Reserve Stabilization Protocol

Prior to the full implementation of the Reserve protocol, the Reserve core team may publish updates to this white paper, even *substantial* updates. It is therefore subject to correction, completion and amendment without notice. Please visit reserve.org for the most up-to-date documentation of the Reserve protocol.

Taylor Brent, Daniel Colson, Matt Elder, Henry Fisher,
Nevin Freeman, Jesper Östman, Elizabeth Van Nostrand

Last updated: May 15, 2019

The volatility of existing cryptocurrencies significantly reduces their usefulness. A cryptocurrency with stable value would permit much wider usage as a stable store of value, medium of exchange, and standard of deferred payment. Demand for a short-term and long-term stable cryptocurrency is obvious. The feasibility of implementing one is not—clear flaws can be demonstrated with many recently proposed designs [1][2][3]. In this paper, we present arguments for why such a coin should implement an exchange-rate peg to a fiat currency first and a basket of assets later, using off-chain foreign collateral that has been tokenized by a diversity of issuers. We then describe the Reserve Protocol, a decentralized stablecoin system that scales supply with demand and is built to maintain 100% or more on-chain collateral backing. This design strikes a careful balance between stability, decentralization, and profitability while supporting arbitrary increases or decreases in demand. For these reasons, we believe the Reserve to be the ideal economic building block for the blockchain ecosystem and a credible alternative to fiat money.

Contents

1 Introduction

Cryptocurrencies have the potential to massively upgrade the effectiveness of money worldwide. They can be sent nearly instantly to anyone anywhere in the world, can't be diluted or devalued by irresponsible governments, and can be programmed to operate inside of financial contracts that rely on code instead of law—each of which is *independently* a major improvement over fiat money. Cryptocurrencies have recently been top-of-mind for consumers, investors, and regulators around the world. Why, then, have they not been adopted?

In addition to technical impediments that are on track to being solved, cryptocurrencies like bitcoin and ether have been highly volatile in market valuation. Their volatility discourages merchants and consumers from using them as a medium of exchange or store of value. Put simply, nobody wants to spend a currency that may be worth twice as much in a month, and nobody wants to store their retirement savings in a currency that may be worth nothing in a year.

Their volatility also prevents them from serving as a standard of deferred payment. Anyone who negotiates rent, wages, or loans in a currency lacking a stable value is unavoidably also speculating on that currency's future purchasing power. Relying on a volatile currency for such needs introduces unnecessary risk and makes it more difficult to coordinate effectively [4].

2 The Opportunity for Stable Cryptocurrencies

Unleashing a fully functional cryptocurrency will be similar to releasing smartphones for the first time. Holding an iPhone, you could tell that mobile browsing was going to be a lot better, but no one predicted that within a few years there would be massive networks of non-professional drivers roving around picking up strangers and taking them wherever they wanted to go. Uber just wasn't what you thought of when someone said "app" in 2007. Similarly with cryptocurrency, while several applications of the technology are clear, it's equally clear that as many or more applications will be a surprise. Money is the most basic platform for commerce, and cryptocurrency is poised to be the most functional and least restricted form of money we've ever invented.

2.1 Growing the Cryptoasset Ecosystem

To start, we can already see the massive uptake of asset-backed stable cryptocurrencies as a means of exchange in the world of cryptoasset trading. Tether is the largest stable cryptocurrency at the time of this writing, with between $1 and $2 billion in market cap [5]. Tether's daily trading volume is often about 100% of its market cap, so even excluding on-chain transactions, it has an annual velocity of 300-400. More notably, Tether has achieved this level of success despite an enormous amount of distrust—while many market participants are happy to include Tether in their short-term trading plans, very few are willing to hold onto it for significant periods of time. This gives many the false impression that stablecoins are a smaller piece of the puzzle than they are. In our

view, a trusted stablecoin has the potential to not only de-risk our ecosystem's primary means of exchange, but to act as a store of value in its own right.

More fundamentally, a stable cryptocurrency is clearly needed for any significant distributed app economy to develop. While holding a different volatile token for every dApp may appeal to speculators, it's simply too cumbersome for normal users. It may be difficult to take this use-case seriously—low transaction throughput makes a flourishing dApp ecosystem seem far fetched—but there's good reason to expect change. Just as faster internet speeds brought about apps that would be impossible with dial-up internet, higher transaction throughput will enable us to build dApps that are currently completely infeasible. In the long run, we believe distributed apps will range from recreational (e.g. irrevocable digital asset ownership inside of games) to mission-critical (e.g. automated compliance and settlement for multi-billion-dollar tokenized financial products).

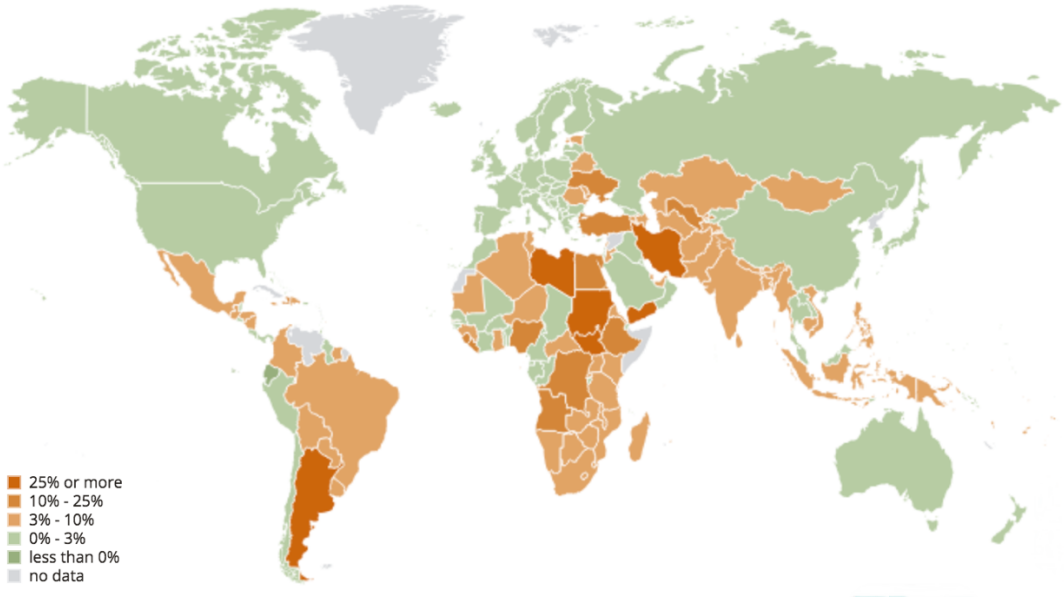
But even before distributed app technology has reached any notable level of adoption, the cryptoasset industry will have good reason to be the first adopter of its own financial technology. Indeed, the primary use case for ether so far has not been gas fees for smart contracts (on the order of 250 million USD so far), but payments in crowdfunding (several billion USD) [6]. We've also noticed a fair amount of commerce happening in bitcoin and ether among various businesses in the industry who don't want to wait around to wire large payments to one another. All of this activity has happened despite ether's volatility and all of the inconvenience that comes along with it.

A cryptocurrency with all of ether's properties but with a reliably stable market value stands to achieve significantly more usage in cryptoasset trading, payment in dApps, crowdfunding, commerce within the industry, and as a treasury currency for industry projects.

2.2 Supporting Emerging Markets

What if fiat currencies lost their value as quickly as the cryptocurrencies of 2018, dropping in value 20-99% per year? Unfortunately, this is exactly what happens to the fiat currencies of many emerging markets. While many of us live out our days safely insulated from the consequences of this reality, many others are not so lucky. Imagine being forced to hold a currency that loses 50% of its value every year, and having little to no alternative. Rapid inflation is widespread, even in 2018[1] [7]:

[1] Inflation and devaluation are not quite the same thing. Devaluation refers to a currency going down in price relative to foreign currencies, whereas inflation refers to increasing prices for goods and services within the currency's local economy.



Country	Inflation Rate (%)
Venezuela	1370000
South Sudan, Republic of	106.4
Sudan	61.8
Yemen	41.8
Argentina	31.8
Iran	29.6
Libya	28.1
Congo, Dem. Rep. of the	23.0
Liberia	21.3
Egypt	20.9
Angola	20.5

The IMF estimations put 11 countries at 20% or higher inflation in 2018, and the Cato Institute's Troubled Currencies Project estimations, which are based on black market exchange rates measured weekly, often indicate that the real rates are significantly higher. According to the Troubled Currencies Project, which is a joint project with Johns Hopkins University, six countries are experiencing over 100% annual inflation at the time of this writing:

Hanke Inflation Weekly

Country	Free-Market Exchange Rate	Date of Information	Hanke Annual Measured Inflation Rate[1] (%)	IMF Year-End Inflation Projection[2] (%)
Venezuela[†]	13,433,000 VEF/USD	10/11/18	54,061	2,500,000
Iran	147,000 IRR/USD	10/11/18	273	47.8
Zimbabwe[*]	5.35 "zollars"/USD	10/11/18	156	6.3
Sudan	49 SDG/USD	10/11/18	143	64.3
Turkmenistan	14.4 TMT/USD	08/09/18	128	9.4
Argentina	38 ARS/USD	10/11/18	119	40.5
Yemen	722 YER/USD	10/11/18	95	30
Turkey	6.08 TYR/USD	10/11/18	68	20
Liberia	161.06 LRD/USD	07/18/18	36	27

Computed by Steve H. Hanke, The Johns Hopkins University [8].

[1] Hanke annual inflation rates are implied using PPP from free and black market exchange rate data.

[2] The IMF's year-end inflation projections for 2018, as of the Oct 2018 World Economic Outlook.

[*] Indicates cumulative calculation beginning on Jan 2, 2018 using Old Mutual Implied Rate and PPP.

[†] The redenomination ratio of Venezuela's new sovereign bolivar (VES) to old bolivar fuerte (VEF) is 1:100,000.

While one might expect citizens of these countries to simply hold foreign currency instead of their country's inflationary currency, governments in these kinds of situations often don't allow that to happen. The more people sell, the less the local currency is worth on global markets—just like when speculators start to lose faith and sell their bitcoin. Governments and central banks have the incentive to preserve the value of their local currency since that's the currency they have the power to mint.[2] Abuse of this power is often the cause of inflation in the first place.

Stable cryptocurrencies are an inevitable new piece on the monetary game board. And it's much easier to stop the movement of physical cash and bank-operated digital money than it is to stop the movement of peer-to-peer electronic cash. This seems to indicate that governments will soon no longer be able to artificially prevent competition over which currency their citizens hold.

We foresee a progression with one of two outcomes:

1. The governments in question realize the threat of massively decreasing demand for their local currency and begin managing their monetary policy more responsibly. This keeps the local currency competitive, and their citizens don't mass-adopt a stable cryptocurrency.

2. The governments in question continue to mismanage their monetary policy, and

[2] While governments and central banks are often independent to some extent, the power dynamics often mean that central banks can be thought of as a part of the government. We simplify to referring to them both as the government from here on out.

eventually the local fiat currency is replaced by a stable cryptocurrency.

While outcome #2 may be more exciting for cryptocurrency speculators, outcome #1 would certainly be less disruptive for the local citizens, who would be spared the damage of going through a currency crisis. For this reason, we consider #1 the ideal outcome—speculators can still do well if stable cryptocurrencies only reach the circulation needed to put this level of pressure on local governments. However, it stands to reason that outcome #2 is also net-positive for the citizens in question in the long term, who would likely be freed from the inflation that would have otherwise ensued for the decades to follow.

2.3 Globalizing Commerce

Despite the level of globalization today, it remains difficult to transact across borders. A widely-used stable cryptocurrency would remove these barriers and allow anyone to transact with anyone else, anytime, anywhere. It would also allow businesses to scale internationally without having to build new infrastructure to interface with local banking institutions in each region.

2.4 Iterating on the Fundamentals of Capitalism

Suppose Bob is extremely wealthy. Do you like Bob? Is Bob a good person? Many today would assume Bob is greedy or dishonest given that he's extremely wealthy. Why is this? If wealth is a measure of how much someone has done for others, then the wealthier someone is, the more we should like them. However, money is game-able, and we all know that—we know that many methods for getting rich don't involve providing much real value. One form of this gaming is the operation of manipulative gambling venues that prey on less informed and intelligent participants, like casinos, or the stock market.[3] A subtler form of gaming is the production and sale of goods and services that are desirable but harmful on net. Cigarettes, delicious but unhealthy foods, and (in our view) clickbait journalism have all earned fortunes while arguably causing a heap of destruction along the way.

Are cryptocurrencies a solution to these insidious problems with capitalism? No. In fact, cryptoassets have likely only made things worse so far, as they have been primarily used to gamble and steal money from others via volatile and manipulated markets. But we believe that stable, programmable money, along with other technological advancements that we hope to build or see built, may present solutions in the future. Consider that (a) the amount of effort going into distributed governance innovation is rapidly increasing, (b) distributed governance over permission or denial of transactions is feasible with smart contracts, and (c) we have cultural momentum in the direction of experimenting with how we could upgrade money. One can begin to see how this

[3] While there is certainly a lot of value to be generated through the allocation of capital, securitization of commerce, risk-hedging, and so on, it's also quite clear that a lot of public market activity is a combination of speculation and manipulation that essentially amounts to gambling, where on average the uninformed retail investor is the chump at the table paying for the sharks.

could lead to exploring new means of pricing in transactions, or new means of governing and automatically policing what is and isn't legitimate capital markets behavior. We are eager to see this experimentation play out, and believe a stable cryptocurrency is a fundamental building block that will open up these possibilities.

2.5 The Nature of the Opportunity

In summary, stability and censorship-resistance are clearly desirable, and programmability may enable new solutions to age-old problems that have hampered the net benefit of capitalism. Demand is likely to be high for a fully featured and fully functional stable cryptocurrency. Network effects are likely to produce a small number of prominent stable cryptocurrencies, and so each competing currency has a challenge in marketing and distribution. But this all assumes it's even possible to create a lasting stable cryptocurrency, which is as yet unproven—the first challenge for the industry is creating the technology itself.

3 The Challenge for Stable Cryptocurrencies

Achieving stability without compromising other important properties is very difficult. Here we present the major design decisions that a stable cryptocurrency issuer must face, and our reasoning for which option is better at each decision point.

3.1 Pegged vs. Floating Exchange Rate

Some floating currencies, for example the US dollar, are relatively stable in value. They are actually the source of all currency stability—if no currency or commodity were stable in the first place, there would be nothing to peg to. So one may wonder: could we create an independently stable cryptocurrency that isn't pegged to anything?

There are numerous problems that stand in the way of this lofty goal. When a central bank stabilizes a currency, it has to measure purchasing power of its currency, predict changes in demand in advance, and manipulate currency supply even when it doesn't have enough other capital to directly purchase its currency from the open market. Perhaps in the future we'll have a sophisticated DAO-based legal system, as well as having relatively stable demand for some long-standing cryptocurrency, which may permit the replication of true central banking on the blockchain. But for the foreseeable future, the barriers are just too high.

Pegging one currency to another, in contrast, is much simpler and easier for cryptocurrency issuers to do manually or automate in smart contracts.

Conclusion Stable cryptocurrencies should be pegged to an existing stable currency, commodity, or basket of assets, at least to start.

3.2 Self-Referential vs. Foreign Collateral

In order to peg a currency's value to some asset or basket, one needs to be able to offer holders of that currency a fixed price in terms of that asset or basket. For example, if you wanted to peg a currency 1-to-1 to the euro, you would need to be able to offer holders of the currency one euro worth of value per unit of the currency.

However, you wouldn't necessarily need to make that offer in euros. You could hold a bunch of gold in a vault, and so long as you were always willing to offer *one euro worth of gold* per unit of the currency, that would do just as well. But if the price of gold goes down, you would need to offer more gold, impacting your ability to maintain 100% collateralization. The more volatile the asset or basket you use to back your currency, the higher the risk that you'll run out of collateral at some point in a down market.

One interesting approach that some stable cryptocurrencies take is to use a newly created, self-referential asset to back the new currency. What does self-referential mean? It means that the value of the collateral token is determined by the success of the new currency. For example, the collateral-token holders may receive a share of transaction fees or a share of newly minted stable cryptocurrency coins during expansionary periods.

A benefit of this approach is that stability begets more stability—if the new stable cryptocurrency is working and being adopted, that will likely drive up the value of the collateral-token, thus increasing the available collateral for the stable cryptocurrency. The problem is that in the same way, instability begets instability—if the new stable cryptocurrency goes through periods of decreases in demand, this can cause expected revenue for collateral-token holders to decline. As expected revenue falls, so does how much people are willing to pay for collateral-tokens. This in turn makes holders of the stable cryptocurrency less likely to believe they will be able to redeem their tokens for an asset that is worth anything, leading to further decreases in demand for the stable cryptocurrency.

Foreign collateral, on the other hand, involves leveraging an asset or basket that has an independent market value. If a currency backed by gold loses demand for some reason, that will have little to no effect on the market price of gold. This separation of expectations between a pegged currency and its backing keeps their prices from affecting each other, and prevents a sudden crash in their value.

Self-referential collateral appears to be viable only if the market consensus about the future usage of a currency is extremely entrenched.

Conclusion Foreign collateral is very likely necessary for bootstrapping a new stable cryptocurrency.

3.3 Pegging to Fiat Money vs. Pegging to Other Assets

Fiat currencies are extremely attractive pegs, because they are simple and highly liquid. However, this imports the inflation of the fiat currency into the stable cryptocurrency, and also exposes holders to geopolitical risk. If our goal is to create a currency with robustly stable purchasing power in the long term, a better solution would be to peg

to a basket of assets. This would likely be composed of a combination of fiat currency, securities, and commodities. The downside of this approach is that it is much more complicated, both conceptually and as a matter of implementation. It also exposes holders of the stable cryptocurrency to the short-term fluctuations in the value of the basket, which initially people may not like.

Conclusion A fiat currency peg makes the most sense in the short-term, but ultimately a basket of assets is very likely necessary to achieve stability in the long-term.

3.4 Partial Backing vs. Full Backing

If the demand for a pegged currency will only ever drop at most by, for example, 50%, then in principle, the issuer only ever needs to be able to repurchase 50% of the circulating supply, and so could hold only 50% backing and maintain perfect stability. You can start to reason about how much demand is likely to drop in the most extreme situations and make guesses about the amount of collateral needed by looking at the history of pegged currencies and when they have and have not broken under stress. You can even run simulations of what might happen given various possible demand histories.

Holding less than 100% collateral backing also comes with a major benefit: if users purchase 100% of the units of currency in circulation for face value, but the system doesn't need to hold all 100% of that capital in escrow as collateral, some of it can be spent! What could you spend it on? For example, you could spend it on marketing, development, and paying dividends to investors who funded earlier marketing and development.

This approach of spending part of the collateral is so tempting that we planned on building our stable cryptocurrency this way at the beginning of our design process. But as we worked on building out our arguments for why the backing only needed to be X% or Y% of Z%, they all fell apart. Why? Because the analogy between pegged fiat currencies of nation states and pegged cryptocurrencies is not sufficiently strong to rely on numbers that have played out in the history of pegged fiat money. There is no similar enough reference class to safely reason empirically about this question.

Relative to nation-based fiat currencies, competition among stable cryptocurrencies should be much higher, and switching costs much lower. As a result, demand drops have the potential to be far larger than anything we have seen in the past. Even if, for example, 70% collateralization has permitted pegged fiat currencies to weather financial crises, 70% may be insufficient for a pegged cryptocurrency to maintain stability.

Two types of potential failures for pegged currencies are:

1. **Bank runs**—when the holders of pegged currencies panic over the possibility that collateral will run out before they have the chance to redeem their currency for collateral, and everyone runs to redeem all at once.

2. **Speculative attacks**—when someone borrows a large amount of the pegged currency, sells it into the market all at once to exhaust the collateral held in reserve,

and then repurchases the currency for less after the peg has broken, pocketing the difference, and then repaying the loan.[4]

Reasoning about the likelihood of either of these possibilities when a stable cryptocurrency has less than 100% collateral is hard, because you have to make guesses about how large masses of people will behave in circumstances we've never really seen before. But reasoning about 100% backing is easy—neither outcome is possible under any drop in demand.

Conclusion If we want to be confident that a new stable cryptocurrency will not be subject to bank runs or speculative attacks, we must maintain 100% collateral backing.

3.5 On-Chain vs. Off-Chain Foreign Collateral

Native on-chain collateral has the benefit of decentralization. Any pure cryptoasset can be truly held by a smart contract, and so can be as censorship-resistant as the consensus mechanism it's implemented on top of. Creating a new stable currency that's actually widely used will be disruptive, and so censorship resistance is a very desirable property. It's tempting to back stable cryptocurrencies with pure cryptoassets. For example, you could back a new cryptocurrency with the base currency of a smart contract platform, like ether, EOS, and so on.

The problem of course is that cryptoassets are all highly volatile at this moment in history. We know of two options for managing this volatility:

1. **Overcollateralization**—holding more than 100% backing, to account for changes in the value of collateral.

2. **Hedging**—holding a combination of long and short positions in some asset, so that changes in the spot market price don't affect the value of the portfolio.

The problem with each of these approaches is that they cost money. In the case of overcollateralization, someone has to put up that extra collateral. While some degree of overcollateralization is feasible via the sale of future network profit (similar to the process of selling shares in a startup), the market's valuation of that future income will likely not be high enough to massively overcollateralize to the level that volatile cryptoassets require. With respect to hedging: while this may be effective at mitigating the impact of volatility, the cost of upkeep cuts into profitability and leads to the system slowly hemorrhaging funds.[5]

Alternatively, one could use tokenized off-chain assets. This comes at the cost of centralization, but appears to be necessary for economic viability since off-chain assets are substantially less volatile. These design choices need to be made in reference to the existing context and constraints, so while purely on-chain backing may well be the optimal

[4]For more details, see https://en.wikipedia.org/wiki/Speculative_attack.
[5]Exchange fees and always paying the bid-ask spread are a couple reasons for this.

approach in a decade or two if some fixed-supply cryptoassets have lower volatility, the volatility of cryptoassets today likely means that holding purely on-chain backing is not a feasible approach.

Conclusion Off-chain assets make for significantly better collateral due to their lower volatility, and so despite the cost of centralization, they are likely the better choice.

3.6 Single-Issuer vs. Multi-Issuer Off-Chain Collateral

Off-chain collateralization typically involves accepting some off-chain asset (for example gold or dollars) in exchange for newly minted coins, holding that off-chain asset somehow, and allowing users to redeem the coin for the collateral at any point.

This design is fundamentally centralized. It comes along with two main risks:

1. **Counterparty risk**—one needs to trust that the people managing the money will be responsible with it.

2. **Third-party risk**—one needs to trust that their money and the organization that manages it is safe from external parties such as hackers, misaligned governments, etc. This is a real threat. Many centralized payment services have been shut down by governments, including Liberty Reserve, GoldAge, e-Bullion, and E-gold [9].

When there is a single issuer holding off-chain assets and offering redemption, a default of the issuer or seizure of the issuer's assets by a third party could lead to complete default, a broken peg, and the market value of the currency going to zero. The probability of such default may be low, but the the consequences would be catastrophic.

However, if there are many different issuers that each hold a fraction of the collateral and each offer redeemability, the risk of complete default can be dramatically reduced. This does come at a cost: an increased probability of *partial* default, since there are more counterparties and more third parties with the power to seize some fraction of the underlying assets. This risk of partial default can be offset through a modest amount of overcollateralization.

Since the third parties that are most likely to intervene are governments, in order to truly diversify the risk of default the issuers would need to be set up in a variety of political jurisdictions.

Conclusion Multiple internationally dispersed issuers can drastically reduce the default risk due to off-chain collateral backing.

3.7 Summary of Design Choices

- A peg is required.
- Foreign collateral is required.
- Peg to fiat in the short-term, and a basket of assets in the long-term.

- 100% backing is required.
- Tokenized real-world assets are probably necessary, at least right now.
- Multiple dispersed token issuers substantially reduces risk of total default.

In this paper we introduce the Reserve Stabilization Protocol, a system that both allows for near-term pegging to fiat currency and naturally transitions to diverse asset-backed stable currency.

4 Overview of the Reserve Protocol

We'll start with a simple explanation of the Reserve Protocol. In the next section, we'll go into much more detail on how each of these components is implemented.

4.1 Basic Attributes

- The Reserve Protocol can be implemented on top of any smart contract platform. It could be operated on its own chain, but it benefits from locating itself where collateral tokens are most liquid. Initially we are developing on the Ethereum Network but ultimately we expect two-way bridges to enable complete interoperability of the Reserve token across all major smart contract platforms.
- The initial production version of the Reserve Protocol will be substantially centralized, and over time each protocol component will be migrated on-chain and released from control by the founding team.
- The Reserve token will initially have a target value of US $1.00, but is designed to go off of the peg to the US dollar in the long term.

4.2 Tokens

The Reserve Protocol interacts with three kinds of tokens:

1. **The Reserve token (RSV)**—a stable cryptocurrency that can be held and spent the way we use US dollars and other stable fiat money.
2. **The Reserve Rights token (RSR)**—a cryptocurrency used to facilitate the stability of the Reserve token.
3. **Collateral tokens**—other assets that are held in smart contracts in order to back the value of the Reserve token, similar to when the US government used to back the US dollar with gold. The protocol is designed to hold collateral tokens worth at least 100% of the value of all Reserve tokens. Many of the collateral tokens will be tokenized real-world assets such as tokenized commodities, currencies, and securities. The portfolio will start off relatively simple and diversify over time as more asset classes are tokenized.

4.3 How the Reserve Token is Stabilized

If demand goes down for the Reserve token, prices will fall on secondary markets. What happens then?

Suppose the redemption price of Reserve is $1.00. If the price of Reserve on the open market is $0.98, arbitrageurs will be incentivized to buy it up and redeem it with the Reserve smart contract for $1.00 worth of collateral tokens. They'll continue buying on open markets until there is no more money to be made, which is when the market price matches the redemption price of $1.00.

The same mechanism works in reverse when demand goes up. If the price of Reserve on the open market is $1.02, arbitrageurs will be incentivized to purchase newly minted Reserve tokens for $1.00 worth of either collateral or Reserve Rights tokens (the latter only if there is an excess pool of Reserve tokens available), and immediately sell them on the open market. They'll continue selling on open markets until there is no more money to be made, which is when the market price matches the purchase price of $1.00.

4.4 How the Reserve Protocol is Capitalized

The Reserve Protocol holds the collateral tokens that back the Reserve token in smart contracts. When new Reserves are sold on the market, the assets used by market participants to purchase the new Reserves are placed into these smart contracts to be held as collateral. This process keeps the Reserve collateralized at a 1:1 ratio even as supply increases.

At times, the Reserve Protocol may target a collateralization ratio greater than 1:1. When this is the case, scaling the supply of Reserve tokens requires additional capital in order to maintain the target collateralization ratio. To accomplish this the Reserve Protocol mints and sells Reserve Rights tokens in exchange for additional collateral tokens.

4.5 What Happens When the Collateral Tokens Depreciate

Collateral tokens are somewhat volatile. While we may be able to select a portfolio with minimal downside risk, the reality is that drops in the collateral tokens' value will happen. When this happens, the Reserve Protocol will sell newly minted Reserve Rights tokens for additional collateral tokens and add them to the backing.

4.6 Preventing Speculative Attacks and Bank Runs

It's theoretically possible for the Reserve to remain less than 1:1 collateralized if the collateral tokens depreciate and no market participants wish to purchase Reserve Rights tokens for more than a minimum price set by the protocol. In this case, the protocol widens the price band it defends for the Reserve token. For example, instead of a very tight band around $1.00, the protocol would adjust the band to range from $0.95 to $1.05 if the collateral tokens had depreciated 5% and there were no demand for Rights.

This means that Reserve tokens would temporarily be redeemable for $0.95, and would cost $1.05 to purchase.

This expanding band approach eliminates the possibility of a bank run, since even if everyone were to redeem, the last redeemer would receive the same rate as the first. It also makes a speculative attack infeasible, as Reserve will stay collateralized until 100% of Reserve tokens are redeemed, and risky to attempt, as the market price of Reserve can float upward during the re-purchasing phase of the attack.

Since the collateral tokens derive their value from their respective markets, which are independent of demand for Reserve, they are likely to re-appreciate over time even if market confidence in Reserve is shaken. When they re-appreciate, the band is narrowed back to a tight range around $1.00.

It may be that this functionality of the Reserve Protocol is never once activated, but since markets can't be predicted in advance, it's necessary to take adequate precautions to prevent total default in such a scenario.

4.7 Moving Off the USD Peg

The Reserve Protocol is designed so that once the portfolio of tokenized assets held in smart contracts is stable enough, the Reserve token can transition to representing a fractional ownership of the collateral tokens. This option is in place so that if the US dollar starts to depreciate, the Reserve can maintain a more stable value.

5 The Reserve Protocol

The Reserve Protocol primarily manages two pools of value:

- The Reserve, a cryptocurrency kept stable at $1.
- The Vault, a pool of other blockchain assets used to purchase Reserves whenever demand for Reserve drops. The protocol aims to maintain at least 100% collateral backing of the value of all minted Reserves.

The protocol is designed to operate as a collection of smart contracts. In addition to the pools of value, it consists of these other active components:

- The Reserve Manager, which keeps the Reserve stable at $1.
- The Vault Manager, which manages the assets in the Vault.
- The Market Feed, which tracks market data on Reserves, Reserve Rights, and the Vault assets.
- The Auctioneer, which runs the protocol's market operations.

5.1 Reserve & Reserve Rights token

The Reserve and the Reserve Rights token are both mintable, burnable, ERC-20 tokens. The Reserve token will have a variable transfer fee, initially set to 0.[6] The Reserve Rights token will be used to keep the Reserve token stable at its target price and vote on governance proposals.

5.2 The Reserve Manager

The Reserve Manager is in charge of manipulating the supply of Reserve to keep its price stable at $1.

5.2.1 Raising the Price

Whenever the market price of Reserve falls below $1, the Reserve Manager will buy Reserves at the market price using Vault assets and burn them. These trades are executed through the Auctioneer with a maximum price and maximum quantity. The maximum acceptable price for buying Reserves is $1 of the asset of exchange, and the maximum quantity of Reserves to trade for is:

$$r \cdot \text{Quantity of Reserves} \cdot \frac{\$1 - \text{Reserve Price}}{\$1},$$

where r is a damping factor[7] to prevent sudden overreactions and price oscillations.

5.2.2 Lowering the Price

Whenever the market price of Reserve is above its target price plus a stability spread,[8] the Reserve Manager will auction Reserve tokens to lower the token supply and thereby lower the price. The auctions work differently depending on whether or not there is an excess pool of Reserve tokens.[9] If this excess pool exists, then the Reserve Manager will sell Reserve tokens from that pool for $1 worth of Reserve Rights tokens each, allowing Rights holders to perform an arbitrage loop that brings the price back down to $1. If there is no excess pool of Reserve tokens, the manager will mint new Reserve tokens and sell them for vault assets. The Auctioneer executes these trades with parameters for minimum price and maximum quantity. The minimum acceptable price for selling

[6] The magnitude of the transfer fee will initially be controlled by the Reserve core team and later will be determined through governance. It's difficult to reason about the effects of a transfer fee a priori, but we think it's important to build flexibility into the system.

[7] This number has not been set yet. Most likely it will be empirically calibrated after the launch of the system, and it may become a dynamic factor based on running estimates of the Reserve's recent price elasticity and liquidity of Vault assets. Its purpose is twofold—first, it lowers the odds that the protocol will overreact to price changes and launch inefficient auctions. Second, if some Vault assets turn out to be illiquid enough to cause problems, this damping factor can slow trading such that the protocol doesn't lose too much money from trading illiquid assets.

[8] The stability spread has not been determined yet—it will depend on the price elasticity of Reserve, exchange fees, and the liquidity of assets held in the vault. At most it will be a few cents.

[9] see the Maintaining the Vault level section for more details.

Reserves is the target price plus stability spread. The maximum quantity of Reserves to trade away is:

$$r \cdot \text{Quantity of Reserves} \cdot \frac{\text{Reserve Price} - \$1}{\$1},$$

where r is the same damping factor as above.

5.2.3 Lowering the Target Price

Under normal circumstances, the Reserve Manager obeys the behavior defined above and aims to defend a peg at \$1. However, the Reserve Manager will defend a peg lower than \$1 when the Vault Ratio drops below 1. In this case, the Reserve Manager will defend a peg equal to:

$$\$1 \cdot \text{Vault Ratio}$$

For example, if the Vault Ratio is 0.9, the Reserve Manager will defend a peg at \$0.90. This behavior prevents a "run on the bank". Instead of defending the \$1 peg until some Reserve holders are left with a worthless token, the Reserve Manager defends a peg that allows all Reserve holders to redeem their token for equal value.

5.3 The Vault Manager

The Vault Manager keeps the Vault level high enough to absorb shocks. The Vault Manager maintains the Vault level in accordance with the Vault Target. The Vault Target is:

$$\$1 \cdot \text{Target Vault Ratio} \cdot \text{Quantity of Reserves}$$

The Vault Manager determines the current Vault level by adding up the value of its assets. The value of each asset is just the quantity of that asset in the Vault times the fast-average market price of that asset, as recorded by the Market Feed.

5.3.1 Diversifying the Vault

There will be multiple assets in the Vault portfolio, such as tokenized commodities, currencies, and securities.

To minimize the risk that a sudden drop in the prices of Vault assets reduces the Vault level to below the Vault Target we use three types of diversification:

- Diversification across asset classes
- Diversification across issuers
- Diversification across jurisdictions

Diversifying the Vault across asset classes mitigates systemic risk associated with particular asset classes. When some assets drop sharply, a well diversified portfolio only drops a little bit, and could even stay stable if it contains anti-correlated assets.

Diversifying the Vault across issuers mitigates counterparty risk originating from the asset issuers themselves. While assets added to the Vault will be thoroughly vetted, asset tokenization involves off-chain components, and thus necessarily has some risk from centralization. In the worst case, an issuer may steal some or all of the underlying assets backing the tokens they issued, which would lead to a sharp drop in the value of their issued tokens. We mitigate this risk by maximizing the diversification of issuers. For each asset type in the vault we will spread out our exposure to that asset across as many independent issuers as possible.

Diversifying the Vault across jurisdictions mitigates counterparty risk originating from the jurisdictions of Vault asset issuers. Even if we can trust issuers, governments may threaten to shut issuers down if they don't give up the assets backing their tokens. Asset seizure or issuer shutdown will likely lead to sharp drops in the value of that issuer's tokens. To protect against this type of counterparty risk, for each asset class, we will spread out our exposure to the asset among issuers from as many jurisdictions as possible.

5.3.2 Managing the Vault Ratio and Vault Portfolio

In the short-run, due to the limited availability of Vault assets, the Vault will be overcapitalized to provide additional security.[10] The Vault ratio will gradually decrease to 1. The ratio decreases in response to two factors: increased availability of high quality assets, and improved quality of existing Vault assets.

When new high quality assets are added to the Vault, we increase the diversification and resilience of our overall Vault portfolio. Since the amount of overcapitalization needed to stay safe decreases as our portfolio diversification increases, when we can add new assets to the vault we will lower the Vault Ratio.

Likewise, when the quality of an existing Vault asset improves, we need slightly less overcapitalization to stay safe. For example, when an issuer improves their safety standards or increases jurisdictional diversification, the counterparty risk of their asset decreases. Thus, in these cases we will also reduce the Vault Ratio.

The management policy of the Vault Ratio and the Vault portfolio changes depending on the maturity of the system. The management starts out centralized and becomes fully decentralized over time. In the early life of the system, portfolio changes are initiated by the development team making a proposal for how to update the portfolio. Proposals can include additions/removals of assets, changes to the target allocation of an asset, and updates to the Vault Ratio.

5.3.3 Vault Portfolio Rebalancing

The Vault Manager aims to maintain a particular portfolio of assets. Due to the volatility of these underlying assets, the portfolio needs to be periodically rebalanced in order to

[10] It is unclear at this time how overcapitalized it needs to be. Overcapitalization is expensive, so we will be working to determine the smallest possible number that will work.

ensure risk remains diversified. Rebalancing occurs through two mechanisms: trades executed by the Reserve Manager, and quarterly rebalancing through governance.

The Reserve Manager adds and removes Reserves from circulation when necessary to maintain the target price. These sales are denominated in the Vault asset that is furthest from its target level. More precisely, when Reserves are being minted and sold for Vault assets, the Reserves will be sold for the asset that is the furthest below its target level. Likewise, when Reserves are being repurchased from the market using Vault assets, the Vault asset that is spent will be the one that is furthest above its target level. Rebalancing through this mechanism won't be sufficient in some cases, though. To account for this, further portfolio rebalancing will occur quarterly as a component of governance.

5.3.4 Maintaining the Vault level

The Vault is primarily capitalized by the proceeds from the sale of minted Reserves—any time a Reserve is minted and sold for Vault assets, 100% of the value of that sale is stored in the Vault. However, Vault assets will not be perfectly stable, and thus the Vault Manager must be able to account for changes in the Vault level. It does this by raising the Vault level when it has dropped too low, or raising the Reserve token supply when the Vault level is too high.

Raising the Vault Level When Vault assets depreciate, the Vault level may fall significantly below the Vault Target. If the Vault level is significantly below the Vault Target and the Reserve Rights token price is over $10, the Vault Manager refills the Vault by minting new Rights tokens and auctioning them for more Vault assets. The quantity to be sold is:

$$r \cdot (\text{Vault Target} - \text{Vault Level})$$

where r is the same damping factor used to rate-limit Reserve auctions.

Raising the Reserve supply When Vault assets appreciate, the Vault level may increase above the Vault Target. If the Vault level is sufficiently above the Vault Target, new Reserve tokens will be minted and held as excess Reserve tokens. The Reserve tokens in this excess pool are available to be purchased by Reserve Rights token holders when the price of Reserve is trading above its target price.

5.4 The Market Feed

The purpose of the Market Feed is to provide the protocol with up-to-date info on the market price, trading volume, and volatility of protocol currencies: the Reserve, the Reserve Rights token, and each Vault asset. The primary input to the Market Feed is the recent, off-chain history of major cryptocurrency exchanges. The primary output of

the Market Feed is an on-chain summary of this data, reported and updated every 30 minutes.[11]

The Market Feed is necessarily an oracle system [10], as the information it requires is unavailable on the blockchain itself. The Market Feed is composed of:

- The on-chain Record Book
- A collection of off-chain, trusted Reporters

Each trusted Reporter periodically fetches market data, summarizes that data, and sends the resulting report to the on-chain Record Book. The Record Book checks the authorization and consistency of reports and maintains long-term summaries of market data.

5.4.1 Reports and Records

Reporters provide packets of off-chain data to the on-chain record book. Each such packet of data is a *report*. Each report summarizes the last 30 minutes of trading from each major exchange on which an asset trades. A report summarizes market data about each of the protocol's assets, including volume, volatility, and average price. Volume is simply the sum of quantities of trades of that asset. Average price is a volume- and time-weighted average of prices across trades. Volatility is the volume-weighted variance of prices in the 30-minute window.

When the on-chain Record Book has accepted a matching set of reports, it combines the summaries with its short history of recent summaries to compute volume, volatility, and price over the last 4 hours.[12] Both the 30-minute *fast average* and the 4-hour *slow average* are used by the rest of the protocol.

5.4.2 Reporters

Each Reporter is a program running outside the Ethereum blockchain and inside a secure, trusted execution enclave. At launch, we plan to rely on reporters we build ourselves. However, decentralized aggregator oracle solutions such as ChainLink [11] are preferred. We will likely switch over to ChainLink (or a similar solution) as it comes online and gains significant adoption.

Until ChainLink or a similar solution is available and trustworthy, we require the following properties of a Reporter:

- Each secure enclave provides cryptographic remote attestation of the installed program.

[11] The reporting period is a tradeoff. Factors affecting its value include market volatility, how quickly the protocol can affect prices, and the costs per operation of each Reporter. The protocol could dynamically adjust this period, though a static period has the virtue of simplicity.

[12] Like with the reporting period of 30 minutes, the slow-average period is a trade-off between how expensive we can make a market-manipulation attack and the protocol's ability to quickly respond to natural changes in the market.

- Each secure enclave provides read-and-tamper-proofing of Reporter memory.
- Each Reporter runs a distinct implementation of the market-summarization program.

5.4.3 The Record Book

The Record Book compares the market reports from its Reporters. If they agree, and further reports from those Reporters' accounts do not appear in the next 2 minutes, then the Record Book accepts the reports.[13] If a clear majority of reports agree, but some minority disagrees, then the majority report is accepted, and minority Reporters lose their authorization. If reports disagree without a majority, then the Record Book concludes there is insufficient information available. No auctions will be launched while there is insufficient price feed information available.

5.5 The Auctioneer

The Reserve Manager and Vault Manager will frequently need to trade assets with the wider market. When they do, they will delegate those trades to the Auctioneer. The properties of a simple trade request to the Auctioneer are:

- The asset A to sell, and whether to mint A or draw it from the Vault,
- The asset B to buy, and whether to burn B or save it in the Vault,
- The minimum acceptable exchange rate of A, denominated in B,
- The maximum quantity to trade of A, of B, or of both, and
- The expiry time for unsatisfied orders.

The Auctioneer maintains an open order book to which external users can submit limit orders. In response to a trade request, the Auctioneer greedily matches the best standing orders on the order books, as constrained by the specified maximum exchange rate and asset quantities.

5.5.1 Executing Trade Requests

Much of the technical inconvenience of decentralized exchange is neatly handled by the 0x protocol and its ecosystem of relays [12]. The Auctioneer tracks a short list of addresses of 0x exchange contracts. It would be a simple matter for the Auctioneer to simply offer asks for the above trades, on any 0x relay network. However, because the Market Price Feed has some latency, the prices that the Auctioneer offers are likely to be always

[13] The report delay guards against attack. Without the report delay, if an attacker obtains a Reporter's secret key, then the attacker can spoof the Reporter by sending false reports just before the Reporter would have. The length of this delay is a trade-off between the protocol's responsiveness to market prices and the protocol's ability to invalidate Reporters under attack.

slightly out of date. If the Auctioneer simply offered these trades unconditionally, it would frequently trade at a disadvantage.

The Auctioneer manages this by starting each trade request with a falling-price auction. On receiving a trade request, the Auctioneer begins a falling-price auction with an acceptance price at 1.5 times the request's acceptable exchange rate.[14] Over the following 20 minutes, the acceptance price drops linearly, block-by-block, until it equals the request's acceptable exchange rate. At any point during this time, external accounts may submit asks as signed 0x messages for the asset that the Auctioneer is selling. The Auctioneer will immediately offer to fill any submitted ask above its acceptance price for the current block, unless it has already sold the maximum quantity of that asset for the current trade request.

The Auctioneer may still have assets to sell by the end of the falling-price auction, either because there are no acceptable trades on the relays it accepts, or because off-chain agents haven't submitted all available asks during the auction. If so, the Auctioneer creates an offer for its remaining assets at the request's exchange rate, and submits the offer to a designated 0x relay.[15]

To minimize the occasions when the falling-price auction has not accounted for the available liquidity, we operate an off-chain *Trading Assistant*. The Trading Assistant conveys available asks from 0x relays to the Auctioneer as soon as the Auctioneer is willing to accept them.

6 An Iterative Automation Approach to Launching Decentralized Software

Decentralized software development comes along with some very significant challenges. Among others, two challenges during initial development are:

1. It's hard to write software without introducing a single bug, and in this field, a single bug can be catastrophic.

2. Software that interfaces with markets or other complicated phenomena will require iteration and calibration.

[14] The ceiling-price multiplier is a tradeoff between higher market responsiveness, and the chances of filling the trade request at lower prices than the market would bear. Ceiling-price multipliers near 1 leave needless opportunities for outside arbitrage. Due to the effective quantization of time on the blockchain, very high ceiling-price multipliers also leave wide opportunities for arbitrage. The ideal ceiling-price multiplier is nearly always high enough that there are often trades available above that factor, but not high enough to completely satisfy fill the Auctioneer's trade request.

[15] This depends on the release of version 2 of the 0x protocol by the time of our launch. Technical considerations prevent smart contracts from making liquidity on 0x relays in version 1 of the protocol. According to both their public timeline and more-recent personal communications with their team, version 2 of the 0x protocol is expected to be ready by late Q4 of 2018. If their release is delayed in a way that threatens our timelines, then we can operate our own future-compatible relay. The patches necessary to the 0x system needed to support just this feature (as opposed to the entire 0x version 2 feature set) are relatively straightforward.

Writing a series of smart contracts that don't permit editing and then launching them all at once, even with a security audit, is not a responsible way to develop this kind of software.

Before implementing complex functionality in smart contracts, the functionality of a contract should be performed manually off-chain, then automated off-chain, then programmed into a smart contract. This allows for iteration and automation of actual system behavior in a production environment before network functionality is substantially codified and iteration cycles are dramatically slowed down.

When initially launching smart contracts, developers should maintain full control of the code for some period of time. This permits fixing bugs quickly in a production environment. Many users are clearly willing to participate in centralized systems, and users who are not can wait for control to be reduced to join the network.

This is the approach we are taking in launching Reserve. In addition to the fully smart contract powered alpha already running on a public testnet, we will follow this sequence when releasing the production version:

- Initially, on-chain functionality will be as simple as possible.
- Before the maturation of the on-chain ecosystem to the point of liquid tokenized real-world assets, the collateral in the vault will likely consist of a tokenized US dollar (powered by the Reserve team but separate from the Reserve token), as well as any other currency tokenization projects we believe meet our standards of quality and transparency.
- The team will manually experiment with different parameterizations of procedures for operating the components of the Reserve Protocol.
- When the team is confident that a particular procedure is the right approach, the development team will automate that portion of the overall protocol on a private, centralized server.
- When an automated component has been running long enough in a private execution environment that the team is confident in its design, the development team will program it in smart contract form, and add that smart contract to the on-chain protocol, maintaining full control of that on-chain code.
- When a smart contract has performed as expected and been subject to sufficient incentives for subversion for a sufficient period of time for the team to be confident that it is without catastrophic bugs, the development team will transition its governance to require voting of the token holders for any change to occur.
- Eventually, the entire protocol will be automated on-chain, and the core development team will retain no privileged control of any kind.

7 Summary

We have described the Reserve Stabilization Protocol. To keep the price of Reserve stable, the protocol adjusts the supply of Reserve in response to changes in demand. The protocol ensures it always has enough backing to repurchase the supply of Reserves through a fully collateralized vault consisting of carefully chosen on-chain assets. Overall we expect this design to result in a stablecoin that balances decentralization, scalability, and stability, and represents the most promising path forward to a feature-complete global cryptocurrency.

References

[1] Nevin Freeman. *Why another stablecoin?* 2018. URL: https://medium.com/reserve-currency/why-another-stablecoin-866f774afede (visited on 06/19/2018).

[2] Nevin Freeman. *Reserve's Analysis of the Basis Protocol*. 2018. URL: https://medium.com/reserve-currency/our-analysis-of-the-basis-protocol-cf1e0713b849 (visited on 09/18/2018).

[3] Reserve Research Team. *Reserve's Analysis of the MakerDAO Protocol*. 2018. URL: https://medium.com/reserve-currency/our-analysis-of-the-makerdao-protocol-4a9872c1a824 (visited on 09/18/2018).

[4] Irving Fisher. *Stabilizing the Dollar*. The Macmillan Company, 1920.

[5] CoinMarketCap. *Tether*. 2018. URL: https://coinmarketcap.com/currencies/tether/ (visited on 10/31/2018).

[6] blurpesec. 2018. URL: https://www.reddit.com/r/ethereum/comments/9gkn2f/how_can_i_determine_the_total_amount_of_ether/e64tgeo/ (visited on 10/22/2018).

[7] International Monetary Fund. *Inflation rate, average consumer prices*. Oct. 2018. URL: https://www.imf.org/external/datamapper/PCPIPCH@WEO/OEMDC/ (visited on 10/31/2018).

[8] Steven H. Hanke. *The Troubled Currencies Project*. Cato Institute - Johns Hopkins University. 2018. URL: https://www.cato.org/research/troubled-currencies (visited on 10/31/2018).

[9] Bitmex Research. *Tether*. 2018. URL: https://blog.bitmex.com/tether/ (visited on 02/18/2018).

[10] Vitalik Buterin. *Ethereum and Oracles*. 2014. URL: https://blog.ethereum.org/2014/07/22/ethereum-and-oracles/ (visited on 03/08/2018).

[11] Steve Ellis, Ari Juels, and Sergey Nazarov. *ChainLink: A Decentralized Oracle*. 2017. URL: https://link.smartcontract.com/whitepaper (visited on 03/08/2018).

[12] Will Warren and Amir Bandeali. *0x: An open protocol for decentralized exchange on the Ethereum blockchain*. 2017. URL: https://0xproject.com/pdfs/0x_white_paper.pdf (visited on 03/13/2018).