

STABLE CRYPTOCURRENCIES

-

FIRST ORDER PRINCIPLES

Craig Calcaterra,* Wulf A. Kaal,** and Vadhindran Rao ***

Abstract

The emergence and proliferation of stable cryptocurrencies necessitate the establishment of first order design principles for stable cryptocurrencies. After highlighting the benefits of stable cryptocurrencies for monetary policy making, overall market stability, and their impact on the emergence of decentralized commerce, the authors introduce First Order Principles for stable cryptocurrency design and their essential functions. The core design features and their interoperative feedback effects revolve around: (1) burning coins through bonds vs. reserves, (2) transaction vs. holding taxes, (3) repegging, and (4) governance.

Key Words: Stable Cryptocurrencies, Liquidity, Corruption, Cost, Speculation, Inflation, Price Stability, Transparency, Feedback Effects, Market Stability, Stability Mechanisms, Monetary Policy, Emerging Technology, Crypto Economics, Token Models, Incentive Design, Velocity, Supply, Demand, Tokens, Blockchain, Distributed Ledger Technology

JEL Categories: K20, K23, K32, L43, L5, O31, O3

* Professor of Mathematics, Metropolitan State University (*Minneapolis, USA*)

** Professor of Law, *University of St. Thomas School of Law (Minneapolis, USA)*

*** Professor of Finance, Metropolitan State University (*Minneapolis, USA*)

Table of Contents

1	INTRODUCTION	2
2	BACKGROUND.....	7
3	FIRST ORDER PRINCIPLES FOR STABLE CRYPTOCURRENCIES.....	14
3.1	CURRENCY MINTING AND BURNING	14
3.1.1	<i>Minting</i>	15
3.1.2	<i>Burning</i>	16
3.2	TRANSACTION TAXES VS. HOLDING TAXES	22
3.3	REPEGGING.....	23
3.4	GOVERNANCE.....	24
3.4.1	<i>Features Subject to Monetary and Fiscal Policy</i>	24
3.4.2	<i>Communication Design</i>	25
3.4.3	<i>Ultimate Power</i>	25
3.4.4	<i>Transcendental Values</i>	27
4	CONCLUSION.....	28

1 INTRODUCTION

Stable cryptocurrencies have been defined as: “a type of cryptocurrency that is designed to maintain a stable value, rather than experiencing significant price changes.”¹ Others define it as: “a new class of cryptocurrencies which offer price stability and/or are backed by reserve asset(s), [combining] the instant processing and security of payments of cryptocurrencies, and the volatility-free stable valuations of fiat currencies.”²

A currency which maintains a stable store of value is more efficient for an economy than one which does not. Neither the renter nor the landlord should sign a contract if its value might halve or double in any given month. A fluctuating currency requires continual recalculation and renegotiation. Therefore, any future decentralized economy will require stable cryptocurrencies.

Since their inception in 2014 with Tether,³ stable cryptocurrencies have primarily been used as a cash equivalent for cryptocurrency portfolios. In 2019, stable cryptocurrencies have grown substantially in popularity as an answer to the high volatility associated with the cryptocurrency markets.⁴ Depending on their design, they can offer additional features such as transparency, privacy, and increased decentralization. Stable cryptocurrencies can also offer lower fees and faster transaction speeds, making them rather useful for international transactions and everyday payments.

¹ *Stablecoin*, BINANCE ACADEMY, <https://www.binance.vision/glossary/stablecoin> (last visited Apr. 24, 2019).

² *Stablecoin*, INVESTOPEDIA (rev'd Shobhit Seth, Sep. 19, 2018), <https://www.investopedia.com/terms/s/stablecoin.asp>.

³ Pete Rizzo, *Realcoin Rebrands as 'Tether' to Avoid Altcoin Association*, COINDESK (Nov. 20, 2014, 12:01 PM), <https://www.coindesk.com/realcoin-relaunches-tether-avoid-altcoin-association>.

⁴ *Stablecoin*, BINANCE ACADEMY, <https://www.binance.vision/glossary/stablecoin> (last visited Apr. 24, 2019).

The evolution of stable cryptocurrencies creates a new opportunity to reexamine earlier decades of monetary policy making and scholarship. In particular, it allows an expansion and reexamination of the quantity theory of money and associated models. In 2014, Robert Sams introduced the first attempt at creating a stability mechanism for cryptocurrencies.⁵ Sams's early academic attempt was quickly followed by commercial applications and expansions of his earlier vision.⁶

In 2019, the leading notable stable cryptocurrency startups and their respective approaches include: Ampleforth,⁷ Paxos Standard Token

⁵ Robert Sams, *A Note on Cryptocurrency Stabilisation: Seigniorage Shares*, BRAVE NEWCOIN (Apr. 28, 2015), <https://assets.ctfassets.net/sdIntm3tthp6/resource-asset-r390/5a940afb21681d19c0b3b76cf69259e1/58ebe9e2-1f28-4a8d-8ce1-26abef07aedef.pdf>.

⁶ See, e.g., Smith + Crown, *The Cryptoeconomics of Seigniorage Shares Stablecoins: Basis and Carbon* (May 28, 2018), <https://www.smithandcrown.com/cryptoeconomics-seigniorage-shares-look-basis-carbon/> (Basis's design and expansion of Sams 2014).

⁷ P.H. Madore, *Crypto Firm Fragments Launches Stablecoin Following 'Ampleforth' Rebrand*, CCN.COM: News (Nov. 12, 2018), <https://www.ccn.com/crypto-firm-fragments-launches-stablecoin-following-ampleforth-rebrand>.

(PAX),⁸ Gemini Dollar (GUSD),⁹ TrueUsd (TUSD),¹⁰ Circle's CENTRE consortium (USD-C),¹¹ Facebook's Stablecoin launch,¹² and of course, Tether,¹³ among several others.

⁸ Josiah Wilmoth, *Paxos Standard: Why the Stablecoin You've Never Heard of Just Might Take Down Tether*, CCN.COM: ALTCOIN NEWS (Feb. 12, 2018), <https://www.ccn.com/paxos-standard-why-the-stablecoin-youve-never-heard-of-just-might-take-down-tether>.

⁹ Jack Mathis, *Gemini's New USD Cryptocurrency Stablecoin: A Whitepaper Deep Dive*, CCN.COM: ALTCOIN NEWS (Dec. 09, 2018), <https://www.ccn.com/geminis-new-usd-cryptocurrency-stablecoin-a-whitepaper-deep-dive>; see also Jeff Kauflin et al., *The Most Innovative Fintech Companies in 2019*, FORBES.COM (Feb. 4, 2019, 10:00 AM), <https://www.forbes.com/fintech/2019/#4da63f0f2b4c>.

¹⁰ COINTOPPER, *Tether(USDT) Vs TrueUSD(TUSD): Which Stablecoin is Better?* (Sep. 5, 2018), <https://cointopper.com/guides/tetherusdt-vs-trueusdtusd-which-stablecoin-is-better>; see also Bloomberg, *Love Crypto But Not Its Volatility? Meet Stablecoins*, FORTUNE.COM (Jan. 30, 2019), <http://fortune.com/2019/01/30/stablecoins-bitcoin-cryptocurrency/>; P.H. Madore, *Exclusive: TrueUSD Partners with Nexo to Provide Holders with Instant Loans on Cryptocurrency*, CCN.COM: EXCLUSIVE (Dec. 19, 2019), <https://www.ccn.com/exclusive-trueusd-partners-with-nexo-to-provide-holders-with-instant-loans-on-cryptocurrency>.

¹¹ CRYPTOGLOBE *Stablecoin Guide: Why are Stablecoins so Important to Crypto Markets?* (Oct. 11, 2018), <https://www.cryptoglobe.com/latest/2018/10/stablecoin-guide-why-are-stablecoins-so-important-to-crypto-markets/>.

¹² Nathaniel Popper & Mike Isaac, *Facebook and Telegram are Hoping to Succeed Where Bitcoin Failed*, N.Y. TIMES, Feb. 28, 2019, at B1;

see also Linas Kmieliauskas, *Facebook is Already Pitching its Stablecoin to Exchanges – Report*, CRYPTONEWS (Mar. 01, 2019), <https://cryptonews.com/news/facebook-is-already-pitching-its-stablecoin-to-exchanges-rep-3453.htm>.

¹³ Nikhilesh De, *Tether to Launch New Version of USDT Stablecoin on Tron Blockchain*, COINDESK (Mar. 4, 2019, 12:01 PM),

Existing projects fall into two broad categories, e.g. collateralized and uncollateralized tokens. Both are subject to significant downsides. Collateralized projects use either fiat currencies or cryptocurrencies as collateral. Collateralized fiat currency pegs bear the brunt of expensive capital requirements and uncollateralized cryptocurrency pegs face heavy volatility pressures and swings.

Most stable cryptocurrency projects that claim to be collateralized with fiat currency claim to be 100% backed. Without a 100% fiat collateralization, such projects would run the risk of arbitrage trade attacks similar to what Financier George Soros used to “break the bank of England”.¹⁴ Fiat currency collateralization is expensive and inefficient because all of the value that is backing the cryptocurrency needs to be liquid, otherwise arbitrage opportunities, such as the Soros attack, are possible. Therefore, the price tag of fiat-backed tokens is, at a minimum, the interest rate of the pegged fiat currency.¹⁵

Cryptocurrency-backed tokens, are even more expensive, because the stability is achieved with the (currently) much more unstable cryptocurrencies. Any cryptocurrency-backed token must be backed with much more than 100% of the current value of the cryptocurrency in case the basket of other crypto currencies’ value drops. For example, in

<https://www.coindesk.com/tether-to-launch-new-version-of-usdt-stablecoin-on-tron-blockchain>; see also Carlo C., *Tether Brings Benefits of P2P Transactions to Fiat Currency Transfers*, COINTELEGRAPH (Nov. 22, 2014), <https://cointelegraph.com/news/tether-brings-benefits-of-p2p-transactions-to-fiat-currency-transfers>.

¹⁴ Devansch Lathia, *How Soros Broke the British Pound*, ECON. REV. AT NYU (Oct. 16, 2018), <https://theeconreview.com/2018/10/16/how-soros-broke-the-british-pound/>.

¹⁵ See generally, Becky Leighton, *What is a Fiat-backed Stablecoin?*, COIN INSIDER (Feb. 6, 2019), <https://www.coininsider.com/what-is-a-fiat-backed-stablecoin/> (“As the name implies, fiat stablecoins are tokens which are associated with the value of a particular fiat currency. Usually, these tokens are based on the US dollar and hold their value fixed at a 1:1 ratio.”).

MakerDAO, if a token is backed by Ether, and Ether drops by half at any moment, then the automated scheme will punish anyone who has not backed their tokens by more than 200%.¹⁶

The uncollateralized schemes include (formerly) Basis and NuBits, which follow the quantity theory of money,¹⁷ algorithmically minting and burning tokens in order to maintain a peg.¹⁸ At the time of this writing no uncollateralized algorithmic project had created a provable stable mechanism for its tokens.

This paper outlines the First Order Principles for stable cryptocurrency projects. The authors emphasize the functioning and interplay between 1. Burning coins through bonds vs. reserves, 2. Transaction vs. holding taxes, 3. Reserves, and 4. Governance.

¹⁶ MAKERDAO, *The Dai Stablecoin System*, <https://makerdao.com/en/whitepaper> (last visited Apr. 25, 2019).

¹⁷ The quantity theory of money predicts that money growth should be neutral in the long run in its effects on the growth rate of production and should affect the inflation rate on a one-for-one basis. In David Hume's pioneering essays of 1752, *Of Money and Of Interest*, Hume stressed that changes in the number of units of money in circulation will have proportional effects on all prices that are stated in money terms. In turn, Hume suggests that changes in the number of units of money in circulation have no effect on economic output, e.g. on how much people produce or on the goods they produce or consume. The quantity theory of money has evolved dramatically since the beginnings of modern monetary theory in Hume's pioneering essay. David Hume, *Of Money and of Interest*, in *WRITINGS ON ECONOMICS* (Eugene Rotwein ed.1970).

¹⁸ Nader Al-Naji, Josh Chen & Lawrence Diao, *Basis: A Price-Stable Cryptocurrency with an Algorithmic Central Bank*, BASIS.IO (Jun. 20, 2017), https://www.basis.io/basis_whitepaper_en.pdf; Jordan Lee, *Nu*, NUBITS.COM (Sep. 23, 2014), <https://nubits.com/NuWhitepaper.pdf>.

2 BACKGROUND

A growing body of evidence suggests that stable cryptocurrencies may play a role in the world economy. In 2018, the IMF estimated that 11 countries are at 20% or higher inflation.¹⁹ Using black market exchange rates measured weekly, the Cato Institute's Troubled Currencies Project estimates that the real rates are significantly higher than the IMF estimates.²⁰ Currency devaluation is rampant in many countries, e.g. Venezuela (2018: -99%), Argentina (2018: -53.2%), Turkey (2018: -38.4%), and Brazil (2018: -20.6%).²¹ In the United States, transacting in cash costs the consumer around 200 billion dollars annually - about \$637 per person.²² The cost of cash is primarily associated with counting,

¹⁹ International Monetary Fund, *Inflation Rate, Average Consumer Prices Annual Percent Change*, IMF DATA MAPPER, <https://www.imf.org/external/datamapper/PCPIPCH@WEO/OEMDC/ADVEC/WEOWORLD>

²⁰ Steve Hanke & Hal Boger, *Inflation by the Decades: Full Dataset*, CATO, (2018), <https://object.cato.org/sites/cato.org/files/troubled-currencies-project-site/inflation-by-the-decades-full-data-set.xlsx>. According to the Troubled Currencies Project, which is a joint project with Johns Hopkins University, six countries are experiencing over 100% annual inflation. *Id.*

²¹ Brian Ellsworth & Girish Gupta, *Venezuela Announce 99.6 Percent Devaluation of Official Forex Rate*, REUTERS (Feb. 5, 2018, 5:25 PM), <https://www.reuters.com/article/us-venezuela-economy/venezuela-announces-99-6-percent-devaluation-of-official-forex-rate-idUSKBN1FP2WK>; Sam Meredith, *Argentina's Peso has Now Fallen 52% Against the Dollar this Year*, CNBC (Aug. 31, 2018), <https://www.cnbc.com/2018/08/31/argentinas-peso-has-fallen-108percent-against-the-dollar-so-far-this-year.html>; Roger Aitken, *Turkish Lira 'Currency Crisis' Not Over, Could Hit 8 Against U.S. Dollar*, FORBES (Aug 16, 2018), <https://www.forbes.com/sites/rogeraitken/2018/08/16/turkish-lira-currency-crisis-not-over-could-hit-8-against-u-s-dollar/#472187cd2301>; Lise Alves, *With Depreciation of Currency, Brazilians Spend Less Abroad*, THE RIO TIMES (Dec. 24, 2018), <https://riotimesonline.com/brazil-news/rio-business/with-depreciation-of-currency-brazilians-spend-less-abroad>.

²² Jonathan Brugge, Olivier Denecker, Hamza Jawaaid, Andras Kovacs, & Ibrahim Shami, *Attacking the Cost of Cash*, MCKINSEY & COMPANY (Aug. 2018), <https://www.mckinsey.com/industries/financial-services/our-insights/attacking-the-cost-of-cash>.

managing, storing, transporting, guarding, and accounting for bank notes.²³ The theft of cash alone costs U.S. retail businesses lose around \$40 billion annually.²⁴ Similarly, according to one study, one in every \$12,400 of cash notes printed may be counterfeit.²⁵ The effect of corruption on economic welfare is significant.²⁶ More corrupt countries also experience significantly lower rates of investment in the respective country.²⁷ Corrupt countries are also subject to a significantly higher inflation rate.²⁸ Several studies demonstrate that the poor and those

²³ Aleksander Berentsen and Fabian Schar, *The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies*, Federal Reserve Bank of St. Louis Review, Second Quarter 2018, pp. 97-106. <https://doi.org/10.20955/r.2018.97-106>.

²⁴ Will Yaowicz, *Cash Costs U.S. Businesses \$40 Billion a Year*, <https://www.inc.com/will-yakowicz/dealing-with-cash-costs-american-businesses-55-billion.html> (last visited April 24, 2019).

²⁵ *Costs of Keeping Ahead of Counterfeiters*, FEDERAL RESERVE BANK OF RICHMOND, (December 2009), https://www.richmondfed.org/-/media/richmondfedorg/banking/payments_services/understanding_payments/pdf/costs_counterfeiters.pdf; Ruth Judson and Richard Porter, *Estimating the Worldwide Volume of Counterfeit U.S. Currency: Data and Extrapolation*, DIVISION OF MONETARY AFFAIRS, BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, (2003), <http://www.federalreserve.gov/pubs/FEDS/2003/200352/200352pap.pdf>.

²⁶ See Andrei Shleifer & Robert W. Vishny, *Corruption*, QUARTERLY JOURNAL OF ECONOMICS, August 1993.

²⁷ Aymo Brunetti, Greogory Kisunko & Beatrice Weder di Mauro, *Credibility of Rules and Economic Growth: Evidence from a Worldwide Survey of the Private Sector*, 12 WORLD BANK ECONOMIC REVIEW 353, 353-84 (1998); Aymo Brunetti & Beatrice Weder di Mauro, *Investment and Institutional Uncertainty: A Comparative Study of Different Uncertainty Measures*, 134 REVIEW OF WORLD ECONOMICS 513, 513-33 (1998); Johann Graf Lambsdorff, *How Corruption Affects Productivity*, 56 KYKLOS 457, 457-74 (2003);

²⁸ Fahim Al-Marhubi, *Export Diversification and Growth: An Empirical Investigation*, 7 APPLIED ECONOMICS LETTERS 559, 559-62 (2000).

with less access to institutions bear a disproportionate share of these costs of using cash.²⁹

Cash and bank notes are gradually losing ground to other payment systems.³⁰ Whereas the overwhelming majority of humans live in cash economies where at least 90% of transactions are conducted in cash, consumers in wealthier economies tend to favor noncash alternatives.³¹ Cash usage in the United States, the United Kingdom, the Netherlands, Sweden, Finland, Canada, France, among other industrialized nations, has fallen well below 50% of total transaction volume.³² Most significantly, in Northern Europe as few as one in every five transactions are made in cash.³³

Central banks and governments around the world have been experimenting with government-sponsored digital and cryptocurrencies since 2015.³⁴ In the case of central banks, such experimentation is

²⁹ *Id.*

³⁰ KENNETH S. ROGOFF, *THE CURSE OF CASH*, (Princeton University Press, 2016); Jonathan Brugge, Olivier Denecker, Hamza Jawaid, Andras Kovacs, & Ibrahim Shami, *Attacking the Cost of Cash*, MCKINSEY & COMPANY (Aug. 2018), <https://www.mckinsey.com/industries/financial-services/our-insights/attacking-the-cost-of-cash>.

³¹ *Id.*

³² “Germany, Japan, and Austria stand apart as wealthy countries where consumers maintain a strong preference for cash at the point of sale, despite universal availability of electronic payments instruments and the broad adoption of electronic transfers for recurring payments.” *Id.*

³³ *Id.*

³⁴ Dr. Garrick Hileman & Michel Rauchs, *Global Cryptocurrency Benchmarking Study*, (2017), https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/global-cryptocurrency/#.XMHF_xNKhTY; Yves Mersch, Member of the Executive Board of the European Central Bank, at the Central Bank of Malaysia Monetary Policy Conference (July 24, 2017)(transcript available <https://www.bis.org/review/r170807c.htm>); *Digital Currency Initiative*, MIT

already close to launch³⁵ or fully operational.³⁶ Several governments have issued their own digital currencies. Most major tech companies in the private sector have been experimenting with cryptocurrency projects since 2017. Examples include Tunisia (eDinar),³⁷ Venezuela (Petro),³⁸

MEDIA LAB, <https://dc.mit.edu/>; *Financial Stability Review 2017*, MONETARY AUTHORITY OF SINGAPORE, <http://www.mas.gov.sg/Regulations-and-Financial-Stability/Financial-Stability/2017/Financial-Stability-Review-2017.aspx>; Jack Meaning, Ben Dyson, James Barker & Emily Clayton, *Broadening narrow money: monetary policy with a central bank digital currency*, (Bank of England, Staff Working Paper No. 724, May 2018); J.P. Koning, *Fedcoin: A Central Bank-Issued Cryptocurrency*, R3 REPORT 15 (2016); Sina Motamedi, *Will Bitcoins Ever Become Money? A Path to Decentralized Central Banking*, TANNUTUVA.ORG (July 21, 2014), <https://tannutuva.org/2014/will-bitcoins-ever-become-money-a-path-to-decentralized-central-banking/>.

³⁵ The Bank of Canada and bank of England announced in 2016 that the technology was not ready for a central bank sponsored crypto currency. Yet, other central banks, such as in Singapore and Sweden have already launched their e-currency projects. Morten Bech & Rodney Garratt, *Central Bank Cryptocurrencies*, BIS QUARTERLY REVIEW 66-67, September 2017, available at SSRN: <https://ssrn.com/abstract=3041906>.

³⁶ Usman W. Chohan, *Cryptocurrencies as Asset-Backed Instruments: The Venezuelan Petro*, (February 7, 2018), available at SSRN: <https://ssrn.com/abstract=3119606>. Venezuela's oil token. Bruce Zagaris, *U.S. Bans Venezuela's New Crypto-Currency and Adds 3 Officials to Sanctions List*, 34 NO. 4 INT'L ENFORCEMENT L. REP. 157, 157-161 (2018); Julie Hirschfeld Davis & Nathaniel Popper, *White House Bans Venezuela's Digital Currency and Expands Sanctions*, THE NEW YORK TIMES, (March 19, 2018), <https://www.nytimes.com/2018/03/19/world/americas/trump-venezuela-sanctions-petro.html>.

³⁷ Richard Kastelein, *Tunisia to Replace Its National Digital Currency, eDinar, With Blockchain-Driven Monetas Currency*, BLOCKCHAIN NEWS (Dec. 28, 2015), <https://www.the-blockchain.com/2015/12/28/tunisia-to-replace-its-national-digital-currency-edinar-with-blockchain-driven-monetas-currency/>

³⁸ Ryan Browne, *Venezuela About to Pre-Sell 'Petro' Cryptocurrency, and Other Countries Could Follow*, CNBC (Feb. 19, 2018), <https://www.cnbc.com/2018/02/19/venezuela-petro-cryptocurrency-pre-sale-starts-february-20.html>

Senegal (eCFA),³⁹ Sweden (eKrona),⁴⁰ Dubai (EmCash),⁴¹ Japan (Jcoin),⁴² and Estonia (Estcoin),⁴³ and Ecuador,⁴⁴ among others.⁴⁵

Several factors explain such early experimentation in the public sector. The end of technological life cycles of legacy systems and associated emerging trends in payment systems necessitate central banks' enhanced examination of cryptocurrency solutions.⁴⁶ Central banks in

³⁹ Samburaj Das, *Senegal Will Introduce a Blockchain-Based National Digital Currency*, CCN (Nov. 28, 2016), <https://www.ccn.com/senegal-will-introduce-blockchain-based-national-digital-currency>

⁴⁰ Afraid of a few commercial entities controlling cash supply in Sweden, the Swedish central bank has kicked off its digital currency project e-krona. Amanda Billner, *Now There are Plans for 'e-Krona' in Cash-Shy Sweden*, BLOOMBERG, (Oct. 26, 2018, 2:25 AM CDT), <https://www.bloomberg.com/news/articles/2018-10-26/riksbank-to-develop-pilot-electronic-currency-amid-cash-decline>

⁴¹ Jon Buck, *Dubai Will Issue First Ever State Cryptocurrency*, COIN TELEGRAPH (Oct. 1, 2017), <https://cointelegraph.com/news/dubai-will-issue-first-ever-state-cryptocurrency>.

⁴² Arjun Kharpal, *Japanese Banks Are Thinking of Making Their Own Cryptocurrency Called the J-Coin*, CNBC: TECH TRANSFORMERS (Sep. 27, 2017), <https://www.cnbc.com/2017/09/27/japanese-banks-cryptocurrency-j-coin.html>.

⁴³ Kaspar Korjus, *We're Planning to Launch Estcoin – and That's Only the Start*, MEDIUM (Dec. 18, 2017), <https://medium.com/e-residency-blog/were-planning-to-launch-estcoin-and-that-s-only-the-start-310aba7f3790>.

⁴⁴ Everett Rosenfeld, *Ecuador Becomes the First Country to Roll Out Its Own Digital Cash*, CNBC: CURRENCIES (Feb. 9, 2015), <https://www.cnbc.com/2015/02/06/ecuador-becomes-the-first-country-to-roll-out-its-own-digital-durrency.html>.

⁴⁵ *Cryptocurrencies by Country*, THOMPSON REUTERS (Oct. 25, 2017), <https://blogs.thomsonreuters.com/answerson/world-cryptocurrencies-country>

⁴⁶ Morten Bech & Rodney Garratt, *Central Bank Cryptocurrencies*, BIS QUARTERLY REVIEW 66-67, September 2017, available at SSRN: <https://ssrn.com/abstract=3041906>.

countries with rapidly declining cash usage⁴⁷ are subject to the most pressure to find solutions for bank note alternatives.

The private sector also continually engages in cryptocurrency experimentation. Most cryptocurrency exchanges are creating their own stable cryptocurrency.⁴⁸ On February 14 2019, J.P. Morgan introduced the first prototype of its blockchain settlement product: JPM Coin, a stable cryptocurrency backed one-to-one by JPM's fiat currency reserves.⁴⁹ Finally, Facebook is developing a stable cryptocurrency in an attempt to break into the financial services business.⁵⁰

⁴⁷ Jonathan Brugge, Olivier Denecker, Hamza Jawaid, Andras Kovacs, & Ibrahim Shami, *Attacking the Cost of Cash*, MCKINSEY & COMPANY (Aug. 2018), <https://www.mckinsey.com/industries/financial-services/our-insights/attacking-the-cost-of-cash>.

⁴⁸ Jeff John Roberts, *Cryptocurrency Exchanges Back \$32 Million Stable Coin Project*, FORTUNE (Aug. 29, 2018), <http://fortune.com/2018/08/29/cryptocurrency-exchanges-back-32-million-stable-coin-project>; Julie Verhage, *Crypto Exchange Coinbase to List Stable Coin Backed by Circle*, BLOOMBERG (Oct. 23, 2018), <https://www.bloomberg.com/news/articles/2018-10-23/crypto-exchange-coinbase-to-list-stable-coin-backed-by-circle>.

⁴⁹ Michelle Davis & Alastair Marsh, *JPMorgan to Use Digital Coin to Speed Up Corporate Payments*, BLOOMBERG (Feb. 14, 2019), <https://www.bloomberg.com/news/articles/2019-02-14/jpmorgan-to-use-cryptocurrency-for-payments-business-cnbc-says>.

⁵⁰ Sarah Frier & Julie Verhage, *Facebook is Developing a Cryptocurrency for WhatsApp Transfers, Sources Say*, BLOOMBERG (Dec. 20, 2018, 6:35 PM CST), <https://www.bloomberg.com/news/articles/2018-12-21/facebook-is-said-to-develop-stablecoin-for-whatsapp-transfers>; Nathaniel Popper & Mike Isaac, *Facebook and Telegram Are Hoping to Succeed Where Bitcoin Failed*, THE NEW YORK TIMES, (Feb. 28, 2019), <https://www.nytimes.com/2019/02/28/technology/cryptocurrency-facebook-telegram.html>.

The rise of an early stable cryptocurrency design, Tether, in terms of its total market capitalization,⁵¹ its stability around \$1 value,⁵² and investors' uses of Tether as a temporary safe haven,⁵³ provides some support for stable cryptocurrencies' ability to create market stability, even if only temporarily. Like all other stable cryptocurrency projects, Tether is still afflicted with significant design challenges.⁵⁴

The total volume of stable cryptocurrencies relative to the rest of the cryptocurrency market is growing consistently. The growth of stable cryptocurrencies can largely be traced back to attempts to combine the utility and benefits of cryptocurrencies and blockchain technology with remedies for the existing fluctuation and volatility in the cryptocurrency markets.⁵⁵ The growth data suggests that demand for products that help manage the volatility inherent in other crypto assets is likely to continue to increase.⁵⁶

⁵¹ COINMARKETCAP: TETHER, <https://coinmarketcap.com/currencies/tether> (last visited Apr 22, 2019).

⁵² Johnson Gitonga, *What is Tether (USDT) and How to Buy It?*, YAHOO! FINANCE (Feb. 5, 2018), <https://finance.yahoo.com/news/tether-usdt-buy-090742535.html> to evidence on how stable Tether is at \$1 value.

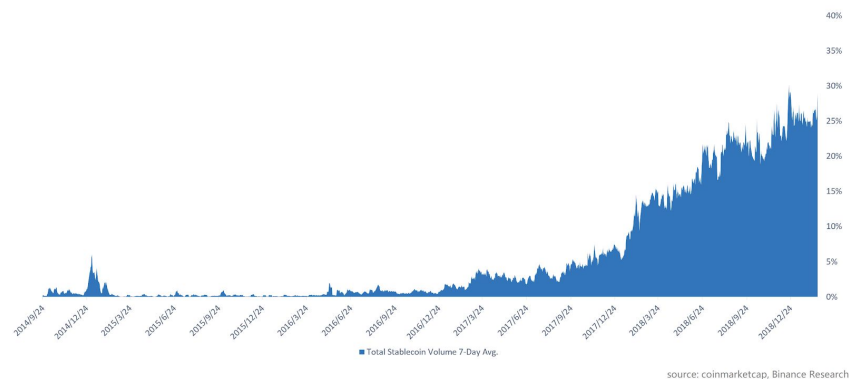
⁵³ Evidence that shows that investors move crypto assets into Tether when the market gets more volatile.

⁵⁴ Tether's issue with being pegged against the US\$ and with that subject to Centralized monetary policy. Andrea Tan, Eric Lam & Benjamin Robertson, *Crypto Markets Roiled as Traders Question Tether's Dollar Peg*, BLOOMBERG, (October 14, 2018, 11:30 PM CDT), <https://www.bloomberg.com/news/articles/2018-10-15/dollar-peg-that-underpins-20-of-crypto-trades-is-under-pressure>.

⁵⁵ *Stablecoin*, BINANCE ACADEMY, <https://www.binance.vision/glossary/stablecoin> (last visited Apr. 24, 2019).

⁵⁶ BINANCE RESEARCH, *Ever-increasing Volume: Contribution of Stablecoin Volume to Total Industry Volume*, in *Can JPM Coin Disrupt the Existing Stablecoin Market?* at 4, (Mar. 1, 2019), <https://info.binance.com/en/research/marketresearch/img/BinanceResearch-JPMCoin.pdf>.

Ever-increasing Volume: Contribution of Stablecoin Volume to Total Industry Volume



3 FIRST ORDER PRINCIPLES FOR STABLE CRYPTOCURRENCIES

Several common denominators allow for the identification of First Order Principles for stable cryptocurrency. Following the quantity theory of money, we discuss how a currency can be designed to maintain a stable store of value through the mechanisms of minting and burning money, transaction taxes vs. holding taxes, and repegging. Most importantly, good governance principles are crucial for every aspect of instituting any long-term stable currency due to inevitable changes in the market and the fundamental obstacle represented by the Folk Theorems of game theory.

3.1 CURRENCY MINTING AND BURNING

The principle idea for creating a stable currency is to use the quantity theory of money (QTM) to determine when and how to print and destroy money.

First there needs to be the notion of a currency's value relative to some ideal stable value. This stable value is most commonly specified by a consumer price index (CPI), though most existing stable coins have chosen the USD as their measure of stable value. This choice of index of

stable value is called the peg. The goal of a stable coin can be a tight peg or loose (within a range of values), fixed or floating (the value can raise or drop within specified rate limits). For simplicity, we will confine our discussion to analyzing a loose fixed peg. For concreteness we assume the target value of the currency is fixed on the USD and allowed to range 10% in value from \$0.90 to \$1.10.

QTM dictates that minting twice as much currency will halve its price, and burning half of the existing currency will double its price. This mechanism can then theoretically stabilize the price of a currency. If the price of the currency rises to \$1.10 as measured by averaging its value on currency exchanges, then minting 10% more currency and releasing it to the market will lower the price to \$1; if the price of the currency drops to \$0.90, then burning 10% of the currency will raise the price to \$1. The relevant equation relating the price P and the quantity of money M is

$$PM = \text{constant}$$

which is derived from the classical equation of exchange.

Such calculations are only valid in the ideal. In practice, the scheme's success depends on *how* the money is printed and distributed or burned.

3.1.1 Minting

The minting of coins requires many choices. For example, there needs to be protocols for deciding the following: 1. What is the margin around the peg? 2. How is the value measured (presumably an average of currency exchange indices)? 3. When and how often is the value of the coin measured (presumably a running average, but specifying this average determines how forex traders will react); 4. How much is printed in response to the price exceeding the margin (do you mint the price dictated by the static QTM, or do you take into account the rate of change of the price)? 5. How is the newly minted money distributed (is it given algorithmically to specific members of the stable coin network, or sold to the market by a DAO created for that purpose, given to a charitable group, etc.)?

For instance, the plan for Basis stable coin was to mint new coins when the price was high and distribute them to their shareholders, which would theoretically sell them immediately on the market to get the best price. However, it is possible the shareholders would collude to drive the price up by holding their new money, in which case the mechanism

would automatically print more, benefitting the colluders. There are many ways to combat such tactics, such as diversifying the shareholders, or automatically selling the new coins on the market then giving the shareholders the results.

At this point it is crucial to recognize a fundamental fact encapsulated in the Folk Theorems of game theory⁵⁷. No matter how complicated the protocols become for creating a stable coin, there are strategies that a powerful and patient player can use to subvert the system to profit at the expense of the group. This means a nimble and responsive governance process is required for any such stable coin scheme, because the rules must always be ready to be adjusted to respond to the changing conditions of the market.

3.1.2 Burning

When the price of the currency is lower than the peg, QTM dictates that currency should be destroyed, i.e., burned, to raise the price. Two broad approaches for burning money is to sell bonds or sell reserves, then burn the proceeds of the sale. These mechanisms should be used to address the two broad reasons a currency may temporarily lose value: larger economic instability and hot money.

3.1.2.1 Bonds

Bonds should be used to address a temporary larger economic instability which lowers a currency's price--due to an act of God, for instance, or war. A bond is a new type of token, separate from the currency token. A bond token may be minted and sold at a price lower than its future redemption value. For example, if the price of the currency is at \$0.90, then enough bonds can be sold so that 10% of the currency is raised in the sale. Then this currency will be burned, raising the price temporarily to \$1. At some future time the bonds will be redeemed for a higher price than they were sold, hopefully when the economy rebounds. If the economy does not improve, this action will fail and another mechanism must be employed, such as a new raft of bonds, or taxes, or a repeg of the currency, depending on the cause of the instability. (The reasons for

⁵⁷ [https://en.wikipedia.org/wiki/Folk_theorem_\(game_theory\)](https://en.wikipedia.org/wiki/Folk_theorem_(game_theory)) Retrieved 6/4/2019.

employing the taxes and repegging mechanisms will be discussed below.)

For instance, the plan for Basis was to mint bonds when the price was low and repay the bonds automatically when the currency price rose above the margin with the first newly minted coins. According to our simulations, this scheme will succeed as long as demand for the currency is growing at a sufficient rate, but it will fail if the demand is stagnant at equilibrium. The financial instrument represented by Basis-type bond is a very complicated option, technically a one-touch up-and-in Asian barrier option with no expiration. Under an assumption of constant demand, this option's value has high variation, making it expensive and inefficient to sell. More generally, since the bonds would sell at a price lower than they were redeemed, the bond queue would grow without bound, leading to lower prices for the bonds and a positive feedback loop which would lead to a death spiral and the failure of the peg.

This cartoon description of the Basis mechanism under the constant demand assumption demonstrates that bonds should only be used in the case when there is a larger force at work, which is temporarily dropping the economy, so that in the future, when the economy has rebounded, bonds can safely be paid off. The expense of bonds in this case is justified by the preventing the costs associated with temporary instability. We also recommend following the example of historical central banks, in minting bonds with fixed expiration so price discovery is more efficient.

A nimble and responsive governance process is again required in order to recognize when the economy is experiencing a temporary instability in the market in order to decide to mint bonds.

3.1.2.2 Reserves

Reserves are necessary to address the instability of a currency due to hot money. Hot money is money that is frequently transferred between institutions or currencies in order to maximize gain in interest or capital. For instance, the hot money from speculation is the leading contemporary cause of instability in cryptocurrencies. As speculators move money from bitcoin to ether, e.g., bitcoin's price drops and ether's price rises.

Most of the value of contemporary cryptocurrencies comes from speculation on the future use of cryptocurrencies for basic service

transactions that do not currently exist. Therefore the vast majority of cryptocurrencies are technically hot money. The best way to prevent price fluctuations due to hot money is to use reserves.

A reserve of foreign currencies and/or assets is collected by a mechanism in the cryptocurrency design when the price goes beyond the upper margin, in this example \$1.10. The manner in which this is handled depends on the design. MakerDAO has a complicated mechanism of individual encumbrance and algorithmic enforcement. For the purposes of this article we will discuss a conceptually simpler mechanism used, for instance, by Reserve stable coin and most national currencies. This latter mechanism uses QTM to mint new coins when the price is above \$1.10 and sells them at market for USD (hypothetically). The USD is then held liquid in reserve in anticipation of a drop in the price of the cryptocurrency. When the cryptocurrency price reaches \$0.90, then enough cryptocurrency is bought with the reserve USD, theoretically 10% of the currency in existence, which is then burned.

In this toy model assuming an ideal QTM situation, it is easy to calculate the cost of defending against hot money with the reserve mechanism. In the next paragraph we demonstrate the obvious result that selling the currency when the price is high to build a reserve, then buying the currency back with the reserve when the price is low will yield an arbitrage profit. This holds under the following two assumptions: 1. The reserve currency is more stable than the base currency, and 2. The cost to implement and maintain the reserve is ignored.

Under the quantity theory of money the price P and the quantity of money M satisfy

$$PM = \text{constant} = C$$

If there are $M = 1000$ currency tokens in existence when the price rises above $P = \$1.10$ we have $C = 1100(\text{tokens} * \$)$ so minting 100 new tokens restabilizes P at

$$P = C/M = 1100(\text{tokens} * \$)/1100 \text{ tokens} = \$1$$

Now assuming the 100 newly minted tokens were sold at \$1.10 the reserve then has \$110 USD. Then when the price drops to \$0.90 when hot money exits the currency, we buy tokens with the reserve USD. Before purchase, our 1100 tokens at \$0.90 gives C as

$$PM = C = 990(\text{tokens} * \$)$$

so buying and burning 110 tokens (which was 10% of the previous total M) gives us anew $M = 990$ so the new P must be $P = \$1$.

Notice that this purchase of 110 tokens at \$0.90 requires \$99 USD, so our reserve finishes by holding $\$110 - \$99 = \$11 > 0$ more than at the beginning.

This shows that maintaining a reserve can defend against the instability due to hot money. The argument assumes 1. the reserve is held in a currency or other asset with stable value, and 2. the price of maintenance for the reserve is not more than the profit that can be achieved in the arbitrage. The first requirement leads to a criticism of the MakerDAO protocol (e.g.), the second requirement leads to a criticism of the Reserve protocol (e.g.).

3.1.2.3 Hot Money Ratio

The assumption of many stable coin designs is that a 100% reserve must be maintained to guarantee the peg will hold. This is due to a basic argument from economics, used by Soros to break the Bank of England, that a currency not fully backed by reserves can theoretically be shorted until its peg is broken to achieve an arbitrage profit.

On the contrary, we argue that a 100% reserve is not always necessary, as is the case with any currency which has an intrinsic worth. At minimum, e.g., a national currency has the intrinsic worth represented by the confidence gained from the ability to pay taxes. A cryptocurrency would have intrinsic worth if there are genuine economic transactions that are reliably being performed with its tokens—especially if there are auditable investments which encumber the value in the token. Soros was not able to break the Bank of England because it wasn't fully backed with foreign reserves, but because the British pound was being pegged at a value that was inauthentic.

In fact no nation holds anything near to a 100% reserve for the obvious reason that it would be too expensive to have a large liquid reserve. The US foreign reserve, e.g., is less than 2% of its money.

Holding any liquid reserve is a loss of opportunity cost that is a type of economic friction its users must subsidize, explicitly in transaction taxes which transparently pay for maintenance of the peg, or implicitly in

holding taxes which bearers of the currency pay, usually through inflation.

Therefore determining the fraction of a currency that is hot money is necessary for efficient defense of its stability. A currency that overestimates this hot money ratio will cost more to use. A currency that underestimates the ratio will be insecure. The tension between these two values of efficiency and security motivates a careful estimate of the hot money ratio.

Contemporarily, we estimate that virtually all cryptocurrency is used for speculation and is therefore hot money and therefore needs to be backed fully. But a well-designed stable coin should anticipate the future when it is used for more authentic economic activity.

3.1.2.4 The Energy of Money

The authors are researching the creation of such a hot money index, by studying what we call the energy of money. We begin with the classical equation of exchange from QTM

$$MV = \Pi Q$$

Here $\Pi = 1/P$ is the price level, and Q is the real value of aggregate expenditures. We think of Q as the momentum of the economy. V is the classical velocity of money, which is much easier to evaluate with blockchain cryptocurrencies than national fiat currencies, since every transaction on blockchain gives fully transparent publicly-available information on the exchange of money. Demand is classically defined as $D := MP$ which is analogous to the mass of the economy. Demand D represents the aggregate of all market demand for the currency for purposes of using it in business transactions and holding it as a store of value for anticipated future use and insurance.⁵⁸ The analogy with the kinetic theory of gases guides much of our thinking on how to evaluate

⁵⁸ Cf., Milton Friedman, “A Theoretical Framework for Monetary Analysis”, NBER Occasional Paper 112, National Bureau of Economic Research, Columbia University Press, 1971.

the efficacy of these quantities as guides to understanding the hot money ratio.

We define energy as $E := QV$. Notice the equation of exchange give us $Q = DV$ and, thereby, the identity $E = DV^2$. The sum of the changes in the volume of transactions times their displacements, or the work it took to bring the system from 0 value to its current state of volume and velocity, is the energy of the system:

$$W := \int FdX := \int dQ \cdot V =: E$$

Here the work integral is formally defined in the previous line: the force F is formally the derivative of the momentum $F = dQ/dt$ and X is the “position of money”, formally the integral of the velocity of money. All this formality is used to draw out the analogy with mechanics. The sum of the changes in the volume of transactions times their displacements is the energy of the network. The sum of all the changes in value and rates of transactions in moving from 0 to the current state gives the total energy, potential and kinetic, of the economy.⁵⁹ Under the assumption

⁵⁹ We are thinking of the energy of an economy in very physical terms of baskets of goods exchanging hands at a certain rate. Following this tangent is beyond the scope of this article, and not directly useful for estimating the confidence we have in an economy, but it may be worth explaining our personal perspective briefly in a footnote. We imagine the baskets of goods quite literally, and the velocity of money represents these baskets of goods changing hands. The energy of an economy is therefore precisely related to the energy that farmers, miners, industrialists and all other kinds of workers spend in bringing us to our current economic state. These workers’ energy can ultimately be traced back to the sun--all plant and animal energy obviously comes pretty directly from the sun, and all our petrochemical fossil fuels come from sequestered plant energy that originally came from the sun. The literal basket of goods (food, fuel, lumber, iron ingots, etc.) is therefore energetically measurable. This

of conservation of energy, the network would not lose or gain confidence value (energy) without accounting for the loss through conversion of value to or from other forms.

With clearly specified definitions of energy we can discuss “frictions” in an economy due to inefficiencies, and we can distinguish “genuine” versus “artificial” network energy to guard against the instability arising from hot money.

3.2 TRANSACTION TAXES VS. HOLDING TAXES

Regardless of the specific protocols that are chosen to attempt to maintain a stable store of value, there are frictions in an economy which must be accounted. In a primitive economy the degradation of the assets in time, such as food spoilage or housing deterioration, are a natural fact that must be accounted. Currency can enable more efficient transactions which prevent the loss of value by degradation via the matching of the coincidence of wants before degradation can occur. Any remaining inefficiencies account for some of the result of inflation. Another cause of inflation is the cost of maintaining the coins. In the case of national fiat paper currencies, we must account for the cost of producing the cash, transporting it, and guarding it against counterfeit. In the case of cryptocurrencies, we must account for the significant cost of maintaining the nodes which create and store the electronic ledgers, redundantly to achieve decentralization, permanently to prove autonomy. Maintenance of the stability of the coin ultimately requires accounting for all inefficiencies in the economy.

Transaction taxes should account for the inefficiencies that result from maintaining the coins. Transaction taxes are fees on transfers of ownership of the coins, e.g., sales taxes. In a blockchain cryptocurrency, transaction taxes should match the cost of running the network, i.e., the cost required to incentivize a sufficient number of nodes to operate in order to maintain the level of decentralization desired, along with the cost required to maintain the stability of the coin (through the

perspective is illustrated at length in Vaclav Smil, *Energy and Civilization: A History*, MIT Press, 2017.

maintenance described above for minting (typically insignificant) and burning (typically significant)).

Holding taxes are typically the implicit result of inflation. Whenever the coin loses value relative to an ideal CPI, the holders of the coin are bearing the cost. Holding taxes should account for the inefficiencies of the economy, instead of the inefficiencies of the maintenance of the currency.

Ideally a good governance mechanism will be able to sagely judge how much of the inefficiencies of the system are due to the economy versus the maintenance of the currency, and implement the taxes appropriately.

In the contemporary climate, however, these taxes or fees are not likely to be implemented appropriately. In the zeal of the early development of the internet, large companies which profit from the increased efficiencies of this new communication medium tacitly bear the burden of maintaining most of the nodes. This has led to a culture surrounding the internet where users expect free service from the nodes. The costs of running an honest internet node are hidden from consumers since the information derived from running a node and the security of knowing their website is secure are more valuable than the costs of providing the public service. Most likely this culture will continue to the decentralized economy, where blockchain users will expect 0 transaction fees but will probably not notice holding fees below 3% annual, which are instituted implicitly by pegging to USD which has a similar inflation target.

3.3 REPEGGING

Regardless of how well the system is designed, there is always the possibility that the fundamentals of the economy will change. This is pithily encapsulated by the term “black swan events”.

For any long-lived currency a major shift in the perception of the value of a currency is at some point inevitable; a shift that is not accounted for by a reserve defending against hot money fluctuations or bonds defending against temporary instability in the larger economy. When such an event occurs, the currency could attempt to soldier along and use its taxes mechanisms to attempt to restabilize its value at the peg,

but it is more efficient to repeg the currency after discovering its more accurate value.

3.4 GOVERNANCE

3.4.1 Features Subject to Monetary and Fiscal Policy

As stressed throughout this chapter, governance of the decision-making body plays a crucial role in the stability design. The stability mechanism can be entirely automated in the day-to-day functioning of the network, employing a predetermined algorithm. However, monetary and fiscal policy choices cannot be fully automated. The parameters for the algorithm must be chosen by hand and adjusted regularly to balance security with maximal efficiency in response to network performance. Such choices need to be made by a decentralized autonomous organization, which we call the Stability DAO or SDAO.

The SDAO is a type of transparent, decentralized, open analog of the US Federal Reserve that ensures that the system maintains its decentralized nature. The SDAO is mandated to continually improve the function of the stable cryptocurrency. The SDAO enables full transparency of policy decision making, stable cryptocurrency-specific monetary and fiscal policy decisions. Moreover, the SDAO determines artificial bond token price floor to ensure SDAO does not borrow excessively in attempt to limit stable cryptocurrency supply.

The SDAO is needed for multiple oracle functions that enable a fully decentralized stability model. The decentralized oracle function of the SDAO includes establishing the specific sources and weights for averaging the information from exchanges, assessment of how often this information is sampled, determination of the specific length of time over which the information is sampled and averaged to determine the price.

Some of the other core functions of the SDAO are reviewed here. What are the specific conditions which dictate when the stable cryptocurrency or bonds are minted, how many stable cryptocurrency coins or bonds are minted, how long auctions are open, and when and how do we stop the bond queue or minting process? When and how is the price repegged in the face of black swan events? In the event of long-term stagnation in demand, when and how should a transaction tax or holding tax be implemented in response to the respective inefficiencies of the network

and the economy? When and how are reserves built, used, and maintained? How much of the network transactions are due to hot money versus authentic economic uses of the currency? What specific types of foreign reserves of currency or assets are used? How much of them are liquid? Who profits from the maintenance of the reserve, how, and when? Finally, the SDAO decides when to implement research supporting the mandate of maximizing stability and efficiency. The SDAO must continually adjust these choices, to balance security with maximal efficiency in response to network performance.

3.4.2 Communication Design

How decisions are made to the questions posed above depends crucially on the quality of information that the governing body has at its command. Governance design determines how information is communicated in a group, since the allocation of power determines who has a voice at what time.

Taking inspiration from engineering, the goal of communication design is to amplify the signal while filtering the noise. Centralized hierarchical systems more naturally lead to strong noise filters, which likely lead to filtering/ignoring the information signals at the edge. Decentralized flat organizations have a tendency to fail from the inverse quality of amplifying the noise at the edge, so that important information cannot find its champion to lead to useful action. Finding the right balance must be a conscious choice.

One of the major differences between centralized and decentralized structures is transparency. Centralized organizations tend to have opaque governance, hiding their decisions, decision making, and even their decision-making process. Decentralized organizations have a much greater tendency toward transparency.

Transparency has distinct advantages and disadvantages for monetary policy. For instance, a currency partially backed by reserves can be successfully arbitrated by Soros' shorting strategy much easier if the quantity of reserves is known.

3.4.3 Ultimate Power

Many choices must ultimately be made about how to specifically design the governance protocols of the SDAO. How will power over decision making be distributed, i.e., as the system progresses in time, who will be

rewarded with more power and who will be punished with loss of power? Secondly, who changes the rules governing the day-to-day functioning of the currency, and who changes the rules governing how to change the rules? The first question concerns executive governance and the second addresses legislative governance. These are extremely deep questions that have plagued every human organization that has ever existed. However, blockchain technology gives us new tools for anonymity, transparency, and permanency of records that can enable fully decentralized governance, while maintaining privacy, distributing power justly⁶⁰ and efficiently, and preventing censorship.

Even a partial investigation of the answers is too involved to contain here, but we refer the reader to our paper discussing on-chain governance design.⁶¹ In that paper we recommend an SDAO design coordinated through reputation-weighted democratic governance. The core objective of the governance design is to create the proper incentives that help independent and selfish actors to be organized and to collaborate productively towards a common goal. From a quite pragmatic perspective, addressing precise choices of parameters in algorithmic token design, the paper identifies which choices relate to which values a group may preference. As a simple example, the profits of a DAO must be chosen to be distributed in some ratio with the members who do the present work which garners the profit, members who have previously done such work which built the reputation of the DAO, members who designed the protocols for how to do the work, and with members who designed the governance structure which initiated the DAO. The choice of distribution weights which determines how much each of these 4 groups shares in the profit should match the current

⁶⁰ Justice is defined as the allocation of power to those who can best use it to profit the group. This definition is created in concert with the definition of corruption given above, as behavior that profits a minority group or individual at the greater expense of the majority.

⁶¹ Craig Calcaterra, On-Chain Governance of Decentralized Autonomous Organizations, (May 2018), available at <https://ssrn.com/abstract=3188374>.

values of the DAO. A greater share for new workers will attract new workers, a greater share for the older workers will signal long-term stability, while a greater share for the protocol designers will attract more innovation.

In the context of the SDAO, the governance design enables the SDAO to identify the ideal protocols for selecting and promoting its values and monetary policy goals. At the same time, the on-chain governance design allows the SDAO to achieve complete decentralization while preserving anonymity.

3.4.4 Transcendental Values

Finally, we repeat the idea that the Folk Theorems of game theory prove that it is impossible to create protocols, no matter how complex or well-engineered, which can eliminate corruption. Corruption is defined as behavior that profits a minority group or individual at the greater expense of the majority. No static set of rules can prevent the corruption that will eventually lead to the failure of any stability design. But a changing set of rules *can* prevent such failure. A nimble governance design can react to and prevent corruption if it devotes enough resources to rewarding such efforts.

The Folk Theorems prove that governance protocols can never be final; rules must continually change in order to react to and anticipate changes in the market and the players' behavior. Therefore, for long-term stability, a group must be organized around a transcendental value that guides the members' behavior. By transcendental value, we mean a value that cannot be specified or contained within with a logical set of rules, but that is nevertheless a goal that is meaningful and can be held in common by the group. A very limited list of examples of transcendental values guiding groups of the past include: harmony, individual rights, equality, equity, beauty, fairness, truth, and "don't be evil". Such values are often in tension, such as harmony vs. individual rights such as free speech, or equality of opportunity (freedom of competition) vs. equality of outcomes (equity). Transcendental values have guided every human organization, religious or secular, for the very reason that they are required by the Folk Theorems to maintain stability as people inevitably discover circumventions to the transcendent intentions behind the explicit and mundane rules.

An organization's values can help harmonize the group in decisions on previously unanticipated behavior, so that the group can efficiently and effectively punish or reward the action, immediately or retroactively. Clear expressions of an organization's values, commonly held, are essential for the design, redesign, and implementation of any governance structure, but such values are far more important in decentralized organizations, which inherently have less motivational structure than centralized hierarchies.

4 CONCLUSION

Stable cryptocurrency designs will play increasingly important roles in the evolution of decentralized economies. They can establish and support core functions that are currently sub-optimally provided in the centralized economies and emerging markets. First Order Principles identify common core design factors for stable cryptocurrencies. The mathematical models and substantive coded implementations of First Order Principles are continually evolving.

