Decentralized Fiat Currencies

Part 1: Price Consensus

jl777 | 5th Aprl, 2017 | v1.0

Abstract: A bridge between the old centralized and the new decentralized financial infrastructures will help accelerate blockchain adoption. It is possible to create decentralized fiat payments by creating a decentralized cryptocurrency that is pegged to local currency. The pegged fiat currency is automatically converted into another cryptocurrency that has market value. The prices are recorded on the Komodo blockchain, and all the nodes use the information to maintain a universal price consensus of each fiat currency.

Introduction

Decentralized Fiat Currencies (DFC) are cryptocurrencies that are pegged to a local currency. People feel confident about using their national currencies, and DFC gives us the means to integrate the most used forms of exchange into the blockchain infrastructure.

The aim of DFC is not to create financial instruments for speculation, but rather to provide something that is stable in value, easy to relate to and understood by a typical user. It is much more like a currency exchange service than a fully fledged forex market.

The technology behind DFC needs two other innovations called delayed Proof of Work (dPoW) and an atomic cross-chain swap protocol (DEX) as well as the Komodo blockchain. This document assumes that the reader is already familiar with the dPoW whitepaper and the DEX paper. The dPoW will be used to make the DFC chains secure, and the DEX will be used to enable atomic cross chain trading of the DFC chains.

There needs to be consensus on prices and a secure way to deposit and redeem. Additionally, there needs to be a way to ensure that the peg will hold or at least have predictable behavior even under extreme conditions.

Price Consensus

The European Central Bank (ECB) provides a reliable price feed service that is used by numerous financial services around the world. However, the price feed must be smoothed out to remove certain attack vectors. Furthermore, there is no price feed during the weekends or other times when the markets are closed.

The nodes can achieve a consensus about the price through the ECB daily price fix. A standard four entry splines, which are smooth polynomial approximations, are created from recent price points. To cover the weekend, when there are no ECB prices, three data points are projected from the Friday price point based on differentials from the prior days.

Given a set of currencies, it will provide prices against all the other currencies. These price pairs are put into a matrix, and the matrix is processed to create a set of normalized values with the property that the ratio of the normalized values map to values that are close to all the input prices.

While all the nodes could maintain and generate these splines and normalized values, with the dPoW implementation, the notary nodes (which are generating most of the blocks) encode the prices into the mined block using OP_RETURN. Small variations of spline values are converted to uint32_t which are billion times normalized values. A fully decentralized price feed can also be implemented just by having each node maintain the same price feed data.

The initial implementation supports the price feed for 32 fiat currencies:

```
"USD", "EUR", "JPY", "GBP", "AUD", "CAD", "CHF", "NZD", "CNY", "RUB",
"MXN", "BRL", "INR", "HKD", "TRY", "ZAR", "PLN", "NOK", "SEK", "DKK",
"CZK", "HUF", "ILS", "KRW", "MYR", "PHP", "RON", "SGD", "THB", "BGN",
"IDR", "HRK",
```

Each of these produces a 32bit value per price feed entry, so with 128 bytes per sample, 1024 price pairs can be generated. That is effectively 1 bit per price. The base/base price is converted to the proportional M1 percentage among the 32 currencies. As such it represents

the percentage of overall normalized M1 market capitalization each currency represents. By tracking the change of this, the shift in a currency's overall value is tracked.

In addition to the ECB's price feed, price points for BTC-USD, KMD-BTC, and BTC-CNY are monitored. With them, the exact conversion of any currency to KMD can be calculated.

DFC Deposit & Redeem

Now we have a decentrally maintained price feed that is recorded on the Komodo blockchain, and next, we can develop a deposit feature. Through the deposit, a Komodo coin (KMD) can be automatically converted into a decentralized fiat currency.

By using the ECB's price feeds, and the price feeds of BTC-USD, KMD-BTC, and BTC-CNY, at any given height, the exact conversion of any currency to KMD can be calculated, and the DFCdeposit function can be created:

```
DFCdeposit <destaddress> fiatamount currency
```

The above will start the deposit process into the currency's assetchain that matches the fiat amount. The specific method is by burning the calculated amount of KMD using OP_RETURN. All the currency assetchains monitor the KMD blockchain for the DFCdeposit OP_RETURN and update a queue of pending deposits. The assetchains are idle and don't mine blocks until there are transactions to process in the memory pool or a pending deposit. The fiat amount of the currency assetchain is then created in a coinbase transaction after the DFCdeposit transaction is notarized.

In redeeming process the locked away KMD is resurrected. A DFCwithdraw function is used to redeem the fiat:

```
DFCwithdraw <destaddress> fiatamount
```

The KMD corresponding to the fiat amount is issued in a KMD coinbase as the assetchain withdraw is notarized.

An alternative method is to use the SuperNET's atomic cross-chain protocol and liquidity provider (LP) nodes to redeem the fiat value. In this approach, the fiat currency could be exchanged straight into BTC.

Thus we can construct 32 fiat cryptos with properties very similar to bitcoin, both from the security and transactional point of view.

Placed Restrictions and Transition Period

The development of DFC is split between two phases: DFC1 and DFC2. The first release is a proof of concept, and its total exposure is capped at a few million KMD. The first use cases focus on short term fiat denominated transactions with a relatively high velocity of money.

The market capitalization of a decentralized fiat currency is somewhat limited by the KMD market capitalization because KMD is used to make DFC deposits. The DFC market cap can be safely increased to be about one percent of KMD's market cap. The amount of max exposure can be increased as the KMD market cap grows.

Through the next DFC2 phase certain advanced financial instruments will be integrated with the pegged fiat currencies. The new phase will make it resistant to extreme price volatility, and thus allows us to remove the maximum exposure limitations. All in all the difference

between DFC1 and DFC2 is technically quite small as most of the fundamental operations are already in DFC1. The DFC2 will be described in the second DFC whitepaper.

The Bridge Between Fiat and Bitcoin

Once the fiat currency is issued into the assetchain, it is a crypto currency and can be used just like Bitcoin. Thus the decentralized fiat currencies can be utilized by online merchants and payment services as fast and secure fiat transactions.

The decentralized exchange in Iguana supports all blockchains generated through assetchains, including decentralized fiat currencies. Through its cross-chain atomic swaps, it is possible to do decentralized fiat to fiat forex trading.

DFC doesn't need any DFCEUR gateways as DFC converts to KMD which can, in turn, be traded to BTC. All we need are BTC <-> EUR gateways and a liquid KMD<-> BTC market. It is possible to utilize the existing infrastructure, such as LocalBitcoins and similar services, to allow the decentralized fiat currencies to be sent to a regular bank account.

decentralized fiat currencies accelerate the cryptocurrency adoption by allowing people to pay in their local currency.

Conclusions

The decentralized fiat currencies are independent cryptocurrencies with their own blockchains. Their blockchain is secured with an additional security layer that is provided by the Komodo's delayed Proof of Work (dPoW) consensus mechanism. The price consensus is maintained decentrally by 64 notary nodes, and the DFC prices are recorded on the Komodo blockchain. decentralized fiat currencies can be acquired by automatically converting Komodo coins (KMD) into one of the 32 fiat currencies.

The DFC technology doesn't require a liquid market for the fiat DFC pairs as the conversion is technical, automatic, and thus guaranteed. Only a liquid BTC-KMD market is needed to move funds to the decentralized fiat currencies. Because of these characteristics, the DFC can attach itself to the existing BTC-fiat infrastructure, and no new fiat gateways are required.

Appendix I

From A Price Feed to DFC Price

Below is a detailed step by step description about how the DFC prices are created.

1. All the notary nodes query the daily ECB price data and then convert the price pairs into abstract singleton currency values. These abstract values have the property that the distance from the currencyA/currencyB price and the corresponding ratio of the abstract values are minimized. A matrix of N*N numbers are reduced to N numbers, quite a lot of data space saved.

2. These abstract datapoints are used to create long term splines. Splines are mathematical equations that fit the data points and have the character that the lines are very smooth and change very slowly. A spline can calculate the smooth price at any point inside the range of initial values; it interpolates perfectly.

3. Every block, the spline data is used to generate a price feed entry and if a notary node mines a block, it includes the price feed data. This allows all the non-notary nodes to get the raw price feed data as it is in the KMD blockchain.

The following is done to calculate the DFCprice:

A. The previous 500+ (537) price feeds are put into a circular buffer.

B. A deterministic random seed to randomize the starting point in the circular buffer.

C. Iterate from the zero point to find the first price point that has a 51% correlation, e.g. over half the other data points are within the specified tolerance of 2%. The first price that meets this condition is the correlated price for the height.

D. The previous 537 correlated prices are smoothed using a noise filter, basically, a ‘dotproduct’ that has the property of smoothing the price. It isn’t an average price, but rather a weighted price relative to the initially correlated price point.

E. To sidestep small reorgs, the value for a specific height is changed to be the value of height -10.

The above is how DFCprices are calculated for each block for all the DFC currencies. The DFCprice is what is used to convert from KMD <-> DFC and all nodes arrive at the same DFCprices.

Due to D. a lot of correlated prices have to be distorted for there to be any substantial change in the DFC price.

Due to C, the majority of price feeds must be distorted for any of them even to be selected to be a correlated price

Due to B, it is not possible to predict what the correlated price will be for any future block

Due to 1, if any notary node(s) try to distort the price feed, it is obvious to all that they are conducting an attack.