



orange is the new green

THE EMERGENCE OF BITCOIN MONEY MARKET FUNDS

THEO MOGENET





contact

contact theo at theo.mogenet@protonmail.com

follow theo on twitter [@theomogenet](https://twitter.com/theomogenet)

get in touch at contact@axiombtc.capital

follow us on twitter [@axiombtc](https://twitter.com/axiombtc)

DISCLAIMER: This document is issued by Axiom Venture Partners Limited ("Axiom"), an appointed representative of Kingsway Capital Partners Limited. Kingsway Capital Partners Limited ("Kingsway") is authorised and regulated by the Financial Conduct Authority in the United Kingdom (the "FCA"). Axiom does not offer investment advice or make any recommendations regarding the suitability of its products. This communication does not constitute an offer to buy or sell shares or interest in any Fund. Nothing in these materials should be construed as a recommendation to invest in a Fund or as legal, regulatory, tax, accounting, investment or other advice. Potential investors in a Fund should seek their own independent financial advice.

Past performance is not necessarily a guide to future performance. Axiom has taken all reasonable care to ensure that the information contained in this document is accurate at the time of publication, however it does not make any guarantee as to the accuracy of the information provided. While many of the thoughts expressed in this document are presented in a factual manner, the discussion reflects only Axiom's beliefs and opinions about the financial markets in which it invests portfolio assets following its investment strategies, and these beliefs and opinions are subject to change at any time.



outline

introduction

pg 1 - 2

I. finding stability amidst uncertainty

the elusiveness of real savings in the contemporary macroeconomic landscape

pg 2 - 4

II. building a Bitcoin-centric money market fund

utilizing Bitcoin's novel properties to construct a real dollar savings instrument

pg 4-10

III. towards a non-custodial future

incorporating discreet log contracts into our design to remove centralization and counterparty risk

pg 10-13

conclusion

a sly roundabout way towards hyperbitcoinization

pg 13

orange is the new green

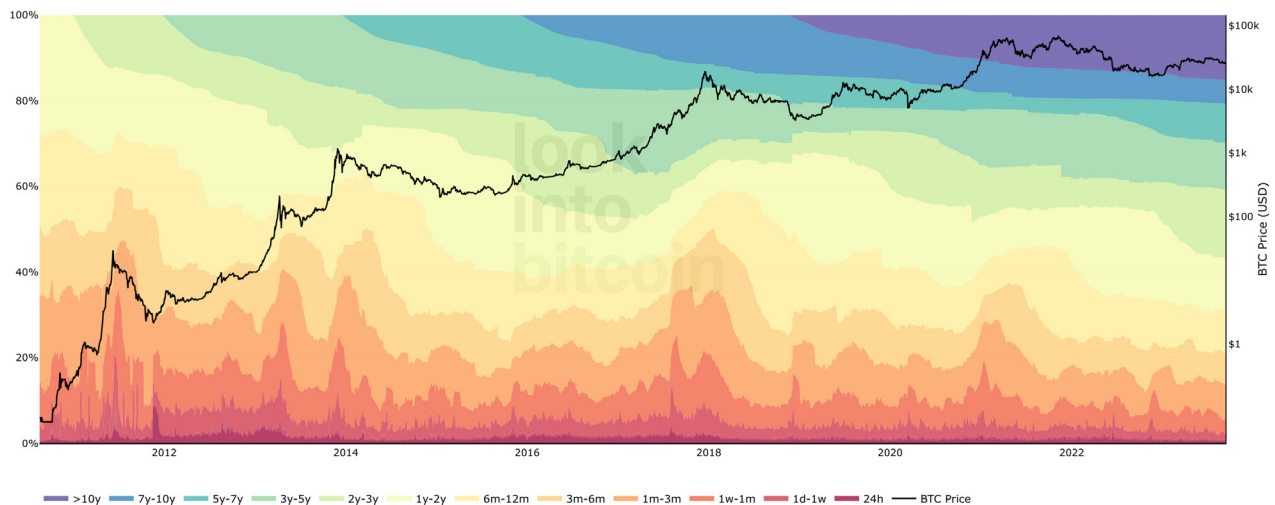
introduction

The transformative power of Bitcoin as a savings technology is now widely acknowledged. No other asset class in history has been able to rival its long-term returns, underpinned by the unique combination of Bitcoin's scarcity and the commitment of its holders to long-term accumulation.

During a recent interview, legendary investor Stanley Druckenmiller shared an insight he gained from Paul Tudor Jones II perfectly illustrating this dynamic: when Bitcoin's price plummeted from \$17,000 to \$3,000, an astonishing 86% of those who acquired it at its peak did not sell.[1] This steadfast "hodl" mentality is vividly illustrated in the "hodl waves" chart, as shown below in Figure 1, a graphical representation of Bitcoin supply categorized by time held.

The chart demonstrates the gradual reduction in circulating supply as long-term holders transfer their coins into cold storage. This process explains in part Bitcoin's appreciation, but also its characteristic volatility, as a significant influx of capital into an asset with a fixed supply naturally leads to pronounced price swings.[2]

This general dynamic is what makes Bitcoin arguably the greatest savings vehicle ever invented, and yet, at the same time, an inadequate solution for storing short-term cash balances. Whether for individuals or businesses, maintaining short-term cash balances in Bitcoin is ill-advised due to this volatility. Even Bitcoin-only businesses acknowledge the necessity of holding fiat currency to navigate the uncertainties of daily operations.



That said, I believe there is a plausible scenario in the medium-to-long term in which Bitcoin absorbs short-term cash balances. To be clear, this would be before attaining anything like the status of a global unit of account, and despite its seemingly disqualifying volatility relative to fiat competition. This may seem self-contradictory at first glance. But I believe that by introducing Bitcoin into a flawed incentive structure, and teasing out its less-than-obvious properties, a compelling solution emerges, incentivizing holders of cash balances to actively contribute to Bitcoin's adoption.

This article delves into this intriguing prospect. It commences by dissecting the challenges faced by holders of cash balances. Subsequently, it explores how Bitcoin can offer a deposit facility superior to existing alternatives. I conclude by examining current prototypes of Bitcoin money market funds and contemplating alternative designs. Unlike "basically risk free" Crypto yield products,[3] throughout the article I will draw attention to the intricate trade-offs integral to designing the types of product discussed.

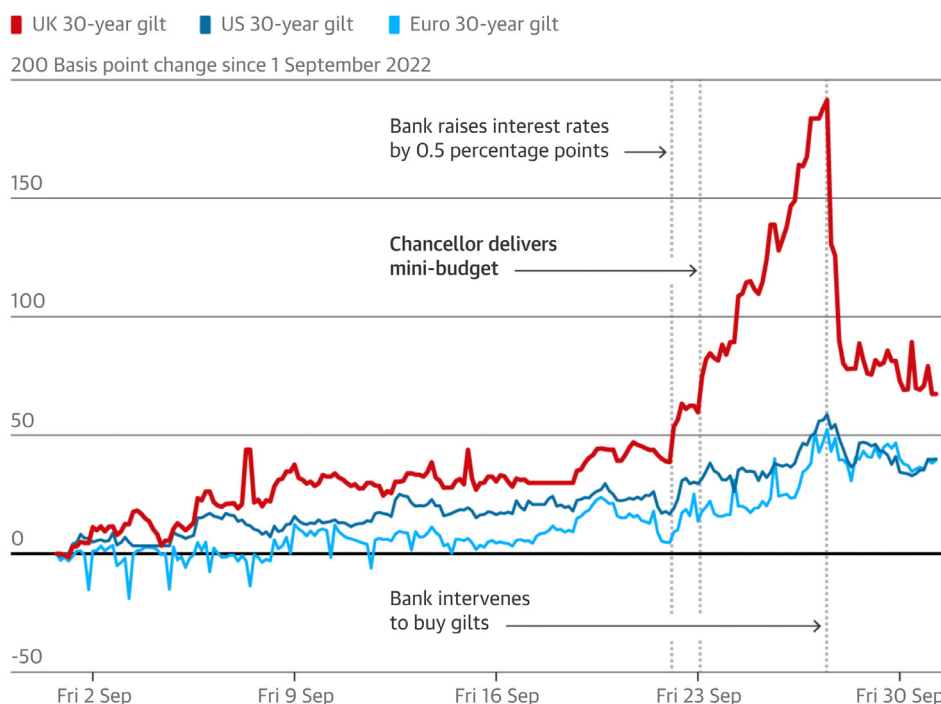
I. finding stability amidst uncertainty

In the realm of economic theory, the rationale for holding cash and its equivalents is rooted in the anticipation of future uncertainty. In practice, however, the erosion of fiat currency's value skews this rationale, compelling economic agents to seek refuge in "highly liquid securities." Indeed, these securities may be offered as collateral to credit suppliers when cash is needed, and also safeguard purchasing power, a feat that cash alone struggles to achieve in the modern fiat system predicated on a foundation of never-ending increases in the money supply.

The term "highly liquid securities"[4] warrants careful consideration, as liquidity is context-dependent rather than an inherent property of an asset. Liquidity translates to the ability to promptly find a buyer or seller and settle a trade at prevailing market prices. Particularly within a credit-based economic structure, the propensity for leverage to accumulate until a tipping point triggers a destabilizing market downturn, colloquially referred to as a "Minsky moment," underscores the contextual nature of liquidity: everything is liquid until nothing is. In such scenarios, the notion of a "liquid" portfolio loses its luster, as selling under duress occurs at less than favorable terms.

While traditionally perceived as exceedingly rare occurrences in so-called "developed markets," liquidation cascades are becoming increasingly commonplace. Within our financial framework, liquidity primarily hinges on credit acquisition through collateral pledging, thus laying the groundwork for a cycle intertwining collateral face value and market liquidity. As the value of collateral depreciates, the issuance of credit diminishes – or goes into reverse – exerting a downward pressure on market prices. Consequently, this prompts liquidation events, subsequently intensifying the erosion of asset values and liquidity. Especially so considering that government securities and other debt instruments, rapidly depreciating in value due to rate hikes, constitute the bulk of such collateral.

A compelling illustration of this concept emerged in the UK last October when the Gilt market teetered on the edge of collapse. The rise in Gilt yields subsequent to fiscal policy announcements from the Chancellor of the Exchequer triggered margin calls for pension institutions that had pledged long-dated Gilts as collateral. In a rush to raise cash to meet their margin requirements they dumped large amounts of Gilts, ironically due to their being thought to be the most "liquid" asset, which further depreciated the capital value of their collateral, thus forcing them to sell even more Gilts. The Bank of England then intervened to avert calamity by buying large amounts of 30-year Gilts, spurred by the realization that such a downturn could imperil the pension industry and decimate a substantial portion of British savings.[5]



Guardian graphic. Source: Bank of England

Figure 2 - timeline of pricing in 30-year government bonds from UK, US, EU

This episode served as a wake-up call to central bankers globally, exposing the precarious balancing act they faced. Their current policy choices—whether to tighten the money supply to curb inflation or risk stifling liquidity and imperiling the financial system—resemble the treacherous path between Scylla and Charybdis.

The implications for money managers are threefold:

1. **Elusive Positive Yields:** Besides new government bonds, genuinely positive yields are nowhere to be found.
2. **Money Market Funds' Resurgence:** The demand for money market funds is amplified by both enticing short-term yields and risks of illiquidity in other markets.
3. **Looming Government Intrusion:** The specter of insolvent governments resorting to convoluted methods to confiscate capital for debt servicing is an escalating concern.

This final threat, though somewhat underestimated across the past four decades or so, will surely garner heightened attention in the foreseeable future. Recent events underscore governments' readiness to wield their currency and banking systems as tools for political and geopolitical manoeuvring.

The freezing of Russian assets by the US and its allies in response to the Ukraine conflict; the targeted scrutiny of crypto banks through Operation Chokepoint 2.0;^[6] the expansion of the OFAC sanctions list; the manipulation of FED swap lines; the exclusion of Iran from SWIFT; and the surge in central bank digital currency (CBDC) initiatives collectively serve as cautionary signals for investors and nations alike.

Despite ongoing discussions surrounding the process of de-dollarization, the prevalence of USD in global trade and financial agreements persists—86% of FX transactions and a significant portion of global debt remain USD-denominated, and the US government is not shy of leveraging the dollar's reserve status to advance its geopolitical objectives.

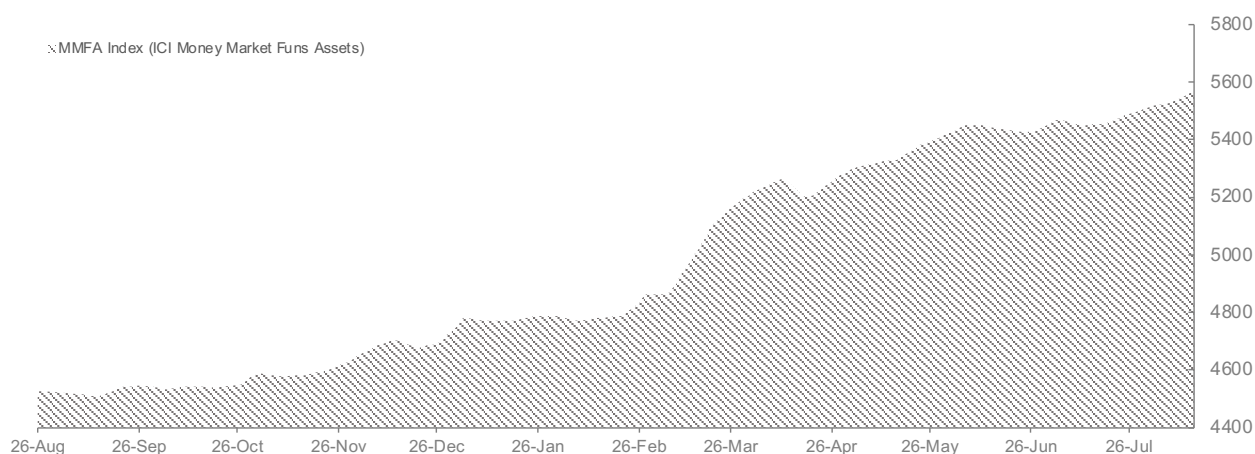


Figure 3 - aggregated money market fund assets (+\$5.5Tn)

With all this framing the global macroeconomic backdrop, the concept of a deposit facility resistant to seizure, capable of yielding positive real returns in USD, assumes profound significance. Such facilities are poised to attract global interest from discerning investors seeking stability amidst a sea of uncertainty.

II. building a Bitcoin-centric money market fund

A. But Where Does The Yield Come From?

The pursuit of optimal real yields is a fundamental task for money managers, traditionally thought to lead to preferencing allocating capital to the most effectively managed monetary zones. These zones can vary across time and space, ranging from Germany to Japan to the US, each having its relative advantages and disadvantages. However, all share a common

characteristic: financial markets as a whole are built up from fiat bond markets specifically, all of which rest on the necessity of unbounded money supply expansion over time.

In stark contrast, Bitcoin operates on an inherently sound and predictable monetary policy. Unlike traditional fiat systems, Bitcoin doesn't necessitate continuous money supply growth to sustain what is essentially a convoluted Ponzi scheme and doesn't hinge on the whims of central planners. Instead, it adheres to a deflationary issuance schedule dictated by algorithmic adjustments of the mining difficulty. While central banks manipulate money's price to influence its supply, the Bitcoin protocol defines supply evolution, and the price of Bitcoin subsequently adjusts. Given Bitcoin's robust monetary framework, this self-contained price discovery, reflecting the opportunity cost of not holding Bitcoin, unsurprisingly commands positive real yields across long enough time horizons if denominated in fiat. In other words, Bitcoin has never stopped monetizing, and I see no reason to believe it ever will.

In the fiat arena, sovereign entities vie for capital inflows to their domestic markets. Higher real interest rates tend to attract more capital, from bond markets



Figure 4 - spread between US10Y & JP10Y (LHS, orange) vs USDJPY (RHS, green)

up. This attraction, however, hinges on the ability to hedge currency risk—a practice primarily realized through FX-swaps. Such derivatives involve the exchange of one currency's performance over some interval for another's, therefore allowing investors to own a foreign security without bearing any currency risk, for a typically small cost. Crucially, differences in monetary policies significantly impact exchange rates, with a nation's superior monetary policy often translating to a more robust currency that outperforms competitors.

A compelling illustration of this phenomenon occurred last year with the Federal Reserve's rate hikes leading to a rally in USD. The prospects of higher yields in the US pushed money managers in Japan to buy UST while hedging their USD exposure, therefore leading to massive capital flight from Japan to the US, a trend reflected by evolution of the USDJPY pair. As the reader can see from Figure 4, the interest rate spread between the US and Japan closely tracks changes in their relative exchange rate.

Now, consider a currency like the Argentinian peso (ARS), notorious for being mismanaged. Hedging against the ARS with a USD exposure incurs significant costs, as there is high expectation of the USD outperforming atop high uncertainty regarding future market dynamics for the ARS. Conversely, swapping USD exposure for ARS exposure could potentially yield a payout in ARS terms. However, within the traditional fiat framework, this avenue for a positive carry USD remains limited, as the USD's perpetual demand inherent to its central role in the system diminishes such opportunities.

Enter a currency like Bitcoin, which consistently outperforms the USD over long-enough time periods due to its robust monetary policy. Hedge Bitcoin against the dollar, and the dynamics flip — now, you receive a payout for hedging. This phenomenon boils down to opportunity cost. Selling Bitcoin exposure for USD exposure essentially means relinquishing returns that, on average, remain positive. As Bitcoin is still in its monetization phase, it remains very volatile and

thus makes a poor cash instrument in a fiat world. But one can still benefit from Bitcoin's superiority even by selling back exposure, given the likely and average result of a stable balance in dollars plus a positive yield.

B. Analysis of Bitcoin Covered Shorts Performance

This is perfectly demonstrated by Bitcoin's derivatives market. It stands as one of the few markets structurally inclined towards contango, where future prices consistently surpass spot prices—providing a pathway to a positive cash-and-carry arrangement by shorting the current dollar value of one's Bitcoin balance.

The largest and deepest Bitcoin derivatives market is the perpetual market. Invented by BitMEX in 2016, perpetual swaps are a true Bitcoin financial innovation leveraging the ability of Bitcoin to settle around the clock.

Traditional futures contracts expire at market close on a certain date, and therefore, for any given asset, multiple futures contracts are always trading in

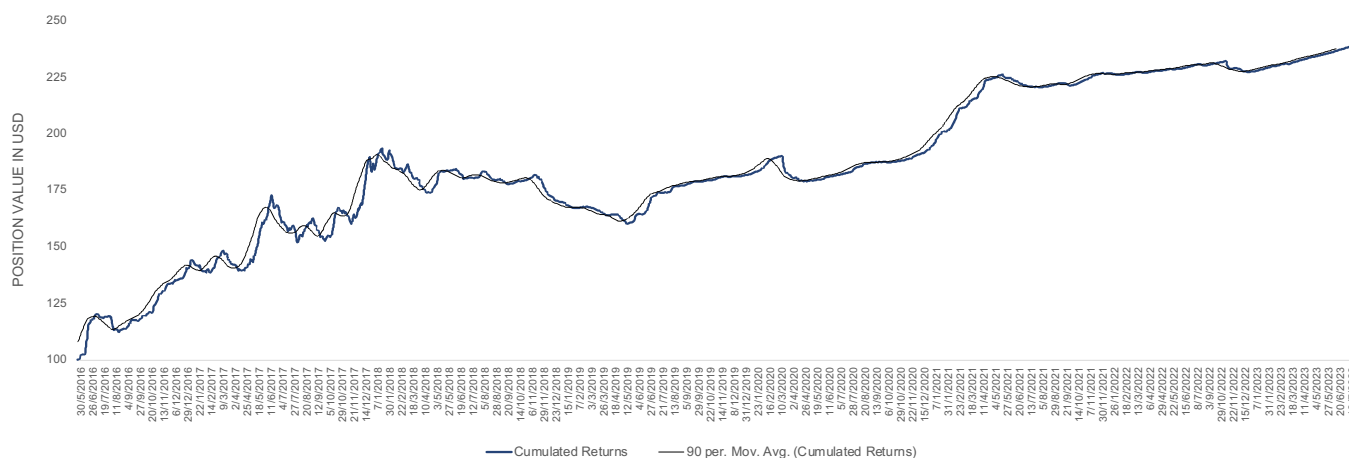
parallel. This approach fragments the order book and forces market participants to roll their old contracts into new ones as the old expire to maintain their net position, with contracts that may trade at significantly different prices due to basis—difference between future price and cash price of a commodity.

Conversely, as aptly expressed by their name, perpetuals trade continuously in a market where premiums are paid between long and shorts on a peer-to-peer basis every 8 hours, thereby closing the spread between spot and futures markets. This allows the convergence towards a single market for Bitcoin futures and also provides market participants with the ability to hedge with little management and no need to roll.

Per BitMEX data, between 14th of May 2016 (launch of perpetuals) and 13th of July 2023, the funding rate was positive 72% of the time.

We can go further and look at the historical performance of Bitcoin hedged against the dollar using perpetual swaps. Below is a chart displaying the performance of a \$100 position held idly in covered shorts since the launch of perpetual markets:

Figure 5 - BTC covered short cumulative returns



Over a span of seven years, this approach would have yielded a remarkable +140% return, averaging around +20% annually, with a standard deviation of 33.3%. By indulging in the erroneous financial orthodoxy of quantifying (even equating) “risk” as “volatility”[7] and using the compounded returns of the Fed Funds rates over the same period as a risk-free benchmark, we get a Sharpe ratio of 3.79 – something very few fund managers can tout.

Figure 6 below compares historical performance of this covered short position, both nominally and in real terms, against US10 treasuries and short-term bank deposits, shedding light on the superiority of the former. This data reflects not only the outperformance but also highlights the trend towards negative real yields in the Treasury market—a factor likely to

motivate market participants to explore alternative avenues for storing their cash.

While these data are encouraging, they still falls short in evaluating the relative competitiveness of Bitcoin covered shorts versus conventional deposit instruments. A more comprehensive approach involves examining the performance of all potential covered short positions under varying entry and exit points. Indeed, what interests a money manager is not the gross performance but rather knowing he can store his cash for any duration without risking capital losses and still offset inflation. So, to gauge this, I wrote a Python script[8] that calculates annualized performance for all feasible covered short positions lasting over a week since the inception of perpetual markets in May 2016.

Asset	2016 (annualized)	2017	2018	2019	2020	2021	2022	2023 (annualized)	Average
BTC Nominal Yield	63.4%	30.9%	-2.2%	7.0%	5.5%	16.1%	0.6%	9.1%	16.3%
CPI YoY	1.3%	2.1%	2.4%	1.8%	1.2%	4.7%	8.0%	5.8%	3.4%
BTC Real Yield	62.1%	28.8%	-4.6%	5.2%	4.3%	11.4%	-7.4%	3.3%	12.9%
4-weeks bank discount (Nominal)	0.25%	0.83%	1.81%	2.08%	0.35%	0.04%	1.61%	4.63%	1.45%
4-weeks bank discount (Real)	-1.1%	-1.3%	-0.6%	0.3%	-0.9%	-4.7%	-6.4%	-1.2%	-2.0%
US 10Y (Nominal)	1.84%	2.33%	2.91%	2.14%	0.89%	1.45%	2.95%	3.64%	2.27%
US 10Y (Real)	0.5%	0.2%	0.5%	0.3%	-0.3%	-3.3%	-5.1%	-2.2%	-1.1%
Difference BTC Bank Discount	63.1%	30.0%	-4.0%	4.9%	5.1%	16.1%	-1.0%	4.4%	14.8%
Difference BTC US10Y	61.5%	28.5%	-5.1%	4.8%	4.6%	14.7%	-2.4%	5.4%	14.0%

Figure 6 - historical performance of covered short position vs comparators

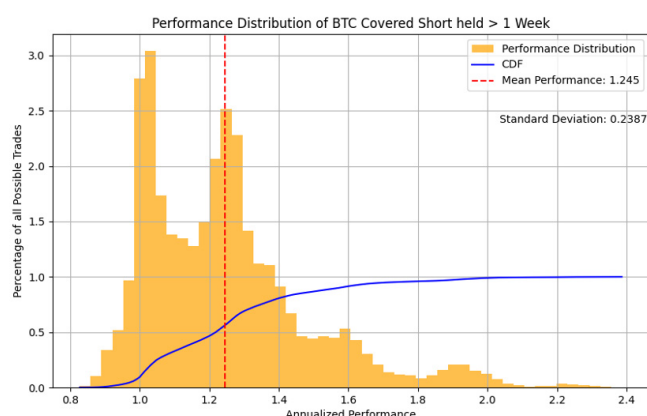


Figure 7 - performance distribution of covered shorts held > 1 week since inception

The cumulative distribution function (blue) for the distribution of the +28m resulting trades indicates that only 8.3% incurred losses (broke the buck), and the mean performance (red) highlights an average return of 24.5% per year.

Beyond the relative benchmark comparison, the evolution of return distribution proves enlightening. As the cumulative performance chart demonstrates, returns become less volatile over longer time intervals while consistently remaining positive. This phenomenon suggests that as Bitcoin and its derivatives market mature, funding rates stabilize and instances of structural negative funding are both shorter and rarer.

During the present cycle, 81% of funding events have been positive, even despite an extended bear market. There were only two periods characterized by meaningful losses due to negative funding: one spanning six months (from 19/5/2021 to 20/11/2021), and the other lasting under five months (from 9/11/2022 to 31/3/2023), resulting in a maximal nominal loss of merely 2.4%.

Moving to the performance distribution of all potential covered short trades within the current cycle, only ~5% led to losses, averaging a performance of 10.3%, and showcasing reduced volatility, from 23% to

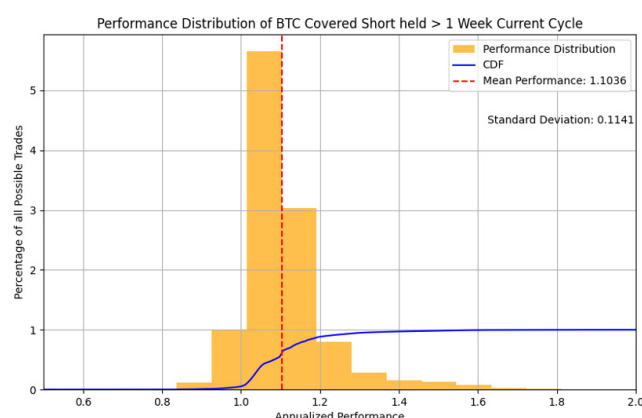


Figure 8 - performance distribution of covered shorts held > 1 week since most recent halving in May 2020

10%. These insights, both in their raw data and trend analysis, foster optimism for a Bitcoin-based deposit facility. They not only exhibit steady returns capable of compensating for occasional losses, but they also illustrate a decrease in the frequency of negative funding periods. Although encouraging, such a trend doesn't preclude future periods of deeply negative funding. If, for instance, the largest stablecoins, such as USDT & USDC, were to implode and fiat off-ramps from exchanges severed, the only option left for market participants seeking refuge would be to hedge their crypto positions through derivatives, which could lead to a prolonged period of negative funding. Another tail risk scenario worth mentioning would be the case of a controversial fork leading to a schism within the Bitcoin community, fostering uncertainty about Bitcoin's future.

This quantitative perspective indicates that hedging Bitcoin's volatility through perpetual swaps generates higher returns than comparable investments such as short-term USD debt-instruments. While the perpetual swap market and the Bitcoin spot market aren't yet liquid enough to absorb the trillions of dollars of cash equivalents in perpetual search for real positive yield, they currently have enough depth to allow billions of dollars of Bitcoin covered short positions – see Figure 9 below.



Figure 9 - Bitcoin price vs open interest. source: coinglass

But, more importantly, such an opportunity could be a huge catalyst for Bitcoin adoption and price appreciation, because running a Bitcoin covered short position requires buying spot bitcoin in the first place. So, as individuals and firms new to Bitcoin seeking new vehicles to park cash turn to this opportunity, we could witness increased buy pressure in bitcoin's spot markets, which will in turn lead to higher liquidity and allow more entities accessing this trade, thus fuelling a virtuous cycle for Bitcoin adoption.

C. Open 24/7/365

Another thing to keep in mind is that Bitcoin takes no vacations and rings no trading bells.

Imagine this scenario: It's a Friday evening, and as you're scrolling through your Twitter notifications on your way home, you discover that Silicon Valley Bank is in deep trouble, and the FDIC is poised to take over the bank. In traditional markets you would have to wait 3 days to take action, whereas with such a Bitcoin Money Market Fund you could promptly unpeg your Bitcoin in a few clicks, thereby making a directional bet on Bitcoin pumping through the turmoil.

Once we grasp the contextuality of liquidity, can we genuinely classify something as liquid if it's rarely tradable? Bitcoin may still lag behind in liquidity when compared to other more established asset classes. However, it holds the potential to become the most liquid asset globally. Firstly, because, as previously mentioned, it represents a pure form of cash and isn't tied to any person or institution's liabilities. Secondly, it can settle around the clock, every day of the year.

A Bitcoin-based money market fund would inherit this uninterrupted activity, a significant advantage when traditional markets operate only 252 days a year from 9 to 5, or even less for many banks.

D. Seizure-resistance

Lastly, such a Bitcoin-based MMF would outshine incumbents thanks to its relative resilience against political and regulatory capture.

In essence, the investment involves holding Bitcoin in a margin account, hedged against the USD. For USD holders facing apprehension from the US State Department, this offers a more flexible and reassuring option compared to an account with a Federal Reserve-regulated G-SIB.

A prime example is China's current predicament. In the midst of an escalating cold war with the US, negotiating bilateral trade agreements in Renminbi with most of its trade partners, and contending with asset seizures by foreign powers, a Bitcoin-based money market fund could prove invaluable.

However, Xi Jinping will not entrust CZ, Brian Armstrong, or indeed BitMex with the CCP's funds, especially after the FTX debacle. So, wouldn't it be nice if we could find some ways to build such a Bitcoin-based deposit facility directly on-chain so that no one ought to be trusted with custody of customer funds?

It just so happens we can...

III. towards a non-custodial future

In practical terms, various methods exist for constructing a dollar-stable product using Bitcoin covered short positions. This decision entails trade-offs: the choice is between maintaining a Bitcoin covered short position through a centralized exchange—a route offering flexibility, high liquidity, and cost-effectiveness but involving counterparty risk—or adopting on-chain derivatives contracts—a route offering greater security by eliminating counterparty risk, albeit at the cost of liquidity and efficiency.

"On-chain derivatives contracts on Bitcoin? When did this become a reality?"

To be precise, there isn't a fully operational on-chain derivatives market for Bitcoin at present. However, all the essential technical components required for such a market to emerge are in place, and several Bitcoin-oriented companies are currently engaged in

experimental ventures. Although this article doesn't delve comprehensively into the entire spectrum of strategies enhancing Bitcoin's programmability, one avenue—Discreet Log Contracts (DLCs) — stands out. Notably, DLCs align seamlessly with our use case and have undergone thorough testing by various teams (SuredBits, Atomic Finance, LN Markets, 10101, etc.).

Discreet Log Contracts

In essence, a Discreet Log Contract (DLC)[9] represents an off-chain agreement between two parties, wherein on-chain enforcement of payment is possible upon the fulfilment of specific conditions. If the reader is familiar with the lightning security model, grasping the mechanics of DLCs should come naturally, as they bear structural similarities. Like the lightning network, DLCs enable parties to exchange off-chain pre-signed Bitcoin transactions from a multisig wallet pre-funded by the two parties. This facilitates unilateral payout claims, even if one party fails to cooperate.

As in Lightning, DLCs employ 2-of-2 multisig and pre-signed off-chain transactions. However, in DLCs, signatures are encrypted in a verifiable way such that they can only be decrypted using a certain oracle attestation—because payment depends on an external event, a third party (termed an "oracle") is necessary to provide relevant information for contract settlement. Fundamentally, DLCs allow either party to utilize their respective key along with the oracle's attestation to publish a valid spending transaction from the multisig to their own address. This transaction exclusively reflects the agreed-upon payout should the bet succeed.

A detailed illustration of this process follows:[10]

Suppose I bet 1 BTC against Allen's 1 BTC, wagering that RFK Jr will win the Democratic Primary in 2024—a binary outcome space. Constructing transactions that spend the 2 BTC from the funding transaction to our respective addresses suffices. In the first pre-signed transaction, spending the 2 BTC to my address, Allen's signature will be tweaked in such a way that I would need the oracle attestation of RFK's victory to make it valid, and conversely, to make the pre-signed transaction spending the 2 BTC to his address valid,

Allen would need the oracle attestation of RFK's defeat. If we concur on the result, I can request Allen's signature to broadcast the pre-signed transaction, thus securing my 2 BTC payout. But, in case Allen refuses cooperation, I can employ the oracle's attestation, issued upon confirmation of the event "RFK Junior won the Democrat Primary," to execute a valid transaction transferring the 2 BTC to my address. Transactions of this nature, enforcing contract results, are termed Contract Execution Transactions (CETs).[11]

In the context of a BTCUSD future contract based on DLCs, complexities arise—in particular because the outcome space is no longer binary. Bitcoin's value could fluctuate anywhere between \$0 and a gazillion dollars in a week. However, in practice, hedging exposure over a defined range—say, between \$20k and \$40k—is sufficient. Theoretically, the outcome space is infinite, but the ability to hedge within specific boundaries meets practical requirements. These boundaries can be further aggregated into larger ranges as market dynamics allow.

Mathematically inclined readers might note that an infinite set of real numbers still exists within a \$20k to \$40k interval. To address this, we can discretize the interval, creating CETs for every \$10 increment between \$20k and \$40k. The level of accuracy, whether \$1000 or \$5 increments, can be chosen based on preference, with the caveat that increased accuracy also translates to greater data storage requirements, as all CETs must be maintained until contract expiration.

Hence, for a perpetual DLC swap with Allen, assuming a \$10 margin of error, I would need to create a CET for each of the 2000 \$10 intervals between \$20k and \$40k—though an efficient trick allows compression of this data, sidestepping the need for excessive local data storage: at contract expiry, the chosen oracle(s) sign a BTCUSD price, enabling either party to employ the attestation for CET transaction completion, thus enforcing the contract unilaterally. This hinges on the fact that neither party can derive a valid CET without first knowing the corresponding oracle attestation.

Continuing to hedge merely involves entering another DLC or "rolling" the position, just as one would in a conventional market.

In essence, DLCs alter the clearing mechanism more than the trading experience itself. However, trade-offs exist, with gains in one aspect balanced by losses in another. DLCs don't require deposit to a centralized exchange[12] and offer commendable scalability, and privacy, yet exhibit capital inefficiency and challenges in transferring the position:

Advantages

- **Privacy:** CETs generated off-chain coupled with indistinguishable on-chain DLC footprints ensure robust privacy—a quality enhanced by the fact that even the oracle remains unaware of contract terms or existence.
- **Scalability:** Since only one CET is validated on-chain, DLCs remain scalable, avoiding transaction bloating prevalent in smart-contract-based DeFi on other platforms.

Disadvantages

- **Capital Efficiency:** DLCs, compared to traditional contracts, suffer capital inefficiency. Both parties must send sufficient collateral in the funding transaction to cover all contract outcomes. Traditional derivatives markets typically employ a capital buffer in line with net positioning rather than total open interest, leveraging economies of scale.[13]
- **Transferability:** Current solutions for transferring an on-chain DLC from one party to another are limited, although it's more feasible within a lightning channel-based DLC.[14] This limitation complicates rolling positions as it entails posting new collateral in a fresh-DLC while still having collateral locked until expiry in the older DLC.

Given these considerations, it's conceivable that non-custodial products, yielding dollar-stable balances, could emerge over the next few years. Nevertheless, these alternatives carry higher costs than centralized counterparts.

Practically, managing DLCs – especially for frequent position rolling – can prove challenging and time-consuming, warranting the engagement of third-party service providers. Such intermediaries would likely offer services like CET backups, oraclizing, and automatic generation of new CETs for position rolling. While these intermediaries wouldn't entail loss of Bitcoin custody, additional costs would be incurred and privacy lost.

Matching buyers and sellers efficiently within a decentralized framework remains a challenge, at present necessitating intermediary creation and management of the marketplace—operating either as an order book or OTC desk. Furthermore, DLC position rolling involves publishing a CET at expiry and a new funding transaction for a fresh DLC, incurring two transaction fees that reduce net profits from Bitcoin covered short positions – though, DLCs could be nested in a lightning channel to facilitate rolling positions. [15] This last point is worth stressing: as maintaining a stable dollar value entail remaining hedged, one could well be forced to open/roll/close a DLC in a high fee environment, especially so during extreme market events as the opportunity cost associated with settlement delay rises.

Yet, even with these extra costs, the funding rate data from Part II indicates potential for accruing positive real yields on stable dollar balances. These costs represent a modest price to pay for access to two complementary instruments, enabling end-to-end financial transactions without intermediaries: Bitcoin for long-term savings and this solution for short-term cash balances – until fiat money fades away and Bitcoin can serve both roles at once.

While the market underlying these derivatives trades will operate on the Bitcoin timechain, stable dollar balance solutions are not one-size-fits-all. An array of products with distinct value propositions is expected to emerge. Some will cater to individuals seeking readily available cash for expenses, while others will cater to corporations and financial institutions seeking inflation- and seizure-resistant deposit solutions. There is even potential for packaging this into mainstream traditional financial products like ETFs.

Interestingly, a Bitcoin wallet named BlinkBTC (formerly Bitcoin Beach Wallet) operated by Galoy has already introduced such a feature. However, it comes with a trade-off: Bitcoin short positions are executed through exchange APIs, and the user doesn't retain custody over their Bitcoin. This design necessitates margin being held at the exchange, entailing counterparty risk. Although this provides deep order book access and cost-effective pegging or depegging of Bitcoin, it involves a level of trust in the wallet provider and the partner exchange.

In a similar vein, LN Markets is currently exploring the concept of an OTC desk for DLC-based Bitcoin futures. This initiative could render the process more appealing, enabling corporations and individuals to hedge their Bitcoin exposure on-chain, with minimal trust requirements, privacy, and relatively low overhead.

Imagine a Bitcoin miner paying for energy in fiat but earning revenue in Bitcoin. The Coinbase transaction obtained by mining a new block isn't spendable for the next 100 blocks, forcing the miner to bear currency risk. A similar situation arises for power companies selling electricity to miners. They supply kWh upfront and send a bill 15 to 90 days later, a timeframe where both Bitcoin's price and hashrate volatility could lead to the miner's bankruptcy, often leaving the power company with a worthless credit. This credit risk could be eliminated by the mining company streaming sats to match consumption in real-time, while the power supplier automatically hedges to maintain a stable dollar value until they choose to convert the Bitcoin to fiat.

While this may look like a niche market, the potential for substantial innovation could drive increased volumes—especially if asset managers offer such products in institutionalized wrappers.

As previously mentioned, high-net-worth individuals, corporations, financial institutions, hedge funds, and even sovereign entities are in search of inflation-resistant and seizure-proof dollar deposit solutions. Though they currently rely on money market funds yielding slight positive rates, this trend may not persist due to ongoing monetary tightening wreaking havoc in the banking sector.

Asset managers, however, cannot offer such products by holding fund assets on centralized exchanges. Even if they were willing, regulatory constraints would prevent it. Yet, by managing assets on-chain, either directly or via an audited third-party custodian, legal objections would likely diminish. While an ETF centered on these concepts might not launch tomorrow, the maturation of on-chain derivatives markets could incite asset managers in jurisdictions more amenable to financial innovation to consider and test such a product.

conclusion: a sly roundabout towards hyperbitcoinization

Our existing financial system is a mirage of wealth and liquidity, sustained by an ever-expanding money supply. Bitcoin emerges as the ultimate shield against the inevitable reckoning that will shatter this illusion. While Bitcoin might not be an effective solution for preserving purchasing power in the short term, it holds the potential to evolve into one. As long as there are daring traders seeking Bitcoin leverage, a promising avenue arises: selling exposure to Bitcoin and reaping substantial premiums atop dollar-pegged stability. The nascence of the market for Bitcoin derivatives contributes to the current premium's volatility, but over time, prices and yields should come to mirror underlying differences in monetary policies, greatly favoring Bitcoin holders.

The horizon beckons for change. No clean balance sheet remains under which to sweep problems, and the fiat mirage is further exacerbated by relentless money printing, only fuelling inflation. Governments are resorting to drastic measures, confiscating private wealth to bail out their faltering regimes—a road that unmistakably leads to financial repression.(16)

In the spirit of "necessity is the mother of invention," I believe the burgeoning interest in money market funds is poised to drive resources towards various implementations of the concepts discussed in this article. Given the prevailing macroeconomic environment, corporations, High Net Worth Individuals, hedge funds, and bond portfolio managers are all primed to embrace such a product. Easy access and secure entry ramps will serve as vital catalysts for adoption.

Anticipating the responses from some fervent Bitcoin advocates who may perceive in this approach a departure from Bitcoin ethos or potential vulnerabilities, it's important to acknowledge and address concerns. While I don't claim a complete grasp of every intricacy proposed, I find the prospect remains worth pursuing. This assertion is buoyed by the grim reality of the hyperbitcoinization scenario outlined earlier. Hyperinflation may loom in many nations, but it's not the desired outcome. As Keynes aptly noted, hyperinflation is akin to shuffling cards and tossing them skyward, with results not a man a million could predict. Thus, a sly roundabout way, allowing Bitcoin to gradually absorb both long-term savings and short-term capital, seems to me a worthwhile endeavor.

In essence, this perspective advocates for Bitcoin to maintain its role as a Jujitsu master, leveraging opponents' strengths to amplify its own impact. It's already masterfully demonstrated this strategy against climate hysterics: why not direct this finesse towards the finance bros?

A masterful mouse trap awaits construction, replete with a tempting yield as bait—a scheme poised to transform Bitcoin's detractors into pawns of hyperbitcoinization. Initially, as they outshine rivals and appease their clients, they will likely embrace this paradigm, characterizing it as one more tool of financial engineering among many. But as Bitcoin increasingly renders all other tools irrelevant, their sentiment will have to shift. And in shifting, they will inadvertently expedite the overhaul of the global monetary paradigm—a transformation that will be irreversible.

Thanks to Allen Farrington, Lyn Alden, Daniel Prince, and Théo Pantamis for their suggestions and corrections.

End Notes:

[1] Source: <https://news.bitcoin.com/bitcoin-fomo-paul-tudor-jones-stan-druckenmiller-invest-millions-btc/>

[2] This wisdom is encapsulated in an expression popular amongst Bitcoiners, “stay humble and stack sats.” stack sats because bitcoin’s superior monetary characteristics almost guarantee it will outperform every commodity in the long run but stay humble because nobody can confidently predict its price behavior over the short-term.

[3] To quote Raoul Pal on now-defunct Terra, clip available: <https://www.youtube.com/watch?v=KiYkijPlqU>

[4] The term “security” refers to a fungible, negotiable financial instrument that holds some type of monetary value. A security can represent ownership in a corporation in the form of stock, a creditor relationship with a governmental body or a corporation represented by owning that entity’s bond; or rights to ownership as represented by an option.

[5] See <https://henrytapper.com/2022/09/29/anatomy-of-a-crisis/> or <https://www.ft.com/content/2a2e7a9b-d984-45c1-8ada-0d0a6e57911b> for a more detailed explanation.

[6] As recounted and analysed by Nic Carter here: <https://www.piratewires.com/p/crypto-choke-point>

[7] At the core of all financial mathematics lies the idea that volatility, often measured by the standard deviation, is a proxy for “risk”. This is untrue because markets are uncertain, not risky: you can’t know a priori the distribution of outcomes; or to put it more scientifically, financial markets are not ergodic, which is a fancy way of saying that as an investor you care more about the performance of your portfolio than the dispersion of the returns in the ensemble, especially if you used leverage. See Peters, O. The ergodicity problem in economics. Nat. Phys. 15, 1216–1221 (2019). <https://doi.org/10.1038/s41567-019-0732-0>.

[8] The reader can download this script, spreadsheets, and all data used in this article [here](#).

[9] Technical introduction to DLC’s available here: <https://github.com/discreetlogcontracts/dlcspecs/blob/master/Introduction.md>

[10] n.b. For brevity, some details are omitted here; for a more exhaustive explanation, refer to articles from Suredbits (available here: <https://suredbits.com/discreet-log-contracts-part-1-what-is-a-discreet-log-contract/>) and Théo Pantamis (available here: <https://blog.lnmarkets.com/cryptography-of-dlcs/>)

[11] For variations, we might agree on uneven odds, like a 3-to-1 victory, achieved by structuring CETs reflecting such payouts

[12] Practically speaking DLCs are not trustless, as contract enforcement still depends on the oracle, but it is possible to choose multiple oracles during the setup phase so that payout can be claimed even if one or multiple oracles are not cooperative or fail to attest. Besides, during the setup phase, parties also exchange pre-signed refund transactions with a timelock thereby enabling parties to get their funds back if all oracles fail to attest.

[13] Again a trade-off exists. If they concur, the two parties could “renew” their current DLC, thus allowing the “winning party” to withdraw some excess collateral, and/or the “losing party” to post more collateral. It can help a lot with position rolling, but diminishes the hedging surface: with such arrangements, some tail risks re-emerge.

[14] Technical explanation available here: <https://suredbits.com/transferring-in-channel-lightning-dlcs/>

[15] See here for more information: <https://10101.finance/blog/dlc-to-lightning-part-1/>

[16] The Road To Financial Repression, Théo Mogenet, available: <https://theomogenet.substack.com/p/the-road-to-financial-repression-fe9>