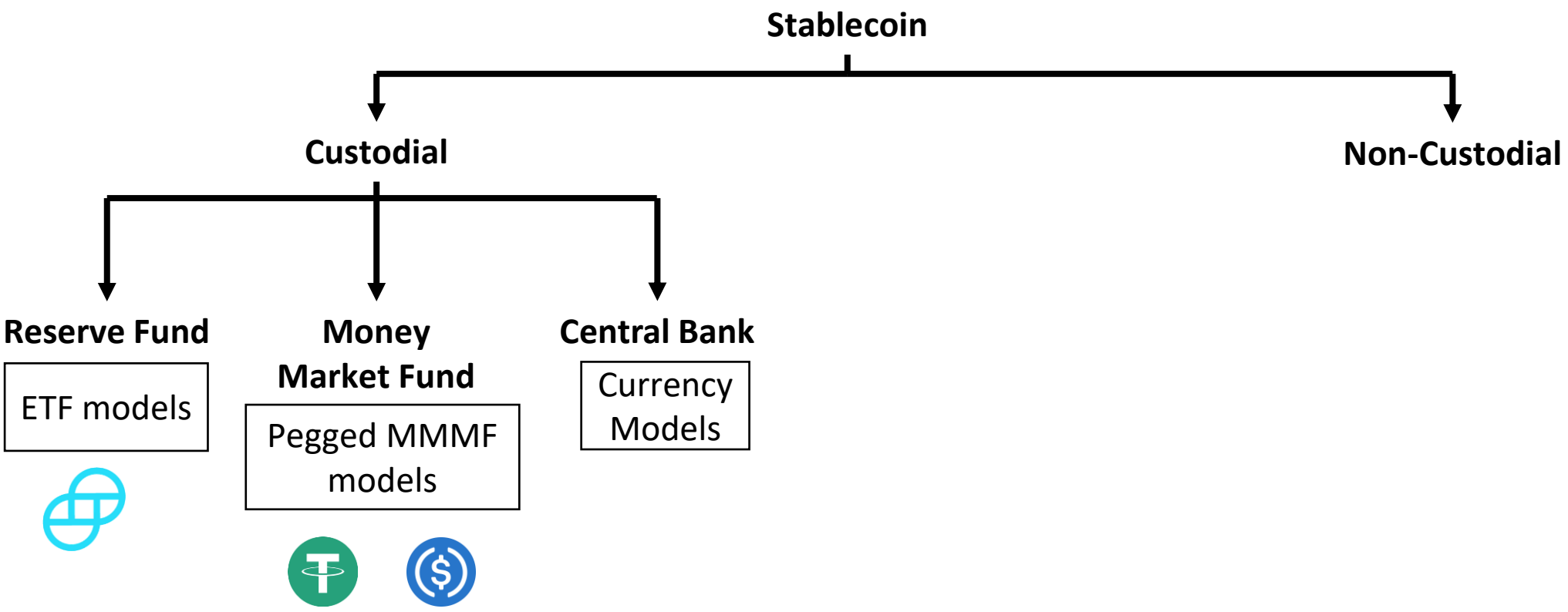
The (Un)Reasonable Design of Stablecoins

Ariah Klages-Mundt

Cornell University

IC3 | 26 Jul 2021

Over past year, many new types of stablecoins…



Over past year, many new types of stablecoins…

Who Absorbs Risk?	Asset Backing			
	Exogenous	< Both >	Endogenous	None
Agents	Dai, Rai, Liquity	Vai	Synthetix, bitUSD	Nubits, ESD, Basis
Equity Token	Duo Network	Iron, Frax	Terra, Steem, Celo	
Protocol Assets	Gyroscope, Fei			

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…

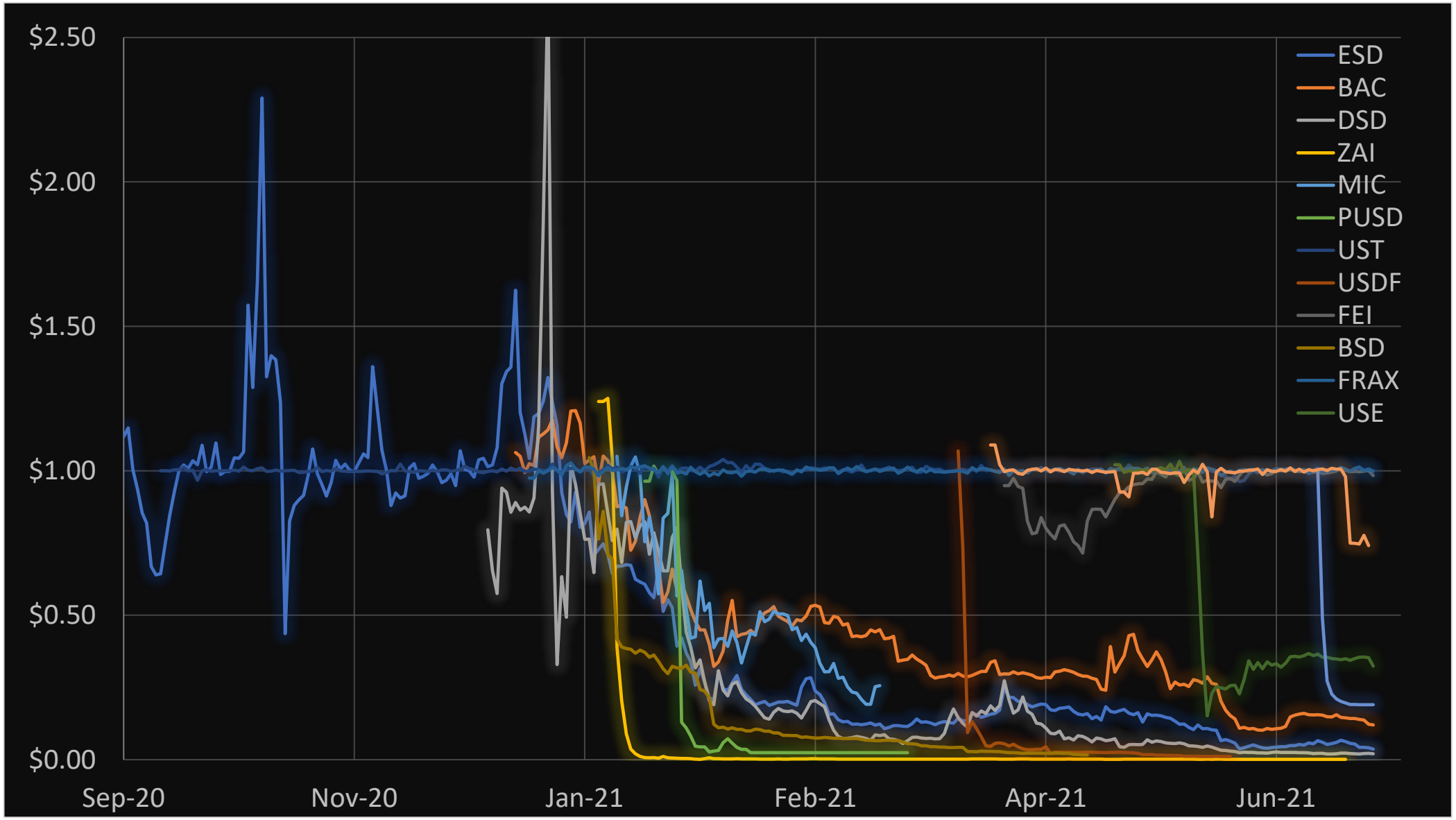
Who Absorbs Risk?	Asset Backing			
	Exogenous	< Both >	Endogenous	None
Agents	Dai, Rai, Liquity	Vai ⚠	Synthetix, bitUSD, Nubits	ESD, Basis
Equity Token	Duo Network	Iron, Frax	Terra ⚠, Steem, Celo	
Protocol Assets	Gyroscope, Fei ⚠			

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 talk: Non-custodial stablecoins (and DeFi more generally)

- Three fundamental design problems
  1. Technical security
  2. Economic security
  3. Economic stability
- Our work exploring these

Work we will draw from

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).

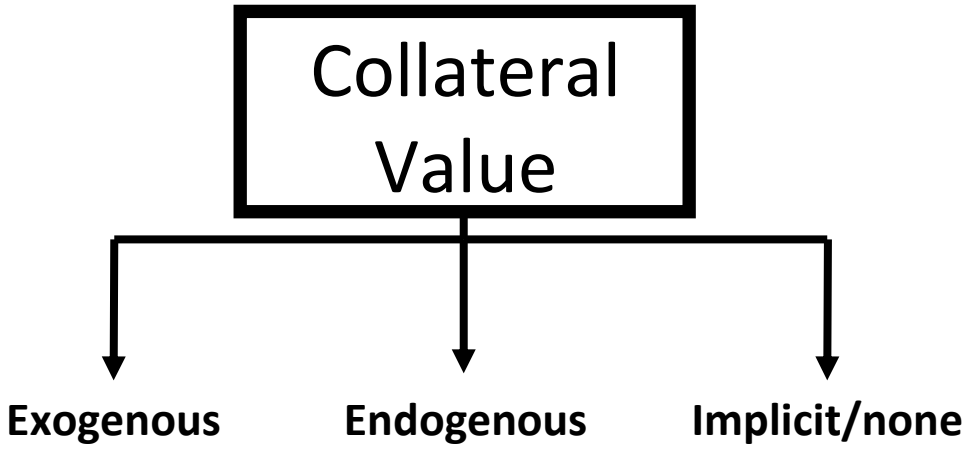
(In)Stability for the Blockchain: Deleveraging Spirals and Stablecoin Attacks. AK, A Minca. To appear in Cryptoeconomic Systems, MIT Press (2021). Preprint 2019.

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

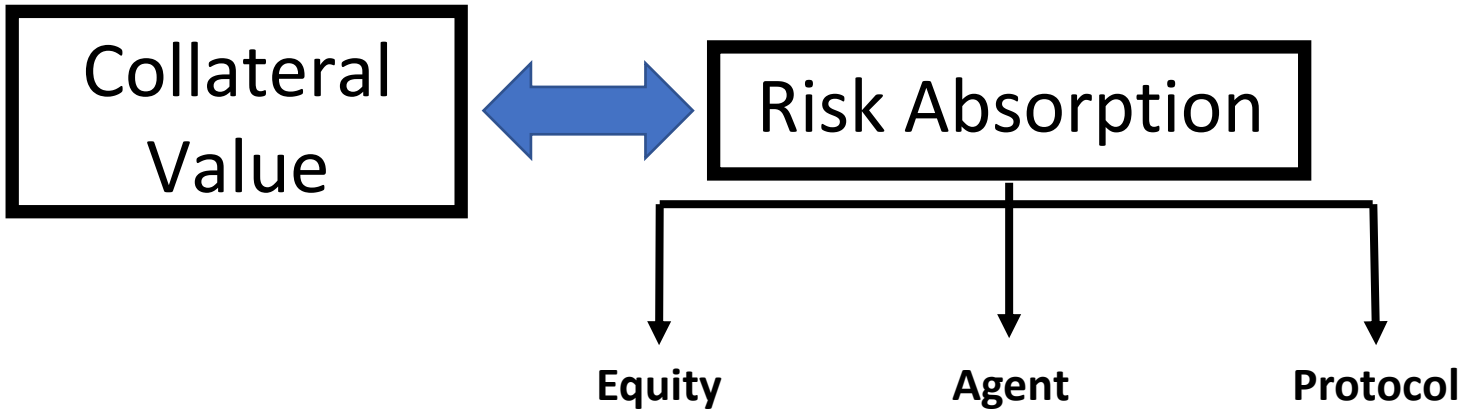
Governance Extractable Value. L Lee, AK (2021 blog post).

Designing an Autonomous Primary Market for Stabilizing Non-custodial Stablecoins. AK, S Schuldenzucker (not yet released)

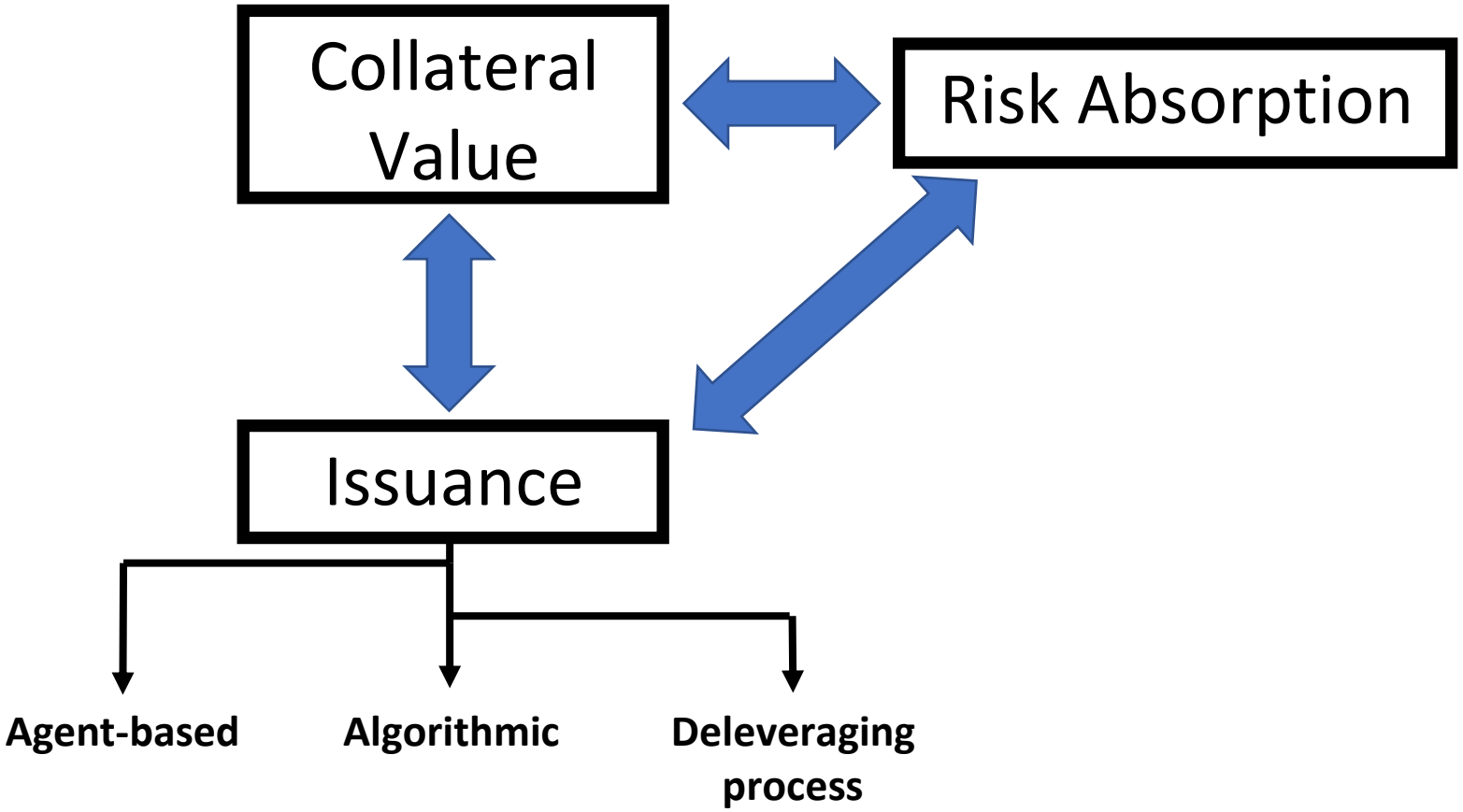
Anatomy of Non-custodial Stablecoins



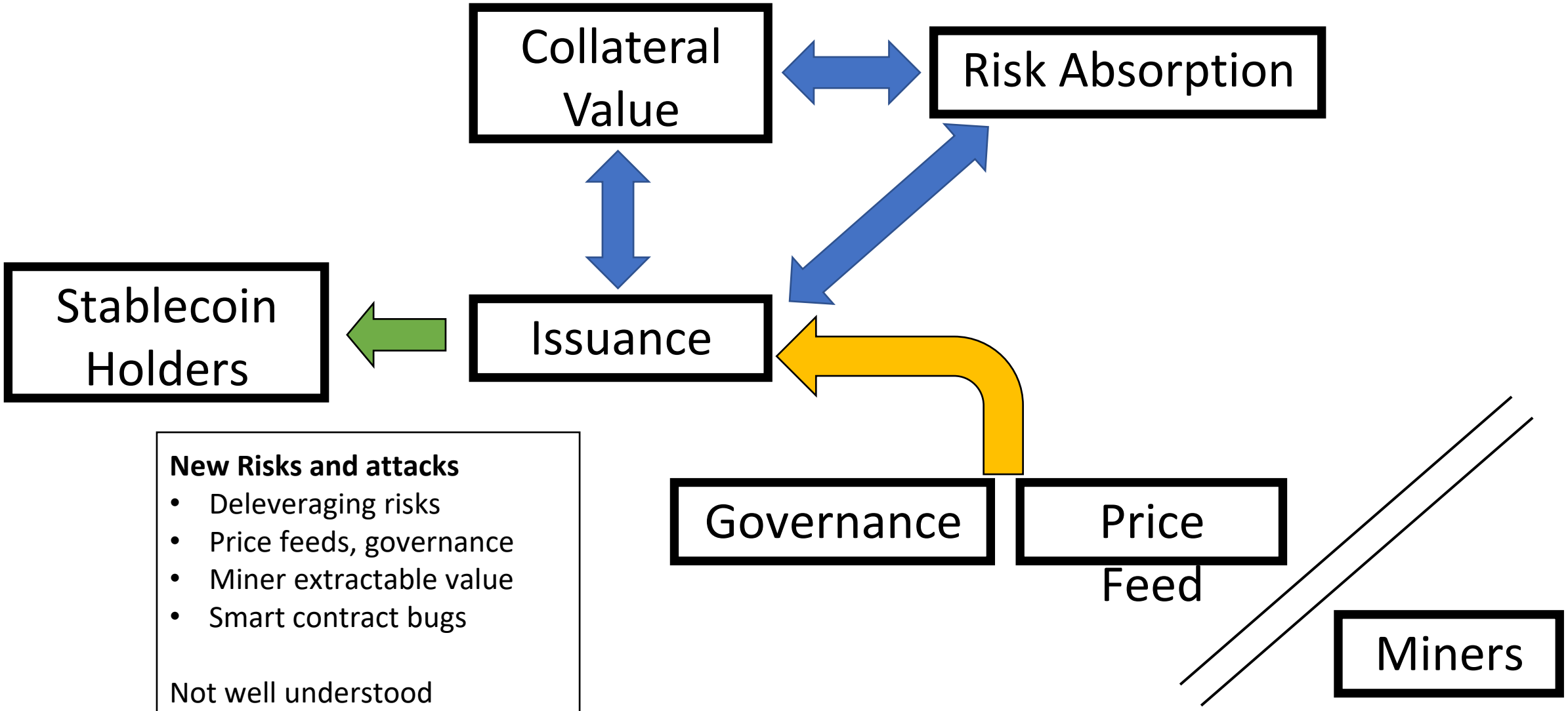
Anatomy of Non-custodial Stablecoins



Anatomy of Non-custodial Stablecoins



Anatomy of Non-custodial Stablecoins



New Risks and attacks

- Deleveraging risks
- Price feeds, governance
- Miner extractable value
- Smart contract bugs

Not well understood

-----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

- Variant later occurred in Dai

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

(In)Stability for the Blockchain, 2019

Stablecoins 2.0, 2020

- Tractable "forking" model of MEV-based reorgs

Our Work on Economic Security

GEV = short-termism and governance attacks (e.g., rugpulls)

- Capital structure models for “price of anarchy”
- “Honest” incentives may not be enough
- Impossibility conjecture about many systems today

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

Stablecoins 2.0, 2020

Governance Extractable Value (blog), 2021

Optimistic Approval mechanism to bypass impossibility

- 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?

-----Deleveraging Spirals in Dai-----

(In)Stability for the Blockchain, 2019

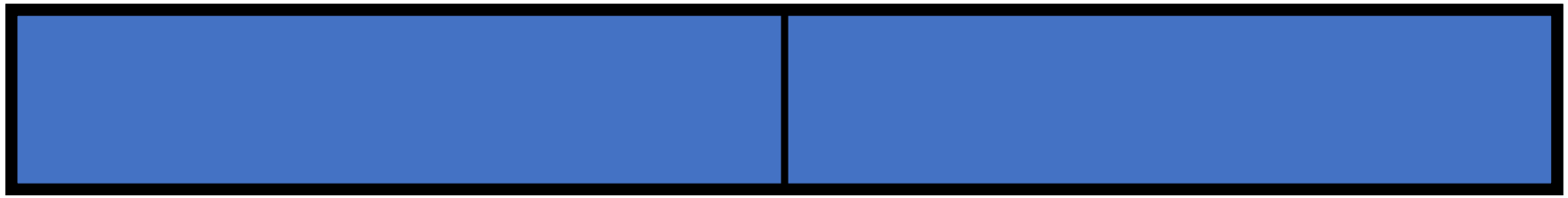
While Stability Lasts, 2020

CDO Structure

A portfolio of underlying assets

CDO Structure

Split into 2 tranches

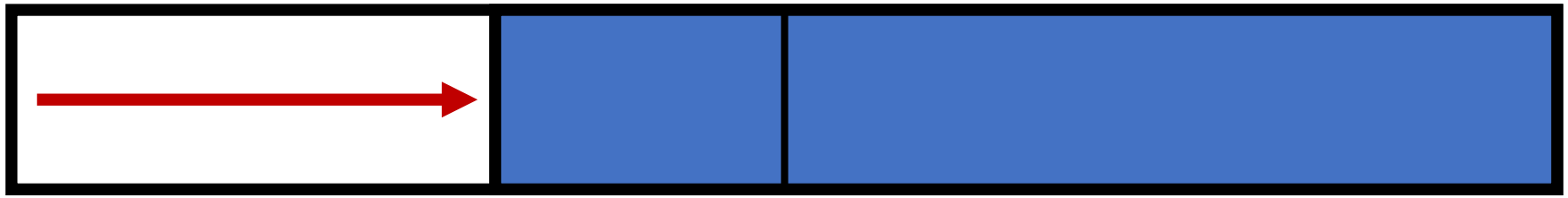


Junior tranche = more risky

Senior tranche = less risky

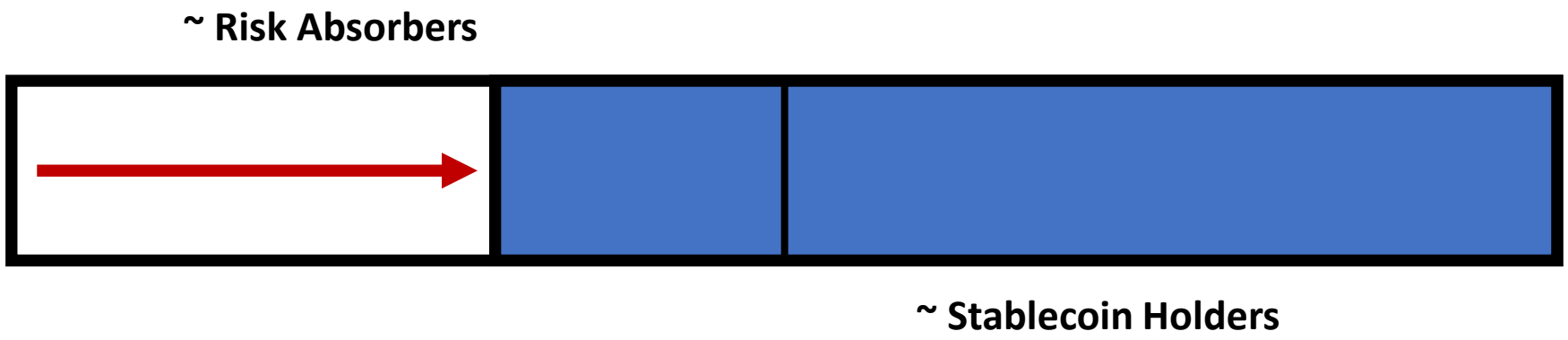
CDO Structure

Losses that occur are first borne by junior tranche

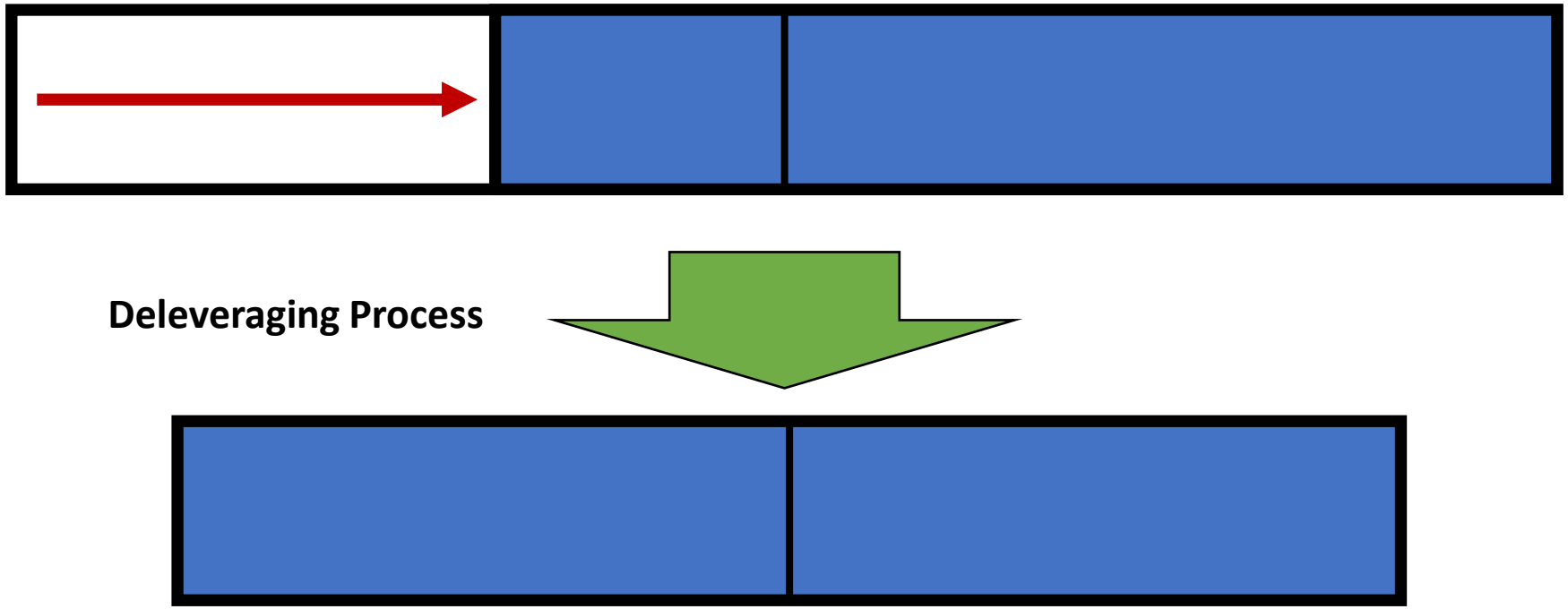


Senior tranche protected

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

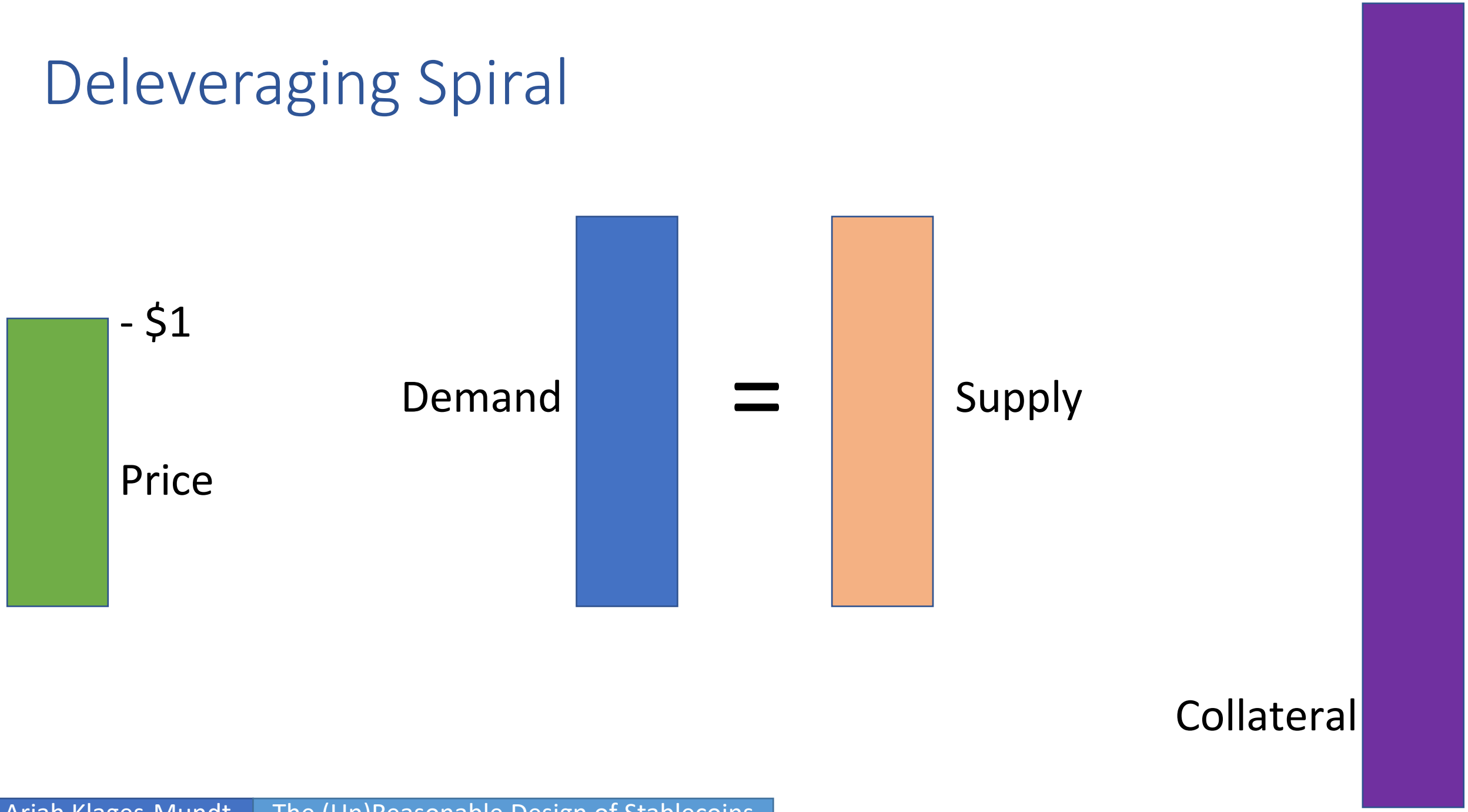
Decision: Change stablecoin supply to maximize next period expected returns

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

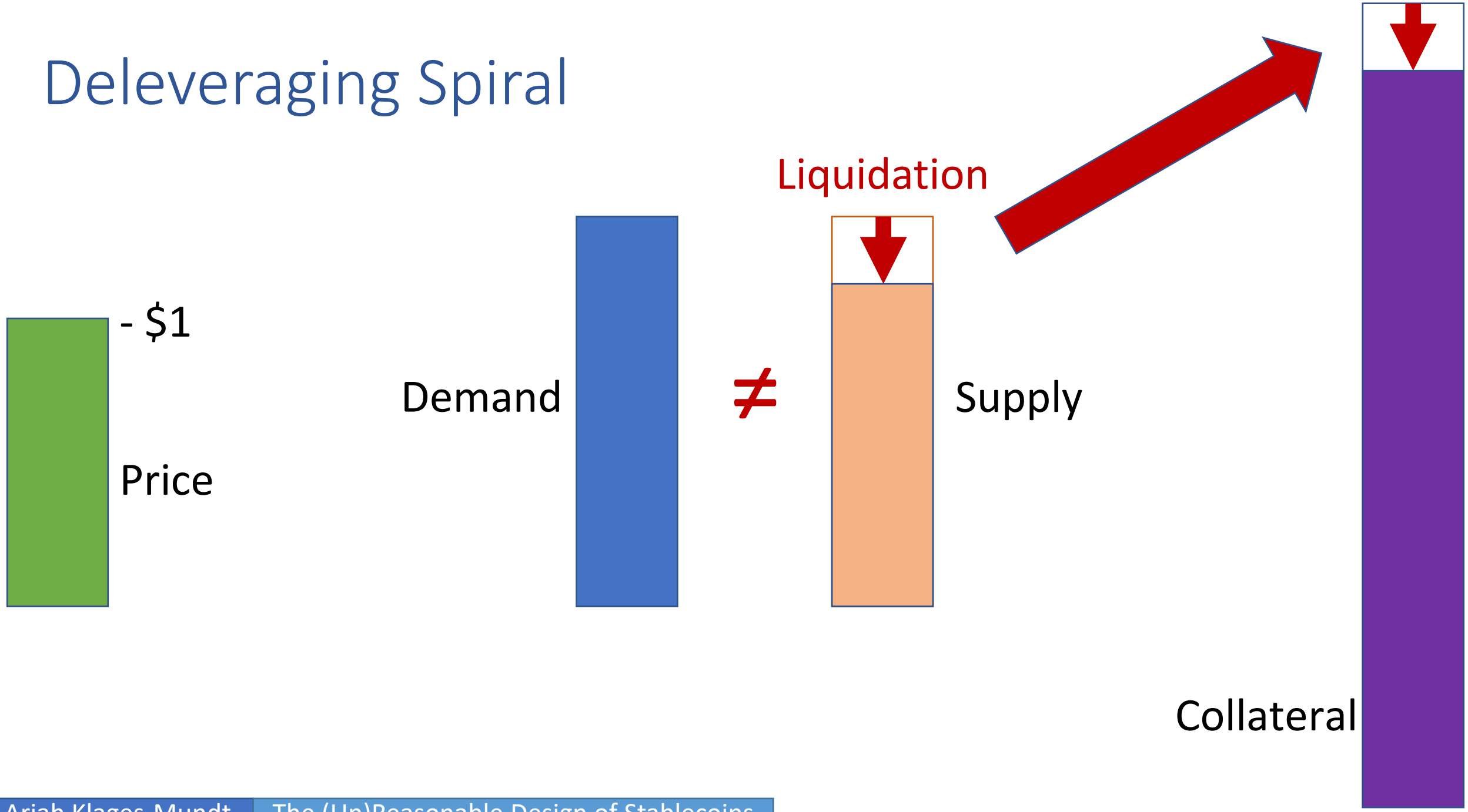
$$\text{s.t.} \quad \bar{N}_t X_t \geq \beta L_t$$

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

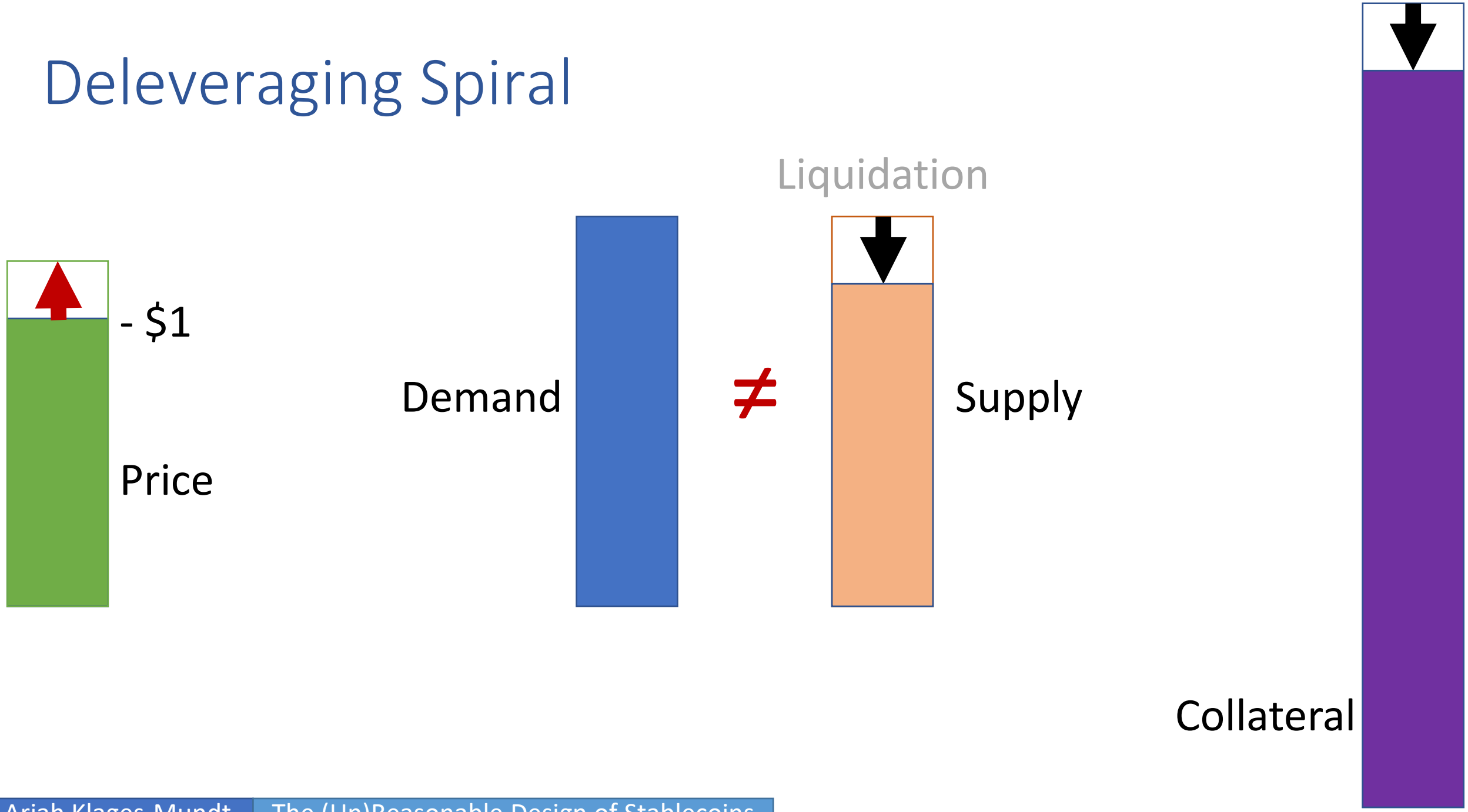
Deleveraging Spiral



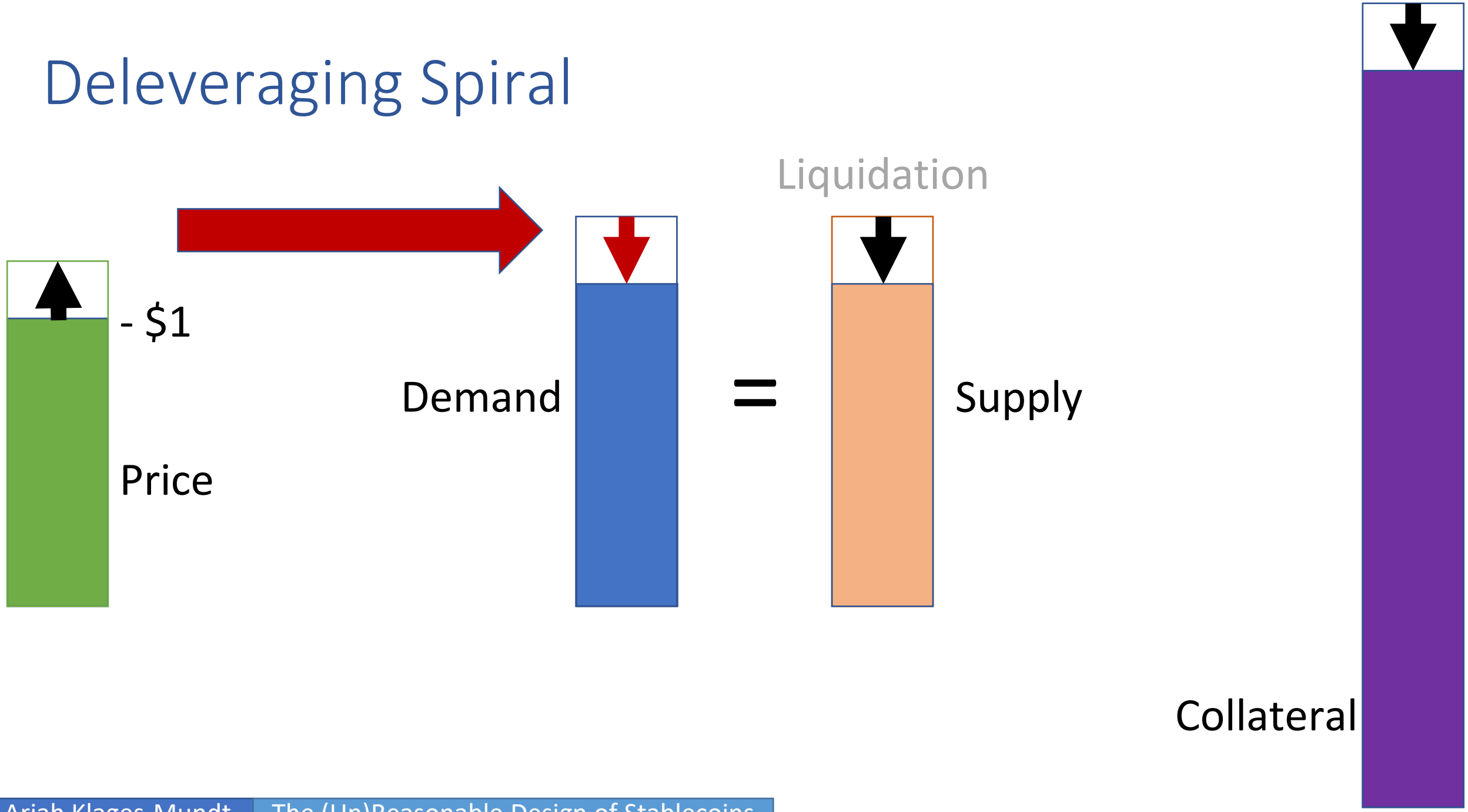
Deleveraging Spiral



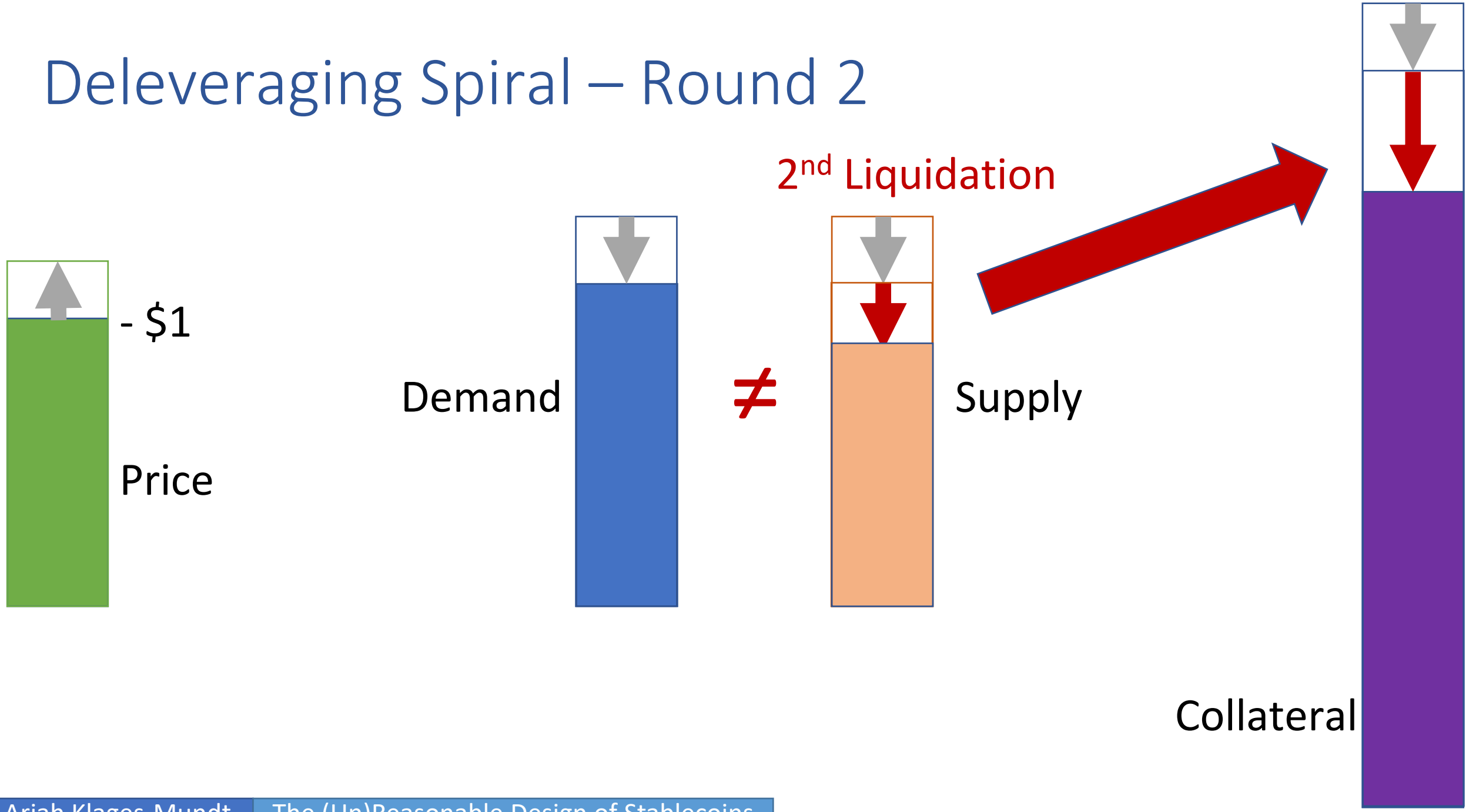
Deleveraging Spiral



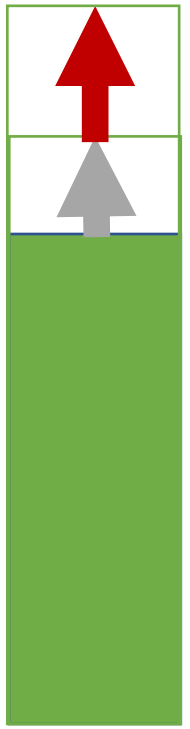
Deleveraging Spiral



Deleveraging Spiral – Round 2



Deleveraging Spiral – Round 2

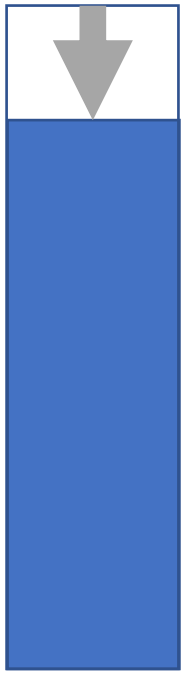


- $1

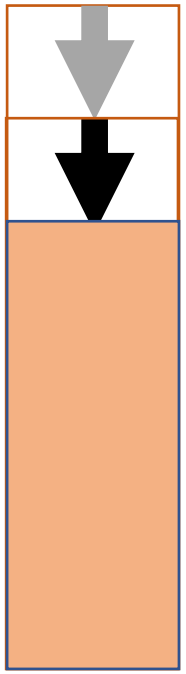
Price

2nd Liquidation

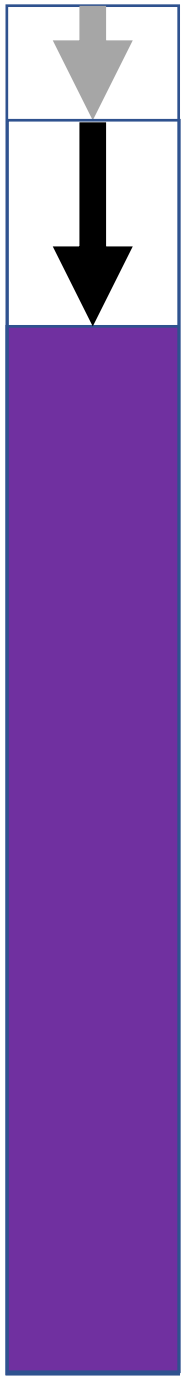
Demand



≠

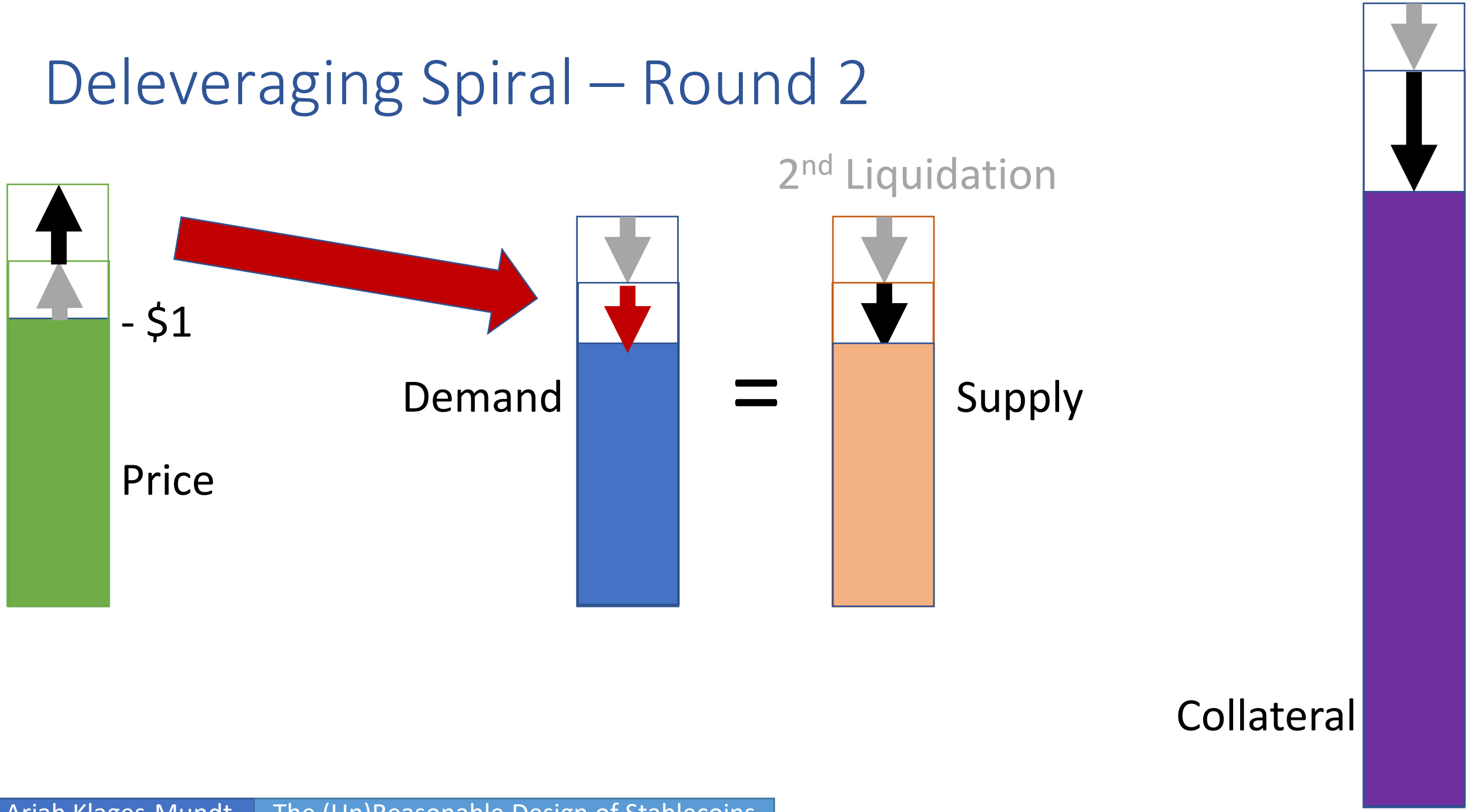


Supply



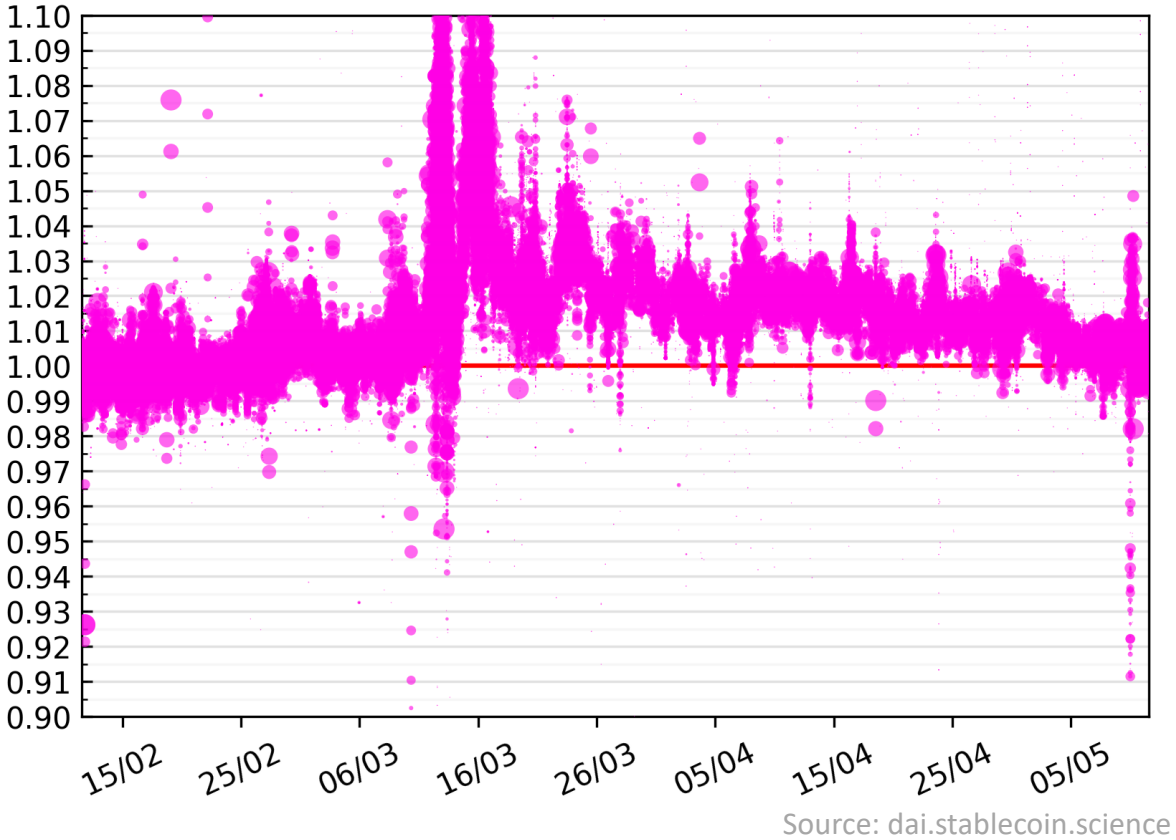
Collateral

Deleveraging Spiral – Round 2



Black Thursday in Dai, March 2020

~50% ETH price crash



Source: dai.stablecoin.science

Liquidation price effect on Dai DEX trades

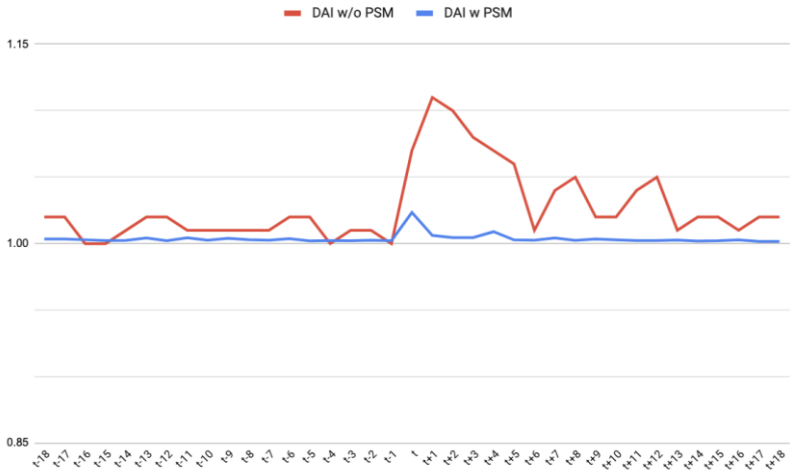
Non-custodial Complications

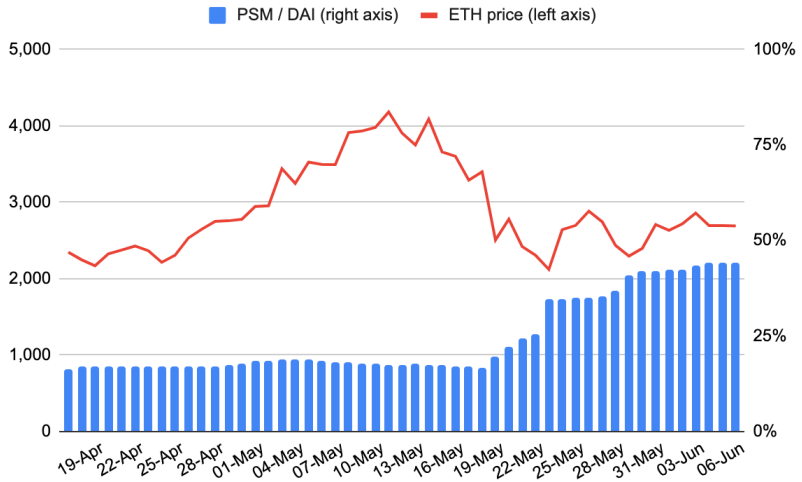
- No stable region when X_t is not ~ submartingale (positive expectations)
- *Seeming contradiction:* goal to make decentralized stablecoin, but can only be fully stabilized by adding uncorrelated assets, which are currently custodial
- Patching this has been major topic since Black Thursday

Non-custodial Complications

Solutions:

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



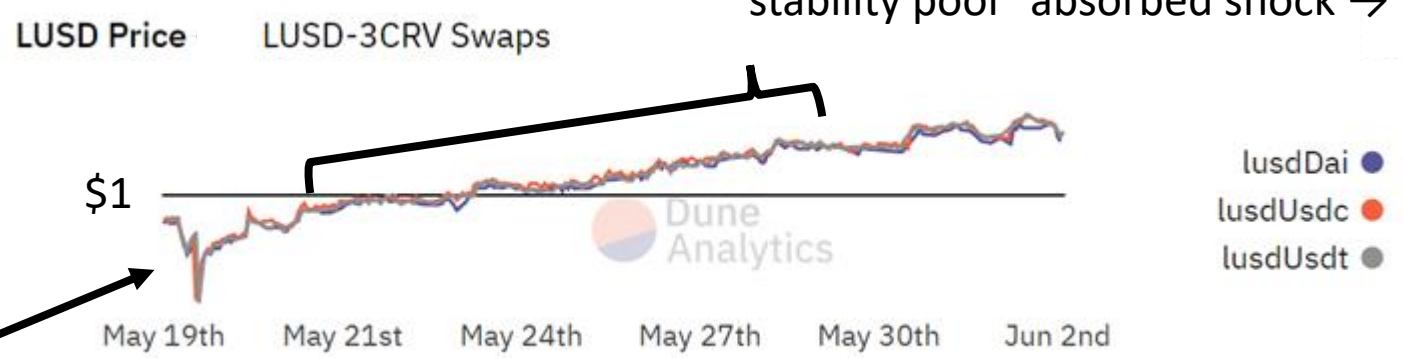


Non-custodial Complications

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:

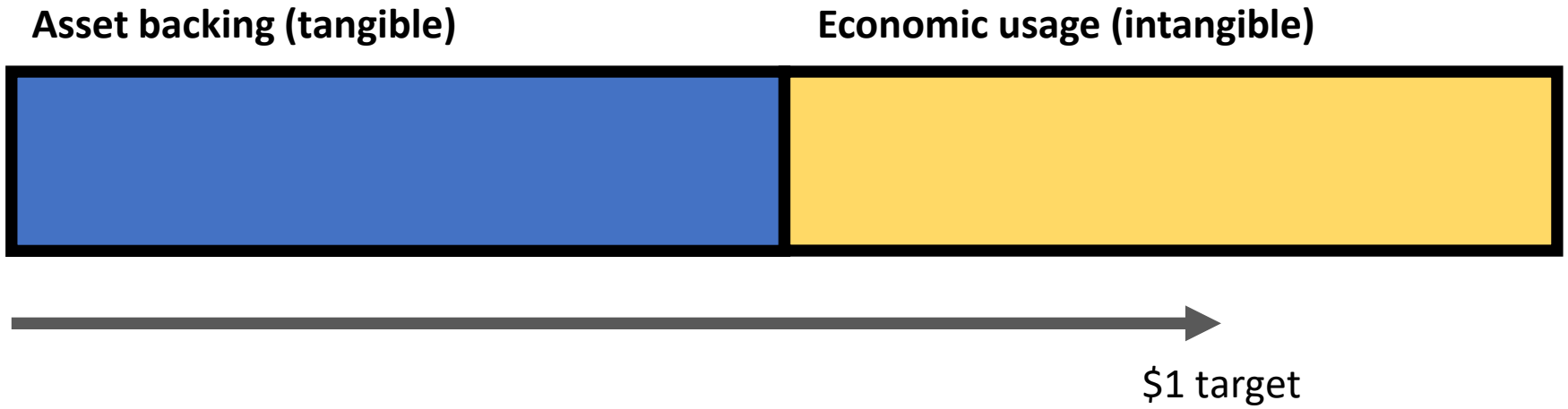
- **Maker:** Since Black Thursday has tethered to USDC (+ custodial risks)
  - Maintaining exchangeability via USDC reserve ("PSM")
- **Rai:** negative rates during crises (equilibrium participation, liquidity?)
- **Liquity (and our 2020 paper):** Dedicated liquidity pools for crises
- **Reserve-backed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

-----Algorithmic Design-----

Gyroscope P-AMM, 2021 (soon)

What Backs a Currency Peg?

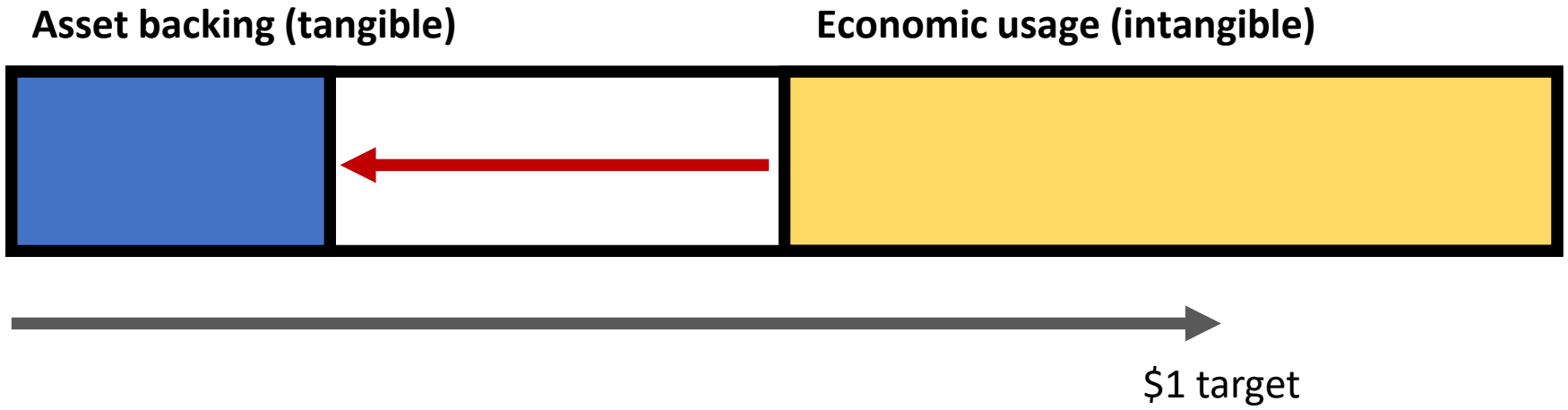
2 sources of value



Peg sustained!

What Backs a Currency Peg?

A shock to one of these…



What Backs a Currency Peg?

A shock to one of these…

Peg breaks!

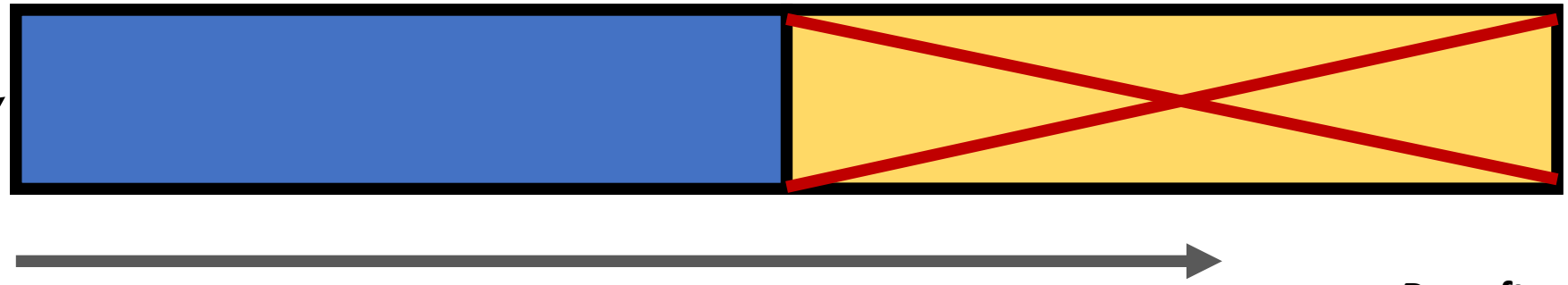
*Highly simplified: see (Morris & Shin, 1998) for more precise model

What Backs Algorithmic Stablecoins?

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

Asset backing (tangible)

~~Economic usage (intangible)~~



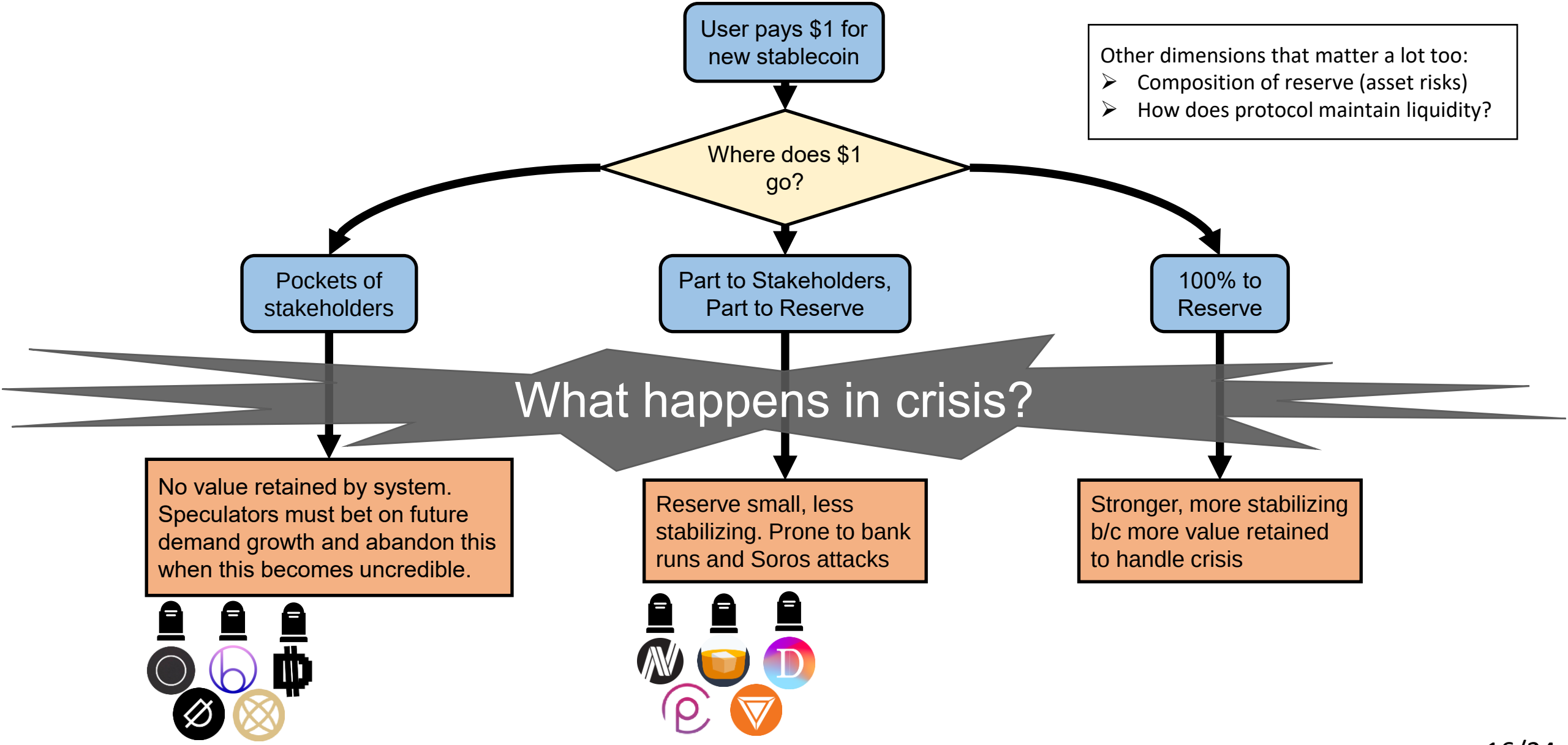
$1 target

Peg often breaks!

What are these assets?

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

Contrasting Algorithmic Stablecoins



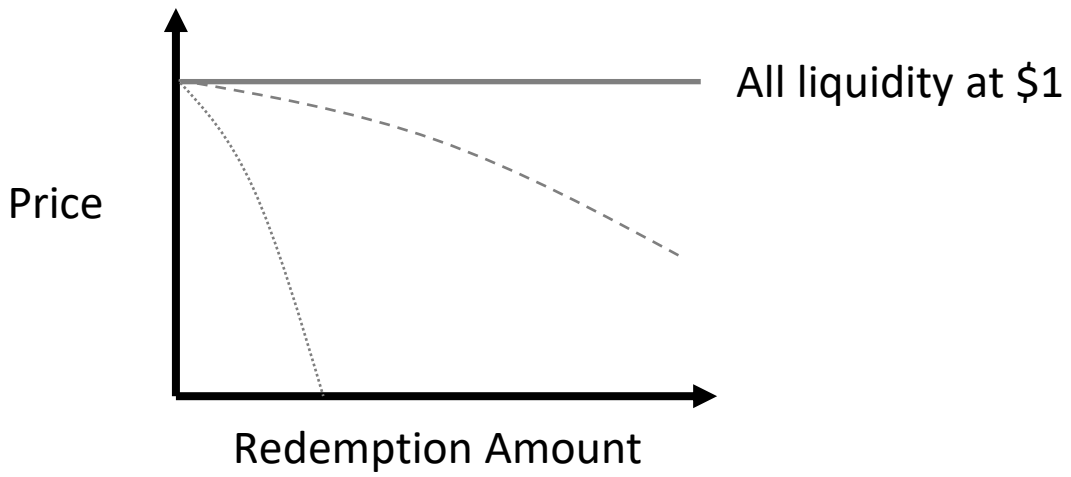
Other dimensions that matter a lot too:

- Composition of reserve (asset risks)
- How does protocol maintain liquidity?

Algorithmic Primary Markets

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

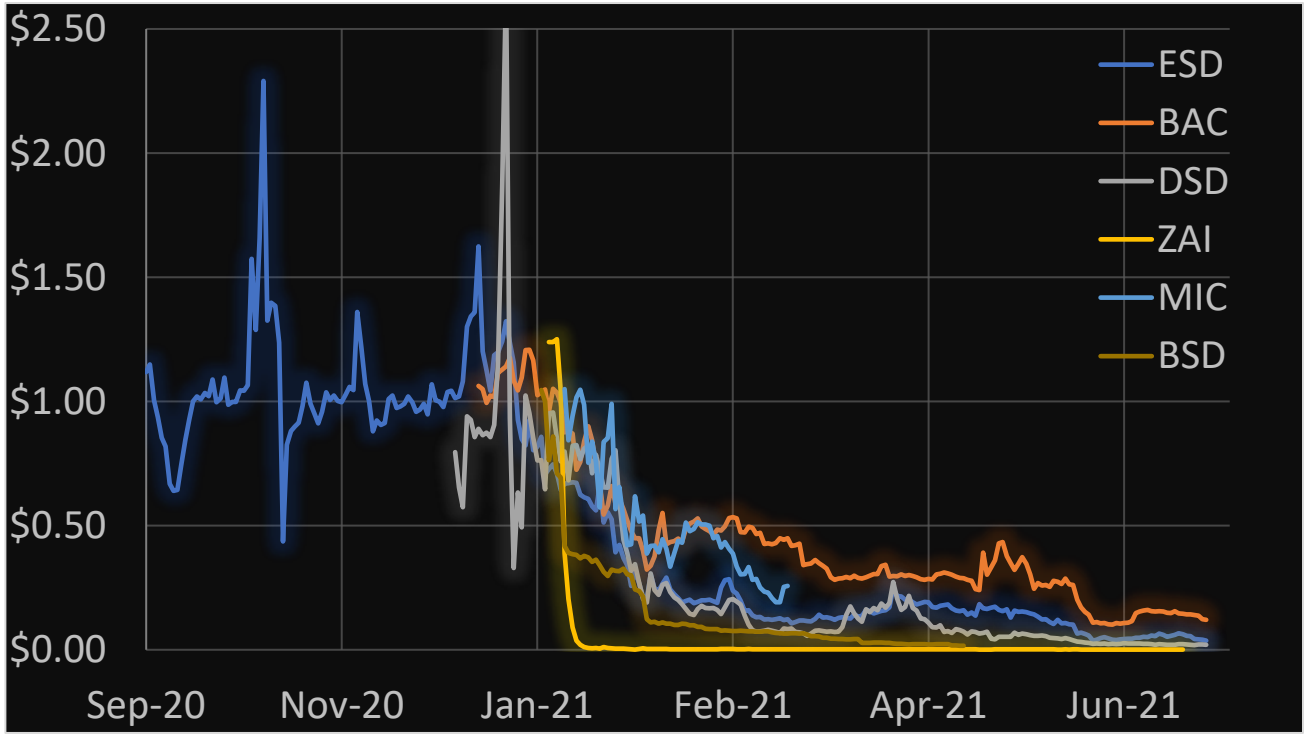
- **A key factor:** What do redemption curves look like?



Algorithmic Primary Markets

Case study 1: Basis/ESD

- Flat at $0 (no asset backing)



Algorithmic Primary Markets

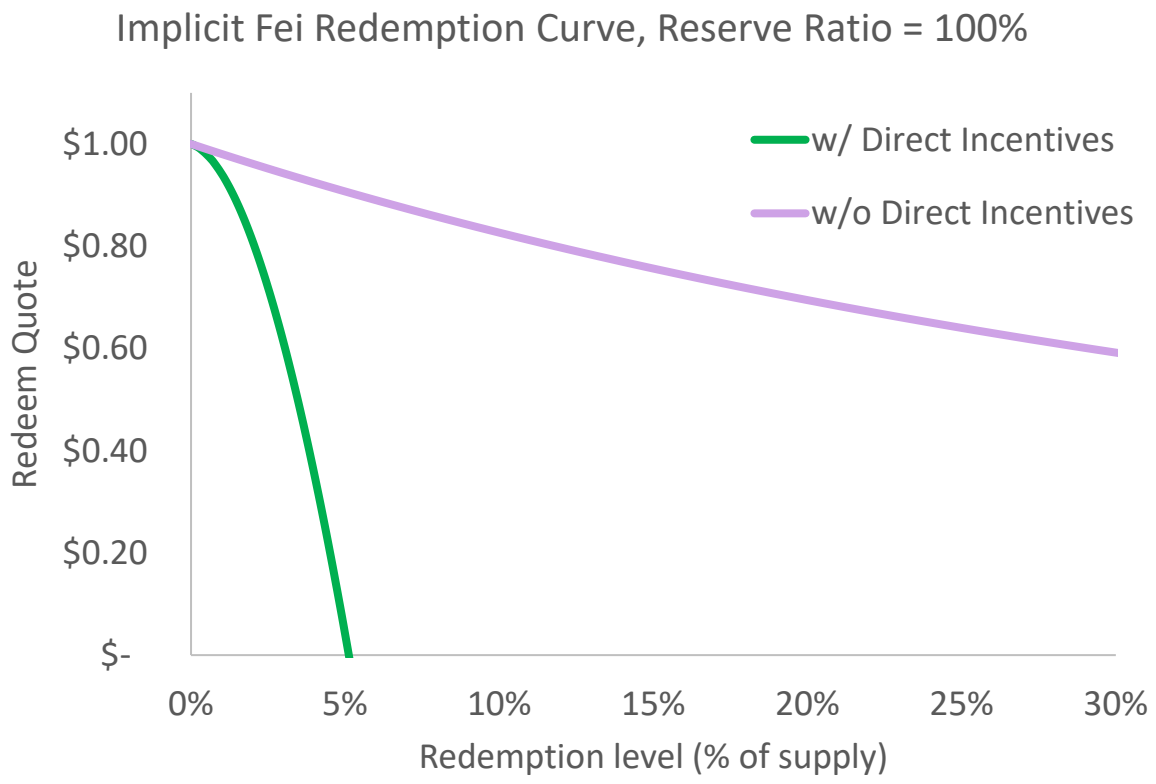
Case study 2: USDC/USDT

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

Algorithmic Primary Markets

Case study 3: Fei

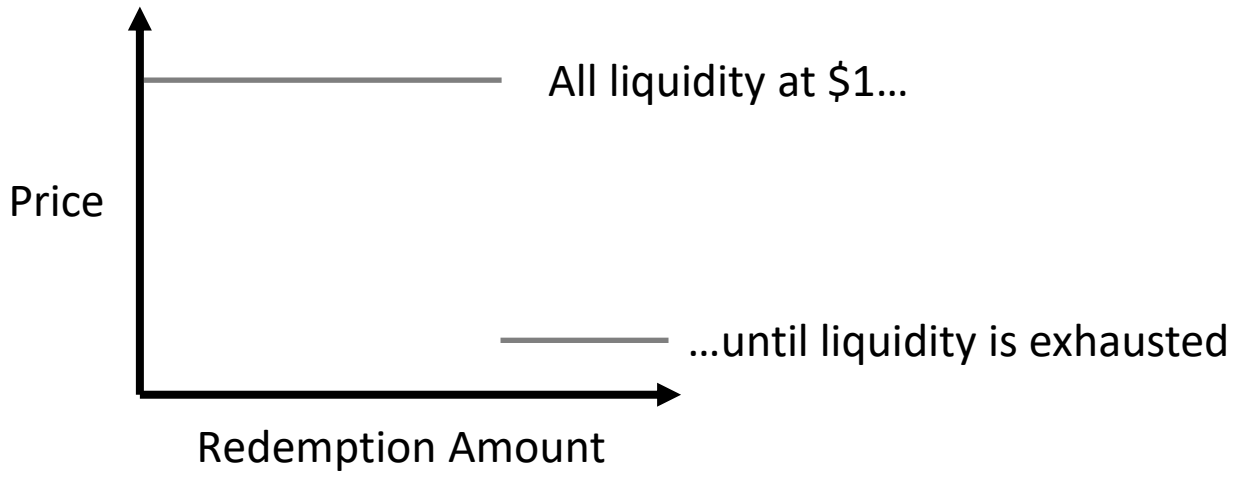
- Implicit redemption curve very steep to $0



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:

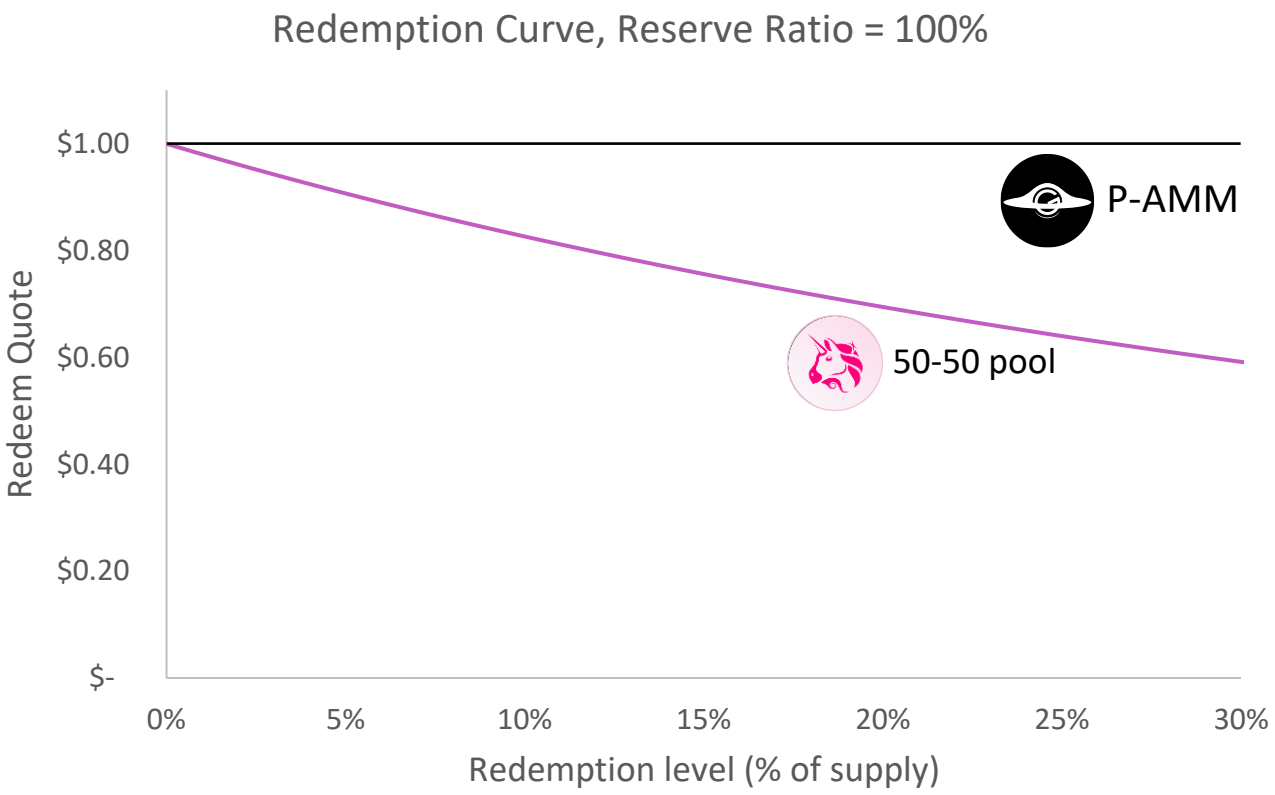
IRON stablecoin:

Designing Autonomous Primary Markets

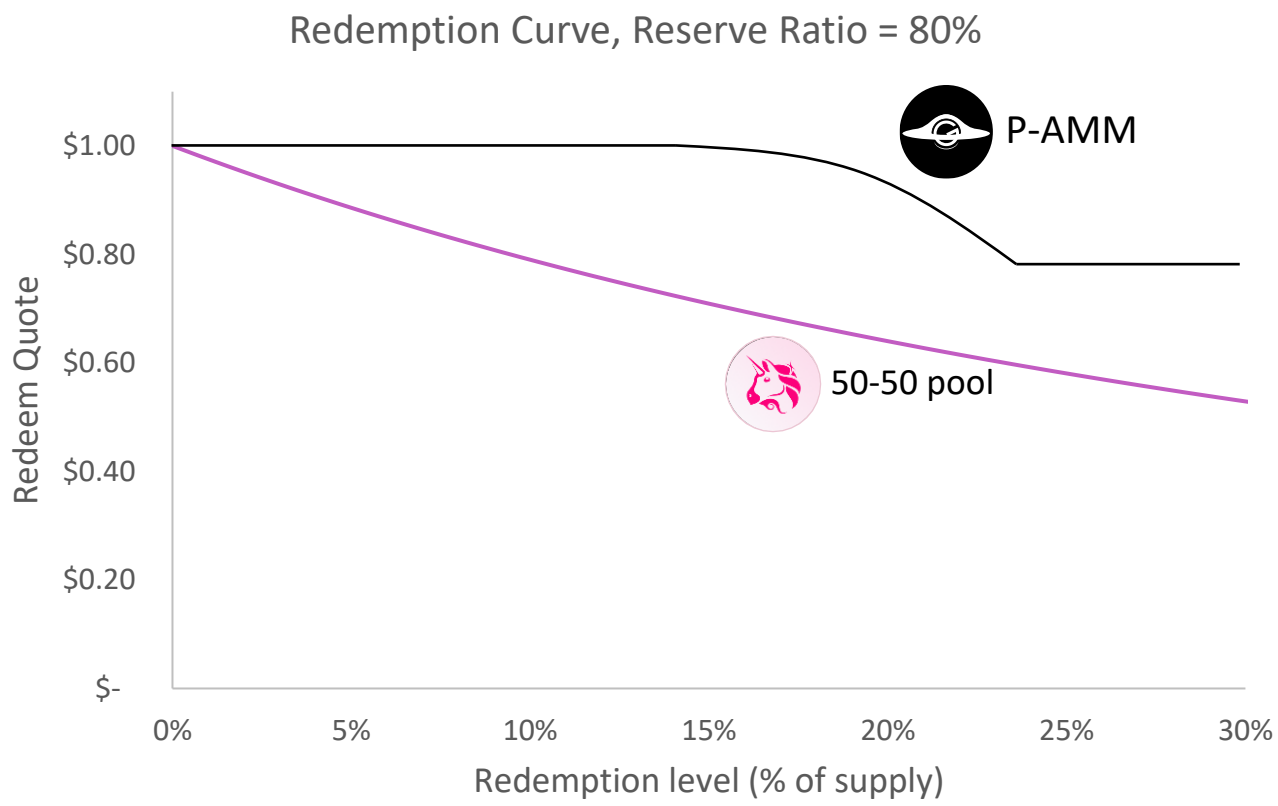
- Current space of primary market mechanisms
  - Ad hoc design
  - Need governance to make quick fixes in crises
- Missing: how to design primary markets with desirable properties that can adapt autonomously?

Gyroscope P-AMM, 2021 (soon)

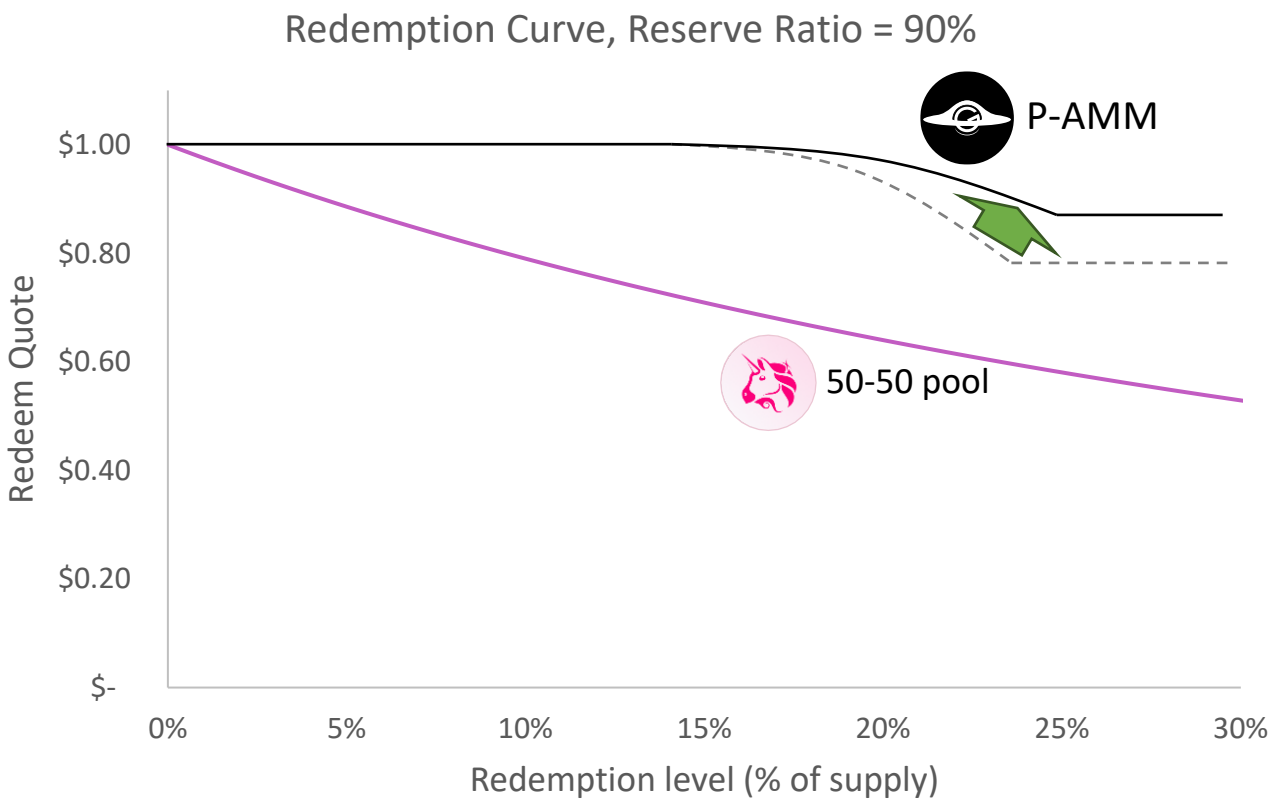
Designing Autonomous Primary Markets



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

The End: Papers available on arXiv

We seed stablecoin and DeFi design problems and models

Fundamental Design Problems

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

Design gap: robust reserve-backed stablecoins designed for liquidity
👉 led us to design Gyroscope: https://gyro.finance/