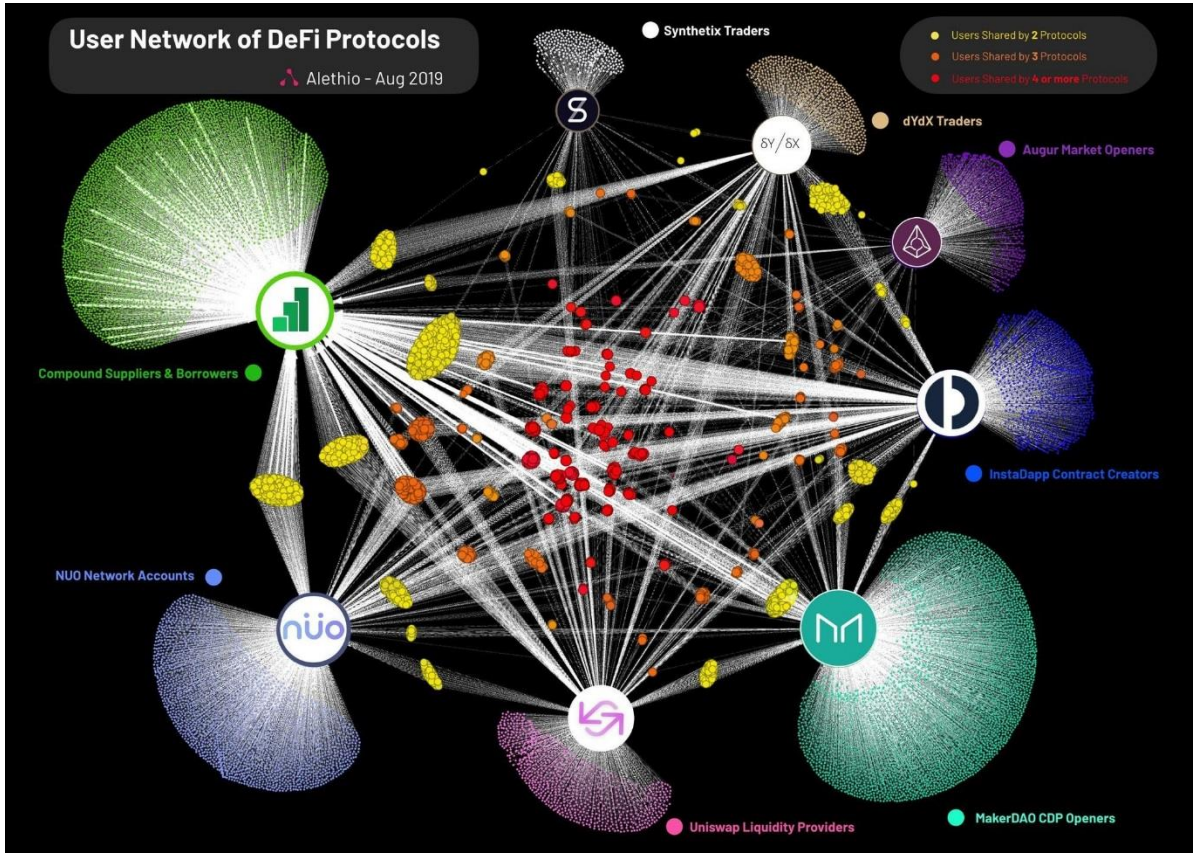
(In)Stability for the Blockchain:
Deleveraging Spirals and Stablecoin Attacks

Ariah Klages-Mundt

Cornell University

Devcon 5

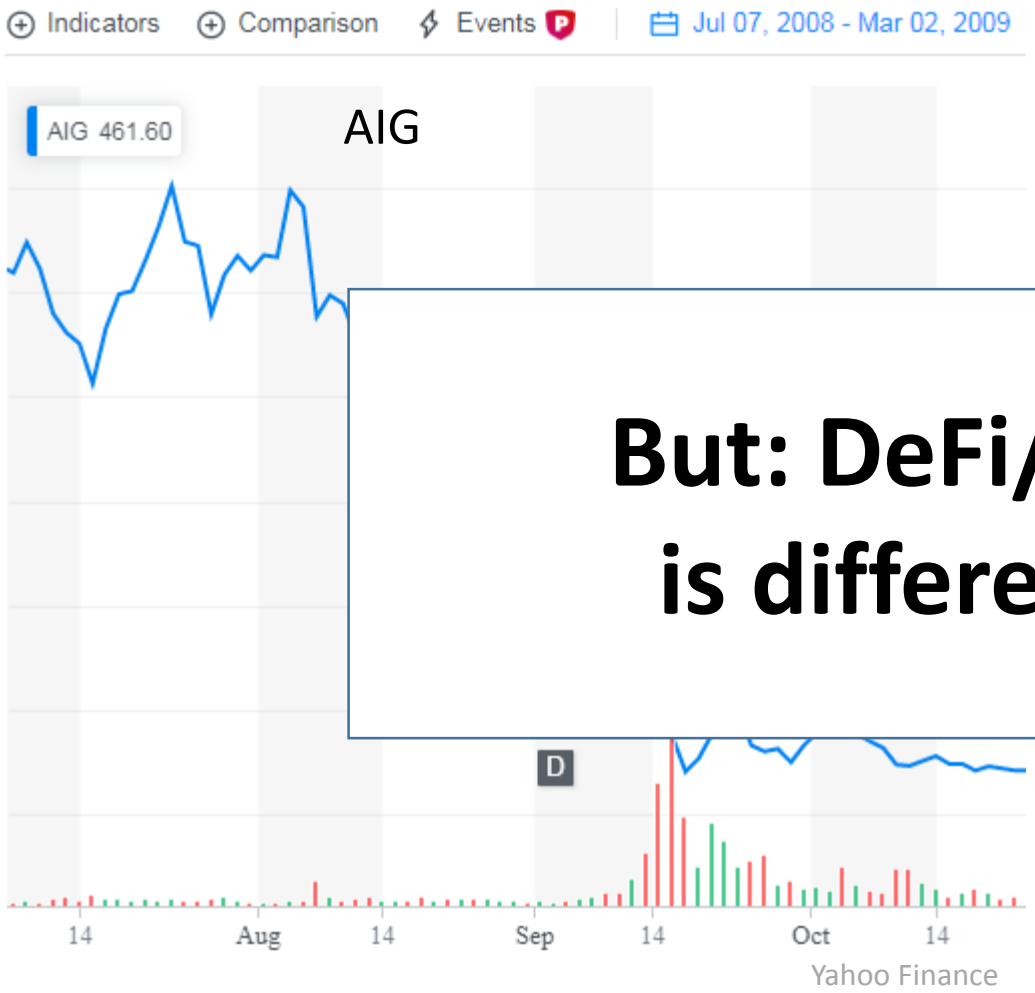
DeFi: Growing & Increasingly Complex



Complex Systems have Complex Risks

Yahoo Finance

Complex Systems have Complex Risks



But: DeFi/blockchain is different, right?!

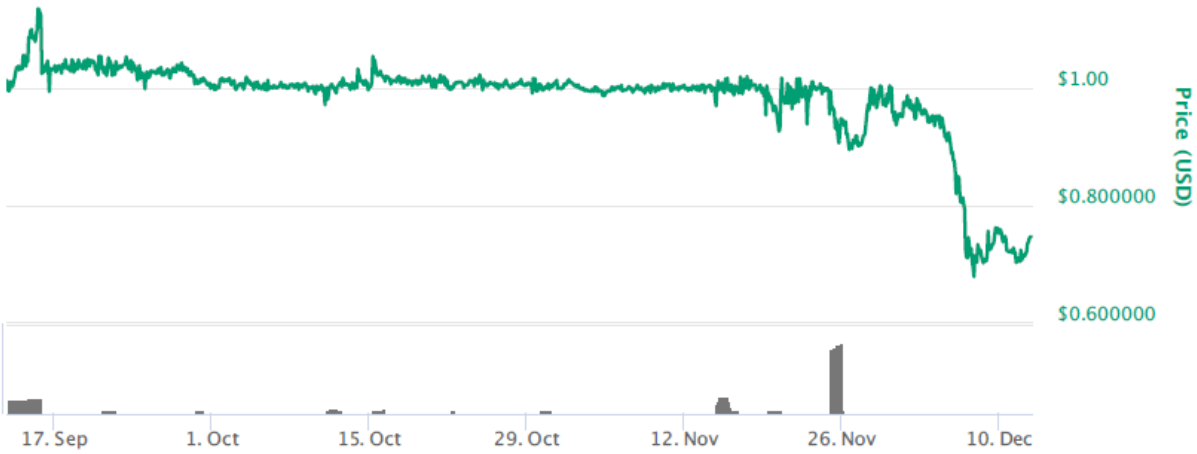
NuBits

coinmarketcap

NuBits

coinmarketcap

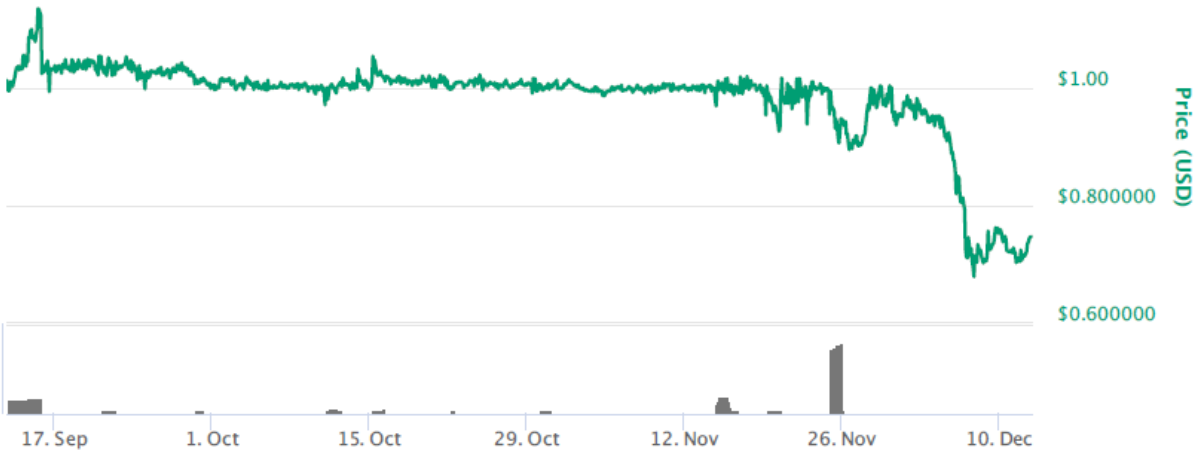
bitUSD



NuBits

coinmarketcap

bitUSD

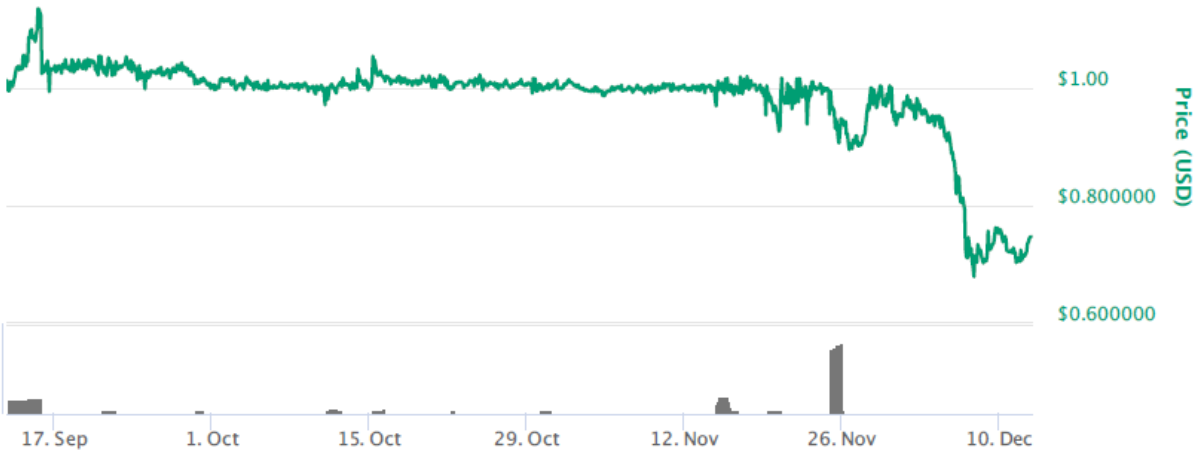


Steem Dollars

NuBits

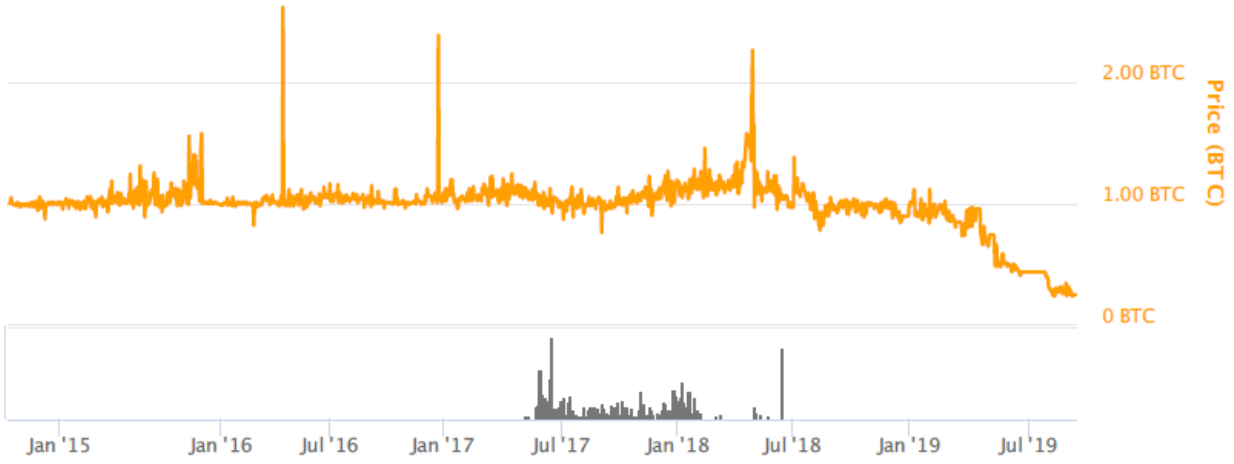
coinmarketcap

bitUSD



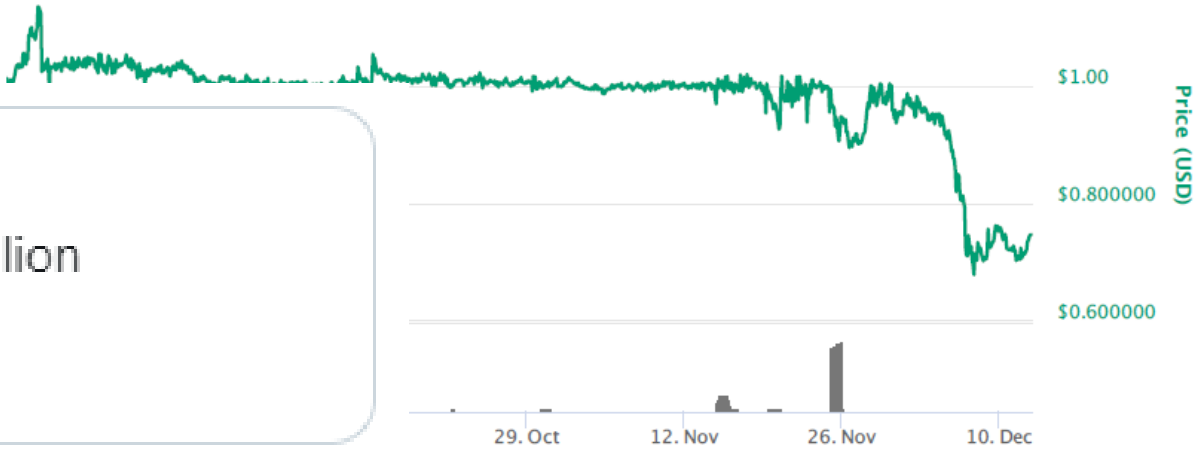
Steem Dollars

bitBTC



NuBits

bitUSD



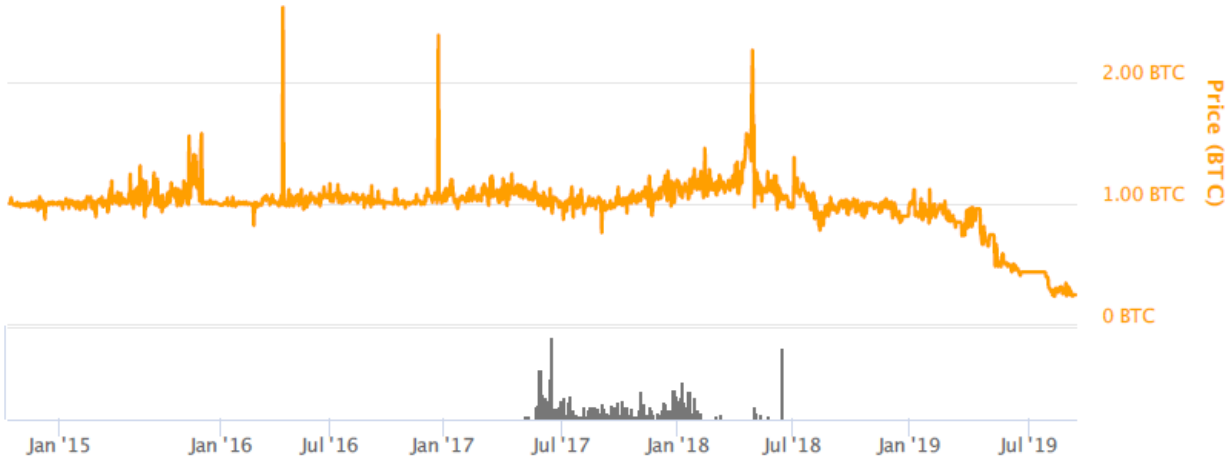
Messari News @MessariNews · Jun 25

Synthetix suffers an oracle attack that lost roughly $37 million

messari.io/article/synthe...

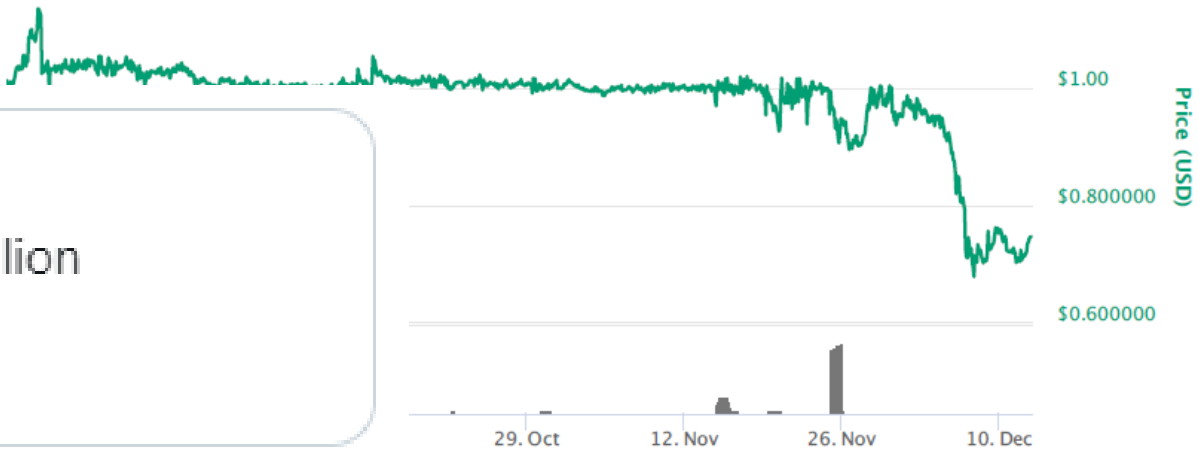
Steem Dollars

bitBTC



NuBits

bitUSD



Messari News @MessariNews · Jun 25

Synthetix suffers an oracle attack that lost roughly $37 million

messari.io/article/synthe...

Steem Dolla

Increasing Robustness of the Terra Oracle

Oracles and Swaps

nplatias 1 Jul 26

Following two oracle attacks in the span of one week, we've been debating how to make similar attacks harder and more expensive to pull off. The goal of this paper is to discuss oracle designs that improve on prevailing implementations, and highlight the tradeoffs that arise. We much look forward to your feedback, this is (and always will be) a work in progress.

Problem: little formal understanding of these systems

- Complex feedback effects
- No truly stable asset efficiently accessible
- Complex interaction of agents

Problem: little formal understanding of these systems

- Complex feedback effects
- No truly stable asset efficiently accessible
- Complex interaction of agents

This talk

- Understanding stablecoins, differences from currency models
- Our paper: a stablecoin model

Stablecoins

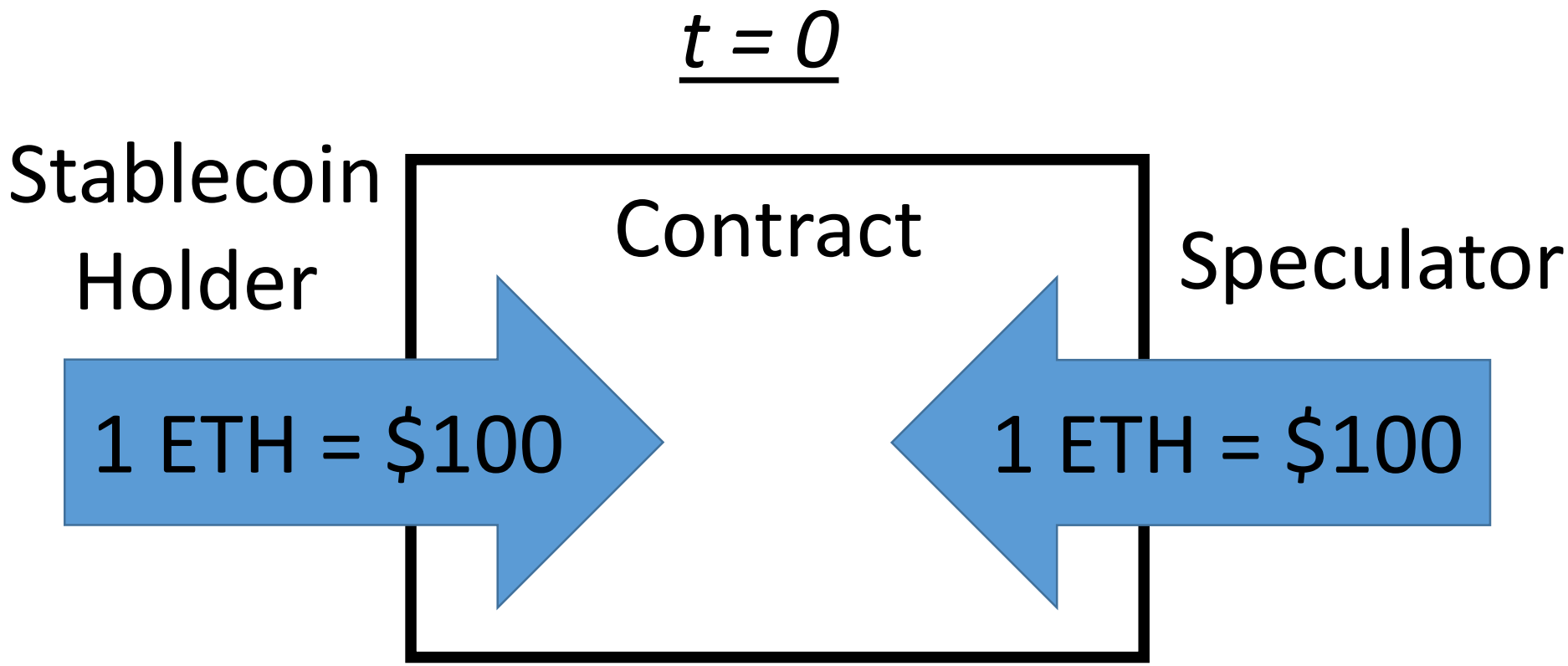
Aim of stablecoins

- Protocol that stabilizes market price/purchasing power
- More usable/adoptable cryptocurrency

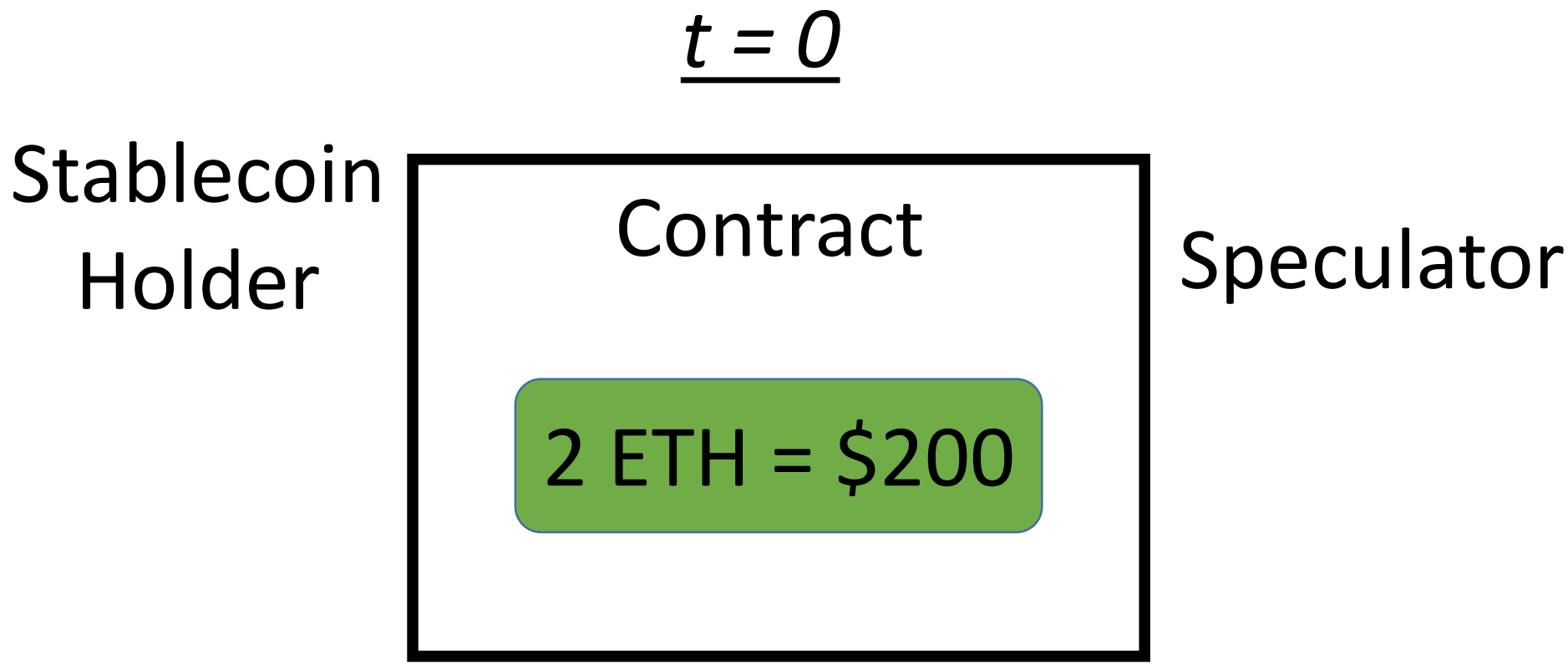
Types of stablecoins

- **Custodial:** reserve assets held off-chain. E.g., Tether
- **Non-custodial:** on-chain mechanisms, E.g., MakerDAO
  - Designs similar, ad hoc

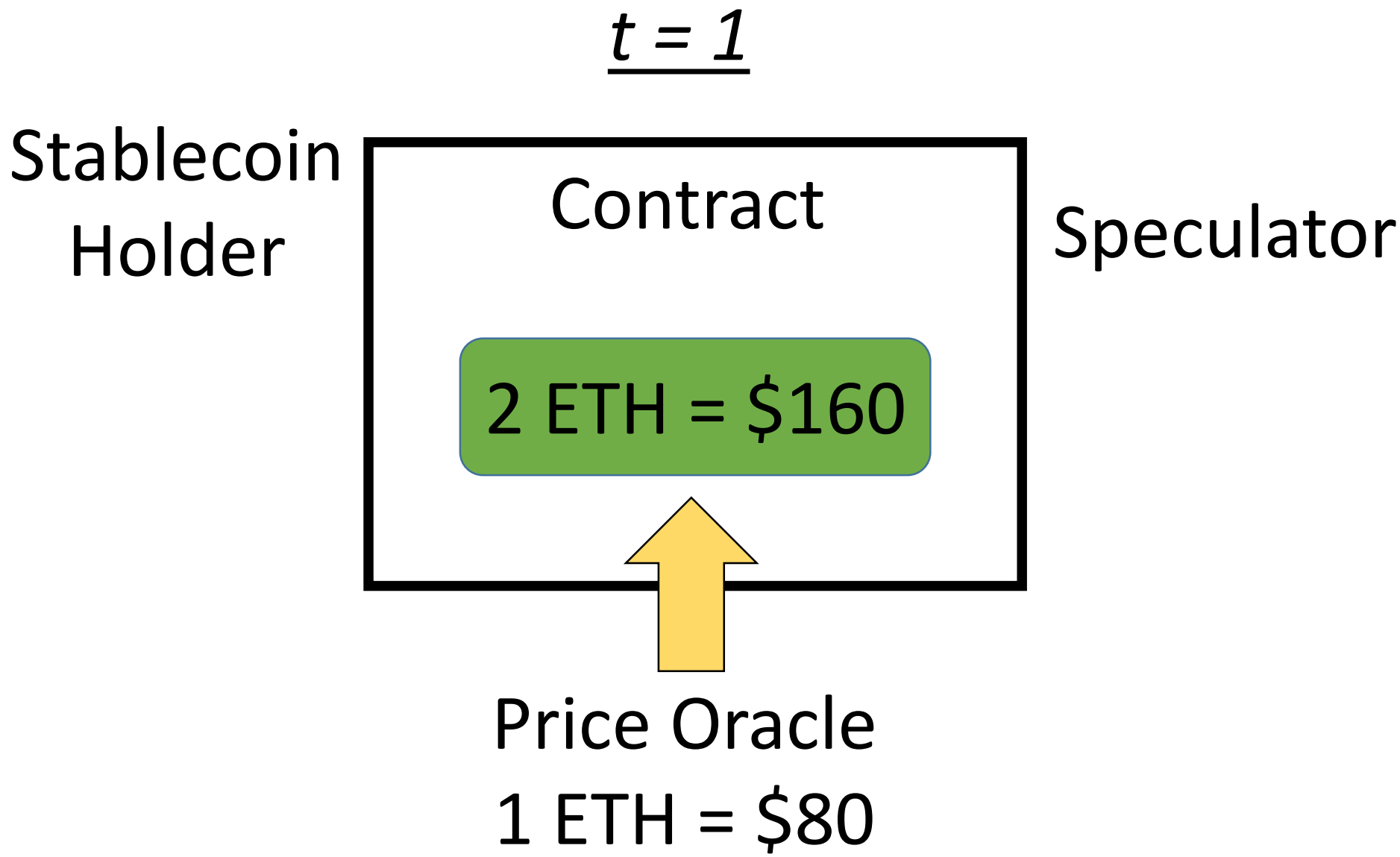
Non-Custodial Contract for Difference



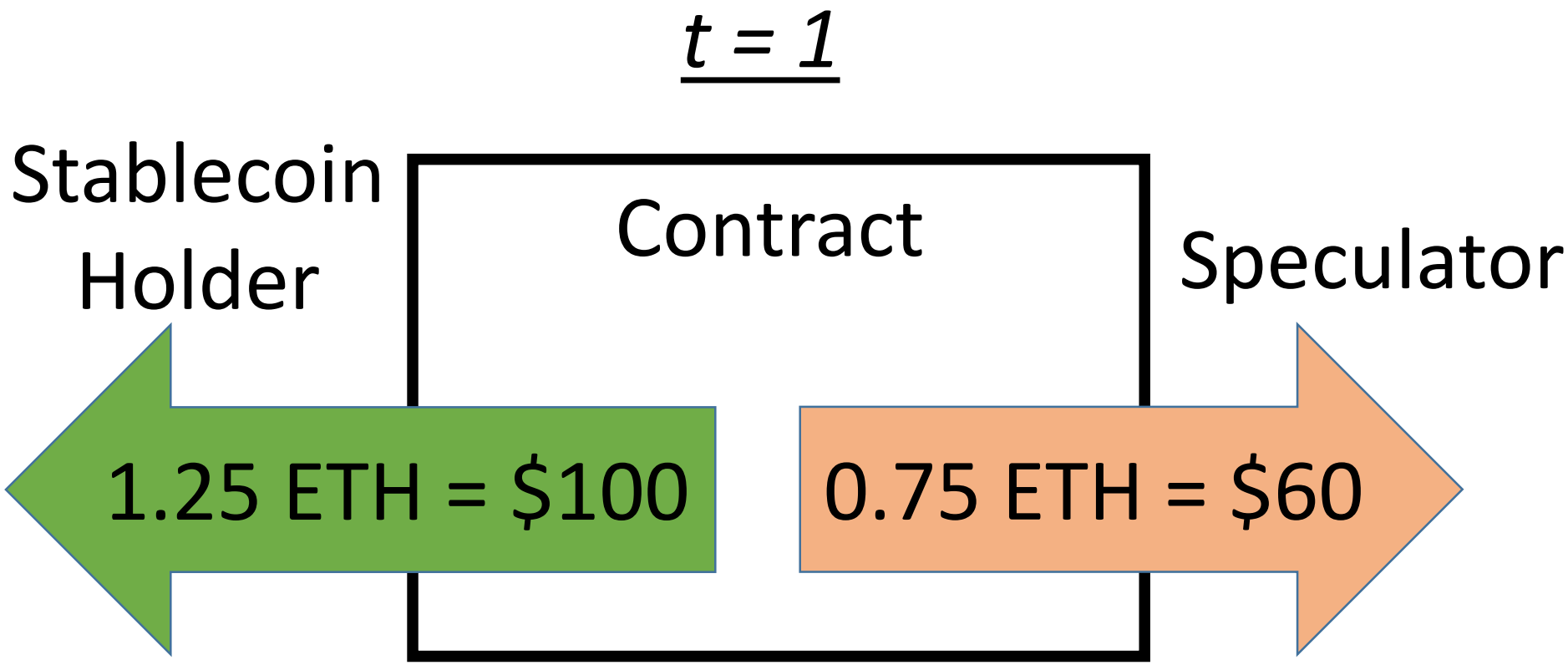
Non-Custodial Contract for Difference



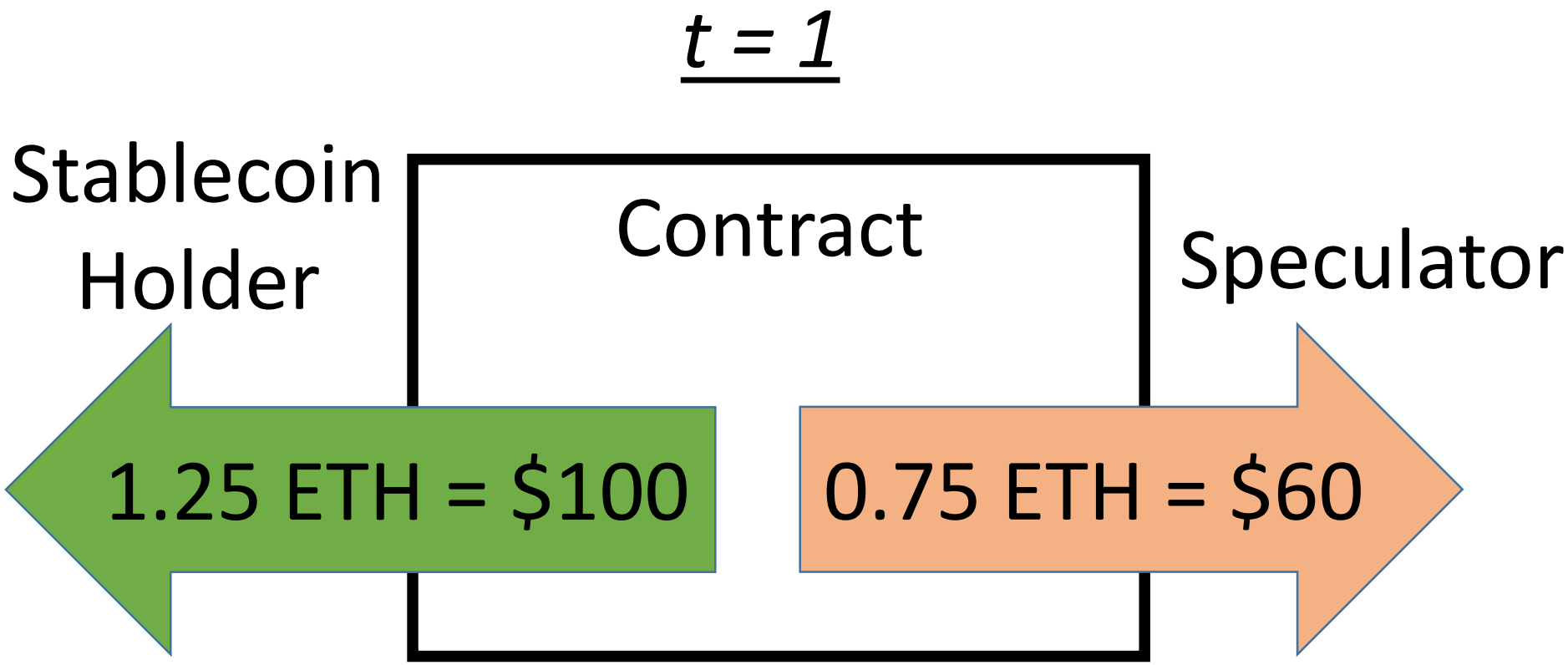
Non-Custodial Contract for Difference



Non-Custodial Contract for Difference



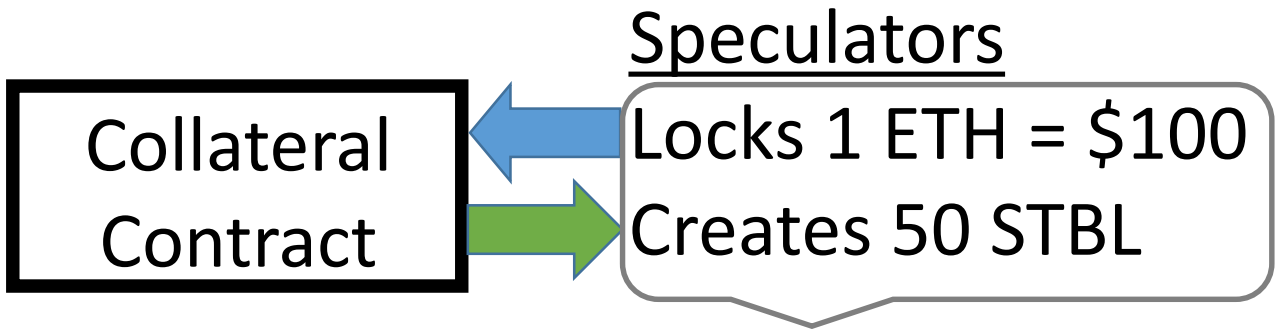
Non-Custodial Contract for Difference



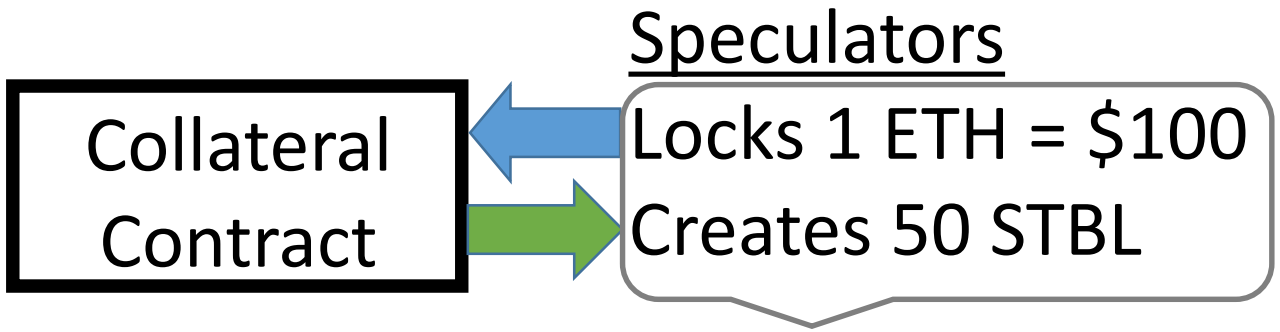
Similar to a forward contract **except:**

- Price is only fixed in fiat terms while payout in units of risky collateral
- *In these markets:* heavy frictions to convert to fiat

Stablecoins with no set expiration



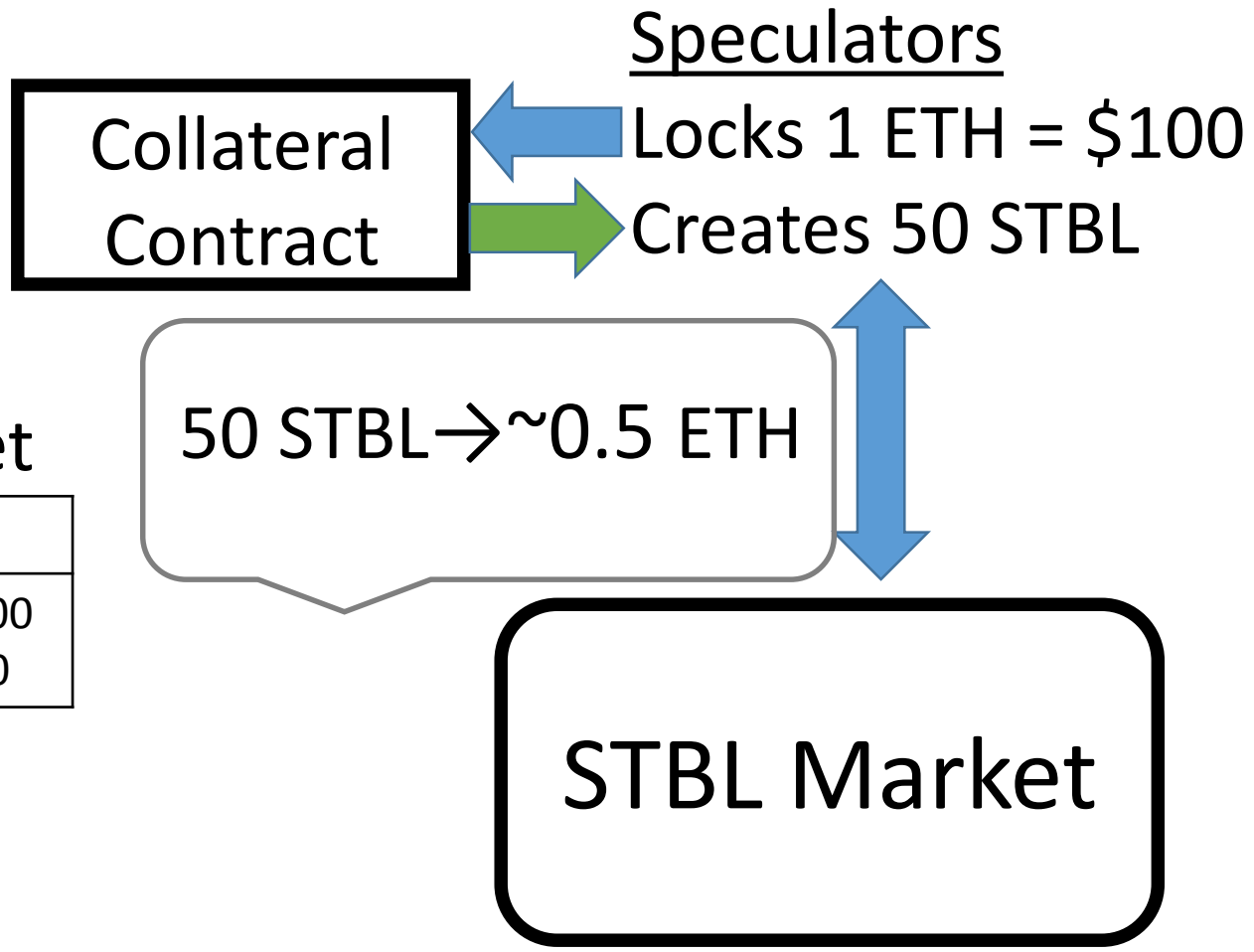
Stablecoins with no set expiration



Speculator Balance Sheet

Assets		**Liabilities**	
ETH (pledged)	$100	Equity	$100
Stablecoin	$50	Smart contract	$50

Stablecoins with no set expiration

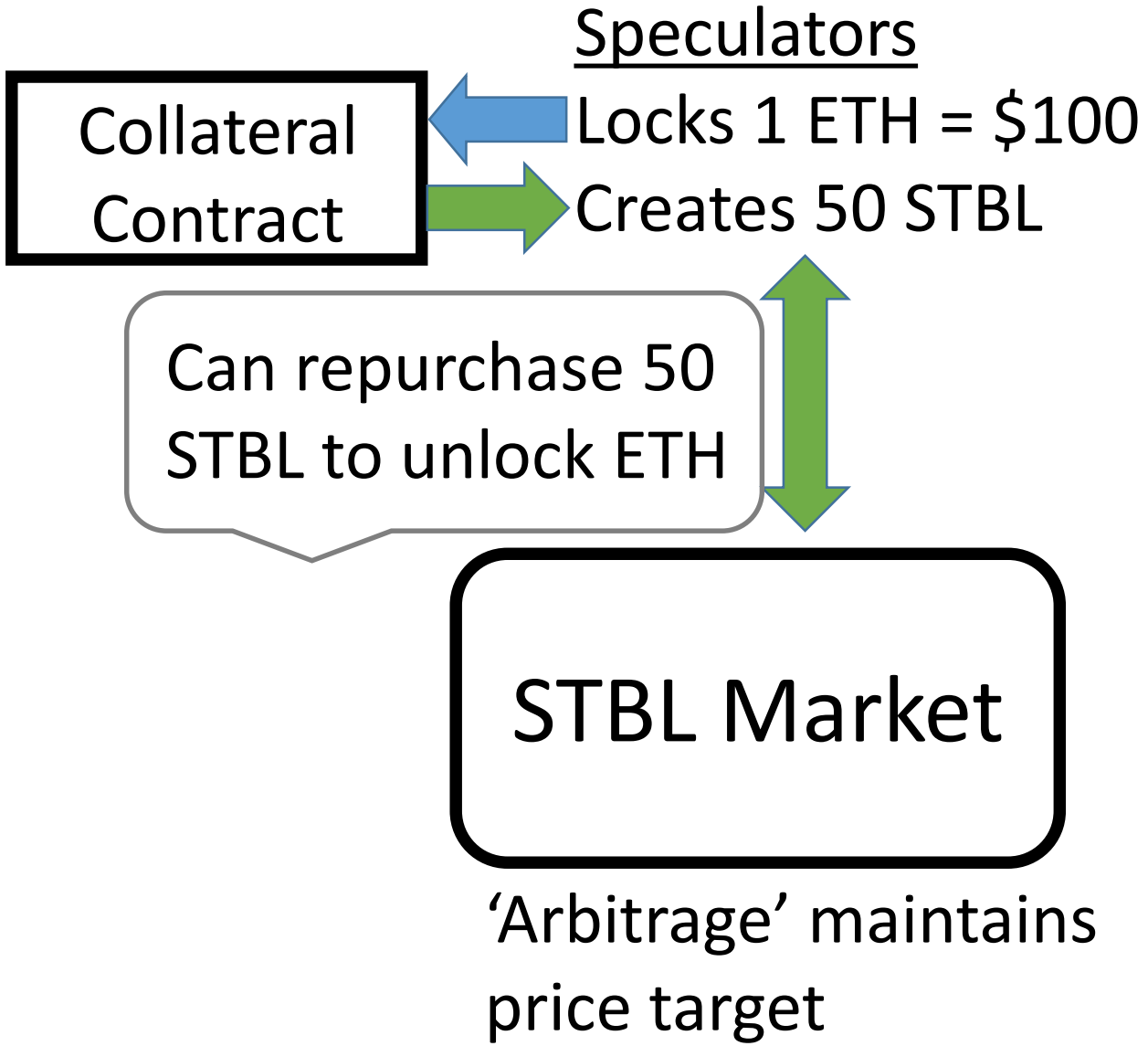


Speculator Balance Sheet

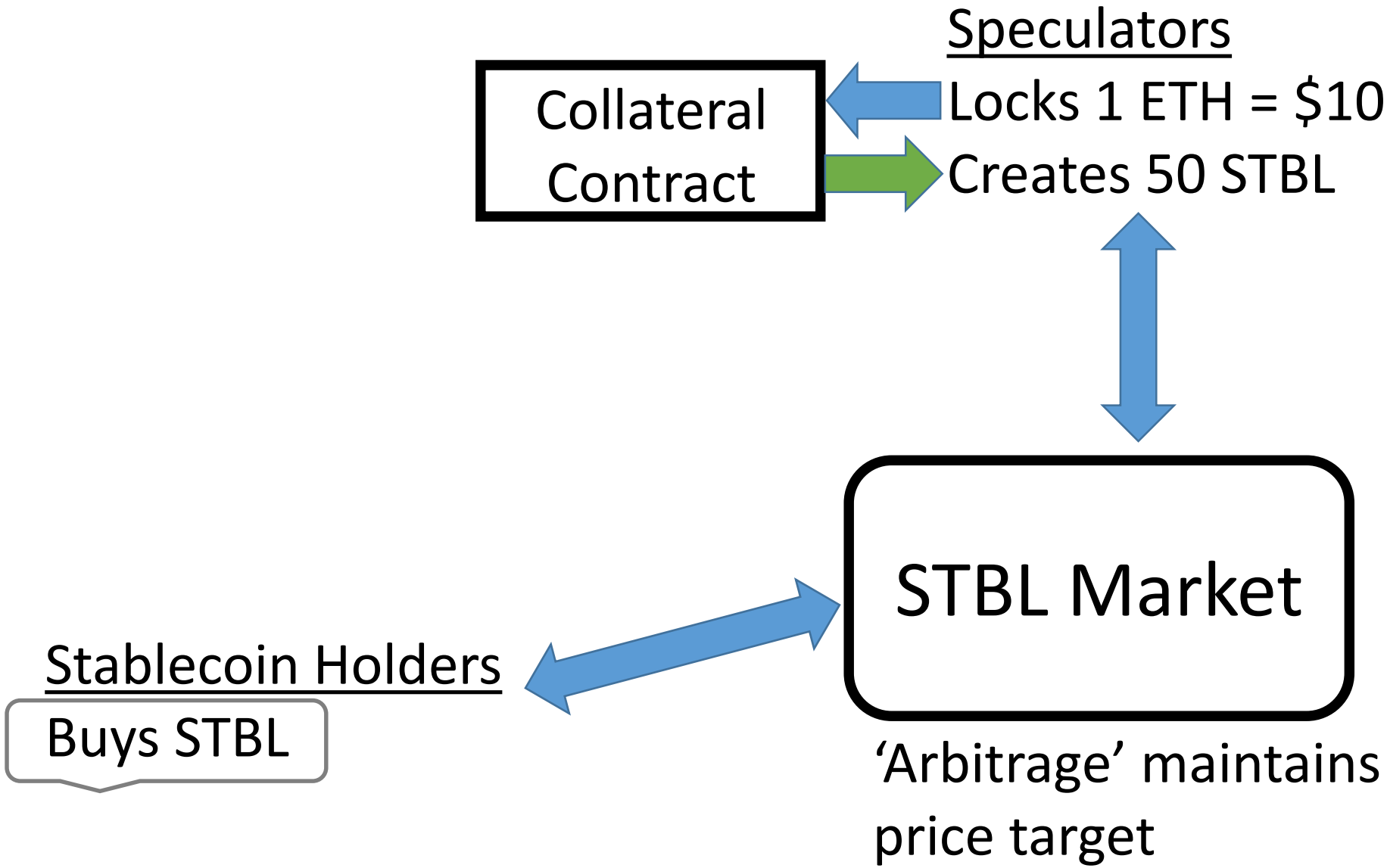
Assets		Liabilities	
ETH (pledged)	$100	Equity	$100
ETH	$50	Smart contract	$50

‘Arbitrage’ maintains price target

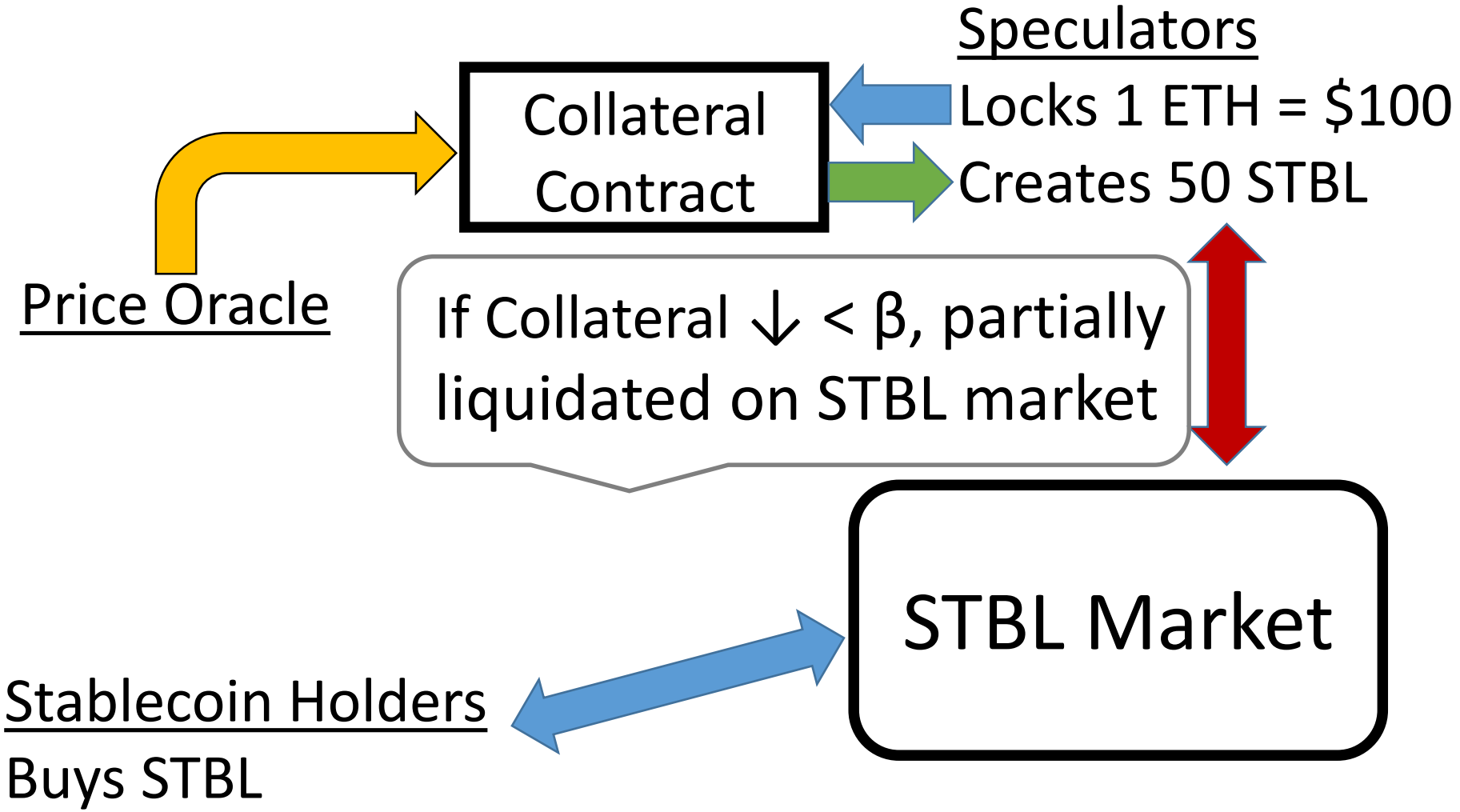
Stablecoins with no set expiration



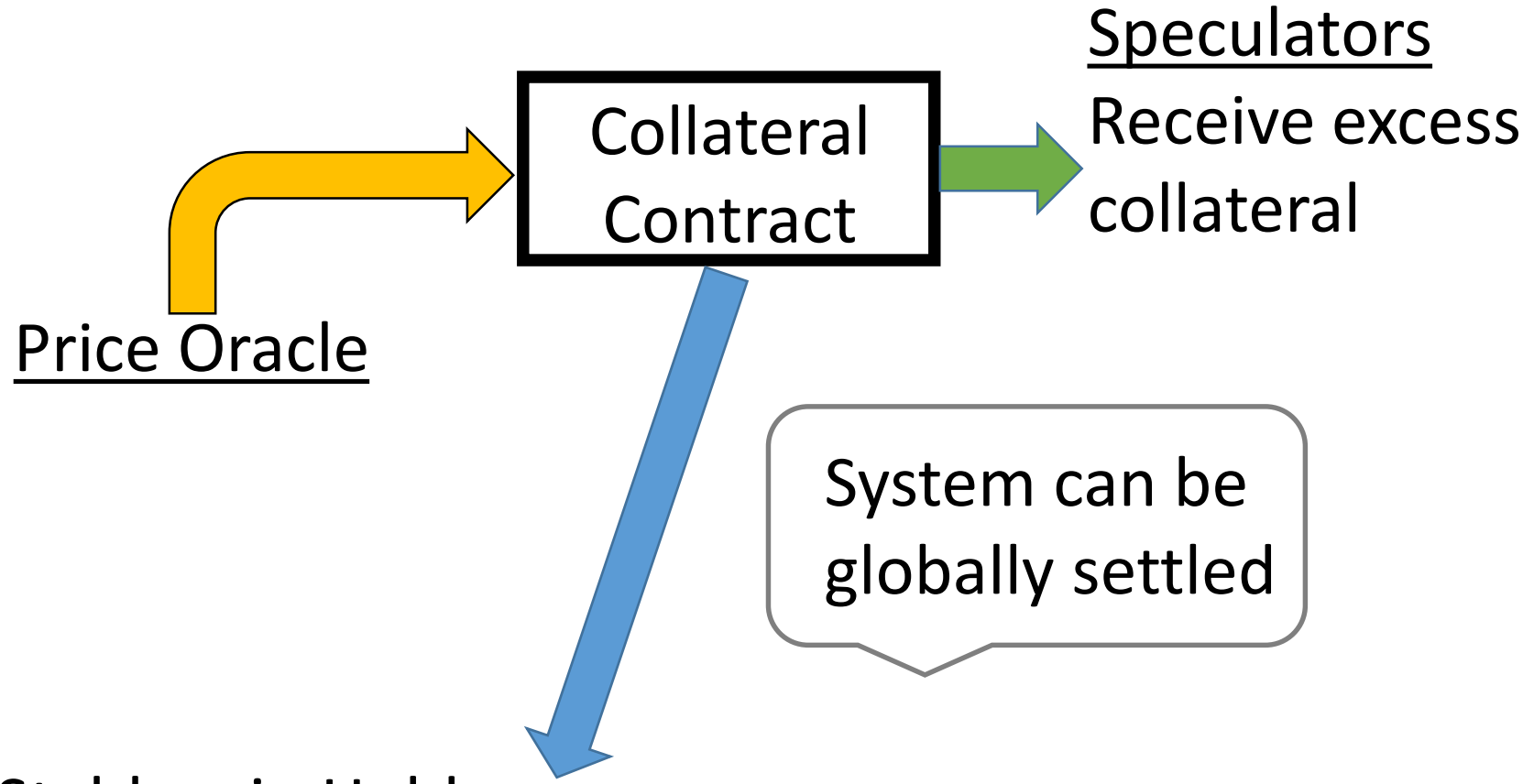
Stablecoins with no set expiration



Stablecoins with no set expiration

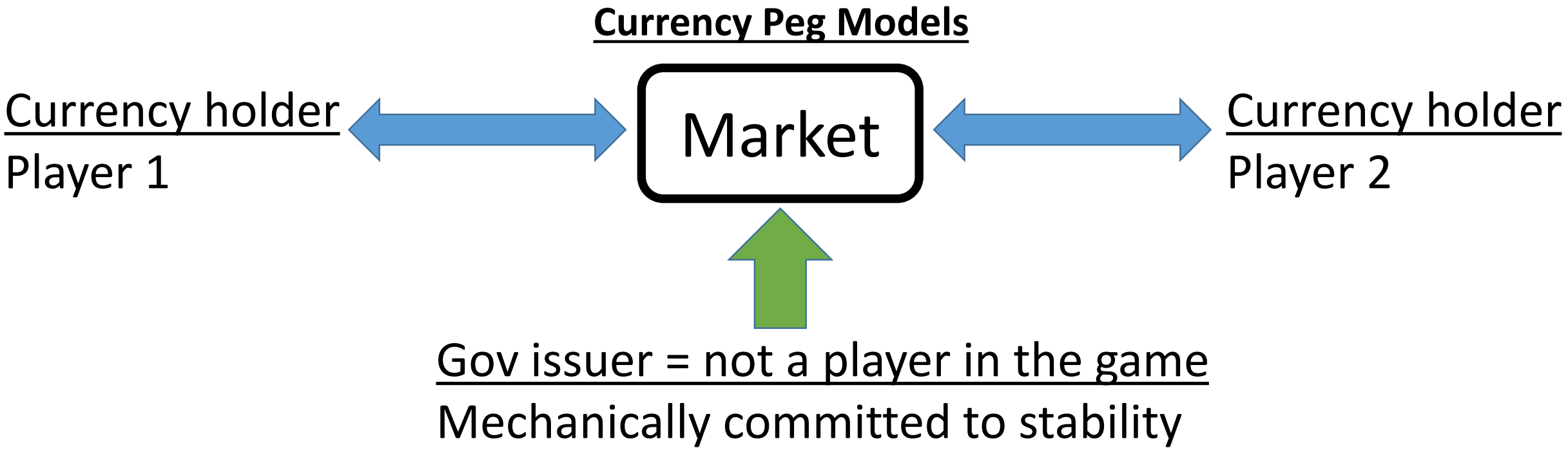


Stablecoins with no set expiration

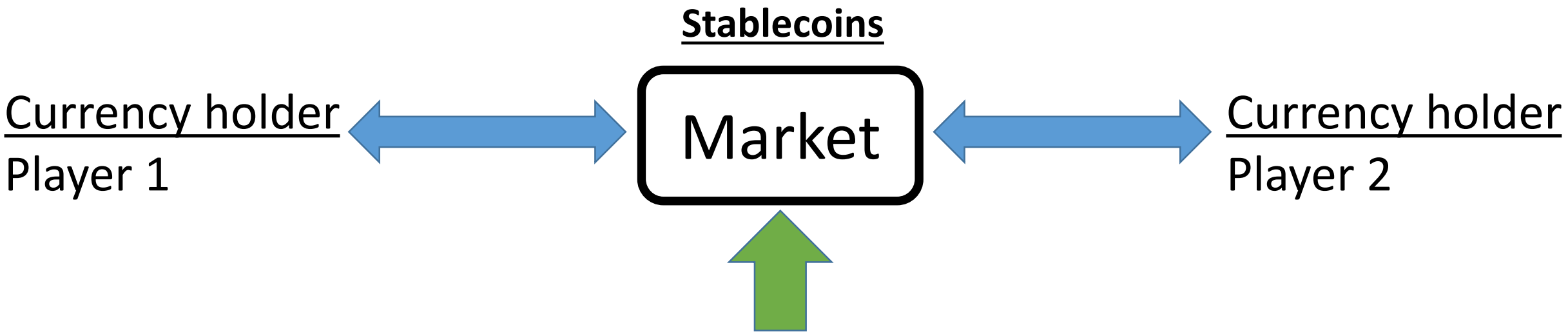


Can we use existing literature on currency peg models? Unfortunately, no

Can we use existing literature on currency peg models? Unfortunately, no



Can we use existing literature on currency peg models? Unfortunately, no



Decentralized speculators = players in the game

- Issue/withdraw stablecoins to optimize profits
- Not committed to maintaining peg!
- **Best we can hope:** protocol well-designed and peg maintained through incentives

Model

Agents

- **Stablecoin Holders** seek stability ⇒ demand with some elasticity
- **Speculator** chooses leveraged bets backing stablecoin

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

- Similar to clearing in Uniswap

Model: Speculator

Decision: Change stablecoin supply to maximize next period expected returns subject to constraints ('honest' behavior)

Liquidation constraint (protocol): over-collateralization requirement

Risk constraint (self-imposed): how much speculator wants to avoid liquidation

- Example: value-at-risk, consistent with margin of safety
- Consider other formulations as well

Dynamics & Liquidity

Analytical Result 1: There is a bound to the speculator's ability to maintain the market

(A lower bound on collateral) – (capital required to enter market)
must be sufficiently high

Dynamics & Liquidity

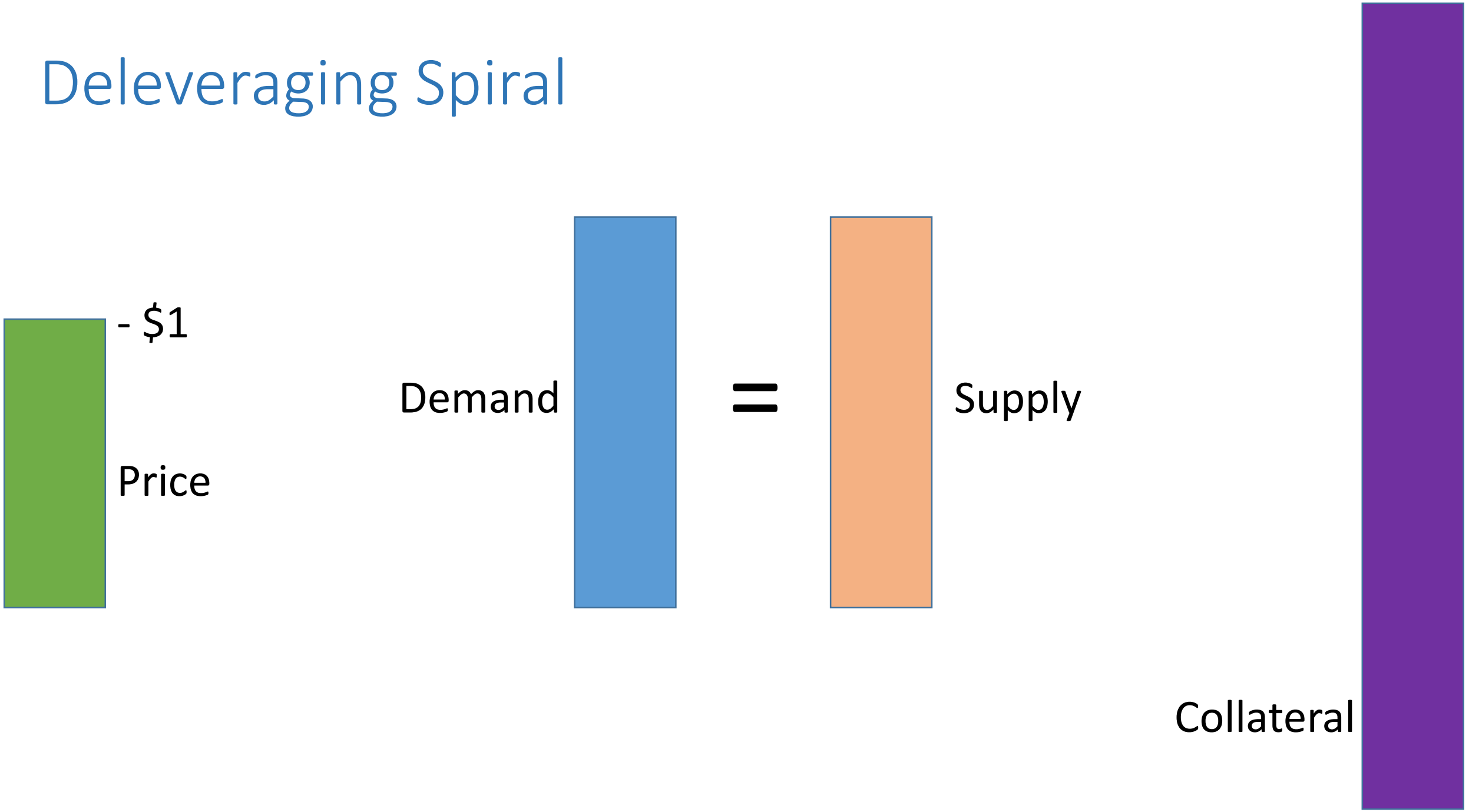
Analytical Result 1: There is a bound to the speculator's ability to maintain the market

(A lower bound on collateral) – (capital required to enter market)
must be sufficiently high

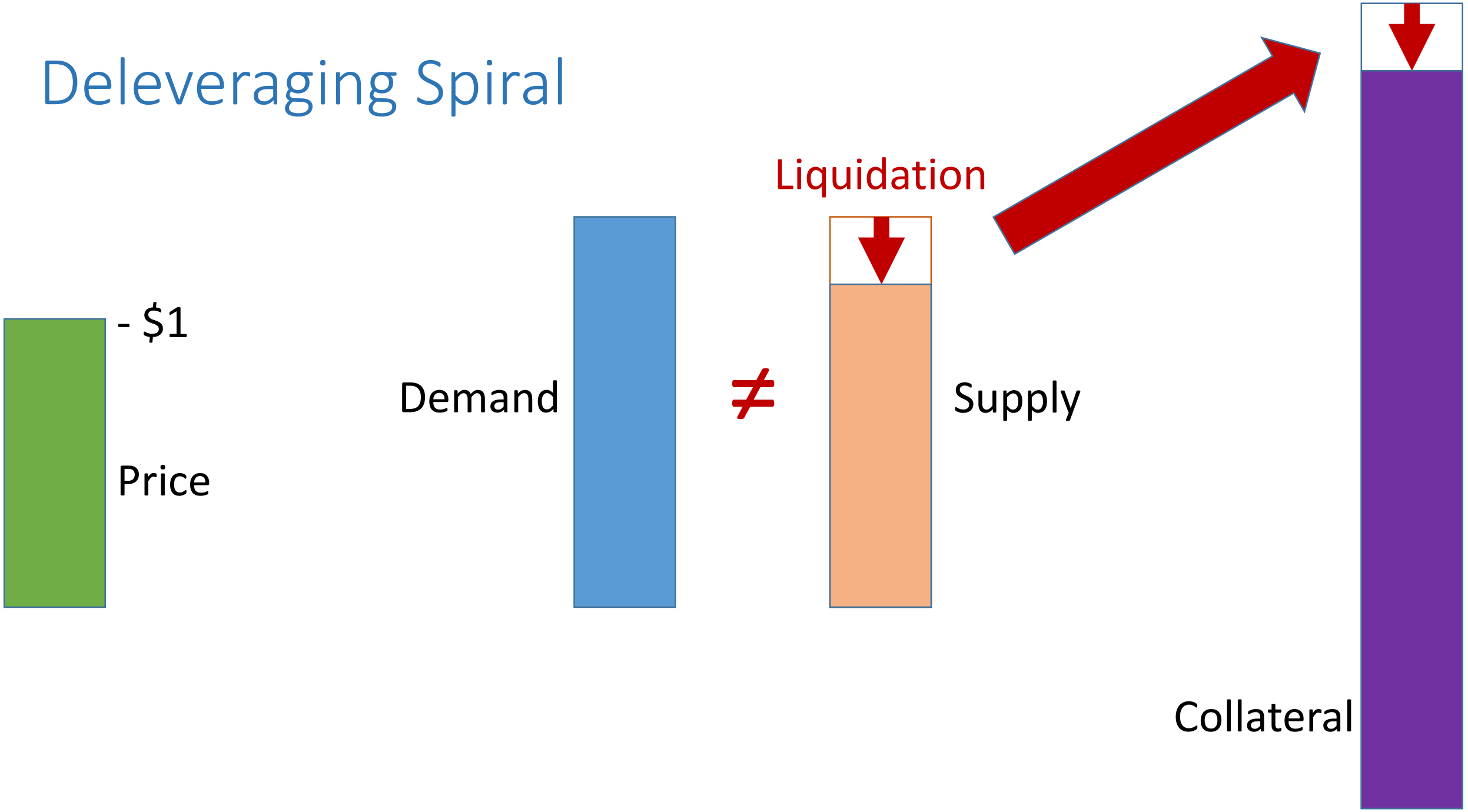
Analytical Result 2: Speculators face limits to how quickly they can reduce leverage, even with new capital

Deleveraging spiral: speculators repurchase stablecoins at increasing prices as liquidity dries up in the market.

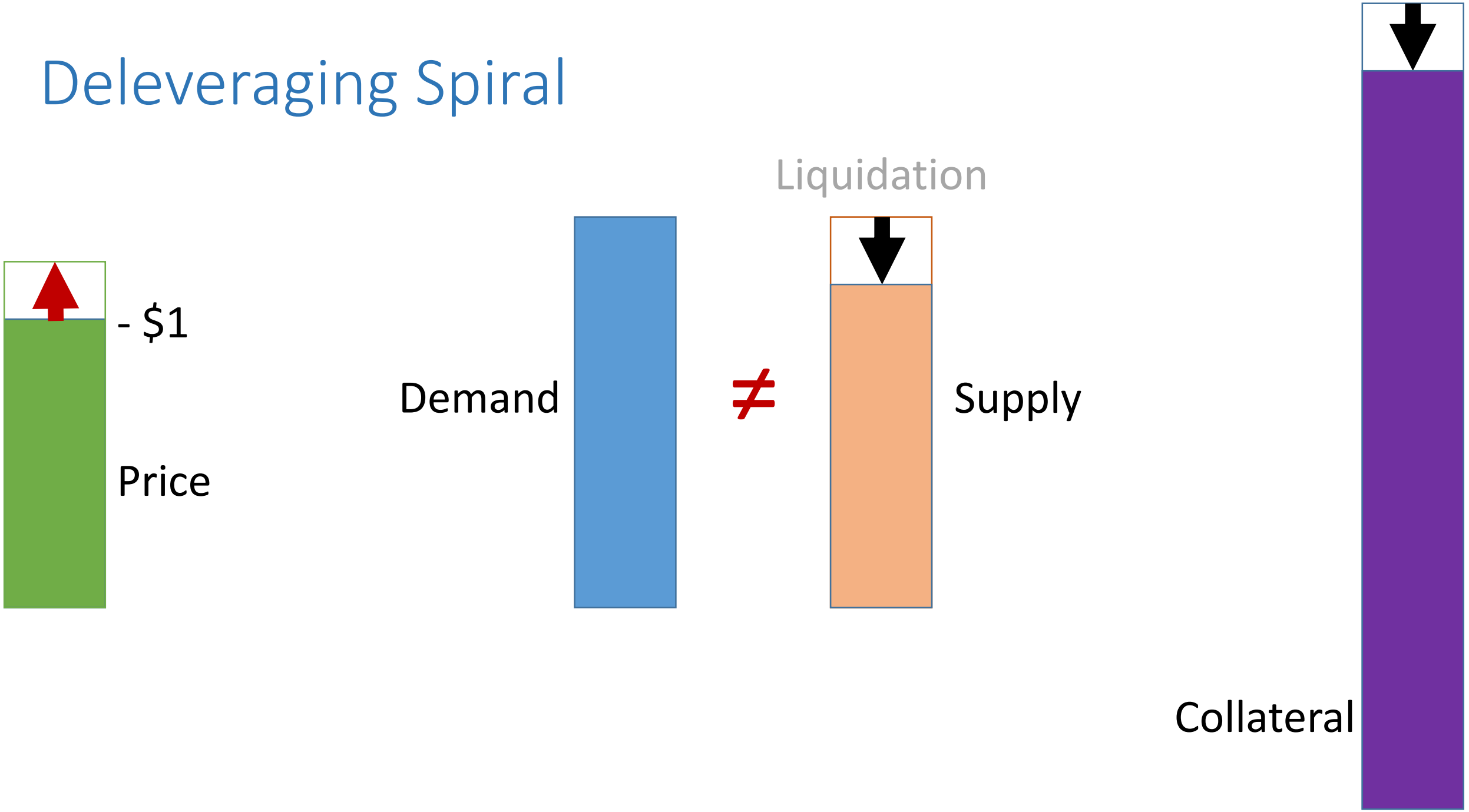
Deleveraging Spiral



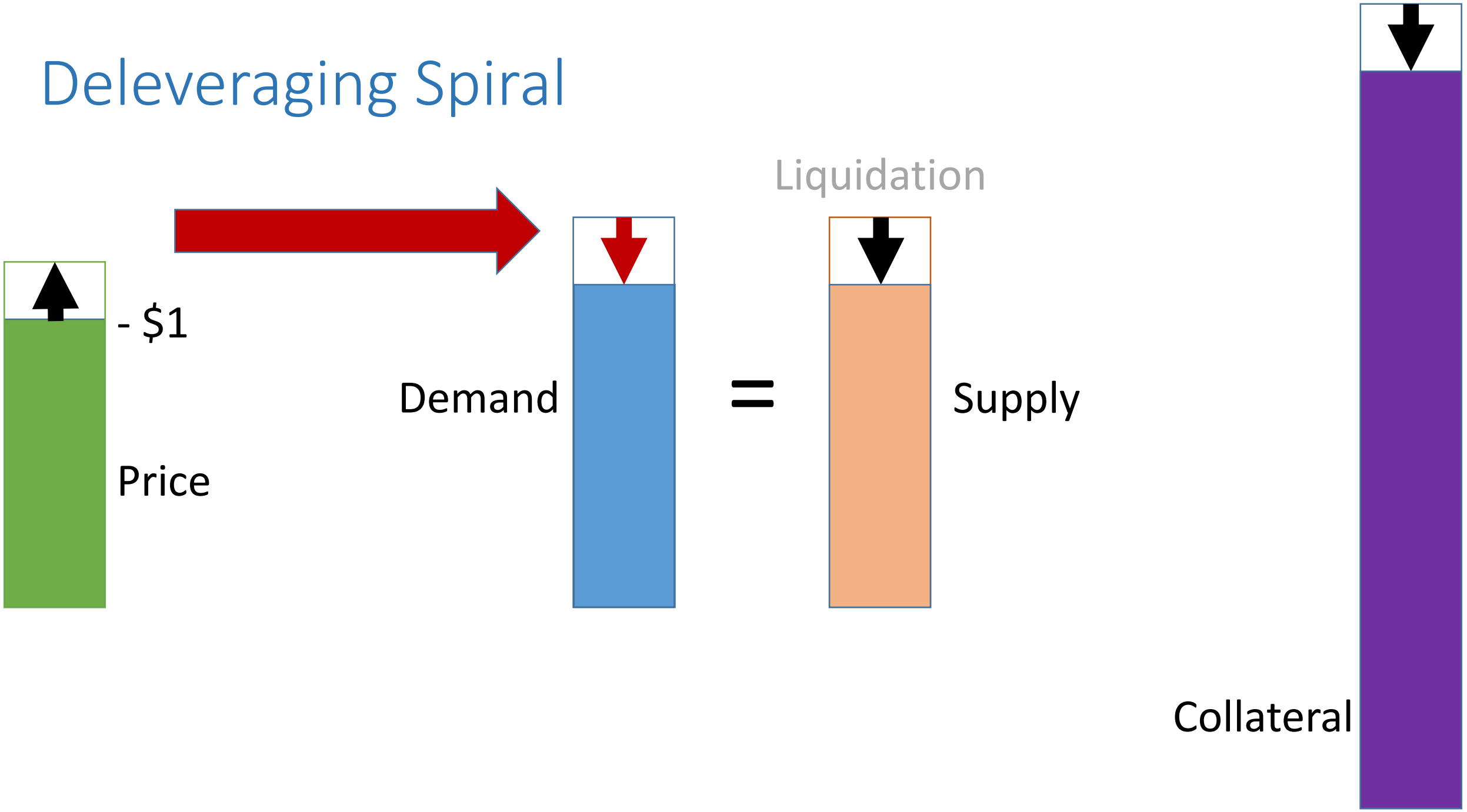
Deleveraging Spiral



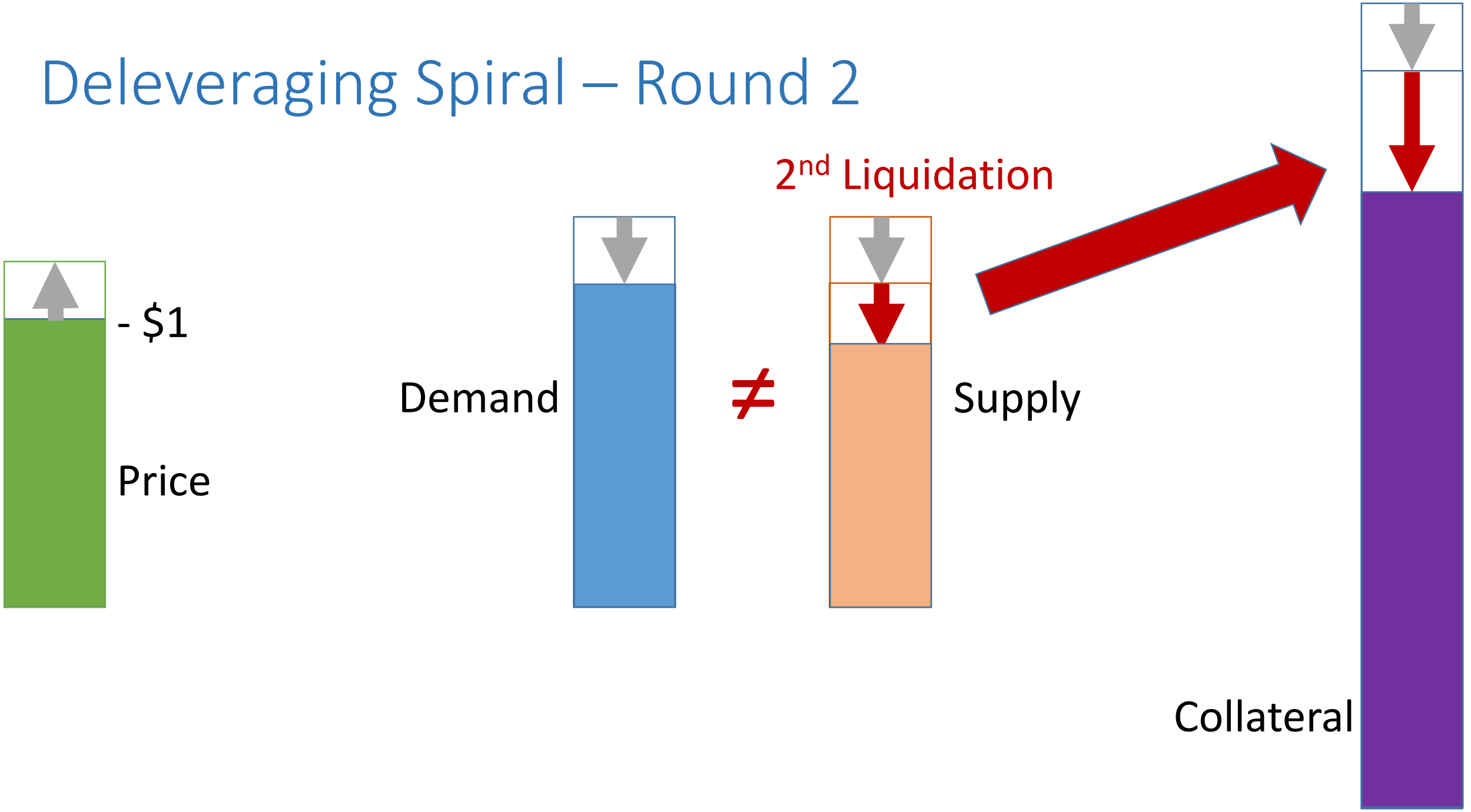
Deleveraging Spiral



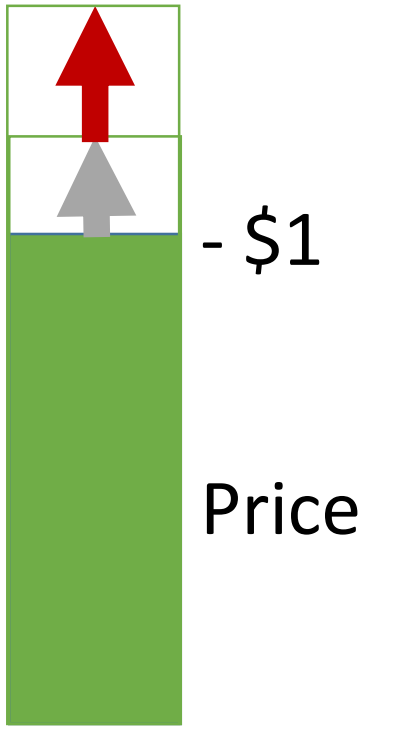
Deleveraging Spiral



Deleveraging Spiral – Round 2



Deleveraging Spiral – Round 2

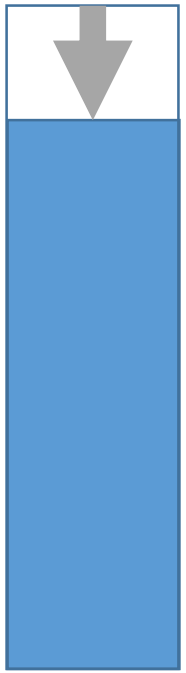


- $1

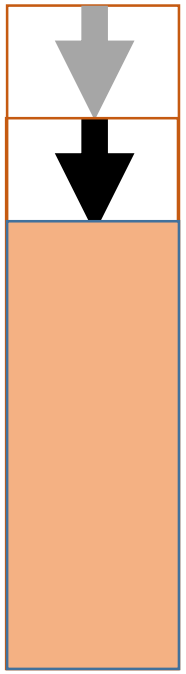
Price

2nd Liquidation

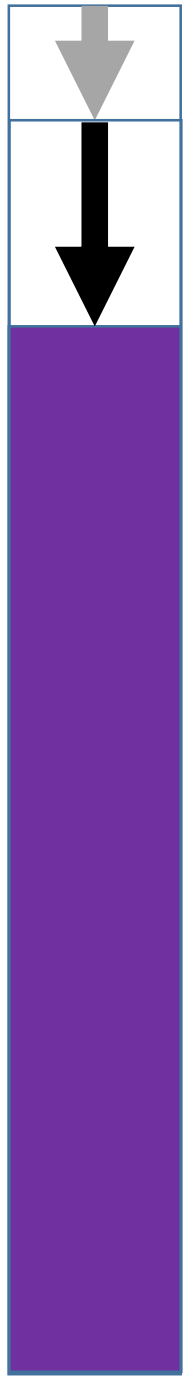
Demand



≠

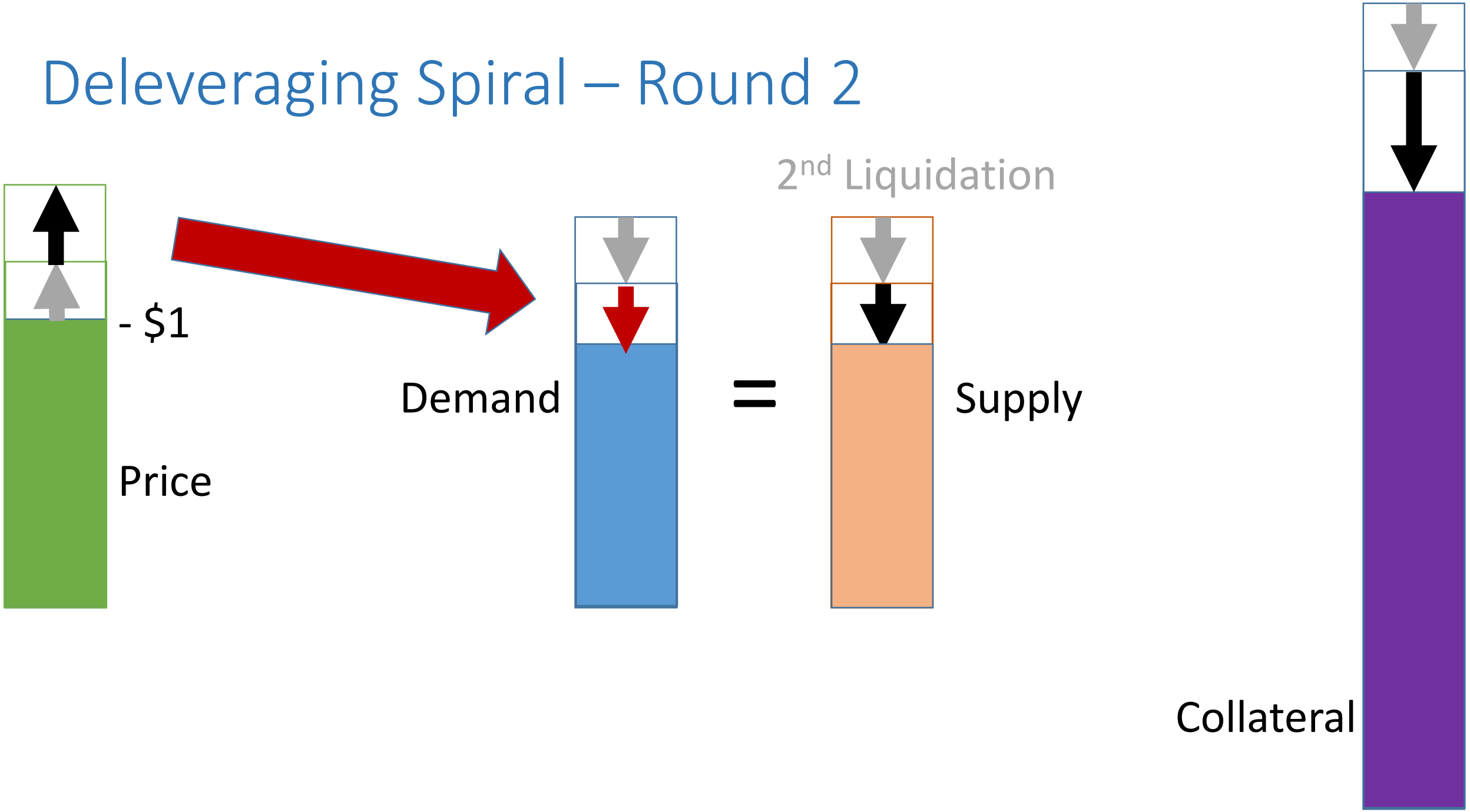


Supply



Collateral

Deleveraging Spiral – Round 2



Stable & Unstable Regions

Analytical Result 3: Assume STBL demand and expected ETH return constant.
Then if leverage constraint remains inactive, the system converges exponentially to a steady state with stable price and zero variance.

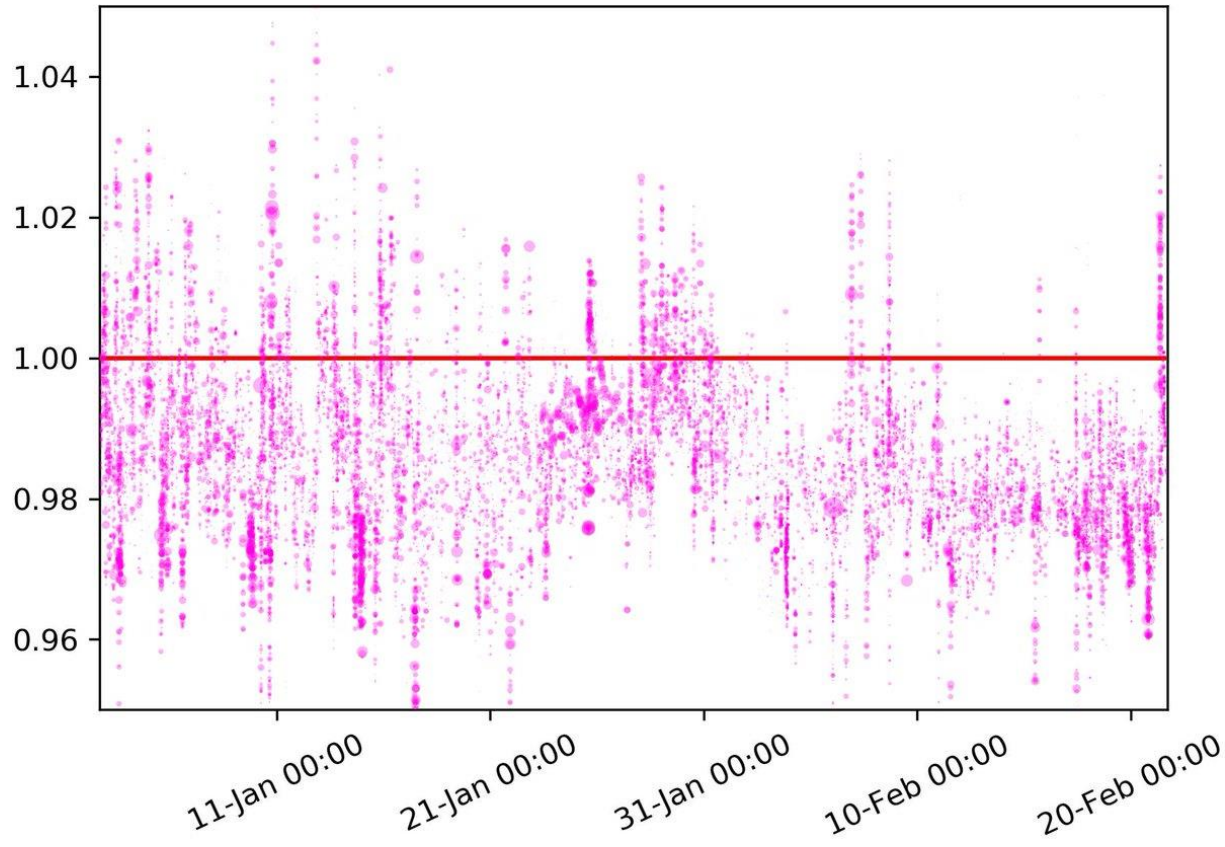
Observation: Steady state may have price < $1.

Conjecture: Outside of 'stable' domain, volatility bounded > 0 with high probability.

- Once outside, more likely to remain outside due to feedback effect
- 'Kink' in probability distribution at boundary

These Effects Explain Data from Dai Market

Dai leverage reduction feedback



Dai normally trades below target

Source: Kenny Rowe, Tweet

Simulation: ‘Stable’ & ‘Unstable’ Regions

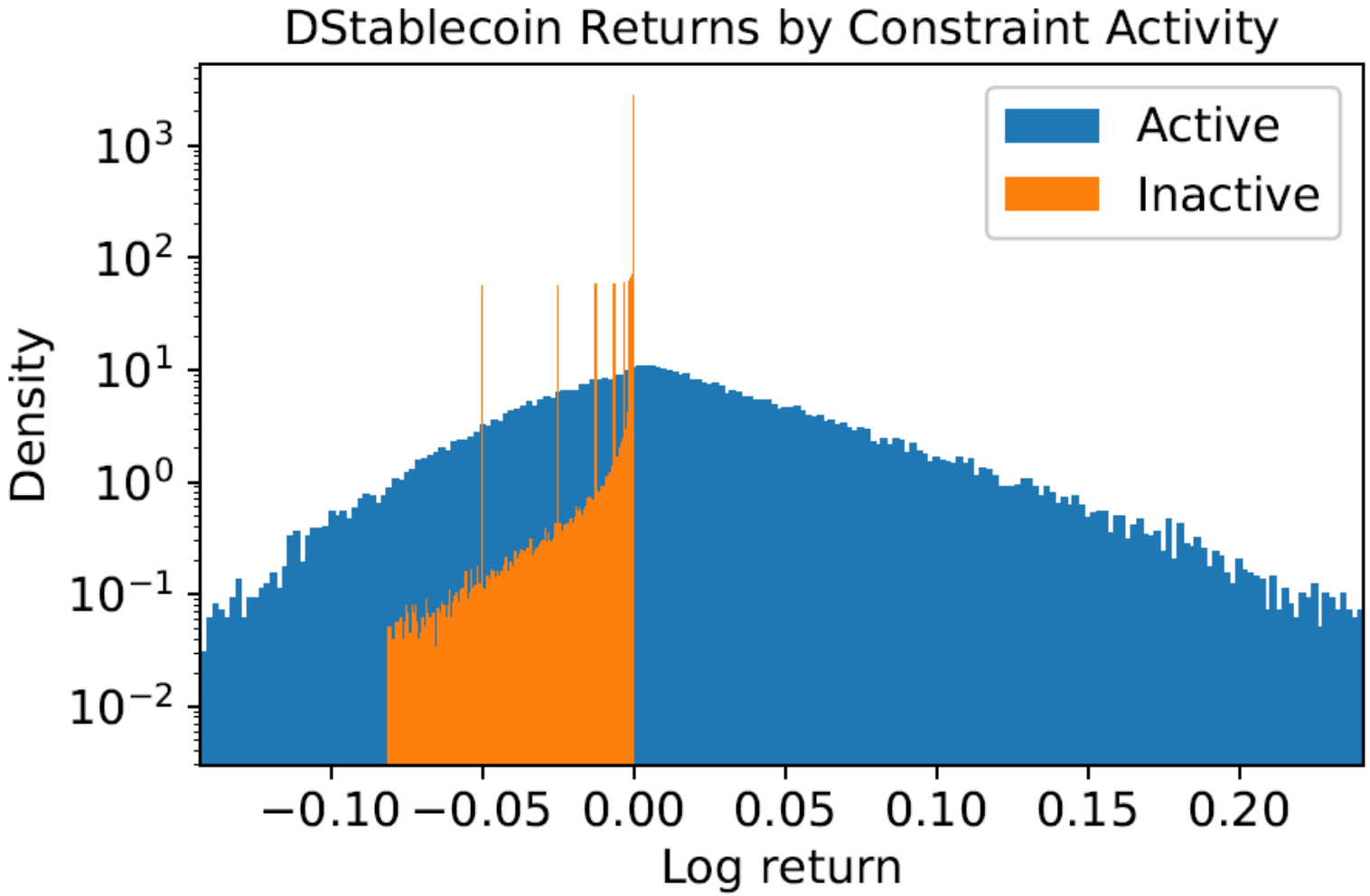
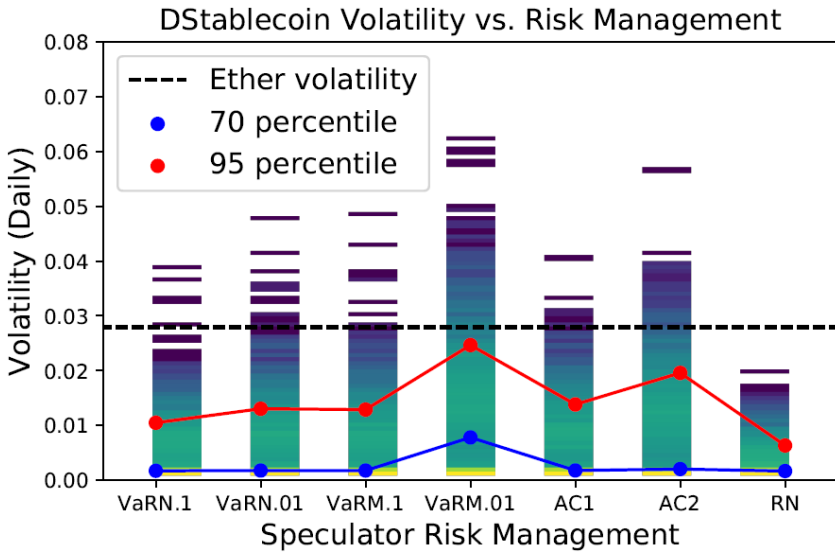
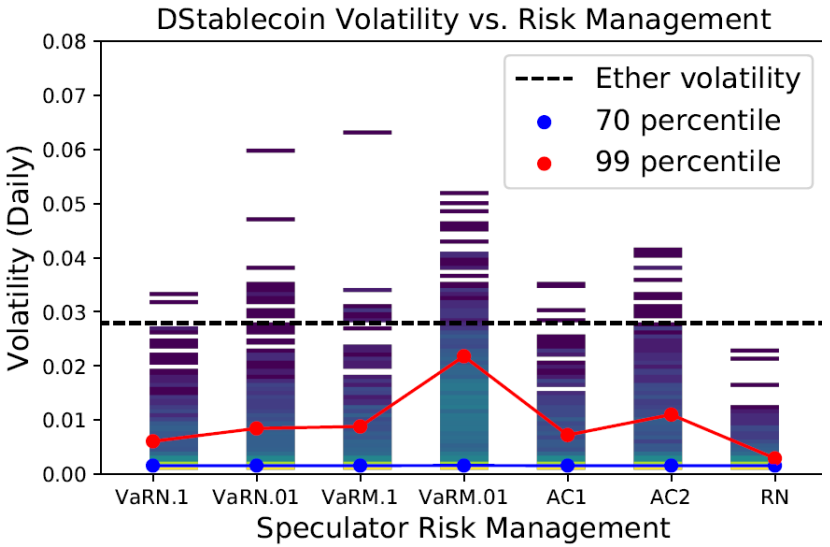


Figure: Constant expected ETH return

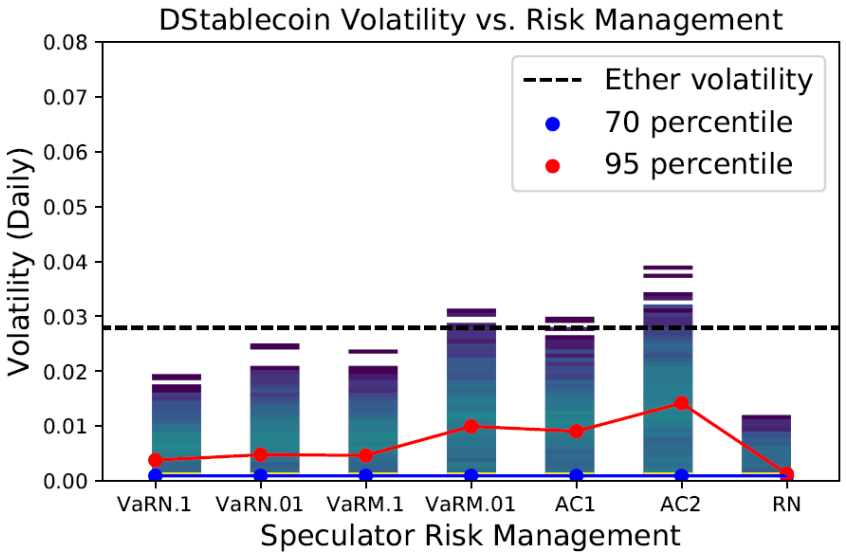
Simulation: Different Speculator Behaviors



(a) t-distr(df=3, μ=0)



(b) t-distr(df=3, μ=r_0)



(c) normal(μ=0)

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 speculators

Attack primitives:

- Deleveraging spirals ⇒ arbitrage-like trades around liquidations
- Real implementations add arbitrage to automate liquidations
- 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

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

1. Buy STBL before liquidation, dry up liquidity
2. In ETH decline, trigger liquidations, earn spread
3. Sell STBL at higher price ($$$)
4. Can enter as new speculator at high STBL prices

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

1. Buy STBL before liquidation, dry up liquidity
2. In ETH decline, trigger liquidations, earn spread
3. Sell STBL at higher price ($$$)
4. Can enter as new speculator at high STBL prices

In model examples:
profitable 8-13%

Economic Attacks

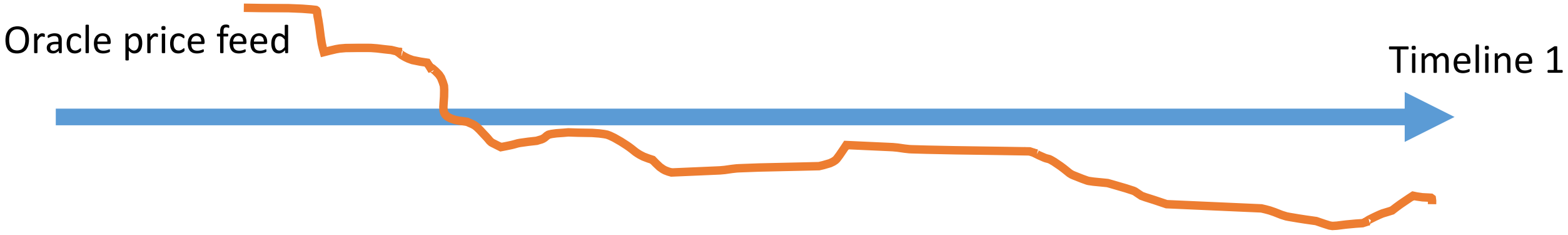
Attack 2: After ETH decline, reorg blockchain to trigger, profit from spiraling liquidations

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

Economic Attacks

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

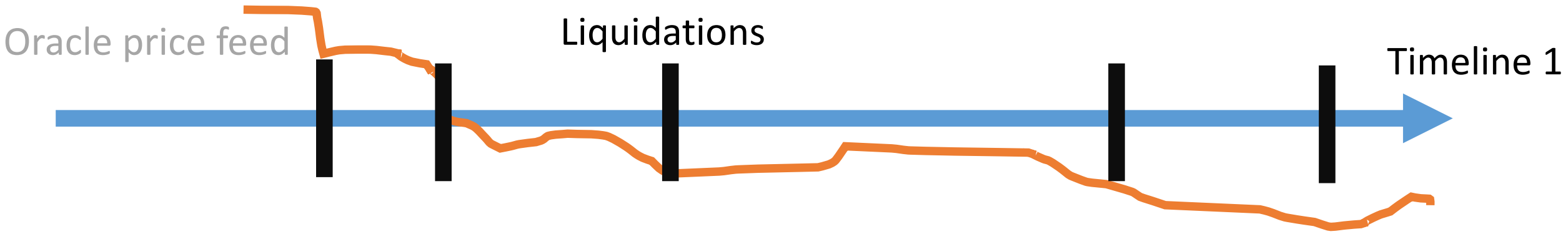
- Change in transaction ordering ⇒ liquidations, extractable value
- Perverse incentive for miners if attack rewards > mining rewards



Economic Attacks

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

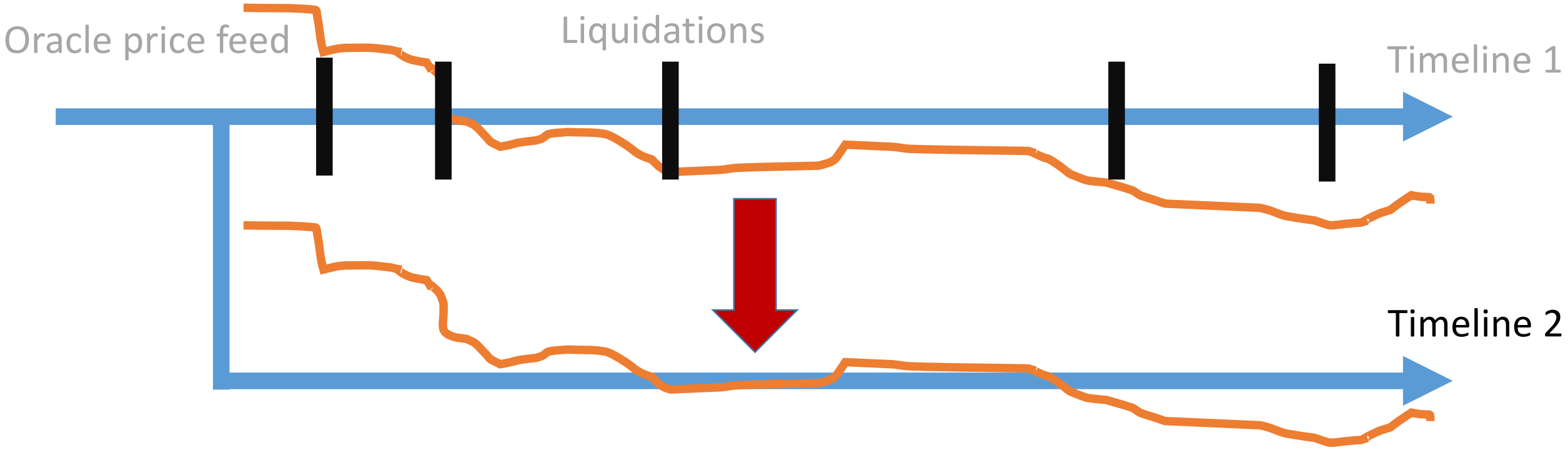
- Change in transaction ordering ⇒ liquidations, extractable value
- Perverse incentive for miners if attack rewards > mining rewards



Economic Attacks

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

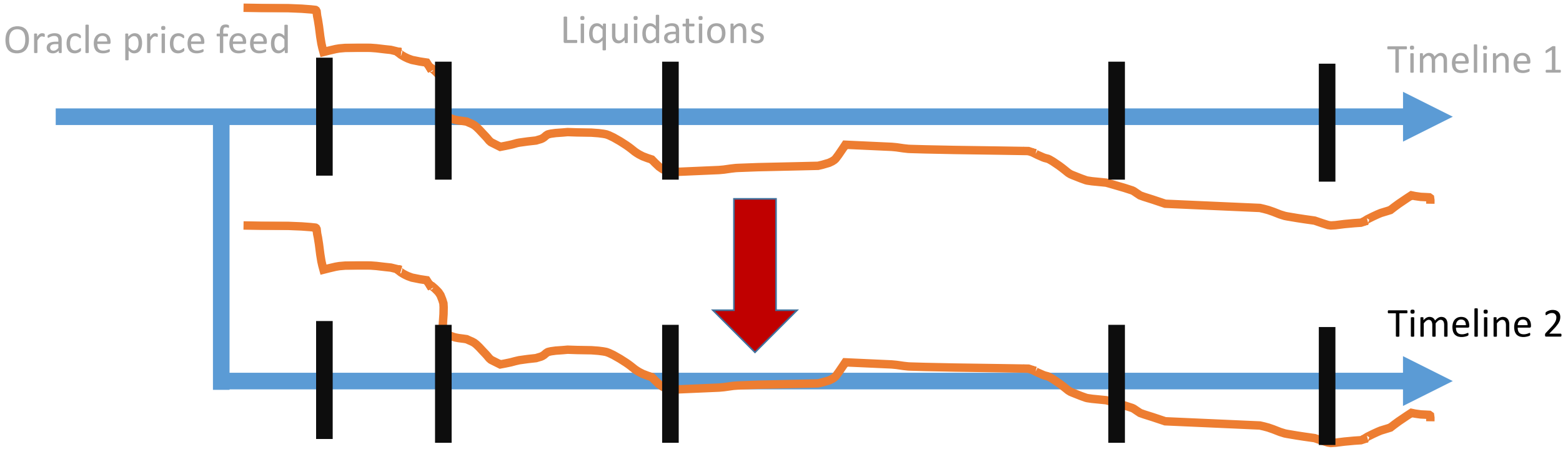
- Change in transaction ordering ⇒ liquidations, extractable value
- Perverse incentive for miners if attack rewards > mining rewards



Economic Attacks

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

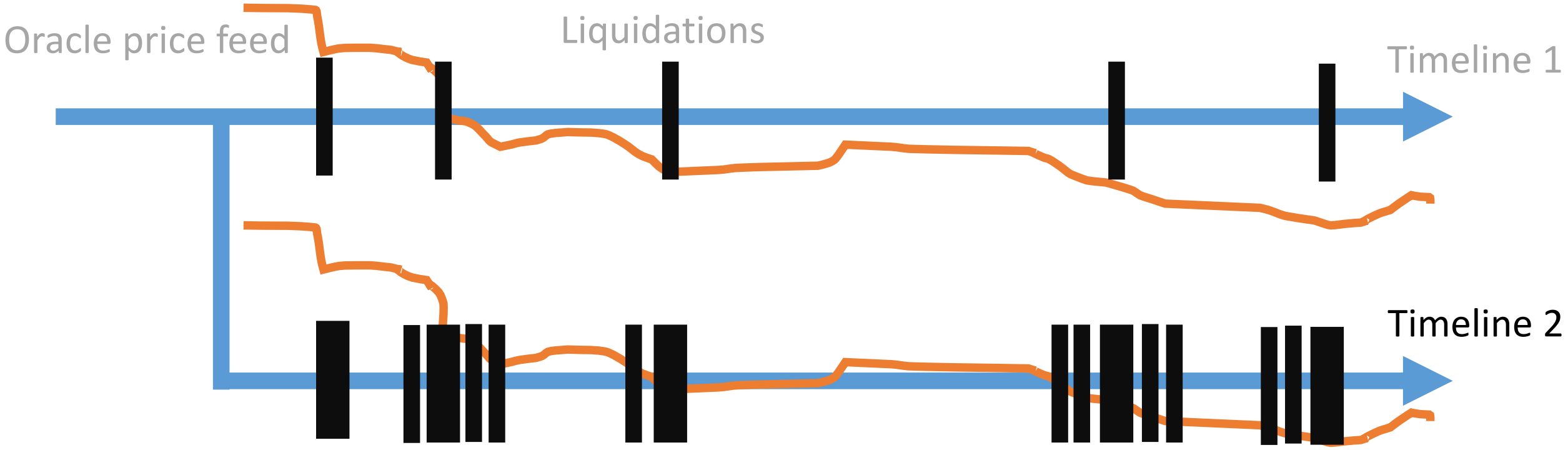
- Change in transaction ordering ⇒ liquidations, extractable value
- Perverse incentive for miners if attack rewards > mining rewards



Economic Attacks

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

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



Design Insights

Design focus: widen ‘stable’ region, limit severity of ‘unstable’ region

Design considerations in Dai

- Fees amplify deleveraging spirals. Can instead make counter-cyclic fees
- Good fee mechanism could reduce speculator herd behavior
- Better ‘last resort’ use of MKR to quell deleveraging spirals

A Key factor: Exchangeability to outside alternatives

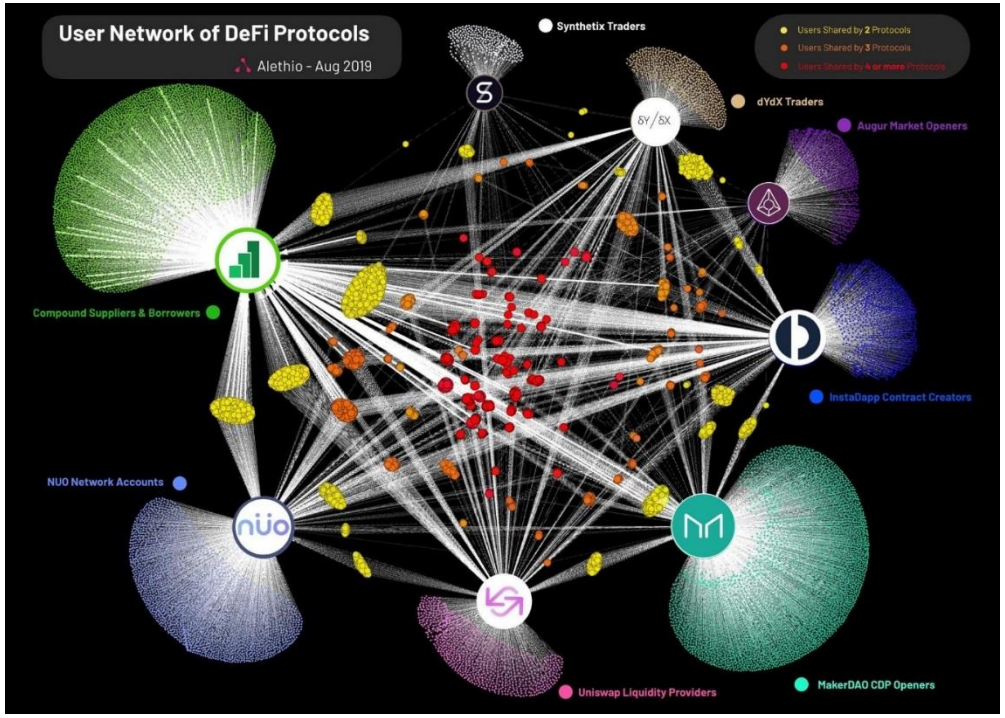
- Lower feedback effects, but introduces shutdown risk
- In many jurisdictions, not an option (e.g., premium in Argentina)

Open Questions

- Expanding strategy space of speculators/attackers
- Understanding governance and oracle risks

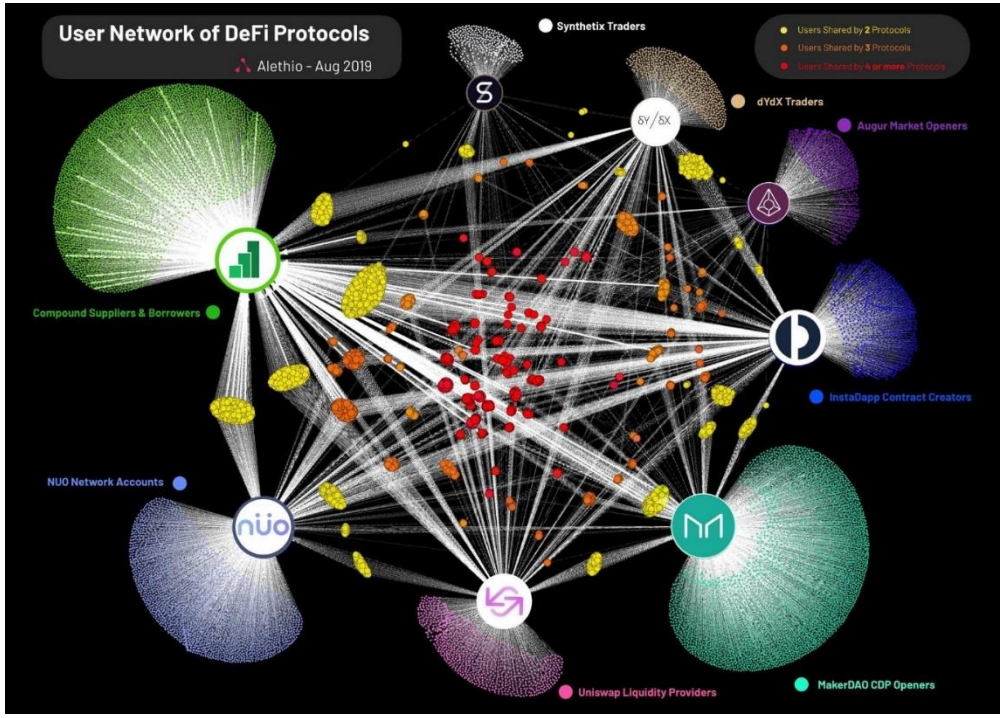
Open Questions

- Expanding strategy space of speculators/attackers
- Understanding governance and oracle risks
- Composability of risks



Open Questions

- Expanding strategy space of speculators/attackers
- Understanding governance and oracle risks
- Composability of risks



- Eventually…learn how to design more crash-resistant systems

Summary

Key takeaways

- Stablecoin collateral consumed faster b/c of deleveraging spirals
- Leads to arbitrage-like trades around liquidations and attack incentives

Summary

Key takeaways

- Stablecoin collateral consumed faster b/c of deleveraging spirals
- Leads to arbitrage-like trades around liquidations and attack incentives

Resources
twitter.com/aklamun
medium.com/@aklamun

Technical foundations
arxiv.org/abs/1906.02152