CompliFi Protocol – a Constant Sum Mechanism for Issuance of Decentralised Derivatives

V1.1

Dmitri Senchenko

August 20, 2020

Abstract

CompliFi Protocol proposes a decentralised mechanism for issuing a wide range of financial derivatives that are fully collateralised at all times and, therefore, carry no counterparty risk. The protocol also features minimal governance, no margin calls or liquidations, and limited sensitivity to blockchain network congestion. The trade-offs required to achieve these properties are finite settlement time, fixed upper bounds on the derivatives' payoff functions and an increased working capital requirement for the issuance process.

1 INTRODUCTION

There currently exists a wide range of opportunities for crypto traders to enter into financial derivative contracts. A number of centralised platforms serve both as originators and trading venues for a diverse range of products. In the decentralised domain, the offering is more limited – DeFi composability allows users to enter into short and leveraged positions and, with some ingenuity, to structure certain more exotic exposures. Risk management systems of both centralised and decentralised platforms carry significant issues. For the former, a key problem is the widespread opacity of internal risk policies and their shortcomings evidenced by the past "clawback" events and arbitrary liquidations of user's positions. For the latter, risk management protocols are (mostly) publicly visible, but often not fully understood from both the economic perspective and in terms of limitations carried over from the underlying consensus protocols. For instance, during periods of peak demand for unwinding of risk positions, the time-sensitive nature of the process exposes users to network congestion risks, which have already been shown capable of severely undermining on-chain collateralisation management and the associated liquidation procedures.

CompliFi protocol takes a different approach to managing risks associated with creating and maintaining derivative positions. Instead of relying on the ability to extract more collateral from risk holders to ensure that the opposite side of the trade can be paid off in full, CompliFi constructs derivatives that are backed by a predetermined pool of collateral. In other words, the protocol issues two instruments with properties that are very close to long and short positions of a chosen derivative, and together they always have a claim on the entire fixed pool of collateral. The required profitability of these instruments is then achieved by changing their relative claim on the collateral based on changes in the chosen derivative's underlying variable.

2 PROTOCOL INTUITION

The protocol is designed around the idea of a "constant sum" of payoffs. To create a chosen derivative, a user or a group of users lock an amount of collateral in a smart contract for a fixed period of time, and in return the smart contract issues each of them with two classes of assets. The first ("primary") class represents the long position in the derivative. The second class forms its "complement", such that together they have a claim on all of the underlying collateral – hence "constant sum". Furthermore, they are designed in such a way that holding equal quantities of each cancels out the underlying risks. In particular, users do not incur any additional risk at the moment of swapping their collateral for the newly issued assets.

At a predetermined point in time, the smart contract fixes the value of whichever underlying variable the derivative is based on – the derivative is now considered "issued". From this point and until a predetermined settlement time, the smart contract induces the primary asset's payoff function to behave as the long position in the chosen derivative by redistributing collateral between it and its complement. At settlement time, the smart contract fixes the relative claims on collateral of the two asset classes according to the last value of the derivative's underlying variable. After that, users are free to swap the assets, in their own time, for the underlying collateral in proportions that result in the primary asset having the same payoff as would have been due to direct holders of the chosen derivative.

From a user's perspective, the motivation to swap collateral for the two sides of a derivative trade can be two-fold. Firstly, they could be seeking a particular exposure offered by the derivative, in which case they would keep the desired side of the trade and sell the other, recouping part of their capital. Secondly, and more interestingly, the protocol creates a new opportunity for an investment bank-like role for users not motivated by desire to hold balance sheet risk. Instead, users could take advantage of the opportunity to issue and sell both sides of the derivative at prices that together yield them more than the value of collateral they have deposited. In other words, there is a natural profit opportunity in supplying the market with in-demand risk exposures by transforming collateral value into "value plus useful risk structure". In this role, users can easily manage their own risk by setting an upper limit on net exposure they are prepared to hold. In particular, issuing any amount of a derivative and holding both sides until settlement allows one to retrieve all of the original collateral without risk, thus limiting any downside to transaction fees and cost of capital.

The inevitable limitation of the protocol arises from the fact that one cannot award more than 100% of collateral to any side of the trade. This fact places an upper bound on any payoff function that this approach tries to mimic. On the other hand, within the confines of the "constant sum" of locked collateral, the protocol can recreate any desired instrument. Furthermore, this limitation is mitigated by the fact that there is significant leeway to lower the probability of hitting the payoff bound to an inconsequential level simply by choosing an appropriate duration for the instrument (i.e. in most cases, the shorter the duration, the lower the likelihood of hitting the bound). This same tactic could also aid, where necessary, in pricing these bounded variants of canonical financial instruments, since a low enough probability of reaching the payoff bound may justify equating the price of the primary instrument to its already-priced canonical counterpart. After that, the complement asset can be priced based on the constant sum property of the mechanism.

3 HOW IT WORKS

Suppose a user seeks to create a derivative with a payoff function $\rho^*(u_t)$ based on the value of some underlying variable u_t (e.g. price of BTC, S&P500, etc.), originated at time $t = 0$ and settled at $t = T$, using some uniform collateral $C > 0$ that changes in price relative to a reference asset (e.g. USD) over time so that at time *T* it is worth $(1 + S_T) \cdot C$ and $S_0 = 0$.

In return for *C,* the user receives at $t = 0$ two classes of assets, A and A', in equal quantities $|A| = |A'| = Q$. At settlement time $t = T$, A and A' can be swapped back for *C* according to a "split" $\sigma \in [0,1]$, such that asset class *A* gets $\sigma \cdot C$ and asset class A' gets $(1 - \sigma) \cdot C$. Correspondingly, individual units of A and A' receive $\sigma \cdot C/Q$ and $(1 - \sigma) \cdot C/Q$.

To create our chosen derivative, we can either specify $\sigma = \sigma(u_t)$ directly, or by setting $\rho_A(u_T) = \rho^*(u_T)$, where ρ_A is the payoff function of *A*. In other words, the asset class *A* represents the primary asset (i.e. long position in our chosen derivative), and A' represents the complement asset. Thus, at $t = T$ the protocol simply needs to observe u_T, evaluate $\sigma(u_T)$ and distribute C to holders of A and A' accordingly.

3.1 Basic Properties

Holding equal numbers of assets from A and A' does not result in any additional fundamental risk relative to holding *C* directly. Only when selling or buying the assets in unequal quantities will users incur additional exposure. This can be illustrated by considering the claim on *C* of a portfolio that consists of one unit of A and one of A'. Value of this portfolio does not depend on *w*.

$$\frac{\sigma(u_T) \cdot (1 + S_T) \cdot C}{Q} + \frac{(1 - \sigma(u_T)) \cdot (1 + S_T) \cdot C}{Q} = \frac{(1 + S_T) \cdot C}{Q}$$

We define investment returns ρ for A and A' based on their respective claims on *C* at $t = 0$ vs. $t = T$, and the change in the price of *C*.

$$\rho_A = \frac{\sigma(u_T) \cdot (1 + S_T) \cdot C - \sigma(u_0) \cdot C}{\sigma(u_0) \cdot C}$$

$$\rho_{A'} = \frac{\big(1 - \sigma(u_T)\big) \cdot (1 + S_T) \cdot C - \big(1 - \sigma(u_0)\big) \cdot C}{\big(1 - \sigma(u_0)\big) \cdot C}$$

We derive the upper bounds $\bar{\rho}_A$ and $\bar{\rho}_{A'}$ for the above investment returns by setting $\sigma(u_T) = 1$ and $\sigma(u_T) = 0$, respectively. For the sake of simplicity, we ignore specifications of $\sigma(u_T)$ where its value never reaches 1 or 0, and suspect that such cases would be rare due to capital efficiency considerations.

$$\bar{\rho}_A = \frac{1 + S_T - \sigma(u_0)}{\sigma(u_0)} \qquad \bar{\rho}_{A'} = \frac{S_T + \sigma(u_0)}{1 - \sigma(u_0)}$$

The choice of $\sigma(u_0)$ determines the upper bounds on investment returns, but does not affect our ability to replicate any desired payoff function, provided that it stays within those bounds. For any given $\sigma(u_0)$, we can derive $\sigma(u_T)$ that results in our chosen $\rho^*(u_T)$ by setting $\rho^* = \rho_A$:

$$\sigma(u_T) = \sigma(u_0) \cdot \frac{1 + \rho^*(u_T)}{1 + S_T} \quad s.t. \;\; 0 \leq \sigma \leq 1$$

4 PRACTICAL EXAMPLES

4.1 Synthetic BTC priced in fiat USD, USDC collateral, 50/50 primary/complement asset split

In this example, we construct a derivative that behaves as a long position in BTC up to a 100% increase in BTC price, whereafter its returns are flat.

Let $u_T = (BTC_T - BTC_0)/BTC_0$ be the normalised change in USD-denominated price of Bitcoin over $[0, T]$, and $S_T = (USDC_T - USDC_0)/USDC_0$ the corresponding change in price of USDC.

$$\rho_A(u_T) = \rho^* = \begin{cases} u_T & for \quad -1 \leq u_T \leq 1 \\ 1 & for \quad u_T > 1 \end{cases}$$

$$\sigma(u_T) = \begin{cases} 0.5 \cdot \dfrac{1 + u_T}{1 + S_T} & for \quad -1 \leq u_T \leq 1 \\ 1 & for \quad u_T > 1 \end{cases}$$

$$\rho_{A'}(u_T) = \begin{cases} 2 \cdot S_T - u_T & for \quad -1 \leq u_T \leq 1 \\ -1 & for \quad u_T > 1 \end{cases}$$

$$\bar{\rho}_A = \bar{\rho}_{A'} = 2 \cdot S_T + 1$$

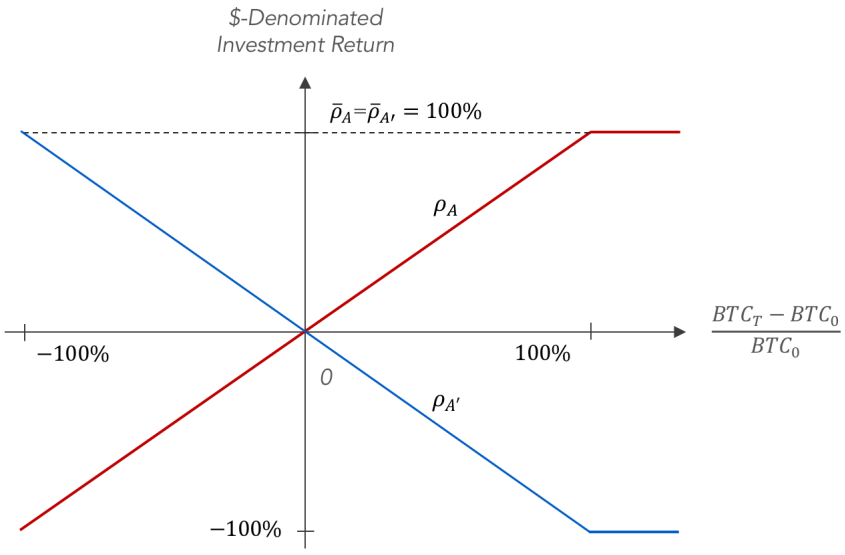

Fig. 1. Synthetic BTC profitability, assuming $S_T = 0$

4.2 2x leveraged[1] BTC priced in fiat USD, USDC collateral, 25/75 primary/complement asset split

In this example, we construct a derivative that behaves as a 2x leveraged long position in BTC up to a price increase of 150%, whereafter its return is flat.

Let $u_T = (BTC_T - BTC_0)/BTC_0$ be the normalised USD-denominated chain in price of Bitcoin over $[0, T]$, and $S_T = (USDC_T - USDC_0)/USDC_0$ the corresponding change in price of USDC.

$$\rho_A(u_T) = \rho^* = \begin{cases} 3 & for \quad u_T > 1.5 \\ 2 \cdot u_T & for \quad 1.5 \geq u_T \geq -0.5 \\ -1 & for \quad u_T < -0.5 \end{cases}$$

$$\sigma(u_T) = \begin{cases} 1 & for \quad u_T > 1.5 \\ 0.25 \cdot \dfrac{1 + 2u_T}{1 + S_T} & for \quad 1.5 \geq u_T \geq -0.5 \\ 0 & for \quad u_T < -0.5 \end{cases}$$

$$\rho_{A'}(u_T) = \begin{cases} -1 & for \quad u_T > 1.5 \\ \dfrac{4 \cdot S_T - 2 \cdot u_T}{3} & for \quad 1.5 \geq u_T \geq -0.5 \\ \dfrac{4 \cdot S_T + 1}{3} & for \quad u_T < -0.5 \end{cases}$$

$$\bar{\rho}_A = 3 + 4 \cdot S_T$$

$$\bar{\rho}_{A'} = \frac{4 \cdot S_T + 1}{3}$$

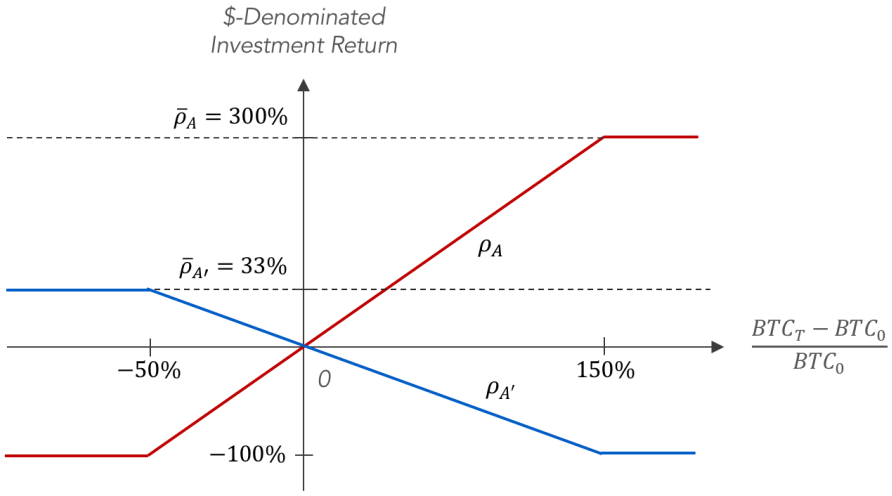

Fig. 2. Synthetic 2x BTC, assuming $S_T = 0$

[1] 2x leverage is defined as 1:1 ratio of equity to debt funding of a BTC long position

4.3 "Insured ETH" for up to 50% loss in USD value, ETH collateral, 50/50 primary/complement asset split

In this example, we construct a fully decentralised derivative that protects its holder from a decline in price of ETH relative to its level at origination. If the price of ETH rises, the derivative behaves as regular unlevered ETH. If price declines by up to 50%, it maintains constant USD value. If price declines further, the holder starts to incur losses.

Let $u_T = S_T = (ETH_T - ETH_0)/ETH_0$ be the normalised change in USD-denominated price of ETH over the period $[0, T]$.

$$\rho_A(u_T) = \rho^* = \begin{cases} u_T & for \quad u_T \geq 0 \\ 0 & for \quad -0.5 \leq u_T < 0 \\ 2 \cdot u_T + 1 & for \quad u < -0.5 \end{cases}$$

$$\sigma(u_T) = \begin{cases} 0.5 & for \quad u_T \geq 0 \\ \dfrac{1}{2 \cdot (1 + u_T)} & for \quad -0.5 \leq u_T < 0 \\ 1 & for \quad u_T < -0.5 \end{cases}$$

$$\rho_{A'}(u_T) = \begin{cases} u_T & for \quad u_T \geq 0 \\ 2 \cdot u_T & for \quad -0.5 \leq u_T < 0 \\ 0 & for \quad u_T < -0.5 \end{cases}$$

$$\bar{\rho}_A = \bar{\rho}_{A'} = 2 \cdot u_T + 1$$

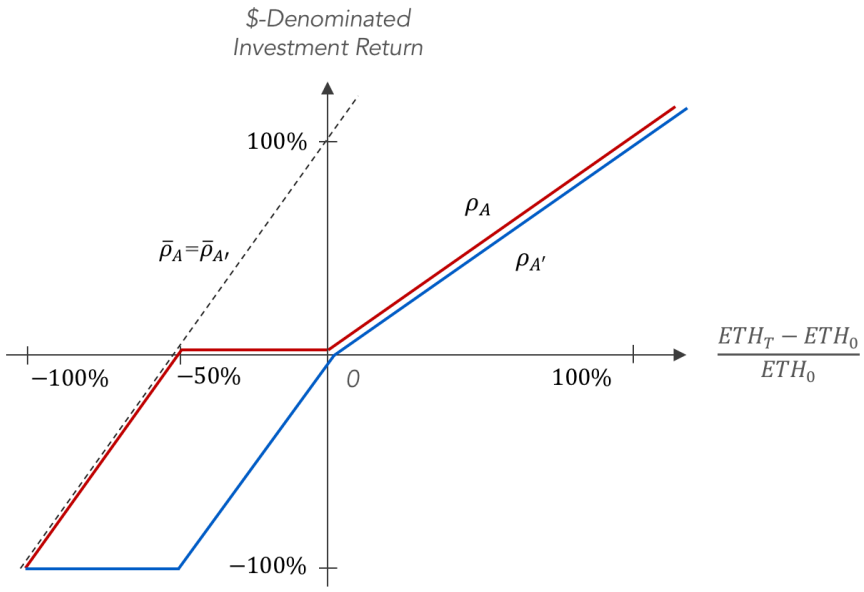

Fig. 3. Insured ETH up to 50% loss

4.4 USD stablecoin with downside protection for up to 75% ETH price decline, ETH collateral, with 25/75 primary/complement asset split

In this example, we construct a fully decentralised derivative backed by ETH that behaves as fiat USD up to a decline in value of ETH of 75%, whereafter the holder starts to incur losses.

Let $u_T = S_T = (ETH_T - ETH_0)/ETH_0$ be the normalised change in USD-denominated price of ETH over the period $[0, T]$.

$$\rho_A(u_T) = \rho^* = \begin{cases} 0 & for \quad u_T \geq -0.75 \\ 4 \cdot u_T + 3 & for \quad u_T < -0.75 \end{cases}$$

$$\sigma(u_T) = \begin{cases} \dfrac{1}{4 + 4 \cdot u_T} & for \quad u_T \geq -0.75 \\ 1 & for \quad u_T < -0.75 \end{cases}$$

$$\rho_{A'}(u_T) = \begin{cases} \dfrac{4 \cdot u_T}{3} & for \quad u_T \geq -0.75 \\ -1 & for \quad u_T < -0.75 \end{cases}$$

$$\bar{\rho}_A = 3 + 4 \cdot u_T$$

$$\bar{\rho}_{A'} = \frac{4 \cdot u_T + 1}{3}$$

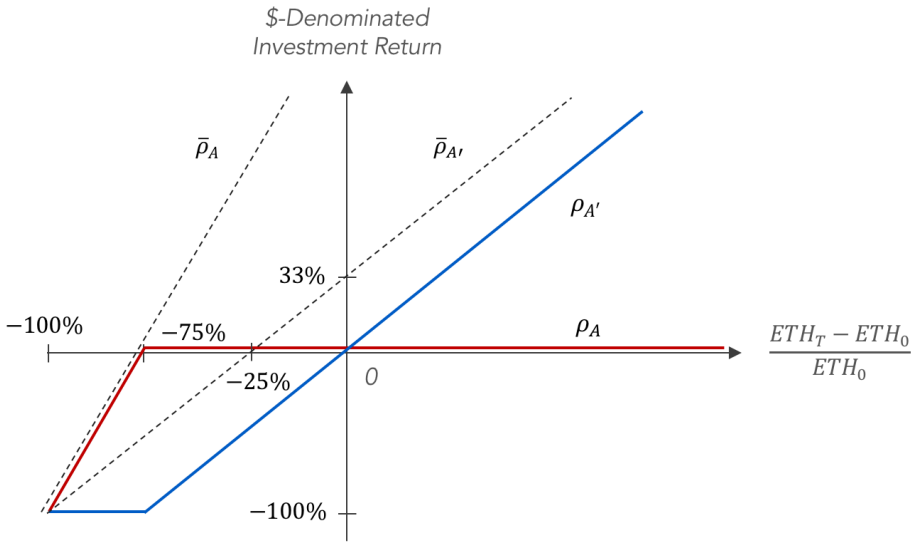

Fig. 4. Decentralised USD-denominated stablecoin