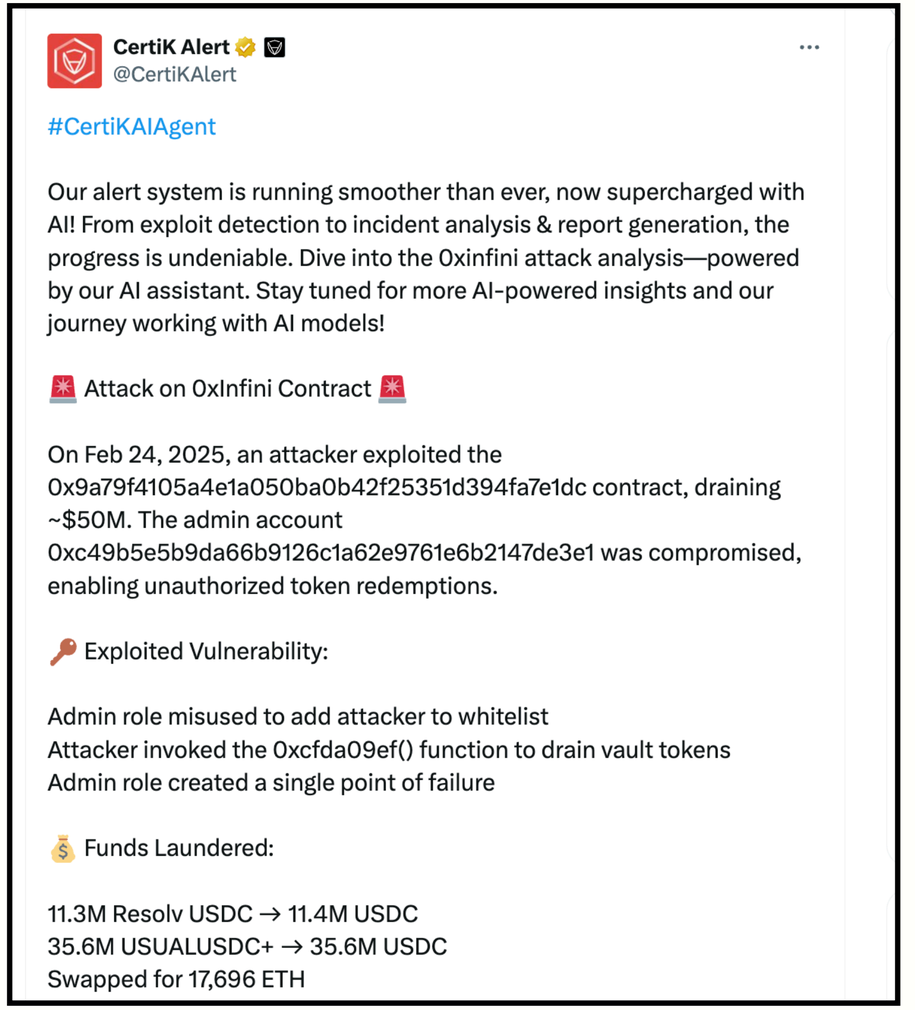
4 days ago

Coinbase to Delist USDT in Europe Amid New EU Regulations

Coinbase has announced plans to delist Tether’s USDT and other stablecoins that do not comply with the European Union’s Markets in Crypto-Assets (MiCA) regulations by December 30, 2024. This decision is part of Coinbase’s efforts to adhere to the new rules, which require stablecoin issuers to obtain an e-money license in an EU member state. Tether has yet to secure this license, prompting the delisting. Coinbase will provide options for users to convert their holdings to compliant stablecoins like Circle’s USDC.

Custodian Stablecoins

- **Examples**: USDC, USDT, Paxos
- **Backing**:
  - dollars or “cash” in a custodian account
- **Peg mechanisms**: issuance and redemption
- **Risks**: counterparty risk, regulatory risk, operational risk



CertiK Alert
@CertiKAlert

#CertiKAIAgent

Our alert system is running smoother than ever, now supercharged with AI! From exploit detection to incident analysis & report generation, the progress is undeniable. Dive into the 0xinfini attack analysis—powered by our AI assistant. Stay tuned for more AI-powered insights and our journey working with AI models!

🚨 Attack on 0xInfini Contract 🚨

On Feb 24, 2025, an attacker exploited the 0x9a79f4105a4e1a050ba0b42f25351d394fa7e1dc contract, draining ~$50M. The admin account 0xc49b5e5b9da66b9126c1a62e9761e6b2147de3e1 was compromised, enabling unauthorized token redemptions.

🔑 Exploited Vulnerability:

Admin role misused to add attacker to whitelist
Attacker invoked the 0xcfda09ef() function to drain vault tokens
Admin role created a single point of failure

💰 Funds Laundered:

11.3M Resolv USDC → 11.4M USDC
35.6M USUALUSDC+ → 35.6M USDC
Swapped for 17,696 ETH

Custodian Stablecoins

Custodian stablecoins are regarded not only as decentralized finance but also as real-world assets (RWA)

Types of Stablecoins

	Centralized	Decentralized
Collateralized	Custodian stablecoins	Synthetic stablecoins
Un(der)collateralized	Central bank digital currency (CBDC)	Under-collateralized stablecoins

CBDC

- **Backing**: fiat
- **Peg mechanisms**: issuance and redemption
- **Risks**: government control and surveillance

Pros:

- Free from credit and liquidity risk
- Lower cross-border payment costs

Cons:

- Financial system stability, policies, …
- Privacy

Types of Stablecoins

	Centralized	Decentralized
Collateralized	Custodian stablecoins	Synthetic stablecoins
Un(der)collateralized	Central bank digital currency (CBDC)	Under-collateralized stablecoins

Why Decentralized Stablecoins?

Decentralized economies deserve decentralized money

— Do Kwon, Co-founder of Terraform Labs

Types of Stablecoins

	Centralized	Decentralized
Collateralized	Custodian stablecoins	Synthetic stablecoins
Un(der)collateralized	Central bank digital currency (CBDC)	Under-collateralized stablecoins

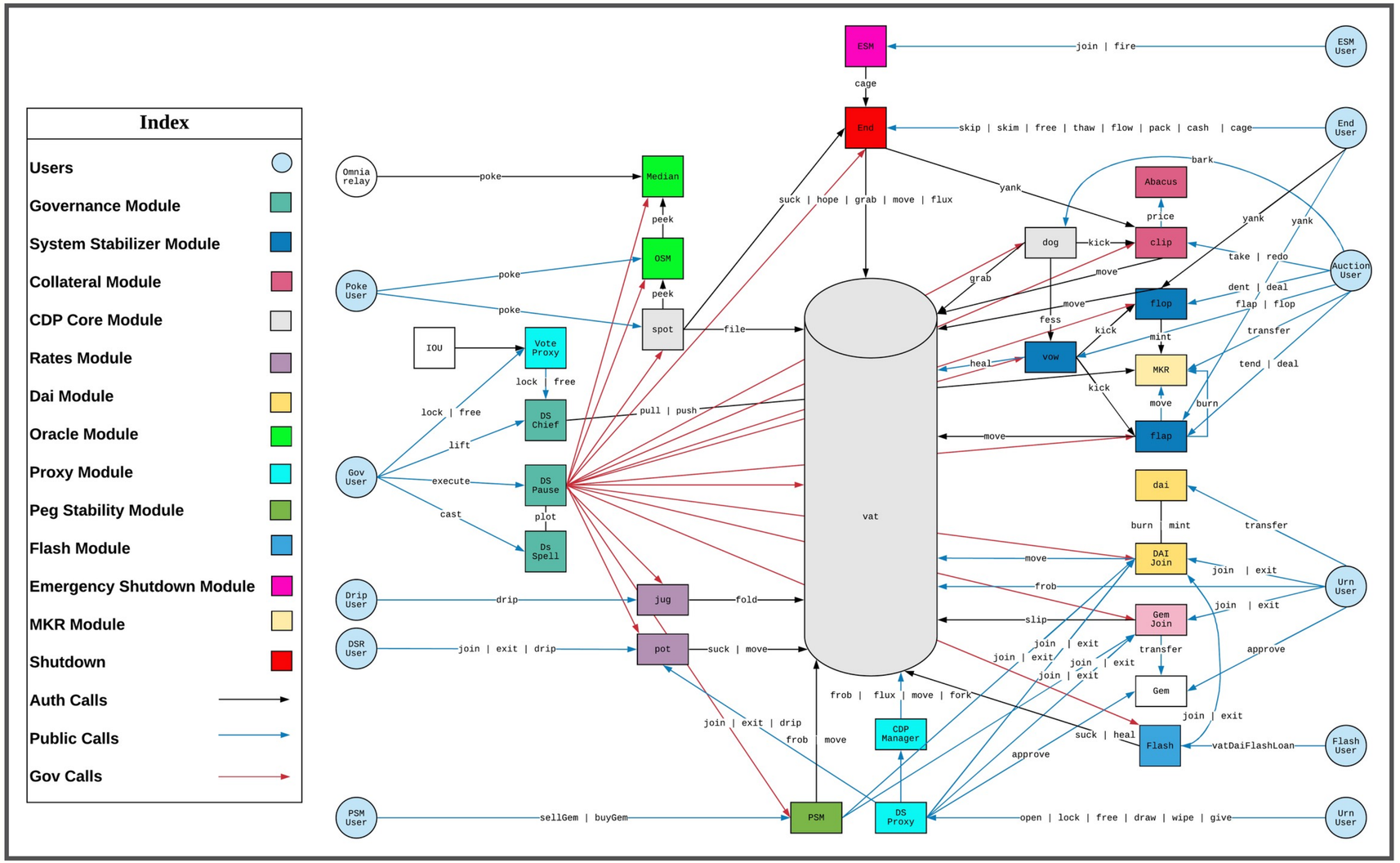
Synthetic Stablecoins

- **Examples**: Maker (DAI)
- **Backing**:
  - native (widely-adopted) cryptocurrencies (ETH, BTC, …)
- **Peg mechanisms**: interest rate
- **Risks**: liquidation cascade, oracle dependency

Synthetic Stablecoins — Maker

- How to mint DAI? 
  - Via smart contract
- How to stabilize DAI without centralization? 
  - Via interest rate, set by MakerDAO and voting by holders of MKR token
- What to do if collateral value drops below safe ratio?

Synthetic Stablecoins — Maker



Synthetic Stablecoins — Minting

Alice's Wallet		
Token	**Balance**	**USD Value**
ETH	1	$3000
DAI	0	$0

Alice's Vault		
Token	**Balance**	**USD Value**
ETH	0	$0
DAI	0	$0

Alice wants to use Maker to get leverage on ETH

Synthetic Stablecoins — Minting

Alice's Wallet		
Token	**Balance**	**USD Value**
ETH	0	$0
DAI	0	$0

Alice's Vault		
Token	**Balance**	**USD Value**
ETH	1	$3000
DAI	0	$0

Alice deposits 1 ETH into her Maker Vault

Synthetic Stablecoins — Minting

Alice's Wallet		
Token	**Balance**	**USD Value**
ETH	0	$0
DAI	2000	$2000

Alice's Vault		
Token	**Balance**	**USD Value**
ETH	1	$3000
DAI	-2000	-$2000

Alice uses her Maker Vault to mint 2000 DAI

Synthetic Stablecoins — Minting

Alice's Wallet		
Token	**Balance**	**USD Value**
ETH	0.66	$2000
DAI	0	$0

Alice's Vault		
Token	**Balance**	**USD Value**
ETH	1	$3000
DAI	-2000	-$2000

Alice trades 2000 DAI to Bob for 0.66 ETH

Synthetic Stablecoins — Minting

Alice's Wallet		
Token	**Balance**	**USD Value**
ETH	0.66	$2000
DAI	0	$0

Alice's Vault		
Token	**Balance**	**USD Value**
ETH	1	$3000
DAI	-2000	-$2000

Alice levels up her exposure to ETH,
and 2000 new DAI is out there in the world

Synthetic Stablecoins — Minting

Alice's Wallet		
Token	**Balance**	**USD Value**
ETH	0.66	$4000
DAI	0	$0

Alice's Vault		
Token	**Balance**	**USD Value**
ETH	1	$6000
DAI	-2000	-$2000

If ETH's price increases from $3000 to $6000?

Synthetic Stablecoins — Minting

Alice's Wallet		
Token	**Balance**	**USD Value**
ETH	0.33	$2000
DAI	2000	$2000

Alice's Vault		
Token	**Balance**	**USD Value**
ETH	1	$6000
DAI	-2000	-$2000

Alice gets 2000 DAI from Bob for 0.33 ETH

Synthetic Stablecoins — Closing the Vault

Alice's Wallet		
Token	**Balance**	**USD Value**
ETH	1.33	$8000
DAI	0	$0

Alice's Vault		
Token	**Balance**	**USD Value**
ETH	0	$0
DAI	0	$0

Alice then repays 2000 DAI to maker,
and closes her Vault

Synthetic Stablecoins — Stabilization

Alice's Vault		
Token	**Balance**	**USD Value**
ETH	1	$3000
DAI	-2000	-$2000

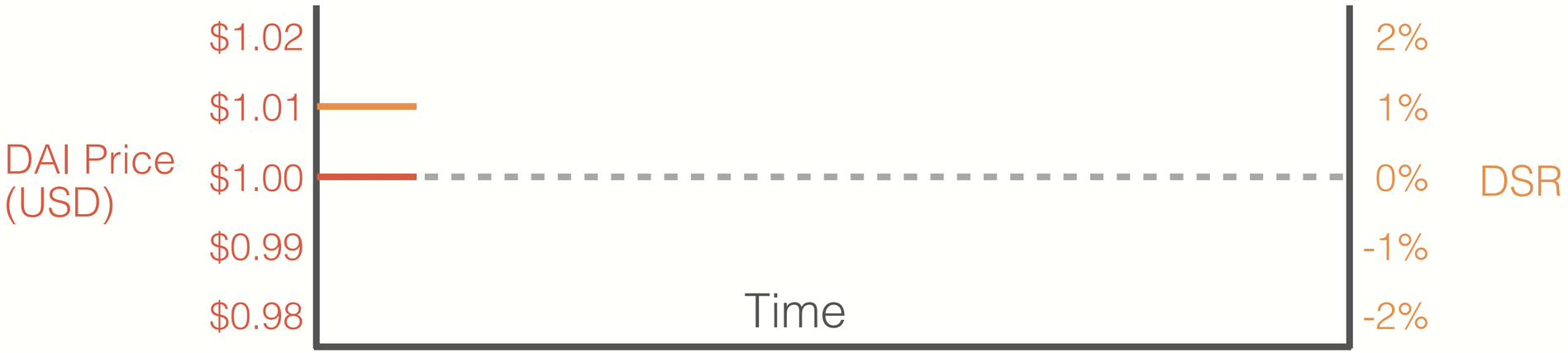
- Alice pays a stability fee as interest for borrowing DAI.
- Most of this stability fee goes to DAI holders through a mechanism called the DAI Savings Rate (DSR).
- Part of it goes to the MKR token that governs the protocol.

Synthetic Stablecoins — Stabilization

Alice's Vault, at time T+1		
Token	**Balance**	**USD Value**
ETH	1	$3000
DAI	-2001	-$2001

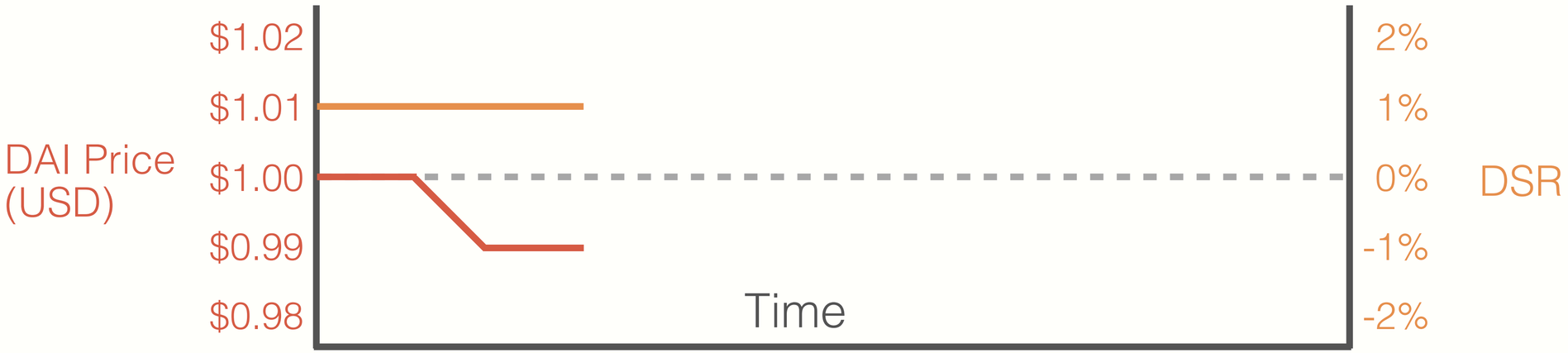
- Alice pays a stability fee as interest for borrowing DAI.
- Most of this stability fee goes to DAI holders through a mechanism called the DAI Savings Rate (DSR).
- Part of it goes to the MKR token that governs the protocol.

Synthetic Stablecoins — Stabilization



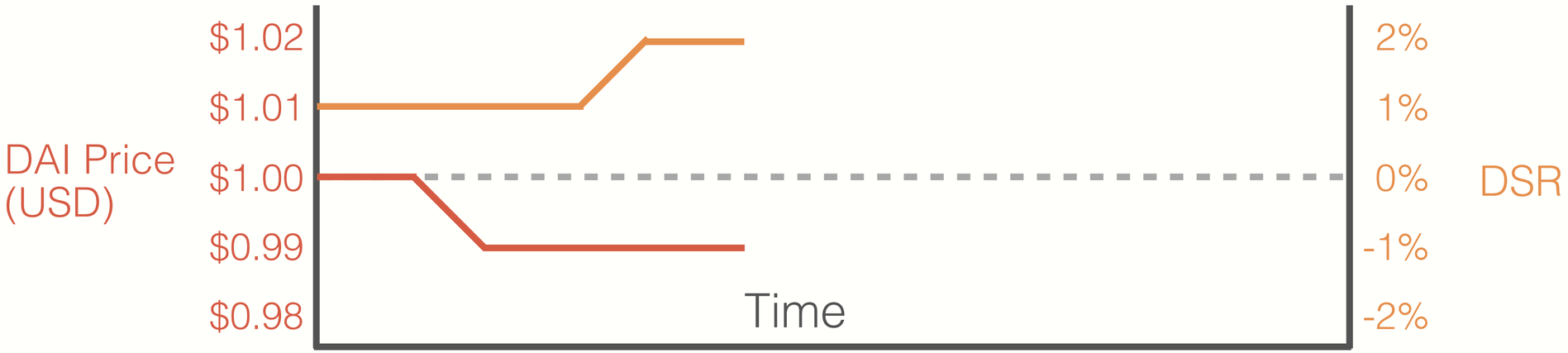
The stability fee and DSR are raised when DAI is trading below $1 (to discourage borrowing and encourage DAI holding), and lowered when DAI is trading above $1

Synthetic Stablecoins — Stabilization



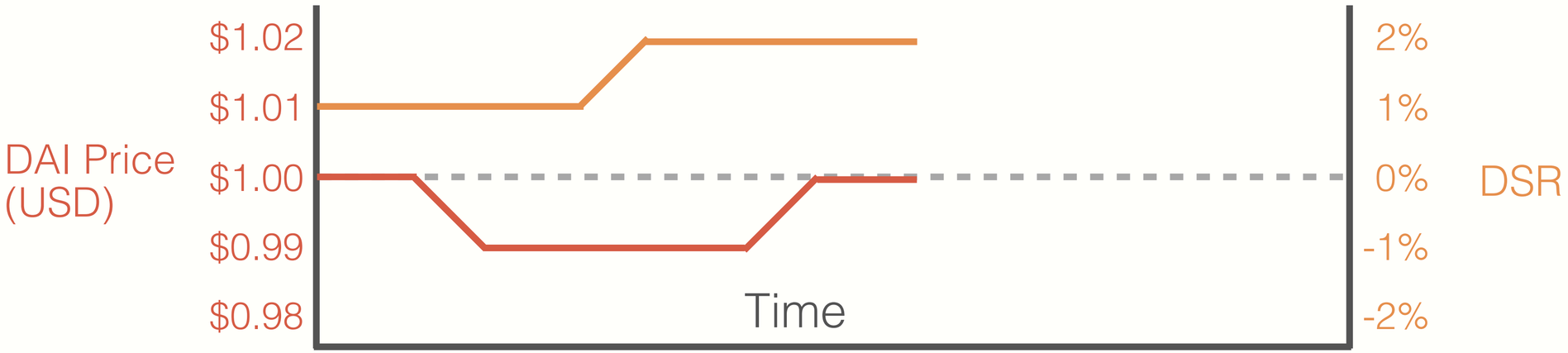
When the DAI price falls below $1…

Synthetic Stablecoins — Stabilization



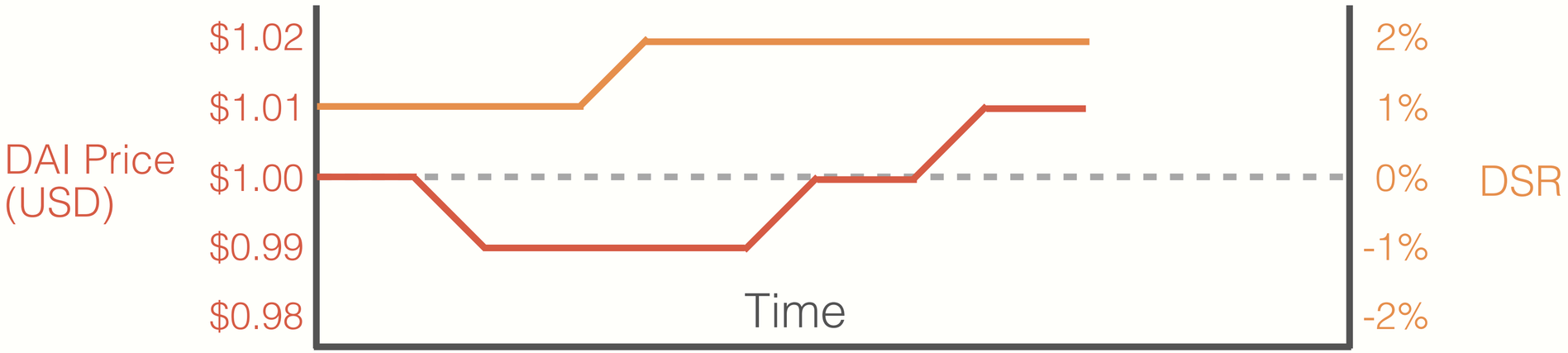
…the DSR (and stability fee) are raised to encourage DAI holding…

Synthetic Stablecoins — Stabilization



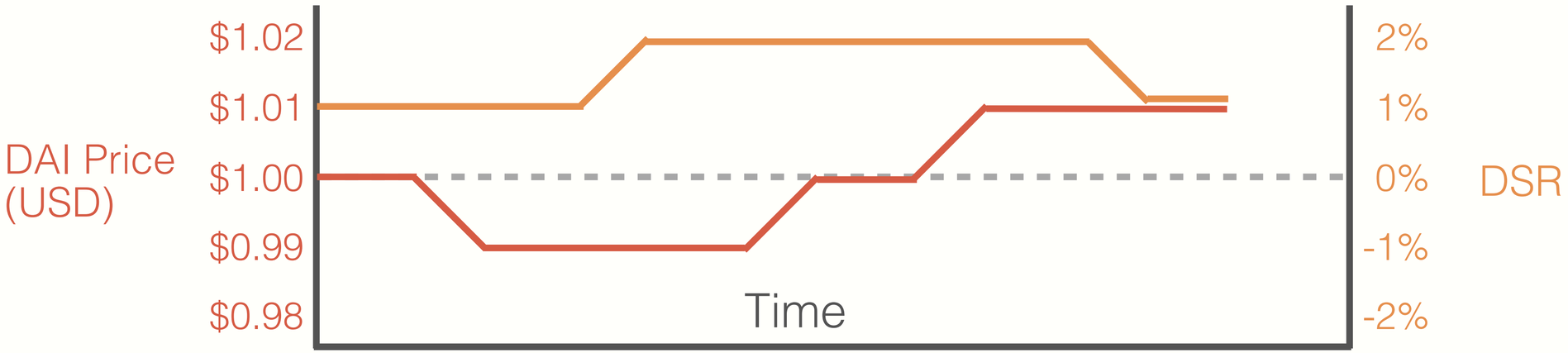
…(hopefully) causing the peg to be restored

Synthetic Stablecoins — Stabilization



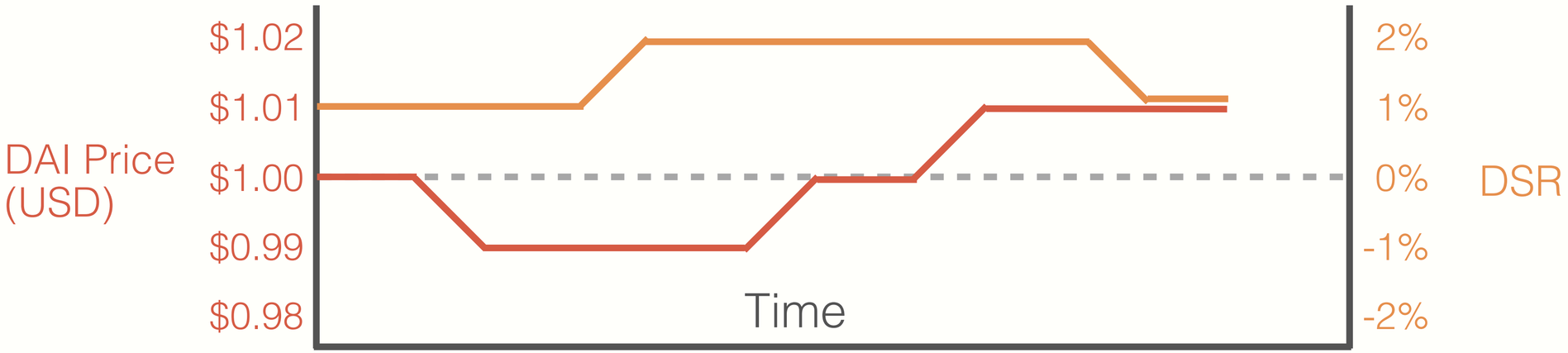
If DAI trades above $1...

Synthetic Stablecoins — Stabilization



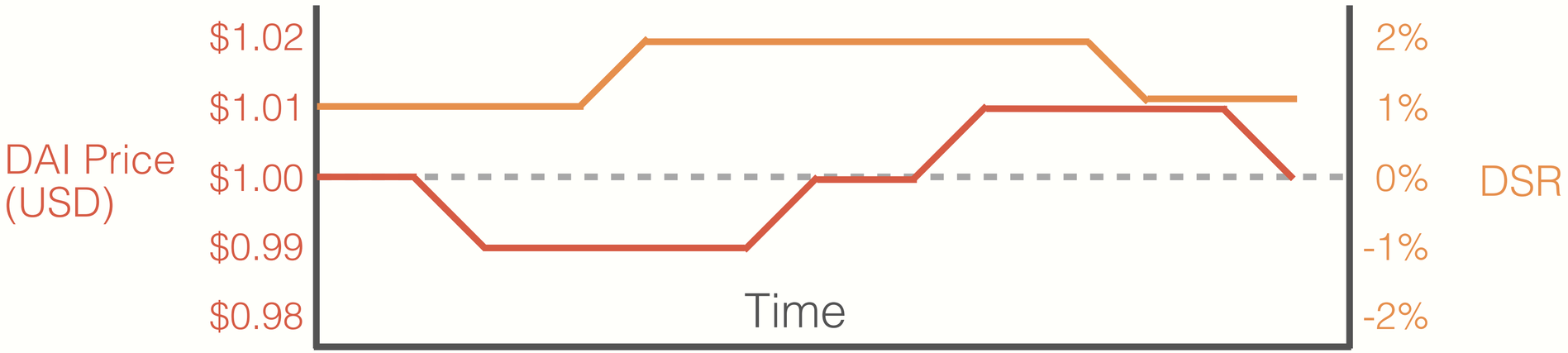
…the DSR is lowered…

Synthetic Stablecoins — Stabilization



…the DSR is lowered…

Synthetic Stablecoins — Stabilization



...until the peg is restored...

Synthetic Stablecoins — Liquidation

Alice's Vault		
Token	**Balance**	**USD Value**
ETH	1	$3000
DAI	-2000	-$2000

Alice's vault is 150% collateralized, since it has $3000 of collateral and $2000 of debt

Synthetic Stablecoins — Liquidation

Alice's Vault		
Token	**Balance**	**USD Value**
ETH	1	$2500
DAI	-2000	-$2000

If the price of ETH falls to $2500, Alice is only 125% collateralized, which means her vault can be liquidated

Synthetic Stablecoins — Liquidation

Alice's Vault		
Token	**Balance**	**USD Value**
ETH	0	$0
DAI	500	$500

In liquidation, the protocol auctions off Alice's ETH in the vault to repay her DAI debt. She gets any extra DAI from the sale, minus fees (to MKR holders)

Synthetic Stablecoins — Liquidation

Alice's Vault		
Token	**Balance**	**USD Value**
ETH	1	$1000
DAI	-2000	-$2000

What if the price of ETH falls sharply to $1000?

Synthetic Stablecoins — Liquidation

Alice's Vault		
Token	**Balance**	**USD Value**
ETH	1	$1000
DAI	-2000	-$2000

What if the price of ETH falls sharply to $1000?

- Collateral auction
- Surplus buffer usage ($50M in total)
- Minting MKR tokens

MKR backstop

Alice's Vault		
Token	**Balance**	**USD Value**
ETH	1	$1000
DAI	-2000	-$2000

Recall that when Alice's Maker vault had less than 150% collateral, the ETH was auctioned off

MKR backstop

Alice's Vault		
Token	**Balance**	**USD Value**
ETH	0	0
DAI	-1000	-$1000

ETH is only sold for 1000 DAI, which is not enough to repay her 2000 DAI debt. The protocol now has a deficit—there is 1000 unbacked DAI out there

MKR backstop

Alice's Vault		
Token	**Balance**	**USD Value**
ETH	0	0
DAI	0	0

The protocol mints new MKR tokens and auctions them off for 1000 DAI, remedying the deficit. Recall that MKR tokens earn fees during normal operation of the protocol

Types of Stablecoins

	Centralized	Decentralized
Collateralized	Custodian stablecoins	Synthetic stablecoins
Un(der)collateralized	Central bank digital currency (CBDC)	Under-collateralized stablecoins

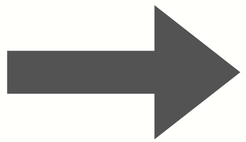
Under-collateralized Stablecoins

- **Examples**: FEI (no longer maintained), USDe, ListaDAO
- **Backing**: diversified portfolio
- **Peg mechanisms**: redemption + surplus reserve
- **Risks**: market risk, oracle dependency

Under-collateralized Stablecoins

“ABC” protocol balance sheet		
Token	**Balance**	**USD Value**
ETH	1	$3000
DAI	1000	$1000
USDC	2000	$2000
ABC	-5000	-$5000

Surplus reserve = $1000

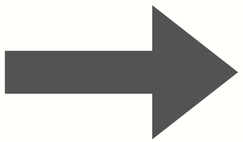


“ABC” protocol balance sheet		
Token	**Balance**	**USD Value**
ETH	1	$3000
DAI	1600	$1600
USDC	2000	$2000
ABC	-5600	-$5600

Surplus reserve = $1000

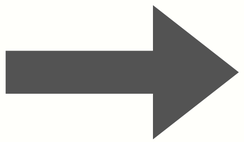
Mint 600 ABC with $600 collateral in

Under-collateralized Stablecoins



“ABC” protocol balance sheet		
Token	**Balance**	**USD Value**
ETH	1	$3000
DAI	1600	$1600
USDC	2000	$2000
ABC	-5600	-$5600

Surplus reserve = $1000

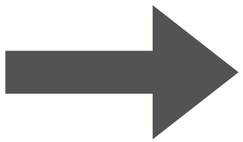


“ABC” protocol balance sheet		
Token	**Balance**	**USD Value**
ETH	1	$3000
DAI	1000	$1000
USDC	2000	$2000
ABC	-5000	-$5000

Surplus reserve = $1000

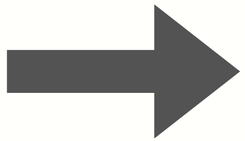
Burn 600 ABC with $600 collateral out

Under-collateralized Stablecoins



“ABC” protocol balance sheet		
Token	**Balance**	**USD Value**
ETH	1	$3000
DAI	1000	$1000
USDC	2000	$2000
ABC	-5000	-$5000

Surplus reserve = $1000

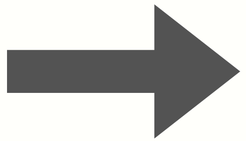


“ABC” protocol balance sheet		
Token	**Balance**	**USD Value**
ETH	1	$2500
DAI	1000	$1000
USDC	2000	$2000
ABC	-5000	-$5000

Surplus reserve = $500

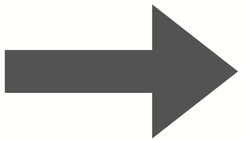
ETH price drops to $2500

Under-collateralized Stablecoins



“ABC” protocol balance sheet		
Token	**Balance**	**USD Value**
ETH	1	$2500
DAI	1000	$1000
USDC	2000	$2000
ABC	-5000	-$5000

Surplus reserve = $500



“ABC” protocol balance sheet		
Token	**Balance**	**USD Value**
ETH	1.1	$2750
DAI	1000	$1000
USDC	2000	$2000
ABC	-5000	-$5000

Surplus reserve = $750

Stake ETH to get 0.1 more ETH

Seigniorage Shares

- **Examples**: Maker (backstop), Terra
- **Backing**: confidence
- **Peg mechanisms**: supply expansion and contraction
- **Risks**: death spiral, oracle dependency

2 Luna Crash

The Fall of Terra

The Fall of Terra: A Timeline of the Meteoric Rise and Crash of UST and LUNA

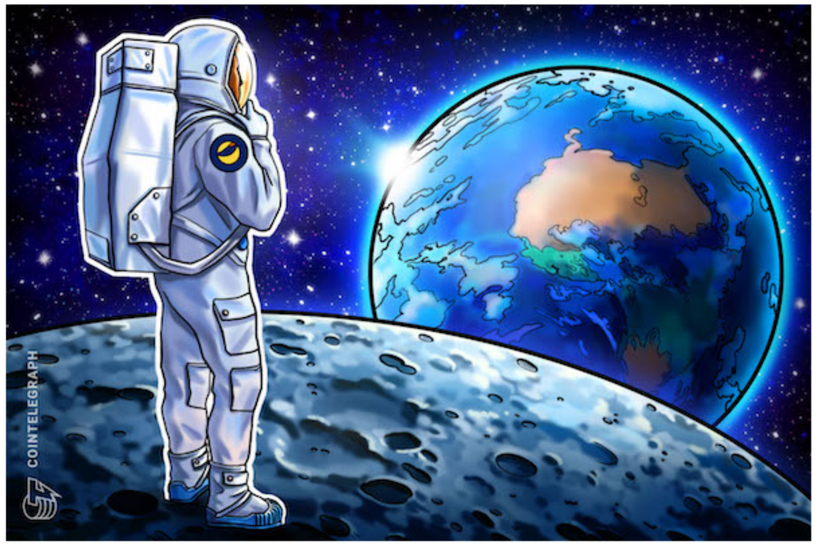
A detailed timeline of Terra's journey from its underdog start as a payments app in South Korea to a $60 billion crypto ecosystem to one of the biggest failures in crypto.

By Krisztian Sandor, Ekin Genç Jun 1, 2022 at 11:37 p.m. Updated Apr 15, 2024 at 6:21 a.m.

(Zoltan Tasi/Unsplash, modified by CoinDesk)

The Fall of Terra

But the most notable incident was CertiK's full-scope audit of Terra, which later collapsed and brought half the crypto industry down with it. The audit has since been taken down as they have taken a more reflective approach, but bits and pieces remain online.



Terra as envisaged by Cointelegraph's art department. They forgot to set the earth and moon on fire, however.

Seigniorage Shares — Terra

- **Terra USD:** UST
- **Backing**: Luna tokens
- **Peg mechanisms**:
  - When UST's price > $1, burn $1 Luna to mint 1 UST
  - When UST's price < $1, mint $1 Luna by burning 1 UST

Seigniorage Shares — Terra

- **Terra USD:** UST
- **Backing**: Luna tokens
- **Peg mechanisms**:
  - When UST's price > $1, burn $1 Luna to mint 1 UST
  - When UST's price < $1, mint $1 Luna by burning 1 UST
  - Plus lots of BTCs

3

Discussion Session

How to form a startup team?