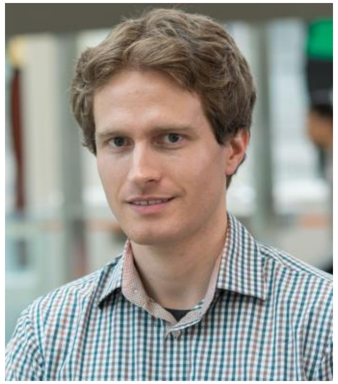
Decentralized Finance

The (Un)Reasonable Design of

Stablecoins

Guest Lecture: **Ariah Klages-Mundt**



Cornell University

Decentralized Finance

Instructors: Dan Boneh, Arthur Gervais, Andrew Miller, Christine Parlour, Dawn Song





Stanford University

Imperial College London

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

Berkeley UNIVERSITY OF CALIFORNIA

Recap

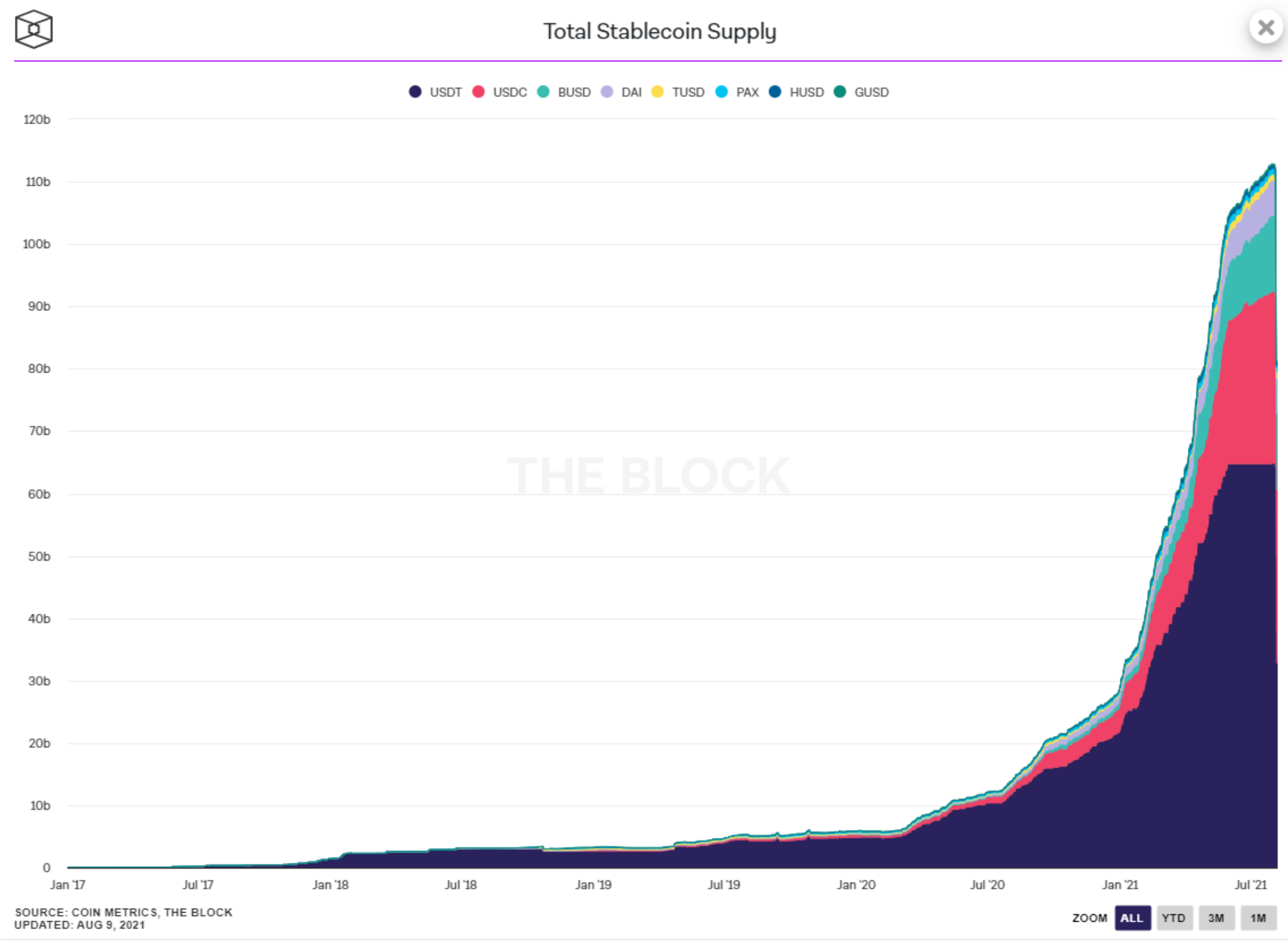
- **Blockchain:** new way for mistrusting agents to cooperate w/o trusted third parties

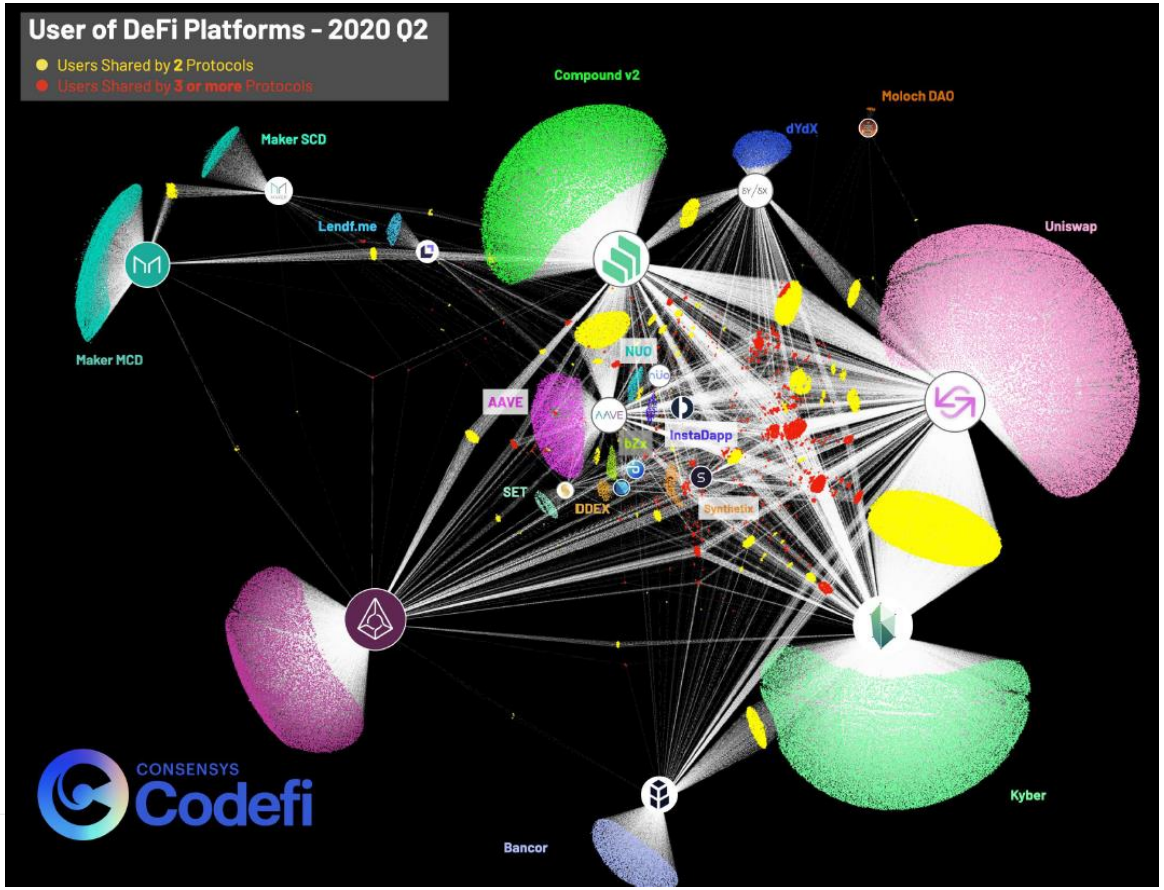
- **Cryptocurrency:** an asset native to a blockchain

- **Smart contracts:** programs that run on the blockchain computer

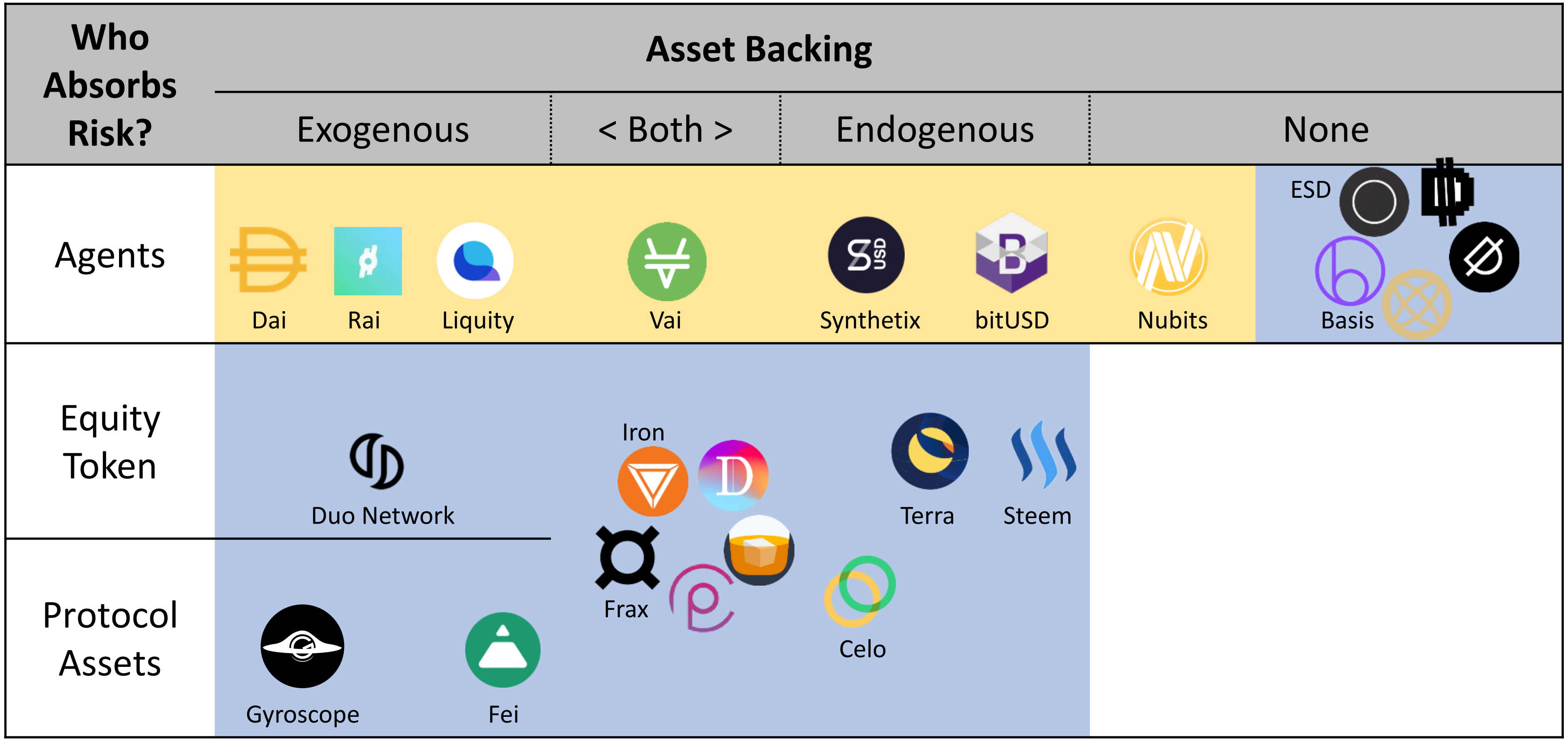
- **Stablecoins:** cryptocurrency with added economic structure that
  - Aim: stabilize price/purchasing power
  - Constructed using smart contracts

Stablecoins: A Growing DeFi Foundation





Over past year, many new types of stablecoins…



Issuance

Agent

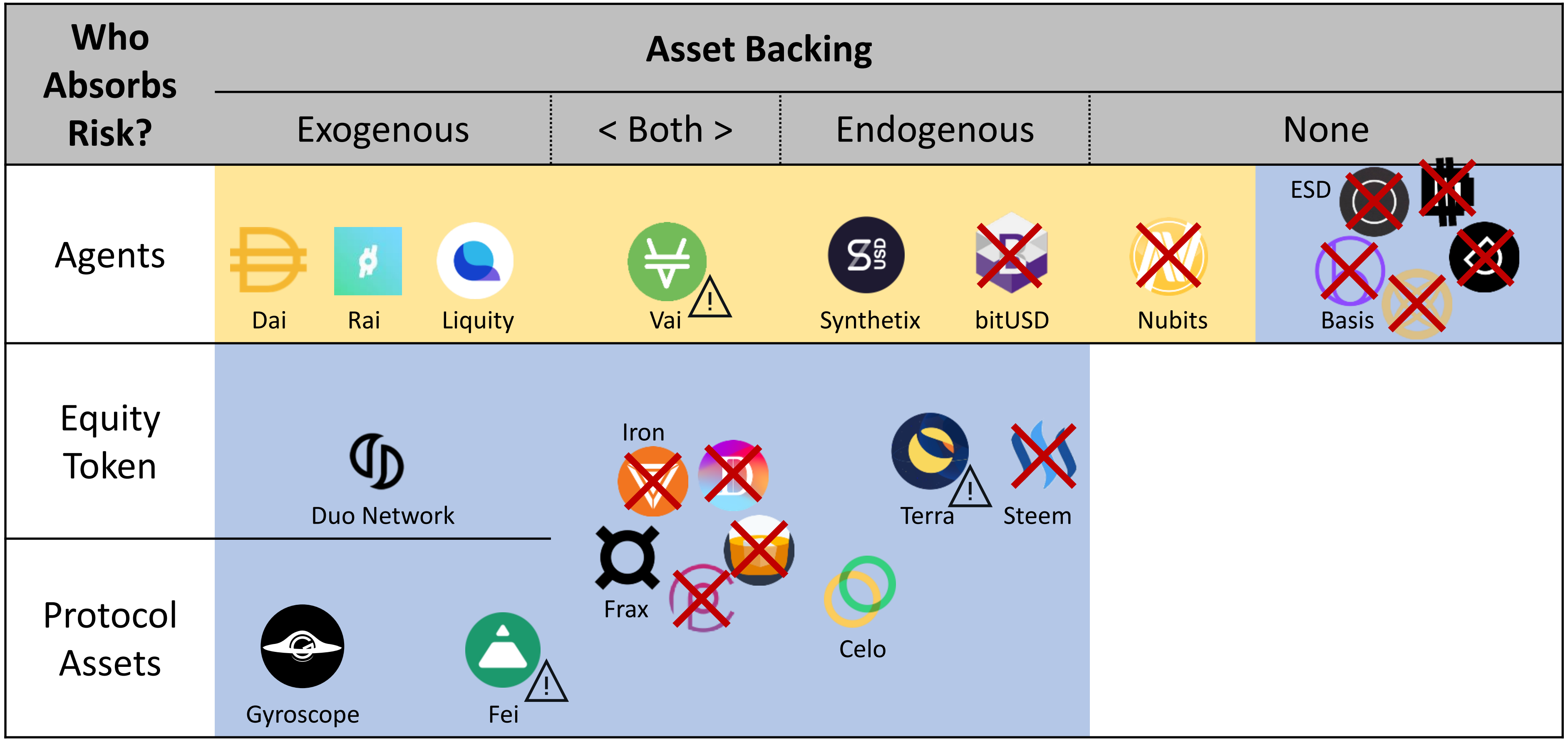
Algorithmic

Exogenous = asset price independent of protocol

Endogenous = asset price self-referential with protocol

Agent = speculative agents decide, as applicable, risk exposure or issuance

Over past year, many new types of stablecoins…



Issuance

Agent
Algorithmic

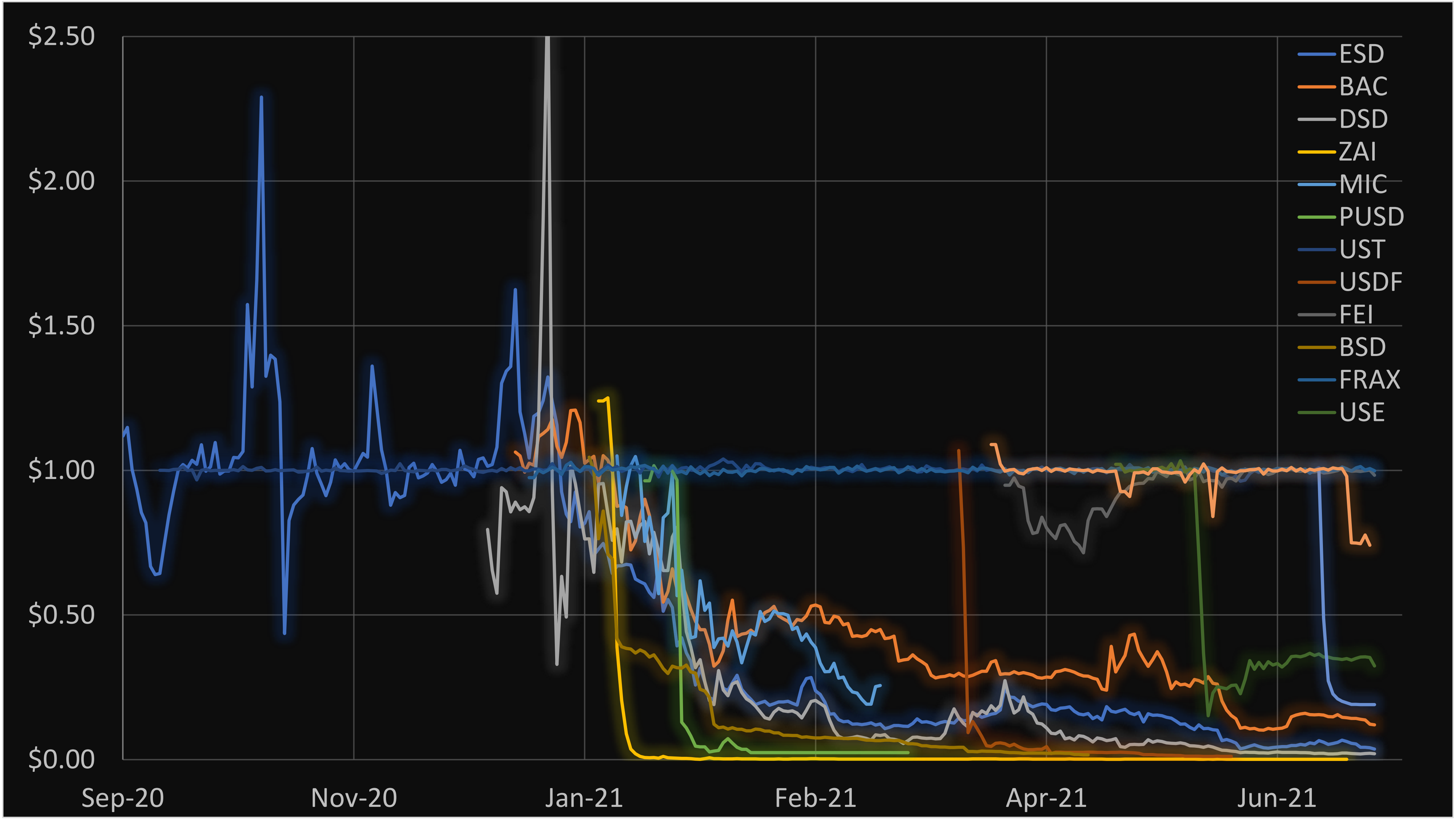
Exogenous = asset price independent of protocol

Endogenous = asset price self-referential with protocol

Agent = speculative agents decide, as applicable, risk exposure or issuance

⚠ = recent problems observed, X = broken

Over past year, many new types of stablecoins…



This Lecture

- Three fundamental design problems
    1. Technical security
    2. Economic security
    3. Economic stability

Part I: Anatomy of Stablecoins

Part II: Technical and Economic Security

Part III: Deleveraging Spirals (Economic Stability)

Part IV: Design of Algorithmic Primary Markets (Economic Stability)

---Part I---
Anatomy of Stablecoins

https://defi-learning.org

Risk-based Overview

Stablecoin

Custodial

Non-Custodial

Risks
- Counterparty credit risk
- Censorship risk
- Traditional financial risks

Well understood!

New Risks and attacks
- Deleveraging risks
- Price feeds, governance
- Miner extractable value
- Smart contract bugs

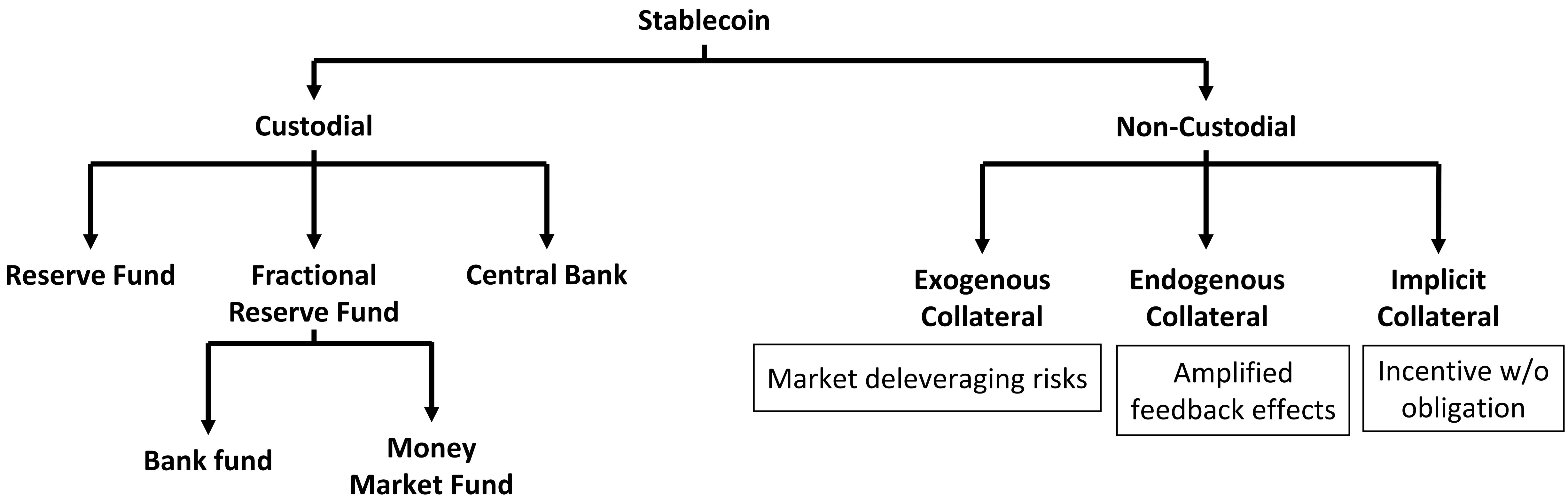
Not well understood

Risk-based Overview

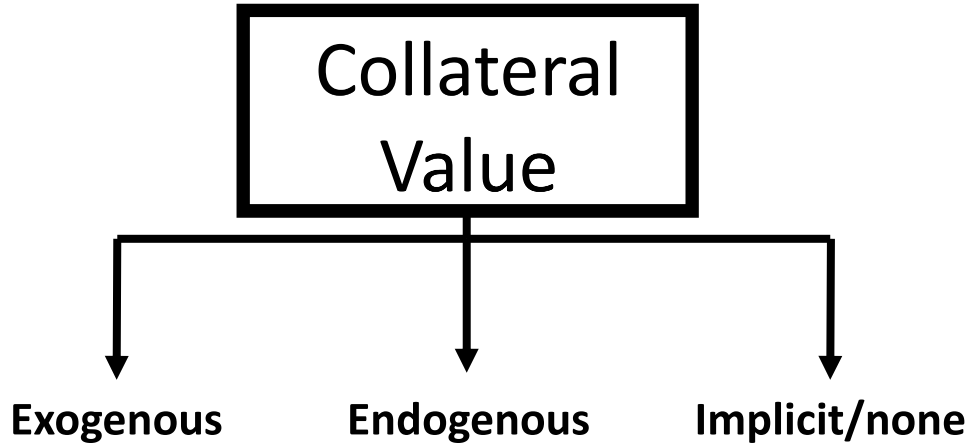
Stablecoin

- **Custodial**
  - **Reserve Fund**
    - ETF models
  - **Fractional Reserve Fund**
    - **Bank fund**
      - Bank run models
    - **Money Market Fund**
      - Pegged money market funds
  - **Central Bank**
    - Currency Models
- **Non-Custodial**

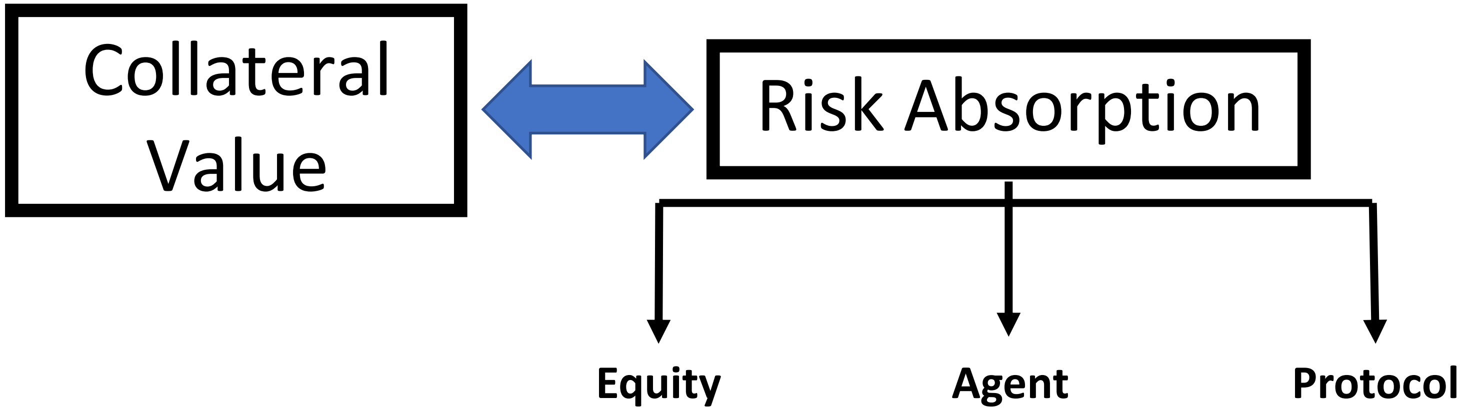
Risk-based Overview



Anatomy of Non-custodial Stablecoins



Anatomy of Non-custodial Stablecoins

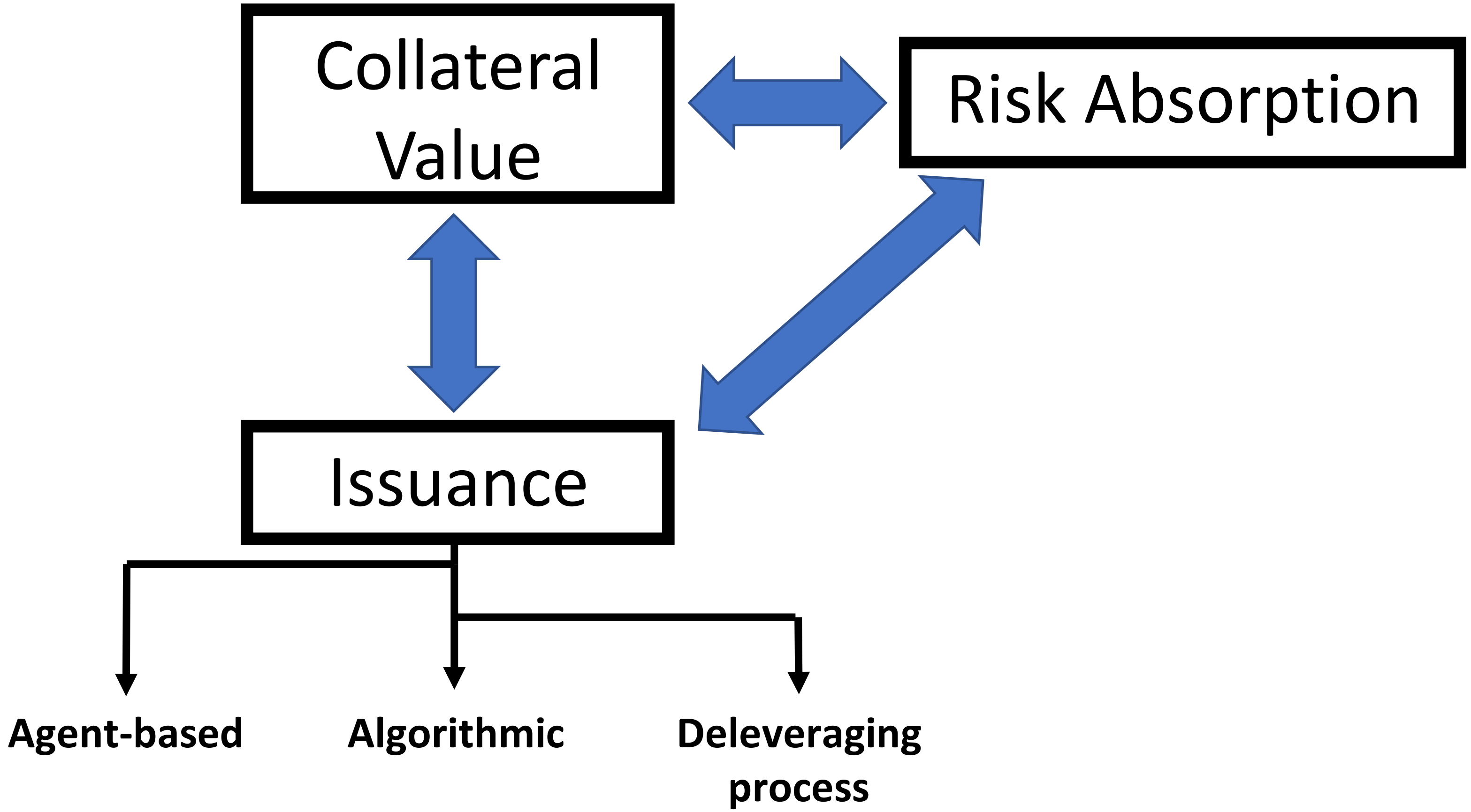


How Risk is Absorbed

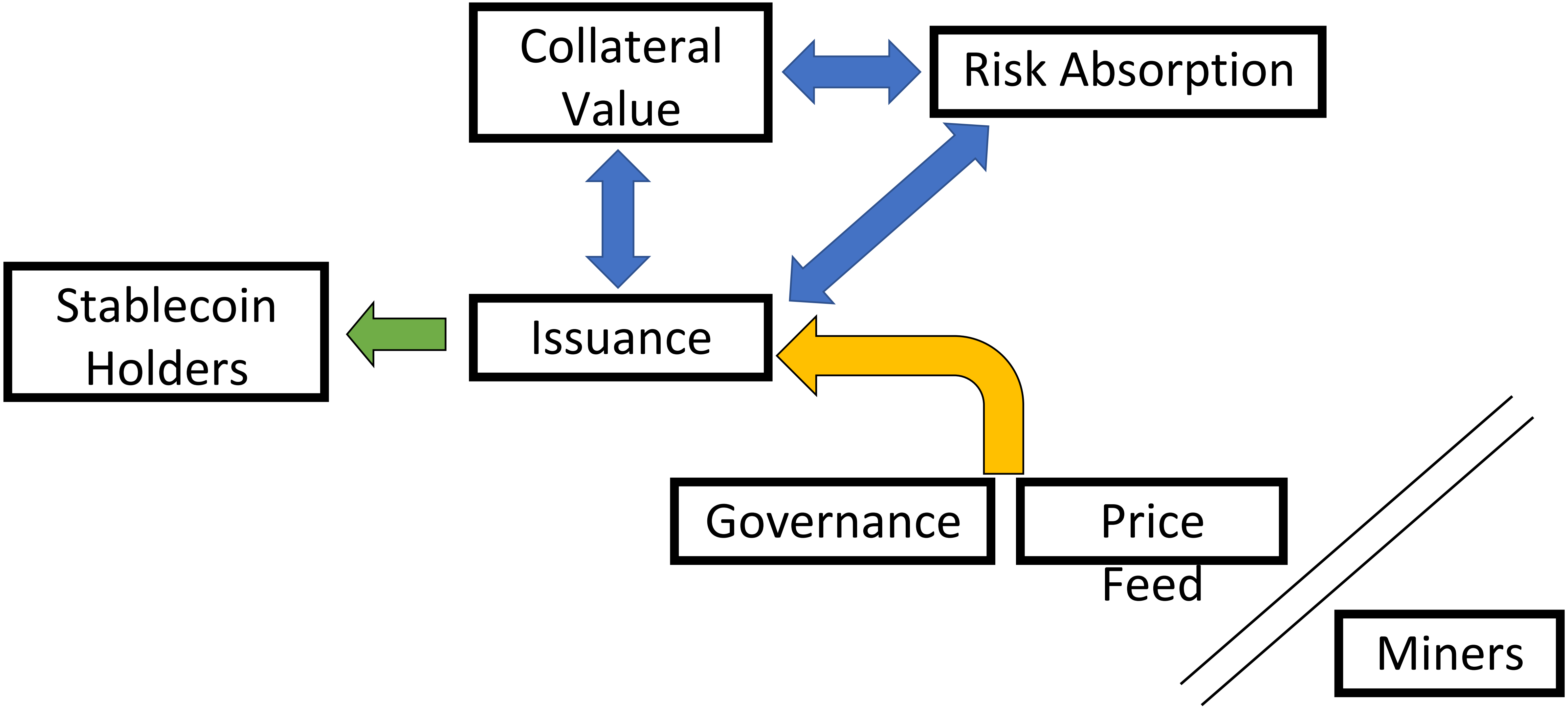
- **Leverage-based:** like a CDO
  - w/ exogenous or endogenous collateral
  - Seigniorage shares: market cap of endogenous “equity shares” meant to absorb volatility
- **Basis design:** speculators meant to maintain peg by betting on future supply expansions (leverage on “implicit collateral”) during a crisis
  - No pre-committed collateral
  - Speculators must bet that supply will expand beyond pre-crisis level
- **Reserve-backed:** protocol market makes around peg using internal reserve

…also various meta-stablecoins

Anatomy of Non-custodial Stablecoins



Anatomy of Non-custodial Stablecoins

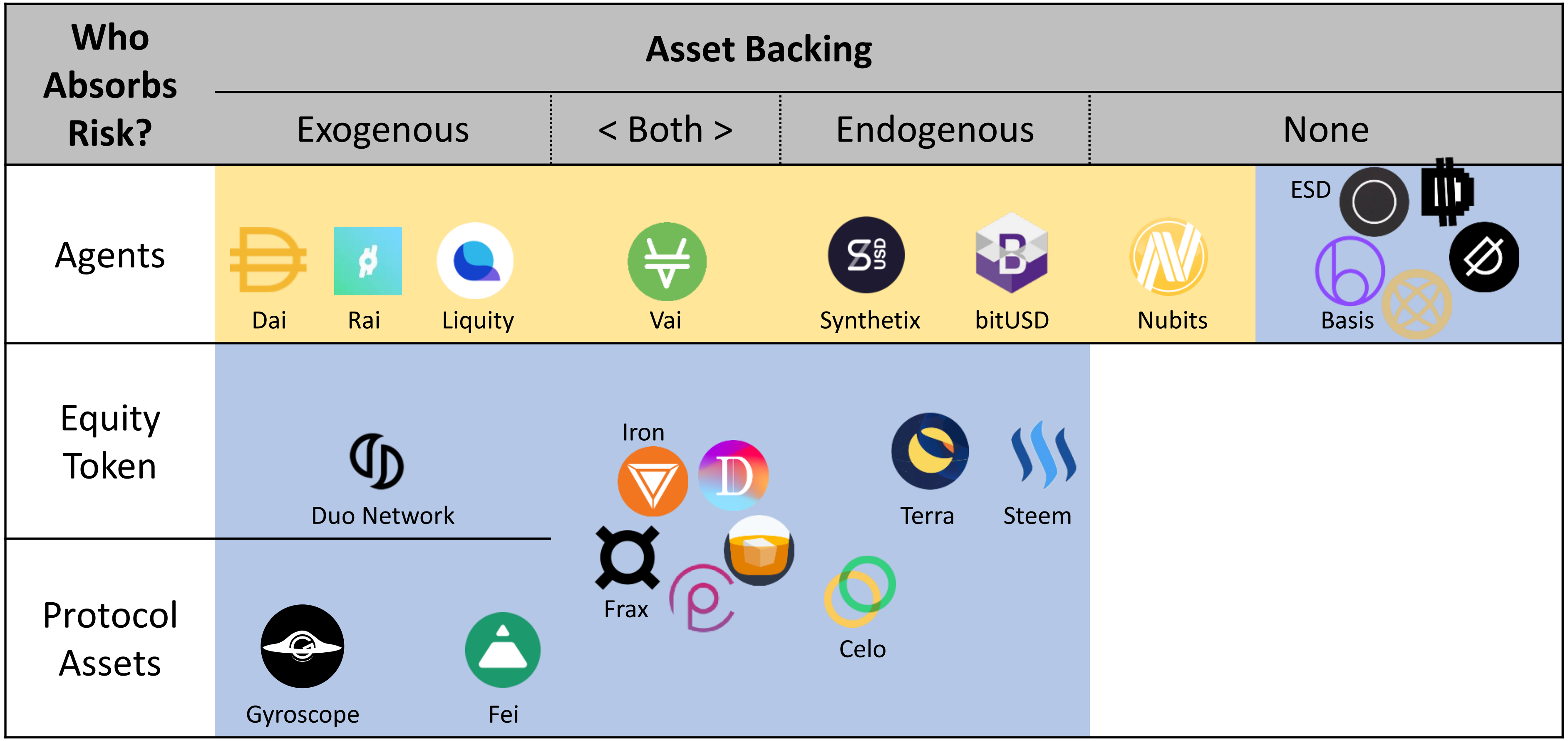


Parallels & Differences

Dai		**Traditional Money**
MKR Governance • Profit-optimizing	~	Central Bank • Stability-seeking
↓		↓
Vaults • Risk absorption • Issuance of endogenous 'stable' asset	~	Commercial Banks • Issuance of assumed stable asset
↕		↕
Dai Holders	~	Depositors

Requires new models

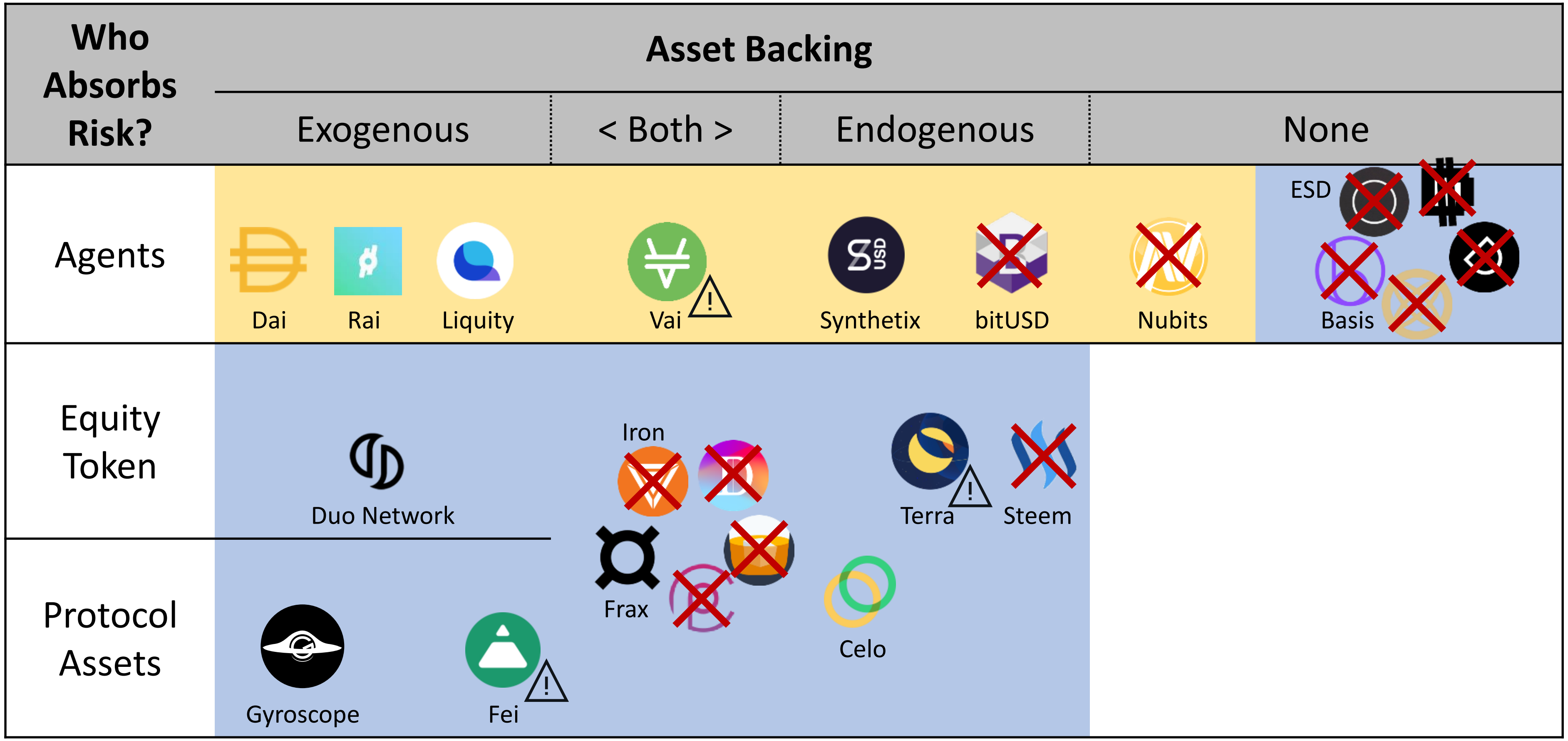
Non-custodial Stablecoins in 3D



Issuance
Agent
Algorithmic

Exogenous = asset price independent of protocol
Endogenous = asset price self-referential with protocol
Agent = speculative agents decide, as applicable, risk exposure or issuance

Non-custodial Stablecoins in 3D



Issuance Agent / Algorithmic

Exogenous = asset price independent of protocol
Endogenous = asset price self-referential with protocol
Agent = speculative agents decide, as applicable, risk exposure or issuance
⚠ = recent problems observed, X = broken

---Part II---
Technical and Economic Security

---Fundamental Design Problems---

Technical Security

Atomic, instantaneous exploits of technical structure (risk-free)

Economic Security

Manipulation of equilibria over some time period (not risk-free)

Economic Stability

Do incentives actually lead to stable outcomes?

Technical Security

Atomic, instantaneous exploits of technical structure (risk-free)

- **Risk-free** because outcomes binary for attacker:
  - Either attack is successful = profit $$
  - Or it doesn't happen = only pay gas fee
- **Examples:** atomic MEV, sandwich attacks, reentrancy, logic bugs – now well-studied!
- **Best addressed:** program analysis, formal models to specify protocols

Origin Dollar Loses $7 Million in Flash Loan DeFi Exploit

DeFi Lender bZx Loses $8M in Third Attack This Year

Sep 14, 2020 at 09:58 UTC • Updated Sep 14, 2020 at 14:20 UTC

'Engineering Error' Led to $34 Million DeFi Hack, Harvest Finance Says

Yearn Loses $11M in 2021's First DeFi Hack

Economic Security

Manipulation of equilibria over some time period (not risk-free)

- Exploits both technical structure ***and economic equilibrium over some time period***
- **Not risk-free** for attacker:
  - Tangible upfront costs to perform manipulation
  - Possibility of attack failure and mis-estimation of market
  - Not atomic
- **Less studied:** governance extractable value, MEV reorg attacks, market manipulation exploits
- **To address:** needs economic models of how these systems and agents work

Economic Security

Manipulation of equilibria over some time period (not risk-free)

Illustration (not clear exploit): Nov 2020

DAI price increase led to a massive $88 million worth of liquidations at DeFi protocol Compound

May 2021: a clear exploit

Venus, BSC's largest lending platform, once again experienced problems. By manipulating the price of XVS, someone borrowed 4100BTC and 9600ETH, generated more than $100m in bad debts. Venus had similar loopholes before, and was loaned 3000 Bitcoins and 7000 ETH.

Our Work on Economic Security

Economic attacks: market manipulation, liquidations, MEV

(In)Stability for the Blockchain, 2019

Stablecoins 2.0, 2020

- GEV = short-termism and governance attacks
- Tractable "forking" model of MEV-based reorgs

Economic Security Attacks

Some new attack primitives:

- Exploitable structure around deleveraging and liquidations
- Liquidations are automated with arbitrage opportunities
- Miners can censor and reorder transactions to extract profit
- Governors can change the rules of the protocol

Economic Attacks

(In)Stability for the Blockchain, 2019

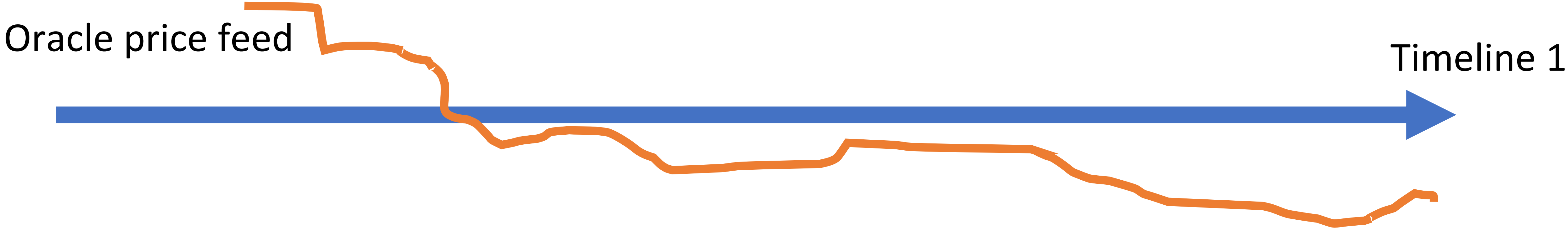
Attack 1: In ETH decline, attacker manipulates market to trigger, profit from liquidations

- Short squeeze-like attack on existing speculators
- Could supplement with a bribe to miners to freeze collateral top-ups

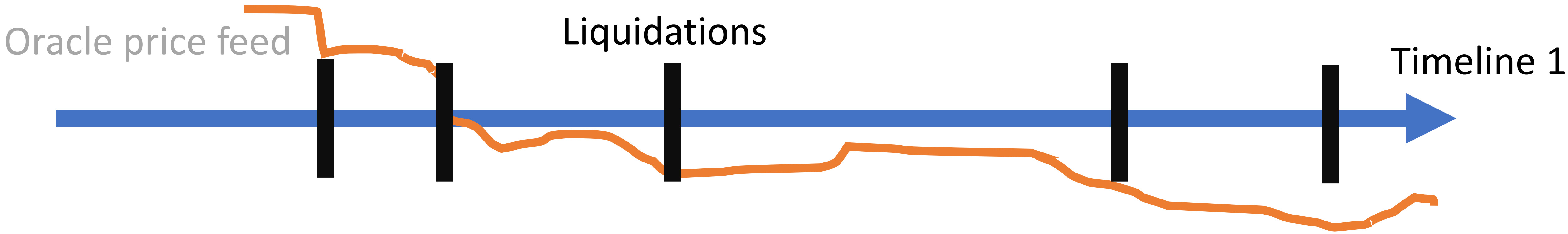
Attack 2: After ETH decline, reorg blockchain to trigger, profit from spiraling liquidations

- Change in transaction ordering $\Rightarrow$ liquidations, extractable value
- Perverse incentive for miners if attack rewards > mining rewards

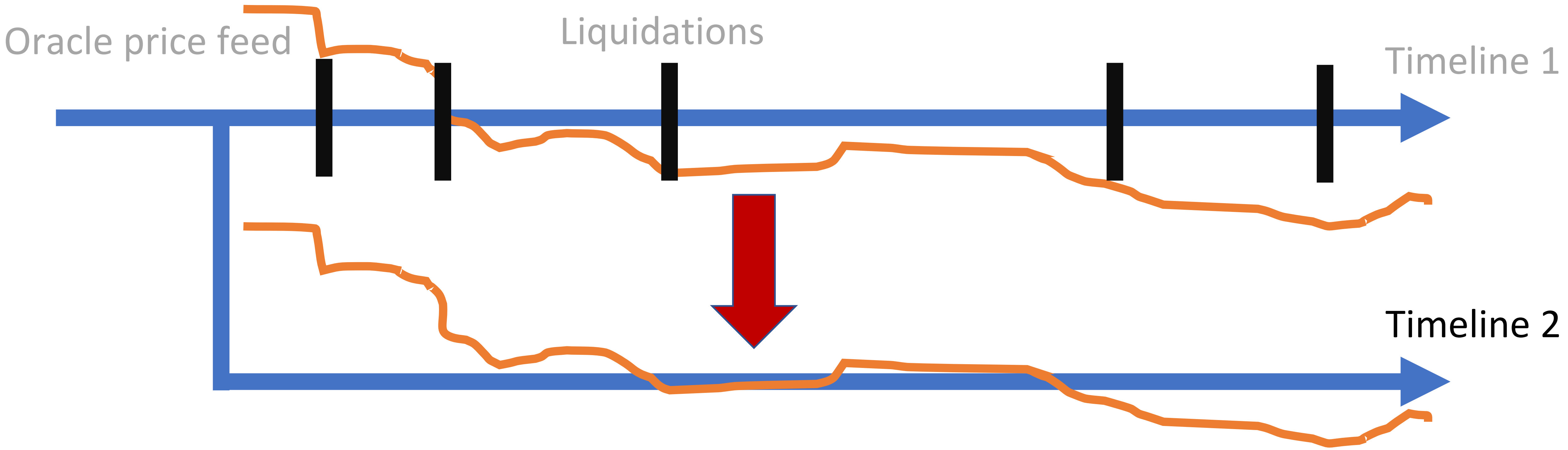
Economic Attacks



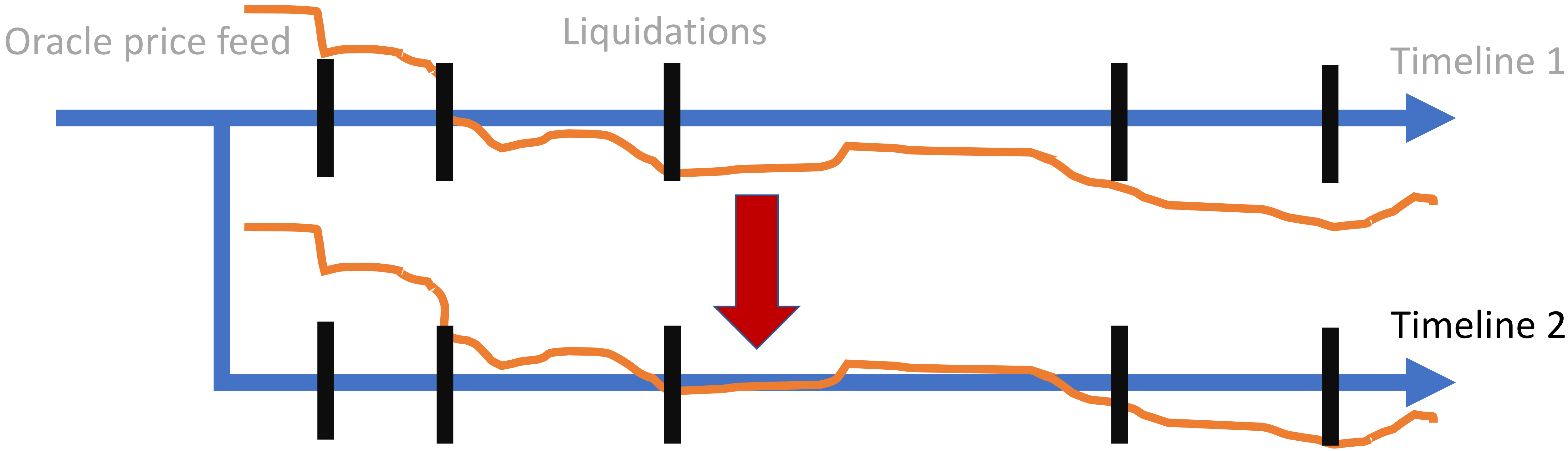
Economic Attacks



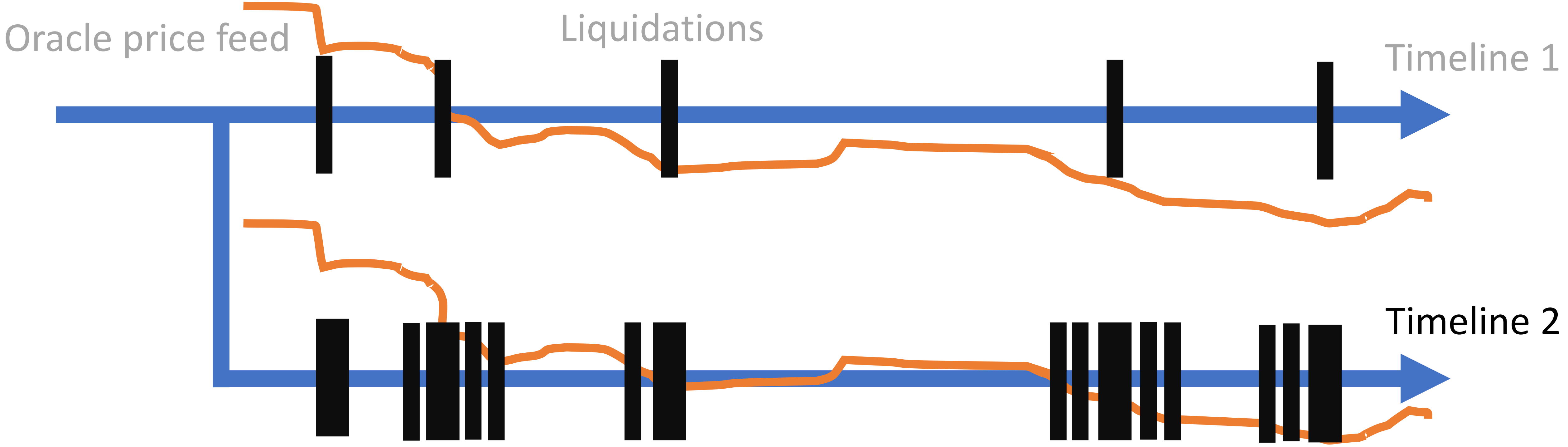
Economic Attacks



Economic Attacks



Economic Attacks



Black Thursday in Dai, March 2020

- Variants on these economic attacks also occurred, costing $8m

Black Thursday for MakerDAO: $8.32 million was liquidated for 0 DAI

- Blockchain forensic investigation: this was the result of mempool manipulation => clearing of liquidation auctions at ~$0 prices

Mempool Manipulation Enabled Theft of $8M in MakerDAO Collateral on Black Thursday: Report

Jul 22, 2020 at 18:41 UTC • Updated Jul 28, 2020 at 19:04 UTC

MEV: Forking Models

- Propose a tractable formulation of multi-round incentives: separate models with specific coupling, and iteratively solvable to find an equilibrium

Output → *Success probability of MEV bribe* Input →

Base Blockchain Model

- ➢ MEV = implicit bribe for miners
- ➢ Model success probability of these bribe incentives to fork

Application Layer Model

- ➢ MEV extracts value in stablecoin, affects participation incentives
- ➢ Participation determines MEV size

← Input *Level of MEV* ← Output

GEV Models

- Originally a type of model to describe IPO incentives
- We extend these models to understand stablecoin incentives, attacks

Three assets

- COL = collateral asset
- STBL = stablecoin
- GOV = governance token

Three types of agents

- Risk absorber (“vault”)
- Stablecoin holder
- Outside GOV holder

Further variations described Stablecoins 2.0 paper

GEV Models

Problem 1: No attack vectors

Governance choice

$$\max_{\delta \in [0,1)} \quad \mathbb{E}\left[\delta F + \kappa\right]$$

$$\text{s.t.} \quad F \text{ is vault choice}$$

Vault choice

$$\max_{F \geq 0} \quad \mathbb{E}[NR + F(Bb - \delta)]$$

$$\text{s.t.} \quad F \leq \beta N$$

$$u \leq \mathbb{E}[NR + F(Bb - \delta)]$$

$$B = \mathbb{E}\left[U\left(\frac{1}{F}\min(F, N(1+R) - \delta F)\right)\right]$$

Governance problem: decide interest rate δ to maximize revenue subject to vault's issuance decision

Vault problem: decide issuance F to maximize expected return from leverage subject to constraints

1. Collateral constraint
2. Participation constraint
3. Stablecoin market pricing

GEV Models

Problem 2: Governance attack vector

<u>Governance choice</u>

$$\max_{\delta \in [0,1)} \quad \mathbb{E}\left[(1-d)\left(\delta F + \kappa\right)\right]$$

$$\text{s.t.} \quad d = \mathbb{1}_{(\gamma N(1+R) > \zeta(\delta F + \kappa) + \alpha)}$$

$$F \text{ is vault choice}$$

<u>Vault choice</u>

$$\max_{N, F \geq 0} \quad \mathbb{E}[(\bar{N} - N)R + (1-d)NR + F(Bb - \delta) - dN(1+R)]$$

$$\text{s.t.} \quad F \leq \beta N$$

$$\mathbb{1}_{(N>0)}\, u \leq \mathbb{E}[F(Bb - \delta) - d\gamma N(1+R)]$$

$$B = \mathbb{E}\left[U\left(\frac{1}{F} \min\left(F, (1-\gamma d)(N(1+R) - \delta F)\right)\right)\right]$$

$$d = \mathbb{1}_{(\gamma N(1+R) > \zeta(\delta F + \kappa) + \alpha)}$$

$$0 \leq N \leq \bar{N}$$

- Fraction of governors can steal fraction of collateral at the expense of their share of GOV + outside cost α to attack

Governance problem: decide interest rate δ <u>and attack decision *d*</u> to maximize revenue subject to vault's issuance decision

Vault problem: decide issuance F to maximize expected return from leverage subject to constraints, <u>factoring in attack possibility</u>

GEV Models

Problem 3: Collusion attack vector

Outside governance choice

$$\max_{\delta\in[0,1),d_{\{n,v,s\}}\in\{0,1\}} \mathbb{E}\Big[d_n\epsilon(\delta F + P_1) + d_v(\gamma_v(F - \mathbf{x}_G) - \alpha) + d_s(\gamma_s(N - \mathbf{y}_G) - \alpha)\Big]$$

$$\begin{aligned}
\text{s.t.}\quad & P_1 = P(\mathbf{x}_G, \mathbf{y}_G, \delta, F) \\
& \mathbb{1}_{(\frac{\mathbf{x}_G}{P_1}\geq\zeta)} \leq d_v \leq \mathbb{1}_{(\epsilon+\frac{\mathbf{x}_G}{P_1}\geq\zeta)} \\
& \mathbb{1}_{(\frac{\mathbf{y}_G}{P_1}\geq\zeta)} \leq d_s \leq \mathbb{1}_{(\epsilon+\frac{\mathbf{y}_G}{P_1}\geq\zeta)} \\
& d_n = (1-d_v)(1-d_s) \text{ and } d_v = (1-d_n)(1-d_s) \\
& \mathbf{x}, \mathbf{y}, N, F, \gamma_v, \gamma_s \text{ from vault and stablecoin holder choices}
\end{aligned}$$

Vault choice

$$\max_{\mathbf{x},N,F\geq 0,\gamma_v\in[0,1)} \mathbb{E}\Big[\mathbf{x}_C R + F(Bb-\delta) + d_n\frac{\mathbf{x}_G}{P_1}(\delta F + P_1) + d_v(1-\gamma_v)(F-\mathbf{x}_G) - d_s N\Big]$$

$$\begin{aligned}
\text{s.t.}\quad & \mathbb{1}^T\mathbf{x} = \bar{x} \\
& 0 \leq N \leq \mathbf{x}_C \\
& F \leq \beta N \\
& \mathbb{1}_{(N>0)}\, u \leq \mathbb{E}\Big[F(Bb-\delta) + d_n\frac{\mathbf{x}_G}{P_1}(\delta F + P_1) + d_v(1-\gamma_v)(F-\mathbf{x}_G) - d_s N\Big] \\
& B = B(F, \mathbf{y}_S) \\
& P_1 = P(\mathbf{x}_G, \mathbf{y}_G, \delta, F) \\
& \delta, d, \mathbf{y} \text{ from outside governor and stablecoin holder choices}
\end{aligned}$$

Stablecoin holder choice

$$\max_{\mathbf{y},\gamma_s\in[0,1)} \mathbb{E}\Big[U\Big(\mathbf{y}_C R + d_n\Big(\min\Big(\frac{\mathbf{y}_S}{B}, N(1+R) - \delta F\Big) + \frac{\mathbf{y}_G}{P_1}(\delta F + P_1)\Big) + d_s(1-\gamma_s)(N-\mathbf{y}_G)\Big)\Big]$$

$$\begin{aligned}
\text{s.t.}\quad & \mathbb{1}^T\mathbf{y} = \bar{y} \\
& B = B(F, \mathbf{y}_S) \\
& P_1 = P(\mathbf{x}_G, \mathbf{y}_G, \delta, F) \\
& \delta, d, \mathbf{x}, N, F \text{ from outside governor and vault choices}
\end{aligned}$$

- Agents can collude to restrict exit of other agents, indirectly steal value
- Agents may strategically bid up GOV price and/or issue bribes

Governance problem: decide interest rate δ and whether to collude with another agent to attack

Vault problem: decide COL-GOV portfolio, level of participation (issuance, locked COL) and governance bribe to maximize expected return

Stablecoin holder problem: decide STBL-COL-GOV portfolio and governance bribe to maximize expected utility (risk-averse)

GEV Models

Some takeaways

- GOV fundamental value ~ geometric sum of discounted fees
- If small relative to collateral, need high α for security
- ‘Price of anarchy’ = extra cost to secure decentralized system vs. centralized (high α)

Conjecture:
In fully decentralized stablecoins (α=0) with (i) multiple classes of interested parties and (ii) highly flexible governance design, no equilibrium exists with long-term participation under realistic parameter values.

Analogy: a bank that's unsecure if equity < 2x AUM → no depositors participate

A Solution: Optimistic Approval

- Give users option to veto governance changes to align vision

----Fundamental Design Problems----

Technical Security

Atomic, instantaneous exploits of technical structure (risk-free)

Economic Security

Manipulation of equilibria over some time period (not risk-free)

Economic Stability

Do incentives actually lead to stable outcomes?

---Part III---
Deleveraging Spirals

(In)Stability for the Blockchain, 2019

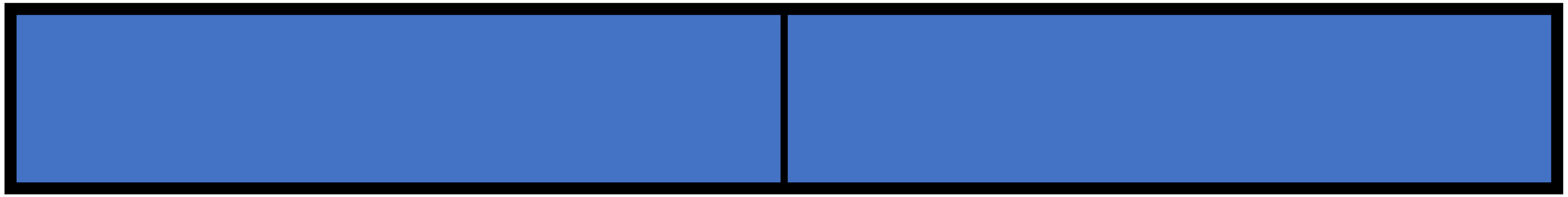
While Stability Lasts, 2020

CDO Structure

A portfolio of underlying assets

CDO Structure

Split into 2 tranches

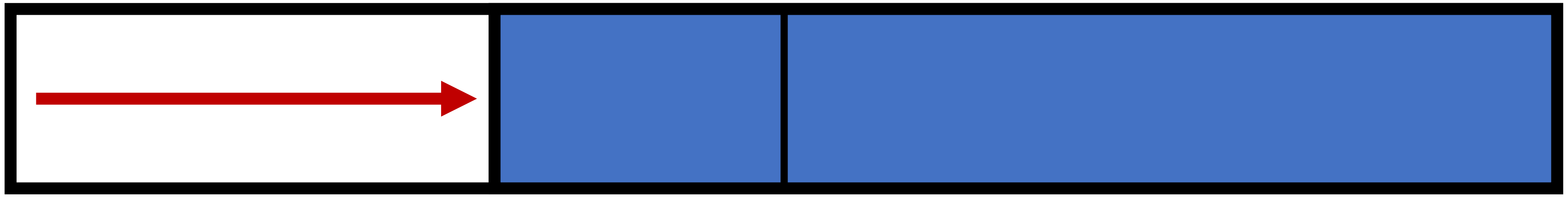


Junior tranche = more risky

Senior tranche = less risky

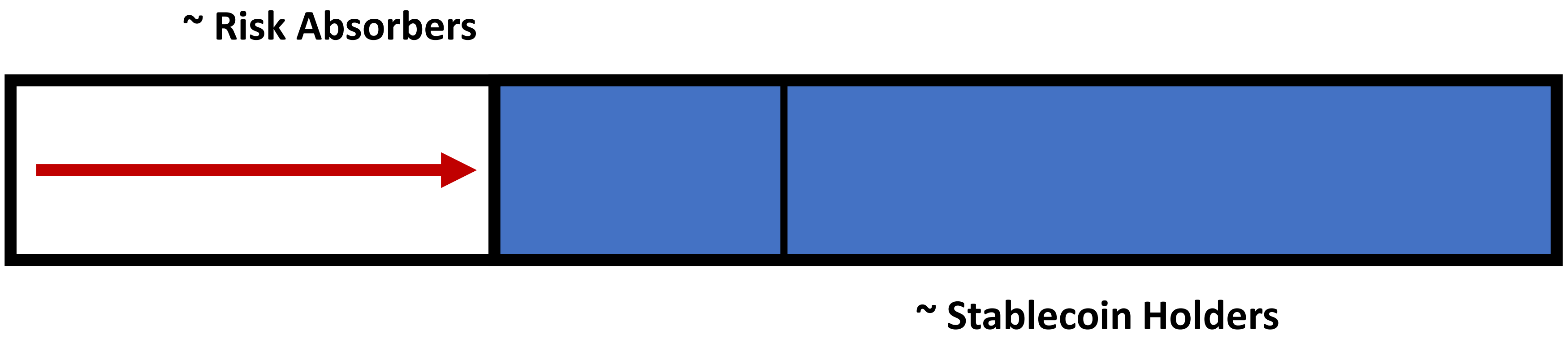
CDO Structure

Losses that occur are first borne by junior tranche

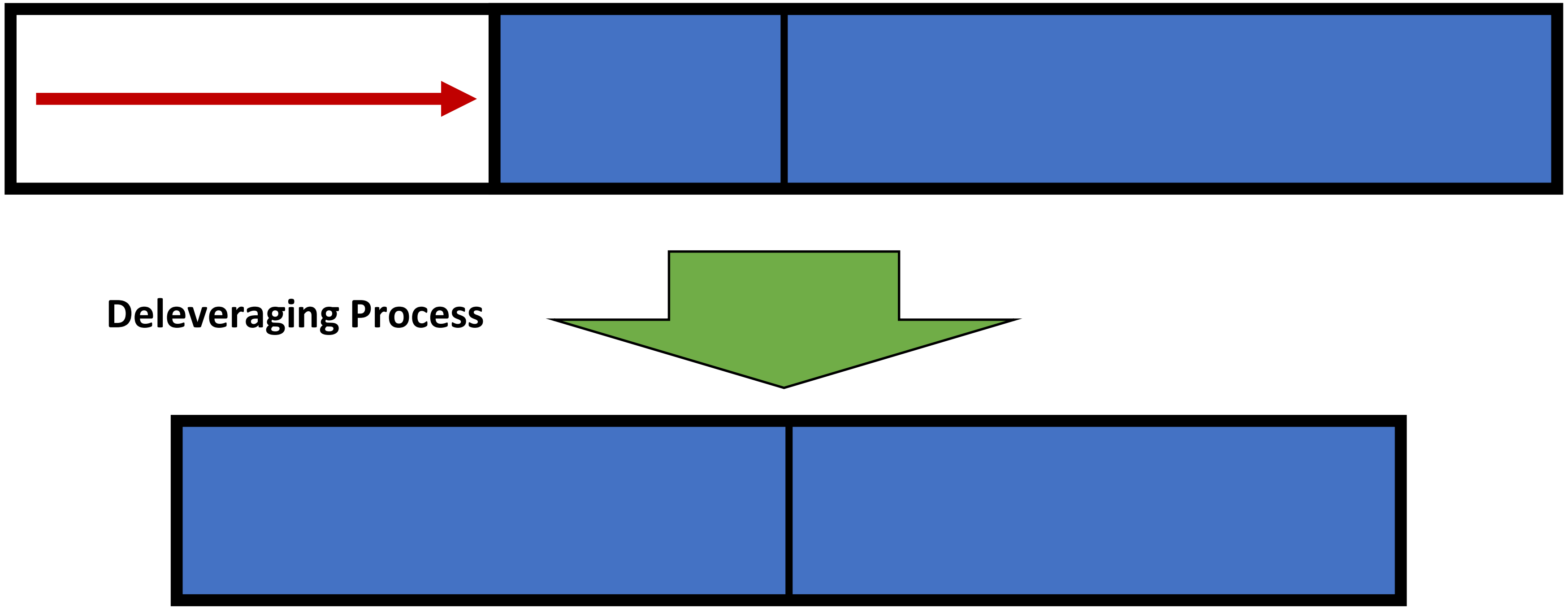


Senior tranche protected

Stablecoin CDO-like Structure



Stablecoin CDO-like Structure



Modeling Price Dynamics

- (Original) Dai supply determined in leverage market
  - Created by speculator choosing to borrow against ETH (risky!)
  - Endogenous price: supply needn’t = demand at $1
  - Traditional financial leverage models not applicable

- Stochastic models of endogenous stablecoin price (K-M, 2020), (K-M, 2019)
  - Deleveraging spirals → short squeeze effect, amplify collateral drawdown
  - 'Stable' and 'unstable' regions for stablecoins

Model: Speculator

Collateral constraint: protocol requires over-collateralization

Price of ETH

Stablecoins "borrowed"

$$\bar{N}_t X_t \geq \beta L_t$$

Amount of ETH

Collateral factor

Model: Speculator

Decision: Change stablecoin supply to maximize next period expected returns

$$\max_{\Delta_t} \quad \mathbb{E}[Y_{t+1}|\mathcal{F}_t]$$

$$\text{s.t.} \quad \bar{N}_t X_t \geq \beta L_t$$

$$Y_t = N_{t-1}X_t - L_{t-1} - \underbrace{\text{liquidation effect}}_{\text{Protocol can liquidate: costs and market effect}}$$

Regions of Stability

Result 1: Bounded probability of large deviations in certain region

Technical idea: Doob's inequality

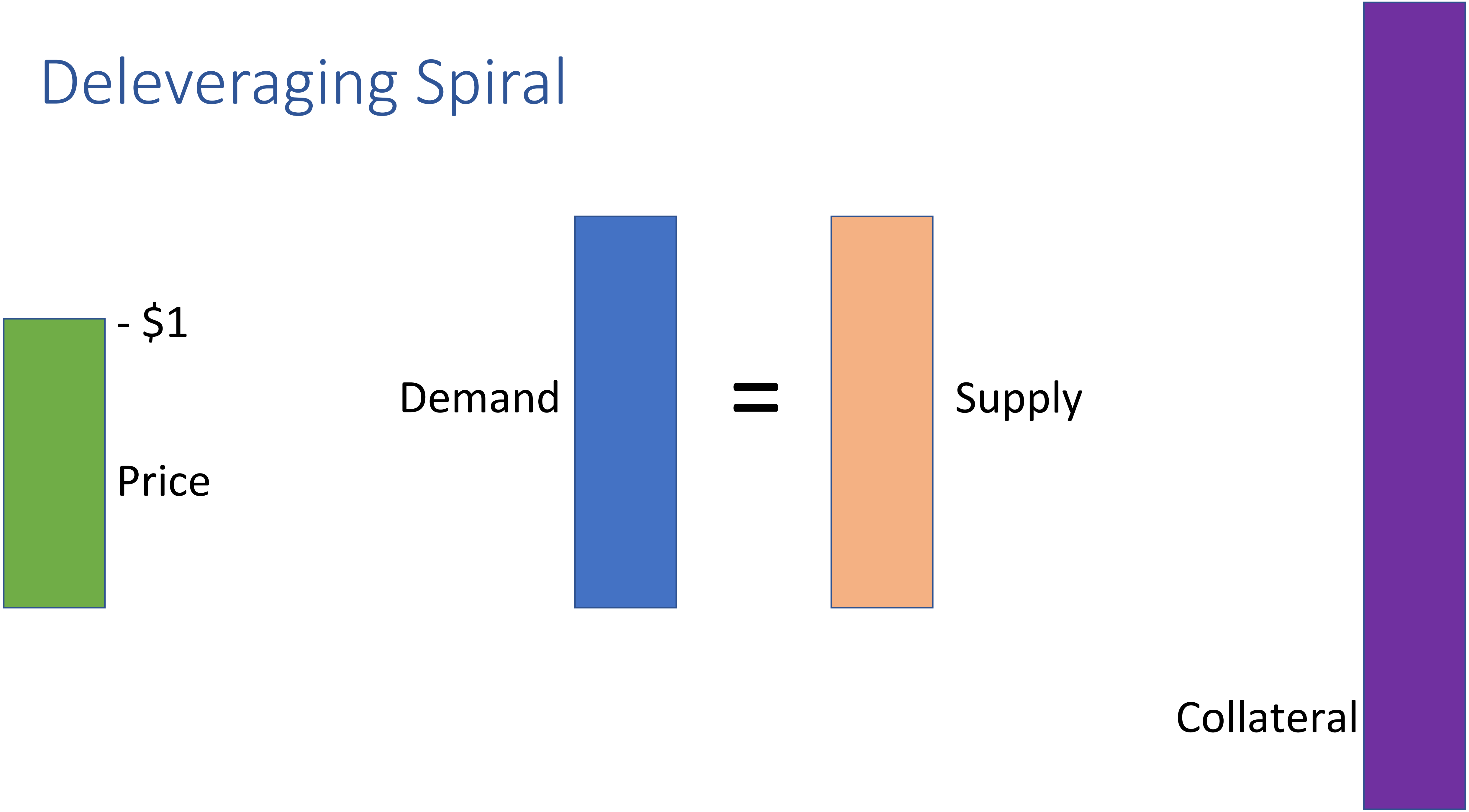
Result 2: Bounded probability of large quadratic variation (QV) in certain regime

Technical idea: Burkholder's inequality

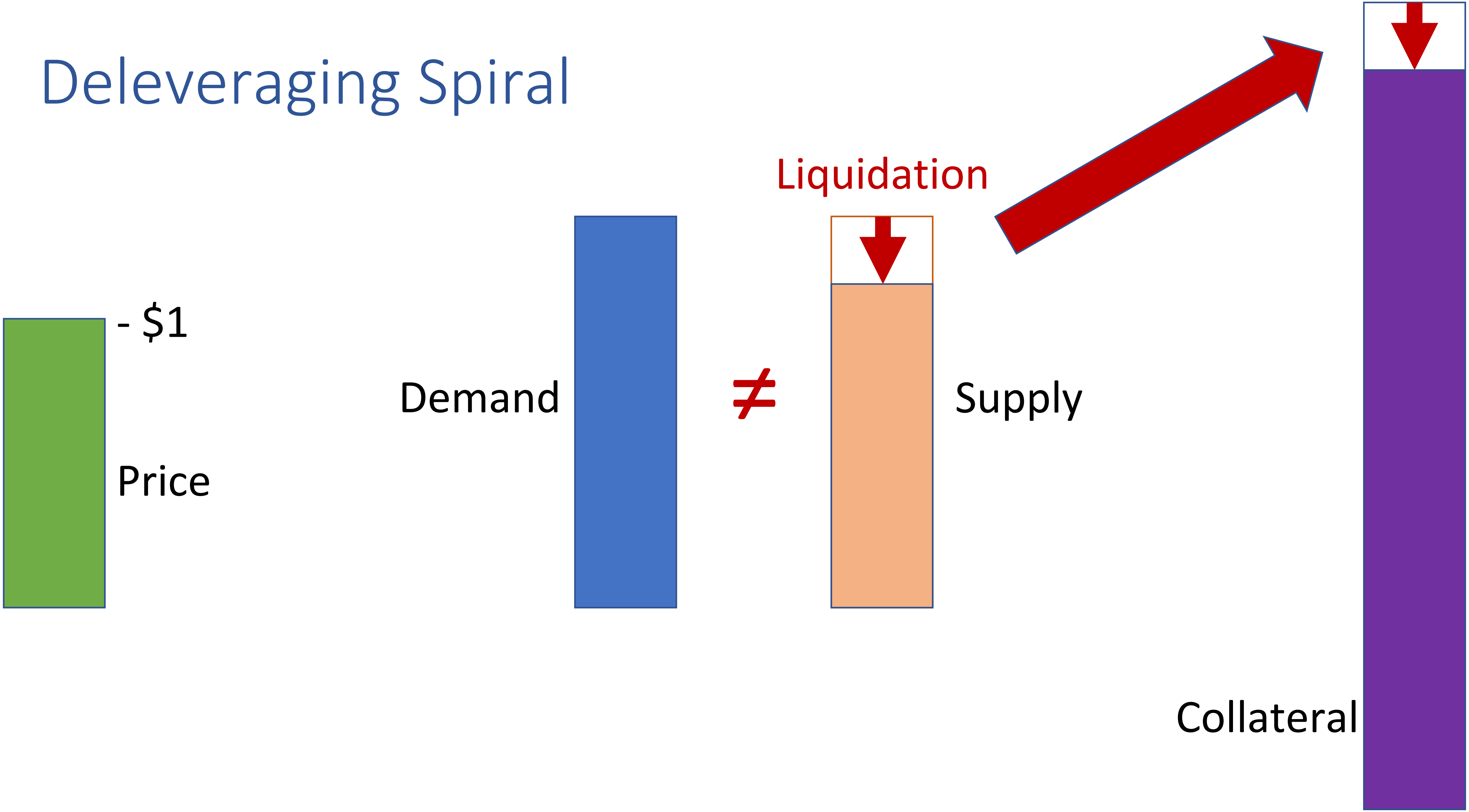
Regions of Instability

Result 3: In different regime, stablecoin experiences short squeeze/deleveraging spiral (formally: submartingale prices)

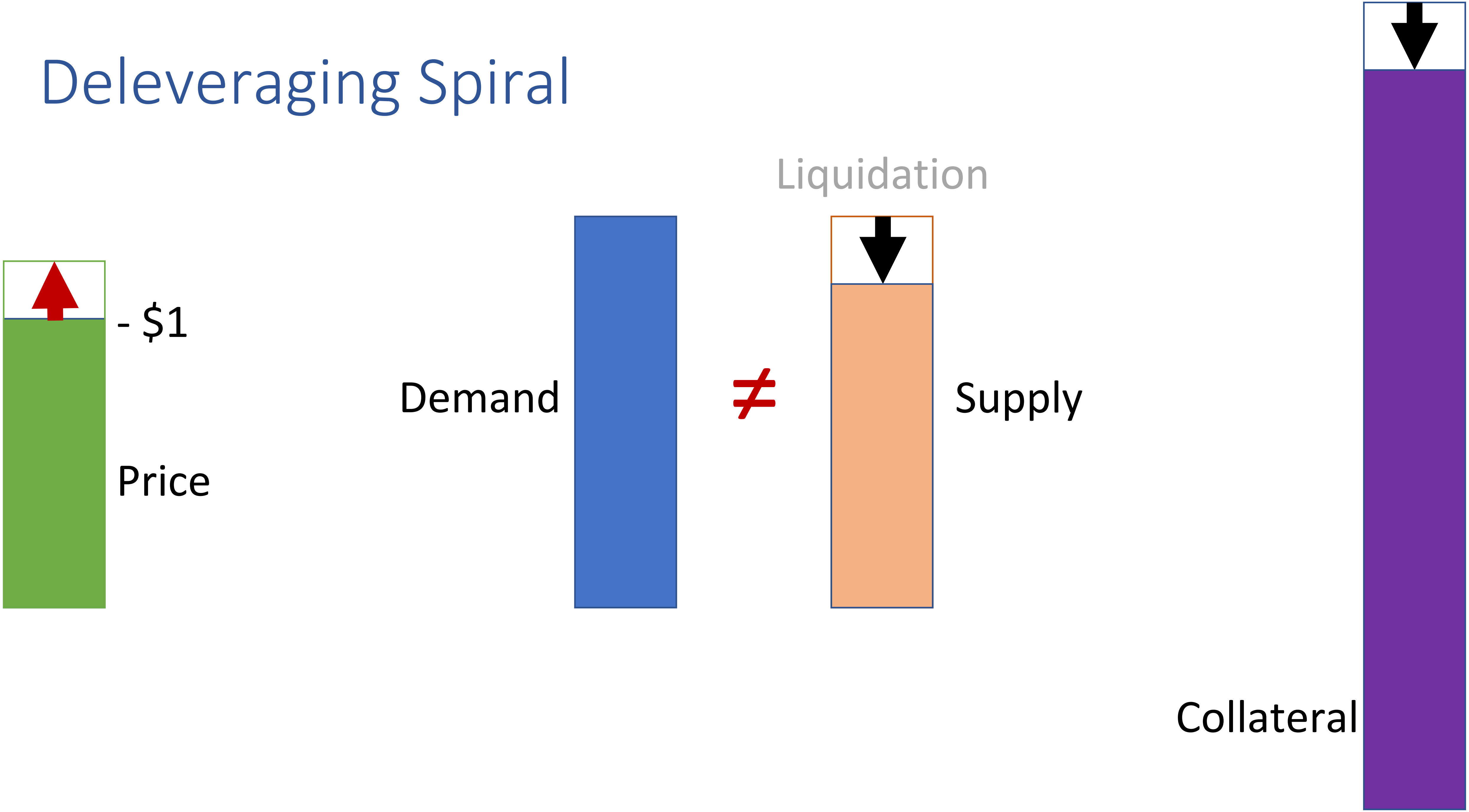
Deleveraging Spiral



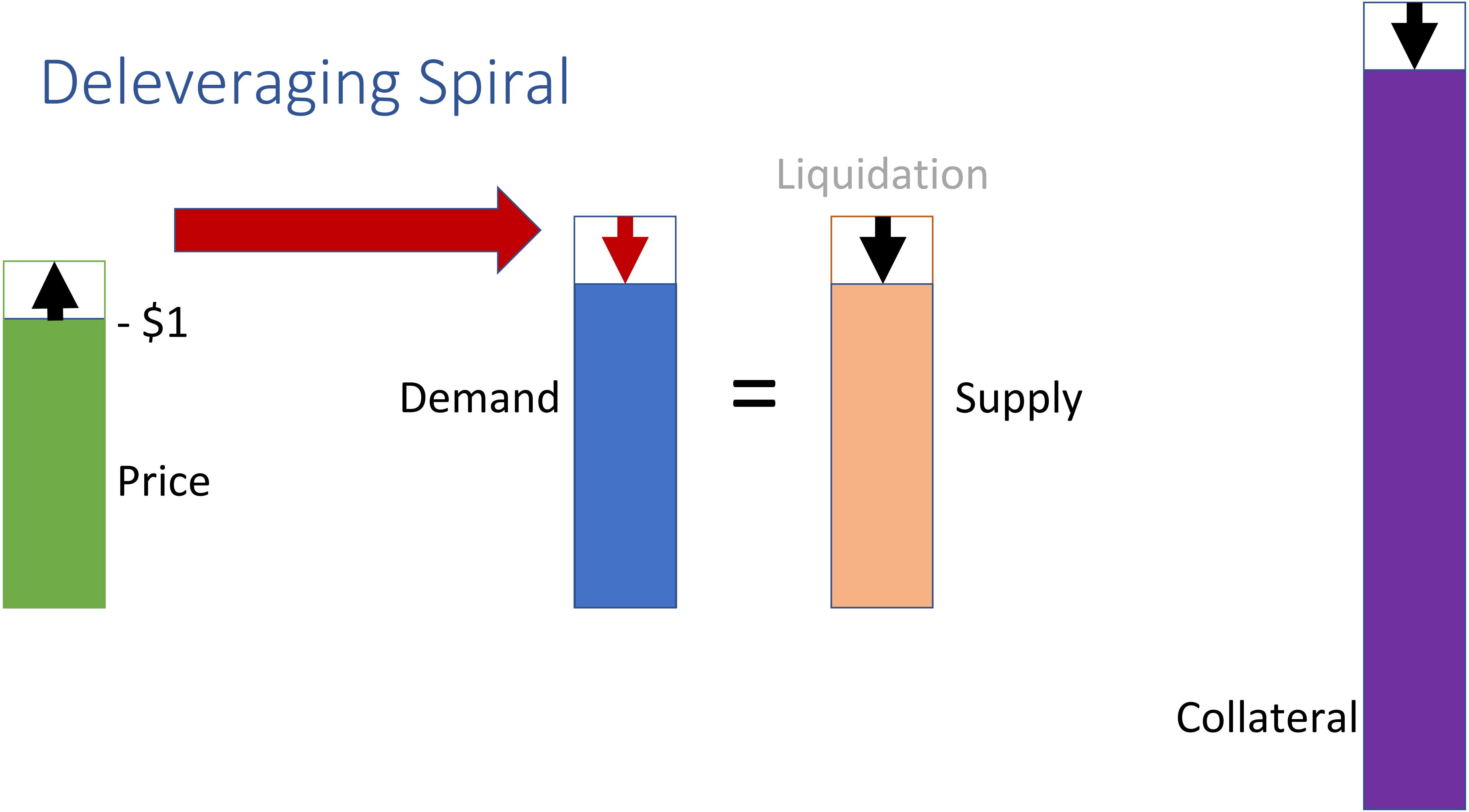
Deleveraging Spiral



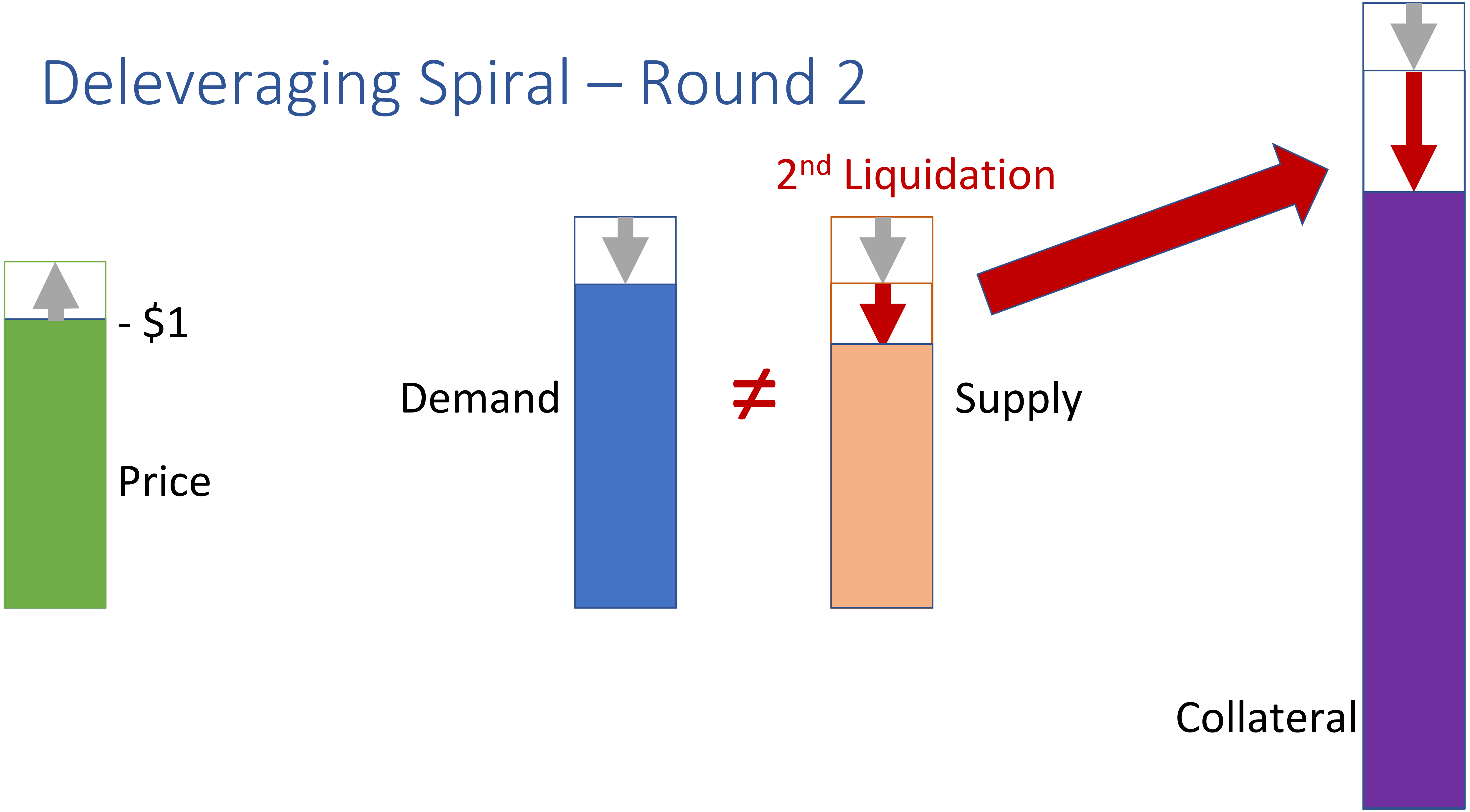
Deleveraging Spiral



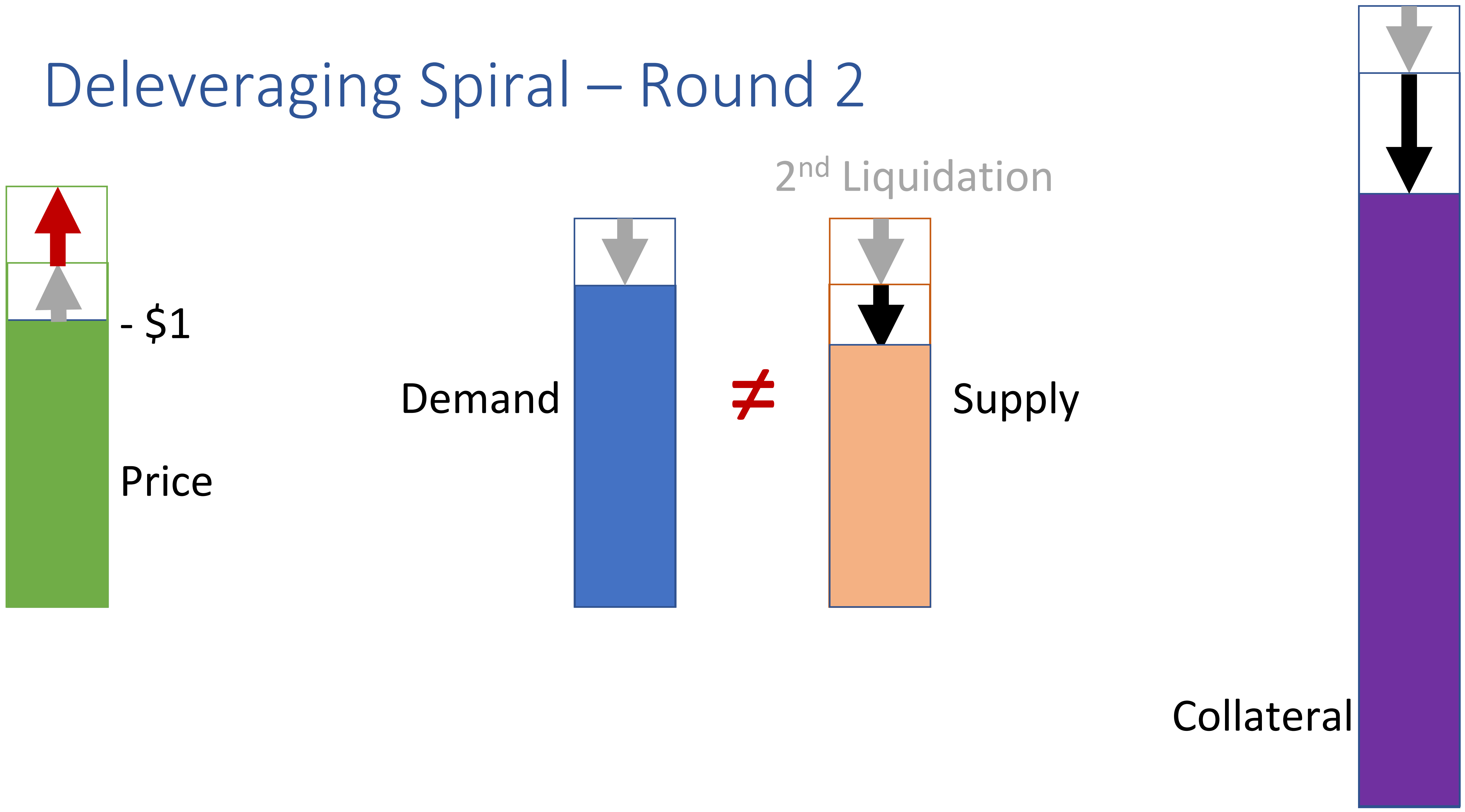
Deleveraging Spiral



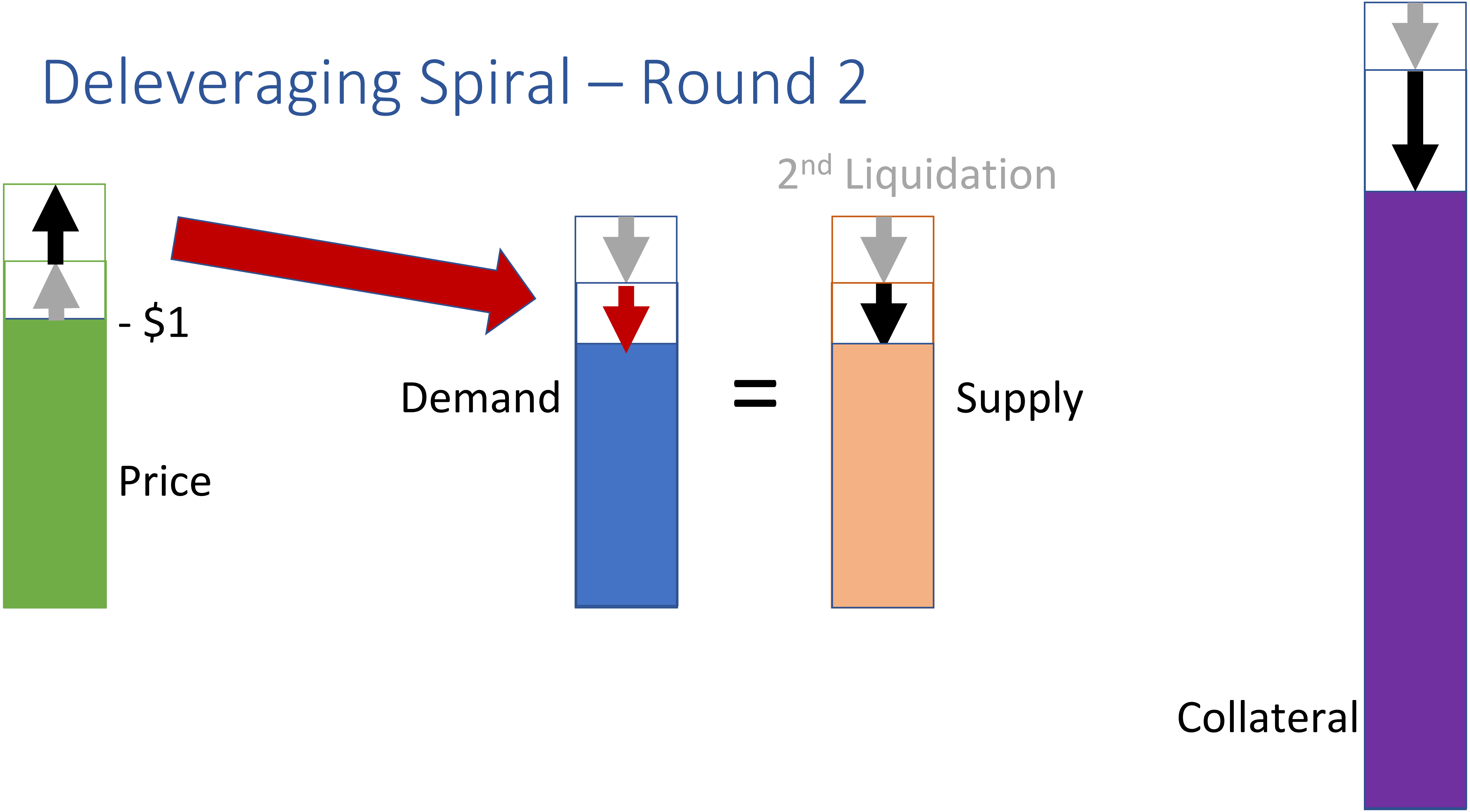
Deleveraging Spiral – Round 2



Deleveraging Spiral – Round 2



Deleveraging Spiral – Round 2



Regions of Instability

Result 3: In different regime, stablecoin experiences short squeeze/deleveraging spiral (formally: submartingale prices)

Result 4: Variance approx. increases by order of $\frac{1}{R_t^2}$ in an ETH return shock and $\frac{1}{N_t^2}$ with different initial collateralization

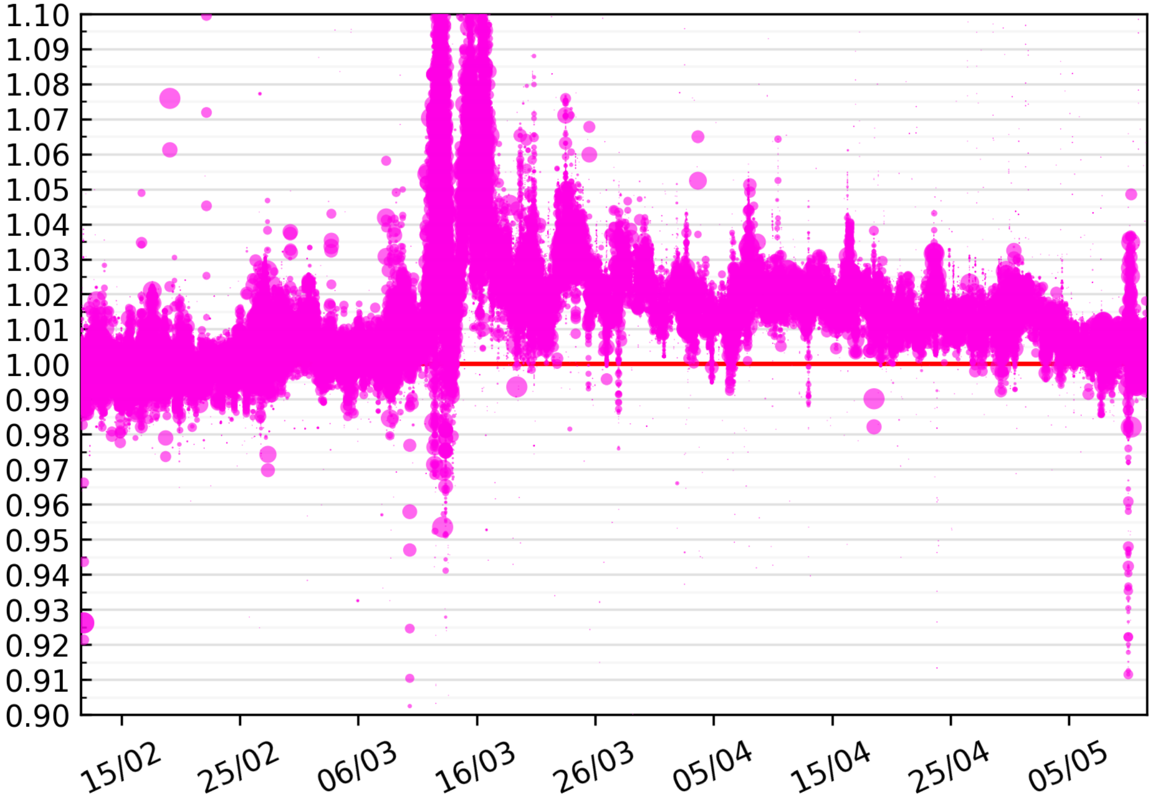
Technical idea: Implicit Function Theorem

Result 5: Starting in the unstable regime, the stablecoin will always have higher forward-looking variance than in stable regime.

- ‘Stable’ and ‘unstable’ regimes well-interpreted

Technical idea: inequalities on variances of convex functions of RVs

Black Thursday in Dai, March 2020



Source: dai.stablecoin.science

~50% ETH price crash

Liquidation price effect on Dai DEX trades

Non-custodial Complications

- No stable region when X_t is not ~ submartingale (positive expectations)

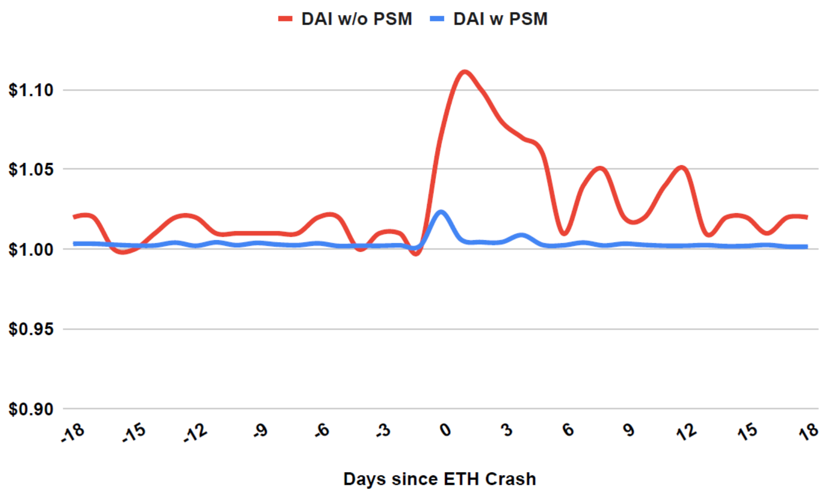
- *Seeming contradiction:* goal to make decentralized stablecoin, but can only be fully stabilized by adding uncorrelated assets, which are currently custodial

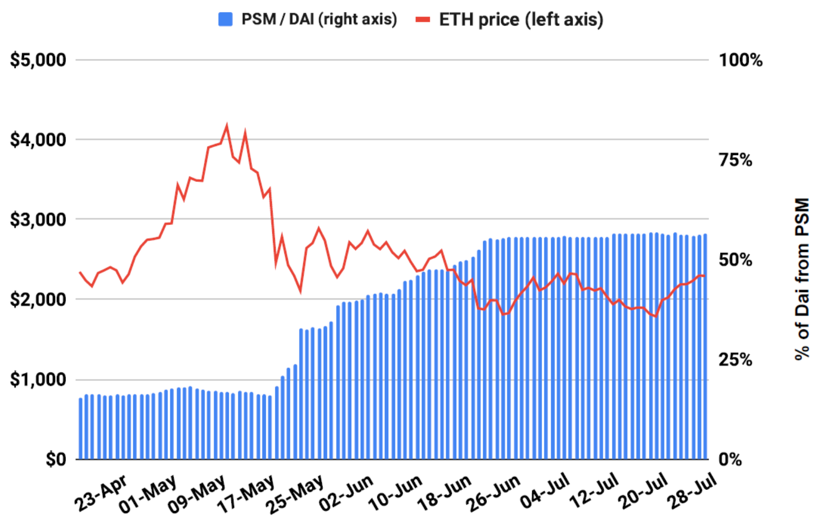
- Patching this has been major topic since Black Thursday

Non-custodial Complications

Solutions:

- **Maker:** Since Black Thursday has tethered to USDC (+ custodial risks)
  - ➢ Maintaining exchangeability via USDC reserve ("PSM")



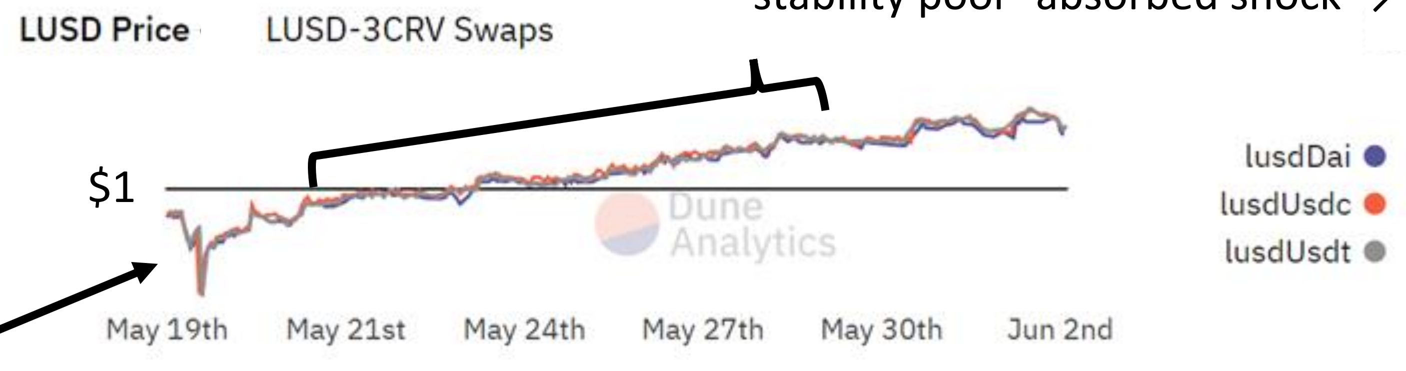


Non-custodial Complications

Solutions:

- **Maker:** Since Black Thursday has tethered to USDC (+ custodial risks)
  - Maintaining exchangeability via USDC reserve ("PSM")
- **Rai:** negative rates during crises (equilibrium participation, liquidity?)
- **Liquity (and our 2020 paper):** Dedicated liquidity pools for crises

"stability pool" absorbed shock → postponed, smoothed effect



Redemptions at start of crisis

Non-custodial Complications

Solutions:

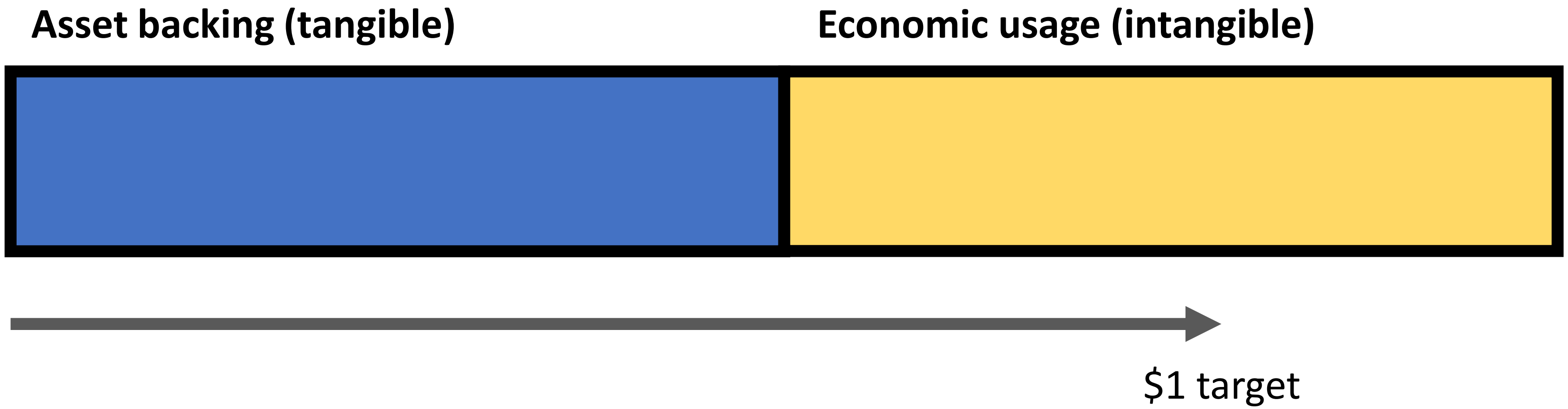
- **Maker:** Since Black Thursday has tethered to USDC (+ custodial risks)
  - Maintaining exchangeability via USDC reserve (“PSM”)
- **Rai:** negative rates during crises (equilibrium participation, liquidity?)
- **Liquity (and our 2020 paper):** Dedicated liquidity pools for crises
- **Reserve-backed primary markets:** Gyroscope

---Part IV---
Design of Algorithmic Primary Markets

Gyroscope P-AMM, 2021 (under review)

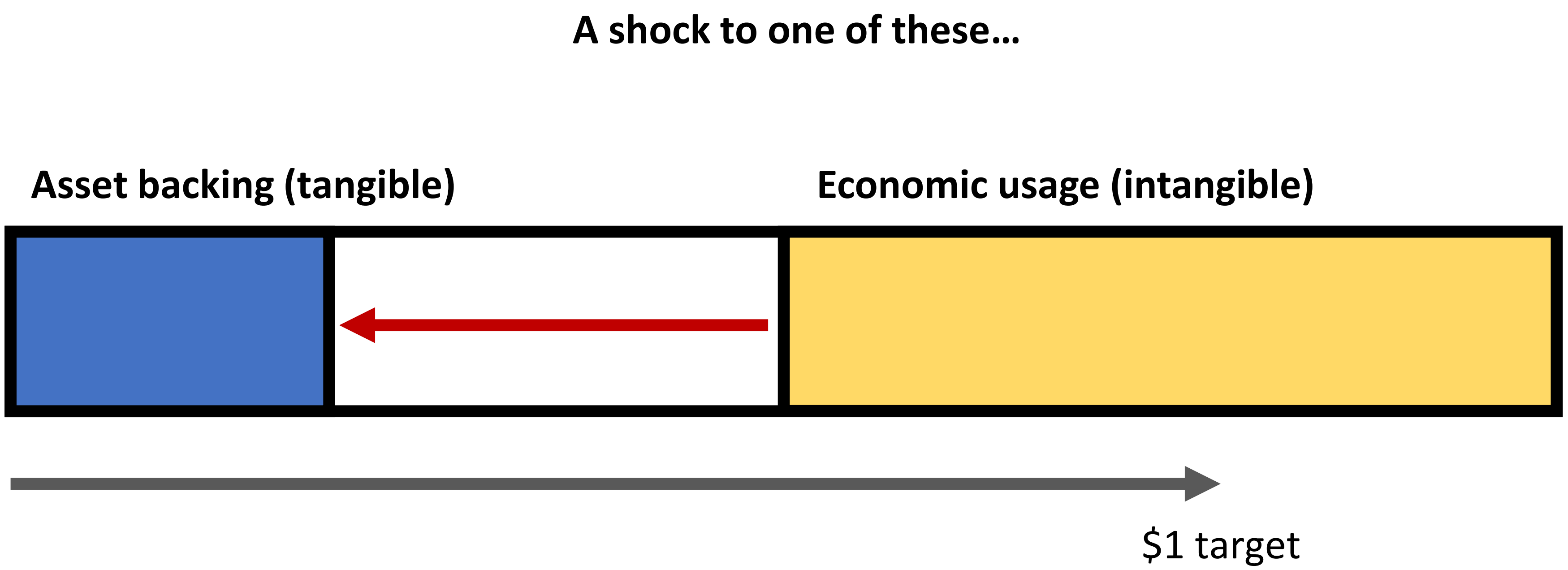
What Backs a Currency Peg?

2 sources of value



Peg sustained!

What Backs a Currency Peg?



What Backs a Currency Peg?

A shock to one of these…

Asset backing (tangible) **Economic usage (intangible)**

$1 target

Peg breaks!

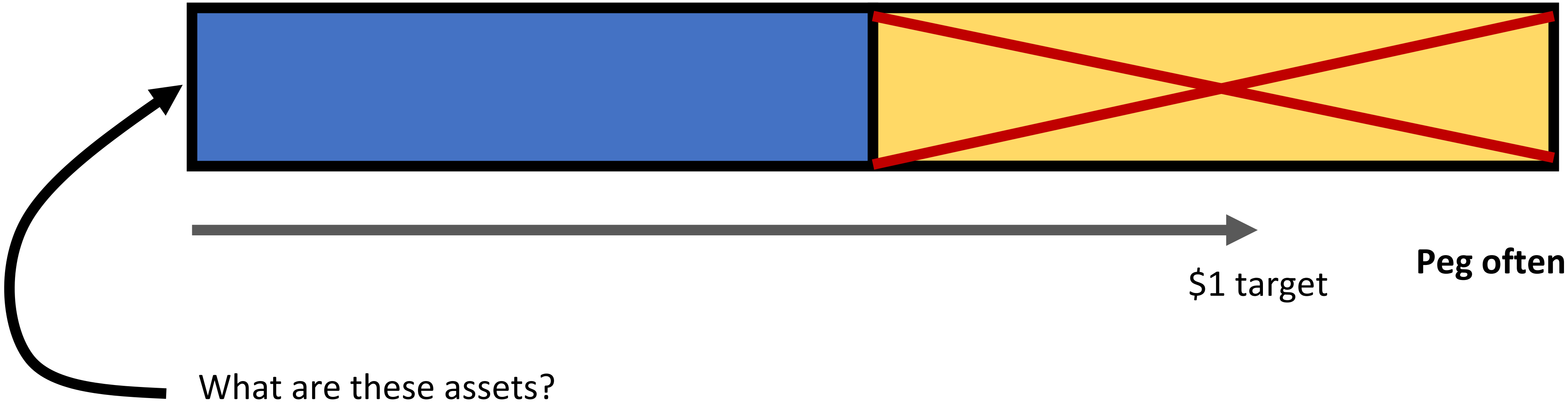
*Highly simplified: see (Morris & Shin, 1998) for more precise model

What Backs Algorithmic Stablecoins?

These systems have no native usage,
but try to start out under-backed

Asset backing (tangible)

~~Economic usage (intangible)~~



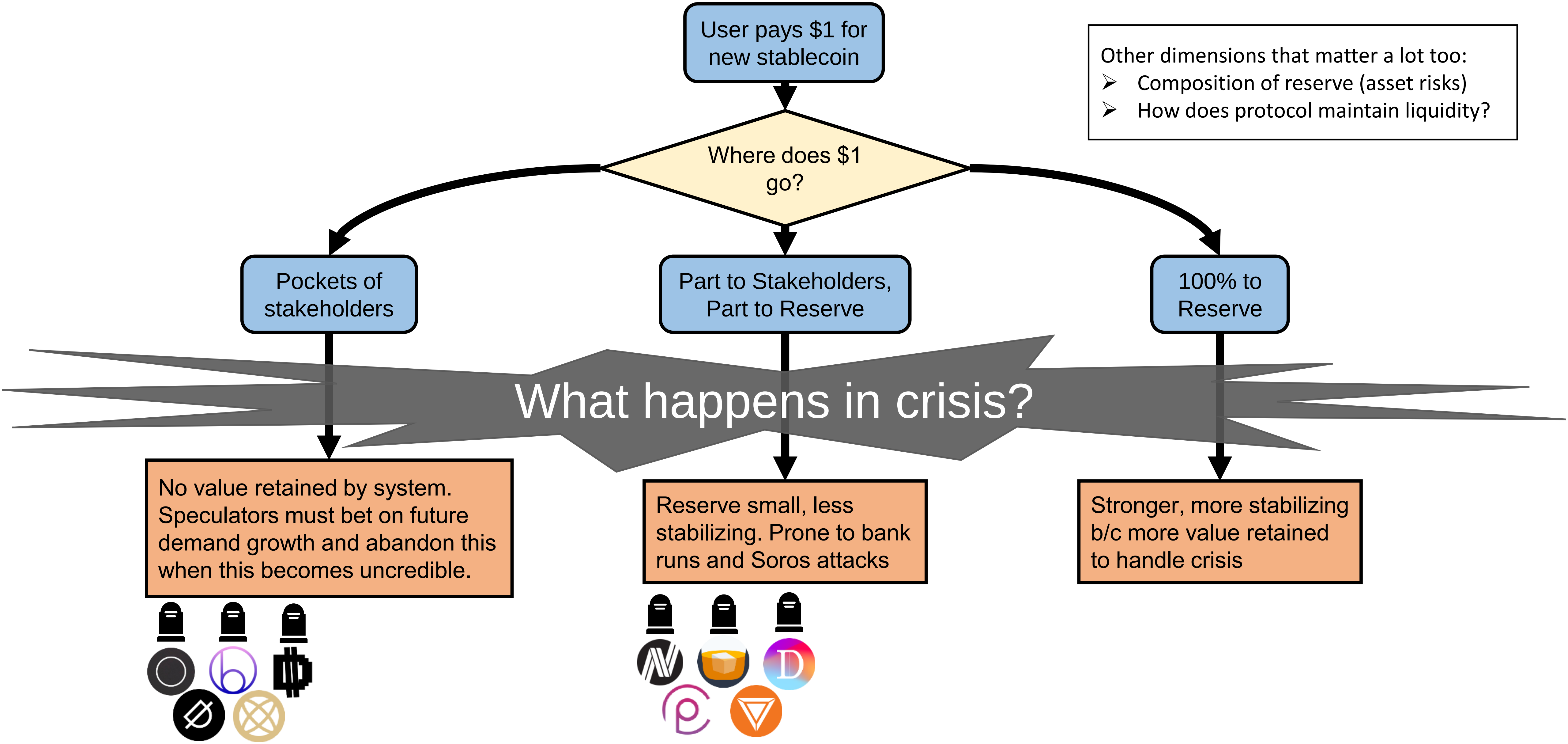
$1 target

Peg often breaks!

What are these assets?

- Seigniorage shares: value of endogenous "equity shares"
- Basis: nothing!
- Reserve-backed: some portfolio

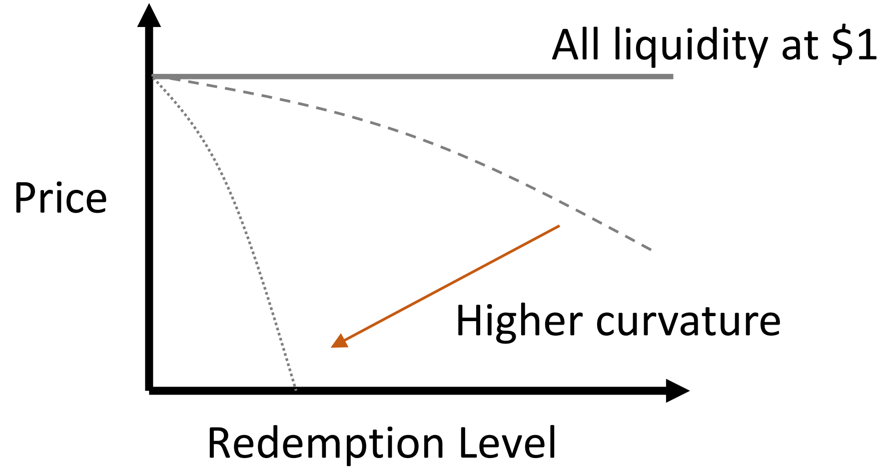
Contrasting Algorithmic Stablecoins

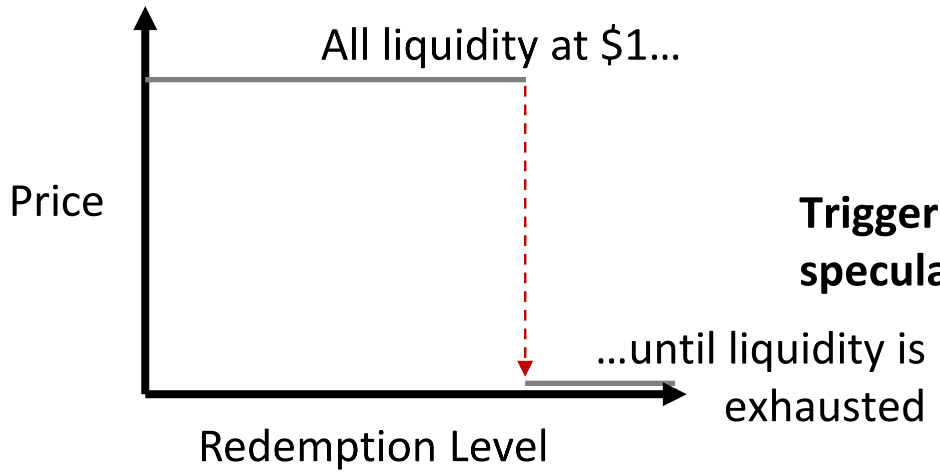


Algorithmic Primary Markets

- **Primary market =** minting and redeeming (open market operations)
- **Redemption curve =** price of redemption as fn. of system state

- **A key factor:** What do redemption curves look like?

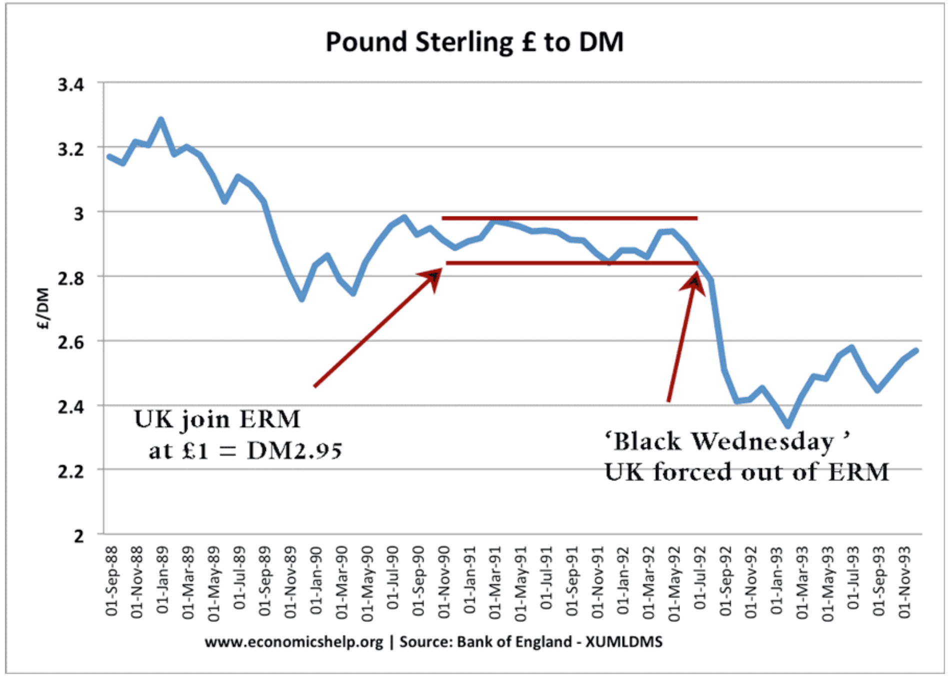




Triggerable by a speculative attack!

Speculative Attacks

- E.g., Soros attack on GBP

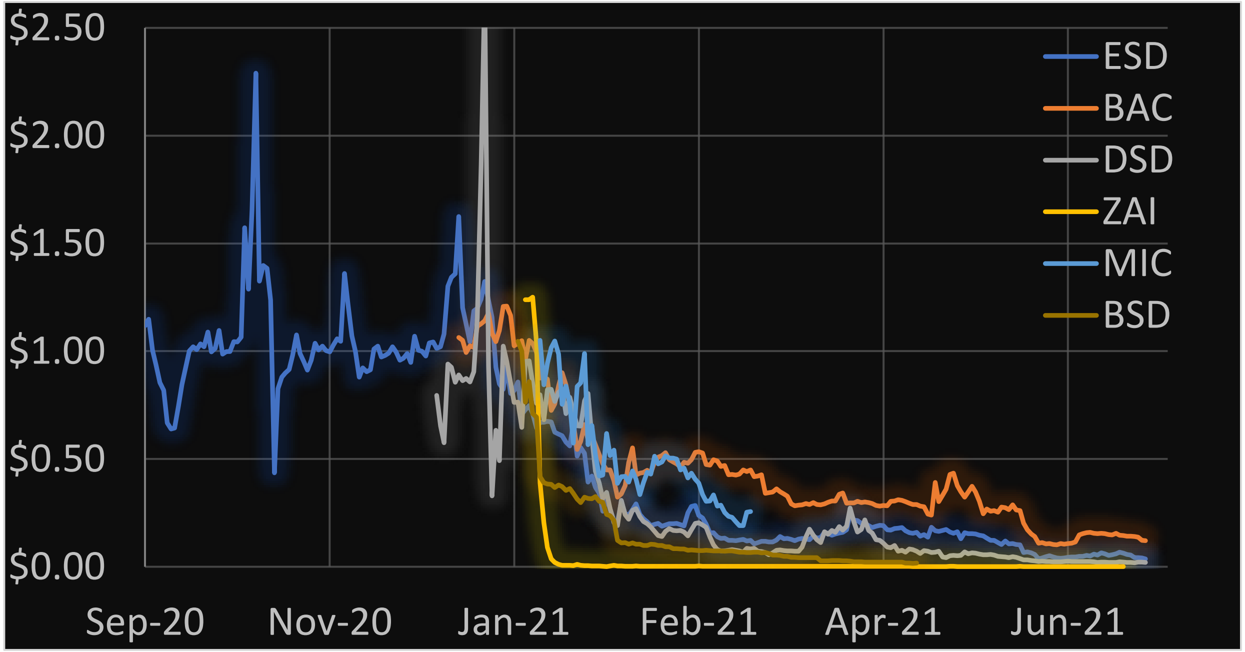


- Studied in international finance literature (e.g., Morris and Shin, 1998)

Algorithmic Primary Markets

Case study 1: Basis/ESD

- Implicit redemption curve for endogenous "coupons"
- When coupon demand disappears, flat at $0 (no asset backing)



Algorithmic Primary Markets

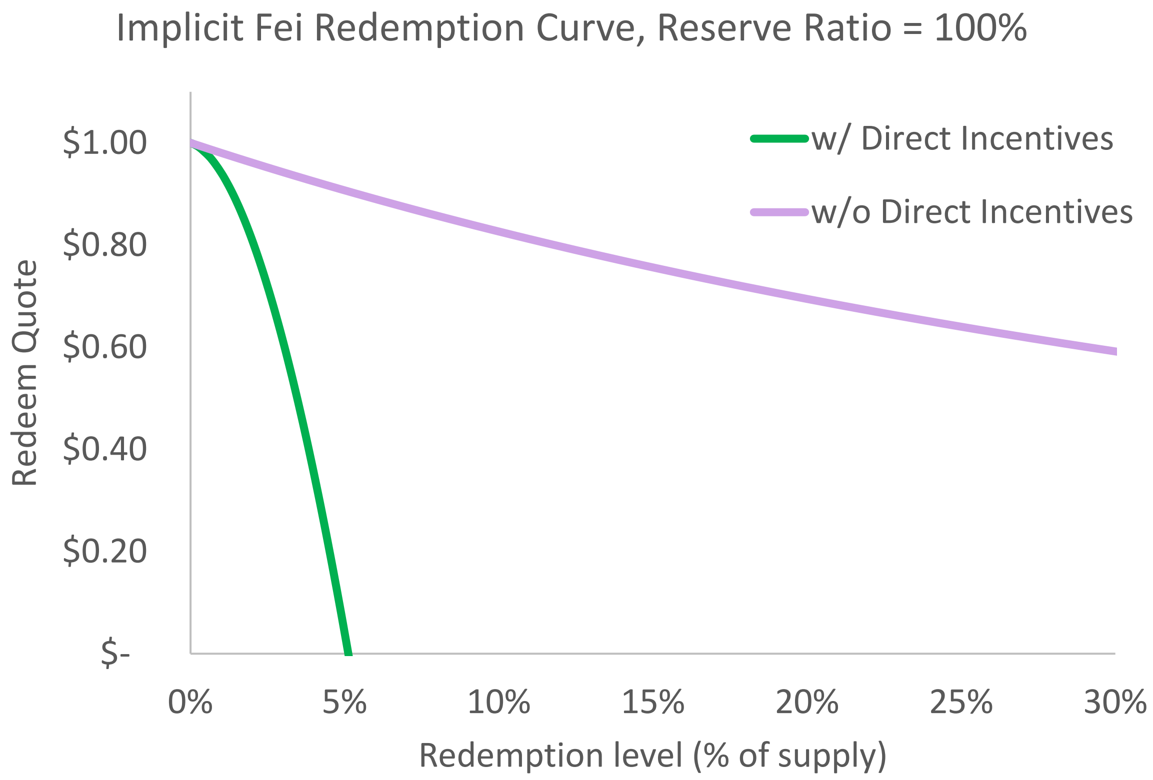
Case study 2: USDC/USDT

- Flat redemption curve at $1
- Off-chain, so must trust issuer to maintain primary market
- Dai PSM wrapped version of this

Algorithmic Primary Markets

Case study 3: Fei

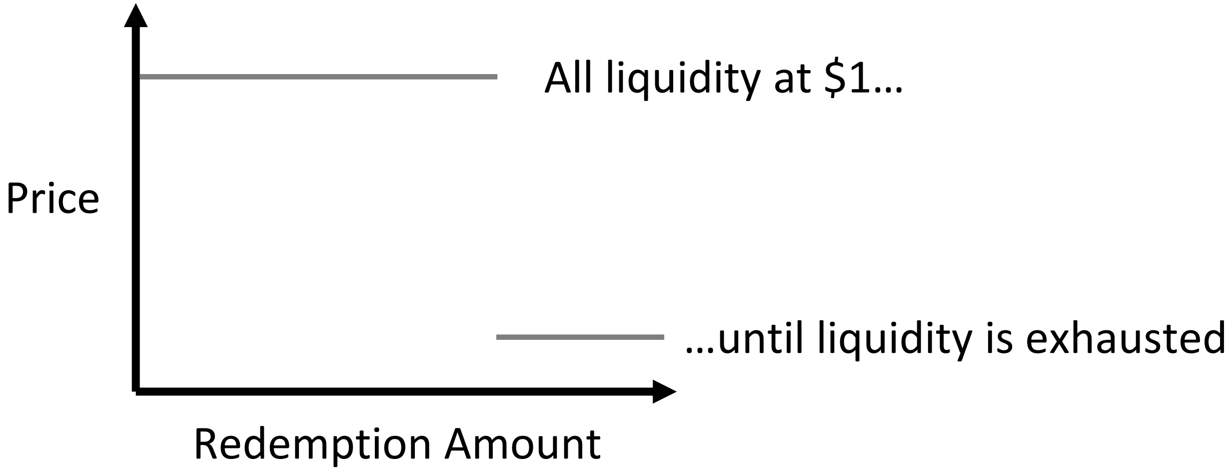
- Implicit redemption curve very steep to $0



Algorithmic Primary Markets

Case Study 4: Seigniorage shares

- $1 redemption, but backing volatile endogenous asset
- Speculative attack could cause collapse of this asset value (UST, Titan)



TITAN endogenous asset backing:

IRON stablecoin:

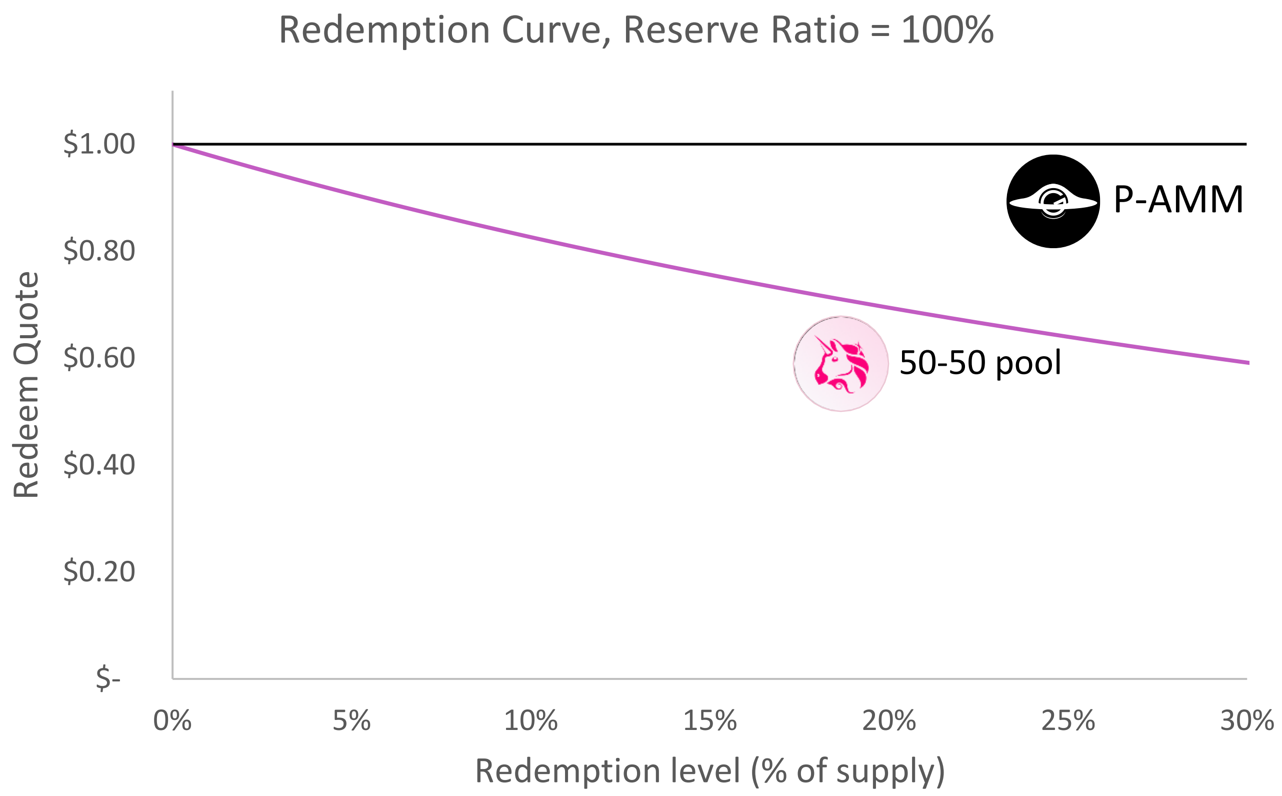
Designing Autonomous Primary Markets

- Current space of primary market mechanisms
  - Ad hoc design
  - Need governance to make quick fixes in crises

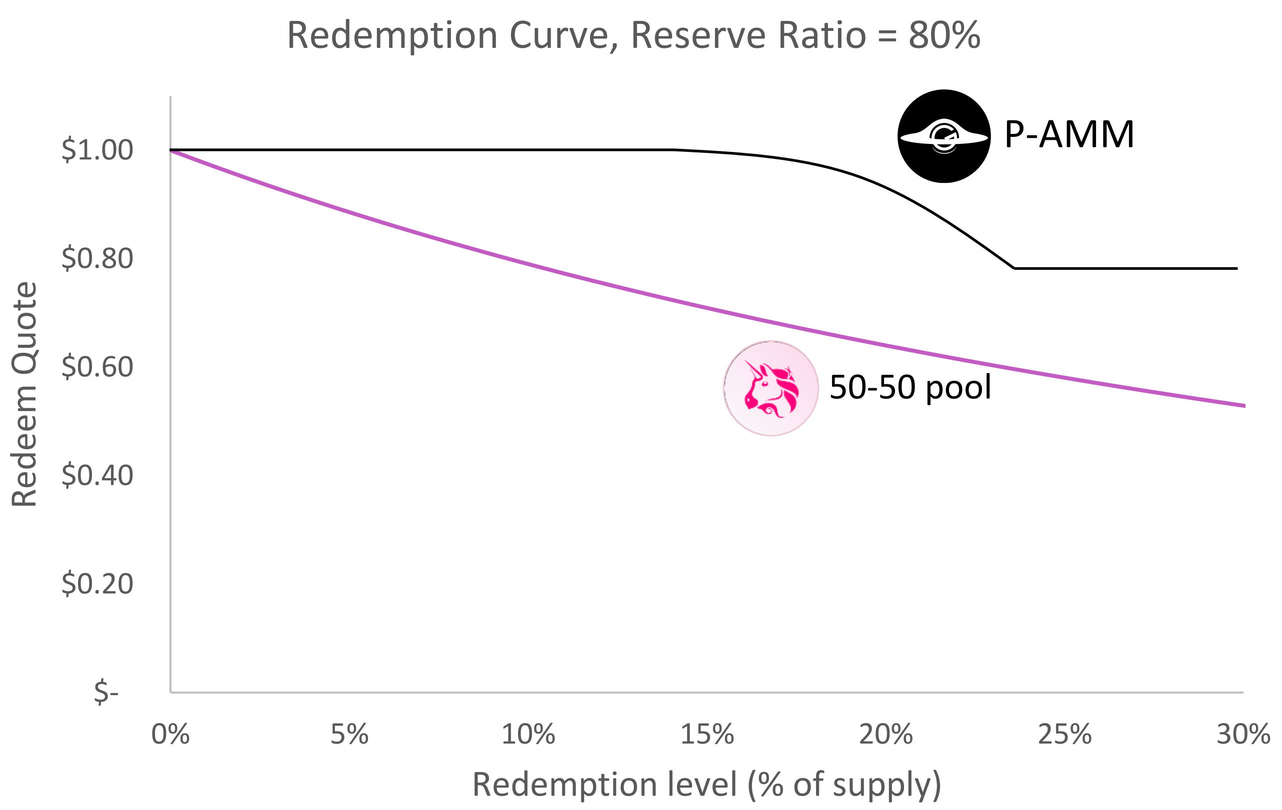
- Missing: how to design primary markets with desirable properties that can adapt autonomously?

Gyroscope P-AMM, 2021 (under review)

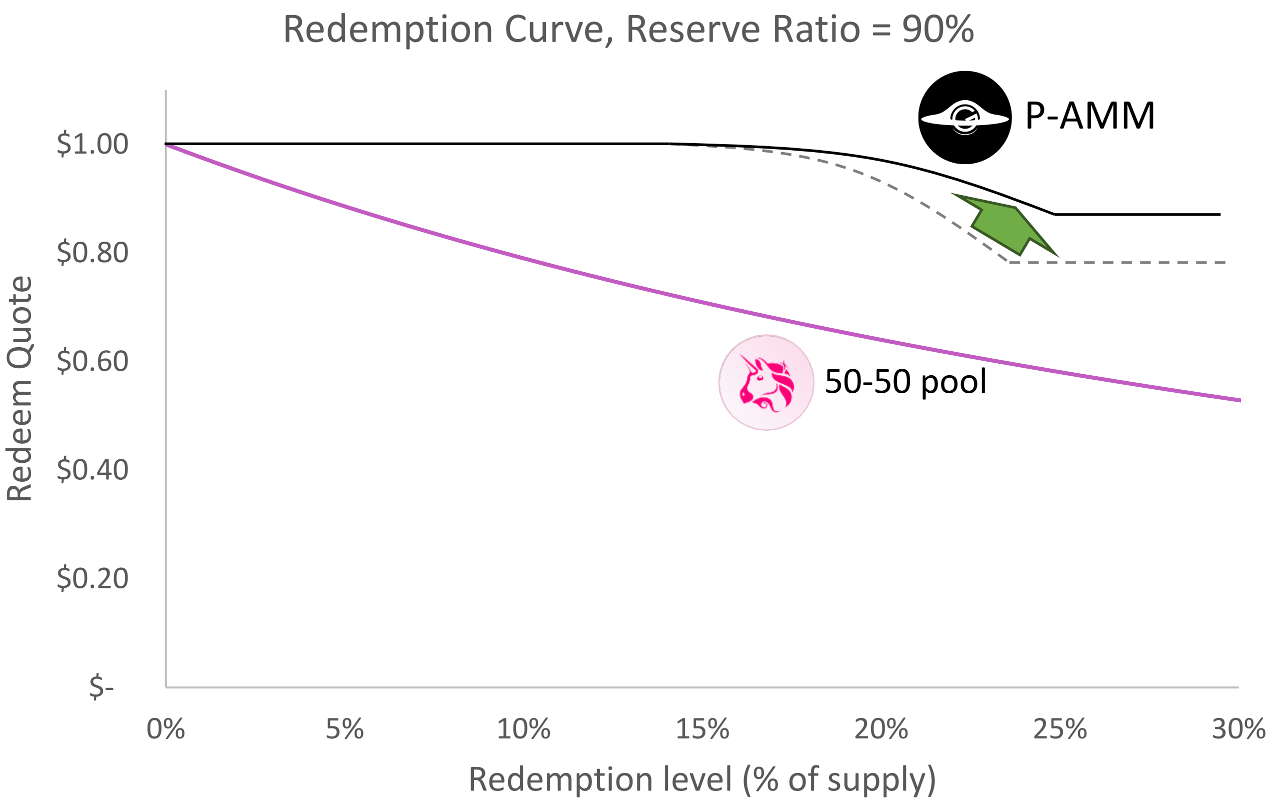
Designing Autonomous Primary Markets



Designing Autonomous Primary Markets



Designing Autonomous Primary Markets



Some Properties

- Bounded loss for protocol and redeemers
  - Reserve assets can't be depleted
- "Path deficiency"
  - No incentive to subdivide trades
- Efficiently computable on-chain
- Shape can deter speculative attacks

Conclusion

Conclusion

Stablecoins = complex on-chain currencies

- Many similarities with traditional finance
- Also many new risks and security challenges

Fundamental Design Problems

1. Technical Security
2. Economic Security
3. Economic Stability

To Dive Deeper

Stablecoins 2.0: Economic Foundations and Risk-based Models. AK, D Harz, L Gudgeon, JY Liu, A Minca. At ACM AFT (2020).

While Stability Lasts: A Stochastic Model of Stablecoins. AK, A Minca (2020).

(In)Stability for the Blockchain: Deleveraging Spirals and Stablecoin Attacks. AK, A Minca. To appear in Cryptoeconomic Systems, MIT Press (2021). Preprint 2019.

SoK: Decentralized Finance (DeFi). S Werner, D Perez, L Gudgeon, AK, D Harz, W Knottenbelt (2021).

Governance Extractable Value. L Lee, AK (2021 blog post).

Designing an Autonomous Primary Market for Stabilizing Non-custodial Stablecoins. AK, S Schuldenzucker (under review, 2021)

☞ Part of Gyroscope stablecoin: https://gyro.finance/