Nomisma: Risk Sharing on the Blockchain*

Lauren Cohen
Harvard Business School and NBER

Dimitrios Kavvathas
Harmony Advisors Ltd.

Christopher Malloy
Harvard Business School and NBER

ABSTRACT

Risk sharing is the basic function of finance. Meanwhile, the broad adoption of cryptocurrencies and the expansion of the entire blockchain ecosystem are hampered by the extreme volatility of cryptocurrency prices. We propose the adaptation of seasoned finance applications with an eye towards revolutionizing the blockchain ecosystem. To do so, we create a new platform that promotes financial system-wide optimal risk sharing by designing and customizing portfolios that deliver fixed income equivalent cash flow profiles with collateralized cryptocurrency underlyings. Our solution increases the appeal of blockchain investments to the average investor, both retail and institutional. The implications of allowing investor separation along the risk aversion and diversification spectrum, by enabling the generation of collateralized cash flow streams tranched according to risk preferences and liquidity profiles, are profound.

Key words: Blockchain, Stable Coin, Securitization, Risk Sharing

* We would like to thank Lucas Gaylord and Kimon Gkomozias, members of the Nomisma Foundation, for extensive technical and research assistance. We also thank Dustin Zacharias and Zhaoheng Gong for excellent research assistance.

Executive Summary

1. The Problem
    - The wider investment world has only barely begun to invest into the blockchain space, in large part due to the enormous volatility in cryptocurrency prices.
    - This type of volatility makes cryptocurrencies an unattractive asset class to many investors, both retail and institutional.
    - Extreme price volatility also slows the adoption of various blockchain-enabled innovations, which are often funded through tokens/ICOs in the cryptocurrency space.

2. The Size and Characteristics of the Market
    - Cryptocurrencies currently account for a very small percentage of the global market portfolio, less than 0.1% of its value (roughly $0.575 trillion USD out of $605 trillion USD).
    - Cryptocurrencies' capitalization has reached roughly 7% of the gold's market capitalization already, despite their relatively recent introduction.
    - Gold and crypto-assets constitute no-one's liability; the element of "trust" underpinning their continual function as a store of value can be further enhanced and "financialized" by introducing claims collateralized by the financial system's / community's belief in its eventual exchange value at extreme events.

3. The Solution: Nomisma and Risk Sharing on the Blockchain

    - Risk sharing and diversification are core concepts in finance. A fundamental application of finance theory is the creation of tools to customize desired cash flow/investment profiles in line with the risk tolerances of investors.
    - The Nomisma Foundation is a new platform designed to structure and price contingent claims that span the cryptocurrency state space and thus generate fixed income and option claims.
    - These claims allow users to match their desired cash flow / risk return profile commensurate to the risk they are willing to undertake.

4. Basic Mechanics
    - Tokens will be issued that allow users to face the Nomisma foundation as a trustless counterparty, via smart contracts, to their desired cash flow / risk return profile.
    - These tokens will cover transaction costs on the Ethereum blockchain and will embed a small fee per payoff structured and delivered and may entitle holders to the hedging gains generated by the replicating portfolios.
    - Users can partake of analytics regarding the pricing of contingent claims on cryptocurrencies / coins.
    - Users will be able to generate any contingent claim, single and multiperiod one, facing the foundation.
        - For the prototype, users shall be able to define a desired a rate of return vs an acceptance of linear principal loss depending on a coin's price performance during a specified time period. This will be priced in equilibrium against a claim that pays out a multiple of the original outlay in case of upside performance.
    - We will thus be generating coin specific interest rate term structures across time as well as hazard rate / "riskiness" spread curves.
    - The end goal is the creation of fixed income claims for each coin.

5. Liquidity

    - Standard marketplaces / exchanges rely on 6 ' mutual coincidences of wants ' x N coins to generate liquidity. (buyer vs seller of call, buyer vs seller of put, collateral arrangements between sellers and buyers)
    - We reduce these 6 degrees down to 2 thus enabling much stronger network effects. Conditional on appropriate regulatory guidance, Nomisma Foundation will continuously act as a buyer of volatility, further reducing dimensionality down to 1.

6. Expansion and Transformation
    - In the second stage we will introduce portfolio pricing and the ability to take advantage of the coin universe cross-correlation variance/covariance properties.
    - Cryptocurrency Clearinghouse:
        - Our expertise in modelling, structuring, risk managing CCOs will be shared with token holders so as to create the ecosystem critical mass that will allow securitization mechanism properties to render crypto universe amenable to tailoring cash flow profiles according to users' risk tolerance and desired payoff profiles.
    - Cryptocurrency Rating Agency:
        - We will create a transparent methodology to rate exposures riskiness

depending on market information.

- Cryptocurrency Trading for All Investor Categories:
    - The platform will provide opportunity for “coin-pickers” to leverage their expertise and “late-adopters”/ “risk averse”/ “crypto-naïve” users (individual or institutions) to be exposed to quantified remote to spot events against a fixed income return

7. The Creation of the Nomisma Stablecoin:
    - What is money?
        - Money is a liability created by the official sector and backed by its tax raising capacity.
        - The best that a cryptocurrency can hope for in its “money-as-asset” generating function is to isolate the “user-implied” safe component of each coin as well as the “safe component” + “crypto universe correlated crash risk” of a perfectly diversified coin portfolio.
    - How does one ensure the stability of a cryptocoin versus a designated fiat currency?
        - We are not providing an accounting algorithm that generates or destroys coins so as to maintain parity with fiat.
        - A coin-specific stablecoin is defined as the downside strike price for the short put on the underlying that implies an interest rate equivalent to the designated fiat currency. This self-reconstitutes based on oracles’ signals so as to maintain fiat currency claim equivalence.
        - There is no artificial limited supply; it is embedded via the supply constraints of each underlying, but translates each coin’s stability, user perception of future returns and relative desirability into a market determined fiat equivalence. Some coins may be able to support stablecoin minting, some not, and some may be able to do so only for certain tenors.
    - Our structuring platform, by offering the ability for the user community to independently, transparently converge towards a solution, will allow the creation of crypto-backed privately generated “safe assets” in a world which suffers from a shortage of such assets.

8. Conclusion
    - Nomisma is a new platform that promotes system-wide risk sharing and cash profile/payoff tailoring according to risk tolerance and cash flow preferences.
    - Our solution increases the appeal of blockchain investments to the average investor, both retail and institutional.
    - As added benefits, the platform will introduce: a) a robust, fungible, and

transparent Nomisma Stablecoin, exhibiting all the characteristics of optimal privately produced money; b) a smart contract based clearinghouse; c) a crowdsourced/market-based creditworthiness assignment engine, and d) a mechanism to match managers with alpha-generating capacity to those looking to hedge or enter the crypto space at varying levels of risk tolerance.

- More generally, Nomisma is a comprehensive intermediation platform that will help incentivize investment into the cryptocurrency space and spawn the next generation of innovation on the blockchain.

Imperfect as our financial system is, I still find myself admiring it for what it does and imagining how much more impressive it can be in the future." Finance and the Good Society, by Robert Shiller.

The blockchain will not reach its potential as a transformative technological innovation without attracting widespread investment from the retail and institutional investment world. While venture capitalists, angel investors, and other early adopters have invested liberally into various cryptocurrencies and blockchain applications to date, the next step in the evolution of the blockchain will require an ecosystem that is more conducive to attracting and catering to investors with varying risk preferences and time horizons.

In this paper we articulate the motivation, the building blocks, and the specific mechanics of a new platform capable of increasing the appeal of cryptocurrency investments to the average investor, both retail and institutional. Our key insight is that finance provides a wide array of tools to aid in risk sharing, and that risk sharing is precisely the area that is most poorly developed within the blockchain at present.

Currently, the blockchain ecosystem lacks an outlet for sourcing fixed income exposures, and does not contain financial intermediaries acting in any kind of platform-stabilizing, or public

good expanding role (as opposed to simply trading in and out of various cryptocurrencies in a speculative manner, surprisingly so in light of the quasi-public good nature of the Ethereum blockchain itself). And yet, the latent demand for these services is immense. We offer a solution to meet this underlying demand by launching a platform where investors such as large pension funds, endowments, insurance companies, and retail investors can generate fixed-income claims' equivalents and participate in line with their risk tolerance in the expansion and evolution of the blockchain. As a natural byproduct, rather than a pained connivance, we propose an algorithmically generated stablecoin, which embeds a robust link to the correlated crash mitigating, supply/ demand implied 'collateral antifragility' properties of the crypto-currency / token in question, as well as the broader coin universe.

The specific platform mechanism we create helps to alleviate common problems associated with the absence of fixed income claims such as: a) the transactional difficulty associated with the inability of an investor to satisfy a borrower's need (and vice versa); and b) informational difficulty related to the inability to assess a borrower's creditworthiness or to diversify across borrowers. Because our platform facilitates risk sharing across time and across states of the world, intermediaries can transact within this environment and provide vital services such as maturity transformation, risk diversification, while also reducing the cost of contracting and information processing.

Our platform applies in organic sequence, the insights of derivatives' claims replication in a spanned state space, as well as the tools of structured finance onto the various decentralized blockchains. Structured finance involves the pooling of economic assets and associated income streams alongside the subsequent issuance of a prioritized capital structure against these

collateral pools. As a result of the prioritization scheme, most manufactured assets are thus safer than the average asset in the pool. The conclusion of a successful securitization is the creation of tradable securities with better liquidity than the underlying instruments. (Note that the growth and vagaries of the US residential mortgage market provide us with a great example for the benefits and the occasional addressable and easily attributable drawbacks associated with the securitization technology.) In the context of a smart contract, blockchain-based financial system, the risk sharing and diversification benefits of financial intermediaries can be achieved by an appropriately designed collateral escrowing and dynamic monitoring as well as algorithmic, transparent implied creditworthiness and stability measurement system.

As incidental deliverables, we will be reframing the monetary theory debate from money / cryptocurrencies as a medium of exchange/ unit of account and the associated crypto drawbacks, into "money as debt" and a store of value, by defining a fixed versus fiat unit of account that is collateralized by escrowed coins and is thus backed; and which retains a constant link to a government's nominal claims, backed by its tax raising capacity.

Further, by providing a transparent and robust metric of cryptocurrency universe valuation versus the fiat currency world, the platform delivers an instrument for system-wide risk monitoring and community support, as well as a platform for rewarding new and existing cryptocurrencies as they become more desirable. At its core, the platform will enable diversification and encourage lower volatility by helping to "complete the state space" of crypto-assets.

This paper proceeds as follows. In Section I we estimate the size of the global market and pledgeable asset portfolio, including the huge fixed income market in its various forms. We then

contrast this with the relatively modest size of the current blockchain-native cryptocurrency market, especially compared with the market capitalization of the 'barbarous relic', thus highlighting the huge market opportunity available for the provision of 'safer', fixed-income-like claims on crypto-assets. In Section II we estimate various characteristics of the current cryptocurrency market for the largest 10-20 cryptocurrencies, including its correlation properties, and demonstrate the benefits of securitization in this market. In Section III we provide a historical overview of the securitization technology aspects of which we will be employing on our new platform. In Section IV we articulate the history, motivation, and production of safe assets, and position our platform in the relevant economic and historical context. In Section V we introduce the mechanics of our new platform (Nomisma), provide detailed descriptions of the relevant claims and tokens that we are creating, and outline the technological infrastructure that we are constructing in order to bring the platform to the market.

I. The Size and Scope of the Global Market Portfolio

The global market portfolio is defined as the set of all investible assets in existence at a specific point in time, weighted by their relative market capitalizations. A core axiom of finance theory holds that this portfolio is mean-variance optimal. That is, an investor with a preference structure that is increasing in expected return, and decreasing in variance (i.e., likes return, dislikes mean-preserving variance) will find it optimal to hold this portfolio. Their chosen amount of leverage (Rf) may vary, but the investor cannot do better than this global portfolio of risky assets plus Rf (two fund separation), in terms of risk-return trade-off. Of course, by market clearing, this is why the portfolio is the observed aggregate global market portfolio to begin with.

Given frictions, heterogeneous beliefs, heterogeneous preferences, etc., this will edge away from the perfectly clean theoretical two fund separation. However, the global market portfolio remains as a powerful theoretical and intuitive tool, and is as such a great benchmark from which to begin consideration of any asset's place in formal asset allocation frameworks.

Moving to the measurement of the global market portfolio, theory dictates that all assets, including non-traded assets, should be included in the global market portfolio. This poses the challenge of establishing valuations for asset classes for which no reliable data is available (e.g. durable consumer goods). The discretionary choice of the universe of asset classes to include in the calculation of the global market portfolio, therefore, is crucial. The existing literature put forth several definitions of the global market portfolio which yield results varying by a factor of two. This paper adopts the view that the set of all pledgeable assets constitutes the relevant global market portfolio. Specifically, we include: global listed equities, global privately held equity, equity and debt held by private market funds, global debt securities, bank loans, global real estate, the global gold stock, global M2 money stock, and the market capitalizations of the 15 leading cryptocurrencies.

Results are shown in Table 1. The total value of the global market portfolio is currently **$605,164,204 (MM), thus over $605 trillion.**

Several assumptions are made to arrive at our valuation: the value of US non-sponsor owned private enterprises is estimated via data made available in the Federal Reserve's Survey of Consumer Finances following a method proposed in Anderson (2009). This estimate is then extrapolated to a global estimate based on the US share of world GDP, which is probably an understatement considering the inverse link between stage of development and business

formalisation Previous studies do not include estimates of the value of global private firms. The estimated value of global real estate is based on a study published by Savills World Research (2017). We assume that the value of commercial properties is reflected in the global equity estimates and therefore only consider Savills' estimate of the value of the global residential real estate stock. The inclusion of the M2 money supply is novel to this study. Finally, the estimate of the value of the global gold stock is based on estimates by the World Gold Council of the total quantity of gold excavated to date.

This study arrives at a substantially higher estimate of the size of the global market portfolio than much of the previous work. This is largely due to the inclusion of the value of non-sponsor-owned privately held companies, BIS data on international debt securities in place of bond market capitalizations, the inclusion of the M2 money stock as well as the on balance sheet corporate claims of financial institutions – all of which we are confident should be included in a robust estimate.

What can be seen from Table 1 is that as of January, 2018, Crypto currencies currently account for a (perhaps unsurprisingly) miniscule percentage of the global market portfolio, less than 0.1% of its value (roughly 0.575 trillion out of 605 trillion).

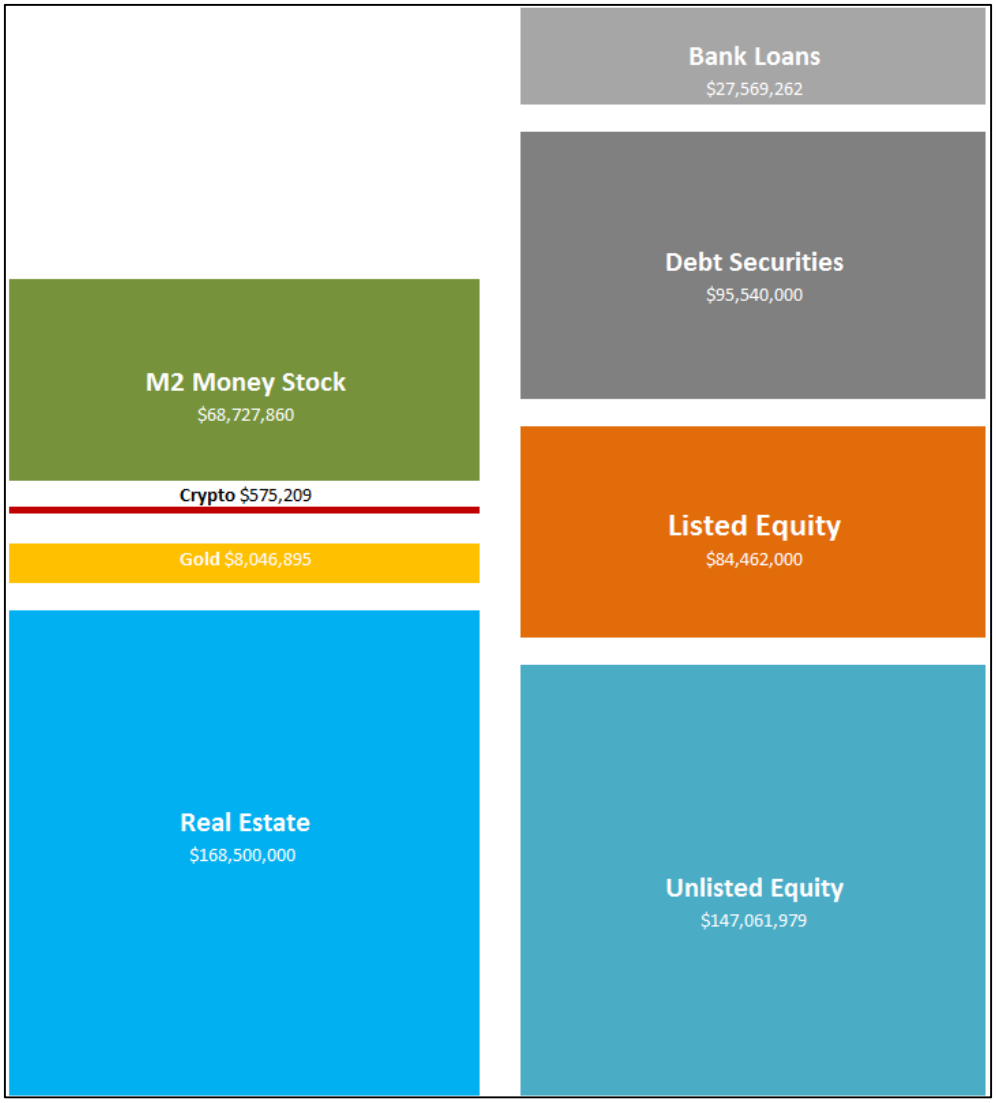
Table 1 – The Size and Breakdown of the Global Market Portfolio (January 1, 2018)

Asset Class	Metric	Value [mm USD]
Public Equities	Bloomberg World Exchange Markets	$84,462,000
Debt Securities	BIS Debt Securities	$95,540,000
Bank Loans	BIS Banking Claims	$27,569,262
Unlisted Equity (US)	Equity in privately held businesses	$19,503,666
Unlisted Equity (ex-US)	Based on US world GDP share	$127,558,313
Private Markets	Total	$4,681,000
	Buy-out	$1,474,000
	Venture Capital	$524,000

	Growth	$315,000
	Other	$151,000
	Real Estate	$795,000
	Private debt	$594,000
	Natural resources	$455,000
	Infrastructure	$373,000
Real Estate	Savils Residential Real Estate	$168,500,000
Money Stock	Global M2 Money Supply	$68,727,860
Gold	All gold mined in history	$8,046,895
Crypto	Total	$575,209
	Bitcoin	$251,473
	Ethereum	$121,689
	Ripple	$76,507
	Bitcoin Cash	$48,946
	Cardano	$20,563
	Litecoin	$13,704
	NEM	$13,027
	IOTA	$10,517
	Stellar	$10,142
	Dash	$8,641
TOTAL		**$605,164,204**

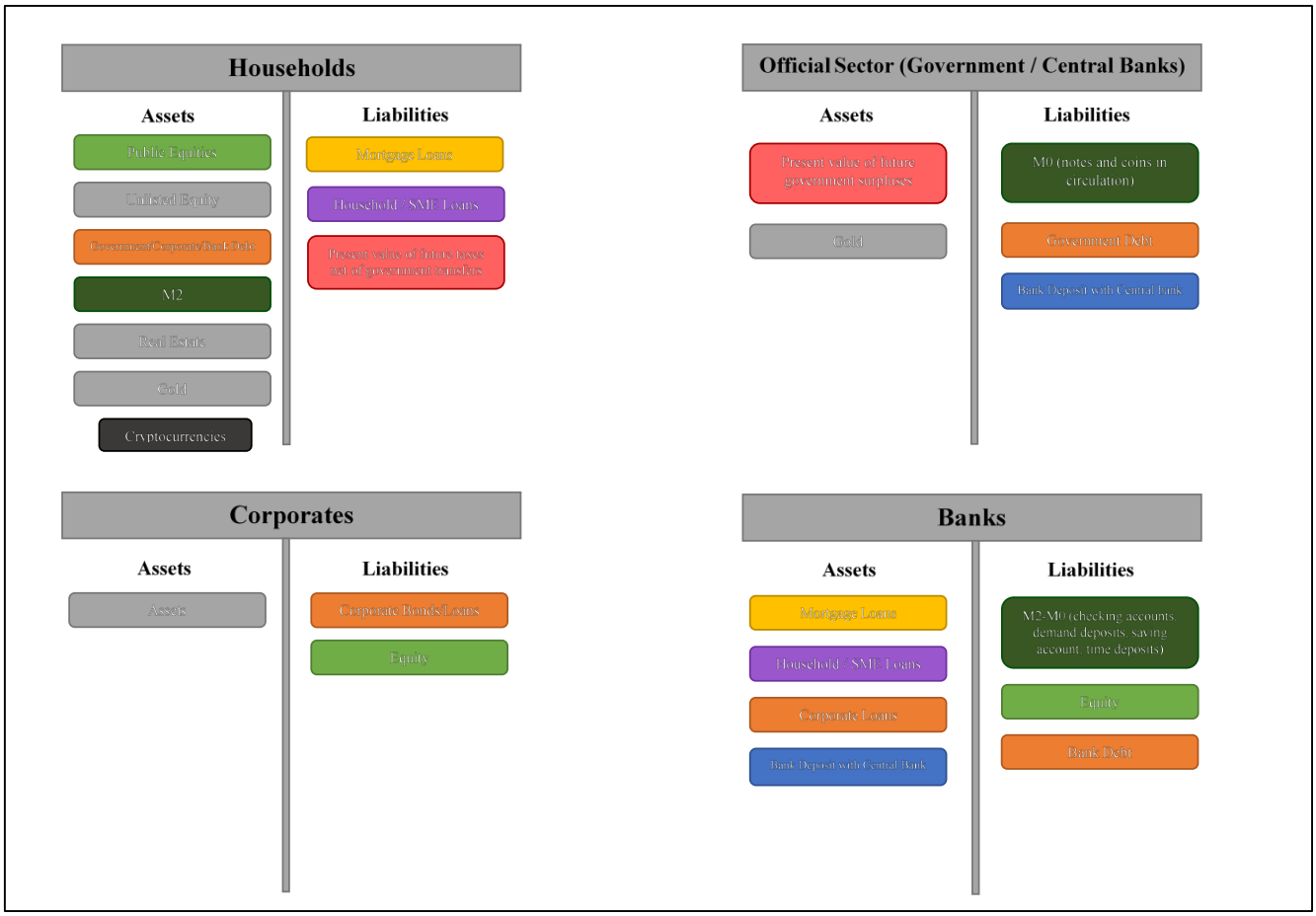
Figure 1 depicts the variation in the components of global market portfolio value. This figure clearly illustrates that the private and public equity markets, along with real estate and debt, dominate the value-weighted global market. Moreover, these markets comprise systemic footprints of nearly every geographical regional market worldwide. Other assets such as gold are smaller, and are held in more geographic concentration, being valued differentially across countries and regions. However, Cryptocurrencies' capitalization has reached roughly 7% of the gold's market capitalization already, despite their relatively recent introduction.

Figure 1 – The Size and Breakdown of the Global Market Portfolio



Importantly, we further wish to motivate the genesis of our platform together with the associated claims to be constructed. All pledgeable assets above, owned by economic agents, with the exception of gold and cryptocurrencies (note that we have abstracted away from commodity inventories, held for investment purposes, that are not captured by bank claims on corporates) are another economic actor's liabilities. Picturing stylised balance sheets of households, government+central banks (official sector) and corporates, the argument renders itself apparent (see **Figure 2** below, plus **Appendix Figure A1** for graphic representation).

Figure 2. Economic Actors' Balance Sheet



Gold and crypto-assets constitute no-one's liability; the element of "trust" underpinning their continual function as a store of value can be further enhanced and "financialized" by introducing claims collateralized by the financial system's / community's belief in its eventual exchange value at extreme events.

II. Crypto Currency Return Dynamics

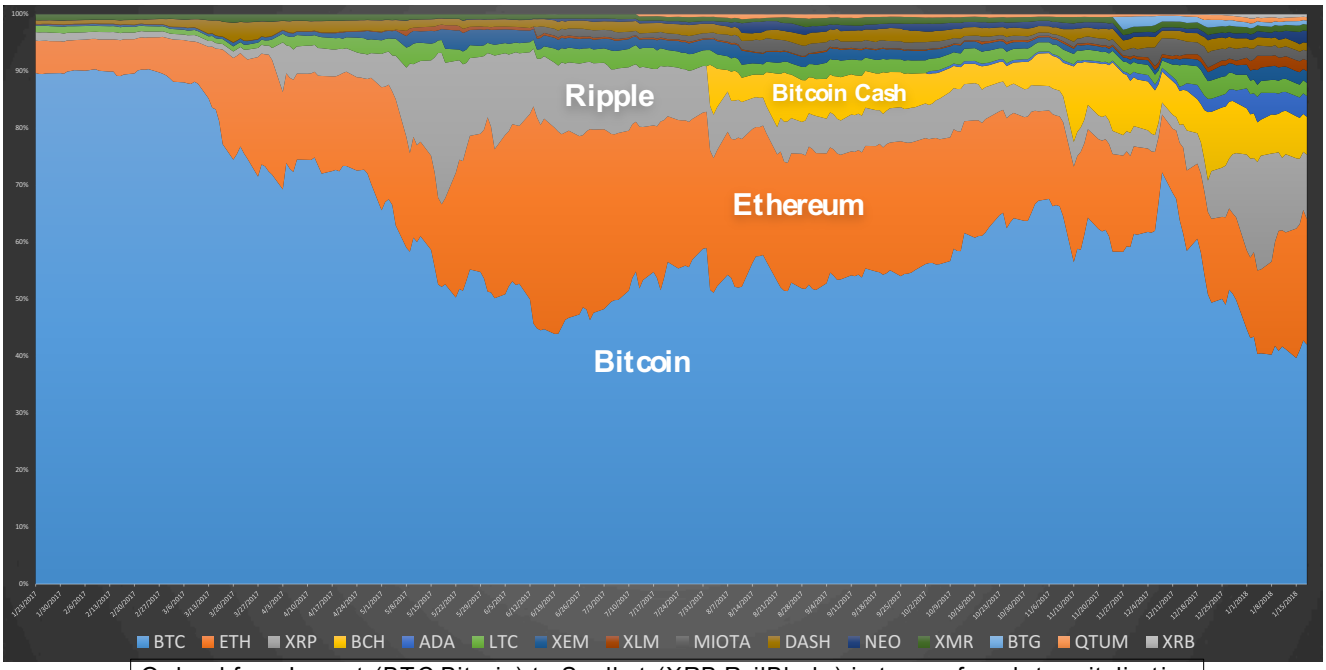
The meteoric recent rise in the market prices of cryptocurrencies has drawn increasingly large amounts of capital into this novel asset class. JP Morgan is estimating the net inflows into

the asset class for the year at around $6 billion (Panigirtzoglou, 2017),[1] which can be understood in the context of a skewed Pareto distribution / very high Gini coefficient cryptocurrency 'wealth' allocation having been concentrated among a small number of steadfast holders. Further, the phenomenon of asset overpricing exhibiting lottery ticket characteristics as well as the implied premium for coin monetization inability, can help inform pricing dynamics (our platform will be addressing both of these issues). The market capitalization of the 15 largest currencies currently exceeds $570bn, eclipsing the market capitalizations of commercial stalwarts including J.P. Morgan, Exxon Mobil, Wal-Mart, and Samsung. If the 15 largest cryptocurrencies constituted a corporation, they would rank 5th in the S&P500 index. Bitcoin taken alone would rank 15th in the index, ahead of Procter & Gamble, Pfizer, Intel, and Boeing.

Bitcoin was the first large-scale cryptocurrency. While it has remained the largest – along with being its highest profile exemplar – the past year has seen a substantial shift in market-share that has accompanied the generalized rise in cryptocurrencies aggregate market-wide capitalization. This can be seen below in Figure 3. Bitcoin began 2017 holding a nearly 80% market share. By 2018, this had fallen to below 50%. While Ethereum began (and ended) this period as the second largest cryptocurrency, it over doubled in market share to 21% of the market in January 2018. Added to this, a number of the other smaller currencies – such as Ripple – increased in market share substantially.

Figure 3 – The Share of Top 15 Cryptocurrencies Market Capitalization (Jan 2017-Jan 2018)

[1] This fact further motivates our platform, considering the inability of the current "piping" to sustain more significant inflows that could be waiting on the sidelines to invest.



Ordered from Largest (BTC:Bitcoin) to Smallest (XRB:RailBlocks) in terms of market capitalization

The relatively sizable market capitalizations of these currencies make their recent return time series even more remarkable. Among the major cryptocurrencies, the one with the highest percentage appreciation, RailBlocks (XRB), has increased 543-fold in value since its inception 9 months ago. In the period from December 11th, 2017 to January 10th, 2018 alone the currency has appreciated 21-fold.

Summary statistics on the return dynamics of cryptocurrencies - along with other large traditional currencies – are given in Table 2.

Table 2 – Summary Statistics of Cryptocurrency Return Dynamics

TICKER	MeanDailyLogret	AnnualizedVol	Kurtosis	Skewness	MaxDailyPercent	MinDailyPercent	Sharpe Ratio
BTC	0.71%	79%	3.56	0.6	25.2	-12.47	2.26
ETH	1.26%	113%	4.89	0.07	33.7	-17.81	2.80
XRP	1.48%	184%	5.74	1.28	179.4	-27.22	2.02
BCH	0.81%	197%	3.59	0.62	54.0	-25.7	1.03
ADA	3.00%	255%	8.84	2.08	136.7	-25.08	2.96
LTC	1.05%	128%	6.8	1.61	66.6	-16.55	2.06
XEM	1.54%	169%	18.01	3.39	170.6	-18.23	2.29
XLM	1.45%	196%	2.98	0.44	106.1	-20.87	1.86
MIOTA	0.70%	182%	4.23	0.25	46.8	-31.41	0.97
DASH	1.13%	121%	4.61	0.1	54.9	-20.28	2.35
NEO	1.91%	194%	4.2	0.32	122.8	-22.14	2.47
XMR	0.90%	122%	3.58	-0.11	53.8	-17.25	1.85
BTG	-1.08%	339%	5.73	0.46	100.2	-35.82	-0.81
QTUM	0.75%	198%	7.52	0.71	75.1	-34.73	0.95
XRB	2.53%	236%	2.81	-0.08	102.4	-25.67	2.70
JPY	-0.02%	8%	3.64	-0.84	1.8	-1.09	-0.66
EUR	0.06%	7%	2.9	0.58	1.4	-0.52	1.74
AUD	0.03%	7%	3.42	0.21	2.0	-0.7	0.85
CHF	-0.02%	7%	2.61	-0.15	1.5	-0.95	-1.00
USD	-0.04%	6%	2.61	-0.4	1.0	-0.78	-2.22
EQUAL WEIGHT CRYPTO PORTFOLIO	**1.49%**	**116%**	**3.06**	**-0.33**	**27.4**	**-15.28**	**3.23**
TOP6 CRYPTO PORTFOLIO	**1.24%**	**108%**	**4.59**	**0.24**	**31.0**	**-19.69**	**2.89**

While the nominal returns are impressive, these cryptocurrencies have also clearly experienced significant realized volatility. The average annualized volatility is well over 100%. Moreover, while some of the Sharpe Ratios of the top 15 cryptocurrencies are large, neither their average Sharpe Ratio (1.85), nor their single largest Sharpe Ratio (ADA=2.96), exceed the Sharpe Ratio of 3.2 for the S&P500 index in 2017.

Examining the time series properties of the top 15 cryptocurrencies yields insights into opportunities to improve the risk-return tradeoff that this asset class offers investors. An equally weighted portfolio of the top 15 cryptocurrencies (EQUAL WEIGHT CRYPTO PORTFOLIO) would have outperformed the individual currencies substantially on a risk-adjusted basis, achieving a Sharpe ratio of 3.23, with a mean daily return of 1.49% - both in excess of the S&P 500, as well. This is due to the relatively low average correlation between cryptocurrencies. On average, the remaining 14 of the top 15 cryptocurrencies display a correlation of just 0.28 with Bitcoin (BTC).

Moreover, none have a correlation of over 0.50 with Bitcoin (BTC). Basic portfolio theory indicates that there are large benefits to be reaped from diversification within an asset class displaying these properties.

Table 3 – Correlations of Cryptocurrency Returns

	BTC	ETH	XRP	BCH	ADA	LTC	XEM	XLM	MIOTA	DASH	NEO	XMR	BTG	QTUM	XRB
BTC	1.00	0.35	0.10	0.19	0.19	0.43	0.02	0.33	0.36	0.31	0.22	0.45	0.21	0.34	0.36
ETH	0.35	1.00	0.37	0.50	0.29	0.73	0.43	0.37	0.35	0.58	0.65	0.54	0.53	0.51	0.41
XRP	0.10	0.37	1.00	0.30	0.59	0.32	0.43	0.54	0.19	0.30	0.35	0.31	0.29	0.40	0.44
BCH	0.19	0.50	0.30	1.00	0.22	0.35	0.33	0.21	0.25	0.64	0.54	0.54	0.63	0.50	0.33
ADA	0.19	0.29	0.59	0.22	1.00	0.27	0.41	0.69	0.48	0.24	0.31	0.46	0.21	0.29	0.29
LTC	0.43	0.73	0.32	0.35	0.27	1.00	0.55	0.36	0.47	0.50	0.35	0.43	0.35	0.51	0.39
XEM	0.02	0.43	0.43	0.33	0.41	0.55	1.00	0.47	0.43	0.29	0.36	0.31	0.28	0.35	0.10
XLM	0.33	0.37	0.54	0.21	0.69	0.36	0.47	1.00	0.58	0.24	0.41	0.60	0.20	0.30	0.28
MIOTA	0.36	0.35	0.19	0.25	0.48	0.47	0.43	0.58	1.00	0.31	0.23	0.61	0.27	0.37	0.43
DASH	0.31	0.58	0.30	0.64	0.24	0.50	0.29	0.24	0.31	1.00	0.41	0.63	0.59	0.38	0.37
NEO	0.22	0.65	0.35	0.54	0.31	0.35	0.36	0.41	0.23	0.41	1.00	0.53	0.32	0.39	0.28
XMR	0.45	0.54	0.31	0.54	0.46	0.43	0.31	0.60	0.61	0.63	0.53	1.00	0.47	0.43	0.45
BTG	0.21	0.53	0.29	0.63	0.21	0.35	0.28	0.20	0.27	0.59	0.32	0.47	1.00	0.43	0.27
QTUM	0.34	0.51	0.40	0.50	0.29	0.51	0.35	0.30	0.37	0.38	0.39	0.43	0.43	1.00	0.41
XRB	0.36	0.41	0.44	0.33	0.29	0.39	0.10	0.28	0.43	0.37	0.28	0.45	0.27	0.41	1.00
JPY	0.10	-0.02	-0.02	-0.13	0.06	0.05	0.14	-0.04	0.17	0.12	-0.32	0.00	0.18	0.01	0.00
EUR	-0.16	0.17	0.04	0.15	-0.08	-0.04	-0.02	-0.10	-0.19	0.16	0.15	0.00	0.06	0.14	-0.04
AUD	-0.27	0.16	0.44	0.06	0.11	0.12	0.08	0.09	-0.17	0.08	0.13	0.10	0.02	0.14	0.09
CHF	0.14	-0.04	0.00	-0.11	0.09	-0.07	0.01	0.11	0.24	-0.04	-0.07	0.06	0.09	-0.10	0.12
USD	0.25	-0.03	-0.03	-0.08	0.11	0.16	0.13	0.16	0.32	-0.07	-0.08	0.10	0.09	-0.02	0.10
EQUAL_WEIGHT	0.33	0.69	0.66	0.58	0.47	0.62	0.56	0.52	0.51	0.59	0.67	0.62	0.47	0.59	0.74
TOP6	0.37	0.64	0.89	0.44	0.59	0.60	0.53	0.66	0.37	0.50	0.49	0.51	0.45	0.56	0.49
USCORP	-0.07	-0.16	0.22	-0.23	0.09	-0.05	0.00	0.24	-0.02	-0.31	-0.01	0.08	-0.14	-0.17	-0.05
USAGG	-0.04	-0.16	0.24	-0.22	0.09	-0.06	0.01	0.26	-0.04	-0.31	0.00	0.08	-0.19	-0.17	-0.02
USGOVT	-0.04	-0.16	0.24	-0.23	0.09	-0.04	0.02	0.26	-0.04	-0.32	-0.01	0.07	-0.19	-0.17	0.00
GLOBALBOND	0.04	0.00	0.14	0.01	0.08	-0.10	-0.10	0.17	-0.20	-0.04	0.22	0.20	0.06	0.07	-0.01

	JPY	EUR	AUD	CHF	USD	EQUAL_WEIGHT	TOP6	USCORP	USAGG	USGOVT	GLOBALBOND
BTC	0.10	-0.16	-0.27	0.14	0.25	0.33	0.37	-0.07	-0.04	-0.04	0.04
ETH	-0.02	0.17	0.16	-0.04	-0.03	0.69	0.64	-0.16	-0.16	-0.16	0.00
XRP	-0.02	0.04	0.44	0.00	-0.03	0.66	0.89	0.22	0.24	0.24	0.14
BCH	-0.13	0.15	0.06	-0.11	-0.08	0.58	0.44	-0.23	-0.22	-0.23	0.01
ADA	0.06	-0.08	0.11	0.09	0.11	0.47	0.59	0.09	0.09	0.09	0.08
LTC	0.05	-0.04	0.12	-0.07	0.16	0.62	0.60	-0.05	-0.06	-0.04	-0.10
XEM	0.14	-0.02	0.08	0.01	0.13	0.56	0.53	0.00	0.01	0.02	-0.10
XLM	-0.04	-0.10	0.09	0.11	0.16	0.52	0.66	0.24	0.26	0.26	0.17
MIOTA	0.17	-0.19	-0.17	0.24	0.32	0.51	0.37	-0.02	-0.04	-0.04	-0.20
DASH	0.12	0.16	0.08	-0.04	-0.07	0.59	0.50	-0.31	-0.31	-0.32	-0.04
NEO	-0.32	0.15	0.13	-0.07	-0.08	0.67	0.49	-0.01	0.00	-0.01	0.22
XMR	0.00	0.00	0.10	0.06	0.10	0.62	0.51	0.08	0.08	0.07	0.20
BTG	0.18	0.06	0.02	0.09	0.09	0.47	0.45	-0.14	-0.19	-0.19	0.06
QTUM	0.01	0.14	0.14	-0.10	-0.02	0.59	0.56	-0.17	-0.17	-0.17	0.07
XRB	0.00	-0.04	0.09	0.12	0.10	0.74	0.49	-0.05	-0.02	0.00	-0.01
JPY	1.00	-0.35	-0.44	0.59	0.46	-0.03	0.05	-0.40	-0.44	-0.42	-0.48
EUR	-0.35	1.00	0.48	-0.75	-0.86	0.06	0.08	0.00	0.05	0.03	0.53
AUD	-0.44	0.48	1.00	-0.57	-0.52	0.18	0.31	0.43	0.45	0.45	0.48
CHF	0.59	-0.75	-0.57	1.00	0.78	-0.01	-0.01	-0.24	-0.29	-0.29	-0.52
USD	0.46	-0.86	-0.52	0.78	1.00	0.04	0.02	-0.15	-0.20	-0.18	-0.54
EQUAL_WEIGHT	-0.03	0.06	0.18	-0.01	0.04	1.00	0.80	-0.04	-0.02	-0.01	0.07
TOP6	0.05	0.08	0.31	-0.01	0.02	0.80	1.00	0.09	0.12	0.12	0.13
USCORP	-0.40	0.00	0.43	-0.24	-0.15	-0.04	0.09	1.00	0.98	0.98	0.53
USAGG	-0.44	0.05	0.45	-0.29	-0.20	-0.02	0.12	0.98	1.00	1.00	0.56
USGOVT	-0.42	0.03	0.45	-0.29	-0.18	-0.01	0.12	0.98	1.00	1.00	0.54
GLOBALBOND	-0.48	0.53	0.48	-0.52	-0.54	0.07	0.13	0.53	0.56	0.54	1.00

In particular, these characteristics make cryptocurrencies an attractive asset class for securitization. A large securitized pool of major cryptocurrencies would offer investors higher risk-adjusted returns than a smaller portfolio of individual cryptocurrencies. A standardized securitized product would also likely allow investors to benefit from greater liquidity and reduced transaction costs while foregoing the need to manually rebalance their portfolios.

However, one aspect of the dynamic of returns is worth noting. Namely, while the average correlation between the cryptocurrencies is quite modest, this masks an underlying latent correlated crash risk. Namely, when examining the daily return series, while the infra-marginal (i.e., normal) days show low correlations, the extreme negative return realization days seemed to be shared by all of the currencies. For example, on December 22, 2017, several currencies experienced simultaneous declines in excess of 20%. This results in the diversified

portfolio of cryptocurrencies experiencing daily return realizations of such magnitudes as -10%, -13%, and even -20% (January 10, 2018). And while some cryptocurrencies are negatively correlated on a day-to-day basis, a cumulative crash risk persists

Along with this crash risk (and correlated crash risk), a second challenge faced by this asset class are the transactions costs. Due to limitations in the underlying protocol, Bitcoin transaction costs have soared over the past year, from $0.296 per average transaction in January 2017 to $28.91 currently. Bitcoin transactions do not carry a mandatory fee payment. Rather, a transacting party can include a fee as an incentive for miners to process the transaction. Miners convert this incentive to a fee-rate, which is defined as the incentive fee divided by the transaction size in vbytes. Since only a fixed amount of transactions can be processed at any given time, miners will prioritize orders with high fee rates. This leads to transaction fees spiking in times of market volatility, such as during the December 22nd, 2017 pullback across currencies. It was precisely on that date that the highest average transaction costs in the history of bitcoin were observed, reaching $55.16. Thus, these two problems also seem to not be independent, sharing the same crash-risk negative realizations.

Any index product that relies on continuous rebalancing would be highly exposed to this phenomenon, since it would be required to rebalance most at times when transaction costs are highest. This technically-induced liquidity risk comes on top of the positive correlation between bid-ask spreads and volatility observed across traditional securities exchanges.

We discuss in more detail in Section V the specific mechanics and novel characteristics of our proposed procedure that will help to mitigate both of these concerns.

III. Overview and Background on Securitization

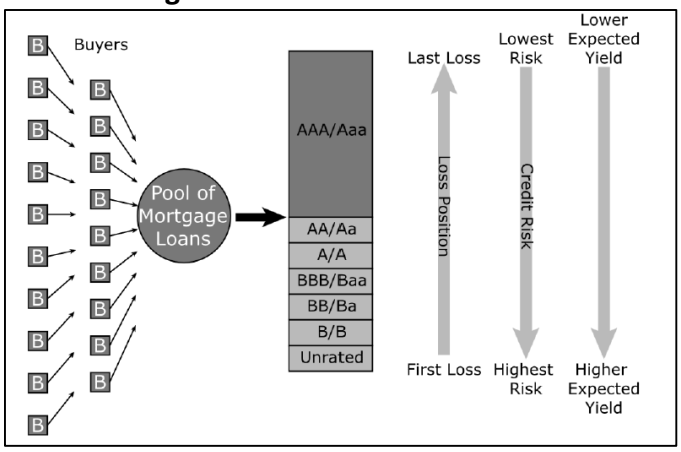
The risk associated with any security can be decomposed into idiosyncratic and systematic risk. Idiosyncratic risk is peculiar to a specific security, uncorrelated across securities, and may be eliminated through diversification. Systematic risk arises from common factor exposure across securities and persists within an asset class regardless of the degree of diversification within the asset class. Finance theory holds that investors are only compensated for non-diversifiable, systematic risk. A well-diversified investor, therefore, will eliminate idiosyncratic risk by holding a sufficiently large basket of securities exhibiting uncorrelated idiosyncratic risk.

A. Collateralized Debt Obligations (CDOs)

Collateralized Debt Obligations (CDOs) are structured asset-backed securities. They are comprised, for example, out of collateral pools of mortgage, credit card, and auto loan securities. CDOs are differentiated from a simple portfolio of their underlying asset basket via the structuring process. The structuring process comprises of assembling a basket of assets with non-zero default risk as collateral in an off-balance-sheet special purpose vehicle. Against this collateral, a prioritized capital structure of claims is issued. The individual positions in this capital structure are referred to as *tranches*. The most senior tranche has the first claim on cash flows from the pool of collateral; the most junior tranche receives the residual cash flow remaining once all other tranches have been paid off. When a small number of defaults occur in the collateral pool, the junior tranche is the first and only tranche to be affected. Only once all more

junior tranches have become worthless, losses are imposed on the most senior tranche.[2]

Figure 4. CDO Collateral Pools



The key factor determining the ability to create tranches that are safer than the underlying collateral is to extent to which defaults are correlated across the underlying assets. The lower the correlation, the safer the senior-most claim.

B. Synthetic CDOs

Synthetic CDOs resemble cash flow CDOs in principle with the key distinction being that they are based on a collateral pool of derivatives, most commonly credit default swaps (CDS). The cash flow is derived from premiums collected from writing the underlying credit default swaps.

Synthetic CDOs were initially structured to allow commercial banks to optimize their

[2] Consider the following example: Three bonds pay $0 each conditional on default and $1 each otherwise. We pool these securities in a portfolio, such that the total notional value of the underlying fund is $3. Three $1 claims are issued against the underlying capital structure. The junior tranche defaults if any of the three bonds default, the middle tranche defaults if two or more of the bonds default, and the final, senior-most tranche only defaults when all three bonds default. Structuring allows originators to create securities of a target credit rating by tailoring their cash flows (as measured by likelihood of default and loss given default) to satisfy the guidelines set forth by the credit rating agencies. By 2007, there were 37,000 structured finance issues rated AAA; 60% of all global structured products, vs. 1% of all corporate issues.

balance sheet and regulatory capital usage, while maintaining incentive alignment grounded upon their credit risk monitoring comparative advantage by sourcing term liabilities from wholesale market. Synthetic CDOs allow the most efficient tailoring of desired cash flow, market and credit risk exposures. The cash flow and synthetic securitization technology continues to find applications, away from the original mortgage loan pooling and now on to consumer, student, auto, SME loans, and almost any stable and predictable cash flow imaginable (including film, pharma royalties, insurance and reinsurance premia, aircraft leases, and more).[3]

IV. On Public and Private Safe Assets: History, Motivation, Category Drawbacks & the Safe Asset Shortage Debate

We motivate our approach towards developing our risk sharing platform by situating our ideas within the broader context of "safe assets" and their provision. We also juxtapose our theoretically, real-world validated economic actor balance sheet consistent framework, with some basic misunderstandings of the quantity theory's tautological aspects that sadly pass for monetary policy discourse in the cryptocurrency space.

Economic agents require assets to store value with an eye towards coping with foreseen and unforeseen difficulties. In all aspects of economic activity, a fundamental demand for safety manifests itself. A safe asset can be defined as an asset taken at face value with "no questions asked" (NQA) (Holmström, 2015). By design it should not benefit an agent to procure information about its value; instead this information should be common knowledge. Thus the ownership of a

[3] In the Appendix we also discuss the properties of CDO^2 securities, which are particularly sensitive to non-linear correlations, as evidenced in the sub-prime mortgage crisis, by directly quoting from Coval et. al (2009).

safe asset carries low liability risk.

A safe asset can be functionally defined as a simple debt instrument that is expected to preserve its value during adverse systemic events (Caballero et al., 2017). This definition emphasizes the three imperative safe asset characteristics. First, safe assets need to be informationally insensitive, i.e. they can be transacted without much analysis and without much concern about adverse selection. Second, safe assets need to be simple, which takes special significance at times of complex economic crises. Lastly, an asset is perceived safe if others expect it to be safe. (As a preview of our platform's foundational argument we highlight that the blockchain ecosystem lends itself naturally to producing "ecosystem native" safe assets. This is due to the fact that distributed ledger technology (DLT) allows for information sharing, simplicity by virtue of open source foundations, and also "safety externalities", which we will be defining as constant recalibration of safety based on the ecosystem's transactional information content. Naturally, the ambition follows to render these "safe assets" relevant to the broader non-crypto "safe asset" universe.)

Assets vary according to their sensitivity to risk factors and their degree of liquidity. The latter can sometimes be thought of as another risk factor priced in equilibrium, sourcing its premium from the covariance of the pricing kernel with the difficulty of obtaining funding, (see Brunnermeier (2008), for example). An asset's own liquidity is the relative speed and ease with which the asset can be sold on a secondary market (Morellec, 2001). A liquid asset can be sold quickly without having to reduce its price to a significant degree, satisfying sudden needs for consumption or investment. Safe assets are typically very liquid, although by construction some can be illiquid (e.g. insured savings deposits). The specialness of safe assets implies the existence

of 'non-pecuniary returns' (convenience yield), in the form of liquidity and safety (Gorton and Ordonez, 2013).

A. The History of Safe Assets

Gorton (2017) argues that almost all of human history can be written as the search for and production of safe assets. Historically, the quintessential safe asset was the gold coin; more recently, the typical safe assets are government-insured demand deposits and short dated G-3 government securities. Sovereign issued safe assets took centuries to develop. Sovereign debt was historically issued to raise funds to fight wars, and default was commonplace. Further developments in political and power structure had to occur before sovereign debt could eventually be viewed as safe (Gorton, 2017).

In summary, there are two ways to produce safe debt: back it by a government's taxing capacity, or by credible collateral. The U.S. Department of the Treasury issues Treasury bonds (Treasuries), which are backed by the Federal Government and are considered safe by investors (albeit admittedly not by the crypto community at large). If anything, a big part of the crypto asset space's increasing growth as well as the quasi-religious fervour associated with some of the acolytes, relates to the Damascene conversion of erstwhile "gold-bugs." This further motivates our work, to "value-agnostically" allow this community to express their monetary / store of value leanings, utilising the "enemy's technology," adapted and augmented for the crypto universe) as risk free.[4]

[4] An additional source of safe assets come from states or cities that issue municipal bonds, which are backed by the

Treasuries have a "money-ness" attribute. When there aren't enough of them, the private sector produces substitutes, at times making the economy fragile. Producing informationally insensitive safe assets is difficult and has historically depended on technology, legal institutions and contract design. Initially, gold coins had several problems that rendered them informationally sensitive (e.g., clipping, weighing, special certification expertise). Later, bills of exchange were the first form of privately produced safe assets (and led to the first financial crises); for them to become money-like, the legal infrastructure needed to develop to provide substance and enforceability to the statement 'pay to bearer.' Gorton, Lewellen, and Metrick (2010) make the point that there is a stable fraction of safe assets to total assets in the US economy, and that the privately produced component has always been substantial.

Privately produced safe debt has the drawback that it is vulnerable to runs were there to be an absence of government backed deposit insurance. Convertibility (short maturity) is important to these debt claims so as to monitor the issuers' creditworthiness, i.e., how it can be assured that the debt is backed. Various solutions have been utilized, from the Suffolk bank system monitoring, to joint liability of endorsers, to government backed deposit insurance or private clearinghouses.

Bank debt can be viewed as a form of insurance allowing agents to smooth consumption over time. For Holmstrom and Tirole (1998; 2001), safety refers to instruments (market and non-market) that can be used to transfer wealth across periods. Short-term safe assets are money or money-like, and long-term safe assets can store value or serve as collateral. Short-term debt

local government's ability to collect tax. Finally, companies issue corporate bonds, which are backed by the issuing company's ongoing operations and sales, or its assets.

issued by the financial sector may provide a closer substitute for short-term Treasuries than long-term Treasuries due to their "money-ness". Liquidity means insuring against the forced liquidation of an investment project in light of an unanticipated shock by holding 'liquid' assets. A bank can hold and distribute liquidity, but in the face of an aggregate shock this solution breaks down, which can require the government to provide liquidity via government bonds.[5]

B. Safe Asset Scarcity

Production capacity of public and private safe assets depends on sovereign fiscal capacity, exchange rates, and price stability track records. Financial system development has thus historically been concentrated among advanced economies, especially the US. The global supply of safe assets hasn't kept up with global demand, manifesting itself in lower interest rates. This shortage of safe assets has distorted financial system incentives towards manufacturing substitutes and encouraging weak sovereigns to attempt engineering their own pseudo-safe assets. The advent of the financial crisis both reduced supply and increased demand for safe assets due to deleveraging pressures, attenuated precautionary motives, institutional developments, and well-intended policies with undesirable side effects.

[5] A financial crisis is an event during which safe debt with NQA attributes becomes suspect. The recent financial crisis was a story of privately produced debt backed by privately produced long-term debt (which both started life as safe assets and turned out to be nothing like it). Holders of short-term debt questioned the backing and started a run on the bank (which during the financial crisis turned out to be SIVs and their asset backed commercial paper (e.g., BNP Money Markets fund), wholesale funded commercial banks (e.g., Northern Rock), repo and prime brokerage client assets' funded investment banks (e.g., Bear Stearns), collateral calls against derivatives claims with originally perceived remote risks (e.g., AIG)). When this switch from information insensitive to information sensitive debt takes place, the optimal response may well be, crucially, not to reveal more information as this will cause further unraveling. This intuition fails though in a decentralized, mutual trust based system, like the blockchain. Information is constantly available to the community.)

Exiting a safety trap (an acute form of a liquidity trap, where injections of cash/lower interest rates fail to stimulate aggregate demand) requires an increase in the supply and decrease in the demand of safe assets, independent of the supply / demand dynamics in other asset classes. Safe interest rates are declining toward their effective lower bounds with the global economy operating below potential. A relative decrease in global wealth and output suppresses relative safe asset demand. Eichengreen (2016) provides a list of the pool of global safe assets underlining its precipitous decline post the financial crisis. Correspondingly, a secular decline in interest rates has been exacerbated, whereas returns on physical capital and expected return on equity have stayed high.[6]

The public good nature of safe assets, i.e. their underproduction versus the societally optimal levels, and the rendered inability of the private sector to produce systemic-risk remote

[6] Note that the following discussion draws heavily from the insights of Caballero, Farhi, and Gourinchas (2017). The main market mechanism to restore equilibrium when safe asset shortage is prevalent is a valuation increase via an interest rate adjustment, which is hampered by the effective lower bound / reversal rate. When we consider open economies, the second margin of adjustment is the exchange rate. In situations where the interest rate is above the full employment consistent real rate, this implies a margin of allocation of global recession dynamics induced by the safety trap which is dependent on relative exchange strength, and domestic producers in the safe asset producing country face an extra burden. Safe assets exhibit public good characteristics. Their issuance benefits are diffused globally and the costs in terms of future imbalances are born locally, whereas beggar-thy-neighbor devaluation costs are born globally and benefits accruing locally. The obvious solution to the shortage of safe assets is for government to issue more of them, but one runs the risk of a coordination failure induced rollover risk and crowding out of private sector substitutes. The fiscal capacity of the government in question is a function of its credibility regarding future tax generating capacity, which can in turn be impaired, as witnessed recently by the violation of the capacity condition by weak Eurozone sovereigns. Policies that increase the supply of safe assets, by exchanging positive beta with zero beta assets stimulate aggregate demand and output. Still, the concern is raised that increasing issuance of safe assets to fulfill global demand may weaken the fiscal capacity of core sovereigns. Core economies are growing weaker than emerging economies and demographic factors are both increasing their own demand for safe assets and reducing their tax generating capacity. If the public sector is not satisfying the demand for safe assets, the private sector is incentivized to do so by financially engineering substitutes. Since safe debt should be one that can be used without being taken advantage by privately informed agents, by tranching cash flows, information is tranched. Financial engineering in the form of pooling of risk of quasi-safe issuers so as to create a layer of safe assets backed by existing securities can help towards alleviating the scarcity. Sufficient overcollateralization may not be enough as the ability of the private sector to self-insure against a truly systemic event is limited, as even the most senior tranches may be subject to an uninsurable tail risk.

ones, motivate our ambition towards satisfying this need via crypto-backed safe assets. We will be working towards addressing shortcomings of the privately produced ones, humbled by the consistent failures up to now, and harnessing the power of DLT. This will allow us to isolate the systemic crypto-correlated crash risk component, which in turn aspires to act as a diversifier against "fiat economy systemic risk."

C. Fiscal Theory of the Price Level

The quantity theory of money attempts to provide testable predictions about the determination of the nominal value of aggregate income. Irving Fisher (1911) described the link between the quantity of money M (the money supply) and the amount of spending on final goods and services produced in the economy (aggregate nominal income for the economy, or nominal GDP) $P \times Y$, where P is the price level and Y is aggregate output (income), with the following equation:

$$M \times V = P \times Y$$

where V is the rate of turnover of money, or the velocity of money. Irving Fisher argued that velocity is fairly constant in the short run, which implied that nominal income as well as the price level is determined solely by movements in the quantity of money (Fisher, 2006). How good a store of value money is depends on the price level, because its value is fixed in terms of the price level (Mishkin, 2007). This (alongside Hume's price-specie flow mechanism and its exchange rate fluctuation implications from the mid-1700s) was the beginning of how economists have worked hard to translate, what is, in essence, a trivial accounting identity, into a business cycle fluctuation

and price level determination theory. It found its crowning achievement in the broad acceptance a few decades ago of Milton Friedman's dictum that "inflation is always and everywhere a monetary phenomenon."

Unfortunately, the "dividend split" implications of the story (where if we halve money in circulation, prices halve in equilibrium), without any regard for transition dynamics, realism and the wealth of understanding about frictions and institutional factors, is the primary ammunition the crypto community utilises to motivate the crypto currency phenomenon. And of course the reality is more subtle than claims that "governments are drowning us in debt/money, hence money is debased." And even more pernicious are claims such as: "because of increases in government debt/money, I can now define something as 'scarce' and by definition it is worth something, because fiat money isn't scarce."

Based on monetarist quantity theory-backed theoretical foundations, the two conventional macroeconomic policy assignments determining the aggregate price level and stabilizing government debt had been assigned under the rubric of "monetary policy" to the central bank, and as 'fiscal policy' to the fiscal authorities. The real theory of the price level, or fiscal theory of the price level, reverses these assignments. The intellectual framework on how we approach macroeconomic issues and the associated implications for coin issuance and valuation on the blockchain, become profoundly different under certain conditions. As noted by Sargent (1994), "Persistent high inflation is always and everywhere a fiscal phenomenon."

Two equilibrium conditions are central to price level determination in all models. The quantity theory of money and the fundamental asset pricing equation link the real market value of nominal government liabilities to the expected present value under the pricing kernel of all

the future primary government surpluses. The quantity theory of money is static and is an identity. The second condition is dynamic, holds in equilibrium and embodies agents' optimization.

The key insight that underlies the real theory is that the ability of government to affect the aggregate price level (i.e., the relative price of goods and nominal government liabilities) comes from its power to tax. It is the fiscal backing that gives fiat money, intrinsically useless, its value. Lerner (1947) views money as a creature of the state, and points out that money's general acceptability, which is an all-important attribute, stands or falls by its acceptability by the state. Bell (2001) shows that the state's power to make and enforce tax laws renders its money the most acceptable form of debt within what can be considered a hierarchy of monies.

By expanding the perspective to consider monetary and fiscal policies jointly, the theory can provide testable implications in a variety of areas.[7] These economic activities can all affect the price level, and serve as potential risk factors to assets. We will discuss a decentralized system with sufficient trust from the public in the rest of the paper. Such a system, built using the technologies of cryptocurrency and blockchain, can potentially minimize those risks.

V. Introduction to Nomisma and the Securitized Blockchain

A primary contribution of the Nomisma platform will be to complete the cryptocurrency

[7] For instance, about the macroeconomic impact of normalizing rates, about how it matters whether a government issues indexed or nominal debt, about the consequences of an interest rate peg, about how quantitative easing actually works, and about how inflation reacts to interest rate hikes or cuts.

"state-space" of assets, thus rendering this asset class amenable and desirable to a wider class of investors. We employ straightforward financial engineering tools to accomplish the task.[8]

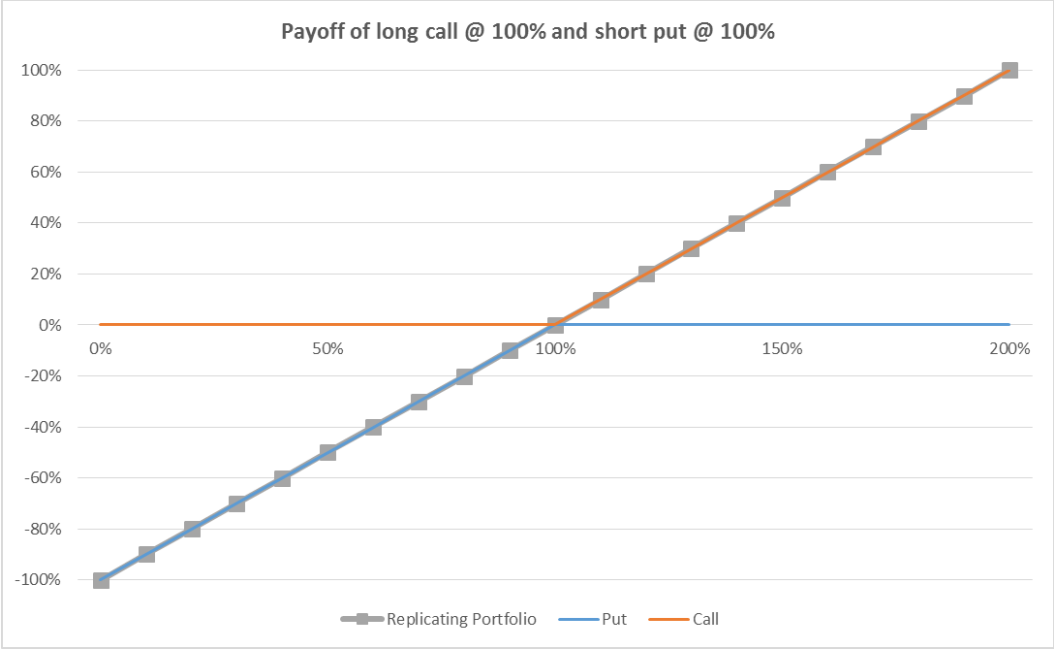
A. Initial Mechanics

We can begin with the simplest short put / long call combination, struck at the current spot price, which implies a convenience yield / implied funding rate for the underlying in question. This allows one to derive an interest rate curve across time, across different crypto-coins.

The first step of our approach is best illustrated through a specific example. Suppose the underlying is Ether. The ETH payoff at time t=1, assuming t= 1 year, is a 45 degree line intersecting the x axis (the Ethereum price in dollar terms) at the current spot price, which we define as 100 (100% of the spot price). The Y-axis is defined as the payoff of any options on Ether. We can decompose the 1 payoff profile of owning 1 ether, into the payoff of being long a 1 year call struck at 100 plus the payoff of being short a put struck at 100.

Figure 5. Replicating Portfolio Payoffs

[8] Also see the **Appendix** (Section 6) for a technical overview of the construction of the Nomisma platform.



The Nomisma Foundation will launch a Transaction that invites bids for the 100 strike calls and offers for the 100 strike puts. There is a Subscription Period for a Transaction launch that allows for a series of bids and offers to be submitted. The resulting steps are as follows:

A Nomisma T-token (NTT, T for "Transaction") is launched together with the platform, which provides the holder with the ability to submit bids / offers during the Subscription Period and is priced so as to cover the platform's Ether mining costs as well as to generate a transparent profit margin associated with the platform usage. The NTT can thus be defined as the token that gives you the right to partake in the platform's capability; it can derive value from establishing that on a first round of tranching, Nomisma revenues include a fee paid every time a full capital structure gets agreed upon and launched, which then gets divided equally (notionally adjusted when tranches are not symmetric around 100% of spot) across tranches for all the costs associated with maintaining the platform. These tokens will be launched with a prospective finite supply and a crypto-standard 'monetary policy'.

Now let us assume that the lowest put offer received is P and the highest call offer received is C. These can be expressed either in fiat or ETH terms. Obviously, selling a put earns the Transaction participant a return at time 0, while buying a call is an out-of-pocket expense for the Transaction participant. Instead of getting paid the premium for the short put exposure, the Transaction participant will pay upfront$(100 - option\ premium\ equivalent\ p)(= P$, which is the equivalent of a zero coupon bond.

$$\text{i. if } P + C < ETH(0), \text{then the Transaction is NOT launched}$$

$$\text{ii. if } P + C \geq ETH(0), \text{then the Transaction is launched}$$

A contract is defined that allows the following steps. The Platform is obliged to keep $(P + C)$ in escrow for the duration of the Transaction. At maturity, escrowed ETH are split according to ETH price at maturity between the put seller / zero coupon bond holder and the call buyer. Note that at the Transaction's launch, it could well be the case, that $P + C > \text{ETH } (0)$, so there is 'excess collateral' in escrow. The Nomisma H-token (for "Hedge") will be launched together with the platform, which entitles holders to partake of the hedge gains associated with all Transactions. These too will be launched on a crypto-standard monetary policy with embedded scarcity, either upfront or eventually.

Expanding further, more generally we can assume an underlying commodity that follows a stochastic process. One can set up the following decomposition of the associated risk exposure from time 0 to time 1 and price today $p(0)$, between D and E:

$$\text{if } p(1) > p(0), \qquad E(1) = p(1) - p(0), D(1) = p(0)$$

$$\text{if } p(1) < p(0), \qquad E(1) = 0, D(1) = p(1)$$

$p(1) = E(1) + D(1)$, thus one should expect $p(0) = E(0) + D(0)$ (this is simply put-call parity in a world where interest rates are zero).

Assuming someone tries to hedge these risk exposures, what constitutes the perfect hedge? One would want to go long the underlying coin at p(0), using the proceeds from selling D and E at prices that should add up to p(0). If they do not add to p(0), one would not sell the decomposition, but rather if they add up to more, one would earn the difference.

So where does this lead? We can now define an underlying commodity "interest rate" = 1 - {D(0)/P(0)} (without loss of generality we can normalize P(0) to 1). Therefore we constructed a (D)ebt and an (E)quity position on the underlying coin, in the spirit of Merton (1973).

Consequently as a first step, we can derive an implied interest curve term structure per coin, which represents the implied interest rates from time t = 1 to T, for example 1 month up to 2 years expiries, backed out from the prices of the 100% strike puts to the corresponding tenors.

Thus, the first stated ambition of the Nomisma platform is to facilitate the creation, take-up, price discovery and liquidity of fixed income-like tailored exposures to crypto-assets. A Transaction participant will be able to bid for a discounted note at her desired implied interest rate, with the corresponding call option allowing the platform to build the replicating hedge portfolio. Our offering will allow the derivation, and ability to take exposure to zero-coupon bonds with price contingent payoffs, which is a foundational step in the development of safe assets on the blockchain.

B. The Creation of a Stablecoin

Now, continuing on with the single underlying coin example from earlier, we can price

and launch Transactions and deliver discounted zero-coupon bonds, which will be priced on a continuum of strikes from 100% up to the strike which equates to an implied funding rate equal to the US government Treasury Bill rate to that date.[9]

Elaborating even further, let us further decompose risk exposure, between S, M and R, where:

$$pD < p(0) < pA$$

$$\text{if} \quad p(1) > pA,\ R(1) = p(1) - pA,\ M(1) = pA - pD,\ S(1) = pD$$

$$\text{if} \quad p(1) < pA,\ p(1) > pD,\ R(1) = 0,\ M(1) = p(1) - pD,\ S(1) = pD$$

$$\text{if} \quad p(1) < pD,\ R(1) = 0,\ M(1) = 0,\ S(1) = p(1)$$

$p(1) = R(1) + M(1) + S(1)$ and similarly at time 0, one would expect $p(0) = R(0) + M(0) + S(0)$.

A "safer/less risky" underlying commodity "interest rate"is defined, as "principal" will be "*impaired*" with a lower probability (p(D)etachment < p(0)), 1-{S(0)/P(0)}. We also define a (S)enior, a (M)ezzanine and a (R)esidual position on the underlying commodity. Naturally, these payoffs are equivalent to a short put, a long call spread and a long call on the underlying and can be priced and risk-managed accordingly.

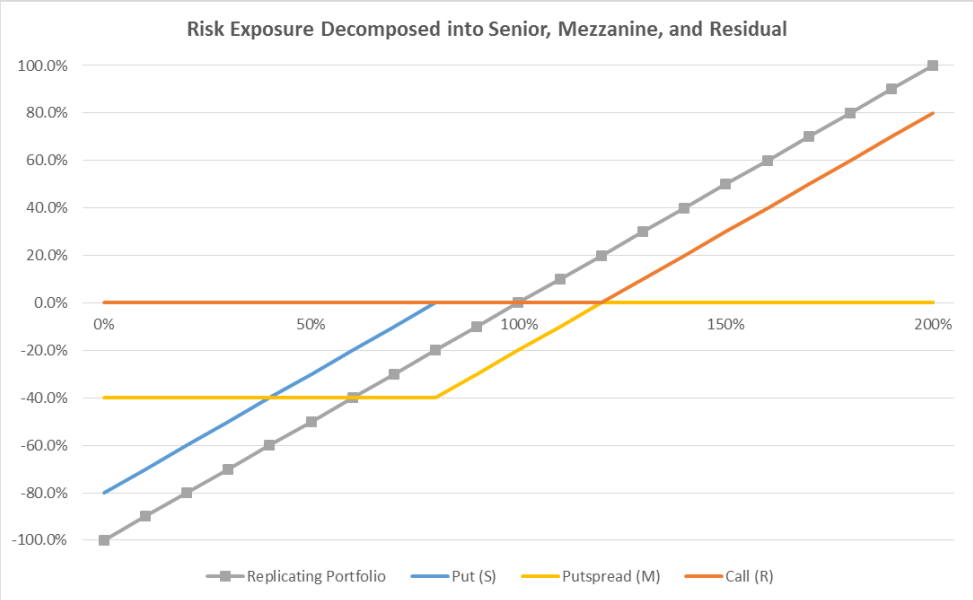
Thus, the market will be able to impute an implied hazard rate curve for each cryptocurrency, which will provide market pricing for each one's relative crash risk and perceived

[9] Note that we purposefully mention T-bills, as in a market where the underlying commodities have, on average, been actively trading for few months or, at most, years, we will be testing the platform and the associated risk management with tenors up to 1 year.

stability. This crucial step will allow the community to direct its investing and funding efforts toward the ones that pass their stability test or equivalently hedge the downside risk of an entrepreneurial venture funded by a promising, but also uncertain, and hence volatile coin.

Continuing with the simple Ether example from earlier, we can also describe a Transaction that consists of a short put at 80% strike, a short put spread between 80-120% of spot and a 120% call. The replicating portfolio remains 1 unit of ETH, which will be escrowed and divided among the Transaction participants at maturity of the Transaction. Both the short 80% put and the short put spread are funded upfront and thus deliver a relatively "safe" (i.e., "senior-type" exposure) and a "riskier" (i.e., "mezzanine-like" exposure) and commensurate implied interest rates.

Figure 6. Risk Decompositions



Here is where we encounter the inklings of how a trivial, but theoretically correct, Stablecoin can be structured versus every underlying coin. It can be defined as the put strike that will render an equivalent interest rate to U.S. T-bills to that same tenor. Any short put contract

can be decomposed into a put with strike S(USD) and a S(USD)/S(Attachment) put spread. The first put is worth a dollar today, discounted by the T-bill rate (or an average of the RRP and IOER rates). At any given point, each crypto coin will have a put strike that will represent its "dollar equivalence," which will be a function of the coin's stochastic process parameters (its volatility, local jumps, and crash risk) and the supply of and demand for implied fixed income exposures. Unlike current "stablecoins" being hypothesized in the blockchain space, it will not be dependent on how a random individual decides to contract or expand supply, or based on an arbitrary number that is minted to create an artificial scarcity. Nor will it be collateralising ERC-20s and issuing another currency, which acts as a unit of account in reality, but at the same time belongs to a foundation that set aside just "a few only" for the "common good."

Consequently, the platform will be able to naturally deliver to the cryptocurrency community a Stablecoin that is market driven, and does not rely on self-serving new coins and trivial algorithms. For every coin, our platform will be imputing a short put strike price that would match the discount rate for an actual dollar (or any actual fiat currency).

A Nomisma ETH/$ (N- ETH/$) is defined as the tranche in the single underlying decomposition, which corresponds to the strike that implies the current dollar collateralized lending rate to that maturity (or whatever is the best riskless fiat proxy; in this case it would be the lending rate to the Fed against government bond collateral, accessible to Fed-Window eligible financial institutions).

When a Transaction Participant buys a fixed income note referencing, for example an 80 strike price put, the moment the full hazard rate curve per underlying coin is market derived and if it turns out for argument's sake that the N-ETH/$ strike is 20%, the participant will end up

owning a N-ETH/$ and being short a 20-80% put spread equivalent note.

They will be able to break-up or reconstitute this decomposition and contractually they will be able to trade them separately. As a service to the community we will be delivering smart contract code that will be automatically subdividing or adding up the market implied N-ETH/$ update strike price. (For example, if at a time, post-launch of Transaction A, the N-ETH/$ strike becomes 15%, because ETH volatility has gone up on a static price environment, or overall downside protection is less well offered, each N-ETH/$ issued at Transaction launch, becomes N-ETH/$ (new) + 15-20% of the put spread tranche). Hence, by virtue of the embedded flexibility these tranches can serve as a Stablecoin and can (and rather should) contractually always, at Transaction maturity, claim a dollar's worth of ETH.

Money-likeness of an asset emanates from lack of information sensitivity. When used in transactions, economic agents are not worried about its future value, at least not in the short term and in most states of the world; hence most money-like assets are mostly short-term, liquid and promise a fixed nominal repayment. Safe assets, by contrast, are perceived not to have exposure to credit, counterparty but also market and interest rate risk.

In normal states of the world, economic actors do not distinguish between these two, but in non-normal times, when perceptions of risk are at their highest, but also because uncertainty of actions of other investors is highest (e.g., due to run risk), public sector liabilities--government bonds, but importantly also, government-backed fiat money--are generally viewed as safer than private sector ones (unless of course non-normal times are caused by the government creating these risks). A Nomisma Generic coin / $ becomes time invariant by virtue of constantly recalculating the loss distribution and constantly adjusting detachment so as to make them

dynamically fungible.

C. Liquidity Considerations

There have been various efforts to launch exchanges that trade derivatives for cryptocurrencies. However, they typically all suffer from a lack of liquidity, which then compounds the structural volatility of the crypto asset class. One of our key contributions is to highlight the fact that these offering do not take advantage of the major insight of derivative pricing, namely pricing by a replicating portfolio.

The Nomisma foundation will launch "full capital structures" per underlying coin, by transparently taking a principal position in any of the components, so as to help the liquidity creation and the ability of the community to take advantage of the opportunities warranted.

We expect the following actions from two sets of early adopters:

1. Holders, especially early holders, to be better sellers of calls / call spreads and buyers of puts / put spreads, which *prima facie* would not provide for a natural source of liquidity in the initial stages.
2. New potential investors, which is the group that we feel will be attracted by the first batch of the new structures available, either engaging in "target buying," i.e., selling lower-strike puts so as to enter a cryptocurrency at their preferred level and earn an income while waiting, or "upside buying," i.e., spending a small premium in the hope of an outsized return.

Importantly, both sides are not needed for liquidity creation for these structures. A full

capital structure embeds its natural hedge; the underlying coin, which the foundation will be holding in escrow, will be on a smart contract formulaic basis and be transparently accessible to the holders / writers of the puts / calls spreads / calls.[10]

Liquidity Challenge& Nomisma's Insight

An initial reading of our proposal – and the above - may elicit concerns about the challenge of generating sufficient liquidity so as to incentivize buyers and sellers of each potential exposure to reveal their preferences and match their desired payout profiles. In other words, if there is a mismatch of those who want to purchase a portion of the security payoff distribution (e.g., "upside") and those who would like to provide that portion (i.e., write the upside), then no transaction would occur. The bottom line is that without sufficient crossings of supply and demand, there is illiquidity, and markets endogenously do not develop, and likely fail.

This is the quintessential issue surrounding launches, and has plagued development in this space. Successful launches of products on exchanges as well as exchanges themselves simply need critical mass of two-way flow.

Nomisma solves this in a number of powerful, innovative, and transparent ways. In order to see this, imagine the payoff diagram of a single crypto coin. This can be decomposed into an infinite number of sub-payoffs, but without loss of generality, consider the simple Put-Call Parity

[10] How does one apply, in a straightforward fashion, the same insights, in order to transparently construct the other side? The hedge for a short call / long put combination is short the underlying coin. We can write a smart contract that commits the seller of the call to pledge the underlying coin as collateral; the premium is paid that similarly stays in escrow and gets settled at expiry.

implied N=3 payoff replication case. One can easily deconstruct the value of the underlying into a: i.) bond-like payoff, augmented with positions in ii.) call, and iii.) put payoff claims. Instead of forcing investors to buy all three of these in an inseparable bundled product, we unbundle the payoffs, and allow investors to buy and sell each.

As mentioned above, all current holders of crypto could provide the natural counterparties to each one of contracts. Along with these, we believe other speculators will provide natural counterparts to a bond-preference investor in the crypto coin. However, Nomisma Foundation itself will also be a backstop and liquidity creator ensuring, backstopping, and functionally assuaging any fears of illiquidity. How would Nomisma do this? Nomisma, will amass a certain stock of crypto coin (call it S). With S, it will break apart each coin, and strip it into its separate payoff units (i.e., bond payoff, long call, short call, long put, short put, etc.). It will then list these decomposed claims, and allow market forces to determine the relative prices of each. In this way, supply and demand – the bedrock of every well-functioning market – will ensure the liquidity of each claim, and along with the law of one price, that it is priced at its efficient value and sourced according to market desire. This backstop along with crossing intermediation will allow Nomisma to drastically reduce the number of counterparties required, and ensure that liquidity and efficient scale is quickly achieved.

Nomisma Market - Simple Example

Indeed, at first glance, focusing for simplicity's sake on one underlying and 2 products, let's proceed with the thought experiment of Nomisma launching a 100% call on crypto 1, along

with the symmetric short put / discount bond on crypto 1.

The current market approach relies on (2+2) potential users with mutual coincidence of wants as well as (1+1) reciprocal collateral arrangements. E.g., a buyer of a call on crypto 1 against a seller of a call on crypto 1. Alongside this, one needs to ensurethat the call seller has enough escrowed collateral to satisfy the buyer's claim at expiration (i.e., 2+1 per contract, 6 in total 'arrangements').

Nomismareduces the required arrangements down to just two (a buyer of call on crypto and a corresponding buyer of a discount bond on same crypto). Obviously moving down from six to two makes for a vastly improved odds of generating sufficient liquidity with considerable momentum.

In addition, one generates many additional paths of potential liquidity creation. As a few examples, the buyer of the discount bond, can be matched with the buyer of the corresponding call, but also perhaps even more naturally with the potential buyer of an outright put. The buyer of the call can also be matched both with the buyer of the discount bond on platform, along with naturally a seller of a call with sufficient collateral.

As mentioned above while every current crypto holder is a natural counterparty for these transactions – providing a built-in base of liquidity – Nomisma also plans to underwrite and create transactions. This will – using the nomenclature above – drop counterparty complexity from order six → order one. In doing so, Nomisma is creating the simplest and most powerfully transparent intermediation transaction chain of any crypto derivative transaction, aiming towards becoming the gold-standard of intermediation in the crypto space. Specifically,

we will be targeting for Nomisma to act as a backstop buyer of calls and puts at a transparently derived level.

D. Native Token Policy and Design

The design of our native token takes into account various, competing at times, considerations. We will be erring on the side of generating more liquidity in our platform and less artificial and contrived 'scarcity.'

We will be aspiring towards initializing and solidifying:

a) Protocol
b) Two-sided marketplace / platform
c) Data

network effects:

i. We have been defining a standard via which information will be conveyed and data will be processed.
ii. We are setting up a marketplace, where 'risk averse' users are matched with 'risk tolerant' ones (and various configurations thereof). The network value emanates less so from the presence of more 'risk averse' or 'risk tolerant' users for themselves, but for the value of each group to each other. More 'risk averse' users increase competition among this cohort for desirable payoff characteristics, but the presence of more 'risk tolerant' users increases the value of the network to

the ‘risk averse’ ones (indirect network effects). The platform network effect gets generated by virtue of the fact that both the supply and demand side needs to work via the protocol to initialize transactions.

iii. User generated data will be central to how the platform generates value to their users. By definition, a consummated transaction embeds information about risk preferences and concomitant market determined variables which are acting as a focal point for the next set of transactions.

E. The Power of Pooling and Diversification

In this section we will introduce the concepts of correlation, the associated diversification, and the pooling of different cash flows that allows one to tailor exposures according to differences in risk tolerance.

Cryptocurrencies, as described in previous chapters, exhibit characteristics consistent with uncaptured diversification benefits, but also correlated crash risk. So how will a tranching exercise for a portfolio of cryptocurrencies work? What is the replicating hedge portfolio, and how can it become functional in the smart contract space?

We begin by describing the basic intuition that constitutes the fundamental building block of pricing baskets, and then demonstrate the role of correlation. Assuming a portfolio of two underlying coins, we can decompose the potential payouts on the basket that exhausts the universe of potential outcomes as:

1. Sum of coin prices at maturity *above* the sum of coin prices today.

2. Sum of coin prices at maturity *below* the sum of coin prices today.

In simple language, the following arguments form a starting point. If the coins are perfectly correlated, they will both end up together above or below the current spot price, thus the replicating portfolio will consist of owning both coins outright. In any other scenario, the replicating portfolio involves dynamically hedging an initial purchase of both coins in some proportion, according to the expected distribution of portfolio losses. The portfolio of coins, once more, provides the (over)hedge.

Importantly, the Nomisma foundation will be managing in a transparent fashion a variety of critical tasks:

a. Providing pricing capabilities to the community for the indicative acceptable distribution of portfolios of coins' returns.
b. Providing the infrastructure that would purchase the replicating portfolio collateral and ensure that it is paid off according to the initial contract to the structure participants.
c. Taking principal risk in certain tranches, if it deems that this would allow for further market completion and more liquidity. This action would always be clearly disclosed (as would be every aspect of this process), namely which tranche is owned by the foundation and at what level the risk is owned.
d. In the future the following token can be launched: The foundation "pre-programs" a dynamic hedging methodology and lets the smart contracts buy and sell the

underlying coins, and passes on the gains and / or the losses versus the actual payouts to structure participants at maturity to the holders of the Nomisma token. Note that the foundation controls the "hedging methodology" but on a transparent crowdsourced basis, every member of the community can get access to the code and contribute to it by holding Nomisma.

F. Ratings

The Nomisma foundation will serve as a transparent, crowdsourced, community-policed rating agency. The task of a rating agency is to assign, while being remunerated by issuers of securities, opinions on creditworthiness--probabilities of default and losses given default estimates. The value of rating agencies in general has been questioned in recent years, as have their incentives, their quasi-monopolistic nature, their lack of transparency, and their responsiveness to current events.

The foundation will develop its methodology to assign probability of breach and losses given breach for every non-residual tranche structured via the platform. This will act as a "translator" into a common creditworthiness language for the various underlyings and portfolios that will be priced on the platform. This will also act as a further enhancer of price discovery, liquidity, and risk diversification, without suffering the drawbacks of their process counterparts outside the crypto world.

Note that ratings based on expected losses under certain extreme and modal scenarios that get dynamically, transparently adjusted depending on actual pricing behavior by definition should be equivalent at time 0 to actual pricing, so one might argue that they are a trivial extension. Nevertheless, there will likely be benefits to enticing participants that do not want to

follow pricing arguments from first principles; and in time these ratings will act as a gravity mechanism for pricing, rather than the opposite, which again will make institutional participation in the market easier.

G. Nomisma as a Clearinghouse

The Nomisma foundation will act as an Ethereum clearinghouse. Members of the community can face each other directly, can enter into a smart contract that governs payoffs under certain states of the world, can monitor extant pricing information for various portfolios, and can utilize the escrow as well as the dynamic hedging methodology. A clearinghouse that has gained the confidence of it users for the above services can easily create network effects that can then be utilized to create a deep liquidity pool for an exchange. Note that writing the smart contract code that allows for applications such as "term borrowing / short selling / dynamic margining" would be a straightforward tool associated with our platform.

In contrast to the single underlying example, one might intuitively argue that there will exist more buyers of senior protection and more sellers of equity protection. Nevertheless we believe that the side that delivers the long-biased replicating portfolio will allow for the market to jump-start together with the Nomisma Foundation taking principal positions. On the one hand, the crypto community may want protection from a correlated crash event; nevertheless our experience related to the community spirit as well as the almost messianic belief about the

cryptocurrency (and blockchain) potential to change the world, retain and grow its valuation, may create natural sellers of senior protection (alongside with outside participants that want to leverage the exact same view; “there definitely is room for some minimum global diversification as well as utility value to the coin universe”). On the other hand, various enthusiasts, not least the rapidly expanding universe of crypto asset managers, will likely feel well placed to take up the task of separating the wheat from the chaff and leverage their view about which coins will be winning; and more importantly avoiding the risk of any of them collapsing.

Overall, there is a natural market ready to be tapped by providing the basic functionality and establishing a trusted platform, by virtue of the embedded trust-enhancing distributed ledger technology features. Also at a later stage, developing the escrow methodology to support periodic coupon payments for underlying derivative structures acting as securitization “raw material” would act as the natural bridge to the broader fixed income world.

H. Robustness and Discussion

Extending the discussion from the prior single underlying example, one can launch more robust Stablecoins by utilizing similar principles. This will extend the concept of the money-ness and safe asset nature of a tranche that implies a loss that delivers an equivalent discount rate to a dollar today. This tends asymptotically to a pure correlated cash risk measure of the whole cryptocurrency universe, and in extreme episodes one can expect diversified portfolios with some hopeful “winners” in them to retain “dollar equivalent properties” in extreme states. The Nomisma / USD stability gets established by dynamically changing tranche attachments between

the rest of senior and Nomisma / USD. There is no artificial scarcity, but rather an algorithm that defines expected loss scenarios that breach 1 dollar in value, where your holdings automatically get adjusted between Nomisma / USD (or ETH, or BTC, etc.) and the rest of senior tranche. There is absolutely no need for another mechanism that is designed for enriching early adopters as described earlier.

Our suggested "money" will deal with the information sensitivity and will not be subject to runs. It will be subject to broad cryptocurrency market systemic risk. There will not be any artificial mechanical scarcity to create "value" where none exists; and creating a perpetual "dividend split / reverse split" machine to create some link to an external anchor like a fiat currency is trivial, unless it is accompanied with an effort by the system designers to create another Ponzi scheme for the early adopters.[11]

Taking a step back, private sector money-like instruments are created by the private sector in many ways, and there many methods based on collateralization to deliver them. For instance, consider "privately issued" money by commercial banks in the days of "free banking" in the US in the 19th century; this was subject to runs, both systemically and on a bank-specific collateral concern basis. We can include here trade discount bills, letters of credit, and secured letters of credit; these are often illiquid, still subject to bank-specific risk as above, and are generally opaque/non-standard/non-transparent. There are further, commodity collateralized credit lines, for example in China recently, including examples like inventory-

[11] Further, it is important to note that we disagree with the usage of the term fiat currency in crypto circles as a homonym of "fake / not real." Fiat currency draws its value from the present value of future primary government surpluses; it is an asset with a future dividend stream and in an "interest on excess reserves" world becomes even more tightly linked, if not identical to nominal government debt.

backed financings that have served as “money” at various instances; precious metal and oil-backed financings are reasonably liquid and can act money-like; high quality commercial paper, which is subject to credit risk, albeit remote, but that bites exactly when safety is most needed; and finally the short-dated AAA ABS CDOs, which were the trigger (or the canary) of the global financial crisis in August 2007. In all of these cases, information invariance breaks down when doubts grow about the quality of the collateral; and the inability and unwillingness in these circumstances to engage in quality control often ends with the market breaking down. Our Nomisma Stablecoin can address all of the above issues (without promising a cure to world poverty or a miracle drug discovery!). Hence, we can solve for the key issues of privately produced money. It will be liquid, and transparent and formulaic by definition; collateral naturally will be risky, but totally visible to everyone; and there will exist a direct linkage with the stability and robustness of the broader cryptocurrency market, via a dynamically adjusting variance/covariance matrix.

I. Crypto Hedge Fund Platform

More and more hedge funds, which specialize in both capturing beta and in harvesting alpha, are launched in the crypto-space each day. Our platform provides an environment for both the traditional hedge fund structure and the one resembling more an early stage venture capital fund investing in ICOs and pre-ICOs to lower the information acquisition and monitoring barrier for potential partners.

A hedge fund manager will be transparently proposing an initially static portfolio of

underlyings (which in a later stage we will introduce functionality for rule-based substitution; even though it can be thought as a succession of static transactions, the beauty of DLT allows the platform to economise on the cost and avoid the cumbersome nature of non-recourse capital vehicles). The liability structure that will be "completing" the recommended holdings will act as a real-time monitoring device for the "coin picking" success, and in tandem with the "ratings" will act as an actual market-based scorecard of investment skill prowess. In summary, the extensions and obvious attractions of the platform are very expansive, which corroborates our excitement about the project.

VI. Conclusion

The wider investment world has only barely begun to invest into the blockchain space, in large part due to the enormous volatility in cryptocurrencies. In this paper, we articulate a foundational solution to this problem through the creation of a risk-sharing platform based on first principles from financial theory. At its core, our platform allows for risk sharing and cash profile/payoff tailoring according to risk tolerance and cash flow preferences. Those features are a necessary condition for investment by the full range of investor types. In doing so, we offer an environment that will lead to natural market completion in the crypto-asset space, as well as liquidity creation via natural replicating portfolios, and a way for the community to share in the "gains from trade." These gains will come not only from the core diversification benefits that the

platform offers, but also from the surplus sharing via the newly created tokens. As added benefits, the platform will introduce: a) a robust, fungible, and transparent Nomisma Stablecoin, exhibiting all the characteristics of optimal privately produced money; b) a smart contract based clearinghouse; c) a crowdsourced/market-based creditworthiness assignment engine, and d) a mechanism to match managers with alpha-generating capacity to those looking to hedge or enter the crypto space at varying levels of risk tolerance. Overall, the goal of creating a comprehensive intermediation platform that will help incentivize investment into the cryptocurrency space and spawn the next generation of innovation on the blockchain is not only immensely desirable, but also easily within reach.

References

Abkowitz, Alyssa. "The Cashless Society Has Arrived — Only It's in China." The Wall Street Journal, Jan. 4, 2018.

Bell, Stephanie. "The role of the state and the hierarchy of money." Cambridge Journal of Economics 25.2 (2001): 149-163.

Borovkova S., Bunk H, Goeij W.,Mechev D and Veldhuizen D., "Collateralized Commodity Obligations: *Modeling and Risk Assessment",* JAI, Fall 2013,16(2)9-29

Caballero, Ricardo J., Emmanuel Farhi, and Pierre-Olivier Gourinchas. "The safe assets shortage conundrum." Journal of Economic Perspectives 31.3 (2017): 29-46.

Eichengreen, Barry. "Global monetary order." Conference proceedings The future of the international monetary and financial architecture. 2016.

Fisher, Irving. The Purchasing Power of Money: Its' Determination And Relation to Credit Interest And Crises. Cosimo, Inc., 2006.

Gorton, Gary. "The history and economics of safe assets." Annual Review of Economics 9.1 (2017).

Gorton, Gary, Stefan Lewellen, and Andrew Metrick. 2010. "The Safe Asset Share." American Economic Review, Papers and Proceedings 102:101–106.

Gorton, Gary B., and Guillermo Ordonez. The supply and demand for safe assets. No. w18732. National Bureau of Economic Research, 2013.

Gkomozias K., "CDO Spotlight: Overview of Modeling Methodology for Commodity CDO structures", S&P Structured Finance Criteria (2006).

Gkomozias K., Tamburrano E., Guadanuolo L., "Chapter 3: Ratings Methodology for FX CDOs and CCOs", Expansion and Diversification in Securitization Yearbook 2007, (2007), ISBN 978-90-411-2661-0.

Holmström, Bengt. "Understanding the role of debt in the financial system." (2015).

Holmström, Bengt, and Jean Tirole. "Private and public supply of liquidity." Journal of political Economy 106.1 (1998): 1-40.

Holmström, Bengt, and Jean Tirole. "LAPM: A liquidity-based asset pricing model." the Journal of Finance 56.5 (2001): 1837-1867.

Lerner, Abba P. "Money as a Creature of the State." The American Economic Review 37.2 (1947): 312-317.

Mankiw, Gregory N. Macroeconomics. New York: Worth Publisher, 2007.

Mishkin, Frederic S. The economics of money, banking, and financial markets. Pearson education, 2007.

Morellec, Erwan. "Asset liquidity, capital structure, and secured debt." Journal of financial economics 61.2 (2001): 173-206.

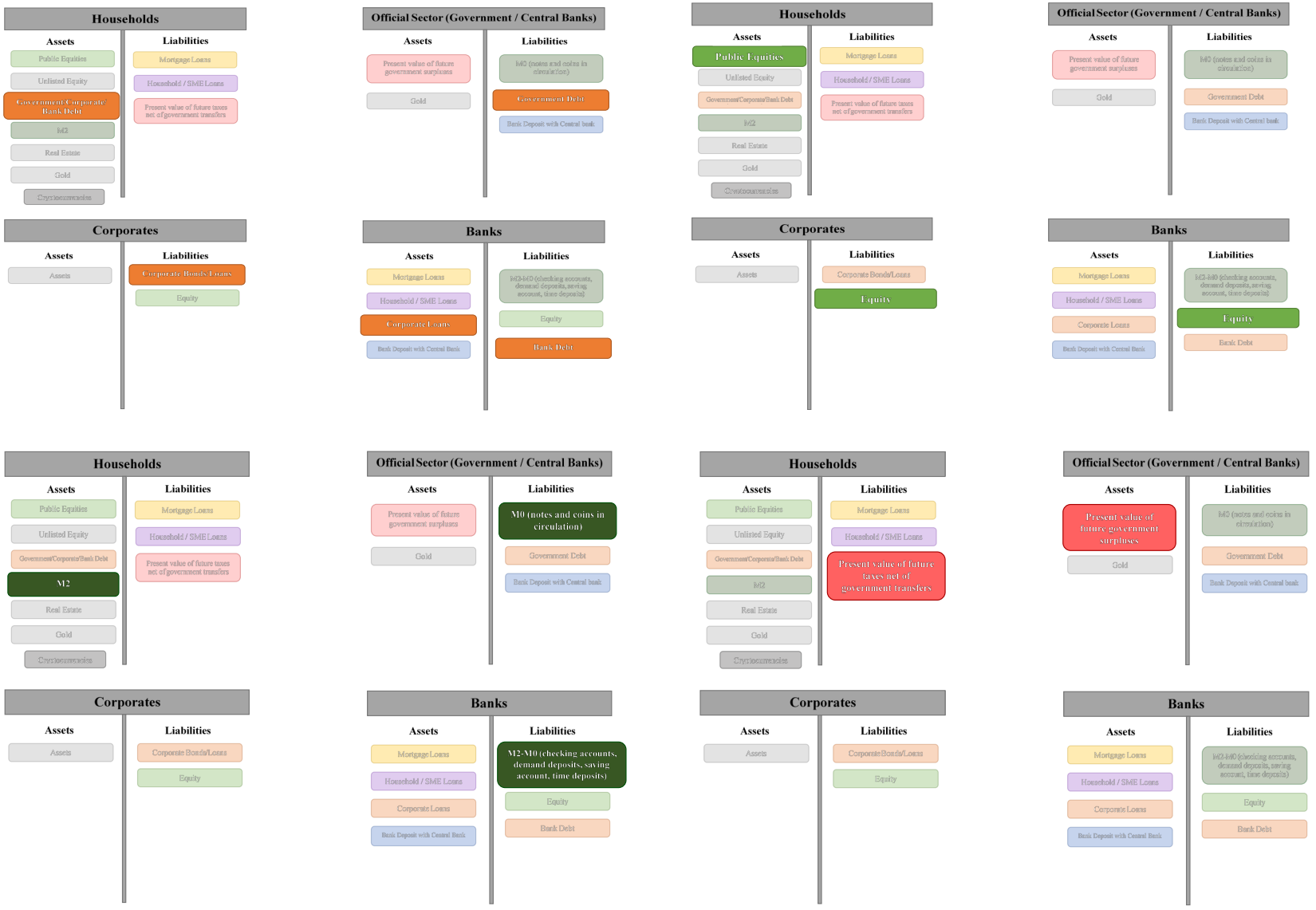
O'Brien R., "Naughty, Naughty Boys and the Collateralized Commodity Bailout", Huffington Post article, https://www.huffingtonpost.com/robyn-o/naughty-naughty-boys-and_b_176945.html

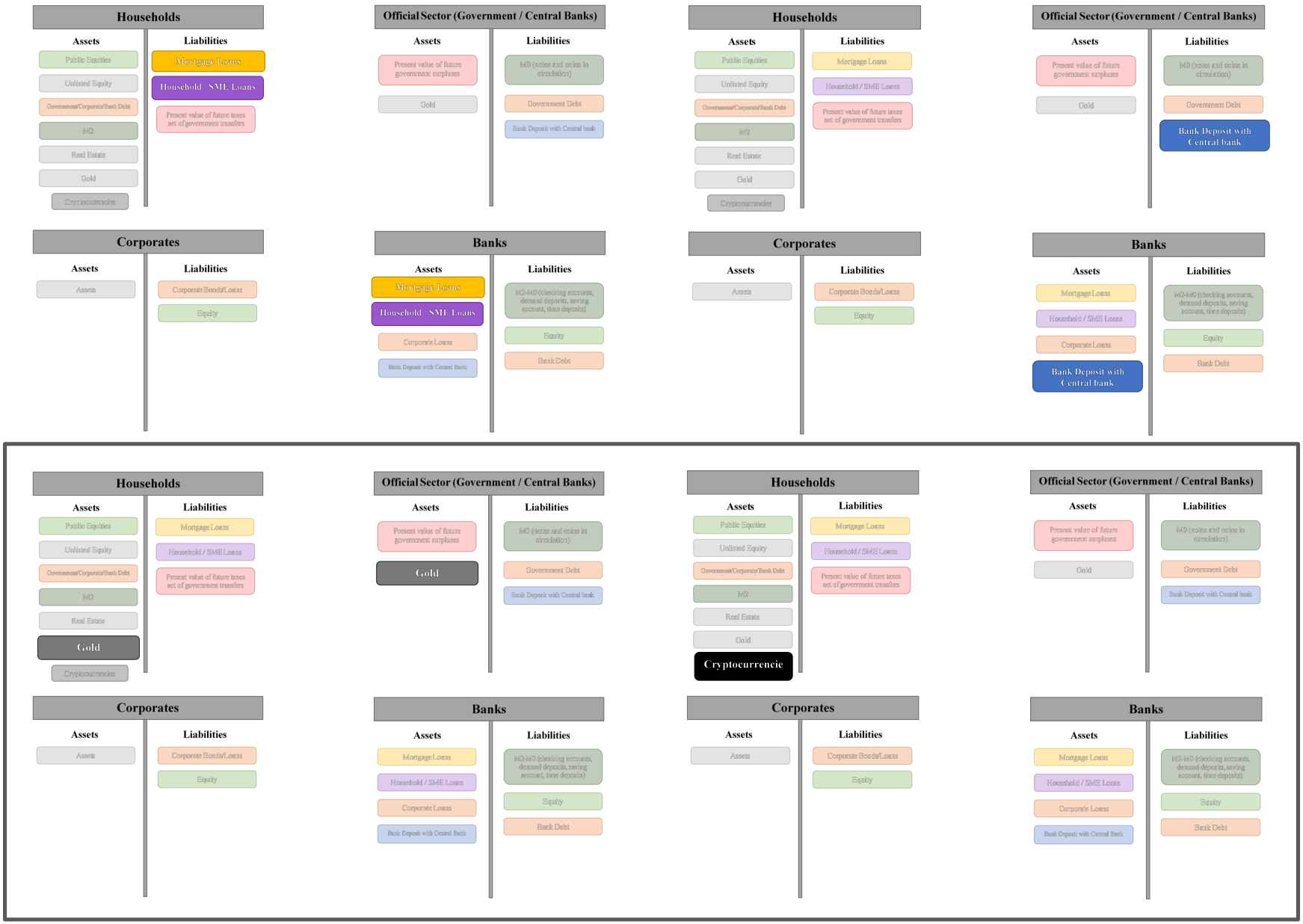
Appendix

This appendix contains the following items:

1. Figure on Economic Actors' Balance Sheet
2. Background on Money as a Safe Asset
3. Background on History of Money
4. Background on CDO-Squared Securities
5. Background and Pricing of CCO's (Collateralized Commodity Obligations)
6. Technical Overview of Nomisma Platform
7. Token Sources of Value

Figure A1. Economic Actors' Balance Sheet




Households
Assets
Liabilities
Public Equities
Unlisted Equity
Government/Corporate/Bank Debt
M2
Real Estate
Gold
Cryptocurrencies
Mortgage Loans
Household / SME Loans
Present value of future taxes net of government transfers
Official Sector (Government / Central Banks)
Assets
Liabilities
Present value of future government surpluses
Gold
M0 (notes and coins in circulation)
Government Debt
Bank Deposit with Central bank
Households
Assets
Liabilities
Public Equities
Unlisted Equity
Government/Corporate/Bank Debt
M2
Real Estate
Gold
Cryptocurrencies
Mortgage Loans
Household / SME Loans
Present value of future taxes net of government transfers
Official Sector (Government / Central Banks)
Assets
Liabilities
Present value of future government surpluses
Gold
M0 (notes and coins in circulation)
Government Debt
Bank Deposit with Central bank
Corporates
Assets
Liabilities
Assets
Corporate Bonds/Loans
Equity
Banks
Assets
Liabilities
Mortgage Loans
Household / SME Loans
Corporate Loans
Bank Deposit with Central Bank
M2-M0 (checking accounts, demand deposits, saving account, time deposits)
Equity
Bank Debt
Corporates
Assets
Liabilities
Assets
Corporate Bonds/Loans
Equity
Banks
Assets
Liabilities
Mortgage Loans
Household / SME Loans
Corporate Loans
Bank Deposit with Central bank
M2+M0 (checking accounts, demand deposits, saving account, time deposits)
Equity
Bank Debt
Households
Assets
Liabilities
Public Equities
Unlisted Equity
Government/Corporate/Bank Debt
M2
Real Estate
Gold
Cryptocurrencies
Mortgage Loans
Household / SME Loans
Present value of future taxes net of government transfers
Official Sector (Government / Central Banks)
Assets
Liabilities
Present value of future government surpluses
Gold
M0 (notes and coins in circulation)
Government Debt
Bank Deposit with Central bank
Households
Assets
Liabilities
Public Equities
Unlisted Equity
Government/Corporate/Bank Debt
M2
Real Estate
Gold
Cryptocurrencie
Mortgage Loans
Household / SME Loans
Present value of future taxes net of government transfers
Official Sector (Government / Central Banks)
Assets
Liabilities
Present value of future government surpluses
Gold
M0 (notes and coins in circulation)
Government Debt
Bank Deposit with Central bank
Corporates
Assets
Liabilities
Assets
Corporate Bonds/Loans
Equity
Banks
Assets
Liabilities
Mortgage Loans
Household / SME Loans
Corporate Loans
Bank Deposit with Central Bank
M2-M0 (checking accounts, demand deposits, saving account, time deposits)
Equity
Bank Debt
Corporates
Assets
Liabilities
Assets
Corporate Bonds/Loans
Equity
Banks
Assets
Liabilities
Mortgage Loans
Household / SME Loans
Corporate Loans
Bank Deposit with Central Bank
M2-M0 (checking accounts, demand deposits, saving account, time deposits)
Equity
Bank Debt

The above is a simplified representation of global balance sheets, abstracting from government debt and equity held on the official sector's asset side (for example, in Japan), public securities on the asset of side of banks, merging unlisted / small business sector with households, allowing us to witness the "absence of a double entry" for the cryptocurrency / store of value commodity universe.

2. Money as a Safe Asset

Money naturally functions as a safe asset. It can be transacted by merely acknowledging its face value, thus it is both informationally insensitive and simple. In most cases, people expect its value to be preserved. In this section, we will give an introduction to its definition, functions, history, and position the quantity theory of money in its rightful historical context.

Economists define money (also referred to as the money supply) as anything that is generally accepted in payment for goods or services or in the repayment of debts (Mishkin, 2007).[12] Money is different from an individual's wealth. Wealth includes not only money but also other assets that serve to store value, such as bonds, common stock, land, houses, art, or jewelry. Money is also different from income. Money is a certain amount at a given point in time, whereas income, by contrast, is a flow of earnings per unit of time.

From the definition of money, economists (e.g., Mankiw, 2007; Mishkin, 2007) point out its three functions in essence: medium of exchange, unit of account, and store of value. The use of money as a medium of exchange promotes economic efficiency by minimizing the time spent in exchanging goods and services. Using money as a unit of account reduces transaction costs in an economy by reducing the number of prices that need to be considered. The benefits of this function of money grow as the economy becomes more complex. A store of value is used to save purchasing power from the time income is received until the time it is spent.

[12] According to this definition, money can not only come in the form of currency, but should also include other items that are used to make purchases, such as demand deposits, if they can be quickly and easily converted into currency.

3. A History of Money

Money emerged as a measurement of value during economic activities of exchange on goods or services. Money historically possessed a characteristic of both commodity and functionality. Most societies once used commodities with intrinsic values as money. This is called commodity money. For a commodity to function effectively as money, it has to meet several criteria (Mishkin, 2007): (1) It must be easily standardized, making it simple to ascertain its value; (2) it must be widely accepted; (3) it must be divisible, so that it is easy to "make change"; (4) it must be easy to carry; and (5) it must not deteriorate quickly.

Commodity money does not always satisfy the criterion that it is easy to carry, especially for large purchases. The invention of paper money followed. The earliest paper money can be traced back to China during the Song Dynasty (11th century), when the technology of printing had reached a sufficiently advanced stage that counterfeiting was extremely difficult. Another issue is that there needs to be some trust in the authorities that issue it before it can be accepted as a medium of exchange.

Currency then evolved into fiat money: paper currency without intrinsic value but decreed by a government as legal tender. Its value is assigned and enforced by the government, so that legally it must be accepted as payment for debts. As timelessly expressed by Adam Smith (1776), "a prince, who should enact that a certain proportion of his taxes be paid in a paper money of a certain kind, might thereby give a certain value to this paper money."

Both commodity money and paper money suffer from problems related to theft and inconvenience in transportation in large amounts. To solve these problems, checks came into being with the development of modern banking. A check is an instruction for a bank to transfer money

from account to account (Mishkin, 2007). Transfers with checks made back and forth cancel each other with no need to move currency, making transactions for large amounts much easier, thereby reducing loss from theft.

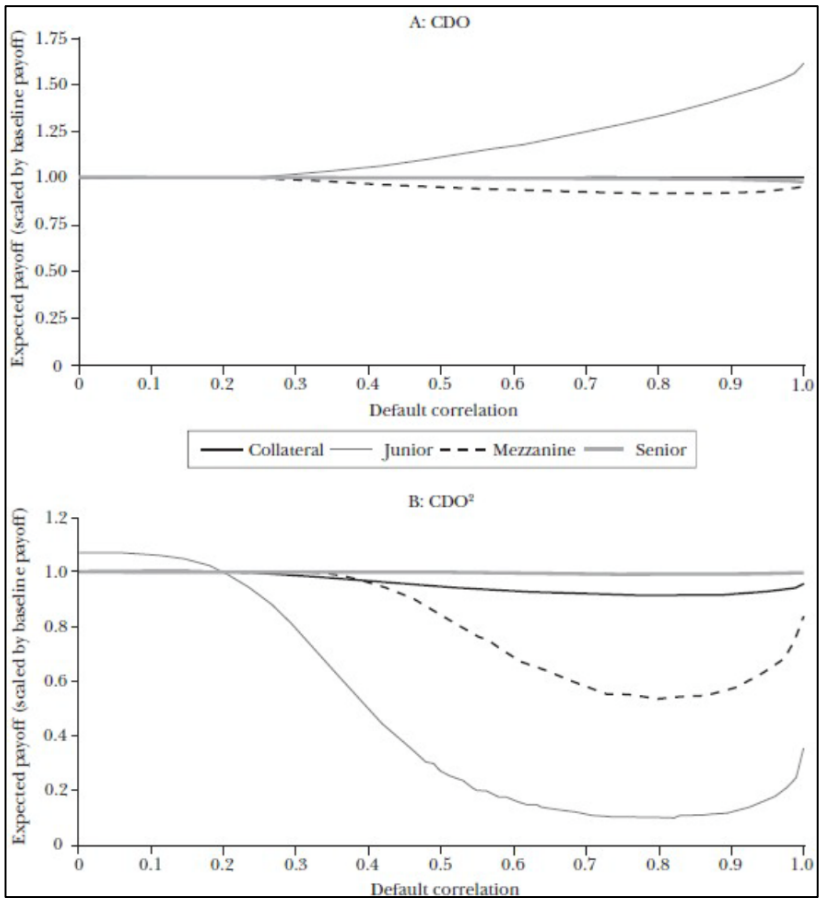
The development of the Internet made it cheap to make payments electronically. Electronic payments technology can not only substitute for checks, but also for cash, in the form of electronic money (or e-money). A cashless society in which all payments are made electronically has yet to come, except arguably in China (Abkowitz, 2018). Mishkin (2007) pointed out three factors against the disappearance of the paper system: high costs to set up the infrastructure, security concerns, and privacy concerns. The recently developed cryptocurrency and blockchain technologies can be a potential solution, which we discuss in this paper.

4. CDO Squared Securities (CDO^2)

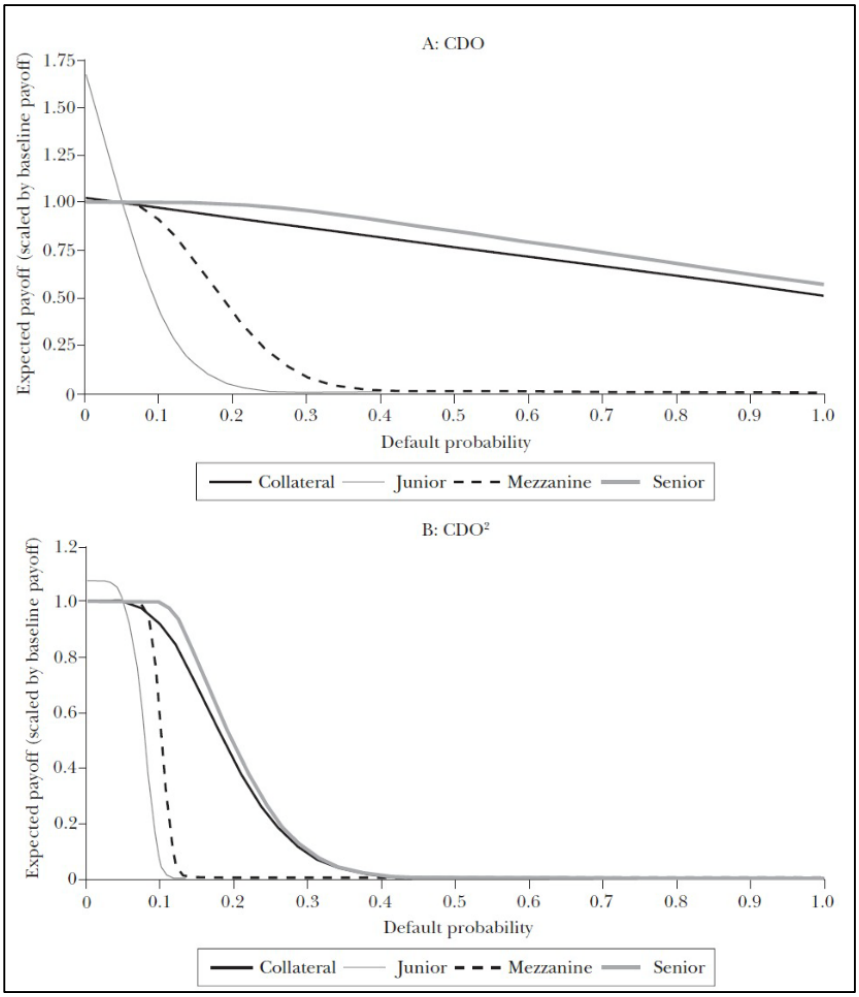
For derivatives manufactured through multiple rounds of structuring, even marginal errors in estimates of the properties of securities at the underlying level can dramatically alter structured finance ratings. In the single-name rating business, rating agencies can afford to remain agnostic about the extent to which defaults may be correlated. The riskiness of CDO tranches is, however, very sensitive to correlation, as it relies on the power of diversification to achieve credit enhancement.

Coval et al. (2009) simulate the payoffs to 40 CDO pools (shown below graphically), each comprised of 100 bonds with a five-year default probability of 5 percent and a recovery rate of 50 percent of face value conditional on default. Within each collateral pool, they construct a capital structure comprised of three tranches prioritized in order of their seniority. The *junior tranche* is the first to absorb losses from the underlying collateral pool and does so until the portfolio loss exceeds 6 percent, at which point the junior tranche becomes worthless. The *mezzanine tranche* begins to absorb losses once the portfolio loss exceeds 6 percent and continues to do so until the portfolio loss reaches 12 percent. Finally, the *senior tranche* absorbs portfolio losses in excess of 12 percent. They construct a CDO^2, to be called *CDO^2 [6–12]*, by issuing a second capital structure of claims against a pool that combines the mezzanine tranches from the 40 original collateralized debt obligations. Pairwise default correlation is set to 0.2 within each collateral pool and defaults of bonds within different collateral pools are assumed to be uncorrelated.

In the case of the CDO, one observes that, as default correlation increases from the baseline figure, risk shifts from junior to senior claims. The mezzanine tranche loses value initially and regains it as the correlation continues to increase. As value shifts in the CDO mezzanine, the expected payoff of the CDO^2 mezzanine declines dramatically.



The authors also examine the effect of errors in estimates of the probability of default of the underlying securities on the expected tranche payoffs. They hold default correlation fixed at 0.2, and find that as the probability of defaults increases, the expected payoff on the underlying collateral decreases monotonically. This effect is transferred to the tranches of the CDO with sensitivity determined by seniority. Changing the baseline parameters has a starker impact on the CDO^2.



A large fraction of CDOs issued in the run-up to the 2008 financial crisis had subprime residential mortgage-backed securities (RMBS) as their underlying assets. RMBSs were themselves tranches from an earlier securitization of a large pool of mortgages. Since substantial lending to subprime borrowers is a recent phenomenon, historical data on defaults and delinquencies was scarce. The possibility of errors in the assessment of default correlations, default probabilities, and the ensuing recovery rates was significant; the magnification of these errors by the re-securitization process helps explain the devastating losses holders of the structured products suffered, in particular in the case of CDO^2.

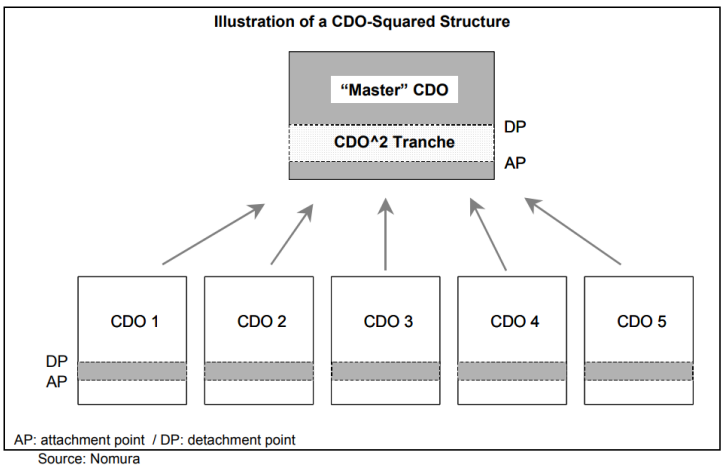
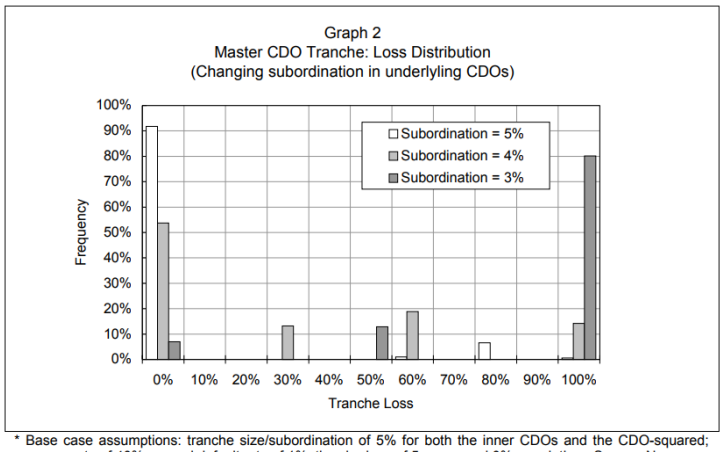


Illustration of a CDO-Squared Structure
"Master" CDO
CDO^2 Tranche
DP
AP
CDO 1
CDO 2
CDO 3
CDO 4
CDO 5
DP
AP
AP: attachment point / DP: detachment point
Source: Nomura


Graph 2
Master CDO Tranche: Loss Distribution
(Changing subordination in underlyling CDOs)
Subordination = 5%
Subordination = 4%
Subordination = 3%
Frequency
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
Tranche Loss
* Base case assumptions: tranche size/subordination of 5% for both the inner CDOs and the CDO-squared; recovery rate of 40%; annual default rate of 1%; time horizon of 5 years; and 0% correlation. Source: Nomura

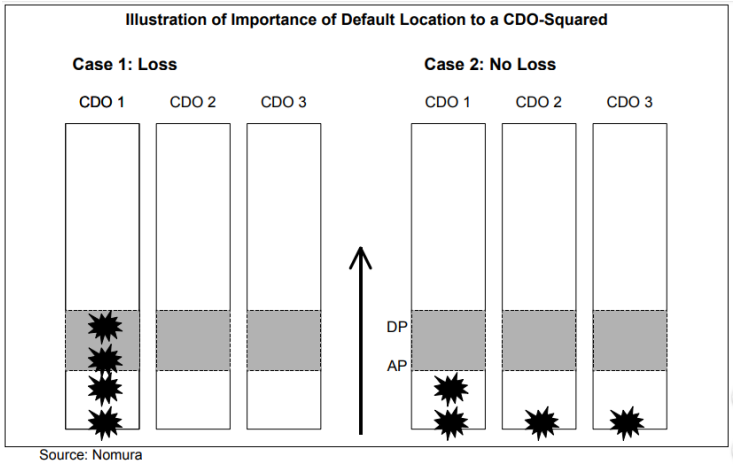


Illustration of Importance of Default Location to a CDO-Squared
Case 1: Loss
Case 2: No Loss
CDO 1
CDO 2
CDO 3
CDO 1
CDO 2
CDO 3
DP
AP
Source: Nomura

5. Collateralised Commodity Obligations (CCO)

Collateralised Commodity Obligations ("CCO") structures provide fixed-income investors with exposure to the commodities market, giving them the opportunity to receive a risk premium by investing in a rated portfolio of commodity products. Commodity risk can be repackaged in a tranched format that matches the investor's risk profile. The investor is exposed to the risk of portfolio losses exceeding the subordination level of the tranche in which he has invested.

Like CDOs, the CCO structure takes advantage of diversification between the sectors in the underlying reference portfolio. In the case of CCOs, the structure would produce better yields than individual commodity sectors. Other advantages that commodities bring to CDO managers is that they have very low correlation to other asset classes, providing better portfolio diversification, and they offer enhanced yield compared with current credit spreads.

Gomozias (2006) developed a model for analysing CCOs, called the mean-reverting jump diffusion (MRJD) model, of which we give an overview in this article. The model combines historical and market analysis on certain commodity sectors with an eye towards the following: aA simple and intuitive model across all commodity sectors

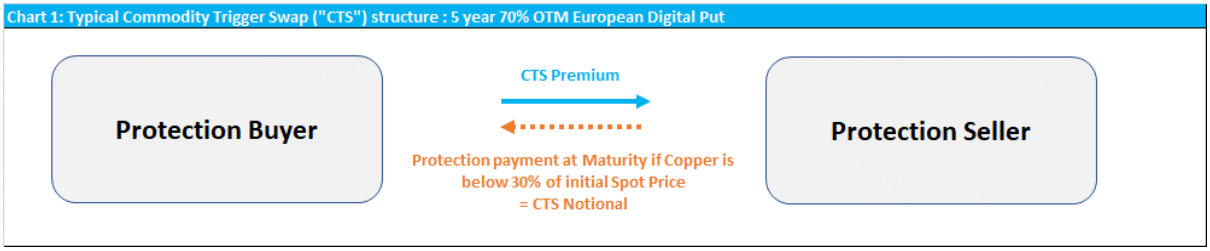
- Model calibration transparency
- Compatibility with other asset classes

This model provides market participants with the flexibility to change its parameters, taking into account differing views of the long-term mean, long-term speed, and volatility of the commodities.

A. The CCO Structure

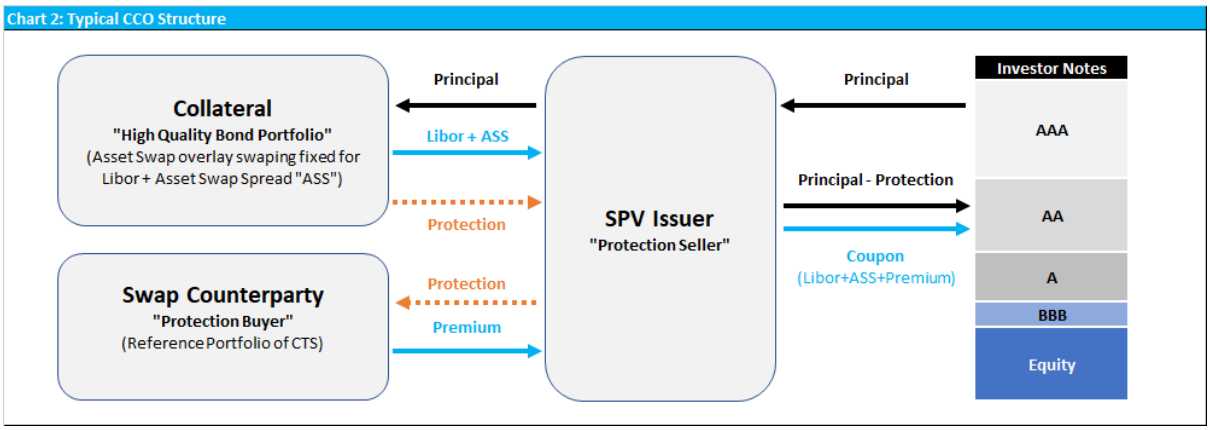
As with traditional synthetic CDOs, CCOs involve an issuance of debt that references a portfolio of assets via a swap. Instead of bonds, loans, and other fixed income debt instruments, the portfolio in a CCO contains derivatives on commodity prices.

The commodity derivatives being referenced in a CCO are essentially deep out-of-the-money (OTM) European-style binary options on the price of the commodity sector. The strike of each option is set at a predefined "trigger level." Typically, there may be more than one trigger for each commodity referenced. This product is called a commodity trigger swap or CTS. A default event occurs if the price is less than the trigger level at the option's maturity, in which case the option would be exercised, leading to a capital loss on the structure. A typical CTS structure is shown in Chart 1 below:



In a typical CCO structure, such as the one shown in the Chart 2 below, the principal of the notes is passed on to the SPV Issuer that immediately invests the principal in suitable and high quality bond collateral, ensuring the repayment of principal. An asset swap overlay on the bond portfolio is used to swap fixed coupons to floating Libor + asset swap spread (“ASS”) for the duration of the transaction. At the same time, the SPV enters a swap with the swap counterparty. Under this swap agreement, the issuer sells “Protection” to the swap counterparty for portfolio losses that exceed a predetermined subordination loss level. The SPV receives a “Premium” based on the option

premiums of the commodity portfolio. This premium along with the Libor + ASS cash flows is passed on to the investors periodically as the coupon on the notes and this is distributed to different tranches in line with the default rate of the tranche. If trigger events occur leading to a portfolio loss that exceeds the predetermined loss level, the SPV sells collateral to make the protection payments to the swap counterparty and this loss is effectively passed on to the investors hierarchically where the Equity tranche absorbs the first losses and then subsequently the BBB and so forth until the AAA tranche.



B. Modelling and Rating Methodology for Single CTS and CCO Structures

Univariate Model Specification for Single CTS

We now provide an overview of the modeling methodology in Gomozias (2006) for single CTS within a univariate framework.

Commodity Spot Prices

Commodity spot prices are modelled using an arithmetic Mean-Reverting Jump Diffusion (MRJD) process on log prices. The jumps take effect for maturities T≤3 Years. The model has the

following general form:

$$\frac{dS}{S} = \beta\left(\xi - \ln S\right)dt + \sigma dW + dJ^{up} + dJ^{down} \quad (1)$$

which implies that the spot price, S, mean reverts to the long-term level of e^{ξ} at a speed β. Introducing the new variable x = lnS, we have:

$$dx = \beta\left(\theta - x\right)dt + \sigma dW + dJ^{up} + dJ^{down} \quad (2)$$

where

$$\theta = \xi - \frac{\sigma^2}{2\beta} \quad (3)$$

is the long-term level of the log price so that the spot price long term level is given by

$$\overline{S} = e^{\left(\theta + \frac{\sigma^2}{2\beta}\right)} \quad (4)$$

and J denotes a Poisson process (a discrete time process) with intensity λ which determines the frequency of the positive "up" and negative "down" jumps of fixed size.

Commodity Sub-Index Prices

The Commodity Excess Return Sub-Indices are designed to reflect the total return performance of an investment in a commodities portfolio. This return is determined by the spot return and the "rolling" return. The spot return is based on the spot price levels of the commodity and the "rolling" return is based on the discount/premium generated by "rolling" the future

positions forward as we approach delivery. This "rolling" return will be positive (negative) if the forward curve is in Backwardation (Contango). Effectively, S&P proposes a diffusion process that is driven by the Spot dynamics and then it is adjusted for the rolling return. The model has the following form:

$$dx = \beta(\theta - x)dt + Rdt + \sigma dW + dJ^{up} + dJ^{down} \quad (5)$$

where x is the spot log-price and R is the annualised "rolling" return. This can be written as:

$$dx = \beta(\Theta - x)dt + \sigma dW + dJ^{up} + dJ^{down} \quad (6)$$

where $\Theta = \left(\theta + \frac{R}{\beta}\right)$ is the "roll-adjusted" Spot Long-Term mean.

Default Probability Estimation

Simulation

For our analysis we have chosen to simulate the following discrete model for spot prices:

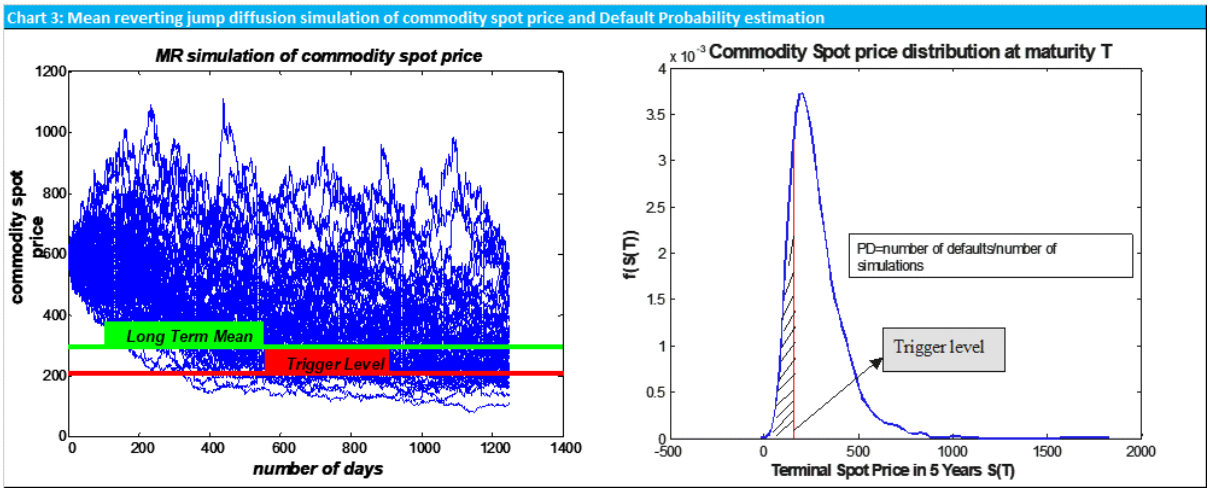
$$x_{t+1} = x_t + \beta(\theta - x_t)\Delta t + \sigma\sqrt{\Delta t}\varepsilon + \Delta J_t^{up} + \Delta J_t^{down} \quad (6)$$

and the following discrete model for Sub-Indices:

$$x_{t+1} = x_t + \beta(\Theta - x_t)\Delta t + \sigma\sqrt{\Delta t}\varepsilon + \Delta J_t^{up} + \Delta J_t^{down} \quad (7)$$

where ε are samples from the standard normal distribution and ΔJ are Poisson samples taking values of either 0 or 1·jump size determined by the Poisson intensity(jumps frequency). Then, the PD is calculated as:

$$PD = \frac{\text{number of paths falling below strike level}}{\text{total number of simulations}} \qquad (8)$$



Analytical Solutions

In the case of no jumps, the Jump-MR diffusion equation in (1) reduces to:

$$dx = \beta(\theta - x)dt + \sigma dW \qquad (9)$$

in which case the stochastic log-price x is normally distributed around $E[x_t]$ given by:

$$E[x_t] = x_0 e^{-\beta\Delta t} + \theta\left(1 - e^{-\beta\Delta t}\right) \qquad (10)$$

with variance

$$V[x_t] = \frac{\sigma^2}{2\beta}\left(1 - e^{(-2\beta\Delta t)}\right) \qquad (11)$$

The PD at any specified price level $K \bullet S_{t=0}$ (where K is the strike level) is found by the cumulative lognormal probability distribution of S where $x = \ln(S) \sim N\left(E[x], V(x)\right)$.

Rating Methodology for Single CTS

A rating can be assigned to each individual PD for a CTS according to the Default Tables of a Rating Agency (S&P) for the specified maturity of the contract.

Multivariate Model Specification for CCO structures

Portfolio Simulation

The univariate simulation can be extended to a multivariate simulation for a portfolio of commodities under certain assumptions about the commodity covariance structure.

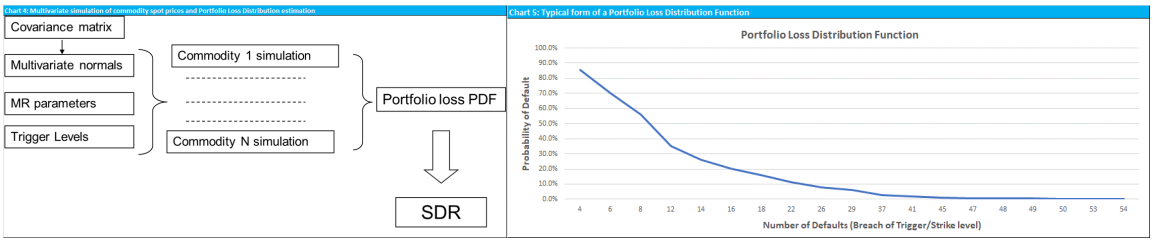
Within the Gaussian context, generating correlated random numbers for the stochastic term of the Monte Carlo simulation can be achieved within the following steps:

a. Generate an n x k matrix of standard normal Z
b. Calculate X = L Z to get correlated standard normal, where L is the left Cholesky factor of the correlation matrix
c. Multiply the columns by σ and μ to produce non-standard normal

Mean reversion parameters for the drift term and Jump parameters for the Poisson term can be added accordingly to produce a single portfolio simulation for many commodities.

Portfolio Loss Distribution and Scenario Default Rate "SDR"

To estimate the Portfolio Loss Distribution, a large number of simulations are produced for the portfolio. Using the Trigger Levels for each commodity, at each simulation we measure the portfolio losses and we estimate the distribution of losses over many simulations. The Portfolio Loss Distribution provides information about the probability of having x losses ("Scenario Default Rate") in the portfolio. A typical portfolio simulation and Portfolio Loss Distribution is provided in chart 4 and 5 below.

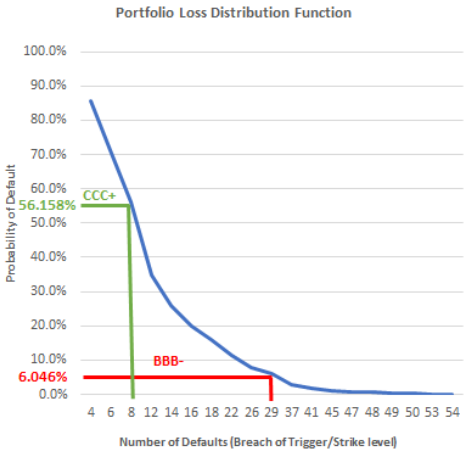


Rating Methodology for CCO tranches & Subordination Level

A rating can be assigned by mapping the corresponding Rating Quantiles for CDO for the appropriate maturity provided by a Rating Agency (e.g., S&P) to the probability axis of the Loss Distribution which also provides the rated tranche subordination level (after which capital for the tranche is impaired due to default losses) or Attachment Point and Detachment Point. An example is provided below where the attachment point of the BBB- tranche can be identified at 27 (1st loss following 26th loss of the Equity Tranche) and Detachment Point at 41. An example is provided below for the full capital structure.

Chart 6: Portfolio Loss Distribution, CCO Tranche Rating & Subordination level

Desired Rating	Rating Quantile	Scenario Default Rate	Monetary Default
AAA	0.118%	56.84%	54
AA+	0.182%	55.79%	53
AA	0.356%	52.63%	50
AA-	0.452%	51.58%	49
A+	0.578%	50.53%	48
A	0.709%	49.47%	47
A-	1.020%	47.37%	45
BBB+	1.704%	43.16%	41
BBB	2.812%	38.95%	37
BBB-	6.046%	30.53%	29
BB+	7.763%	27.37%	26
BB	11.403%	23.16%	22
BB-	15.886%	18.95%	18
B+	20.087%	16.84%	16
B	26.089%	14.74%	14
B-	34.945%	12.63%	12
CCC+	56.158%	8.42%	8
CCC	70.313%	6.32%	6
CCC-	85.650%	4.21%	4



C. Pricing methodology for CCO tranches

The pricing of the CCO tranches refers to the fair estimation of the spread over Libor provided as coupon backed by the "Premium" and "ASS" generated. A typical pricing is shown below in Chart 7, where the spread increases with lower seniority in the capital structure as the default risk of the tranches increases.

Chart 7: CCO Tranches payout

Tranche	Attachment Point	Detachment Point	Size	Size($)	Coupon
AAA	53	95	44.21%	$ 44,210,526	Libor + [60-80bp]
AA	48	53	5.26%	$ 5,263,158	Libor + [140-160bp]
A	41	48	7.37%	$ 7,368,421	Libor + [220-250bp]
BBB	26	41	15.79%	$ 15,789,474	Libor + [350-400bp]
Equity	0	26	27.37%	$ 27,368,421	Libor + [13-15%]
			100.00%	$ 100,000,000	

The pricing methodology follows typical present value arguments, where the "PV of spread payments for each tranche" needs to equal the "PV of the expected loss for the same tranche" so that each tranche is paid a risk free floating rate plus a spread depending on the default risk of the associated tranche.

The expected loss "EL" is defined as EL = PD * (1-RR) * EAD where "PD" is the probability of

tranche default (area under the Loss distribution curve between probability of the attachment and detachment points), “RR” is the recovery rate (0 for binary options but maybe Spot-Strike for vanilla options etc.), and “EAD” is exposure at default is the number of trigger events times the notional referenced by each CTS.

6. Overview of Nomisma Platform: Functionality and Technical Specifications

A. Functionality

Nomisma Platform Process

A user ready to enter a Nomisma facing claim, customizes the claim on the website and clicks to submit it. The web host sends a request to the Geth client, which deploys a multi-signature transaction containing the claim details and an escrow account. The user is prompted to deposit funds into the escrow along with NBT, the native token to Nomisma, and has an opportunity to view the details of the contract on-chain before it is deployed given her signature. Nomisma co-signs the multi-signature transaction and the claim exists autonomously on the blockchain. A final contract receives the funds from the claim contracts, buys the underlying, and settles the claims at maturity. This process is illustrated in the Platform Mechanics Figure below.

Off-chain

The Nomisma website allows users to customize, buy, and sell various claims with cryptocurrencies as underlying reference assets. Transactions take place when two claims are matched with the same underlying asset, maturity, and strike price of the claims. A user holding NBT may submit a claim with a bid, which will remain pending until matched or canceled. A transaction board displays outstanding claims for users to take. When a user takes an outstanding claim, the transaction is executed on the blockchain.

Off-Chain to On-Chain

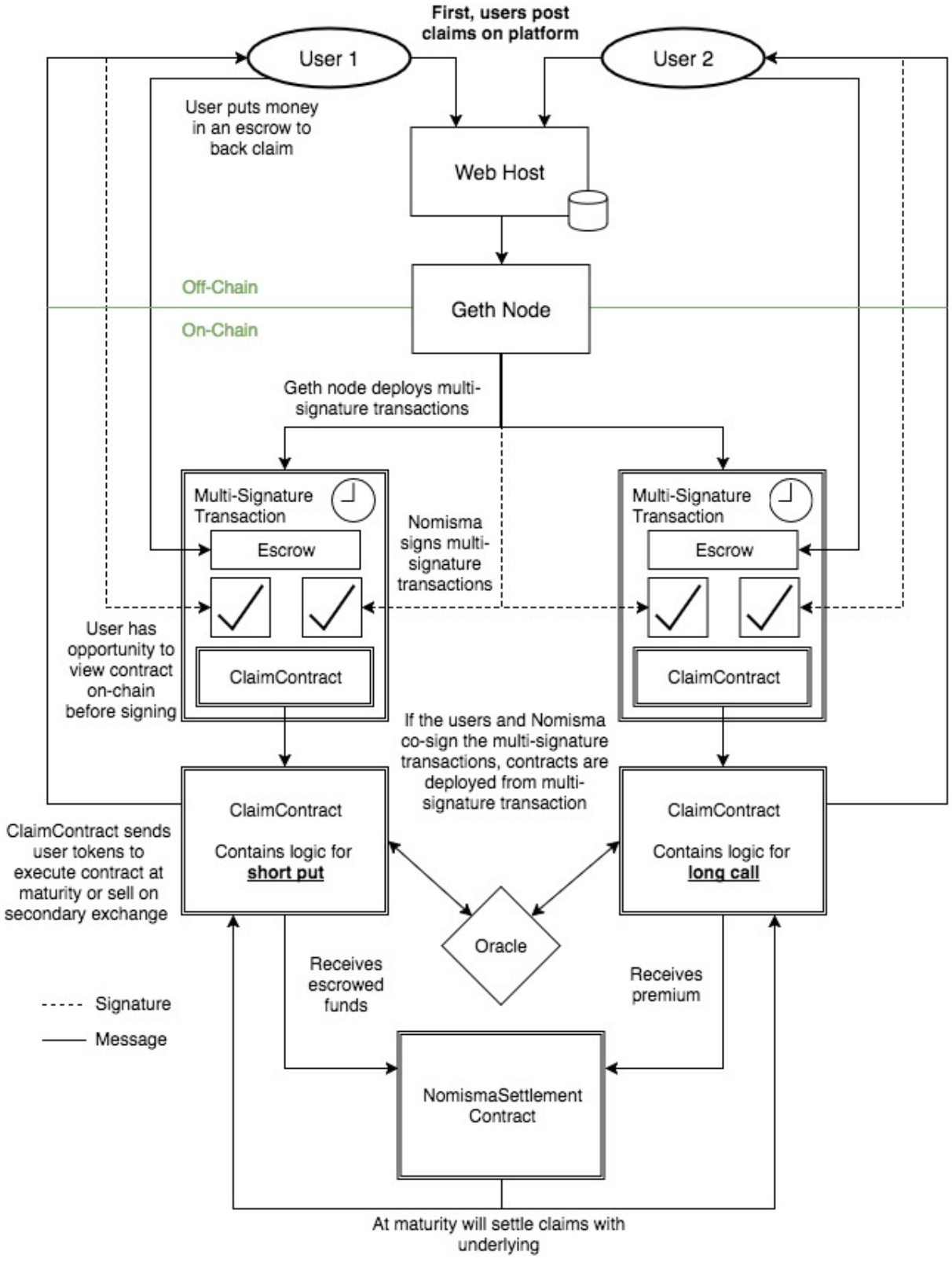
Upon submitting a claim, the user is prompted to deposit collateral for the claim plus transaction structuring costs in an on-chain escrow and sign a multi-signature transaction containing a timelock and the details of the claim. When two matching claims are found, Nomisma will co-sign the multi-signature transactions with the claims of both users, subsequently deploying the claims as autonomous smart contracts. These smart contracts are referred to as "ClaimContracts".

On-Chain

ClaimContracts issue tokens to users long a claim. The Geth server messages the deployed ClaimContracts to send the funds escrowed for the claims to NomismaSettlementContract, an autonomous contract that buys the underlying asset of the ClaimContracts. Any excess funds after buying the underlying go into a separate escrow, to eventually be dispersed to NBT holders. Upon maturity of the ClaimContracts, NomismaSettlementContract settles the claims by sending the purchased underlying to the triggered ClaimContract. [13]

[13] For our prototype, we use Oraclize to request price data so that ClaimContracts may know whether the conditions have been satisfied. We acknowledge the potential security vulnerability associated with price oracle utilisation. Price oracle security constitutes a priority of our development work.

Platform Mechanics Figure



Prototype Design Appendix

Security and Secret Keys

The Nomisma Foundation will never store the secret keys of its users, however it must maintain an address, deploy contracts on Ethereum, and sign transactions which require the use of secret keys. The prototype maintains PCI DSS security standards and is expected to receive an audit before deploying on the main chain (Bradley, 2007). Geth node runs on a physically separate instance that can only receive communication from the IP address of our webserver. We have addressed webserver inaccessibility contingencies. The Geth node will be storing all the necessary secret keys for the prototype.

This approach will be used only to deploy on the Ropsten and Rinkeby test networks for prototyping. Migration onto Mainnet will happen post key architecture improvements. Our tentative solution for more robust key storage will involve, in addition to currently implemented PCI DSS security, multiple physically separated Geth nodes so that funds are stored in multiple contracts with different master keys and child keys spread out in a network (Gutoski & Stebila, 2015).

Claim Contract Design

ClaimContracts have the common interface:

```
Constructor //set up initial parameters of contract
issueTokens (internal) //issue executable tokens to buyers
redeemTokens // Does not have default, custom claim logic goes here
checkTokenValidity //return whether the token is valid
checkSufficientBacking //checks if amount in Backing Escrow is sufficient
getMaturity //return array of expiration block #. For a simple claim, array contains only 1 int
```

```
getStrike
getUnderlying
getEscrowAddress //allows anyone to see funds in escrow
killContract //unlock backing escrows and return funds to underwriter(s)
```

Token functions issue, accept, and return the validity of tokens. The motivation behind a token based model is to allow for secondary derivative markets and finer granularity. ClaimContract tokens use the ERC20 standard. Although Solidity automatically creates getter functions for public variables, we've implemented custom getter functions to improve the contract's interface. Our *killContract* function implements *selfdestruct*, but with some custom logic.

Software Stack

The prototype stack consists of TypeScript, Angular4, Node.js, and DynamoDB, hosted on AWS. The servers are in JavaScript to utilize existing infrastructure integrating web hosts with Ethereum. [14] The enterprise grade product will use a different stack to allow for higher concurrency and fault tolerance.

MetaMascara is used for client side communication with Ethereum. A Geth server, connected to the web host, deploys the multi-signature transactions and signs as Nomisma. Contract migrations and management are done with Truffle.

[14] We recognize our solution is not fully decentralized and have plans to implement IPFS and FileCoin

Technical References:

Bradley, T. (2007). PCI compliance implementing effective PCI data security standards. Burlington, Mass.: Syngress.

Gutoski, G., & Stebila, D. (2015). Hierarchical Deterministic Bitcoin Wallets that Tolerate Key Leakage. *Financial Cryptography and Data Security Lecture Notes in Computer Science,*497-504. doi:10.1007/978-3-662-47854-7_31

Schelling, T. (1980). The strategy of conflict (Rev. ed.). ed.). Cambridge: Harvard University Press.

7. Token Sources of Value

Our token generating methodology will aim to encourage truthful revelation of risk preferences, creation of a deep liquidity pool by sourcing risk from diverse user risk habitats, attract consistent suppliers of volatility and correlation protection, and discourage 'multi-tenanting' by allowing preferred risk profile tailoring.

We see five main potential sources of value (along with platform running costs) for the Nomisma token (NBT).

i. Access fee: covering the ability to access the platform in order to utilize the analytics and access historical transaction information.
ii. Usage fee: covering the ability to initialize transactions as well as the proceeds spent to initialize and maintain transactions up to claim expiry.
iii. Structuring fee: every transaction that gets replicated 'on platform' will generate only a percentage x of 100% backing, 100-x gets withheld.
iv. Intermediation fee: every transaction that gets matched without replication on the platform implies a percentage fee charged to both sides.
v. Arbitrage/Principal P&L: if the sum of lodged collateral > cost of replicating portfolio, upfront riskless P&L is generated. Further, if implied volatility bought by the Nomisma Foundation generates gamma trading profit (loss), this is a further source of P&L.

Nomisma Fee and Nomisma P&L

Nomisma tokens will allow, according to transparent predetermined formulas, participation on the above value generating streams. 1-4 will be diverted towards *Nomisma Fee* and 5 towards

Nomisma P&L.

i. Considering that the Nomisma Foundation stands ready to provide desired fixed income equivalent exposures, equivalently to buy calls/puts, i.e. volatility, the side that will be encouraged at initiation with more attractive pricing, potential fee waivers and preferential preICO pricing conditional on commitment to bid for fixed income exposures (offer puts), will be the 'risk averse' side.

ii. Considering further that 'on platform' naturally occurring transactions constitute the hedging portfolio desire of existing crypto holders (selling covered calls/buying puts), we anticipate the quick emergence of a volatility smile (and the corresponding correlation dynamic). We expect similar out-of-the-money puts to be more expensive than calls, with at-the-money ones priced in between.

iii. Token policy will attempt to create a separating equilibrium among uses between risk tolerant and averse ones also along the participation or not in defined downside P&L scenarios.

In the spirit of delivering a transparent and well-structured ICO in order to achieve our true goal for providing investors 'risk-sharing on the blockchain,' as well as steering clear of what our experience renders questionable practices, we will go against the grain as far as three common ICO practices are concerned:

i. There will not be any foundation, in the non-profit sense of the word, overseeing operations. There will be a for-profit company, the Nomisma Foundation, with proper governance, a board of directors and an advisory board, which will be transparent on a smart-contract basis. Extant laws and regulations provide for ecosystem participant

protections, shareholding and token pricing will be reflective of the value of the services provided and the fees contractually diverted as per above.

ii. We will not create an algorithmic token supply. All fee streams will be ETH and fiat linked and will generate more or less value towards the tokens. The Nomisma Foundation will own enough to stabilize their value on the upside on a transparent basis. The ETH-linked valuation will be denominated in small enough increments so as to facilitate payments of all of the above 'micro fees' as well as recurring 'sweep' of all P&L generated to all the rightful claimants.

iii. There will not be a 'mad scramble' for subscription, a 'winding down clock,' nor an 'early bird price special.' We will most probably employ a modified Dutch auction format for the ICO event. Considering that natural first users of our platform are both currently exposed and unexposed individuals and institutions, we want to minimize embedded incumbent advantage toward the aim of further democratizing financial access to these markets.

We will not be engaging in a proactive effort to list our token in any exchange. We will be maintaining liquidity around *Nomisma Fee* and *Nomisma P&L* tokens as a natural adjunct to maintaining the platform as liquidity streams get generated and directed, transactions consummated and, as P&L gets generated (will be shared with the participating token-holders).