Hedgehog: from hedging to stability

Kevin Foesenek
support@banq.link
www.hedgehog.financial

Abstract. A protocol that allows decentralized hedging against depreciation of on-chain assets known as tokens. The use of hedging results in underlying assets stabilized for changes in demand of the hedged asset. The underlying asset is stabilized by market forces. This is different from current stable token implementations that mostly rely on oracles combined with an algorithmic stability mechanism to maintain a peg to an existing stable currency. The proposed protocol uses a bonding curve and requires no oracles or additional consensus mechanism such as token-based voting.

1. Introduction

The innovation of blockchains resulted in an increased development of (decentralized) financial applications. This gave rise to applications that are on a spectrum of decentralization. There are applications with code execution that only relies on the security provided by the blockchain and there are applications that are lower on the spectrum, with for example the use of oracles or smart contract ownership patterns, that require a separate consensus mechanism like token-based voting.

A financial application on the blockchain is a stable token. Stable token design mostly pegs a token to the value of an underlying stable asset like the dollar. Currently there are two options to maintain the peg, first centralized parties that hold the underlying asset and issue the token or second on-chain protocols that use separate consensus mechanisms for oracles that are needed to peg to the asset. There is need for a non pegged stabilized token that does not require a separate consensus mechanism.

To stabilize an asset without a separate consensus mechanism we propose the use of a hedging protocol that stabilizes against the changes in demand of the underlying asset itself. The hedging protocol also needs to be without a separate consensus mechanism. For price hedging of assets on the blockchain there currently are two main options within the spectrum of decentralization. First centralized exchanges that allow a shorting position and second on-chain protocols that use separate consensus mechanisms for oracles that allow buying shorting positions. There is need for an option without the use of separate consensus mechanisms.

In this paper we propose a hedging protocol without the need of a separate consensus mechanism. It uses a bonding curve to generate an automated market for asset hedging that can be used to create a token stabilized against the changes in demand of the underlying asset. The token is not pegged, market forces for hedging stabilize the token.

2. Blockchain

Blockchains and in particular code execution combined with a blockchain makes it possible to build new financial applications. The in this paper proposed hedging protocol relies on this method for secure decentralized execution of the code on the Ethereum blockchain [1].

The current Ethereum blockchain uses proof of work to reach consensus on the longest chain that contains the current state after all transactions and corresponding code executions. It can be seen as a single state machine. Use of the Ethereum blockchain is proposed because of the strong security guarantees with the current significant hashing difficulty. Further it has a wide range of assets build based on standards that makes integration efficient. Also the underlying state execution machine named the Ethereum Virtual Machine (EVM) is used in other projects, making potential migration simplified. Finally the Ethereum community is actively researching and building Ethereum 2.0 with which they hope to fix known problems with blockchains like the energy inefficiency because of proof of work. Where the fist step to a different consensus mechanism named proof of stake already is made with the deployment of the beacon chain.

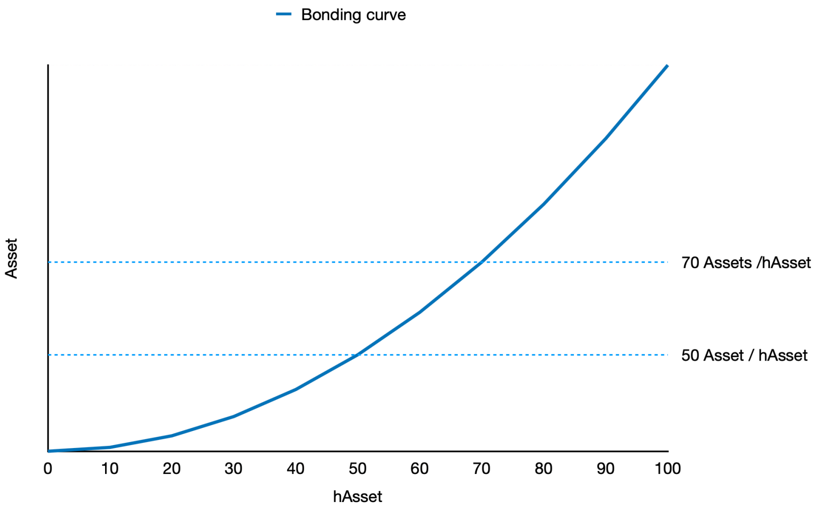
3. Bonding curve

A bonding curve is a mathematical formula used to determine the relationship between price and supply of assets [2]. Combined with code execution on blockchains bonding curves can be used to create autonomous applications with a minimal trust assumption. The automation of the bonding curve eliminates the need to trust separate governance systems.

We propose the use of a quadratic bonding curve for the hedging protocol, where the total tokens minted (*totalhAssets*) determines the amount of total assets (*totalAssets*) in the pool. The more assets in the pool the less tokens minted for new asset deposits.

$$totalAssets = totalhAssets^2$$

We propose a quadratic bonding curve on the premise that markets mostly move exponentially. The premise is based on the market movements of blockchain assets in past years and supported by the widespread use of log graphs to visualize market graphs. We propose a quadratic curve not an exponential curve because it is comparable to an exponential curve with a slightly less steep curve and it requires minimal code to implement, resulting in minimal execution cost for the user of the protocol. Exponential implementations are more expensive to compute.



4. Hedging

Hedging in this paper is regarded as taking a separate financial position that offsets depreciation or appreciation of an assets. In traditional finance hedging can be done with multiple financial products, for example options and futures. In the case of the blockchain the main assets to hedge are tokens. Because the changes in demand of these tokens, mostly measured in the dollar price of an asset, are not available on-chain creating a purely algorithmically hedging protocol is an unsolved problem.

We propose the use of single sided markets, with one asset per market, that simulate a prediction market for changes in demand of the assets. The problem is creating this market whiteout the option to measure the changes in demand on-chain. A quadratic bonding curve that rewards users for timely deposits and punishes users for late withdraws can be used. This creates a prediction market for deposits and withdraws in and out of the pool. When a user expects more assets to be deposited in the pool the user can choose to predict this by deposition early in the pool. Then when the user expects no more deposits and/or withdraws the user withdraws from the pool. If the user predicted the deposit successfully the withdraw will result in more assets than originally deposited. If the user predicted wrongly the withdraw will result in less assets than deposited. The remaining step is connecting predictions of deposit to predictions of changes in demand of an asset.

Narratives are increasingly identified as strong market forces [3]. This is also shown in the price movement of Bitcoin known as the first implementation of a blockchain. If someone owns a bitcoin they own an entry in a decentralized ledger on the Bitcoin blockchain, the narrative of a store of value seems to be the proposition that allows this entry to have value. The value can be seen in the price against traditional finance currency like the dollar. Based on this strong force of a narrative we propose that the pool deposit predictions can be connected to price deprecation simply by narrative. If a sufficient part of the pool follows this narrative it will create market forces following that narrative. In addition the narrative of deprecation with a pool that rewards early deposits is natural. This is because rational investors look for methods to offset (potential) losses. The potential of a reward from timely deposit is a valid method and naturally can be expected to become a method for offsetting losses. Because the hedging narrative follows naturally a sufficient liquid quadratic bonding curve pool can be expected to result in a hedging market.

Further research is needed in solidifying the narrative of price depreciation for the pools. A potential current research subject is additional floor option pools that allow any user to take floor option that will limit the risk that a significant portion of the pool is withdrawn. This would limit the users pool risk, resulting in less pool sell pressure from potential fear of mass withdraw.

5. Asset stability

A algorithmically stable asset is an actively researched topic. The volatility of blockchain assets results in a need for stable blockchain assets. Current on-chain designs use an oracle based solution that use the oracle price to maintain a peg. A well known design is that of makerdao's dai [4] that uses collateral debt positions to mint stable tokens. The collateral debt positions are liquidated if the collateral in it does not cover the dollar value of the stable tokens minted. Based on the historically maintained peg this is a design with strong guarantees. Still it needs additional trust from the separate governance mechanism of the oracle used in the protocol.

We propose a new asset class stabilized directly for changes in demand of the asset in the pool without additional governance systems. This is achieved by creating an asset with inverse movement of the asset by using a hedging market. This asset class is complementary to pegged stable tokens like dai. For example it can be used as collateral. The stability of this new asset class is reliant on the market forces of the hedging market. A basket of these stabilized assets can be made for multiple on-chain assets like ETH.

With sufficient hedging liquidity in the pool the hedged assets value (*AHv*) is less volatile than the underlying asset value (*Av*).

$$AHv < Av$$

If the market is not sufficiently liquid and does not follow the depreciation narrative then the volatility potentially will be greater than the underlying asset. For example in the starting period of low liquidity in the bonding curve it is expected that the volatility is greater because the main reason for deposit in the pool will be expected growth of the pool itself. Since the bonding curve rewards early deposits liquidity will be attracted and increase. It is unknown what liquidity is needed for stability, therefore there is no fixed optimum in the bonding curve. The market is expected to find the needed liquidity based on the demand for hedging in the pools.

6. Implementation

The hedging protocol is implemented in solidity the main programming language used on the Ethereum blockchain. In the implementation only the computation from hedge token amount to underlying asset amount is implemented. This because the square root is a more expensive implementation that can be done off-chain. On deposit the asset amount to deposit for a specific amount of tokens to mint is calculated using “calculateAssetIn”. On withdraw the asset amount to withdraw on a specific amount of tokens to burn is calculated using “calculateAssetOut”.

```
function calculateAssetIn(uint256 token_amount) public view returns (uint256) {

      uint256 asset_balance = IERC20(asset).balanceOf(address(this));

      uint256 token_balance_new = totalSupply.add(token_amount);

      uint256 asset_balance_new = token_balance_new.mul(token_balance_new);

      return asset_balance_new.sub(asset_balance);

}
```

```
function calculateAssetOut(uint256 token_amount) public view returns (uint256) {

      uint256 asset_balance = IERC20(asset).balanceOf(address(this));

      uint256 token_balance_new = totalSupply.sub(token_amount);

      uint256 asset_balance_new = token_balance_new.mul(token_balance_new);

      return asset_balance.sub(asset_balance_new);

}
```

This minimal implementation limits the code bug risk and has a consumption of ~90k gas for a single deposit or withdraw transaction. At current gas prices of 100 Gwei on the Ethereum blockchain this results in a cost of 0.009 ETH. Which at the current dollar price for ETH of ~$1,850 results in a cost of ~$17. Because of the more complex code implementations of other applications on the Ethereum blockchain, this is significantly lower than most applications. The short term expected integration of layer two code execution implementations can be used to reduce these gascost to a minimal.

7. Conclusion

We proposed an on-chain hedging protocol based on bonding curve markets without the need for a separate governance system. The hedging protocol can be used to create assets stabilized for changes in demand of the underlying asset. The hedging market is reliant on the depreciation narrative for the hedging pools and minimizes trust with its minimal implementation where users only rely on the Ethereum blockchain and market forces from the narrative. The resulting stabilized assets are complementary to existing stable tokens based on a pegged design.

Future research is focussed on an additional floor option implementation that can add focus to the depreciation narrative by limiting risk from mass withdrawal out of the protocol.

References

[1] Vitalik Buterin. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, 2013. URL https://ethereum.org/en/whitepaper/.

[2] Simon de la Rouviere. Tokens 2.0: Curved tokens bonding in curation markets, 2017. URL https://medium.com/@simondlr/tokens-2-0-curved-token-bonding-in-curation-markets-1764a2e0bee5.

[3] Robert J. Shiller. Narrative Economics: How Stories Go Viral and Drive Major Economic Events, 2019.

[4] MakerDao. The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System. URL https://makerdao.com/en/whitepaper/.