statiCoin and riskCoin

Paul Edge

Genki Financial Services
genkifs@gmail.com

October 16, 2017

Abstract

There is a high demand for stable token within the Ethereum ecosystem. This paper describes how the statiCoin contract meets this demand by openly, cheaply and efficiently creating fully fungible, Ether backed ERC20 compatible tokens, without requiring individual counterparties.

I. Introduction

STABLE coins are a necessary addition to the Ethereum ecosystem as they allow merchants to sell goods with the knowledge that the payment received will retain a fixed value. statiCoin is GENKI financial services solution for taming the volatility of cryptocurrencies. The system is composed of two types of ERC20 token; a statiCoin token and a riskCoin token. The statiCoin token is designed to be of equal value to a given currency. The riskCoin token is a more sensitive version of the exchange rate between the currency and ethereum token (ETH). In essence, exchange rate risk is removed from the statiCoin token and transferred to the riskCoin token. This gives statiCoin holders a price stable asset and riskCoin holders a "geared" asset that has a heightened sensitivity to changes in the exchange rate. The priority objective is for the statiCoin owners to be confident that they can redeem their coins at any time for a value equal to a fixed amount of fiat currency.

II. Definition of the riskCoin price

The riskCoin price is a function of the exchange rate, the number of statiCoins, the number of riskCoins and the total amount of ETH held in the contract. Formally, using the definitions in Table 1, it is defined as:-

Table 1: *Definitions*

Variable	Description
R	Number of riskCoins issued
S	Number of statiCoins issued
E	Total amount of ETH
X	Exchange rate, amount for 1 ETH
Y	Cost of 1 riskCoin

$$Y = \frac{EX - S}{R} \tag{1}$$

This is the value of the contracts ETH in fiat, less the number/value of statiCoins shared over the number of riskCoins. Essentially, riskCoin holders are entitled a proportion share of the total amount of ETH in the contract after all statiCoin holders have been paid. Note that the riskCoin price can go negative. In this case, the price is set to zero and no riskCoins can be created or redeemed; statiCoins may still be redeemed but not created.

A zero riskCoin price does not mean that riskCoins are worthless. There is a non-zero probability that the riskCoin price will become positive in the future, allowing the riskCoin to be redeemed for ETH. This future possibility of redemption has a value analogous to a financial call option, without expiry.

i. Leverage ratio

The leverage ratio shows how the riskCoin price behaves when the underlying ETH price changes.

$$\frac{dY}{dX} = \frac{E}{R} \tag{2}$$

The rate increases with the amount of ETH in the contract (i.e. more statiCoins) and decreases with the number of riskCoins.

III. Creation of coins

To create a statiCoin, simply send an amount of ETH to the NewStatic() function in the Minter contract which, after a delay, will credit the senders address with an amount of coins equal to the amount of ETH sent multiplied by the ETH price. Similarly, to create an riskCoin, send an amount of ETH to the NewRisk() function of the Minter contract which, after a delay, will credit the sender with riskCoins worth the ETH sent multiplied by the ETH price, divided by riskPrice.

i. Restrictions on the creation of coins

riskCoins cannot be created when the price is below 0. statiCoins cannot be created when the riskCoin price is 0, or when the leverage (eq:(2)) is too high (greater than the value in the Leverage() function of the Minter contract). This ensures that the ETH in the contract are not backing too many statiCoins.

IV. Redemption of coins

After coins are redeemed, ETH is returned to the address holder. To redeem a statiCoin, call the RetStatic(*value*) function where the *value* parameter is the quantity of statiCoins to redeem. For ETH to be returned to an address, a small amount of ETH must be sent to the RetStatic() to cover the cost of retrieving a price quote from outside the Ethereum blockchain, and there must be a quantity of statiCoins registered to that address. Excess ETH sent to RetStatic() will be immediately returned to the sender address. Similarly, to redeem riskCoins, call the RetRisk(*value*) function where *value* is the quantity of riskCoins to be redeemed. Again, some ETH must be sent to cover the cost of retrieving data and any over funding will be immediately returned.

i. Restrictions on redemption of coins

The only upper limit on the volume of coins that can be redeemed in a single transaction is the amount owned. [1]

riskCoins cannot be redeemed when the price is below 0.

statiCoins cannot be redeemed when there is no longer any ETH in the contract. When the contract has no ETH it is declared Bankrupt and resets itself.

V. Method of price query

Quotes are provided by the Pricer contract which currently uses Oracelize to query data from outside the Ethereum blockchain system. Each time a coin is minted or melted, a call to the Oraclize service is made. This service requires a nominal amount of ETH to function. When minting, the Oracelize fee is paid from GENKI's fee. When melting, ETH needs to be included with the number of coins that are to be redeemed. If too much ETH is sent when melting then excess ETH will be returned to the sender.

Oracelize was chosen as it is currently the easiest way to import off chain data. The Pricer contract is designed to be upgradeable, so an improved Pricer contract may be substituted at a later date (with 2 days notice).

VI. Source of exchange rate prices

KRAKEN was chosen as an exchange rate data source as it proves an open API with a 24

[1] A redemption limit could easily be bypassed by transferring coins to multiple wallets. The minter contract would have no way of knowing whether any addressed were controlled by the same actor.

hour volume weighted average price for various currencies. Blended quotes from multiple exchanges would be preferable, but Oraclize currently only allows one URL to be called at a time.

The 24 hour volume weighted price is chosen as it is assumed to be unlikely that a single individual (or group) would be able to significantly influence an exchange for a period of a day. If the **current** 24 hour volume weighted price were returned then it would be possible to predict the direction of future movements of the average price with some certainty. The delaying of 24 hours allows for all currently known price information to be removed from the future price quote[2]. The delay for minting/melting also reduces the likelihood that the coin supply will be affected by trading sentiment, although the coins may still be traded immediately on an exchange.

As Ethereum matures, the delay time period could be reduced as exchange rates become more liquid and the ability for a single actor to influence prices reduces. The Pricer contract can be replaced by one with a shorter delay, assuming that suitable data feeds are available.

VII. statiCoin price equivalence

The current value of a statiCoin is equal to the current exchange price, even though the amount of ETH is returned on the basis of a one day ahead quote. For example, to redeem a statiCoin borrow some ETH and buy a fraction of fiat every fraction of 24 hours, at the end of which the Minter contact will return approximately the amount of ETH spent. The more frequently the ETH is converted into fiat, the smaller the trading error.

Alternatively, the statiCoin could be sold directly via an exchange without having to melt the coin. If too low a price were offered by the exchange then an arbitrage opportunity would exist. Traders would buy the cheap statiCoin, melt it, follow the trading strategy outlined above and take the difference in profit. Similarly, if the statiCoin were trading too high then statiCoin owners could sell their holdings then buy back a fraction of ETH at a time over the next 24 hours and end up with more ETH than they would have if they melted the coin

VIII. Features

statiCoins and riskCoins have the following features.

- Amount of collateral behind the contract is immediately visible.
- Quick positive or negative spikes have little effect due to the 24 hour averaging.
- All code is open and on chain.
- Coins are fully ERC20 token compliant.
- Coins can be transferred between addresses without having to melt/mint new coins.
- No fees for transfer of tokens.
- Low fee on token creation.
- All statiCoins for a given contract are alike.
- All riskCoins for a given contract are alike.
- statiCoins can be redeemed at any time.
- riskCoins can also be used to short on a particular currency.

IX. Risks - Where this will fail

Define the strke price as

$$K = \frac{S}{E} \tag{3}$$

which is simply the number of statiCoins divided by the amount of ETH. Strike price for riskCoin is the exchange rate where the riskCoin price turns negative. It's the price point above which the ETH stored in the contract can pay all statiCoins in full. If the ETH price is below the strike price then the statiCoins will continue to be paid in full until there is no ETH available in the minter contract. This

[2] For example, lets say the average price for the previous 6, 4 hour periods was $X_1, X_2, X_3, X_4, X_5, X_6$ so the 24 hour price is $(X_1 + X_2 + X_3 + X_4 + X_5 + X_6)/6$. In 4 hours time, the new price will be $(X_2 + X_3 + X_4 + X_5 + X_6 + X_7)/6$ so the difference in price is $(X_7 - X_1)/6$. Imagine we know that $X_1 = 1, X_2 = 2$ up to $X_6 = 6$ but we don't yet know X_7. For the 24 hour average price to decrease, X_7 would have to drop from 6 to 1, which is unlikely.

contract will default if the ETH price stays low (making the riskCoin price zero) for a long period and a large number of static holders melt their coins. This contract offers no protection against extreme devaluations of ETH.

If all statiCoins are redeemed:-

- and the riskCoin price is positive, then contract ETH is shared between riskCoin holders until new statiCoins are minted.
- and the riskCoin price is negative, then ETH given to statiCoin holders until no more ETH is available.

The value of a statiCoin will only reduce when the ETH price has been below the strike price for a long period of time, and a large proportion of static holders have already melted their coins.

If all riskCoins are redeemed then statiCoins are returned at the exchange rate when the last riskCoin was withdrawn.

When the amount of ETH in the contract reaches 0, the contract creates a bankruptcy event, destroying both static and riskCoin contracts. On bankruptcy, all coins for that currency are destroyed.

Due to statiCoin's reliance on data outside the Ethereum blockchain, this contract cannot be considered to be truly decentralized. Prices will be incorrect if the Kraken API reports erroneous prices via their API. If this were to recur regularly then the Pricer contract would be changed to refer to a more reliable data source. When Oraclize encounters an error in the URL it returns a blank value to the Pricer contract. In this case the last correct price is used to calculate the value to return.

X. Show me the money

This project does not require an ICO or any initial backers. External investment is used to back the promises of both coins. The users of the contract are both it's customers and investors. No "stability fee" or interest charge is made for transacting with or issuing statiCoins. Conversely, no dividends are paid to riskCoin holders, so the only form of benefit for riskCoin holders is the possible return of a greater amount of ETH when the riskCoin is melted at a future point in time at a (hopefully) higher price.

Where is the profit for GENKI? Basically, there is none. To cover setup costs and marketing the Pricer contract charges a fee for each static or risk coin minted. Initially this will be 0.2% , but this is likely to reduce as competitors enter the market. This fee also ensures that GENKI has a long term interest in monitoring the statiCoin contracts to make sure they are healthy (i.e. a suitable blockchain oracle is used and web feed price source is correct). No fees are paid when melting a coin, ensuring that coins are redeemed for their full value.

GENKI will be providing additional solutions based upon the statiCoin contracts as well as consulting services.

XI. Contract structure

Full source code is available at github.com/genkifs/staticoin and on Etherscan. A testnet version is available on Kovan.

i. statiCoin

This contract creates a standard ERC20 token with unlimited issuance. The contract holds the total number of coins issued and the amount given to each address. Sending ETH to this contract will trigger the fallback function to generate a statiCoin.

ii. riskCoin

This contract creates a standard ERC20 token with unlimited issuance. The contract holds the total number of coins issued and the amount given to each address. Sending ETH to this contract will trigger the fallback function to generate an riskCoin.

iii. Minter

This contract gives permission to the statiCoin and riskCoin contracts to mint and melt coins, calculates the amount of coins to mint and the amount of ETH to return, depending on the price provided by the Pricer contract. All Ether that is backing the coins is stored in this contract. The Freeze function halts all execution of the contract and lets all holders redeem their coins at the last known exchange price which is fixed indefinitely. If there is not enough ETH to support all claims at the given price and time then claims are paid pro-rata. Theoretical riskCoin prices can be queried using current issued quantities and user defined amounts.

iv. Pricer

Pricer contract is designed to be upgradable by GENKI. A new Pricer contract will be created whenever the pricing URL changes or if a better method of administrating the contract becomes available. There is a delay of 2 days after the address of the Pricer contract has been changed to allow users to withdraw their funds if they disagree with how the new Pricer contract is constructed. This removes the need to place trust in GENKI as owners of the contracts.

XII. Mathematical Features

As the price of riskCoins is dependent on the number of statiCoins and the number of riskCoins, it is important to show that adding or removing either statiCoins or riskCoins will not change the price of riskCoins. Users cannot affect the current price of riskCoins so there is no dependence on the management of an outside party in these contracts.

i. Same price if adding statiCoins

Define $E_S = \frac{S}{X}$ as the total ETH attributable to S and $E_R = \frac{RY}{X}$ as the total ETH attributable to R, so $E = E_S + E_R$.

Sum of all ETH is the number of statiCoins, divided by the ETH price plus the number of riskCoins divided by the riskCoin price.

$$E = \frac{S}{X} + \frac{RY}{X}$$

Now, let's increase the number of statiCoins by an amount ΔS.

$$\begin{aligned}
\hat{S} &= S + \Delta S \\
\hat{E} = \hat{E}_S + E_R &= \frac{S + \Delta S}{X} + E_R \\
&= E_S + E_R + \frac{\Delta S}{X} = E + \frac{\Delta S}{X}
\end{aligned}$$

Inserting into eq:(1)

$$\begin{aligned}
\hat{Y} = \frac{\hat{E}X - \hat{S}}{R} &= \frac{(E + \frac{\Delta S}{X})X - \hat{S}}{R} \\
&= \frac{EX + \Delta S - S - \Delta S}{R} = Y
\end{aligned}$$

So because $\hat{Y} = Y$ this shows that increasing the number of statiCoins doesn't effect riskCoin price.

ii. Same price if adding riskCoins

Similar algebra can be performed when increasing the quantity of riskCoin by ΔR.

$$\begin{aligned}
\dot{R} &= R + \Delta R \\
\dot{Y} &= \frac{\dot{E}X - S}{\dot{R}} \\
\dot{E} &= E_S + \dot{E}_R \\
&= E_S + \frac{(R + \Delta R)Y}{X} \\
= E_S + E_R + \frac{\Delta RY}{X} &= E + \frac{\Delta RY}{X} \\
\dot{Y} &= \frac{(E + \frac{\Delta RY}{X})X - S}{\dot{R}} \\
\dot{Y} &= \frac{EX + \Delta RY - S}{R + \Delta R} \\
\dot{Y}(R + \Delta R) &= EX - S + \Delta RY \\
= YR + \Delta RY &= Y(R + \Delta R) \\
\dot{Y} &= Y
\end{aligned}$$

Again, as $\hat{Y} = Y$ this shows that increasing the number of riskCoins does not effect riskCoin price.

XIII. Other stable coin approaches

i. Backed by off chain fiat

Banks (e.g. [Santander]) can issue tokens on the Ethereum network that are backed by real assets held off chain by each institution. One approach involves backing each token, one for one, with actual fiat (in which case regular off chain auditing is required). Unfortunately, according to the [Financial Times] "the hoarding of cash creates a host of other costs. Part of it is storage and transport, though they are not the biggest problems. [...] Bank robbers, earthquakes and other unforeseen disasters, on the other hand, are a problem. Or rather, the delicate issue of finding an insurer willing to take on those risks while charging a reasonable fee. [... The estimated annual insurance cost] would probably be between 0.5 per cent to 1 per cent of the value of the banknotes being stored. "

ii. Backed by balance sheet

Balance sheet backed tokens are equivalent to buying unsecured, 0% interest bonds from the issuing institution, with the same level of credit risk. If the issuer were to go bust then the tokens would be worthless.

iii. Central bank issued

This would be the ideal solution to having a fiat asset on the block chain. Digital tokens issued by a central bank through the Ethereum blockchain would have the same legitimacy as the paper and metal tokens they currently issue without credit risk. Unfortunately central banks do not seem willing to issue on a public blockchain at this point in time (and are more likely to pursue their own solutions [coinspeaker.com])

XIV. Ethereum stable tokens

Ethereum already has various stable offerings. The following shortlist is non-exhaustive.

i. Decentralized Capital

Decentralized Capital's tokens are backed by off chain fiat, charging a 0.2% transaction fee for both creating and destroying tokens and 0.3% for withdrawing from dapps. Ironically, given their name, Decentralized Capital's solution still requires centralized custodians for their capital.

ii. Digix

Digix is an asset-tokenisation platform built on Ethereum issuing Digix Gold Tokens (DGX), a gold-backed token for Ethereum. using smart contract deployment to switch between physical gold bullion and tokens in the EIP20 standard. It suffers from similar problems as off chain fiat, regarding holding costs. The stability of DGX is relative to gold which, in fiat terms, is not a stable asset.

iii. Maker

Makerdao seeks to minimize the price volatility of its own stable token, the Dai, against an international basket of currencies. Unfortunately the Dai does not provide stability against individual currencies (such as US dollars), limiting the appeal to merchants. Dai holders are also charged a stability premium to pay for bankruptcy insurance, making the Dai a depreciating asset which, by definition, is not stable. Their Collateralized Debt Positions (the risk takers of the Dai token) are not fungible with one another.

iv. Governments

Although [Singapore] used the Ethereum protocol to implement the blockchain trial for their financial system, it was via a private network which was incompatible with the public Ethereum implementation.

XV. Non-Ethereum stable cryptocurrencies

Other blockchains are attempting to create stable tokens with varying degrees of success, but these solutions suffer from the drawback that they cannot be used within the Ethereum ecosystem.

i. Bitshare

Bitshare provide market-pegged assets, such as the bitUSD, which are crypto tokens that trade for "at least the value of their underlying asset", e.g. $1. These stable assets are backed by Bitshares, which are also used to pay the proof of stake miners of the Bitshare network. The Bitshares holder can "insure" a bitUSD position by maintaining a 300% of the position in his exchange account, and a margin call will be forcibly executed should the holdings be reduced to 200% or less. [Bitreview] note that there is no guarantee that a user will find someone willing to pay a dollar for a bitUSD, either due to market forces or lack of liquidity.

ii. Tether

Tether is a bitcoin based, fiat backed technology, providing a token with a one to one ratio with the underlying (i.e. one Tether=USDT is one US dollar) by holding on deposit the corresponding fiat currency. Tethers may be redeemable/exchangeable for the underlying fiat currency or for the equivalent spot value in Bitcoin[3]. A fee of 0.1% is paid on both deposits and withdrawals, giving a round trip fee of 0.2%.

iii. NuBits

The NuBits price is ultimately controlled by the quantity of NuShares in circulation. When demand for NuBits increases, raising the price vs the US dollar, NuShareholders introduce new NuBits into circulation on an exchange. When demand falls the supply of NuBits can be reduced by holders of NuBits volunteering to take their currency out of circulation in exchange for a monetary incentive. Overall this mechanism ensures stability although from April 2016 to September 2016 the NuBit/US dollar price fell drastically below parity.

XVI. Legal

TLDR: Use at your own risk.

The coins issued by the contracts are not legal tender and are in no way to be used to replace, substitute or imitate any existing fiat currency. Coins are not to be issued to entities residing under regulatory regimes prohibiting ownership or usage. Use of these contracts is at the owners risk. Genki cannot be held responsible for any damages, costs, expenses, anticipated savings, losses, errors, taxes, third party transactions, fees or delays encountered when interacting with these contracts. Genki is not responsible for any problems that may result from the use of your internet connection, our website, the Ethereum platform, Kraken.com, Oraclize.it, or any problems arising from the Ethereum code. Dissatisfaction with any goods or services purchased from, or sold to, a third party must be resolved directly with that third party. The contracts are provided as is and without any representation of warranty, whether express, implied, or statutory.

The limitations of liability of these contracts are agreed by the parties on the basis that the user is aware of the volatility of the foreign currency and Crypto currency markets. Genki reserves the right to amend, change, add, remove, or alter portions of the above text.

References

[coinspeaker.com] ZHANNA LYASOTA. (2015). Bank of England Says Central Banks Consider Using Blockchain Technology coinspeaker.com/2015/07/21/banks-interested-bitcoin-technology-blockchain-10849/ *coinspeaker.com*,JULY 21ST, 2015 .

[Financial Times] Claire Jones and James Shotter. Banks look for cheap way to store cash piles as rates go negative ft.com/content/e979d096-5fe3-11e6-b38c-7b39cbb1138a *ft.com*, AUGUST 16, 2016 .

[Santander] Ian Allison. Santander and EtherCamp building bridges between bank accounts and Ethereum

[3] Although this is not clear from the small print

ibtimes.co.uk/devcon2-santander-ethercamp-building-bridges-between-bank-accounts-ethereum-1582242 *ibtimes.co.uk*, September 20, 2016 .

[Singapore] Anthony Coggine. Singapore Central Bank to Use Blockchain Tech for New Payment Transfer Project cointelegraph.com/news/singapore-central-bank-to-use-blockchain-tech-for-new-payment-transfer-project *cointelegraph.com*, June 09, 2017 .

[Bitreview] David M. bitreview.com/altcoin/bitshares *bitreview.com*, May 24, 2015.