The Kowala Protocol: A Family of Distributed, Self-Regulating, Asset-Tracking Cryptocurrencies

Eiland Glover and John W. Reitano

Abstract

Cryptocurrencies such as Bitcoin, Ether, and Dash exhibit significant volatility. Consumers, merchants, traders, investors, miners and developers have a need for a cryptocurrency whose value can be counted on to remain roughly stable from one day to the next and whose operation does not depend on potentially unreliable third parties such as banks.

Cryptocurrencies with automated value-pegging mechanisms, such as NuBits and BitUSD, have suffered repeated failures due to malfunction and lack of adoption, while companies that hold centralized, one-to-one reserves in fiat, such as Tether, have proven vulnerable to the whims of banks and governments.

The *Kowala Protocol* is our proposed method for creating a new family of cryptocurrencies which maintain stable values while retaining other benefits of cryptocurrencies, such as decentralization, security, privacy, speed of transfer, and low transaction costs.

Why A Stable Cryptocurrency Is Needed

Beyond the considerable benefits that most cryptocurrencies bring, a stable cryptocurrency will provide unique benefits to many stakeholders, such as consumers, merchants, investors, traders, miners and developers.

Some use cases of a stable cryptocurrency for **consumers** are:

- avoiding cryptocurrency volatility when purchasing real-world products and services;
- avoiding volatility of less stable fiat currencies (such as of those of Venezuela, Zimbabwe, Nigeria, etc)
- providing a stable store of value; and
- gaining access to bank-like services offered by third parties (for consumers without easy access to bank accounts denominated in stable fiat currencies).

Some use cases for **merchants** are:

- avoiding volatility when selling products and services for cryptocurrency; and
- gaining access to bank-like services offered by third parties (for merchants without easy access to bank accounts denominated in stable fiat currencies).

Some use cases for **investors** are:

- parking funds in a decentralized, stable asset.

Some use cases for **traders** are:

- pursuing arbitrage opportunities in new cryptocurrency markets;
- parking funds in a decentralized asset that has stable value; and
- trade in and out of stable asset at low cost and high speed.

Some use cases for **miners** are:

- pursuing mining profits without investing in expensive hardware and electricity costs;
- reaping mining rewards consistently, no matter whose machine solves the block; and
- having the option to sell or lease acquired mining rights.

Some use cases for **developers** are:

- incorporating payment functionality into apps and websites without the need to establish a merchant account; and
- incorporating such payment functionality while avoiding cryptocurrency volatility.

What is the Kowala Protocol?

The Kowala Protocol defines a method for constructing a family of distributed, self-regulating, asset-tracking cryptocurrencies called *kCoins*.

Each kCoin is designed to be traded on open exchanges and to maintain a close to one-to-one value relative to any widely traded asset such as a currency (USD, EUR, JPY, etc.) or other asset. Each kCoin is identified by a symbol consisting of the letter "k" followed by the symbol of the underlying asset. For example, the kCoin of USD is kUSD, that of EUR is kEUR, and so forth.

kCoins constantly gather market information from endorsed sources and regulate their value through three core mechanisms: variable block rewards, variable fees, and an active and well-informed trading market. In time, these mechanisms always return each kCoin to parity with its underlying, tracked asset. The certainty of each kCoin's eventual return to parity, in turn, creates pure arbitrage opportunities for traders seeking to profit from slight fluctuations in kCoin market prices around the peg.

We chose the Ethereum codebase (https://github.com/ethereum/go-ethereum) as the starting point for the development of kCoins in order to access both Ethereum's strong feature set (especially its sophisticated smart-contract facilities) and the collective abilities and ongoing efforts of its development team. On top of this foundation, each kCoin adds the value stabilization and market observation features described above. Because every kCoin needs a robust exchange market to function properly, each kCoin is implemented as a distinct, independent blockchain with its own tokens, smart contracts, mining community, etc .

Note: The discussion below applies to any kCoin, but, for ease of explanation, we will use the specific example of kUSD—the kCoin pegged to the U.S. dollar—in most of the remainder of this whitepaper.

Overview of Core Mechanisms

At its core, the Kowala Protocol consists of three mechanisms that keep the market price of kUSD at or very near $1.

The section *Mechanism 1: Block Reward Algorithm* below describes how a variable block reward is used to push the market price toward the target of $1 when necessary.

The section *Mechanism 2: Stability Fee* describes how, in the scenario in which the market price is below $1 and the block reward algorithm is not sufficient to bring it back to $1, a special, variable fee is applied to each subsequent transaction until the market price begins to rise.

The section *Mechanism 3: Trading Activity* describes how traders, informed by the previous two mechanisms and motivated by a desire for profit, are expected to engage in trading activity that accelerates the return of the market price of kUSD to $1.

Kowala Roles

Kowala will function as a transparent and reliable entity to perform the following functions:

- publish approved exchange APIs to guard against the malfunction or hijacking of the exchange APIs themselves;
- publish summary statistics on kUSD market activity, such as price history, trading volumes, block rewards, etc.;
- pursue technical development of the Kowala Protocol;
- publish information about about the Kowala Protocol to a wide audience; and
- conduct ongoing basic research on kCoins including extensive agent-based modeling.

The Kowala board of directors will govern Kowala based on the principles of financial transparency, accessibility, and wide adoption. Kowala is a Cayman exempted company and wholly-owned subsidiary of Kowala, Inc., a Delaware corporation.

Mechanism 1: Block Reward Algorithm

To calculate the block reward, we will need to introduce four new concepts.

The first concept is a *dead-end address*, which is a wallet address that is precluded from having outbound transactions and thus whose balance can increase but not decrease.

The second concept is the *available coin supply*, which is the total value of all coins that are available for sending via transactions; formally this is defined with the following function:

$$availableCoinSupply(b) := totalCoinSupply(b) - \sum_{d \in D} balance(d, b)$$

where `totalCoinSupply(b)` refers to the total number of coins issued as of block number b, D is the set of all dead-end addresses, and `balance(d, b)` is the balance of dead-end address d as of block b. In other words,, the available coin supply is the total number of sendable coins.

The third concept is the block reward cap, `cap(b)`, which is defined as:

$$cap(b) := max(0.0001 \times availableCoins(b-1), 82)$$

The fourth concept is the *market price of* kUSD, which is based on information gathered from certain recent transactions, which we call p*rice-determining transactions* (see *Price-Determining Transactions* below). The market price, `p(b)`, is defined as:

$$p(b) := \frac{\sum_{t \in T(b)} P_t V_t}{\sum_{t \in T(b)} V_t}$$

where $T(b)$ is the set of price-determining transactions for block b, $P(t)$ is the price of transaction t, and $V(t)$ is the volume of transaction t. If the price of a transaction is expressed in BTC, it will be converted to a dollar price by using a well-defined determination of the price of in USD of 1 BTC (see *BTC Price* below).

With all these concepts in place, we are ready to define the block reward, reward(b), as:

$$reward(b) := \begin{cases} 42 & b = 1 & (initial) \\ min(1.01r(b-1), cap(b)) & b > 1, p(b) \geq p(b-1) > 1 & (divergent - rising) \\ max(\frac{1}{1.01}r(b-1), 0.0001) & b > 1, p(b) \leq p(b-1) < 1 & (divergent - falling) \\ r(b-1) & otherwise & (convergent) \end{cases}$$

The calculation of the block reward is split into four scenarios: *initial*, *divergent-rising*, *divergent-falling* and *convergent*.

During the initial scenario, which applies only to the first block, the block reward is set to the arbitrary value of 42.

Next, we consider the divergent-rising scenario, which occurs when, over the course of two consecutive blocks, the price of kUSD is over $1 and rising or flat. In this scenario, we set the block's reward to 1% more than the previous block's reward, subject to the block reward cap, which prevents prolonged periods of block reward increase from growing too quickly.

We initially hypothesized that, when large numbers of newly minted coins are earned by miners, a large portion of such coins will reach exchanges as market sell orders and drive down the price of kUSD. A detailed agent-based behavior model with multiple market scenarios supports this hypothesis (see *Agent-Based Modeling* below). For this reason, we posit that for the divergent-rising scenario, no further mechanism is needed to reduce the price to $1.

Analogously to the divergent-rising scenario, the divergent-falling scenario occurs when, over the course of two consecutive blocks, the market price of kUSD is under $1 and is falling or flat. When this happens, the divergent-falling portion of the block reward function states that we should set the block's reward to the the previous block reward divided by 1.01 (subject to a minimum of 0.0001 kUSD).

Repeated applications of the formula in the divergent-falling scenario during a prolonged drop in price can lower the block reward to nearly zero. For example, in this scenario, reducing the block reward from 1 kUSD to 0.0001 kUSD takes only 925 blocks (3.9 hours at 15 seconds per block). However, even a near-zero block reward may not be sufficient to raise the price of the

coin if there is a large drop in coin demand during the same period. In the section *Mechanism 2: Stability Fee* below, we will address this insufficiency by introducing a way to materially reduce the total coin supply.

Finally, the convergent scenario occurs whenever neither of the other three scenarios occur—that is, when $b > 1$ and the price for the current block is exactly at $1 or is closer to $1 than it was for the previous block. In this scenario, we consider that the previous block's reward is working well, so we set the current block's reward to the same value.

Mechanism 2: Stability Fee

The Kowala Protocol specifies that every transaction sender be charged special fee, called a *stability fee*, amounting to a small percentage (ranging between 0.001% and 2%) of the transaction amount; the stability fee is charged in addition to the cost of each transaction's "gas", which is used *to* compensate miners for the marginal cost of processing each transaction. The primary purpose of the stability fee is to reduce coin supply during prolonged periods when the market price fails to recover from a price below $1. Rather than being sent to the miners, the value represented by the stability fee is effectively destroyed by being sent to a dead-end address.

The stability fee should conform to the following constraints:

- under normal conditions, the stability fee is very low when considered as a percentage of the transaction amount (say, less than 0.1%); and
- in the abnormal condition of a prolonged drop in demand for kUSD, the stability fee should still represent no more than 2% of the transaction amount, and should be lowered back down to a minimal value once normal conditions return.

In real-time uses of a payment system, we will also need to define a formula for an *estimated stability fee*, which should conform to the following constraints:

- it is easy to calculate; and
- it is always either equal to or just slightly above the actual fee.

For the purpose of defining the stability fee and estimated stability fee, we will introduce a few functions. First, we define the price change rate, p'(b), as:

$$p'(b) := \frac{241 \sum_{i=b-240}^{b} p(i)i \; - \sum_{i=b-240}^{b} p(i) \sum_{i=b-240}^{b} i}{241 \sum_{i=b-240}^{b} i^2 \; - \; (\sum_{i=b-240}^{b} i)^2}$$

Next, we define the *stability fee rate*, $s(b)$, and *estimated stability fee rate*, $e(b)$, for block b,

which represent a fraction of the transaction amount:

$$s(b) := \begin{cases} 0.00001 & b = 1 \\ s(b-1) & b \, mod \, 240 \neq 1 \\ min(1.023 s(b-1), 0.02) & b > 1 \,\&\, b \, mod \, 240 = 1 \,\&\, reward(b-1) = 0.0001 \,\&\, p(b) < 1 \,\&\, p'(b) <= 0 \\ max(\frac{1}{1.023} s(b-1), 0.00001) & otherwise \end{cases}$$

$$e(b) := \begin{cases} min(1.023 s(b), 0.02) & b > 1 \,\&\, reward(b-1) = 0.0001 \,\&\, p(b) < 1 \,\&\, p'(b) <= 0 \\ s(b) & otherwise \end{cases}$$

With these new functions defined, we are now ready to define the stability fee and estimated stability fee for block *b* and transaction *t* using the following formulas:

$$stabilityFee(b,t) := s(b) Amount(t)$$

$$estimatedStabilityFee(b,t) := e(b) Amount(t)$$

where *Amount(t)* is the amount of kUSD being sent in transaction *t*.

Our modeling shows that the stability fee is applied infrequently in anticipated market conditions, but is effective in raising the price of kUSD when applied (see *Agent-Based Modeling* below).

Mechanism 3: Trading Activity

Given sufficient time, the first two mechanisms above will cause the price of kUSD to revert to parity (i.e., 1 USD per kUSD). We label this tendency to revert to parity the *first-order effect* of the Kowala Protocol. Once the first-order effect has become recognized among market participants, we then expect several *second-order effects* to come into play.

First, since the parity price is the only particular price to which kUSD has a natural inclination to return, it constitutes a game-theoretic focal (or Schelling) point. The absence of perfect communication and trust among disparate human market participants along with the status of the parity price as a focal point increase the likelihood that the price of kUSD will return to parity.[1]

Second, whenever deviations of the price from parity do occur, they will give rise to short-term profit opportunities for professional arbitrageurs. The source of these opportunities is the difference between the time horizon of relatively patient arbitrageurs and that of other market participants for whom the short-term need to move into or out of kUSD exceeds concern over these price deviations. Although arbitrageurs may exploit these profit opportunities purely for

[1] See https://en.wikipedia.org/wiki/Focal_point_(game_theory)

self-interest, their trading activity has the positive effect of accelerating the return to parity.

Third, confidence in the reversion to parity will strengthen further as participants observe a history of such reversion in the marketplace.

All of these second-order effects depend on the existence of a well-functioning USD/kUSD (or equivalent BTC/kUSD) exchange market. Since the existence of such exchange markets are in the interest of exchanges, miners, and users of kUSD, it is highly likely that they will arise through the self-interested activities of these groups.

Kowala will continually improve the Kowala Protocol, provide tools to software developers, and make full and detailed information on the Kowala Protocol's mechanisms available to the public so that users and arbitrageurs may develop their own trading strategies.

For its part, Kowala plans to participate in independent, open-market, profit-seeking trading activities based on the same information publicly available to all.

Price-Determining Transactions

A transaction is considered a *price-determining transaction* for block b if it satisfies all of these requirements:

- It includes a price, expressed in BTC or USD.
- It includes a transaction amount, expressed in kUSD.
- It includes a transaction completion time (expressed in seconds since the epoch in UTC).
- The transaction completion time is on or before the creation time of the previous block (block $b - 1$) and after the creation time of the block that is two blocks back (block $b - 2$).
- It is published as a market transaction of USD for kUSD or Bitcoin for kUSD on an exchange whose API is endorsed by Kowala (see Endorsement API's below).

The price-determining transactions are used to calculate the market price of kUSD mentioned in the section *Mechanism 1: Block Reward Algorithm* above.

BTC Price

The calculation of BTC Price in USD, $btc(b)$, is based on the volume-weighted average of the price published by well-known exchanges that trade USD/BTC. Only those exchange APIs that are included in the BTC Price Endorsement API (see *Endorsement APIs* below) will be used in this calculation.

Endorsement APIs

Kowala will maintain two endorsement APIs to counter exchange API malfunction or hijacking:

- *Exchange Endorsement API*: This API will indicate to the mining clients which of the currently implemented exchange APIs should be used when calculating block rewards and fees.
- *BTC Price Endorsement API*: This API will indicate to the mining clients which of the currently implemented BTC price APIs should be used in calculating block rewards and fees.

Mining Sectors & mTokens

Before the launch of kUSD, 2^{30} (1,073,741,824) unique tokens (called *mUSD*) will be generated to facilitate the allocation of kUSD mining rewards. The kUSD client software (or an associated smart contract) will prevent additional mUSD from being created in the future.

As with Ethereum, the block hash space for kUSD blocks is the set of integers 0 through 2^{256} - 1. The Kowala Protocol specifies that this space be partitioned into 2^{30} *mining sectors*, and that the mUSD be associated on a 1-to-1 basis with these mining sectors in a smart contract-based database. The mining sectors are used in the Proof-of-Control mechanism described in the next section.

In addition to being associated with a mining sector, each mUSD will also be associated with cryptographic addresses and other meta-information used to securely manage ownership, delegation of mining responsibilities to third parties, and the recipient address for block rewards.

Just as kUSD is mined using mUSD, other kCoins will be mined using their own corresponding sets of tokens, generically referred to as mTokens. For example, kEUR will use mEUR, kGBP will use mGBP, etc.

Proof-of-Control

To reward early participants in kUSD and to avoid the wasteful use of large amounts of electricity for crypto-mining, the Kowala Protocol allocates block rewards not by proof-of-work or proof-of-stake, but by a novel mechanism we call proof-of-control (PoC).

In PoC, the owner of an mUSD holds the exclusive right to mine within the associated mining sector. To exercise this right, miners register their mUSD in a block reward roster by cryptographically proving that they control the private keys associated with the ownership addresses of their mUSD. When a potential new block is generated and a corresponding

solution found via mining, a block hash is mapped to its containing sector, which is then mapped to the associated mUSD. Only if this mUSD is registered in the block reward roster will the block solution be submitted to the network and the block reward awarded to the recipient address associated with the mUSD. The owners of mUSD may perform their mining contributions either directly or by contracting with third parties to mine on their behalf.

Note that PoC requires owners of mUSD not merely to prove their ownership, but also to actively contribute to the network by mining (i.e., solving block hashes). Thus the block rewards that miners receive are due only to their own efforts, not to the efforts of others.

Reduced Energy Usage

Because each miner has exclusive rights to receive rewards within its territory, there is no incentive for miners to use powerful, energy-wasting mining hardware to outperform their fellow miners. This approach provides security by distributing blockchain validation-by-consensus across many independent parties (because only active miners receive block rewards) but uses very little electricity compared to typical cryptocurrency consensus mechanisms. For example, one analyst estimates that there are between 5,000 and 100,000 Bitcoin miners who collectively consume approximately 774 megawatts of electricity.[2] By comparison, we estimate that 100,000 miners of kUSD would use less than 5 megawatts of electricity.

Continuous Agent-Based Modeling

We have created a sophisticated agent-based software model to test the simultaneous use of all three mechanisms that form the Kowala Protocol. We have run a significant number of simulations against various permutations of the model, including:

- variations in constants used by the Block Reward Algorithm
- variations in constants used to define the Stability Fee
- variations in starting conditions
- market demand fluctuations, including mass panics
- rapidly increasing and decreasing numbers of participants
- excessive optimism and pessimism of arbitrageurs and prospectors

The algorithms and constants described in this whitepaper reflect the results of our testing, and the Kowala Protocol incorporates only the behaviors which consistently and reproducibly yielded the best results in our models.

Future agent-based modeling will be based on actual historic market data. Kowala will regularly create large-scale simulations of established marketplace behavior and conduct predictive

[2] See https://bravenewcoin.com/news/number-of-bitcoin-miners-far-higher-than-popular-estimates

research into further refinements to the Kowala Protocol. These enhanced simulations will feature agents whose behavior is derived from genetic algorithms informed by actual, historic market decisions. Kowala will also model potential attacks by malicious actors in order to preempt them and to uncover other unforeseen vulnerabilities.

Ownership of mUSD

As mentioned above, before the launch of kUSD, Kowala will generate 2^{30} (1,073,741,824) mUSD, which will be used to allocate mining rewards. These mUSD will be distributed as follows:

1. Up to 10% of the total generated mUSD will be sold to early investors, development team members, and advisors as soon as is practical, in order to raise funds for the development of kUSD;
2. 15% of the total generated mUSD will be retained indefinitely by Kowala; and
3. the remaining 75% of all mUSD will be sold in one or more public token offerings within 12 months of the first sales in part 1 above. Note that owners who acquire mUSD after the kUSD launch will not receive any portions of block rewards generated before the time of acquisition.

In the near future, Kowala also plans to separately launch other kCoins and sell the associated mTokens. These kCoins may include kEUR, kJPY, kGBP, kBTC, and others. A purchase of mUSD does not, in itself, grant the purchaser the right to acquire any of these other kCoins or mTokens.

Leasing of mUSD Mining Rights

For owners of mUSD who do not wish to maintain their own mining equipment, the kUSD client software will allow any mUSD owner to authorize a mining operator to mine on his or her behalf. For such mUSD owners, the operator will likely be paid a fee for performing the kUSD mining, while the mining rewards themselves will be accrue to the mUSD owner's wallet. Kowala will not perform mining on the behalf of mUSD holders.

Current Research Area: PID Controllers

Our approach of continuously incorporating market feedback into our coin-supply adjustments is broadly reminiscent of the concept of a PID-controller, a sophisticated engineering model of goal-seeking action coupled with continuous feedback from a sensor. We are currently investigating the possibility of improving our mechanisms by expressing them as PID-controllers.[3]

Current Research Area: Seigniorage Shares

Though developed independently, our approach to coin supply management is similar in its goals to to the approach recommended by Robert Sams in his paper "A Note on Cryptocurrency Stabilisation: Seigniorage Shares". [4] We are currently investigating how to incorporate some of the ideas in Sams' paper into our model, particularly the idea of using a Schelling competition to provide decentralized, trustless-yet-trustworthy information on current asset exchange rates.

Conclusion

This whitepaper has identified the problem of volatility in cryptocurrency and proposed the Kowala Protocol as a robust solution to this problem. Although we have established through extensive modelling that the protocol works in many anticipated scenarios, more work is needed to demonstrate with higher certainty that the specific mechanisms described here will work in a real-world market. We invite others to contribute to improving the Kowala Protocol by visiting https://kowala.tech and to participate in the development of the kUSD client software located at https://github.com/kowala-tech/kUSD.

[3] See https://en.wikipedia.org/wiki/PID_controller, http://www.eurotherm.com/temperature-control/principles-of-pid-control-and-tuning, and http://www.eurotherm.com/temperature-control/pid-control-made-easy.

[4] See https://bravenewcoin.com/assets/Whitepapers/A-Note-on-Cryptocurrency-Stabilisation-Seigniorage-Shares.pdf.