Figure 9 - Bitcoin price vs open interest. souce: 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.