AnyHedge: A Decentralized Hedge Solution against Arbitrary Assets on Bitcoin Cash

imaginary_username (im_uname#102)

John Nieri (emergent_reasons#100)

Jonathan Silverblood (Jonathan#100)

Special reviewer AwV2AmxlAwLtZmLX

Correspondence: anyhedge@generalprotocols.com

Abstract

We present AnyHedge, a Bitcoin Cash futures contract that aims to mitigate volatility through trading of risk in a peer-to-peer, non-custodial, blockchain enforced, fully collateralized way. With trust reduced to a blind oracle, the futures contract offers a unique set of advantages and disadvantages over existing stability solutions. AnyHedge is transactional in nature and does not require a central point of failure. The user experience is different from traditional fiat or stablecoin based solutions. As liquidity increases, it enables a variety of automated, behind-the-scenes use cases aimed at taming volatility. Compared to alternative solutions, AnyHedge has a unique set of difficulties and respective mitigations.

Contents

1. Introduction
2. Problem description
3. Existing solutions
4. A decentralized stability solution based on peer-to-peer risk trading
5. Regarding price orientation
6. High level execution of AnyHedge
    - A) Intent
    - B) Contract parameters
    - C) Funding
    - D-1) Redemption under Maturity conditions
    - D-2) Redemption under liquidation conditions
    - D-3) Mutual redemption
7. Liquidity
8. Incentives
9. User experience
10. Comparison with other solutions
11. Impact on Bitcoin Cash ecosystem
12. Attack scenarios
13. Chain reorgs and splits
14. Centralization pressure

15. Different setups
16. Conclusion
17. Supplement A: Detailed example execution of AnyHedge on Bitcoin Cash

1. Introduction

Ten years since the creation of Bitcoin, thousands of cryptocurrencies of various network sizes have emerged offering a wide variety of functions, properties, and trade-offs. By removing middlemen, offering alternatives to unsatisfying monetary policies, and protecting against financial censorship, Bitcoin and its derivatives have achieved some success as currencies.

While usage across the cryptocurrency ecosystem has grown through market cycles, volatility still hampers widespread use and adoption. To have utility, a floating currency, whether sovereign-backed or market-based, must allow users to hold it for a reasonable period of time without fear of losing purchasing power. The current reality however, is that the value of any given cryptocurrency routinely moves more than 10% in a single day due to poor liquidity, speculation, and the relatively small size of the cryptocurrency market. Some people think that a critical mass of adoption will naturally solve this problem, but that critical mass remains elusive for all cryptocurrencies.

In this paper, we describe AnyHedge, a Bitcoin Cash collateral based solution to the volatility problem that does not require any system-wide central points of failure, has limited exposure to potential programming flaws, is difficult to censor, and does not require system-wide coordination to function. All parties involved in the system do not have to send, receive or hold any external asset at any point, and are only dependent on price oracles which they can freely choose.

2. Problem description

Many cryptocurrencies, including Bitcoin Cash, aim to be a medium of exchange. A desirable medium of exchange must at a minimum have the following traits independent of its network effects:

1. The medium must be able to transfer value with less friction than other assets for a given use case.
2. The medium must inspire confidence that it will hold value over a reasonable amount of time, such that transacting parties find it desirable to use and hold it for speculation-free exchange.

Throughout the history of cryptocurrency development, many properties have emerged to address (1) under various scenarios. Privacy, censorship-resistance, low cost of transaction and fast settlement all provide advantages over fiat in this regard. However, cryptocurrencies that solve (1) in various forms typically do not address (2). Compared to competently managed fiat currencies that have a fine tuned inflation target, the value of cryptocurrencies can swing wildly.

As a result, cryptocurrency pricing of goods and services must be updated too often and becomes unreliable for users and merchants. Commerce is further hampered by frequent mismatches of expected future value. A pessimistic merchant can be reluctant to accept the cryptocurrency while an optimistic customer can be reluctant to spend.

Merchants are likely to immediately exchange received cryptocurrencies for more stable assets to avoid speculation. On the spending side, customers may "spend and replace" to compensate for optimistic sentiment. However, these measures effectively negate the low friction advantage of cryptocurrencies.

3. Existing solutions

Several broad categories of solutions to this problem have appeared.

1. Exchange to fiat

Many merchants prefer to exchange the cryptocurrency they receive into fiat currencies. The exchange results in a position that is often more stable than cryptocurrencies, as well as being liquid and familiar. Examples include BitPay, local underwriting as in North Queensland, Australia, and other exchange deposit based solutions.

Fiat exchange suffers from the friction inherent to interfacing with a centrally controlled currency. It is subject to onerous regulations and processing that incur costs similar to traditional payment gateways, erode censorship-resistance and eliminate the inherent efficiency of cryptocurrencies.

2. Fiat-backed stablecoins

Fiat-backed stablecoins emerged as a response to fiat exchange issues and attempt to offer the best of both worlds. They are created and sent digitally much like cryptocurrencies. However instead of having their value determined only by the market, they peg their value to fiat currency backing held under custody of a central entity. Holders of stablecoins can, with certain conditions, exchange them for the fiat currency that backs them. Having roots in enterprises that predate modern cryptocurrencies such as Liberty Reserve, there are multiple stablecoins today that have seen various degrees of adoption such as Tether (USDT), USD Coin (USDC), TrueUSD (TUSD) and HonestCoin (USDH).

Fiat-backed stablecoins take advantage of the current regulation landscape where use of fiat-backed instruments tends to be less regulated than direct interfaces with fiat currencies. The creation and redemption of stablecoins incurs as much or more burden as direct fiat exchange, but that complexity is managed by the issuer. The sending and receiving of stablecoins themselves receive less scrutiny, restoring some of the cryptocurrency-like properties. Furthermore, as stablecoins have a stable, liquid and familiar user experience similar to fiat currencies, they are easier to understand, trust and adopt.

Stablecoins do have some inherent limitations. Their value depends on their fiat currency reserve, and that reserve establishes a large custodial risk. The custodian can steal, falsify or otherwise manipulate the reserve and trigger a catastrophic loss of value throughout the stablecoin's ecosystem. The simple presence of such a risk marks a key difference between fiat-backed stablecoins and permissionless cryptocurrencies: they have clear central points of vulnerability and failure.

The regulatory advantage of stablecoins is also fragile and subject to change. Their central issuing authorities can easily be pressured into extending heavy handed scrutiny beyond redemption and creation. We have already seen an incident of direct, protocol-level blacklisting and it is reasonable to expect regulatory pressure for such measures to increase on stablecoin custodians.

3. Crypto-collateralized algorithmic stablecoins

To address the above shortcomings of fiat-backed stablecoins, a relatively recent development is algorithmic stablecoins such as MakerDAO's DAI and Reserve Protocol's RSV. While they differ in exact mechanisms, these algorithmic coins are typically over-collateralized by volatile crypto-assets instead of directly backed by fiat. As a result, they can be programmed to exist purely on a decentralized blockchain. There is no need for a centralized redemption gateway that forms the basis of the entire system. This mitigates the censorship and regulatory risks of fiat-backed stablecoins to a certain extent, while retaining the pleasant user experience of an easy-to-understand token representing fiat value.

Algorithmic stablecoins, however, have two primary risks associated with them. The first is the inherent risk with using volatile, illiquid assets to back "stable" value. As the underlying asset depreciates, the entire system will need to be downsized in a controlled manner. A catastrophic market downturn may result in systemic problems, such as Global Settlement in DAI, that lead to political intervention or other unexpected edge cases. This risk does not exist in fiat-backed stablecoins with a proper reserve where they simply draw down toward zero when demand falls.

Unintuitively, another risk of algorithmic stablecoins is centralization of control. Due to the need to adjust collateral policies over time, algorithmic stablecoins typically have a second layer of governance tokens, as seen in MKR of MakerDAO and RSR of the Reserve protocol. Necessity of these governance tokens reintroduces the risk of centralized capture and control. In the worst case, poorly designed incentives can lead to apathetic holders of the governance coin, and vulnerability to sabotage by a minority of stakeholders.

Finally, all software has the potential for bugs and vulnerabilities. Any bug or vulnerability in the complex central smart contracts that control algorithmic stablecoins will have a systemic, potentially existential impact.

4. Derivatives

There is a fourth type of volatility mitigation that is not directly tied to fiat currencies or fiat-backed currencies. Many major cryptocurrency exchanges, even those without a fiat interface, have markets for fiat-denominated futures. These markets match bearish actors who seek stability with bullish actors who seek additional risk-taking, and use a variety of derivatives to satisfy both sides on a contractual basis. The derivatives may include futures, forwards, options, leveraged longs and shorts, lending and borrowing among others. They are available on a wide variety of well-known platforms, ranging from purely fiat-denominated exchanges such as Chicago Mercantile Exchange (CME), to custodial cryptocurrency-only exchanges such as BitMEX, to fiat-crypto spot markets such as Binance, Bitfinex and Huobi.

While derivatives generally have custodians that can and have abused trust, they are typically transactional and are not exposed to the same systemic risks. That transactional nature also introduces unique strengths and weaknesses compared to other stability solutions. They have more flexibility in configuration at contract creation that is only limited by the availability of counterparties. That flexibility can also work against derivatives where a variety of parameter sets reduces fungibility and divides derivatives into smaller pools of liquidity, leading to a generally worse user experience than stablecoins. The custodial nature of derivatives also exposes users to the well known custodial risks of censorability and central points of failure.

4. A decentralized stability solution based on peer-to-peer risk trading

Observing the shortcomings of each approach above, we propose AnyHedge, a novel, transactional, collateral-based solution that has no systemic dependencies or single points of failure.

An AnyHedge contract involves at the minimum three parties: Hedge, Short, and Oracle. Only Hedge and Short have coins involved while Oracle does not need to be aware of the contract at all. It operates much like a subset of traditional futures and forward contracts.

- Hedge is an entity who seeks to secure future value against an external asset such as the US Dollar, using coins of a native cryptocurrency such as Bitcoin Cash.
- Short is a counterparty who seeks to take volatility risk of an external asset, betting that the external asset will fall in value against the coins they provide for collateral. In 5. Regarding price orientation we describe the orientation of prices, Bitcoin Cash per external asset, that make this counterparty short on the external asset as opposed to long on Bitcoin Cash.
- Oracle is an entity who provides cryptographically signed price messages for the external asset.

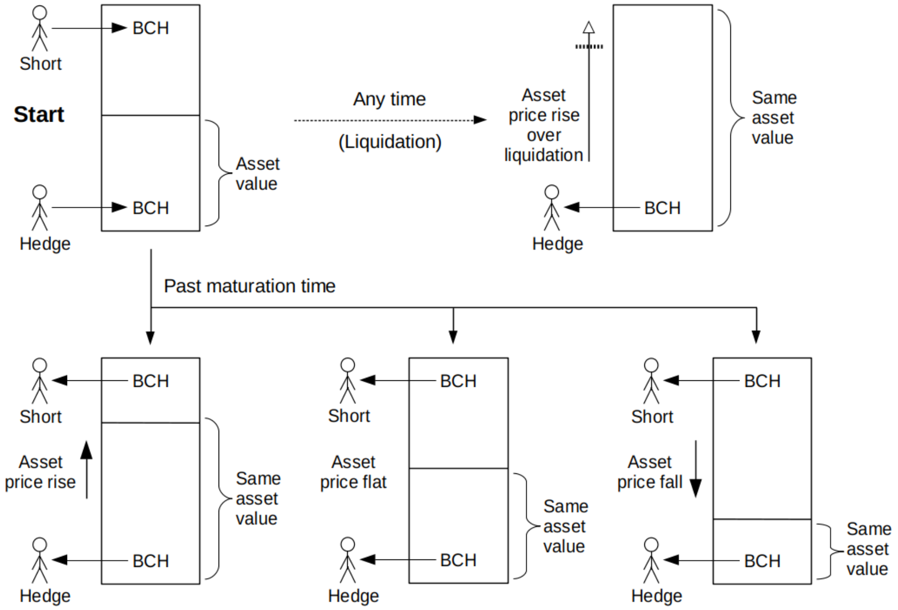
Hedge and Short agree on a few simple parameters that define the main behavior of the contract.

- Maturity is the time after which the contract can be redeemed under normal conditions.
- Fixed Value is the amount of external asset that Hedge would like to protect against volatility.
- Volatility Pool is the collateral provided by Short to protect Hedge's Fixed Value.

The contract uses signed messages from Oracle to determine the price of the external asset.

Hedge enters the contract with an amount of coins equal to Fixed Value, and exits the contract at Maturity with coins equal to Fixed Value. Short enters the contract with coins for Volatility Pool. As the price of the external asset fluctuates, so does the size of Short's Volatility Pool in order to maintain Hedge's exit at Fixed Value. If the price of the external asset falls relative to the cryptocurrency, Short's Volatility Pool grows due to the contract requiring less coins to cover Hedge's exit at Fixed Value. If the price of the external asset rises, Short's Volatility Pool shrinks. In essence, Hedge gains a peg on the external asset for their coins, while Short amplifies the risk and reward for theirs.

Before Maturity, if the price of the external asset rises to a threshold where all of Short's Volatility Pool is required to cover Hedge's exit at Fixed Value, the contract enters liquidation. In liquidation, Hedge immediately receives coins worth Fixed Value. Given enough liquidity, Hedge can immediately enter a new contract to minimize or eliminate slippage.



AnyHedge contracts have the following properties:

1. Each transaction is self-contained. Parameters and circumstances within a contract do not affect any other contracts.
2. Oracle does not need to be aware of any transactions, its sole task is to provide accurate price information.
3. Given access to an Oracle, Hedge and Short can permissionlessly enter a contract independent of any other coordination mechanism or parties.
4. Exact parameters of the contract, including incentives and even pegged asset type, remain private until redemption.
5. At no point do claims to funds leave Hedge and Short. No custodian is involved.

The contracts can be constructed with a wide variety of configurations. Amount of Fixed Value, size of Volatility Pool which determines liquidation risk, Maturity, premiums paid from Hedge to Short or vice versa, and fixed fees to arbitrary parties are all configurable.

5. Regarding price orientation

We expect AnyHedge to debut with USD as the external asset. It may seem counterintuitive that the risk-taking party is a Short betting on the fall of "USD price", i.e. amount of Bitcoin Cash (BCH) per USD. In popular usage, the price is usually shown as the reverse, and this party can be described instead as a Long betting on the rise of "BCH price", i.e. USD per BCH. This inversion from popular convention is necessary due to the nature of AnyHedge, where the external asset can be anything and not limited to popular fiat currencies. As all contracts are ultimately settled in BCH, pricing all external assets in BCH is the more consistent approach, and is used throughout this paper.

6. High level execution of AnyHedge

Bitcoin Cash has all the properties needed to satisfy the requirements of AnyHedge.

- UTXO (Unspent Transaction Output) design reduces systemic risk common to other solutions
- P2SH (Pay to Script Hash) significantly increases privacy and security of contracts
- CDSV (Check Data Sig Verify) allows AnyHedge to work with Oracle data and enforce contract rules
- Other OpCodes necessary for timing and value calculations such as OP_CAT, OP_OR, OP_DIV, OP_MOD, OP_SPLIT, OP_NUM2BIN, and OP_BIN2NUM.

We also document 17. Supplement A detailed example execution of AnyHedge on Bitcoin Cash.

Here we describe a high level execution of AnyHedge in four steps with the US Dollar (USD) as the external asset.

A) Intent

B) Contract parameters

C) Funding

D) Redemption

A) Intent

The intent of the contract can be described with a few settings.

- `hedge_value` Fixed Value that Hedge wants to preserve until Maturity.
- `start_price_bch_per_unit` The start price for the contract.
- `largest_allowed_price_rise` A percentage specifying how far the external asset price can rise from the start price before liquidation. This determines the size of the Volatility Pool collateral that Short must provide. When the allowed rise is small, Short provides less BCH than Hedge, the impact of price changes is amplified for Short, and the contract has less resistance to volatility. When the allowed rise increases to 100%, Short and Hedge provide the same amount of BCH, the impact of price changes

becomes comparable for both, and the contract has more resistance to volatility. When the allowed rise is larger than 100%, Short provides more BCH than Hedge, the impact of price changes is reduced for Short, and the contract has strong resistance to volatility.

- `maturity_date` The contract can be redeemed on or after this date.
- `trusted_price_oracle` Hedge and Short must identify an oracle that they trust to provide reliable price data.

Hedge and Short agree on the following intent.

```
hedge_value =                10.00 USD
start_price_bch_per_unit =   0.0045 BCH per USD; (222.22 USD per BCH)
largest_allowed_price_rise = 33%
maturity_date =              +1 week from today
trusted_price_oracle =       For example, a well established exchange
redemption_addresses =
  Addresses provided by Hedge and Short to receive funds at redemption
```

B) Contract parameters

More detailed contract parameters are derived from the intent.

- `liquidation_price_high_bch_per_unit` When the external asset price increases, this is the earliest price that triggers liquidation.
- `liquidation_price_low_bch_per_unit` When the external asset price decreases, this is the earliest price that triggers liquidation. At the extreme, a price decrease consumes Hedge's BCH until 1 satoshi covers the entire hedge value. Any value above zero can be selected. However here we use a fixed large decrease (90%) that effectively avoids liquidation due to price decreases, but also ensures that liquidation will work in such an extreme case.
- `total_satoshis` This is the combined pool of BCH that the contract splits between Hedge and Short when the contract is redeemed. The size of the pool is calculated so that there is enough BCH to cover Hedge's value at the highest allowed price.

Hedge and Short calculate and agree on the following contract parameters.

```
liquidation_price_high_bch_per_unit
  = start_price_bch_per_unit * (1 + largest_allowed_price_rise)
  = 0.005985 BCH per USD; (167.08 USD per BCH)
liquidation_price_low_bch_per_unit
  = start_price_bch_per_unit * (1 - 0.90); i.e. static 90% price drop
  = 0.00045 BCH per USD; (2,222.22 USD per BCH)
total_satoshis
  = hedge_value * 1e8 sats_per_bch * liquidation_price_high_bch_per_unit
  = 5,985,000 satoshis
```

C) Funding

Hedge and Short pay into the AnyHedge contract as follows.

```
hedge_satoshis_in
  = hedge_value * 1e8 sats_per_bch * start_price_bch_per_unit
  = 4,500,000 satoshis;
    (equivalent to hedge_value of 10.00 USD at start of contract)
short_satoshis_in
  = total_satoshis - hedge_satoshis_in
  = 1,485,000 satoshis; (equivalent to 3.30 USD at start of contract)
```

Due to bearish market conditions for USD relative to BCH at the time of contract creation, Short also agrees to pay a premium to Hedge as part of the funding transaction.

D-1) Redemption under Maturity conditions

After funding the contract, there are 3 different types of redemption that Hedge and Short can do. First we describe redemption at Maturity, the standard outcome.

After 1 week, the contract reaches Maturity and can be redeemed. `trusted_price_oracle` provides a signed message with a price and time stamp, and the contract verifies that the signature is valid. In order to ensure a valid calculation of payout for Hedge's Fixed Value, the contract creates a new value `end_price_bch_per_usd` which is clamped within the allowed boundaries of `liquidation_price_low_bch_per_unit` and `liquidation_price_high_bch_per_unit`. The price in the message is `0.004 BCH per USD; (250.00 USD per BCH)` and is already within the allowed boundaries. Therefore `end_price_bch_per_usd` is equal to the message price.

In order to ensure that the contract is redeemed with the price at Maturity, the contract verifies that the time stamp in the message is for the maturity date.

The contract performs payout calculations as follows.

```
end_price_bch_per_usd = 0.004 BCH per USD; (250.00 USD per BCH)
hedge_satoshis_out
  = hedge_value * 1e8 satoshis_per_BCH * end_price_bch_per_usd
  = 4,000,000 satoshis;
    (equivalent to 10.00 USD, the original hedge_value)
short_satoshis_out
  = total_satoshis - hedge_satoshis_out
  = 1,985,000 satoshis; (equivalent to 4.96 USD)
```

The contract then sends `hedge_satoshis_out` and `short_satoshis_out` to the respective addresses in `redemption_addresses`. Hedge receives BCH worth exactly their original hedge_value in USD and Short receives more BCH than their original collateral due to the decrease in price of USD during the contract period.

D-2) Redemption under liquidation conditions

Another possible outcome after funding is liquidation. In this case, there is unexpectedly high price volatility that consumes Short's Volatility Pool collateral.

After 4 days, before the contract reaches Maturity, `trusted_price_oracle` provides a signed message and the contract validates it as above. Also as above, the contract creates a new value `end_price_bch_per_usd` and clamps it within the allowed price range. The price in the message is `0.006024 BCH per USD; (166.00 USD per BCH)` which is slightly higher than the boundary, `liquidation_price_high_bch_per_unit`. Therefore `end_price_bch_per_usd` is clamped to the boundary price, and liquidation becomes possible because the end price is at the boundary. In order to ensure that the contract is redeemed with a price that occurred before Maturity, the contract verifies that the time stamp in the message is after creation date and before the maturity date.

The contract performs payout calculations as follows.

```
end_price_bch_per_usd = 0.005985 BCH per USD; (167.08 USD per BCH)
hedge_satoshis_out
  = hedge_value * 1e8 satoshis_per_BCH * end_price_bch_per_usd
  = 5,985,000 satoshis;
    (equivalent to 10.00 USD, the original hedge_value)
short_satoshis_out
  = total_satoshis - hedge_satoshis_out
  = 0 satoshis;
    (all satoshis used to satisfy hedge_value at this extreme price)
```

D-3) Mutual redemption

The last redemption available to AnyHedge is a failsafe mechanism. Hedge and Short can pay out all funds in the contract in any way they want as long as they both agree.

After 2 days, Hedge would like to exit the contract early and agrees on a split and a fee with Short. In a single trustless transaction, they submit their signatures, split `payout_satoshis`, and Hedge pays the agreed fee to Short.

7. Liquidity

To be useful as a stability solution, AnyHedge must meet the needs of all contract parties. Especially, takers with high time preference must be able to fill their desired volume of contracts within a short time and with predictable premiums. Fulfilling these needs requires a large amount of liquidity which we describe as easily accessible market makers competing at all times on both Hedge and Short sides. In this section, we explore different setups in matchmaking, their impacts on liquidity, and the trade-offs they incur.

1. Centralized

While AnyHedge is decentralized in nature, it still requires that Hedges and Shorts find each other efficiently. Decentralized exchanges are an excellent fit for AnyHedge but they face a difficult problem: centralized exchanges currently provide the most responsive and scalable matchmaking, and by extension attract the most liquidity with the lowest spread. For this reason, we foresee that AnyHedge will first be deployed on centralized exchanges, with centrally controlled and permissioned order books combined with a non-custodial client-side wallet. This setup preserves all advantages of AnyHedge, including no custodial risk, except that the exchange is aware of the details of the contract.

The order book is an important point of failure in the stability mechanism and therefore centralized control over it is a risk. However, just as liquidity is scattered across many centralized exchanges today, as AnyHedge adoption grows the market will become more resilient to censorship and failure of any single exchange.

2. Federated

Using the non-custodial nature of AnyHedge, exchanges can open up an API for their maker orders, allowing them to trustlessly coordinate AnyHedge contracts with external takers while guaranteeing their own fees. This offers a good balance for the implementing exchanges. As the liquidity pool deepens, more volume is attracted and both exchanges can benefit. Liquidity sharing is traditionally achieved by arbitrage but that may be difficult here because the contracts are less fungible than typical asset pairs. Exchanges can negotiate among themselves how they intend to divide the fees and they can refuse connection to unauthorized or uncooperative peers. Over time, multilateral cooperation can evolve into a de facto federation with users getting the benefits of a wide view of liquidity, a measure of robustness against censorship and an unfragmented, highly liquid order book. We envision that the global and trustless pool of demand will in fact attract a new class of second layer services such as point of sale systems and peer-to-peer banking, growing the whole market for participating exchanges.

3. On-chain

AnyHedge is not fundamentally reliant on exchanges. Any two willing parties who have access to an oracle can enter a contract. However in practice, liquidity discovery and efficient matchmaking immediately becomes a problem without a centralized book. We envision that just as OTC trading desks exist elsewhere, tools will be released for ad-hoc contracts independent of any exchange. Where they suffer in liquidity and trading speed, they make up by enjoying high degrees of privacy, independence from a permissioned order book, and greater flexibility to choose or even provide their own oracles.

Bitcoin Cash covenant-based funding contracts can also be created to facilitate such independent trading. An on-chain maker can fund a P2SH output that establishes all contract parameters except for the counterparty's payment details. A counterparty who agrees with the terms can complete the funding and redeem the funding contract into a complete AnyHedge contract. The presence of these funding contracts on the blockchain will act as a censorship resistant, trustless, permissionless order book with global liquidity. However at least in the medium term, we expect the relatively high friction of fees and race conditions for funding and revocation to lead to less liquidity than centralized and federated options.

8. Incentives

AnyHedge incentivizes participation from Hedge, Short, Oracle and the optional order book facilitator. It is important to recognize these incentives, as described below, when working with or modifying the system.

Hedge is the obvious target audience, and benefits from removal of volatility in a non-custodial and trust-minimizing way. Parties receiving BCH in their activities are the natural users on this side, which includes miners, merchants and services that mainly deal in BCH. Initially, we expect them to be willing to pay a premium up to but not more than exchange fees to fiat or transferable stablecoins over the time they expect to remain in crypto. As the benefits of non-custodial setups become more widely understood, they may be willing to pay more. Such fees can can range from 0.3% at Binance to 7% at LocalBitcoins, depending on desire for availability, censorship-resistance and reliability.

Short absorbs risks from the Hedge to have a chance at amplifying their exposure and increase their upside when the external asset falls in value relative to BCH. This group is typically made up of speculators who expect the external asset to fall in value with respect to BCH, but can also be traders who have long exposure elsewhere in the market. We expect them to be willing to pay a premium that is competitive against lending rates for leveraged shorts elsewhere. For example, USDT, an asset typically borrowed for similar purposes, has a lending rate on Coinex generally at 12-15% APR (Annual Percentage Rate).

It is worth noting that the market premium may go to either Hedge or Short depending on relative demand at any given time.

In addition to the two primary parties, at least one reliable Oracle must be present. In order to avoid legal complications and disputes related to collusion, we expect oracles to actively avoid knowledge of contract details. Emitting accurate, reliable and independent messages will maximize the value and demand for a given oracle. Initially, we expect Oracle to be a free service provided by existing players such as exchanges. As volume grows and more reliable guarantees are desired to facilitate important trades, oracles may begin to charge fees for their signed messages through regular contracts with exchanges, or per-contract fees paid in a non-custodial way. Although we expect that oracles will generally publish messages publicly on the blockchain to increase user confidence, oracles can easily delay public broadcasts and provide paid access to a timely message feed. Oracle providers may also derive income from additional services, such as automatic redemption and liquidation of AnyHedge contracts.

Finally, as described in the previous section, exchanges are critical as facilitators of high liquidity with their managed order books. Unlike most other assets, AnyHedge contracts free the exchanges from custodial risk and therefore lower their operating costs to the price of implementation and maintenance of non-custodial interfaces. The uniqueness and utility of AnyHedge itself can also attract volume to an exchange.

9. User experience

We expect to first deploy AnyHedge in a centralized exchange via non-custodial wallets and then expand to other exchanges that will ideally be federated. As liquidity builds up, non-exchange products such as merchant solutions can be built on top of and contribute to the overall liquidity. Highly privacy aware users or those needing censorship resistance may start using decentralized order books.

Deployment with custodial wallets is possible, but it is unlikely to gain widespread adoption. A custodial AnyHedge wallet acquires the censorability and custodial risk of existing custodial futures products, while maintaining an onchain footprint. This makes such a setup unlikely to be competitive with existing solutions. It is possible some forms of custodial solution may offer better user experience and gain adoption, but we do not expect them to be dominant.

A typical setup will likely start with a non-custodial client-side wallet either implemented as a script embedded in a web page, or a dedicated program the client runs outside the browser. If a dedicated client is developed, it can either be standalone, or integrate into an existing extensible wallet such as Electron-Cash.

In its most basic form, funding an AnyHedge contract requires both parties to be online for interaction. For market makers, this means they will need to stay online to find takers, a reasonable requirement considering their general need to adjust to changing market conditions.

To maximize liquidity and ensure good user experience, we expect AnyHedge order books to settle around a small number of fixed parameters such as duration, allowed price change before liquidation, and hedge amounts. Market makers can compete by offering different premiums on both the Hedge and Short side. Common parameters are even more valuable in the context of federated liquidity and a future secondary market of transferable AnyHedge contracts.

On the taker side, we expect speculators to use the full order book for optimal efficiency. For application-specific uses of AnyHedge we expect that more convenient user interfaces will be available that expose an underlying ask book through fixed premiums, similar to popular swap services. Both trading and application-specific interfaces should be possible regardless of whether the liquidity comes from centralized exchanges or a federated liquidity pool.

On the other end of the user spectrum, ad-hoc contracts with arbitrary parameters are possible for sophisticated users with specialized needs. Construction of these contracts is similar to existing multi-signature transactions where one party specifies parameters, constructs a transaction, and passes it to the other party to be fully signed and broadcasted.

When sufficient liquidity is available, merchant solutions can offer automated hedging in arbitrary units for received Bitcoin Cash. Providers of automated solutions may even enter long term contracts with liquidity providers independent of existing order books to offer predictable, stable premiums.

Another way to package AnyHedge contracts is as a fixed deposit account. Savers may enter longer term hedging contracts, with services that assist with renewal at maturity or liquidation. These arrangements are strongly linked to real market conditions where savers will earn or pay a premium depending on supply and demand.

10. Comparison with other solutions

1. Fiat-backed stablecoin

AnyHedge compares favorably to fiat-backed stablecoins in custodial risk: there is no large reserve of funds under third-party custody that can be embezzled. It also has advantage in censorship-resistance, as contracts can be formed ad-hoc on-chain, avoiding censorable creation and redemption interfaces. It is notable that incentives for malice in a centralized stablecoin grows with the value under custody, which is not a concern for AnyHedge due to its transactional nature.

The disadvantage of AnyHedge lies in user experience. Fiat-backed stablecoins offer a mostly fungible, currency-like experience, while AnyHedge necessarily requires coordination with a second party. The need for coordination can be mitigated with automated one-click interfaces and transferable contracts that mimic traditional bond markets as described below. We expect mostly businesses and sophisticated users to adopt AnyHedge, some of which may use it as a foundation to create user-friendly products and services.

2. Crypto-collateralized algorithmic stablecoin

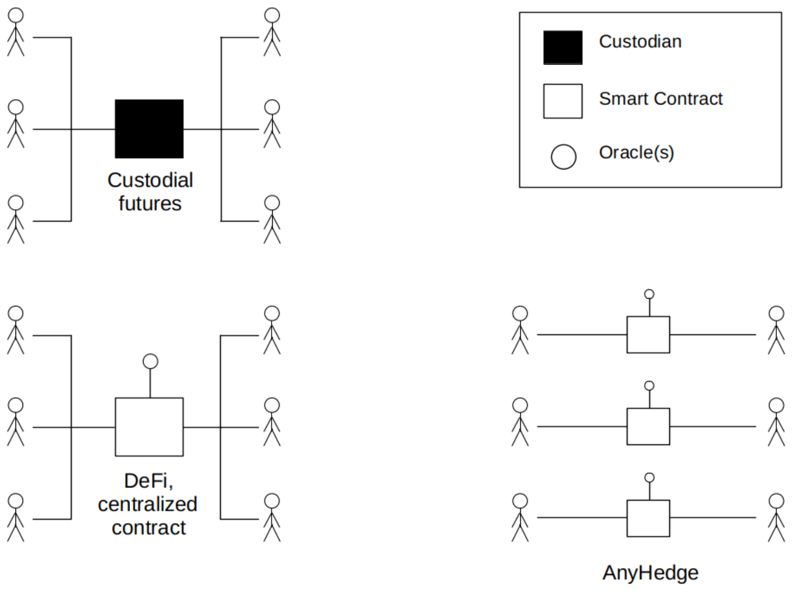
While there may seem to be no explicit custodial risk associated with algorithmic stablecoins, governance and systemic risks remain. AnyHedge compares favorably in these regards due to its transactional nature: there is no central party whose compromise would affect the whole market. Similar to the case of fiat-backed stablecoins, incentives for malice also grow with size at central points of failure such as governance bodies and unified oracles. Even in the case of AnyHedge code vulnerabilities, upgrades can be seamlessly deployed for new contracts. Old contracts are also protected to a limited degree by the use of P2SH. As the exact script and parameters are not revealed during creation of the contract, a third party attacker cannot compromise funds until the script is revealed by redemption. This is described in more detail in “Attack scenarios” below.

AnyHedge faces a similar user experience disadvantage as it does with fiat-based stablecoins. It also has the same potential to displace and create new value on the back-end.

3. Custodial derivatives

In a sense, custodial derivatives can be seen as the direct competitors of AnyHedge. The user experience is similar and so is the nature of hedging. However, while mitigations exist, custodial derivative solutions face counterparty risks that have proven time and again to be quite vulnerable, especially in the face of large market swings. AnyHedge, on the other hand, is not subject to the same risks of contracts failing to be honored. The collateral is already in place at inception and in the worst case, the contract can be easily liquidated before there is slippage. This is on top of the difference in censorability and custodial risk of funds, which custodial exchanges are inherently exposed to.

On the other hand, we expect custodial derivatives to still have an edge in matchmaking speed and liquidity. They also offer a much wider variety of products until additional non-custodial products are developed, some of which are listed below under “Different setups”.



11. Impact on Bitcoin Cash ecosystem

We expect AnyHedge over time to build liquidity, volume and adoption, and become a significant part of the BitcoinCash ecosystem. Once sufficient volume is achieved, we expect it to have the following effects:

1. Merchant adoption

AnyHedge allows merchants to seek stability at low cost or even profit, while simultaneously retaining all the benefits of Bitcoin Cash. Wider adoption by merchants will strengthen the permissionless nature of the ecosystem.

2. Mitigating custodial risk for speculation

Currently the dominant use case for cryptocurrencies is speculation. In particular, leveraged speculation with cryptocurrencies, as seen at BitMEX, is very popular with millions of dollars of volume each day looking to take on additional risk. These speculators are currently exposed to censorship and custodial risk where the exchanges may freeze or confiscate their funds. Furthermore the custodians are typically exposed to counterparty risks and costs such as insurance for leveraged defaults during unexpectedly large volatility. AnyHedge provides an alternative, non-custodial and trustless way for speculators to increase their exposure to volatility.

3. Increased demand and utility for Bitcoin Cash

In addition to simple upward price pressure, we expect widespread use of Bitcoin Cash-denominated AnyHedge contracts to increase demand for Bitcoin Cash as collateral, directly impacting long term viability as peer-to-peer electronic cash. Note that this is contrary to fiat-denominated derivatives, which drain demand from cryptocurrencies. This effect should be especially apparent in contracts hedging against other speculative assets such as precious metals and alternative cryptocurrencies, where Bitcoin Cash absorbs speculative demand from their overall spot markets.

12. Attack scenarios

Aside from vulnerabilities inherent to any cryptocurrency use cases such as loss of private keys, implementations of AnyHedge should minimize user exposure to the following vulnerabilities.

1. Oracle compromise

An adversary can compromise an oracle and then provide false pricing data or emit messages with bad timing, thus influencing contracts to their benefit. This can cause damage in unfair contract maturation, premature liquidations or prevention of just liquidations. To discourage these attacks, oracle providers should be properly incentivized, kept as unaware of contract details as possible, and regularly checked for consistency. To minimize the impact of these attacks, AnyHedge contracts may make use of multiple oracles.

2. Oracle dispute

A faulty oracle can emit ambiguous data that invites dispute from contract parties. For example, an oracle may sign two messages for the same time period or have a delay in message emission. In addition to the mitigation in the oracle compromise scenario, we also expect that over time a diverse market of oracles will form, with the most reputable providers becoming more widely used.

3. Time resolution

The messages oracles emit may not be of sufficient time resolution to cover all possible liquidation needs. There is a trade-off between higher time resolution and vulnerability to temporary price irregularities. In general, as the liquidity of Bitcoin Cash and the external asset increase, the time resolution of oracles can also be increased with confidence.

4. Market manipulation

Similar to derivatives in custodial exchanges, parties with ample capital can manipulate market conditions and create sharp prices changes, which in turn trigger liquidations. Custodial exchanges may even be considered less vulnerable due to their ability to apply human judgement and roll back trades. This is an inherent weakness to automated non-custodial solutions and parties should pick an oracle that robustly aggregates price information to minimize this vector.

5. Untimely redemption

If there is an oracle message that allows a liquidation, then the contract can be liquidated. However if the liquidation is not carried out in a timely manner, then the contract may enter maturity. Then liquidation and maturity both become valid and the maturity transaction may preempt the liquidation.

Generally, any delay in liquidation or maturity redemption may lead to slippage. To ensure this scenario is minimized, AnyHedge parties should employ automated services that watch oracle price feeds and execute redemptions for them.

6. Contract construction

An inadequately or maliciously built client can fail to do necessary verifications when constructing AnyHedge contracts, opening up the possibility of one party cheating the other in parameters or even outright theft. Users should be careful in selecting reputable clients whether provided by an exchange or a standalone outfit.

7. Fee market

At all stages of its existence, funding, liquidation and maturation, an AnyHedge contract is vulnerable to hostile fee market conditions. A transaction can fail to pay sufficient fees given chain congestion, opening it to delays and race conditions. AnyHedge benefits from being built on Bitcoin Cash, where fees are expected to be highly predictable over time.

8. Software vulnerabilities

Both the constructing software and smart contract script itself may contain unexpected vulnerabilities that allow for parameter manipulation or even outright theft. In solutions with a central contract, as commonly found on Ethereum, such a vulnerability can be existential and either result in catastrophic failures, as seen in the DAO, or require widespread, disruptive and difficult to coordinate migrations. AnyHedge benefits from its transactional nature in this regard, and is further protected by being hidden behind P2SH until redemption. If a vulnerability is discovered, an upgraded version can be deployed smoothly for all new constructions with minimal disruptions, as there is no central contract to be migrated from. For existing contracts, they are only immediately vulnerable to parties with complete knowledge of their contract parameters. We expect those knowledgeable parties to be highly limited such as the participating parties themselves, any involved exchange, and any automation services they may employ. In the case of a known vulnerability, the redeemers can ensure safety, even when they must reveal the script, by sending their redemption transaction directly to a trusted miner or group of miners with the understanding of block inclusion without rebroadcast.

13. Chain reorgs and splits

Building a contract on a permissionless blockchain carries the inherent risk of being exposed to irregularities of the underlying chain. In the case of Bitcoin Cash, this manifests primarily as chain reorganizations and splits. Reorganizations can either occur naturally due to propagation latencies, or as a result of malicious hash-power-based attacks. A split in this context refers to deliberate extensions of alternative tips which subsequently gain their own value.

As an external source of data, block-height-based oracles should remain deterministic in the event of reorgs and splits. In other words, oracles must not sign different data for the same timestamp or block height, as long as they keep the headers of corresponding blocks as proof. As block emission is used only as a proxy to time, there is no special requirement to adhere specifically to a block that wins an orphan race. On the other hand, signing two messages for the same height with different price data creates race conditions and opens contracts to potential disputes. An oracle that double-signs should be considered compromised, and discouraged from further use.

Assuming the oracle maintains a trustworthy feed, contract maturation should be mostly unaffected by reorganizations. In some cases, there will be the inconvenience of rebroadcasting maturation transactions if they are excluded in the reorganized chain and mempool. More worthy of attention is the case of liquidation. A liquidation transaction, especially when close to maturity, can be removed via reorganization and enter a race condition against a maturation transaction. For a typical reorganization to impact a contract, the remaining time must be very small and therefore the price difference will be small with limited impact on the outcome. This race condition and liquidations in general can be minimized by using a reasonable amount of collateral.

In extreme cases of deliberate attack, a high-value liquidation can even be evaded in the hopes of a price recovery by colluding with large miners. We do not expect such attacks to be a large concern because they are subject to the same disincentives against large scale double-spend based attacks. That is, the Bitcoin Cash price drop consequent from such an obvious attack makes it unlikely for invested ASIC miners to collude.

In the case of an economically significant and persistent chain split, the oracle must decide which chain its prices will be based on. Since the contract exists on both chains after the split, its redemptions will also be replayable on both chains. On the unsupported chain, redemptions will likely result in inaccurate outcomes based on prices for the supported chain. On the supported chain, redemptions can be expected to result in a relative gain for Hedges given the typically lower price on both chains after a significant split. If AnyHedge is widely adopted, complications in contract redemption may provide a disincentive against deliberate chain splits. Alternatively, concerns of a persistent split may dampen demand for AnyHedge over the period of uncertainty.

It may be possible for the oracle to adopt a dual chain model where it aggregates prices from both chains in its feed. However, this is likely to lead to even more complicated situations, as users face the uncertainties of redeeming on both chains. Additionally, new and unreplayable contracts would be unable to continue using the feed. It may be more reasonable for the oracle to simply pick a chain to support, so that complications will be limited to contracts that cross the split.

14. Centralization pressure

The design of AnyHedge does not involve a central, systemic point of failure, and can be executed by any combination of Hedge, Short and Oracle. Centralization pressure will exist on various parts of AnyHedge and we expect it to ease as adoption and diversity rises, as described below. Failure of the ecosystem to diversify may result in a system that is more fragile than expected.

1. Oracle Pressure

While an AnyHedge contract is designed to use any oracle the Hedge and Short desire, in practice we expect there to be a limited number of public and reputable oracles. At scale, if the choice of oracles is too limited, failure or compromise of oracles can present a systemic risk to the setup similar to their semi-centralized role in other decentralized finance systems. As adoption of AnyHedge and other oracle utilizing contracts increases, we expect a market for properly incentivized oracles to emerge with diverse business models, easing this pressure.

2. Liquidity pressure

AnyHedge contracts can be constructed ad-hoc between any two willing parties. However, finding a willing counterparty at a desired set of parameters, in a timely fashion, and at a reasonable premium is essential for AnyHedge to have significant utility at scale. If matchmaking activity is concentrated in the hands of few centralized exchanges, they can censor and otherwise impose non-optimal conditions on AnyHedge users.

As AnyHedge is not fundamentally tied to any outlet, we expect that censorship and non-optimal conditions will be countered as liquidity flees either to other exchanges, decentralized setups or ad-hoc bazaars. Federation between exchanges can further discourage these pressures from rising in the first place.

3. Regulatory pressure

Regulatory pressure is a common concern for all cryptocurrency activities including derivatives. Regulatory bodies can attempt to impose reporting and tracking burdens, reducing the number of exchanges that can comply. The non-custodial nature of AnyHedge should afford it an edge over custodial solutions when it comes to regulatory pressure. Assuming liquidity and oracles are sufficiently distributed, there are only limited ways regulatory bodies can censor the system as a whole. Even at exchanges that regulatory bodies apply pressure to, they can censor but not compromise funds.

15. Different setups

1. Transferability

To improve user experience for takers, a market maker can play both sides of the contract in construction. The maker constructs and funds the entire contract which has an additional covenant clause allowing the maker to sell one side of the contract to another party. This setup makes a reasonable trade-off where the maker assumes all initial complexity and a temporary up front cost, while the taker has a greatly simplified experience. Overall it provides a bond-market like interface while remaining non-custodial. It also provides a more convenient and intuitive way to provide liquidity without exchange order books.

2. Renewals

For use as savings accounts or long-term speculation, some Hedges and Shorts may desire to stay in their positions for longer than the contract maturity date. Waiting for maturity to seek the next contract may be deemed a hassle, and present unwanted risks while in between contracts.

The simplest way to stay in a contract is to interact with a willing counterparty to renew terms of the contract via mutual redemption. Note that as long as two signatures are present, they can simply transfer the funds to a new contract address.

Alternatively, renewable contracts may be constructed where either Hedge or Short have the option to extend the maturity date of a contract, with otherwise identical parameters. Renewable contracts would typically have different pricing compared to new contracts.

3. Non-stabilization contracts

While AnyHedge is designed around the need to mitigate volatility, there is no fundamental reason why the contracts cannot be designed to cater to wider speculative needs. For example, instead of providing constant fiat-value output for the Hedge, the script can instead amplify outputs on the downside as well to cater to proper Longs. A wide range of derivative products are possible in this fashion, and will be developed according to market demand.

16. Conclusion

We have described a novel smart contract based derivative that mitigates volatility using the base layer of Bitcoin Cash without exchanging for other assets or tokens. Any given contract fundamentally involves only Hedge, Short and Oracle, and is completely independent from other contracts. AnyHedge can mitigate volatility for any asset as long as the three parties are present, and setups can be upgraded or patched per transaction without central coordination. Exchanges and other services can provide convenience, liquidity and other benefits but are not strictly necessary. AnyHedge takes advantage of the most fundamental qualities of Bitcoin Cash and we expect usage to increase overall utility.

17. Supplement: A detailed example execution of AnyHedge on Bitcoin Cash

Please refer to the document titled, “A detailed example execution of AnyHedge on Bitcoin Cash”.