in the currency fall. Rational behavior would be to use such currencies as a store of value rather than a medium of exchange, and in practice that is what has happened.

Stable-value cryptocurrencies would bring a number of benefits to the cryptocurrency ecosystem. For one, stable prices remove a considerable barrier for using cryptocurrencies as a medium-of-exchange; salaries, prices of goods, fixed obligations, can all be set in a stable value cryptocurrency without requiring either party to speculate on the future value of the currency. Further, financial contracts are more easily built with a stable value coin, because the issuer can separate the function of the contract from the price risk of the currency in which it's denominated.

While a single stable-value currency would be helpful, a thriving cryptoeconomy is best-served by a family of stable-value currencies, much as it is well-served by the family of variable-value crypto-assets that we have today. Certainly a cryptocurrency pegged to the US Dollar has several uses, from social payments in the US, to user-initiated dollarization in hyper-inflationary markets, to the efficient settlement of high-frequency crypto-asset trades. At the same time, a cryptocurrency pegged to the Euro would also be useful for many purposes, as would a cryptocurrency pegged to the price of a basket of goods in Greece, as would a cryptocurrency pegged to the price of a barrel of oil, or housing in San Francisco. Stable-value local, regional, and utility currencies allow people to hedge price risk in their lives by denominating a portion of their personal economy in currencies that are stable vis-a-vis the price of the goods they regularly use.

## 3.1 Elastic Coin Supply and Shifting Volatility Risk

Several protocols have been proposed for a decentralized stabilized value cryptocurrency (for example [17, 2, 1, 19]). While a full review of these proposals is outside of the scope of this paper, they generally share two properties. First, rather than a deterministic coin supply rule (in which the coin supply and growth rate are determined in advance, independent of exogenous information), they each introduce an elastic coin supply rule, that stabilizes the value of the coin by adjusting the supply of the coin to match the demand. Second, they each introduce a multi-asset ecology, in which one coin is intended to be stable, while one or more complementary crypto-assets bear the risk of a decrease in stablecoin demand (and receives a reward in the case of an increase in stablecoin demand). In essence, they each shift volatility risk from the coin holders to the complementary asset holders.

The Celo protocol utilizes the same two key intuitions, with five novel features: (a) it introduces a multi-asset tiered reserve that supports several local and regional stable value currencies, (b) it sets expansion and contraction parameters that are tuned to the reserve ratio defined by the tiered reserve, (c) it introduces a decentralized exchange in which the different local and regional currencies and the reserve currency can be traded amongst one another without a central party, and that the protocol can use to perform expansions and contractions, (d) it releases block rewards and other incentives in the reserve currency, and (e) it has a governance mechanism in which long-term stakeholders in the reserve currency are responsible for governing the assets held in reserve and the new local currencies that are introduced.

## 3.2 Protocol Summary

At a high level, the protocol proceeds as follows:

1. The protocol establishes a fixed supply of assets, called Celo (also referred to as the Celo native asset), a portion of which is distributed over time. From the initial asset distribution, a portion is placed in reserve and diversified.

2. The protocol also establishes a means-of-payment currency, called the Celo Dollar, that is intended to be pegged roughly to the US Dollar, that adheres to the following elastic coin supply rule:

   When coin supply needs to expand (when the price of Celo Dollar is above the peg), the protocol creates new coins, as in [17, 1, 2]. But rather than distributing them to token holders, it uses