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

Ariah Klages-Mundt, Andreea Minca

July 26, 2019
P2P Financial Systems, European Central Bank

Problem: No models to understand stablecoin design

- Complex feedback effects
- No truly stable asset easily accessible

This paper: Develop a first model of noncustodial stablecoins

- Dynamic model with feedback effects, yet remains tractable
- Characterize dynamics and liquidity $\implies$ deleveraging spirals
- Analytically show 'stable' and 'unstable' regions
- Explains actual stablecoin movements
- Suggests attacks from speculators and miners
- A foundation for future design study

Focus of the talk:

1. Introduction to stablecoins
2. Motivate how stablecoins are distinct from traditional currency literature

Briefly:

3. Our model
4. Analytical results on dynamics & liquidity
5. Simulation results
6. Motivations for follow-up work

So please refer to the paper (on arXiv) for more in-depth discussion!

Cryptocurrencies

- **Blockchain:** a new way for mistrusting agents to cooperate without trusted third parties
- **Ethereum:** generalized scripting functionality, allowing 'smart contracts' that execute algorithmically in a verifiable and somewhat trustless manner
- **The promise:** cryptographic security, privacy, incentive alignment, reduced counterparty risk
- **A tradeoff:** their price is highly volatile
  - Price tied to network effects, adoption, further technical progress, regulatory hurdles

Introduction to Stablecoins

Aim of stablecoins

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

Types of stablecoins

- **Custodial**: reserve assets held off-chain. E.g., Libra
  - Introduces counterparty risk that cryptocurrencies otherwise solve
- **Noncustodial**: on-chain contracts collateralized in cryptoassets, e.g., MakerDAO's Dai
  - Operate in public/permissionless blockchain setting, in which any agent can pseudonymously participate. Malicious agents can participate, which can introduce new economic attacks

Stablecoin Volatility

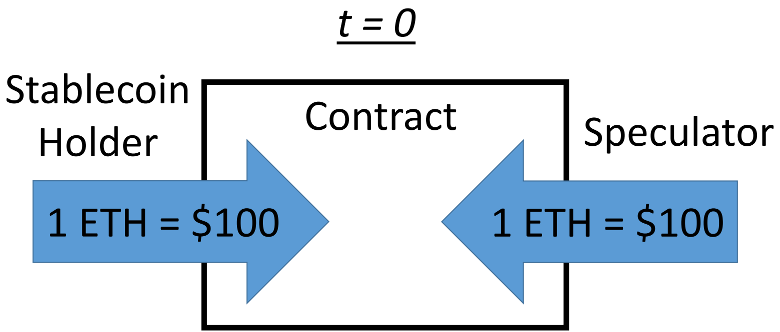
Current stablecoins not robust

- Designs all similar and ad hoc
- Markets can break down during extreme events

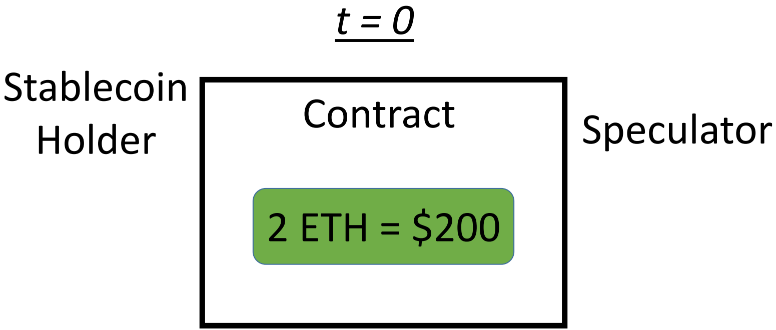
NuBits Charts

bitUSD Charts

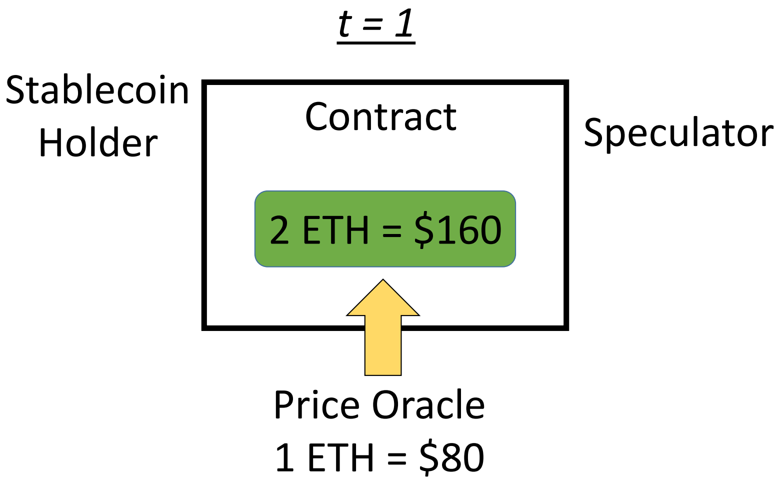
Noncustodial Contract for Difference



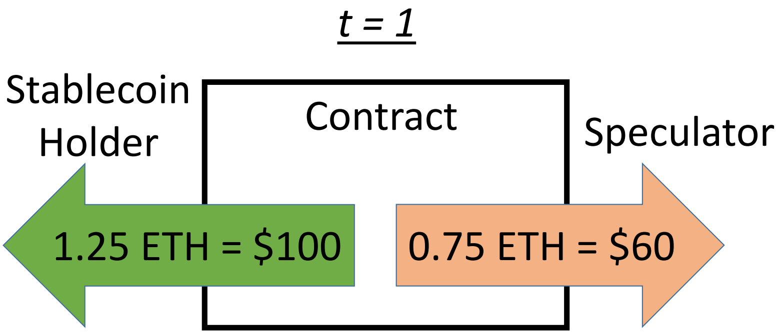
Noncustodial Contract for Difference



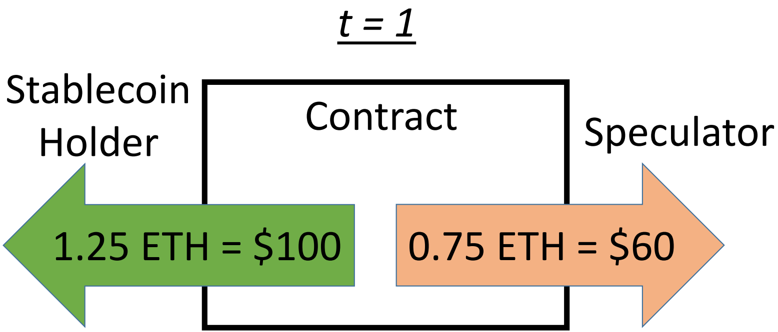
Noncustodial Contract for Difference



Noncustodial Contract for Difference



Noncustodial 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

DStablecoins - no set expiration

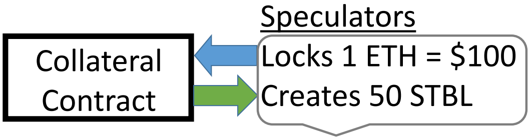
Variants on contracts for difference:

- Tranche-like risk transfer structure
  - Losses/gains borne by speculators, stablecoin holders hold instrument like senior debt
- Oracle provides information from off-chain markets
- Dynamic deleveraging process balances positions according to protocol rules
  - Important difference from CDOs! Critical to understand deleveraging effects
- Agents can change positions through pre-defined process
  - Settlement times are random and dependent on the protocol and agent decisions

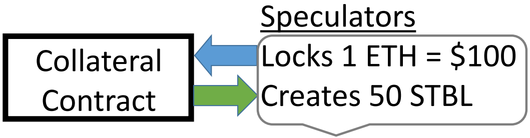
Noncustodial risks

- Risk of market collapse (this paper)
- Oracle/governance manipulation

DStablecoins - no set expiration



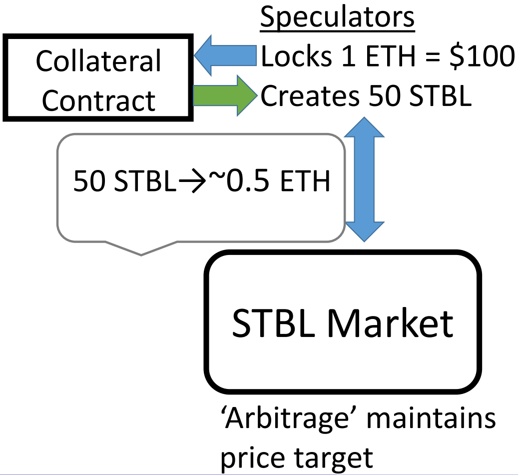
DStablecoins - no set expiration



Speculator Balance Sheet

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

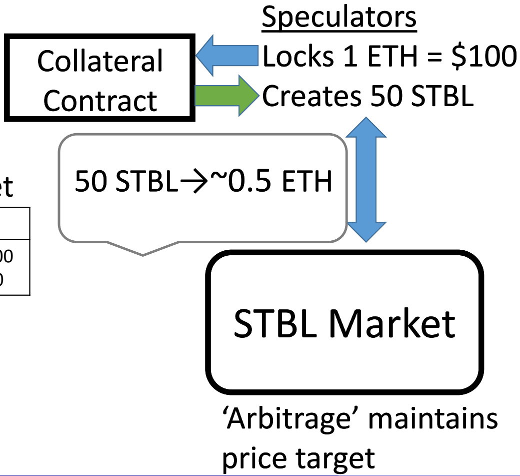
DStablecoins - no set expiration



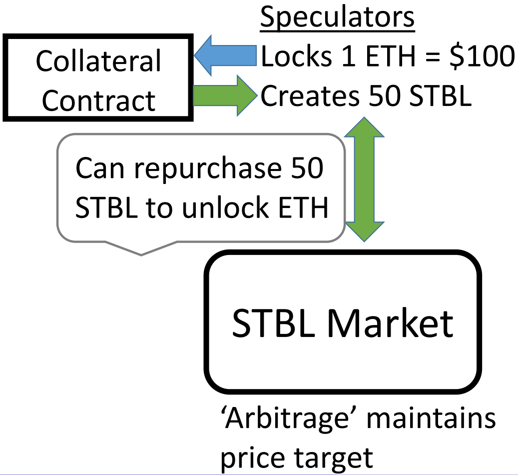
DStablecoins - no set expiration

Speculator Balance Sheet

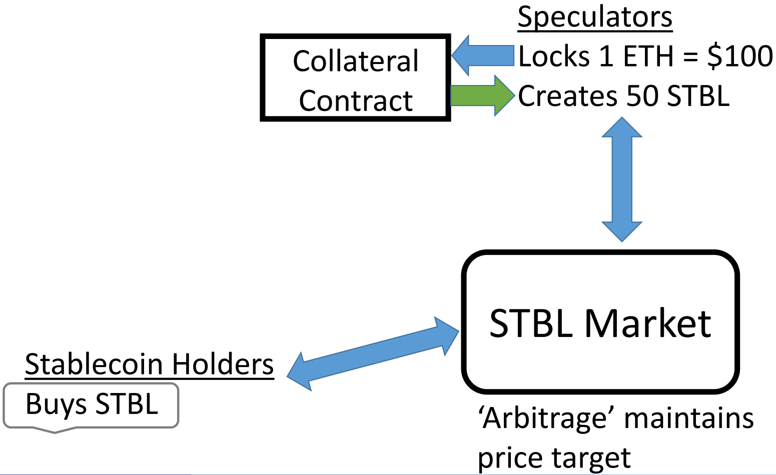
Assets	Liabilities
ETH (pledged) $100 ETH $50	Equity $100 Smart contract $50



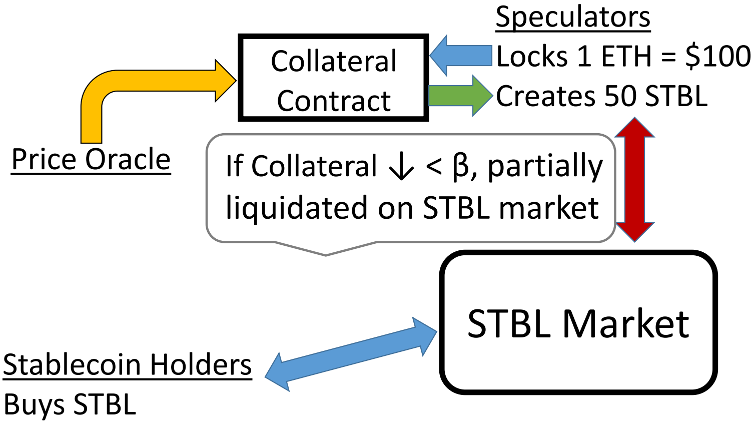
DStablecoins - no set expiration



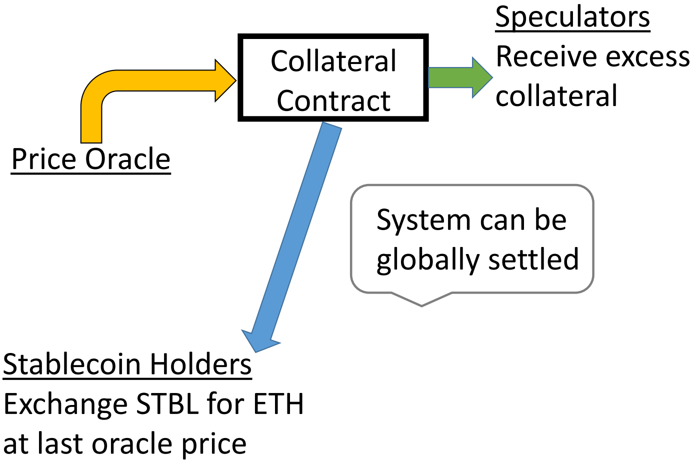
DStablecoins - no set expiration



DStablecoins - no set expiration



DStablecoins - no set expiration



Academic Literature

Work on custodial stablecoins [Lipton et al., 2018], [Griffin et al., 2018]

[Chao et al., 2017] presents a tweaked DStablecoin design that restricts leverage to pre-defined bounds using automated resets

- Stablecoin holders are liquidated from positions during these resets
- Maintaining stablecoin position involves re-buying in at possibly inflated prices at resets

They develop a PDE method to value their proposed stablecoin

- Stability results rely on assumption that payouts are exogenously stable
- Payouts actually made in ETH, not efficiently convertible
- Ignores endogenous price effects from re-buying into stablecoins

Of the many designs, it is unclear which deleveraging method would lead to a system that survives longer

Academic Literature

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

In traditional currency peg models, e.g., [Morris & Shin, 1998]:

- Gov. issuer mechanically committed to stability, not a player in the game

In contrast, in stablecoin systems:

- Issuer role is replaced by decentralized speculators, who issue and withdraw stablecoins to optimize profits. **They are not committed to maintaining a peg.**
- Best we can hope: protocol well-designed and peg maintained whp through incentives
- Agents' decisions affect price of the 'stable' asset and future incentives

Model

Simple model, but versatile, inspired by [Aymanns & Farmer, 2015]

- Dynamic model complex enough to take into account feedback effects
- Agents solve optimization problems consistent with a wide array of documented market behaviors and well-defined financial objectives
- Tractable and modular foundation to build on (can add more features later)
- Provides core of more general simulation environment

Assumption: In this first model, there is no movement out of the blockchain system to fiat

- This actually applies to some agents
- In reality, there is going to be some movement, but it is by nature limited and costly

If relaxed (working on this), the effects in this model might be damped, but probably still exist (and indeed we see evidence in data)

Model

Agents

- **Stablecoin holder** chooses portfolio weights to seek stability
  - Leave generic where possible; assume specific form for some results
- **Speculator** chooses leverage in speculative position behind stablecoin

Assets

- **Ether**: risky asset with exogenous price p_t^E
- **DStablecoin** with endogenous price p_t^D

DStablecoin market clears by setting demand = supply in USD (blackbox stable) terms

- Similar to clearing in Uniswap DEX
- Related to quantity theory of money

Model Outline

$t = 0$: agents have endowment, prior beliefs

In each period t:

1. New Ether price revealed
2. Update Ether expectations
3. Stablecoin holder decides portfolio weights
4. Speculator, seeing demand, decides leverage
5. DStablecoin market is cleared

Rationale

- Sophisticated agents able to front-run DEXs [Daian et al., 2019]
- Evidence demand may not decrease tremendously with price (SBD)

Model: Speculator

Choose Δ_t to maximize next period expected returns s.t. constraints

Liquidation constraint (protocol): $\lambda_t := \frac{\beta \cdot \text{liabilities}}{\text{assets}} \leq 1$

Risk constraint (self-imposed): $\ln \lambda_t = \mu_t - \alpha \sigma_t^b$
VaR example: $\lambda_t \leq \exp(\mu_t - \alpha \sigma_t)$. Consistent with a margin of safety

Δ_t	Change to DStablecoin supply
μ_t	Expected Ether return
σ_t^2	Expected Ether variance
β	Collateral threshold
α	Inverse measure of riskiness
b	Cyclicality parameter

Analytical Results about Dynamics & Liquidity

Proposition

There is a bound to the speculator's ability to maintain the market

(A lower bound on collateral) - (capital available to enter market) must be sufficiently high

Proposition

Speculators face limits to speed of leverage reduction, even w/ new capital.

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

'Stable' and 'Unstable' Regions

Proposition

Assume

- *DStablecoin demand constant*
- *Expected Ether return constant*

Then if the leverage constraint remains inactive, the system converges exponentially to a steady state with stable price and zero variance.

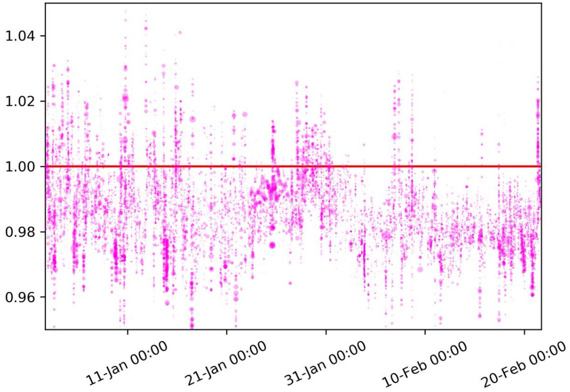
Observation: Steady state may have price $< \$1$.

Conjecture: Outside of 'stable' domain, volatility bounded > 0 whp.

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

These Effects Explain Data from Dai Market

(a) Dai leverage reduction feedback



(b) Dai normally trades below target

Source: Kenny Rowe, Tweet

Simulation: ‘Stable’ and ‘Unstable’ Regions

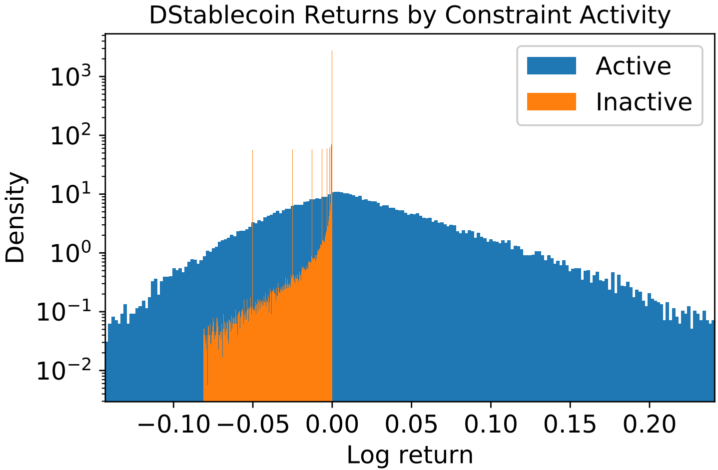
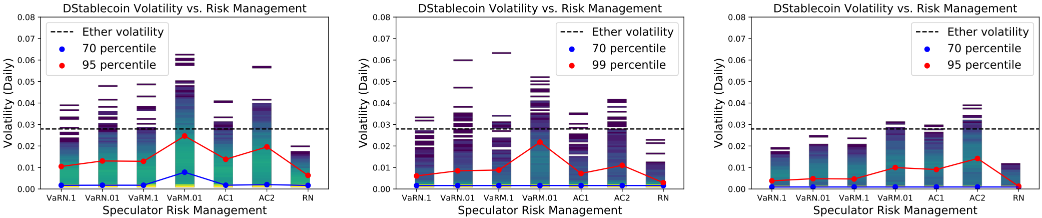


Figure: Constant expected ETH return.

Simulation: Different Speculator Behaviors



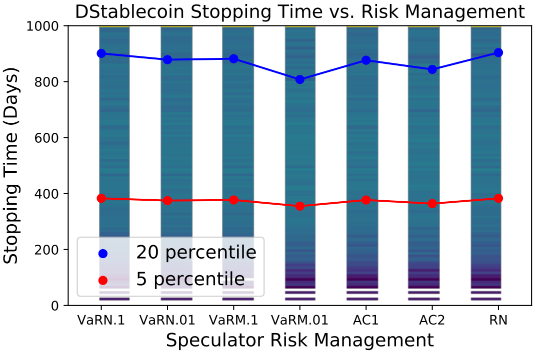
(a) t-distr(df $= 3, \mu = 0$)　(b) t-distr(df $= 3, \mu = r_0$)　(c) normal($\mu = 0$)

Figure: Heatmaps of DStablecoin volatility for different speculator risk management methods.

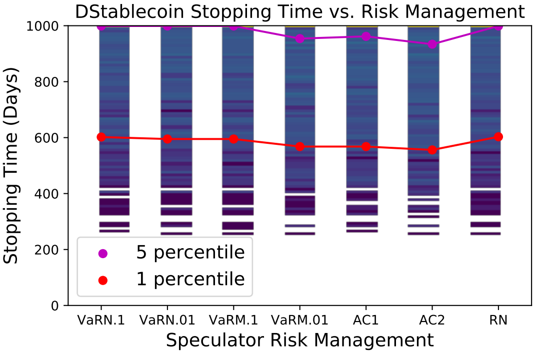
Simulation: DStablecoin Failures

DStablecoin **failure/stopping time** when

1. Speculator's liquidation constraint unachievable, or
2. DStablecoin price remains below $0.5 USD



(a) t-distr(df $= 3, \mu = 0$)



(b) normal($\mu = 0$)

Discussion: A Profitable Economic Attack

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

The attack: Attacking speculator manipulates the market to trigger and profit from spiraling liquidations

This can cause perverse incentives for blockchain miners

- Attack rewards can be > mining rewards
- Miners can censor or reorder transactions to extract value
- Incentive to re-write blockchain to trigger liquidations in present

Discussion: 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

Summary

This paper: Develop a first model of noncustodial stablecoins

1. Dynamic model with feedback effects, yet remains tractable
2. Analytical results
   - Characterize dynamics, liquidity, deleveraging spirals
   - Show 'stable' and 'unstable' regions
   - Explains actual stablecoin movements
3. Simulation results
   1. Support for 'stable' vs. 'unstable' regions
   2. Speculator behavior affects volatility
   3. Failure dominated by collateral returns
4. Discussion
   1. Suggests attacks from speculators and miners
   2. A foundation for future design study