Blockchain Derivatives: On-Chain vs. Off-Chain Architectures

Sonya Smith

Introduction

Derivatives contracts are a form of security that derives value from an underlying asset. Such derivatives include swaps, futures contracts, puts, and many more. Such contracts are executed legally, drawn up by lawyers and bankers acting as market-makers to sell these products to investors on a spread, that is, with a difference between the price of the two sides of the contract. This means that typically derivatives are between two parties with an underwriting institution. However, this underlying institution is a flaw in the system. The goal of this project is to replace underwriting institutions with Ethereum, transferring the entire operation onto a decentralized platform and making it execute between two parties on a trustless platform.

Problem definition and motivation.

As an illustrative example, let us consider the example of shorting an asset. Typically when one invests in an asset, they buy it with the hope that it will rise in value relative to some other asset, usually currency. This in turn allows the investor to collect a profit in his or her portfolio. In this situation, the trader is considered to be “long” on that particular asset.

There are many cases in which investors may not want to go long on an asset, but rather expect the asset to decline in value. If he or she owns the asset as part of his or her investment portfolio, the answer is simple: sell the asset at the current price as a way of locking in the current value of the asset, protecting you against future losses. Alternnatively, if this is not possible, due to lockup provisions or legal requirements, the investor may wish to purchase a put option. This allows the investor to pay a premium for the right

to sell the asset at a given price in the future. However put options inevitably require another investor or an institution to take the other side of the bet. This requirement means that puts are only available for highly traded assets, such as shares of stock in large companies. Options for more thinly traded assets can be prohibitively expensive, if it is even possible for an outside buyer to assume such a large economic risk. In this case, it may be desirable for the investor to consider shorting the asset.

Shorting an asset is a process by which certain investors borrow assets on collateral. They then sell these assets into the market with a contract which requires them to repurchase the shares in the future. For their trouble, the creditor receives premiums, effectively acting as interest on a loan.. The long buys the asset at market price and has a guaranteed seller some amount of time down the road.

A short sale depends upon two major third parties. First, the prospective short must find an investor willing to lend out shares. This requires the short to post margin and pay premiums. In addition, the contract typically requires an institution to underwrite the contract. This has a number of disadvantages. First, most such contracts have a provision known as a buy-in whereby the lending portfolio manager can require early termination of the arrangement. This early termination can result in locked-in losses for the short as it requires the immediate return of the capital the lender has contributed to the arrangement. Second, underwriting institutions typically charge fees to underwrite the contract, handle margins, do legal work on the contracts, collect payment, etc. Finally, having a centralized underwriting institution is disadvantageous for investors. It requires investors to trust an institution, perhaps a cryptocurrency exchange or a bank. Such institutions can fail, and when they do the money investors have entrusted the institution with is effectively lost with little chance of recovery. This can happen for reasons having to do with everything from fraud to economic failure. This can be frustrating for investors and negatively impact the market as a whole. What’s more, granting large institutions the right and power to manage a large book of contracts creates an obvious informational advantage for the institution. Information, in the investment world, is perhaps the most important commodity above all else. It allows market participants to invest confidently and with a clear understanding of risk. Granting large amounts of market power to large institutions is precisely what centralizing the mechanisms by which investors buy and sell assets is exactly the cumulative effect that one should expect from the current state of affairs. It is my belief that such a system is much more suited to a decentralized platform, one in which contracts can be executed between investors without reliance on third parties. The aim of this project is to explore the elimination of any third parties by exploring the possibility of using decentralized exchanges to determine valuation for assets and then executing the terms on the Ethereum blockchain.

Prior Work

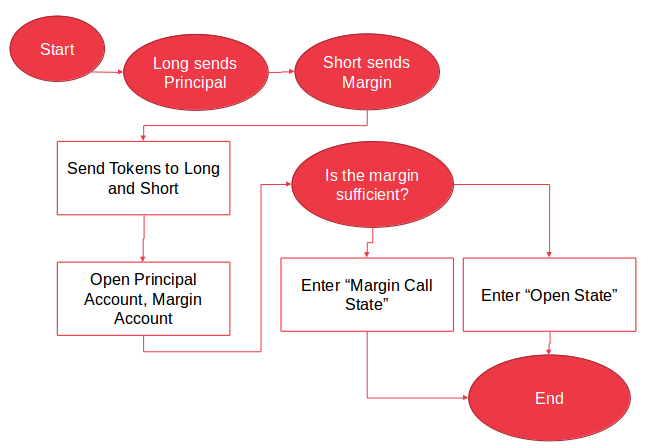
The most relevant prior work for this project is the academic paper “On the Feasibility of Decentralized

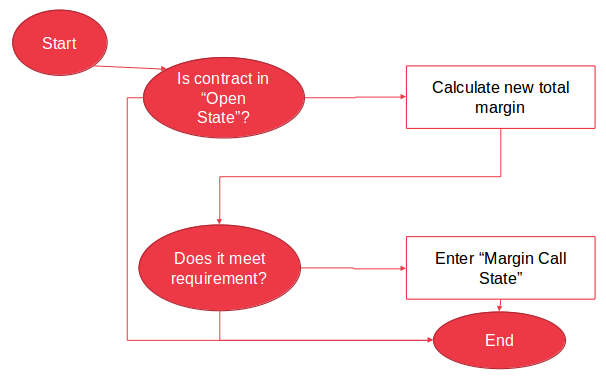
Derivatives Markets”. This paper describes an project, called Velocity, that aims to do a similar thing to the ultimate aim of this project: to create a decentralized derivatives market using zero-sum contracts mediated between two parties. This project consists of a hybrid on-chain/off-chain model. The on-chain part of the project revolves around a simple solidity smart contract that handles the actual logic of the zero-sum derivative. The paper also explores cost collars as a potential application of this technology. In this example, the paper describes a system whereby an off-chain price server fetches a price from a price history database. The specific source for this price data is the Poloniex exchange API. The price history collects the order book information from the Poloniex exchange and compiles it into a database from which prices are calculated by the PriceGeth server. This has a number of advantages. First, it enables the contract to execute cheaply by taking price calculations off-chain. Taking these calculations off-chain is also essential in order to create derivatives based on non-blockchain assets, as no reliable system exists for putting these assets securely on the blockchain as of yet.

This approach also has some severe limitations. For one, the paper explicitly requires the operator of the PriceGeth server not to have any sort of market participation in the contract itself. This is problematic as there is no reliable way to enforce this system, nor to prevent collusion between the PriceGeth server operator and other market participants. In truth, the PriceGeth server has the unfortunate side effect of effectively centralizing the entire operation, thus rendering much of the supposed advantages of decentralization moot.

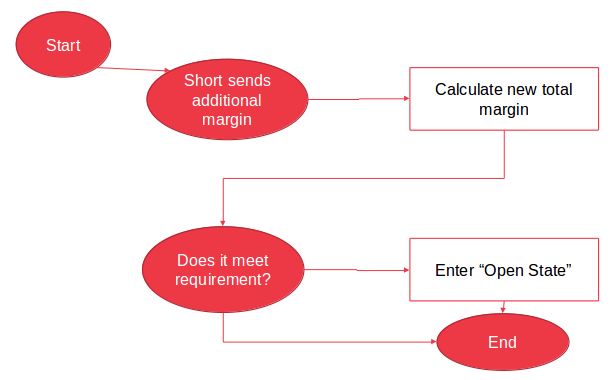
Another important piece of prior art is the Blockchain Board of Derivatives, also known as the BBOD. This system is yet another hybrid operation, consisting of an on-chain and off-chain part. In particular, the contract itself runs on ethereum and settlements are made on a daily basis to update investors on the state of their invested contracts. This allows investors to have greater confidence in buying derivative assets using this system. However, it once again falls into the obvious limitations inherent to hybrid applications, namely, it does not fully decentralize the system, and while the daily settlements have the advantage of making it harder for the central authority to manipulate the market for its own benefit, it by no means makes this system impossible. It also may make it very difficult for any one market participant to have a monopoly on a mass of trading information and the ensuing competitive advantage, but nonetheless the BBOD itself is still underwriting the entire transaction.

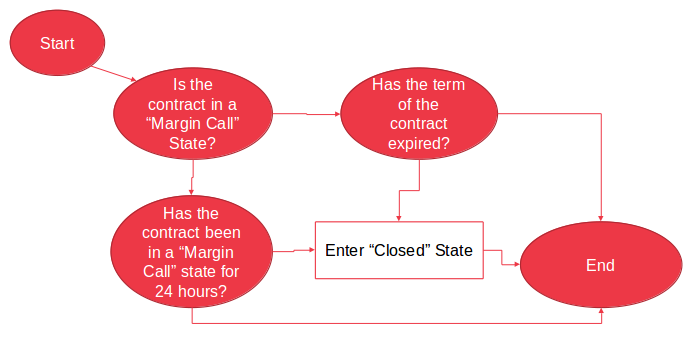
Design and Architecture

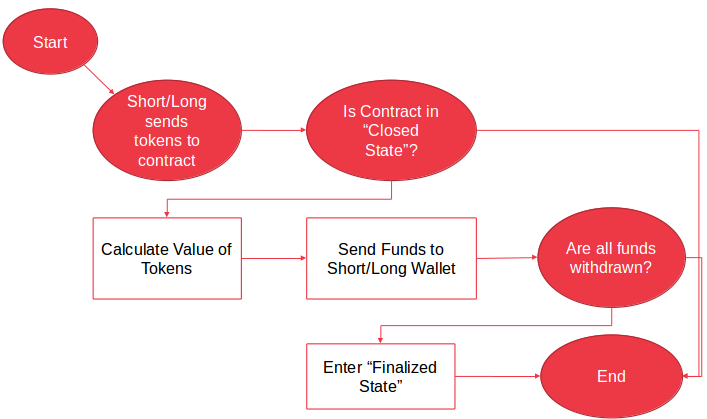
Here is the openContract function, which exists to start a contract on an asset. This is the same for both on-chain and off-chain price calculation.



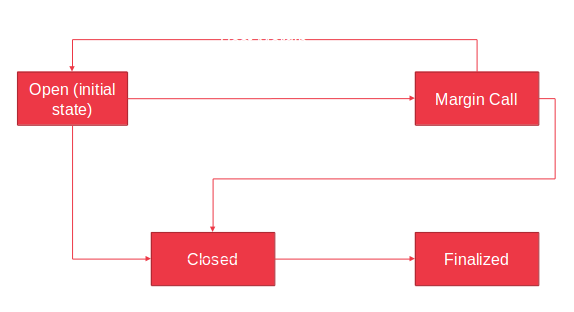
This describes the marginCall functionality. This functionality is called when the value of the principal increases in excess of the margin requirement. This requires the short to post additional margin in order for the contract to remain solvent.

Here is the mechanism by which the long posts additional margin. The margin here is put into the long’s margin account after it is determined that the margin is sufficient to cover the shortfall.

This is the closeContract function which allows



This is the withdrawal function which allows both long and short to access the funds that are in the contract once it is closed.

This state diagram shows an overview of the general logic of the contract. As you can see, the contract begins in an open state and always resolves to a finalized state. There is no way for a contract participant to exit the contract. Everything is underwritten by the blockchain.

Testing Setup and Procedure

The testing setup involves adding real price information picked by hand from an exchange (binance) for commodity trades involving BTC/ETH trades. The goal is to test both on-chain and off-chain price calculation and the resulting gas price. The gas prices involved were determined using Ropsten test network, and the contracts were deployed and functions were called using MyEtherWallet. Development was done using Remix IDE

Results

This graph shows the growth in gas price for a price calculation function (getPrice) as the order book for an on-chain asset grows. This is important to understand the way in which these functions scale as the order book grows longer. As can be seen here, the growth is substantial, but linear.

Here we can clearly see that for an order book of any size, the offchain function is significantly cheaper per transaction. However, because the on-chain function requires calling only when a margin call is made, for less volatile assets this difference might actually work in the favor of the on-chain solution.

Issues and Limitations

The final test results are heavily limited. In addition, the real-world applications of this technology are severely hamstrung by the limited selection of decentralized exchanges that can securely provide a basis for the all-important on-chain price calculation. In turn, future work will need to be done in this area to better provide such resources the the investment community. In theory this will have manifold benefits over and above the ones described here as it will allow all investors to freely participate in totally decentralized markets and exchanges. In the short term, however, such markets have serious challenges before they become viable for mass use. Much of the work being done is represented in the Saturn Network and its exchange, which was used in the design of this project as an example of how a future exchange might work as a basis for derivatives contracts.

Conclusions and Future Work

Unfortunately, the on-chain price calculation for derivatives is likely to be prohibitively expensive for highly volatile assets, the same kind of assets which as of yet make up the only assets tradable on blockchain-based exchanges. As a result, any such derivatives market is unlikely to be viable in the short term.

However, over the long haul, this application shows potential for future blockchain applications. These applications can go beyond the world of simple derivatives and using decentralized exchanges can provide a wealth of services to investors.

One potential example of future work would be extending the blockchain derivatives idea to include cost collars. These contracts exist to provide a form of insurance toward investors. An investor makes a guarantee on an asset, that if the value of the investment principal goes above a certain amount, the investor will pay the other investor the funds in excess of the amount. A similar guarantee is made on the opposite side, if the value declines below a set floor, the investor who owns the principal is paid by the other investor to compensate.

References

Eskandari, Shayan, et al. *On the Feasibility of Decentralized Derivatives Markets*. Concordia University, 2017, users.encs.concordia.ca/~clark/papers/2017\_wtsc.pdf.

“Introducing Blockchain Board of Derivatives : Defining Moments.” *Medium*, 8 Oct. 2017, Introducing Blockchain Board of Derivatives : Defining Moments.

Staff, Investopedia. “Collar.” *Investopedia*, DotDash, 18 Oct. 2018, www.investopedia.com/terms/c/collar.asp.

Jagerson, John. “Short Selling.” *Investopedia*, DotDash, 7 Dec. 2018, www.investopedia.com/terms/s/shortselling.asp.