Powerswap Platform

Powerswap Platform Foundation

Abstract

This paper, presents an AMM (Automated Market Making) platform on coin/coin exchange, callable bull and bear contracts, and Satoshi perpetual options. The token/token swap, named as Powerswap, have two types of players, investors and liquidity providers. Investors use Powerswap to exchange digital tokens and trade with liquidity providers. Powerswap uses the power sum invariant with the extension of virtual balance. Unlike the constant product AMM, power sum AMM allows for high market depth, controlled by price volatility. Virtual balance further reduces atomistic arbitrage within a block by miners. The callable bull and bear contracts (CBBC) allow for investors to speculate on the price of bitcoin, Ethereum and Gold using any tokens of their possession with high leverage. CBBC contracts have three types, investors, liquidity providers and callers. Investors trade with liquidity providers to speculate on the price movements of the underlying asset using any type of tokens. The callers make sure the equity of investors will not go down below zero and settle investors' accounts when the equity falls below a prespecified level. The advantage of CBBC over conventional futures contracts is that it allows investors to speculate using the tokens of their own. The Satoshi perpetual option (SPO) contract has an exponential decay which allows for simplified pricing with high leverage. It differs from fixed maturity options in that the

option never expires but the payoffs will decay. This contract will still give investors hope even after it passes half-life of the contract. Like CBBC, SPO allows speculation of BTC, ETH and gold settling in any alternative coins. We also discuss the issue of platform tokens for the three smart contracts and plan to offer pegged tokens using powerswap contracts and a flexible supply controlled by smart contracts

TABLE OF CONTENTS

1, INTRODUCTION

Blockchain technology has been around for more than 10 years but real applications have been scarce. One recent development is on trading using decentralized exchanges. Decentralized exchanges (DXes) have surged in trading volume lately. In particular, constant product automatic market maker (AMM) is leading the way. We discuss a few protocols using AMM design. We consider coin/coin swap, callable bull and bear contracts, Satoshi perpetual option contracts, and finally a cashflow based stable coin design.

2, POWERSWAP

We propose a new protocol that has the same feature as that of Uniswap but with smaller slippage.

We start with the constant price case

$$x + P_{\frac{y}{x}} y = k$$

Take x to be USDT and y to be UCNY, then $P_{\frac{y}{x}}$ is about 1/7, that is the value of y in terms of x.

When the price fluctuates, we cannot have a constant price equation. Consider the following power function variation

$$x^r + \left(P_{\frac{y}{x}} y\right)^r = k$$

Notice that when $r = 1$, this equation reduces to the linear function

$$x + P_{\frac{y}{x}} y = k$$

When r goes to zero, this equation converges to

$$\ln(x) + \ln(y) = constant$$

which is equivalent to $xy = constant$, that is the Uniswap protocol. Therefore, the invariant curve lies between the constant price one and the constant product one.

2.2, LIQUIDITY PROVIDERS

Liquidity tokens LT is generated according to the following formula. Let Dx and Dy be the number of X and Y tokens added to the liquidity pool. Tx and Ty be the number of X and Y tokens currently in the liquidity pool. The ratio of Dx and Dy has to be proportional to that of Tx and Ty. Then the number of liquidity tokens generated DLT is given by the following formula

$$DLT = TLT\left(\left(1 + \frac{DX + DY}{TX + TY}\right)^{F} - 1\right)$$

Notice that when F is small, this reduce to a linear relationship. One approximation is

$$\frac{DLT}{TLT + DLT} = \frac{1 - \sqrt{1 - \frac{4F(1-F)(DX+DY)}{DX+DY+TX+TY}}}{2(1-F)}$$

$$\frac{DLT}{TLT} = \frac{1 - \sqrt{1 - \frac{4F(1-F)(DX+DY)}{DX+DY+TX+TY}}}{1 - 2F + \sqrt{1 - \frac{4F(1-F)(DX+DY)}{DX+DY+TX+TY}}}$$

Let

$$\theta = \sqrt{1 - \frac{4F(1-F)(DX+DY)}{DX+DY+TX+TY}}$$

$$\frac{DLT}{TLT} = \frac{2F * (DX+DY)}{TX + (1-2F)(DX+DY) + (TX+TY+DX+DY)\theta}$$

Further Taylor expansion we get the following approximation

$$DLT = \frac{TLT \times F \times (DX+DY)}{TX+TY+(1-F)^2(DX+DY)}$$

Therefore the price of the liquidity tokens is higher as more liquidity tokens are minted.

On the other hand when liquidity tokens DLT are burned, users receive Dx and Dy of X and Y tokens respectively

$$Dx = Tx\left(1 - \left(1 - \frac{DLT}{TLT}\right)^{\frac{1}{F}}\right),$$

$$Dy = Ty\left(1 - \left(1 - \frac{DLT}{TLT}\right)^{\frac{1}{F}}\right).$$

Applying Taylor expansion to above equations gives

$$Dx = Tx\left(\frac{1}{F}\frac{DLT}{TLT} - \left(\frac{1}{F} - 1\right)\left(\frac{DLT}{TLT}\right)^2\right),$$

$$Dy = Ty\left(\frac{1}{F}\frac{DLT}{TLT} - \left(\frac{1}{F} - 1\right)\left(\frac{DLT}{TLT}\right)^2\right).$$

2.3, ANTIARBITRAGE

The last block price will be used when coins are swapped. This way miners are unable to arbitrage within the block, this will significantly increase the profit of LP providers. In addition, virtual balances are used in updating prices which reduces manipulation across blocks.

2.3, PROTOCOL FEE

In the future, a 16% transaction fee can be moved as the protocol fee to an address controlled by the project developers and belongs to the owners of the platform token, Taurus Bull and Bear Coin (TBBC), described later

3, CALLABLE BULL AND BEAR CONTRACTS

3.1, CBBC

A **callable bull/bear contract**, or **CBBC** in short form, provides investors with leverage. It was first introduced in Europe and Australia in 2001, and it is now popular in United Kingdom, Germany, Switzerland, Italy, and Hong Kong. CBBC is actively traded among investors in Europe and Hong Kong, as it caters to individual investors' behavioral biases (like preferences for skewness).

CBBC has two types of contracts, *callable bull contract* and *callable bear contract*, which are always issued in the money. By investing in a callable bull contract, investors

capture its potential price appreciation. Conversely, investors buying a callable bear contract are trying to make a profit in a falling market.

CBBC is typically issued at a price that represents the difference between the *spot price* of the underlying asset and the *strike price* of the CBBCs, plus a small premium (which is usually the funding cost). The call price is the average of the stock price and the strike price.

CBBC implemented in our smart contracts will never expire, however, anyone can call back the contract and has the positions liquidated once the price is lower than the call price. Contract holders can also liquidate their positions any time they want. In addition, to avoid too much risk for liquidity providers, the maximum gain is capped by an upper bound proportional to the leverage. The maximus price change an investor can receive is the initial price times a percentage and currently is set at 10%.

A property of CBBC is that it caters to people who prefers skewness as recent behavioral finance research argues that skewness also matters and investors can trade due to their different preferences and opinions regarding skewness.

3.2, PRODUCT CBBC

Normally, CBBC is traded using one of the trading pair as the settlement token. For example, let ETH/USDT be the price CBBC is traded on, then the payoff will be in the units of USDT, that is the price change of ETH in terms of USDT.

A product CBBC is similar to quantos in that the price is quoted in one token but the settlement is in another token. For example, the price of ETH is quoted in USDT but the settlement is in UCNY, another token and the gains and losses is (P2-P1)*UCNY for a bull contract and (P1-P2)UCNY for a bear contract.

Product CBBC allows UCNY holders speculate on ETH/USDT price change without having to first convert to USDT, when UCNY/USDT liquidity is low and UCNY price may be prone to manipulations.

3.3, CBBC SMART CONTRACTS

The CBBC smart contract has three type of player, investors, liquidity providers and callers.

Investors: This type of players can open and close his positions any time they want. An investor need to fill in the initial capital he wants to put in, leverage level, bull or bear. The smart contract will determine the strike price, the call price and upper bound

(bull) or lower bound (bear). The strike price will the price such that the investor's equity will be zero. The call price is the average of the strike price and current token price. :

Liquidity providers: Liquidity providers trade with investors. They receive transactions fees. Moreover, because investors use high margins, liquidity providers make money most of the time and thus their returns have negative skewness

Callers: Callers can be anyone who tries to liquidate positions. When a caller call a bull position, if the price is lower than the call price, the call is successful and investor's positions are liquidated. Otherwise, the call fails and the position remains. Similarly, when a caller call a bear position, if the price is higher than the call price, the call is successful and investor's position is liquidated. Otherwise, the call fails and the position remains open.

3.4, CBBC PLATFORM TOKENS (TOKEN OF BULL AND BEAR CONTRACTS， TBBC)

TBBC is the CBBC platform token. For CBBC contracts using X token as settlement tokens, 1/3 of transaction fees will be sent to the X/TBBC powerswap contracts and corresponding TBBC will be moved to a pool owned by TBBC holders.. This way the price of TBBC will appreciate against X. In addition, owners of the TBBC pool will have more TBBC. As more investors use these contracts, TBBC will appreciate more

4, SATOSHI OPTION CONTRACTS (SPO)

4.1,SPO

In the design of bitcoins, the award for mining halves every four years. This feature is similar to a radioactive delay. In the following option contract we adopt a similar feature and we term these option contracts as Satoshi Option Contracts.

$$C(t) = 2^{-\delta t}\frac{1}{n}\left(\left(\frac{S(t)}{K}\right)^{n} - 1\right)^{+} KX(t)$$

$$P(t) = 2^{-\delta t}\frac{1}{n}\left(1 - \left(\frac{S(t)}{K}\right)^{n}\right)^{+} K\,X(t)$$

We consider n=0, 1, 2 which corresponds to logarithmic, linear and quadratic Satoshi options. In addition we consider the following binary Satoshi option contracts.

$$C(t) = 2^{-t/\tau}1_{S(t)>K}KX(t)$$

$$P(t) = 2^{-t/\tau}1_{S(t)<K}KX(t)$$

Pricing will be determined using a double jump model following Duffie, Pan Singleton (2001).

An advantage of the Satoshi perpetual options contracts are that they are the simplest to implement using smart contracts. A property of the smart contracts is that it is difficult to call back past prices and thus we cannot read past prices with low gas fees. For contract

opening and closing, it must be operated in a decentralized way with some user giving commands. The execution of opening and closing American options relies only on prices on the current block and thus is much easier.

3.3, SPO SMART CONTRACTS

The SPO smart contract has two type of player, investors, liquidity providers.

Investors: This type of players can open and close his positions any time they want.

An investor need to fill in the initial capital he wants to put in, the half life, and the strike price of his contract. The price of the contract and his positions will be determined by the SPO smart contract.

Liquidity providers: Liquidity providers trade with investors. They receive transactions fees. Moreover, because investors use high margins, liquidity providers make money most of the time and thus their returns have negative skewness

5, PLATFORM TOKEN POOL

Transactions fees will be sent to a pool owned by TBBC holders. All the alternative coins will be converted to TBBC and TBBC will be sent to the TBBC pool. This way TBBC price will appreciate and owners of the pool will receive more TBBCs.

The liquidity pool of the TBBC token is created with at least 25million TBBC. In the initiation stage, 25million TBBC is sent to the contract. 5000 liquidity coins are created

and sent to the initiator. After that the minting and removal of liquidity coins are determined using a power function formula.

Let the Total platform liquidity token be TPL=TotalPlatformLock. The tokens locked in the TBBC pool as TOTBBC=TotalTBBC， The deposit is DOTBBC=DepoitTBBC。 Then the returned liquidity coins quantity is DPL=DepositPlatformLock

$$DPL = TPL\left(\left(1+\frac{DOTBBC}{TOTBBC}\right)^{F}-1\right)$$

F is set at 0.5

Using some approximation, we get

$$\frac{DPL}{TPL}=\frac{1-\sqrt{1-\frac{4F(1-F)DOTBBC}{DOTBBC+TOBBC}}}{1-2F+\sqrt{1-\frac{4F(1-F)DOTBBC}{DOTBBC+TOBBC}}}$$

$$\frac{DPL}{TPL}=\frac{1-\sqrt{1-\frac{4F(1-F)DOTBBC}{DOTBBC+TOBBC}}}{1-2F+\sqrt{1-\frac{4F(1-F)DOTBBC}{DOTBBC+TOBBC}}}$$

Let

$$\theta_{TBBC}=\sqrt{1-\frac{4F(1-F)DOTBBC}{DOTBBC+TOBBC}}$$

$$\frac{DPL}{TPL}=\frac{2F*DOTBBC}{TOBBC+(1-2F)DOTBBC+(DOTBBC+TOBBC)\theta_{TBBC}}$$

Taylor expansion we have

$$DPL = \frac{TPL * F * DOTBBC}{TOTBBC + (1-F)^2 DOTBBC}$$

As F < 1, the more TBBC there is in the pool the more valuable is the liquidity token.

Removal of liquidity tokens to receive TBBC is obtained using the following formula

$$DOTBBC = TOTBBC\left(1 - \left(1 - \frac{DPL}{TPL1}\right)^{1/F}\right)$$

Taylor expansion yields

$$DOTBBC = TOTBBC\left(\frac{1}{F}\frac{DPL}{TPL} + \left(1 - \frac{1}{F}\right)\left(\frac{DPL}{TPL}\right)^2\right)$$

The platform token poll will receive the 1/6 transaction fees from the Powerswap contracts and the 1/3 transaction fees from the CBBC and SPO contracts will all be sent to the platform pool. Notice that the price of TBBC will increase as transaction fees from alternative tokens are converted to TBBC and added to the TBBC platform pool. So the liquidity holders of the platform pool will receive more TBBC at a higher price.

6, PEGGED COINS

Stable coins is an important part of the crypto currency market. There are three kinds of stable coins: stable coins using fiat currency as collateral such as USDT, USDC; stable coins using digital assets as collateral such as DAI and stable coins using pure algorithm such as Ampleforth and Basis. The first kind will incur lots of legal cost and is not truly decentralized. Stable coins using digital collaterals can suffer crashes when digital assets

crashes too fast. Finally the algorithm based stable coins do not have any value support and people holding these stable coins may incur significant losses.

In this section we offer a new concept of pegged coins. We will use the cashflows from the exchange to support the pegging. We plan to create four pegged coins, PBTC, PETH, PUSD and PGLD that pegs to BTC, ETH, USDT and PAXG respectively. PBTC will be pegged to 1 millionth of BTC, PETH to one thousandth of ETH, PUSD 1:1 to USDT and PGLD pegged to 1 thousandth of PAXG.

Here is how it works: take USDT and PUSD. we will create two smart contracts. The first is PUSD/TBBC and the second pair is PUSD/USDT. As TBBC increase in value due to the cashflows from the platform smart contracts. This creates an arbitrage opportunity among PUSD/TBBC, PUSD/USDT, and TBBC/USDT. Arbitragers will move PUSD out of PUSD/USDT and move it to PUSD/TBBC. As a result, PUSD will appreciate over USDT. When the quantity of PUSD falls below 0.95 of the quantity of USDT in the powerswap contract pair, the smart contracts automatically increased the quantity of PUSD to the same as that of USDT.

On the contrast, if there is a depreciation of PUSD such that the quantity of PUSD is more than 1.05 times the quantity of USDT in the pegging contract. The supply of PUSD

will depreciate to the same as that in the pegging contract. As a result the price of PUSD/USDT will be constrained to the interval between 0.95 and 1.

The design is similar to AMPLEFORTH. However, there are two key differences. First is the asymmetry in rebasing supplies. When the pegged coin decrease in value, the quantity of all PUSD will shrink in our design which is also true in the Ampleforth design. However, when the pegged coin increase in value, only the supply in the powerswap liquidity pool and the owners' pool will increase in supply. This design will create incentives for investors to pour pegged coins into the liquidity pool and the owners' pool and thus creates more liquidity. Second, the ampleforth stable coins are not supported by cashflows. On the contrary, the pegged coins in our design is supported by transaction fees from the smart contracts.

As the contracts will have more transaction fees coming in, the supply of PUSD will be more likely to increase then to decrease.

The platform token poll will receive the 1/6 transaction fees from the Powerswap contracts and the 1/3 transaction fees from the CBBC and SPO contracts will all be sent to the platform pool. Notice that the price of TBBC will increase as transaction fees from alternative tokens are converted to TBBC and added to the TBBC platform pool. So the liquidity holders of the platform pool will receive more TBBC at a higher price.

Pegged coins can be used in lending and borrowing throw smart contracts, we will discuss that in another document.

6, FINANCING

Powerswap platform has coin/coin exchange, callable bull and bear contracts, Satoshi perpetual options and a new pegged coin design using the support of transaction fees. The stable coin can be used in lending as users prefer tokens that have a stable price in their lending and borrowing schemes. Powerswap will be a one shop stop for various financial needs of investors.

For the derivatives, users will be able to speculate on bitcoin, ethereum and Paxos gold coin price changes. This will be first time that users are able to trade using any coins they have in their hands. Using CBBC and SPO, they will be able to choose leverage of their own choice.

The pegged coin design will allow users to be able to borrow stable coins using their digital assets as collaterals and we are building a platform of token exchanges,

The platform plans to raise 1.5 million dollars with 10 million TBBC. The money will be used to increase liquidity in smart contracts on powerswap, hire more programmers to improve customer experience and to attract more tokens to be listed on the powerswap platform.

The platform will be decentralized and belongs to the powerswap community. TBBC will also be used as a voting instruments to determine future developments of the platform.

7, INVESTMENT AND RETURN

How can an investor participate in the powerswap platform? There are three ways that an investor can profit from the powerswap platform.

1: Purchase TBBC on powerswap and deposit it in the ownership pool. The investor will receive 1/3 of the transaction fees on all derivatives and 1/6 of the transaction fees on powerswap token pairs.

2. Add to liquidity to powerswap liquidity pools including trading pairs and derivatives. The investor will receive 5/6 of the transaction fees on trading pairs and 2/3 transaction fees on derivatives.

3. Just trade using powerswap pairs and take positions in derivatives. Any one participated will receive 400 TBBC one year later.

4. Liquidity providers can forgo transaction fees and instead choose to receive TBBC. By participating in the owners' pool, he will have a share in future transaction fees in the whole platform.