Decentralized Finance

The (Un)Reasonable Design of

Stablecoins

Guest Lecture: Ariah Klages-Mundt
Decentralized Finance

Instructors: Dan Boneh, Arthur Gervais, Andrew Miller, Christine Parlour, Dawn Song
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
### Who Absorbs Risk?

<table>
<thead>
<tr>
<th>Agents</th>
<th>Equities</th>
<th>Protocol Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dai</td>
<td>Duo Network</td>
<td>Gyroscope</td>
</tr>
<tr>
<td>Rai</td>
<td>Iron</td>
<td>Frax</td>
</tr>
<tr>
<td>Liquity</td>
<td>Terra</td>
<td>Celo</td>
</tr>
<tr>
<td>Vai</td>
<td>Steem</td>
<td></td>
</tr>
<tr>
<td>Synthetix</td>
<td>Fei</td>
<td></td>
</tr>
<tr>
<td>bitUSD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nubits</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Asset Backing

<table>
<thead>
<tr>
<th>Exogenous</th>
<th>&lt; Both &gt;</th>
<th>Endogenous</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESD</td>
<td>Basis</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Exogenous
- asset price independent of protocol

### Endogenous
- asset price self-referential with protocol

### Agent
- speculative agents decide, as applicable, risk exposure or issuance

### Algorithmic
- issuance

---

Over past year, many new types of stablecoins...
### Who Absorbs Risk?

<table>
<thead>
<tr>
<th>Agents</th>
<th>Exogenous</th>
<th>&lt; Both &gt;</th>
<th>Endogenous</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dai</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rai</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Liquity</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vai</td>
<td>Synthetix</td>
<td>bitUSD</td>
<td>Nubits</td>
<td></td>
</tr>
</tbody>
</table>

### Asset Backing

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

---

**Over past year, many new types of stablecoins...**

<table>
<thead>
<tr>
<th>Equity Token</th>
<th>Protocol Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Duo Network</strong></td>
<td><strong>Gyroscope</strong></td>
</tr>
<tr>
<td><strong>Iron</strong></td>
<td><strong>Synthetix</strong></td>
</tr>
</tbody>
</table>

**Issuance**

- **Agent**
- **Algorithmic**
Over past year, many new types of stablecoins...
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

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
  - Central Bank
    - Currency Models

- Non-Custodial
  - Bank fund
    - Bank run models
  - Money Market Fund
    - Pegged money market funds
Risk-based Overview

Stablecoin

Custodial
- Reserve Fund
- Fractional Reserve Fund
- Central Bank
  - Bank fund
  - Money Market Fund

Non-Custodial
- Exogenous Collateral: Market deleveraging risks
- Endogenous Collateral: Amplified feedback effects
- Implicit Collateral: Incentive w/o obligation
Anatomy of Non-custodial Stablecoins

Collateral Value

- Exogenous
- Endogenous
- Implicit/none
Anatomy of Non-custodial Stablecoins

- Collateral Value
- Risk Absorption
  - Equity
  - Agent
  - Protocol
## How Risk is Absorbed

<table>
<thead>
<tr>
<th>• Leverage-based: like a CDO</th>
</tr>
</thead>
<tbody>
<tr>
<td>• w/ exogenous or endogenous collateral</td>
</tr>
<tr>
<td>• Seigniorage shares: market cap of endogenous “equity shares” meant to absorb volatility</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>• Basis design: speculators meant to maintain peg by betting on future supply expansions (leverage on “implicit collateral”) during a crisis</th>
</tr>
</thead>
<tbody>
<tr>
<td>• No pre-committed collateral</td>
</tr>
<tr>
<td>• Speculators must bet that supply will expand beyond pre-crisis level</td>
</tr>
</tbody>
</table>

| • Reserve-backed: protocol market makes around peg using internal reserve |

...also various meta-stablecoins
Anatomy of Non-custodial Stablecoins

Collateral Value

Issuance

Risk Absorption

Agent-based
Algorithmic
Deleveraging process
Anatomy of Non-custodial Stablecoins

- Collateral Value
- Risk Absorption
- Issuance
- Governance
- Price Feed

- Stablecoin Holders
- Miners
Parallels & Differences

**Dai**
- MKR Governance
  - Profit-optimizing
- Vaults
  - Risk absorption
  - Issuance of endogenous ‘stable’ asset
- Dai Holders

... Requires new models...

**Traditional Money**
- Central Bank
  - Stability-seeking
- Commercial Banks
  - Issuance of assumed stable asset
- Depositors
# Non-custodial Stablecoins in 3D

<table>
<thead>
<tr>
<th>Who Absorbs Risk?</th>
<th>Asset Backing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Exogenous</td>
</tr>
<tr>
<td>Agents</td>
<td>Dai</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Equity Token</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duo Network</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protocol Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gyroscope</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Issuance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
</tr>
<tr>
<td>Algorithmic</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Who Absorbs Risk?</th>
<th>Asset Backing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Exogenous</td>
</tr>
<tr>
<td>Agents</td>
<td></td>
</tr>
<tr>
<td>Dai</td>
<td></td>
</tr>
<tr>
<td>Rai</td>
<td></td>
</tr>
<tr>
<td>Liquity</td>
<td></td>
</tr>
<tr>
<td>Vai</td>
<td></td>
</tr>
<tr>
<td>Synthetix</td>
<td></td>
</tr>
<tr>
<td>bitUSD</td>
<td></td>
</tr>
<tr>
<td>Nubits</td>
<td></td>
</tr>
<tr>
<td>Basis</td>
<td></td>
</tr>
</tbody>
</table>

#### Equities

- **Duo Network**
- **Iron**
- **Terra**
- **Steem**

#### Protocol Assets

- **Gyroscope**
- **Fei**
- **Frax**
- **Celo**

**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

https://defi-learning.org
---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
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

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

(In)Stability for the Blockchain, 2019
Stablecoins 2.0, 2020
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

**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

Oracle price feed

Timeline 1
Economic Attacks

- Oracle price feed
- Liquidations

Timeline 1
Economic Attacks

Oracle price feed

Liquidations

Timeline 1

Timeline 2
Economic Attacks

Oracle price feed

Liquidations

Timeline 1

Timeline 2
Economic Attacks

Oracle price feed

Liquidations

Timeline 1

Timeline 2
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
MEV: Forking Models

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

**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
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**

\[
\max_{\delta \in [0,1]} \mathbb{E} \left[ \delta F + \kappa \right] \\
\text{s.t.} \quad F \text{ is vault choice}
\]

**Vault choice**

\[
\max_{F \geq 0} \mathbb{E} [NR + F(Bb - \delta)] \\
\text{s.t.} \quad F \leq \beta N \\
\quad u \leq \mathbb{E} [NR + F(Bb - \delta)] \\
\quad B = \mathbb{E} \left[ U \left( \frac{1}{F} \min(F, N(1 + R) - \delta F) \right) \right]
\]

**Governance problem:** decide interest rate \( \delta \) 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
**Problem 2: Governance attack vector**

Governance choice

\[
\begin{align*}
\max_{\delta \in [0,1]} & \quad \mathbb{E}\left[(1-d)(\delta F + \kappa)\right] \\
\text{s.t.} & \quad d = \mathbb{1}_{(yN(1+R) > \xi(\delta F + \kappa) + \alpha)} \\
& \quad F \text{ is vault choice}
\end{align*}
\]

Vault choice

\[
\begin{align*}
\max_{N,F \geq 0} & \quad \mathbb{E}\left[(N - N)R + (1-d)NR + F(Bb - \delta) - dN(1+R)\right] \\
\text{s.t.} & \quad F \leq \beta N \\
& \quad 1_{(N > 0)} u \leq \mathbb{E}[F(Bb - \delta) - d\gamma N(1+R)] \\
& \quad B = \mathbb{E}\left[U\left(\frac{1}{F} \min\left(F, (1 - \gamma d)(N(1+R) - \delta F)\right)\right)\right] \\
& \quad d = \mathbb{1}_{(yN(1+R) > \xi(\delta F + \kappa) + \alpha)} \\
& \quad 0 \leq N \leq \bar{N}
\end{align*}
\]

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

**Governance problem:** decide interest rate $\delta$ and attack decision $d$ to maximize revenue subject to vault’s issuance decision

**Vault problem:** decide issuance $F$ to maximize expected return from leverage subject to constraints, factoring in attack possibility
Problem 3: Collusion attack vector

- 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 $\delta$ 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 $\sim$ geometric sum of discounted fees
• If small relative to collateral, need high $\alpha$ for security
• ‘Price of anarchy’ = extra cost to secure decentralized system vs. centralized (high $\alpha$)

Conjecture:
In fully decentralized stablecoins ($\alpha=0$) 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 $\rightarrow$ 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

https://defi-learning.org
CDO Structure

A portfolio of underlying assets
CDO Structure

Split into 2 tranches

Junior tranche = more risky

Senior tranche = less risky
Losses that occur are first borne by junior tranche

Senior tranche protected
Stablecoin CDO-like Structure

~ Risk Absorbers

~ Stablecoin Holders
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

\[ \bar{N}_t X_t \geq \beta L_t \]

Price of ETH \quad Stablecoins “borrowed”

Amount of ETH \quad Collateral factor
Model: Speculator

**Decision:** Change stablecoin supply to maximize next period expected returns

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

\[
Y_t = N_{t-1} X_t - L_{t-1} - \text{liquidation effect}
\]

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

- $1

Price

Demand = Supply

Collateral
Deleveraging Spiral

- $1

Price

Demand

≠

Supply

Liquidation

Collateral
Deleveraging Spiral

Price - $1

Demand ≠ Supply

Liquidation

Collateral
Deleveraging Spiral

- $1

Price

Demand

Supply

Liquidation

Collateral
Deleveraging Spiral – Round 2

- $1

Price

Demand ≠ Supply

2^{\text{nd}} \text{ Liquidation}

Collateral
Deleveraging Spiral – Round 2

- Price: $1

Demand ≠ Supply

2nd Liquidation

Collateral
Deleveraging Spiral – Round 2

- $1

Price

Demand

Supply

2nd Liquidation

Collateral
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

~50% ETH price crash

Liquidation price effect on Dai DEX trades

Source: dai.stablecoin.science
Non-custodial Complications

• No stable region when $X_t$ is not $\sim$ 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

---

**Diagram:**

- LUSD Price
- LUSD-3CRV Swaps

“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

Asset backing (tangible)  Economic usage (intangible)

$1 target

Peg sustained!
What Backs a Currency Peg?

A shock to one of these...

Asset backing (tangible)  Economic usage (intangible)

$1 target
A shock to one of these...

What Backs a Currency Peg?

*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

User pays $1 for new stablecoin

Where does $1 go?

- Pockets of stakeholders
- Part to Stakeholders, Part to Reserve
- 100% to Reserve

What happens in crisis?

- No value retained by system. Speculators must bet on future demand growth and abandon this when this becomes uncredible.
- Reserve small, less stabilizing. Prone to bank runs and Soros attacks
- Stronger, more stabilizing b/c more value retained to handle crisis

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

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

- E.g., Soros attack on GBP
- Studied in international finance literature (e.g., Morris and Shin, 1998)
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

Implicit Fei Redemption Curve, Reserve Ratio = 100%

![Graph showing implicit redemption curve with and without direct incentives. The curve is steep, starting at $1.00 and dropping sharply to $0.20 as the redemption level increases from 0% to 30% of supply. There is another curve showing the redemption without direct incentives, which is less steep.](image)
Case Study 4: Seigniorage shares

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

Price

All liquidity at $1...

Redemption Amount

...until liquidity is exhausted

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

Redemption Curve, Reserve Ratio = 100%

Redeem Quote vs Redemption level (% of supply)
Designing Autonomous Primary Markets

Redemption Curve, Reserve Ratio = 80%

Redeem Quote

Redemption level (% of supply)
Designing Autonomous Primary Markets

 Redemption Curve, Reserve Ratio = 90%

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


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


**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/](https://gyro.finance/)