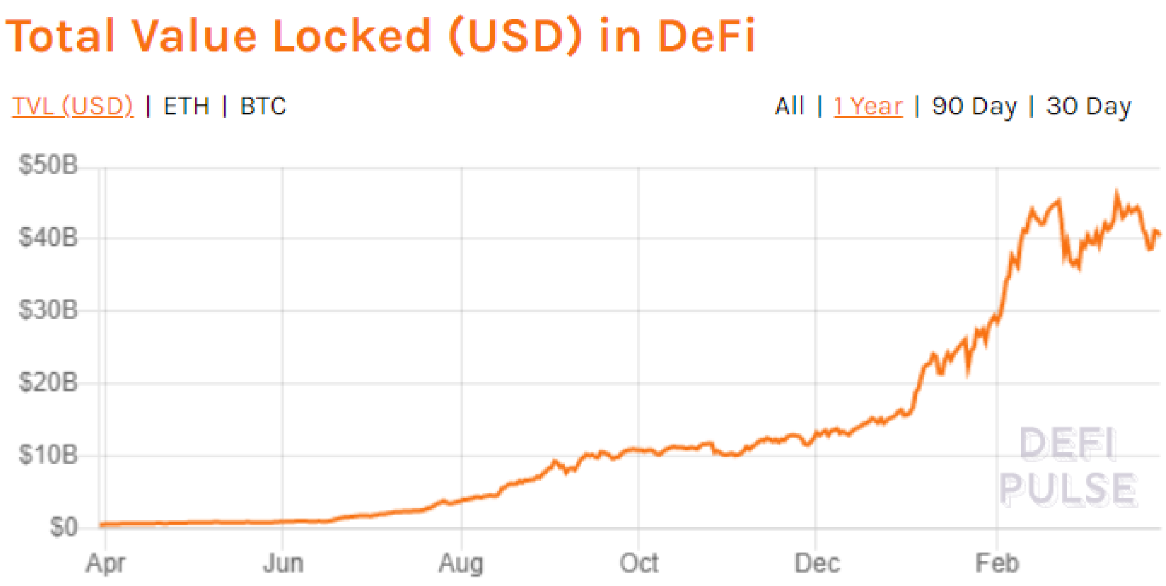
The (Un)Reasonable Design of Stablecoins

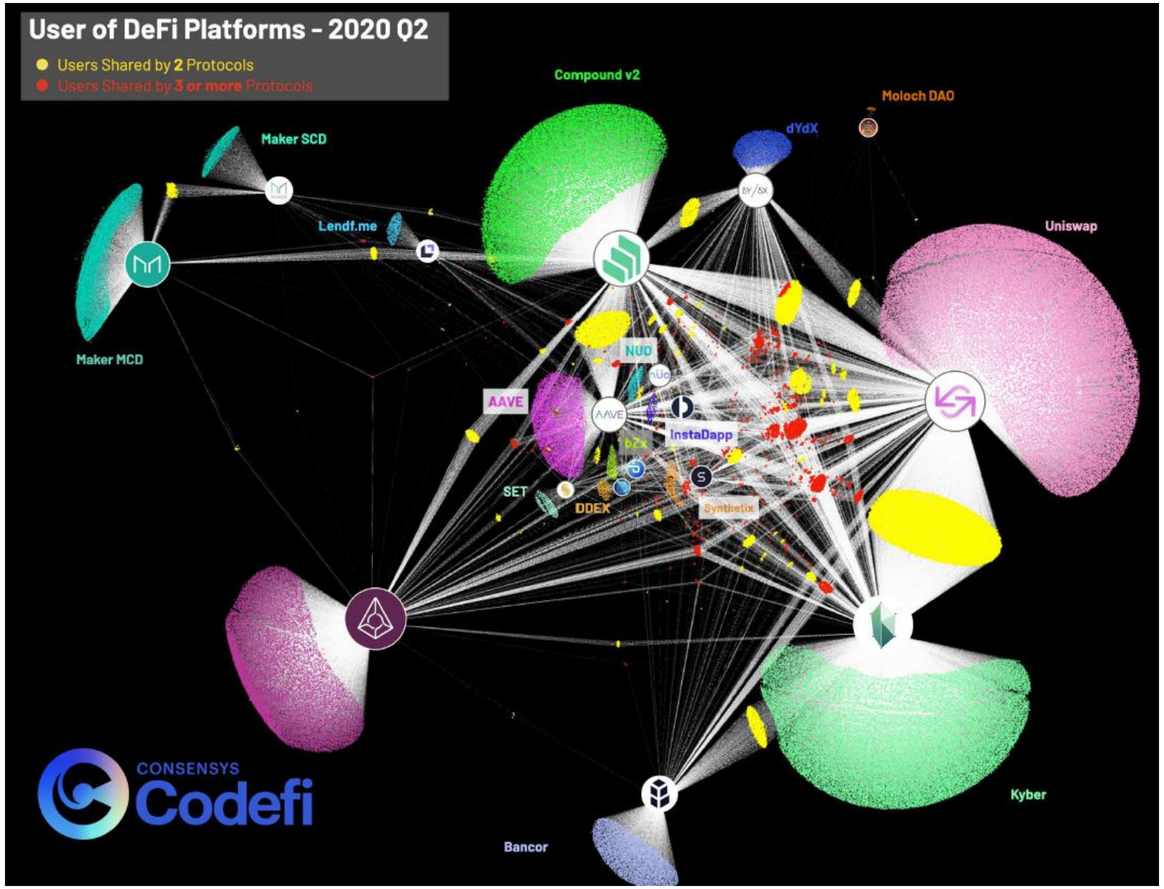
Ariah Klages-Mundt

Cornell University

IC3 | 29 Apr 2021

A Year of DeFi

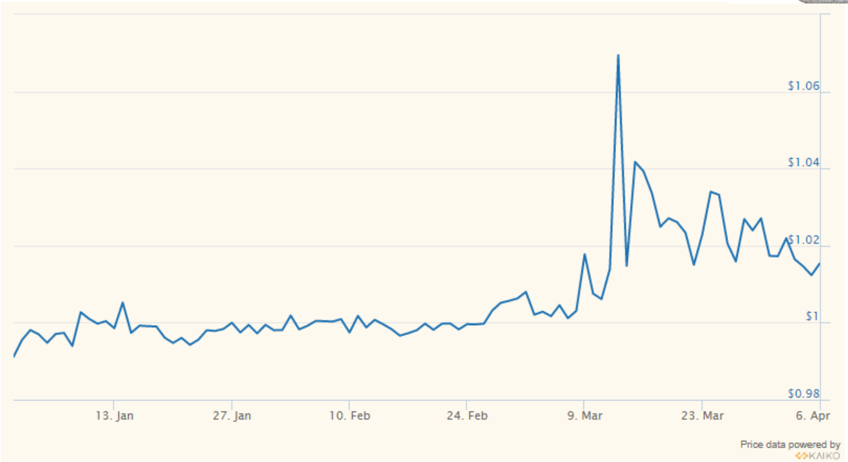




A Year of DeFi **Crises**

ETH price

DAI price



Deleveraging spirals anticipated in (K-M, 2019)

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

A Year of DeFi Crises

ETH price

veraging spirals anticipated in (K-M, 2019)

Developer Flags Big-Money Loophole for Stealing All the ETH in MakerDAO

Dec 9, 2019 at 15:05 UTC ▪ Updated Dec 9, 2019 at 15:29 UTC

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

DAI price

Miners Trick Stablecoin Protocol PegNet, Turning $11 Into Almost $7M Hoard

Apr 22, 2020 at 09:20 UTC ▪ Updated Apr 22, 2020 at 17:03 UTC

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

A Year of DeFi Crises

Stablecoin: cryptocurrency with added economic structure that aims to stabilize price/purchasing power

- We lack risk-based models spanning design space, trade-offs
- **Our work:** fills this gap and seeds future stablecoin research

This talk

1. Decomposition of Design Space
2. Fundamental Design Questions
3. Price Dynamic Models
4. GEV and MEV models

Papers available on arXiv

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).

----Decomposition of Design Space----

Risk-based Overview

Stablecoin

Custodial

Non-Custodial

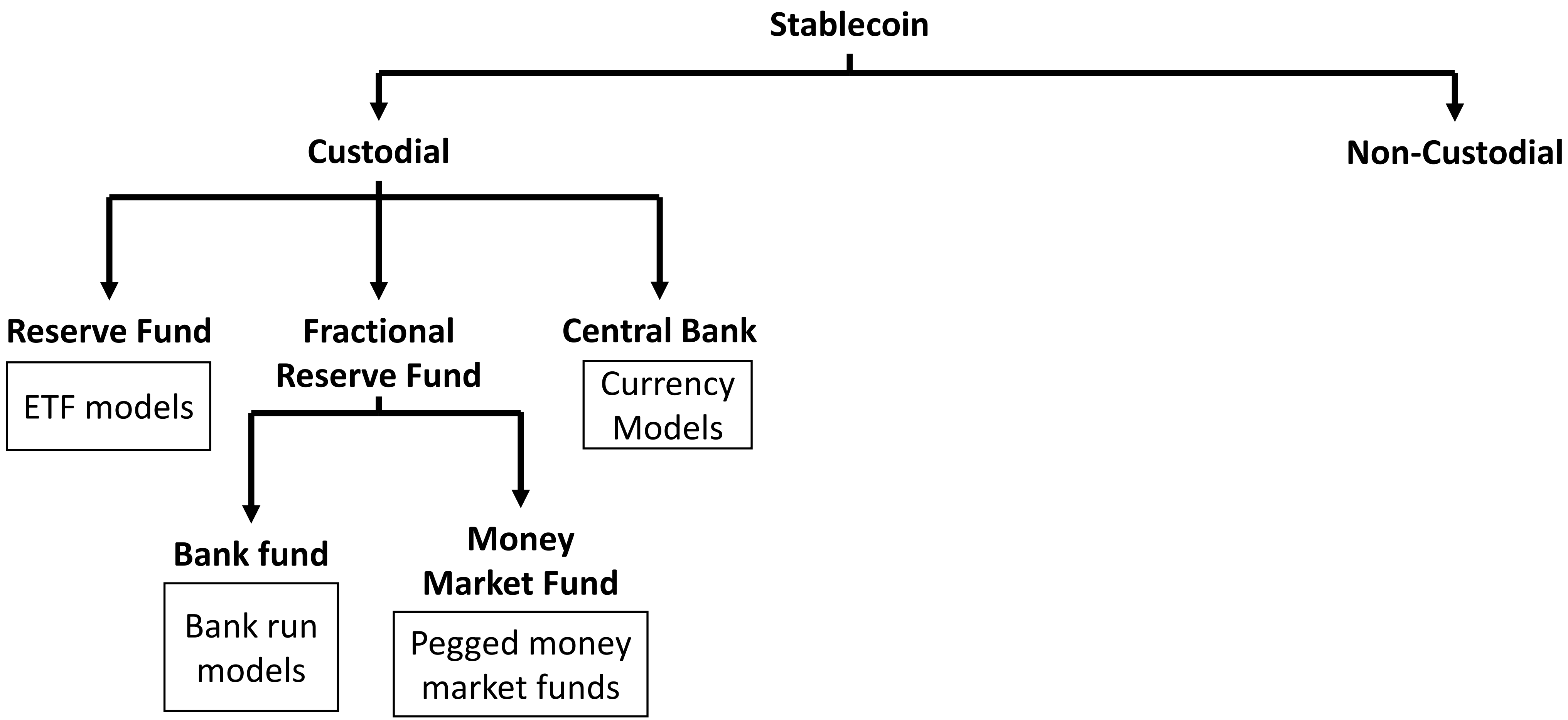
Risks
- Counterparty credit risk
- Censorship risk
- Traditional financial risks

Well understood!

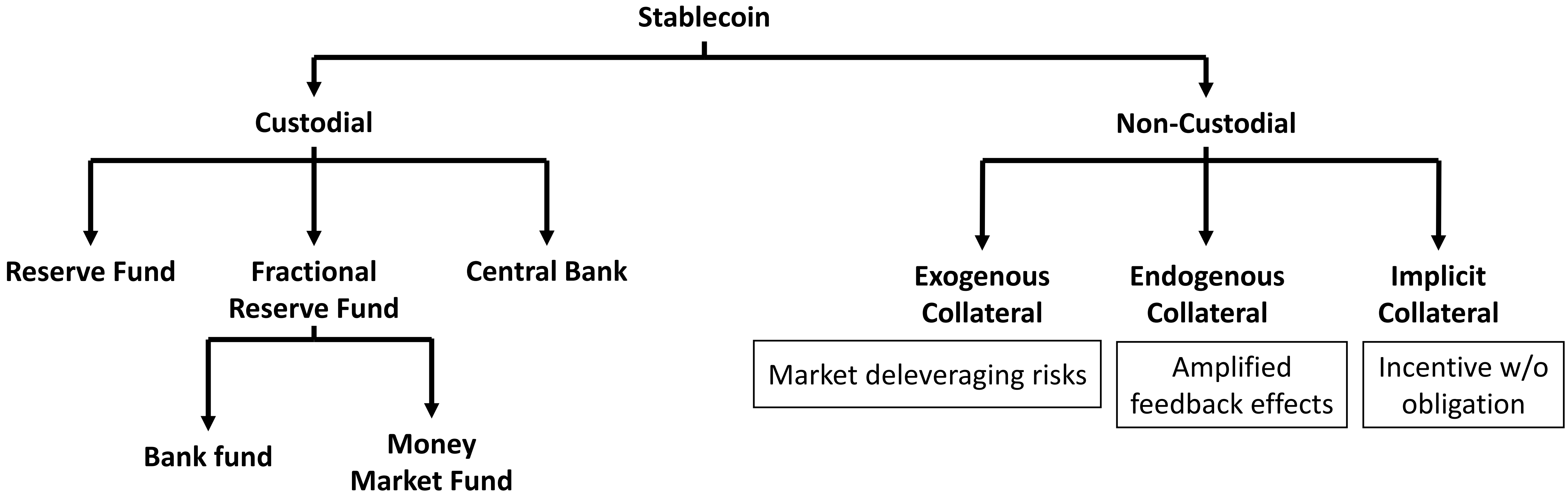
New Risks and attacks
- Deleveraging risks
- Price feeds, governance
- Miner extractable value
- Smart contract bugs

Not well understood

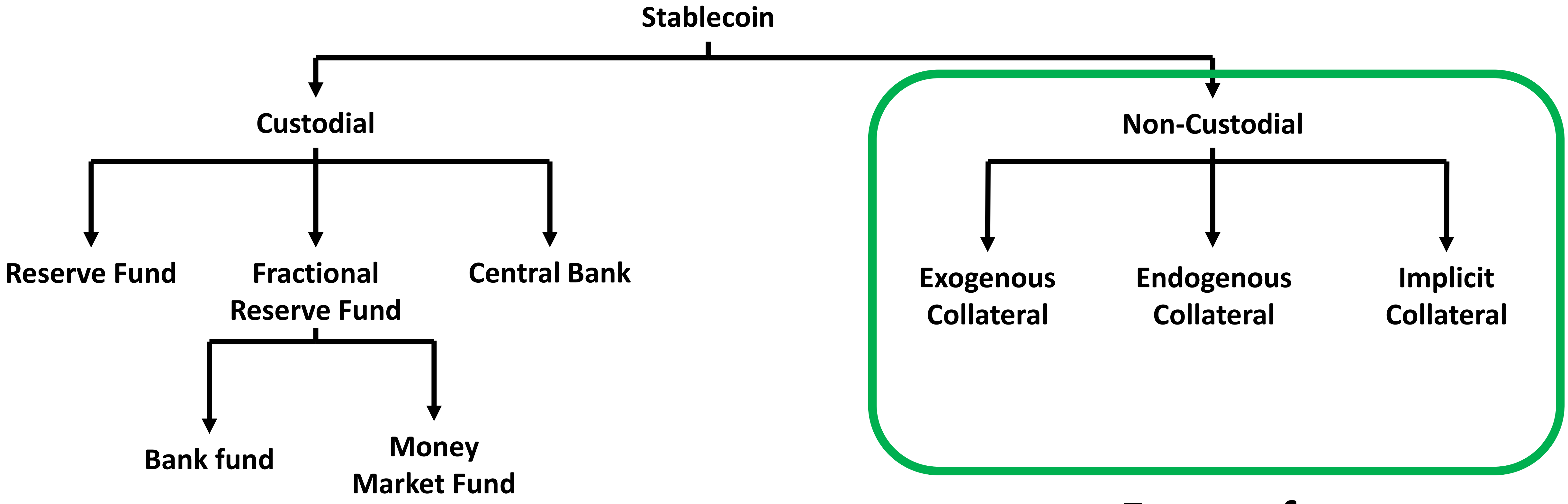
Risk-based Overview



Risk-based Overview



Risk-based Overview



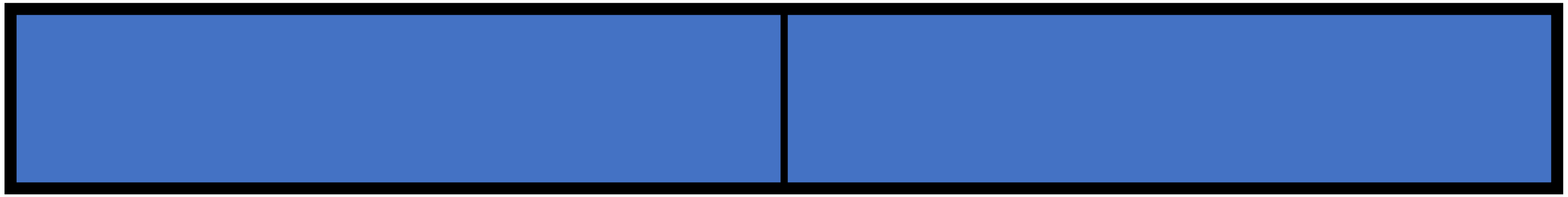
Focus of rest of the talk

CDO Structure

A portfolio of underlying assets

CDO Structure

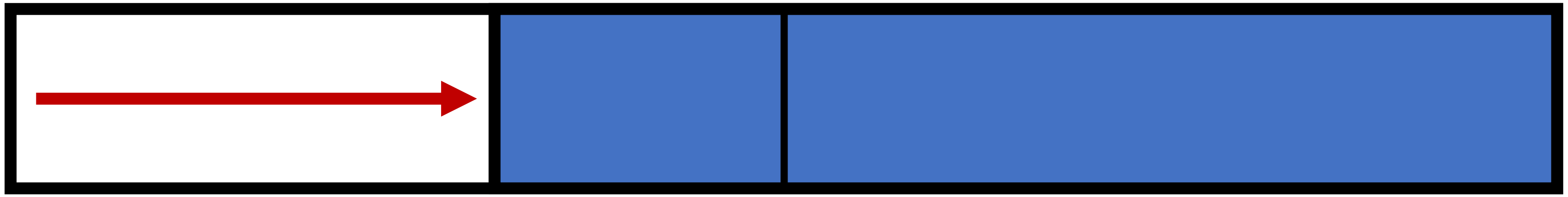
Split into 2 tranches



Junior tranche = more risky **Senior tranche** = less risky

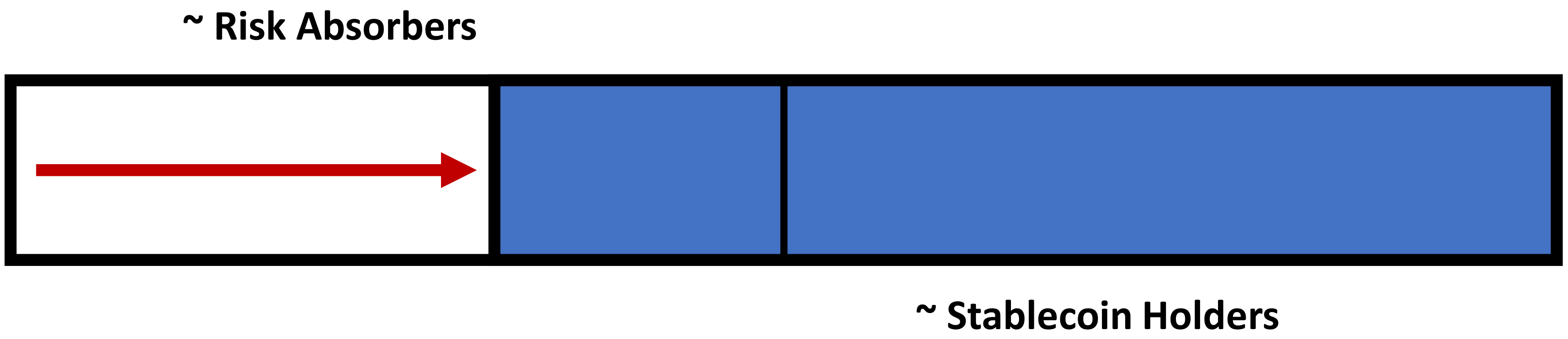
CDO Structure

Losses that occur are first borne by junior tranche

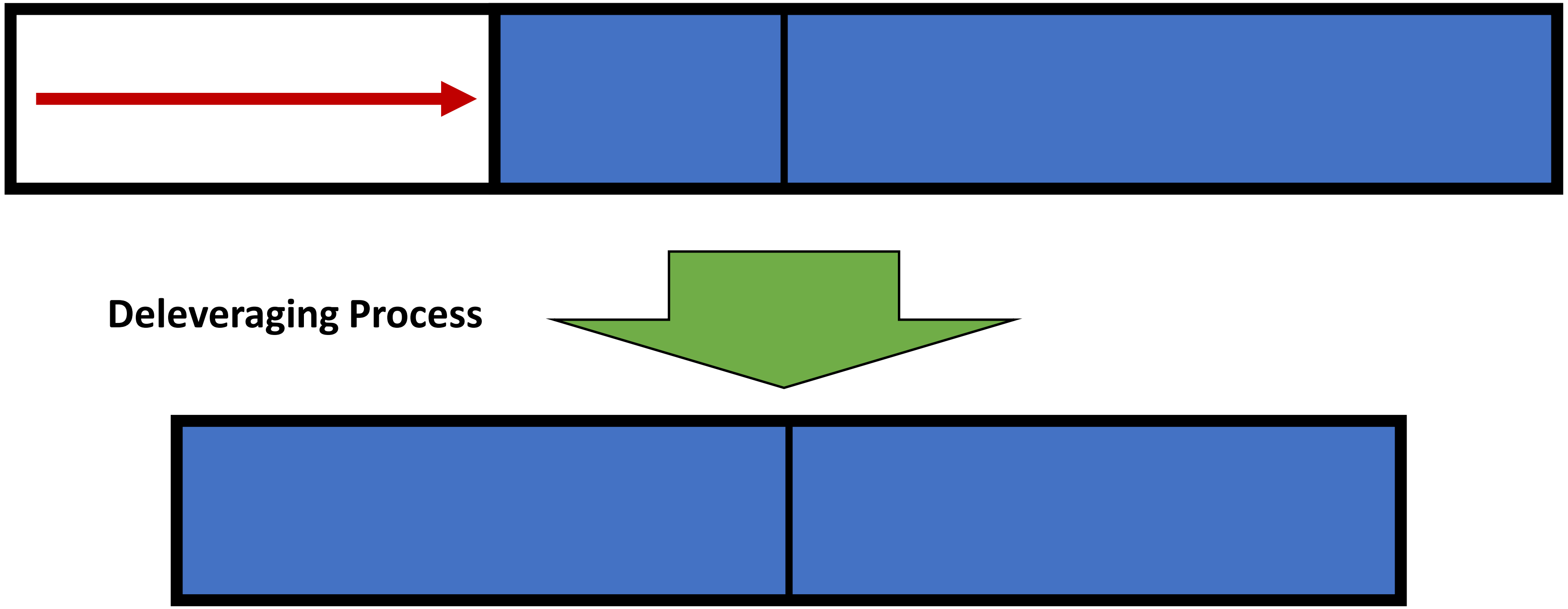


Senior tranche protected

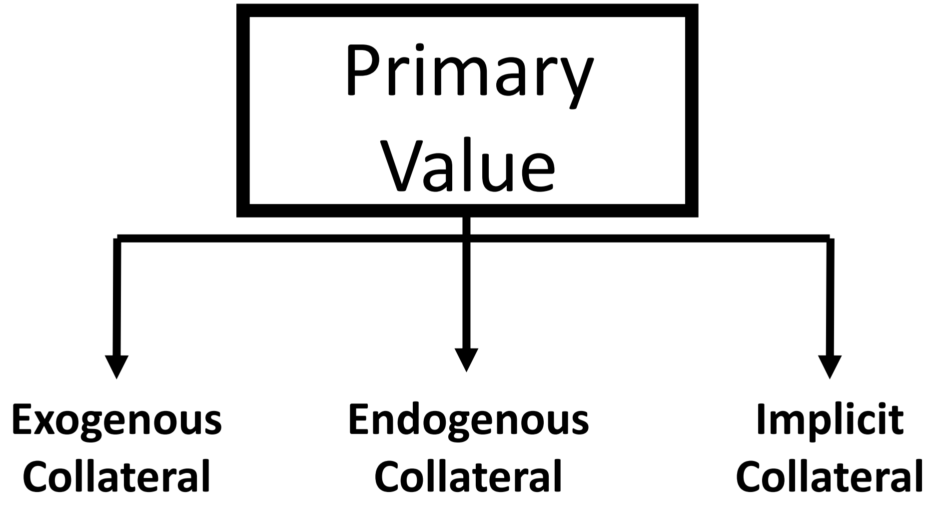
Stablecoin CDO-like Structure



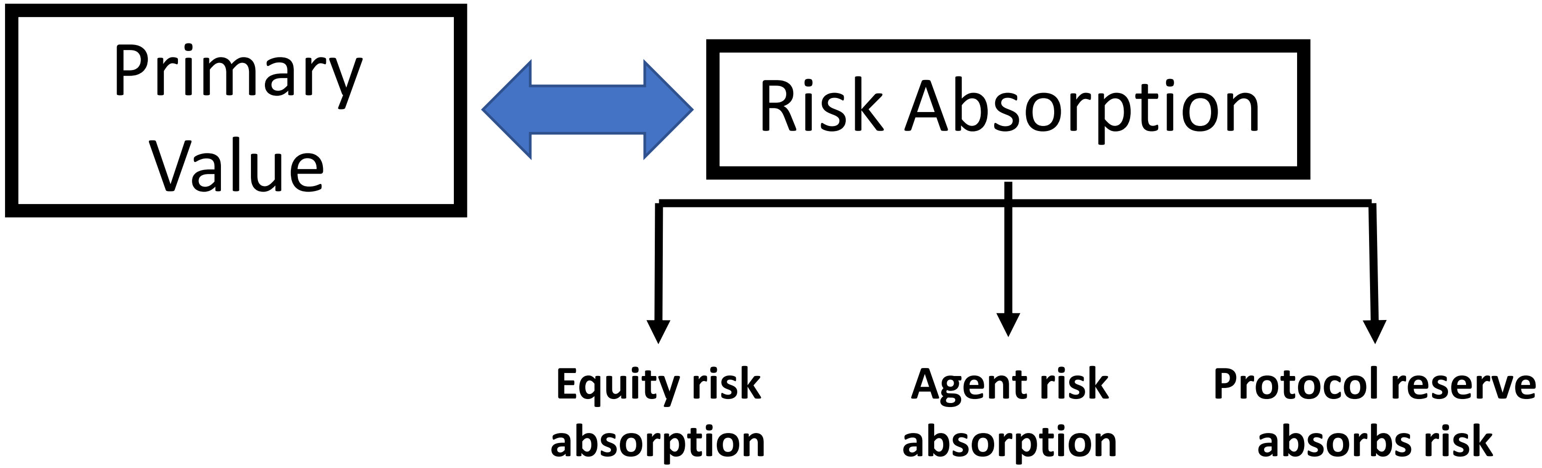
Stablecoin CDO-like Structure



Anatomy of Non-custodial Stablecoins



Anatomy of Non-custodial Stablecoins

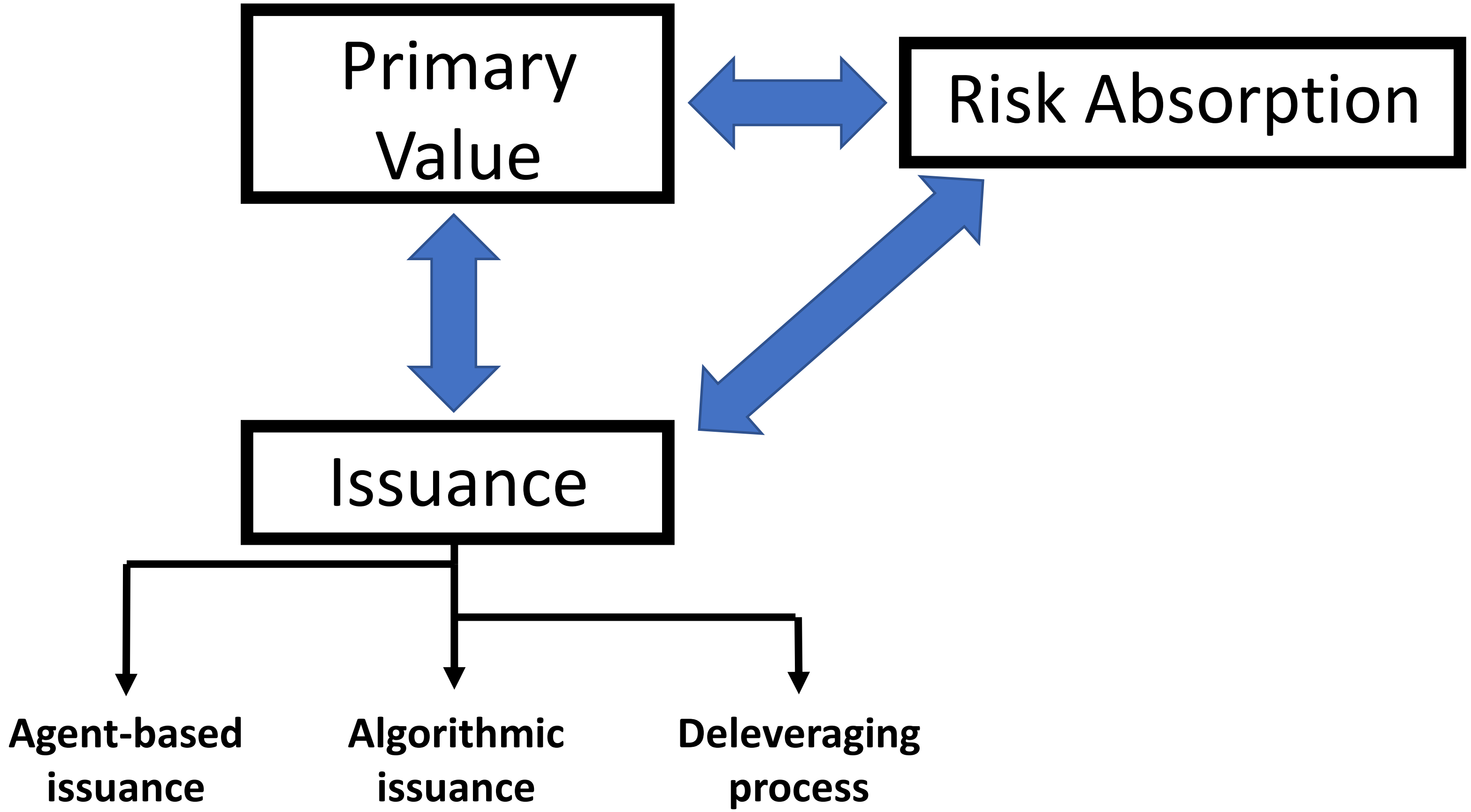


How Risk is Absorbed

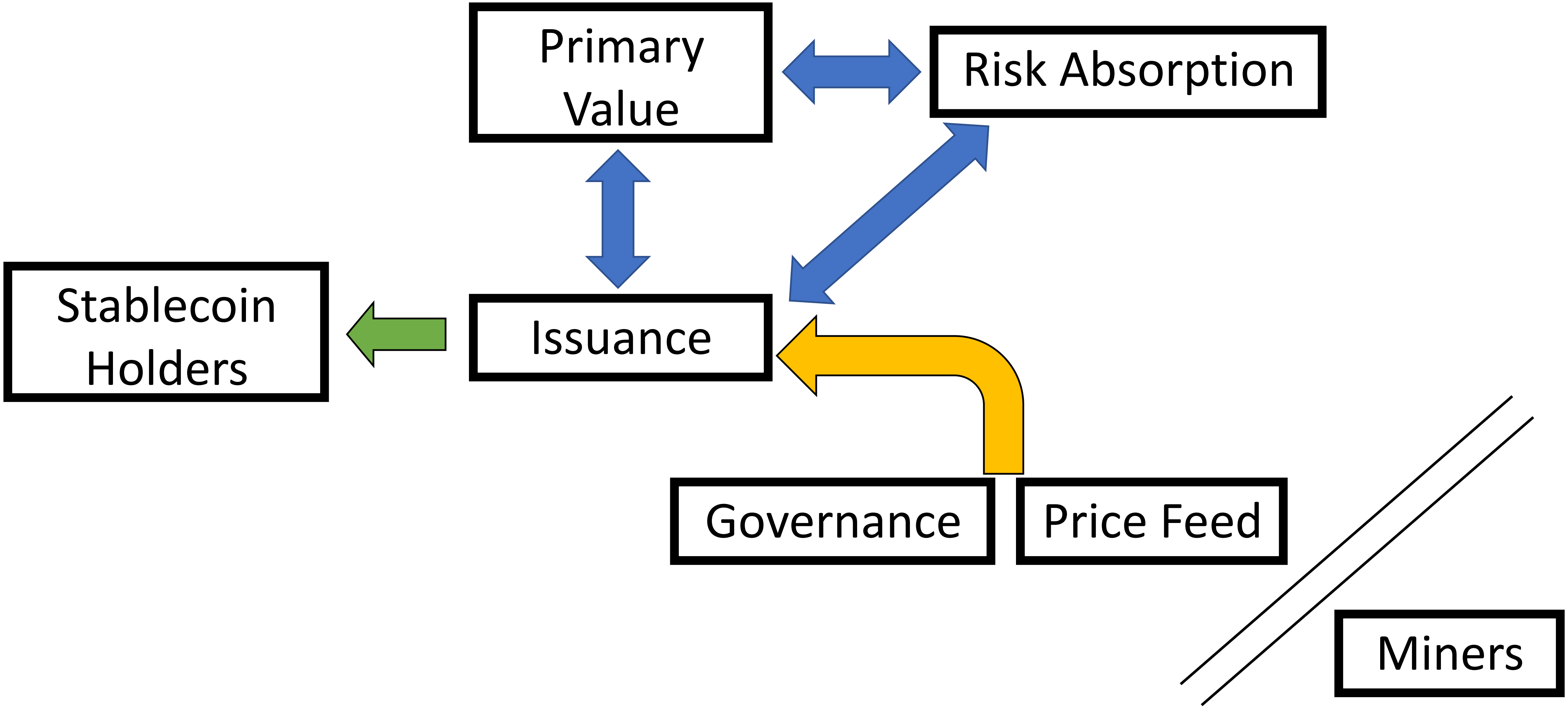
- **Leverage-based:** like the CDO model
  - w/ exogenous or endogenous collateral
  - Seigniorage shares: market cap of endogenous “equity shares” meant to absorb volatility
- **Basis design:** speculators meant to maintain peg by betting on future supply expansions (leverage on “implicit collateral”) 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



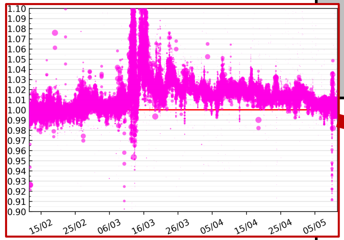
Existing Stablecoins in 3D

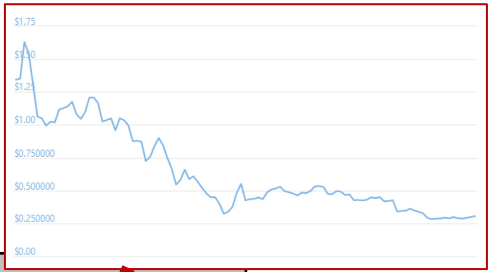
Risk Absorber	Primary Value: Exogenous	<>	Endogenous	Implicit
Agent	Dai, Rai, Liquity		Synthetix, bitUSD	Nubits, Basis Cash, ESD
Equity	Duo Network		Terra, Steem Dollars	
Protocol	Gyroscope, Fei	Frax	Celo Dollars	

Issuance

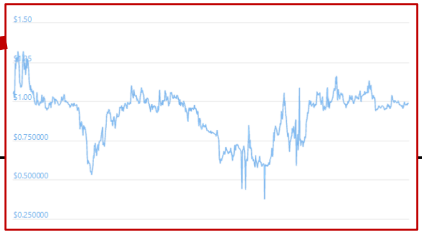
Agent
Algorithmic

Existing Stablecoins in 3D





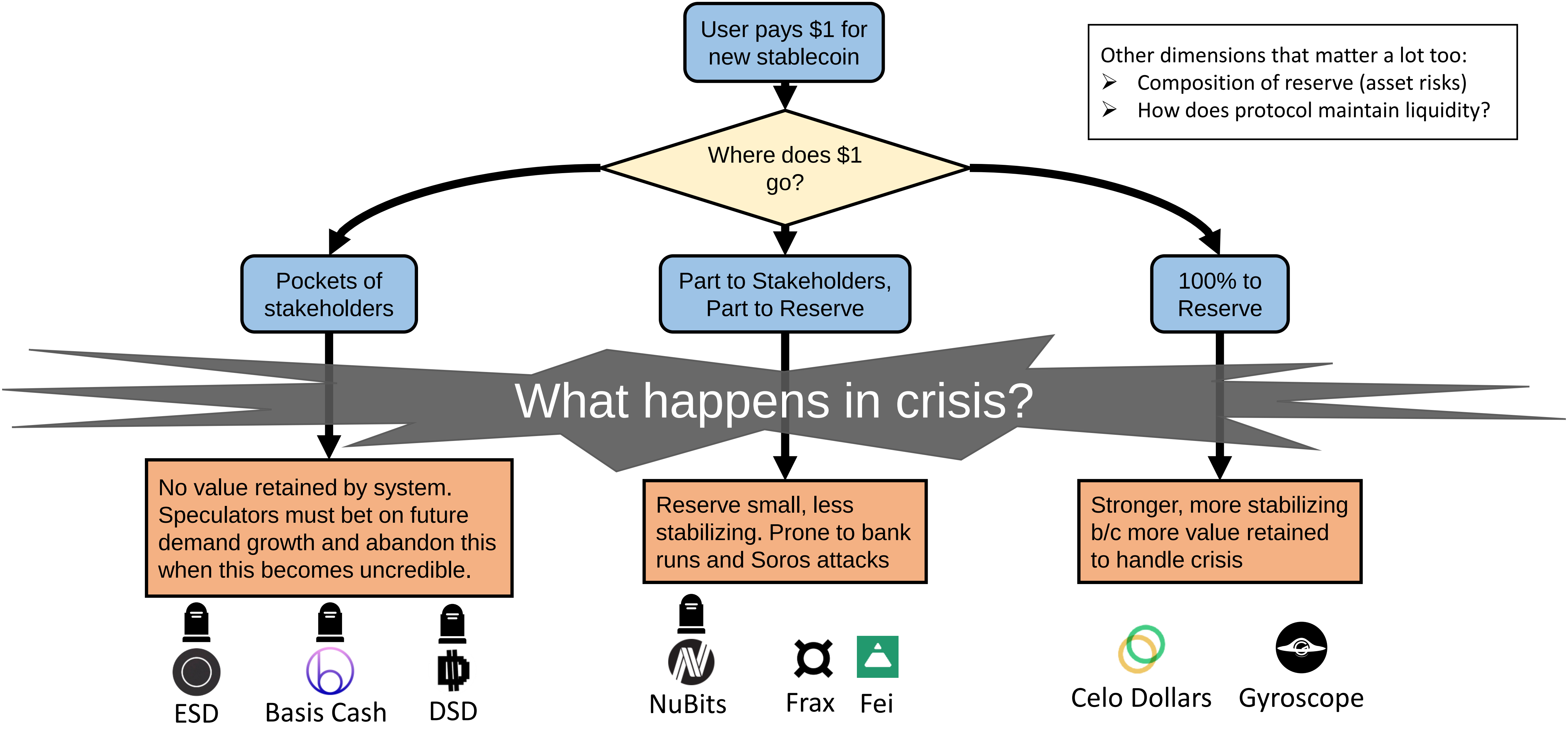

Risk Absorber	Primary Value: Exogenous	Primary Value: <>	Primary Value: Endogenous	Primary Value: Implicit
Agent	Dai, Rai, Liquity		Synthetix, bitUSD	Nubits, Basis Cash, ESD
Equity	Duo Network		Terra, Steem Dollars	
Protocol	Gyroscope, Fei	Frax	Celo Dollars	




Issuance

Issuance
Agent
Algorithmic

Contrasting Algorithmic Stablecoins



Parallels & Differences

Requires new models

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

----Fundamental Design Questions----

Question 1 (Incentive Security)

Is there mutually profitable continued participation across all required parties?

- Governance Extractable Value (GEV)
- Miner Extractable Value (MEV)

Question 2 (Economic Stability)

Do the incentives actually lead to stable outcomes?

----New Models----

Price Dynamic Models

Model how issuance incentives lead to (in)stability

GEV: Capital Structure Models

1-period incentives, participation, attacks

MEV: Forking Models

Multi-period incentives, participation, attacks

Price Dynamic Models

- **Financial literature:** an asset that is assumed stable is borrowed against collateral, feedback effects on collateral asset liquidity
- **Non-custodial stablecoins:** 'stable' asset also has endogenous price, participation

- 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 of Leveraged-Based Stablecoins

Agents

- **Stablecoin Holders** want stability, have imperfectly elastic demand
- **Speculator** decides supply of stablecoins secured by its collateral position

Assets

- **ETH:** risky asset with exogenous price
- **STBL** stablecoin with endogenous price over-collateralized in ETH

Stablecoin market clears by setting demand = supply in USD (target) terms

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 subject to constraints (‘honest’ behavior)

$$\max_{\Delta_t} \quad \mathbb{E}[Y_{t+1}|\mathcal{F}_t]$$
$$\text{s.t.} \quad \bar{N}_t X_t \geq \beta L_t$$

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

Some assumptions to make model tractable for analytical results

Regions of Stability

Result 1: Bounded probability of large deviations in certain region

Technical idea: Doob's inequality

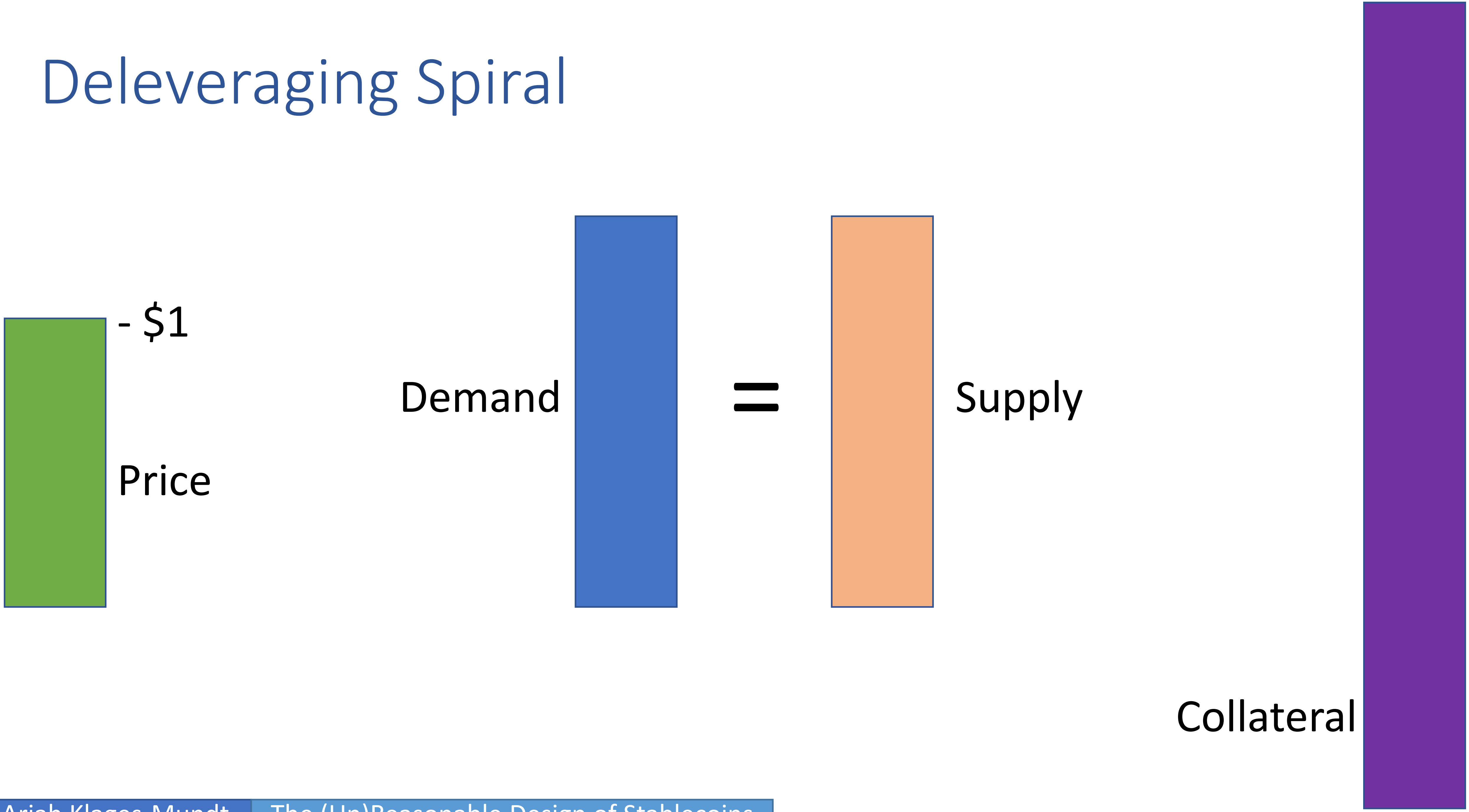
Result 2: Bounded probability of large quadratic variation (QV) in certain regime

Technical idea: Burkholder's inequality

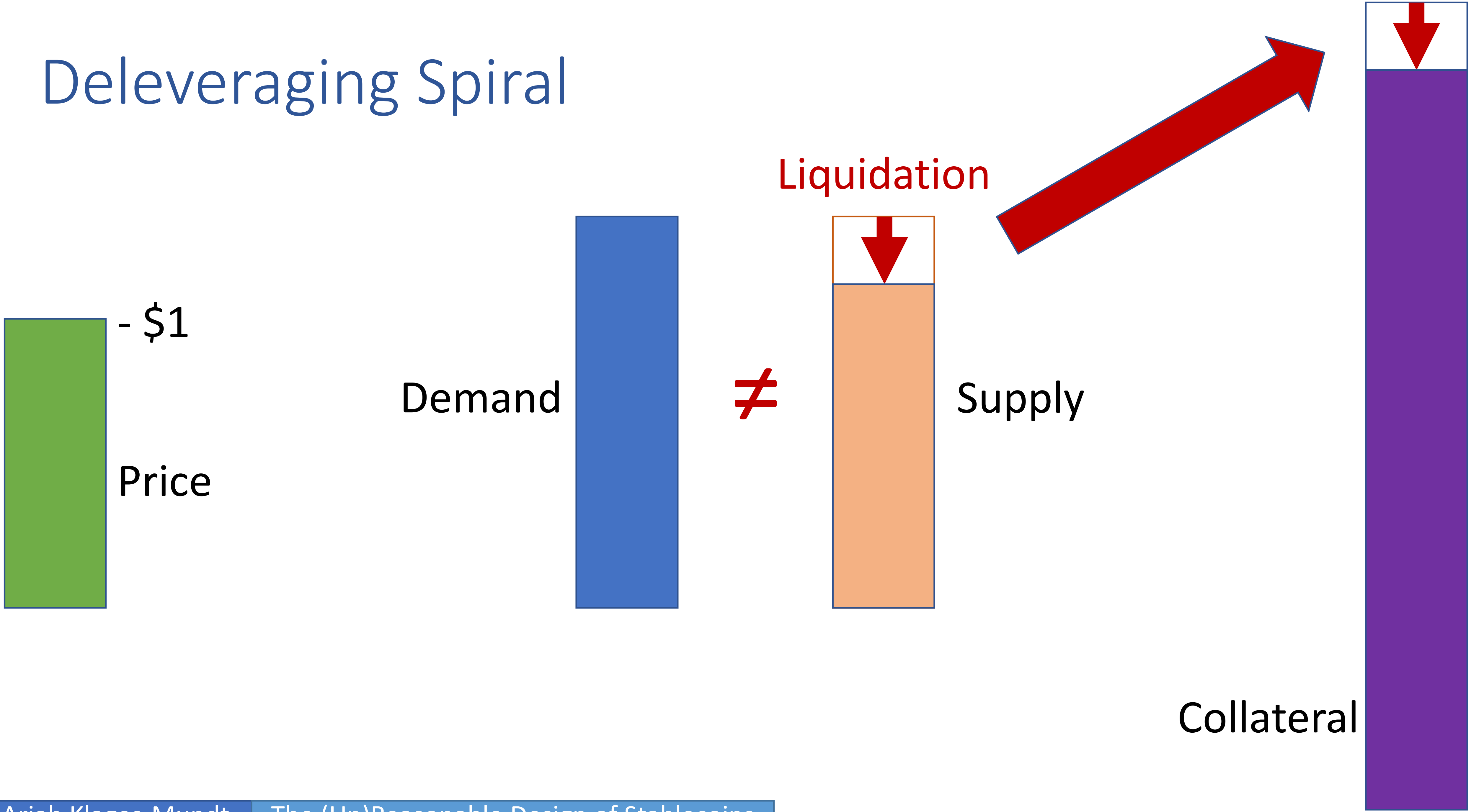
Regions of Instability

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

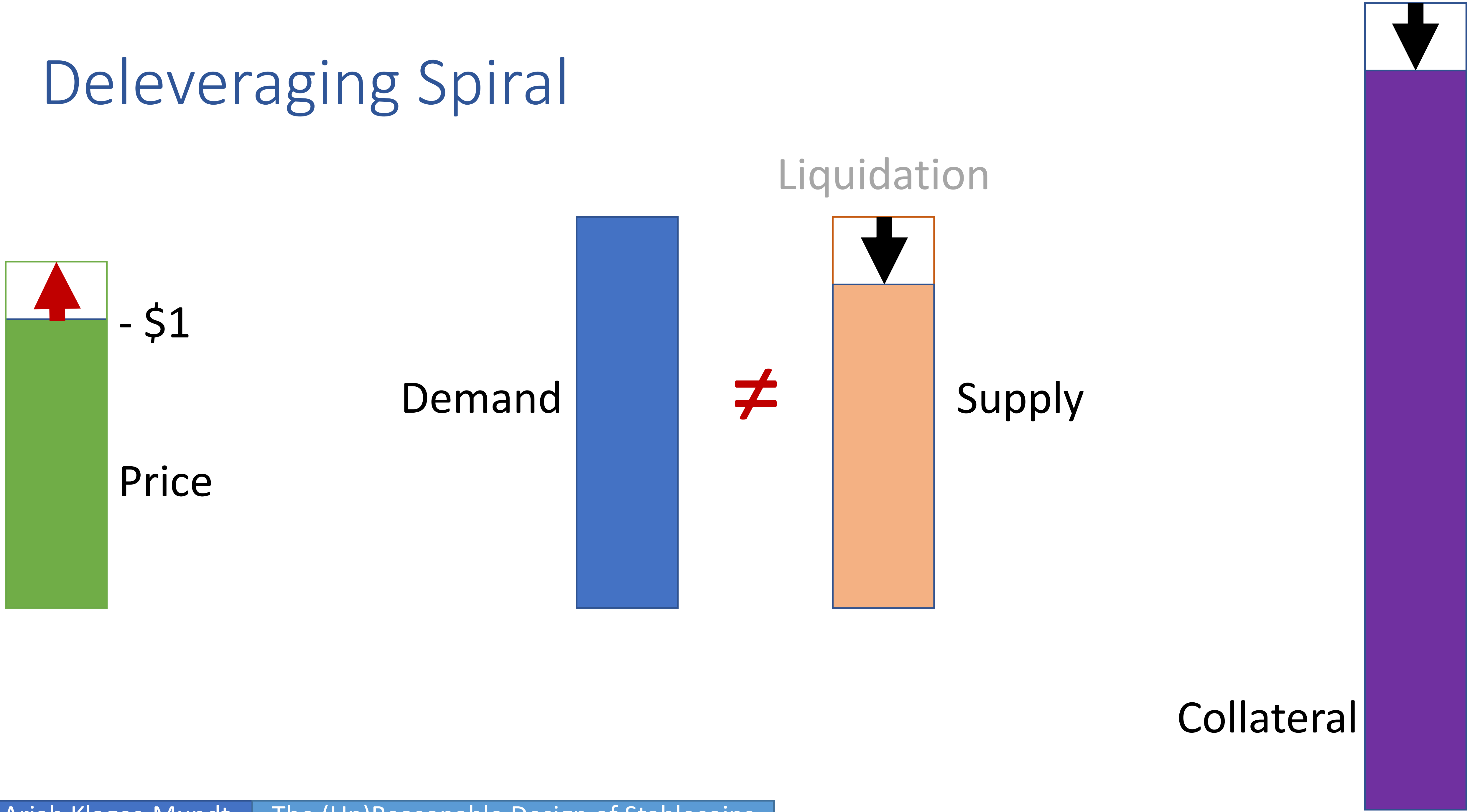
Deleveraging Spiral



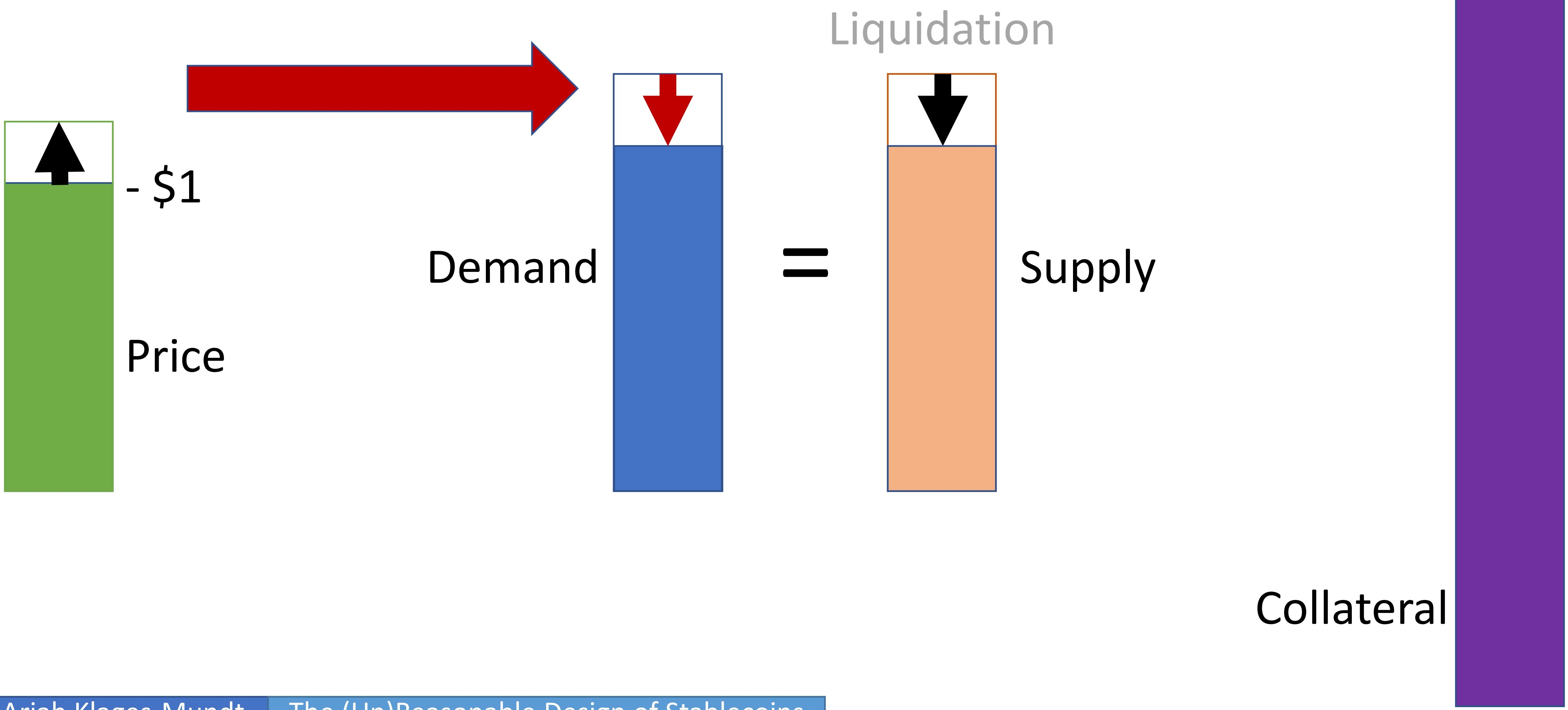
Deleveraging Spiral



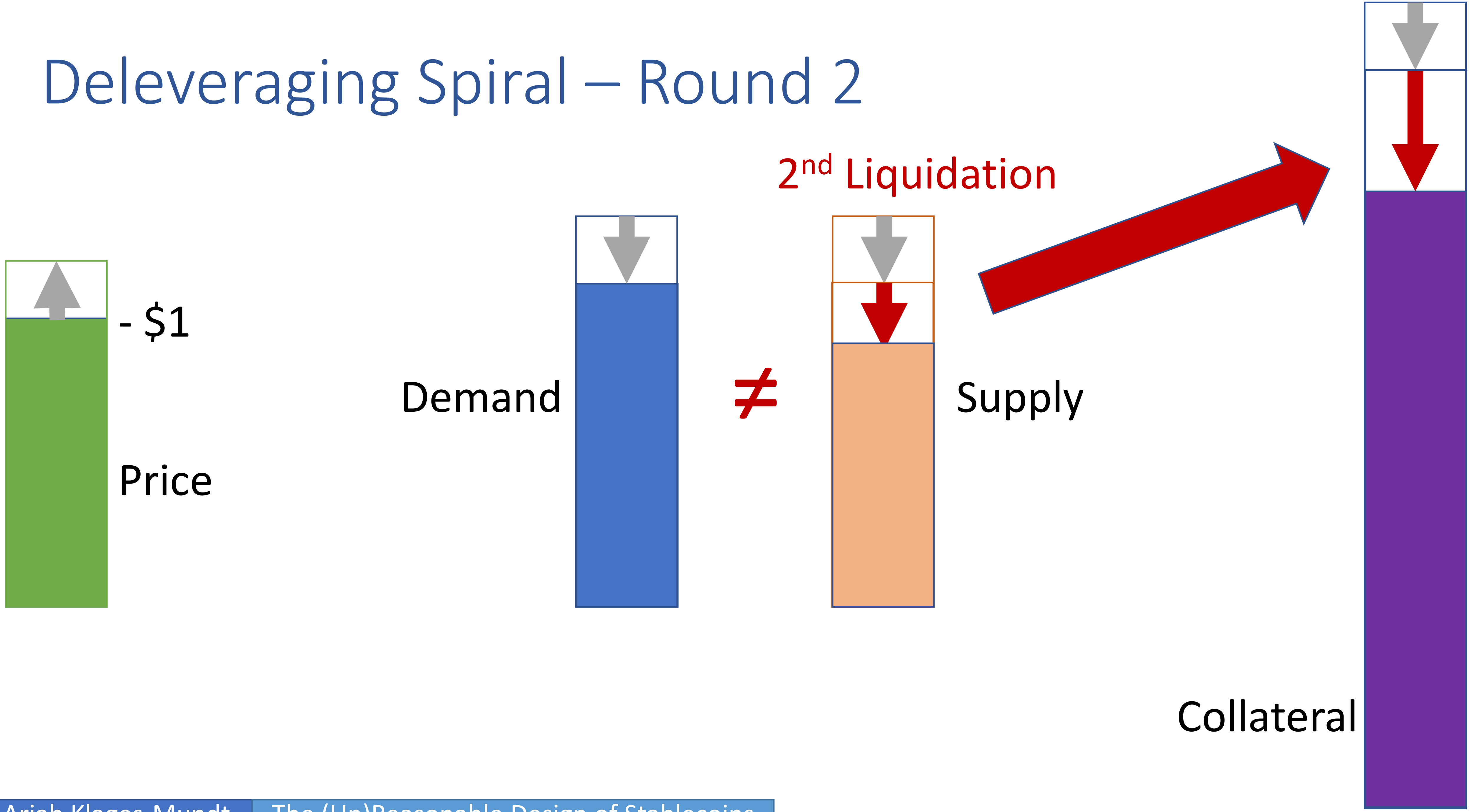
Deleveraging Spiral



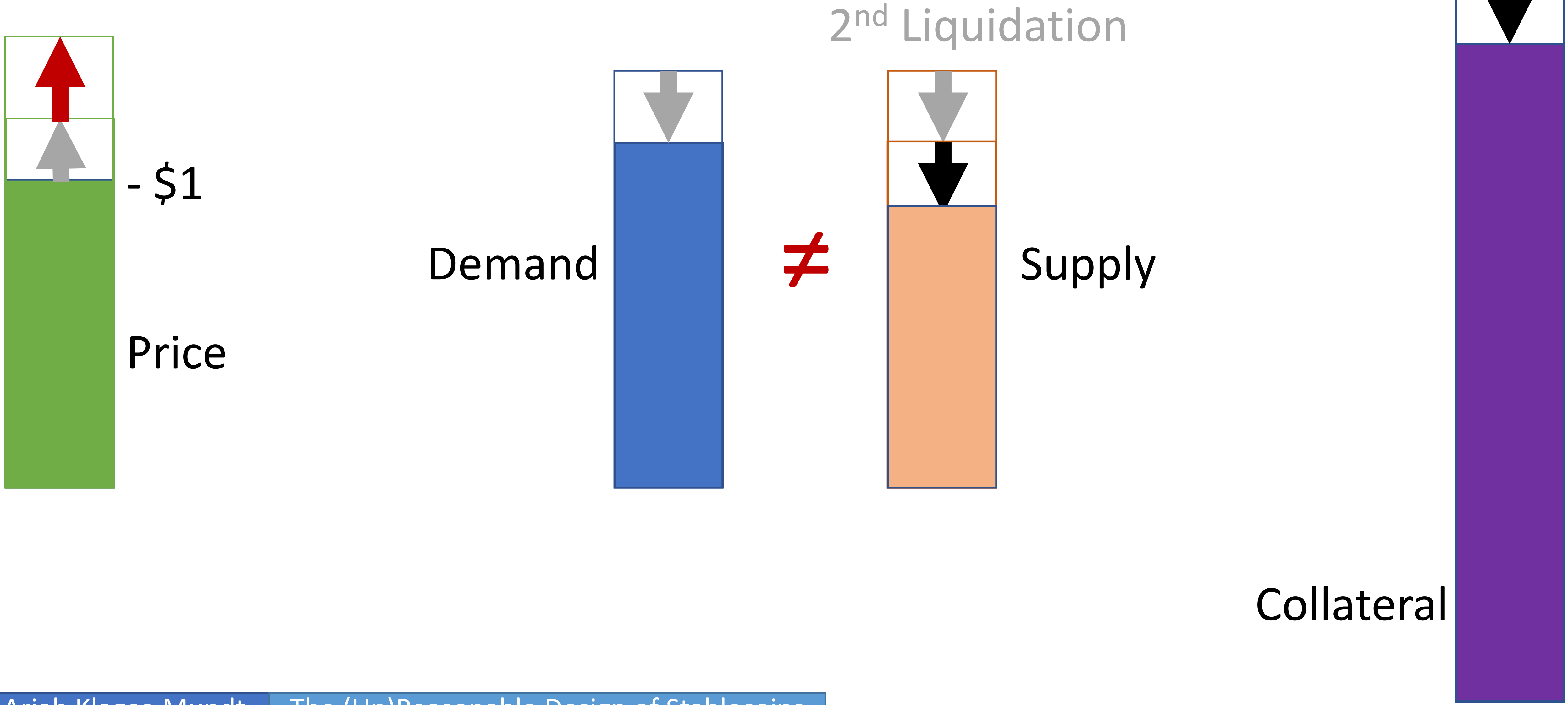
Deleveraging Spiral



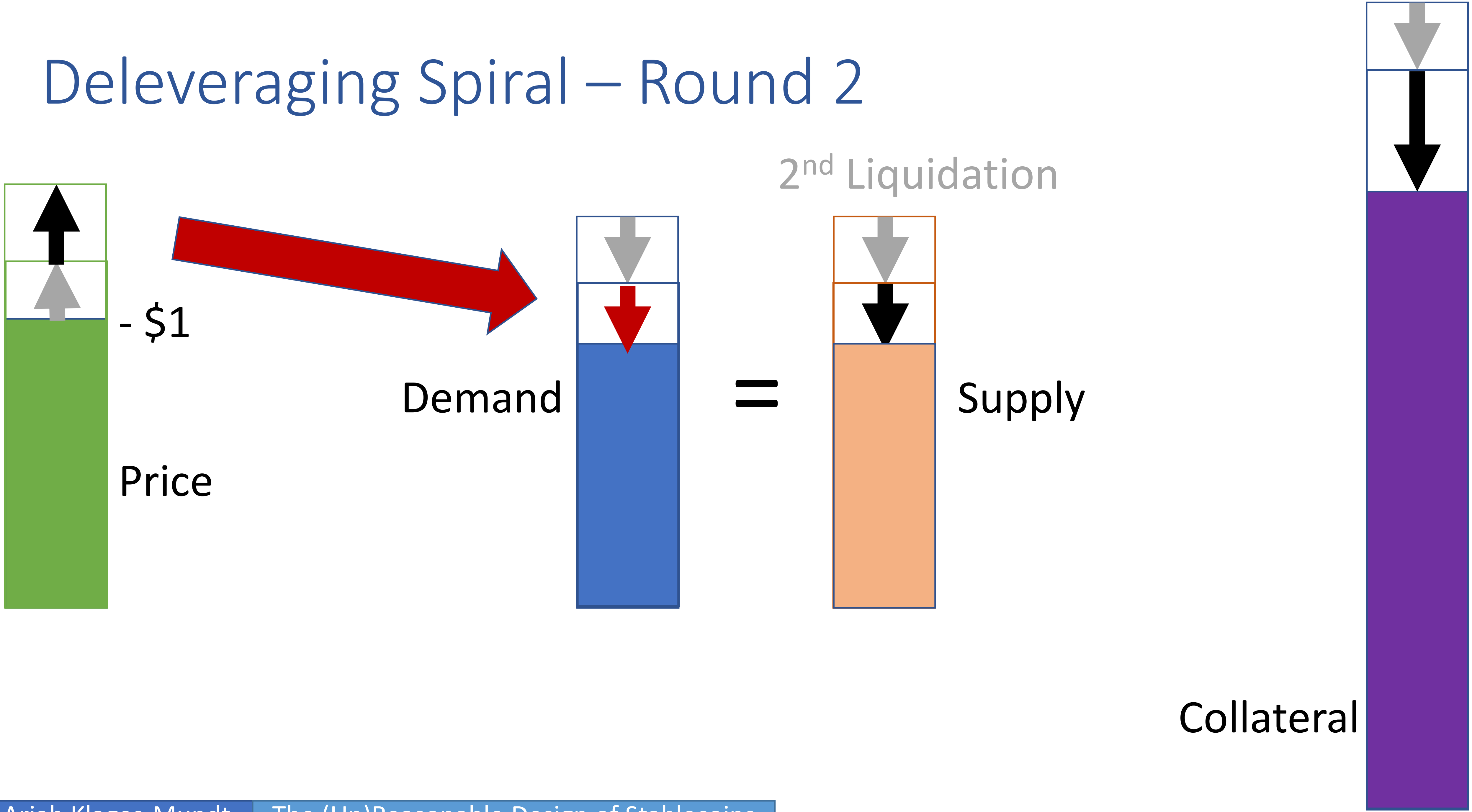
Deleveraging Spiral – Round 2



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

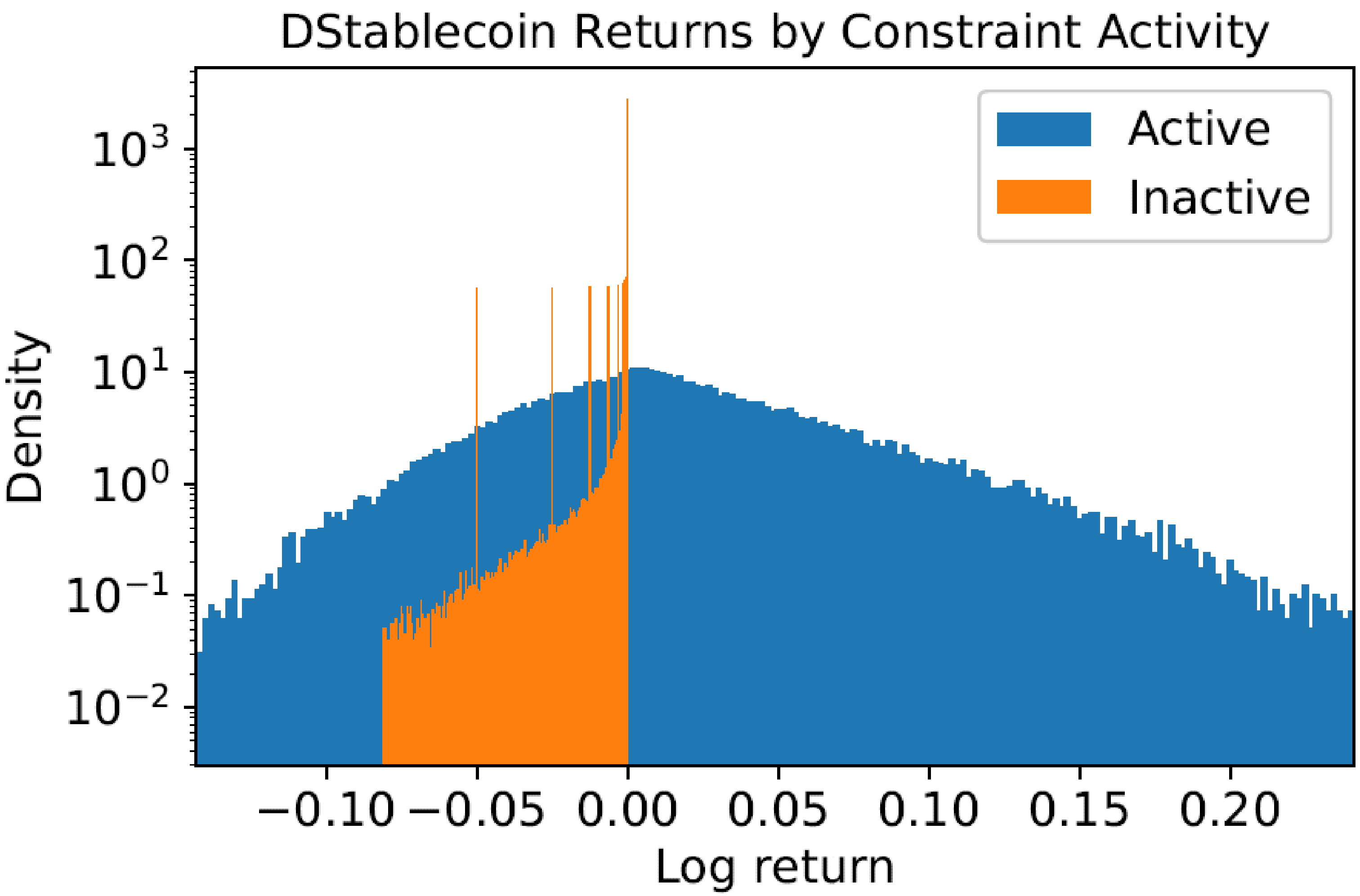
Technical idea: Implicit Function Theorem

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

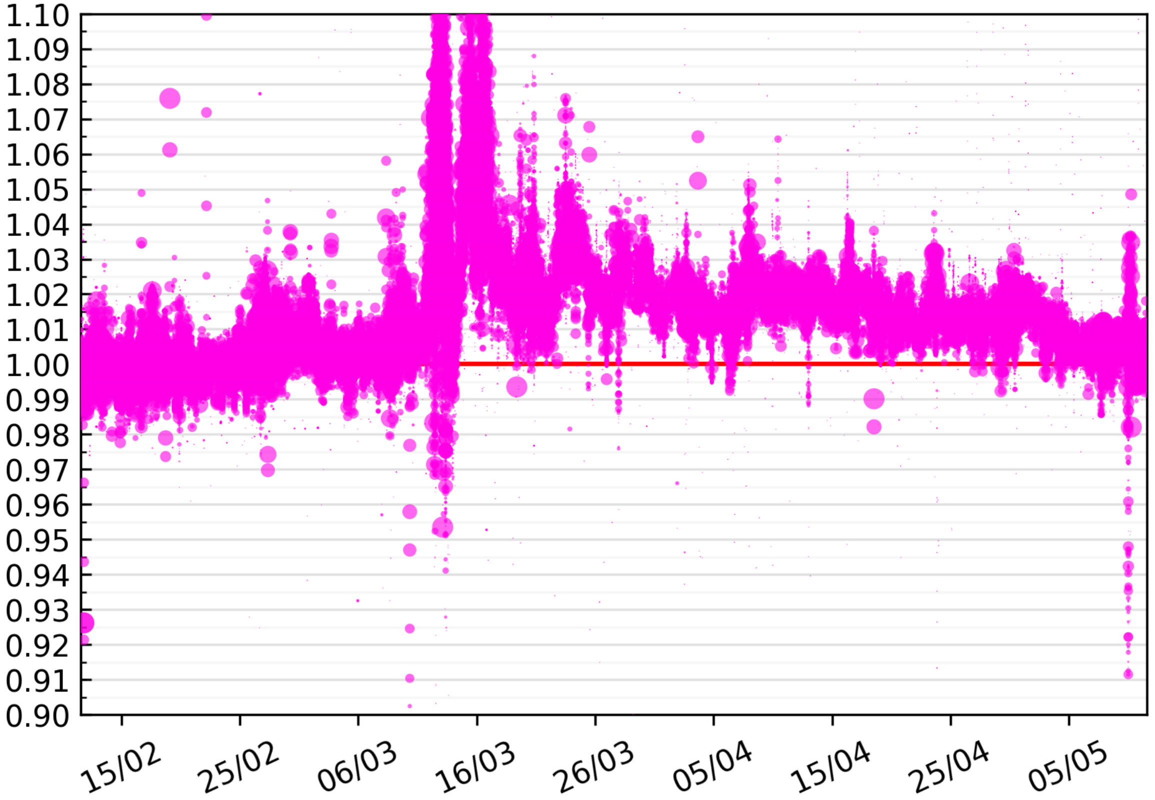
Simulations: ‘Stable’ & ‘Unstable’ Regions



*Using a simpler agent-based model from a different paper

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

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 buffers:** Dedicated liquidity pools for crises
- **Reserve-backed mechanism:** generalization of Maker PSM

Question 1 (Incentive Security)

Is there mutually profitable continued participation across all required parties?

- Governance Extractable Value (GEV)
- Miner Extractable Value (MEV)

Question 2 (Economic Stability)

Do the incentives actually lead to stable outcomes?

Developer Flags Big-Money Loophole for Stealing All the ETH in MakerDAO

Dec 9, 2019 at 15:05 UTC • Updated Dec 9, 2019 at 15:29 UTC

$10.8M Stolen, Developers Implicated in Alleged Smart Contract 'Rug Pull'

----New Models----

Price Dynamic Models

Model how issuance incentives lead to (in)stability

GEV: Capital Structure Models

1-period incentives, participation, attacks

MEV: Forking Models

Multi-period incentives, participation, attacks

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

Governance choice

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

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

F is vault choice

Vault choice

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

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

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

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

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

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

- 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

$$
\begin{aligned}
\max_{\delta \in [0,1), d_{\{n,v,s\}} \in \{0,1\}} \quad & \mathbb{E}\Big[d_n \varepsilon(\delta F + P_1) + d_v\big(\gamma_v(F - \mathbf{x}_G) - \alpha\big) \\
& \quad + d_s\big(\gamma_s(N - \mathbf{y}_G) - \alpha\big) \Big] \\
\text{s.t.} \quad & P_1 = P(\mathbf{x}_G, \mathbf{y}_G, \delta, F) \\
& \mathbb{1}_{(\frac{\mathbf{x}_G}{P_1} \geq \zeta)} \leq d_v \leq \mathbb{1}_{(\varepsilon + \frac{\mathbf{x}_G}{P_1} \geq \zeta)} \\
& \mathbb{1}_{(\frac{\mathbf{y}_G}{P_1} \geq \zeta)} \leq d_s \leq \mathbb{1}_{(\varepsilon + \frac{\mathbf{y}_G}{P_1} \geq \zeta)} \\
& d_n = (1 - d_v)(1 - d_s) \text{ and } d_v = (1 - d_n)(1 - d_s) \\
& \mathbf{x}, \mathbf{y}, N, F, \gamma_v, \gamma_s \text{ from vault and stablecoin holder choices}
\end{aligned}
$$

Vault choice

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

Stablecoin holder choice

$$
\begin{aligned}
\max_{\mathbf{y}, \gamma_s \in [0,1)} \quad & \mathbb{E}\Big[U\Big(\mathbf{y}_C R + d_n\Big(\min\Big(\frac{\mathbf{y}_S}{B}, N(1+R) - \delta F\Big) + \frac{\mathbf{y}_G}{P_1}(\delta F + P_1)\Big) \\
& \quad + d_s(1 - \gamma_s)(N - \mathbf{y}_G)\Big)\Big] \\
\text{s.t.} \quad & \mathbb{1}^T \mathbf{y} = \bar{y} \\
& B = B(F, \mathbf{y}_S) \\
& P_1 = P(\mathbf{x}_G, \mathbf{y}_G, \delta, F) \\
& \delta, d, \mathbf{x}, N, F \text{ from outside governor and vault choices}
\end{aligned}
$$

- 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 <u>and whether to collude with another agent to attack</u>

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

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

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

----New Models----

Price Dynamic Models

Model how issuance incentives lead to (in)stability

GEV: Capital Structure Models

1-period incentives, participation, attacks

MEV: Forking Models

Multi-period incentives, participation, attacks

Economic Attacks

Attacking a stablecoin is different than a traditional currency attack

- Focus **not** on breaking willingness of central bank to maintain peg
- Instead, involves manipulating interaction of agents

Attack primitives:

- Deleveraging spirals $\Rightarrow$ arbitrage-like trades around liquidations
- Liquidations are automated with arbitrage opportunities
- Miners can censor and reorder transactions to extract profit

Economic Attacks

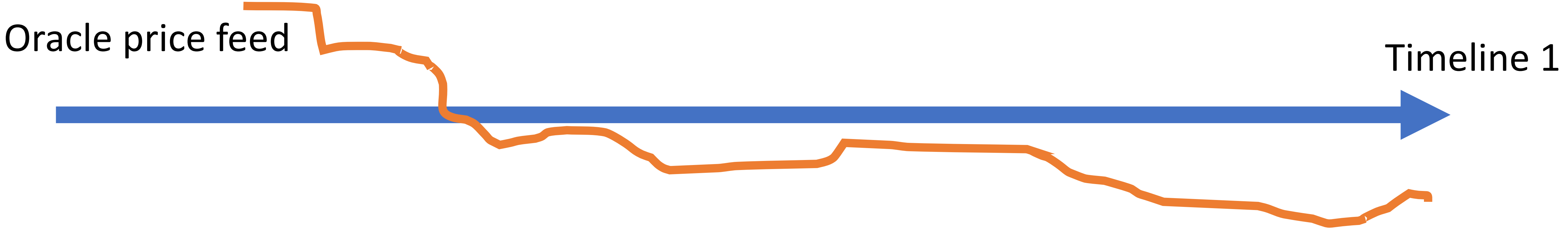
Attack 1: In ETH decline, attacker manipulates market to trigger, profit from liquidations

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

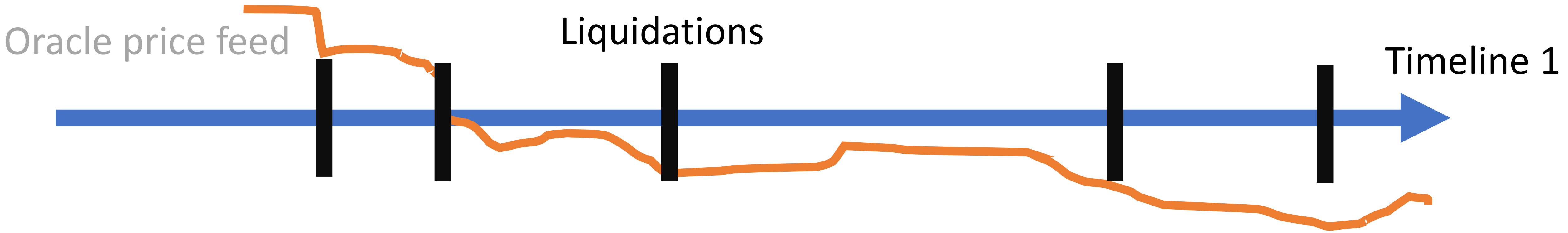
Attack 2: After ETH decline, reorg blockchain to trigger, profit from spiraling liquidations

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

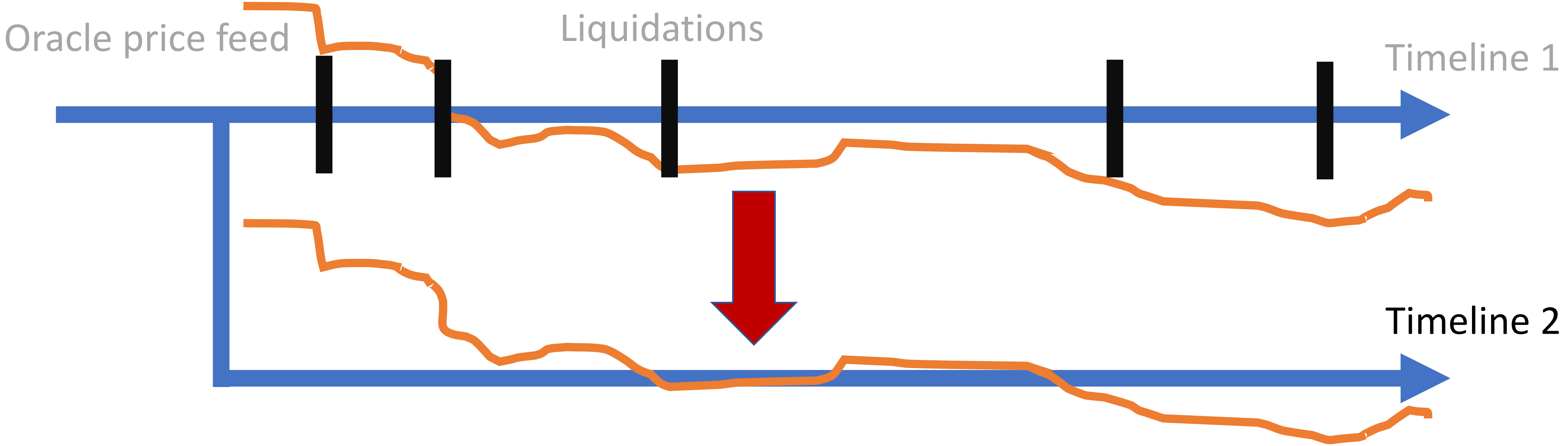
Economic Attacks



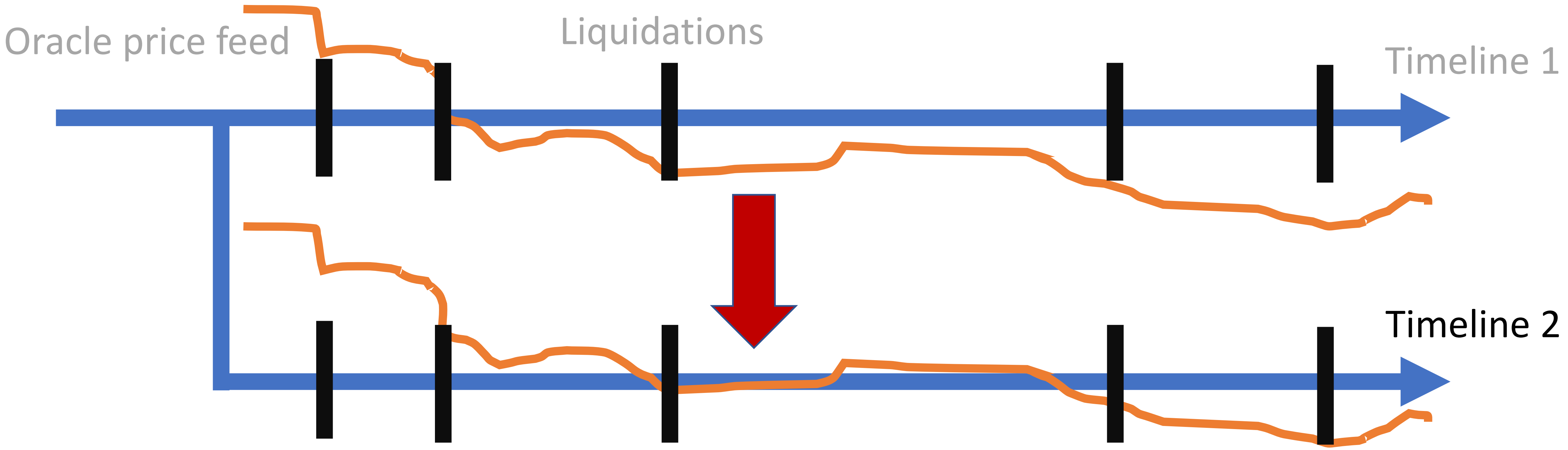
Economic Attacks



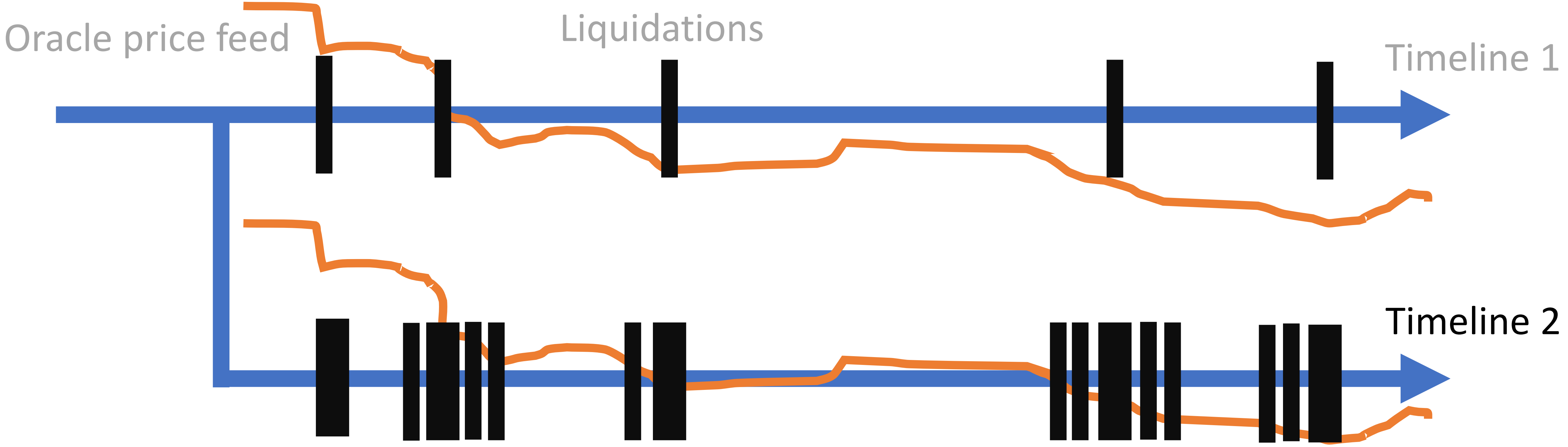
Economic Attacks



Economic Attacks



Economic Attacks



Black Thursday (again) 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

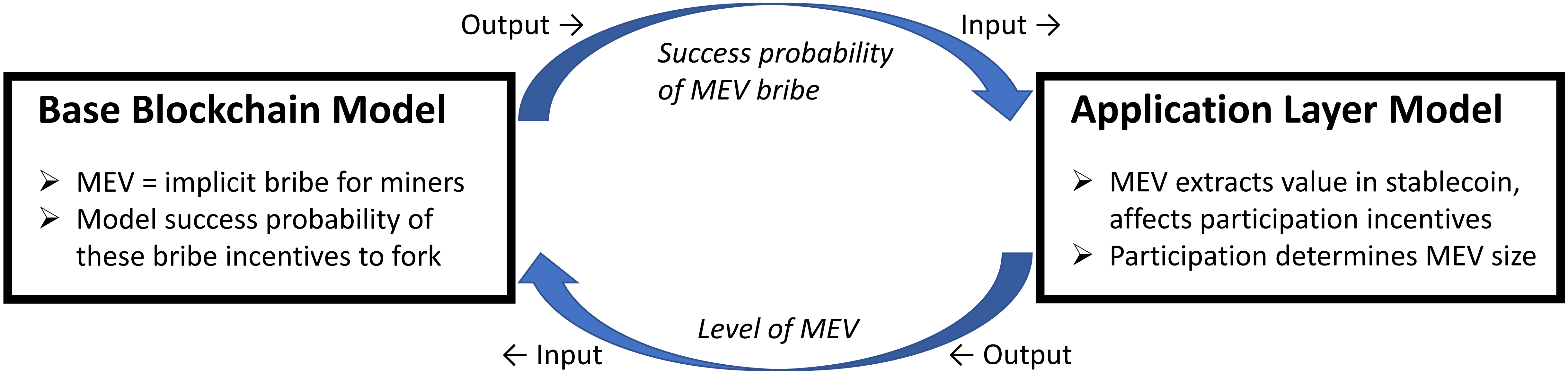
- Blockchain forensic investigation: this was the result of mempool manipulation => clearing of liquidation auctions at ~$0 prices

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



The End: Papers available on arXiv

We seed stablecoin design questions and models

Main take-aways

1. Primary non-custodial stablecoins are leverage-based
   - ➢ Need mechanisms to combat deleveraging spirals
2. Amplified risks in endogenous and implicit collateral stablecoins
3. GEV and MEV models critical to incentive security

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