ORC-Stable (Symbol: ORCS [Aurk-Ess]): A non-collateralized unforkable stable privacy-preserving cryptocurrency designed to be used as a medium-of-exchange and as a non-sovereign high-velocity reserve asset powered by realtime Orch Network platform

Ren Timer (ren@orcs.fund)

Bitmessage: BM-NBqZhDGg7vGFCFebhRhT48jNTr8nDbBD

Version 0.1.07

For most updated version, please look up at https://orcs.fund

CONTENTS

Serial	Title	Page Number
1.	Abstract	3
2.	Introduction: Why do we require a price-stable truly decentralized cryptocurrency?	4
3.	Use Cases and Applications of a stablecoin	5
3.1	The Increasing Demand for a Non-Sovereign Non-Collateralized Debt-free High-velocity Privacy-preserving Reserve Asset	5
3.2	A Stable cryptoasset for traders and speculators	7
3.3	The Emerging Decentralized Economy	8
3.4	Debt, Credit and Derivatives Markets	8
3.5	Developing Markets with volatile fiat currencies	10
3.6	Anti-fragility Insurance and Protection against Blackswan/Tail events	11
3.7	Total Addressable Market (TAM)	12
4.	How ORCS enforces price-stability?	12
4.1	The ORC-Stable (ORCS) Protocol	14
4.2	Expansion and Contraction of ORCS via ORCE	16
4.3	A Post-USD Interplanetary Economy	17
5.	The Competition	17
5.1	Tether(USDT)	17
5.2	BitShares	18
5.3	Dai	19
6.	Conclusion	21
7.	Contact	21

Abstract

Extreme price volatility of BTC, ETH and other cryptocurrencies is one of the biggest barriers to widespread adoption that cryptocurrencies face today. Unlike fiat currencies, today's cryptocurrencies do not have a central bank that implements monetary policy to keep purchasing power stable, meaning that changes in demand can induce massive fluctuations in price. If users cannot be sure that the purchasing power of their accounts will remain stable, they will never adopt a cryptocurrency as a medium of exchange over a price-stable alternative. Moreover, without price stability, it is difficult for credit, debt and derivatives markets to form on top of a cryptocurrency because every contract taking payments in the future must charge a large premium to factor in price risk. For example, imagine you received a salary of 10 ETH per month—if the price of ETH dropped, you might face difficulties in paying off your monthly bills.

The Orch Stable (Symbol: ORCS) protocol powered by truly decentralized unforkable realtime blockchain federation Orch Network accomplishes this by algorithmically adjusting the supply of ORCS tokens in response to changes in the following variables and a vector:

1. current transaction fee and hashrate of ORCS subprotocol;
2. Periodic Game-theoretic Truth Game outcome on current ORCS exchange rate;
3. External datafeed on CPI index;
4. Current Coinship Index level of Coinship derivatives exchange running parallel as a subprotocol of Orch Network.

This implements a monetary policy similar to that executed by central banks around the world, except it's much more robust, decentralized, protocol-enforced algorithm, without the need for direct human judgment. For this reason, ORCS can be classified as a non-collateralized non-sovereign high-velocity reserve asset that does not have any counter-party risks.

Introduction: Why do we require a price-stable truly decentralized cryptocurrency?

Today, very few people use cryptocurrencies for normal, day-to-day transactions. But why? Some would say it's because cryptocurrencies are slow and expensive to use. While that's true of Bitcoin and many older cryptocurrencies, it's certainly not true of some newer protocols. For example, Dash claims it can confirm transactions in under a second and handle thousands of transactions per second at fees of less than $0.15 per transaction, with fees expected to decrease further over time. Others would say it's because cryptocurrencies aren't reliable or trusted. Monero (XMR) is a very trusted privacy-preserving currency, still it did capture its potential value which could be 100x plus higher than it's now.

There are many protocols with firm backing from respected investors and strong development teams. Furthermore, Bitcoin itself has shown that the blockchain model is extremely robust from a fault-tolerance perspective. Some would say cryptocurrencies aren't widely used because there is an inherent chicken and egg problem: Because everyone uses local currency, merchants don't have an incentive to accept anything else. But we actually think the opposite is true. As long as some customers want to pay in cryptocurrency, it costs merchants almost no overhead to accept it, and it costs them sales if they don't. In fact, because cryptocurrencies are immune to fraudulent chargebacks, and transaction fees can be much lower than fees for credit and even debit cards, merchants should actually prefer cryptocurrency payments. We can find two clues to the real problem by examining the perspectives of the merchant and the customer in turn.

- First, consider the merchants that do accept cryptocurrency payments today. Overstock, Namecheap, Virgin Galactic, Square, Lionsgate and PureVPN , for example, allow customers to pay in Bitcoin using a service called BitPay. However, none of these merchants keep their money in Bitcoin—instead, they immediately convert any Bitcoin they receive into USD. Why? Well, these merchants are not in the business of speculating on Bitcoin. They don't want exposure to Bitcoin market risk any more than they want to hold their money in barrels of oil. What if Bitcoin dropped 90% one day? If you ask people who love cryptocurrencies, they might mention many of the attributes they love—for example, the convenience, the control, and the semi-anonymity. But we bet they still can't stomach the idea of keeping their life savings or quarterly revenue invested in such a volatile asset. In other words, in order for cryptocurrencies to become more than just a playground for speculation, there is a severe need for them to be a stable store of value.

- Second, imagine trying to make a purchase using Bitcoin. Because merchants want to collect a fixed amount of USD for their services, you're faced with a constantly adjusting BTC price for your potential purchase. This is a terrible user experience. Even worse, imagine receiving a job offer that pays 1 BTC per month. If the price of BTC happened to drop one month, you can't pay your bills. Alternatively, if you borrowed money via a loan that demands a monthly payment of 1 BTC, a price swing in the other direction could leave you in default. We'll discuss this more later, but the fundamental problem is that today's price-volatile cryptocurrencies subject any contract promising or taking future payments to extreme price risk. From this, we can see that in order for cryptocurrencies to become a viable medium of exchange or unit of account, there is again a severe need for price stability.

Any currency has three fundamental functions: A store of value, a medium of exchange, and a unit of account. We believe that price stability is a gatekeeper to the mainstream adoption of a currency

for any of these purposes. In this whitepaper, we introduce Orch Stable or ORCS, the first non-collateralized unforkable high-velocity cryptocurrency to implement robust, decentralized, and protocol-enforced price stability. Specifically, we discuss the following topics:

• Use cases for a price-stable cryptocurrency: A number of valuable use cases in which a price-stable cryptocurrency would be preferred over the best alternative today.

• How ORCS implements price stability: A specification of a non-collateralized unforkable realtime fully-decentralized, price-stable cryptocurrency protocol, and why it is robust. • Expansion and Contraction of ORCS via ORCE (Orch Equity) and deferred payouts.

• Other Attempts at a Stable Coin: The Competition and downsides of their stablecoin mechanisms.

Use Cases and Applications of a stablecoin

The Increasing Demand for a Non-Sovereign Non-Collateralized Debt-free High-velocity Privacy-preserving Reserve Asset

There are institutional investors like John Pfeffer or Pfeffer Capital who feel the need for a non-sovereign inflation-free alternative reserve asset which apparently fits non-permissioned cryptocurrencies like Bitcoin. This particular alternative reserve asset will be for long-term of storage of wealth free from downsides of fiat hard currencies including US Dollar and Euro such that carries counter-party risks of central banks and large-scale local/global catastrophes, both natural and man-made.

But we have made an argument previously as to why Bitcoin is not the right candidate to be a non-sovereign reserve asset in the following Steemit article linked here: https://steemit.com/ico/@orch/mzufd-intergalactic-money-the-deep-impact-of-a-self-evolving-infinitely-scalable-general-purpose-realtime-unforkable-public-blockchain

While we agree with his following statement: “A non-sovereign, non-fiat, trustless, censorship-resistant cryptoasset would be a far better alternative for most foreign currency international reserves. IMF SDRs are already a synthetic store of value, so could also be easily and sensibly replaced by such a cryptoasset.”, this necessarily does not make BTC the right candidate for several reasons:

1. BTC is not a self-improving self-evolvable fully censorship-resistant cryptoasset which is a must for it to qualify as a viable reserve asset and appeal to long-term institutional and high networth investors. Bitcoins miners are mostly corporate entities having large investments in ASIC-based mining equipment. It’s not impossible to corner 51% mining power by a centralized resourceful entity compromising double spending protection and other trustless security measures built-in. So BTC is not truly decentralized.

2. The underlying hash algorithm and encryption protocol of BTC known as SHA-256 can be broken by multi-qubit quantum circuits and quantum computers under active development in labs across the world. So BTC is not future-proof and its very existence is threatened unless its core developers continuously modify and improve its underlying security model and technology. 3. Bitcoin is not infinitely-divisible that’s it’s not only upwardly non-scalable, the same is true for its

downward scalability. In fact, BTC has only 8 decimal places known as Satoshis (1 satoshi = 0.00000001 BTC)

Futuristic protocol tokens such as infinitely scalable minerless Orch(ORC) should be more attractive to long-term investors looking for an alternative non-sovereign, non-fiat, and trustless, censorship-resistant privacy preserving high-velocity cryptoasset.

A Stable cryptoasset for traders and speculators

A Low-Volatility Cryptoasset for Traders Today, many traders on cryptocurrency exchanges convert their cryptocurrency into USD when there's turbulence in the crypto markets. But this is problematic for a few reasons. First, some of the top crypto exchanges in the world are crypto-only, meaning they don't support conversions into fiat currencies. On such exchanges, traders are in desperate need of a price-stable cryptocurrency that they can use to wait out dips in the broader crypto market. To fill this need, a centralized solution known as USD Tether has arisen—but, for reasons discussed later, a centralized solution like Tether is unlikely to work in the long term, and Tether has faced significant negative sentiment as a result. To that end, Tether's USD2.7 Billion market cap proves the need, but it is also incapable of serving it long term. Additionally, exchanges often list their trading pairs against some base currency. To trade these pairs effectively, users must hold some amount of that base currency, and they must also understand and evaluate prices as defined in that base currency. If this base currency were a volatile asset like Bitcoin, people would have to hedge any Bitcoin exposure they didn't want and constantly convert the price of the trading pair to their local unit of account. Most traders who don't have access to automated trading tools have a difficult time hedging or making conversions, and exchanges catering to a wider audience have a strong need for a stable cryptoasset like ORCS. Only a price-stable non-collateralized non-sovereign cryptocurrency can fulfill these needs of cryptocurrency traders. Because cryptocurrency traders are naturally already enthusiastic about new protocols, this is also where we expect the initial demand for ORCS to come from (i.e., the "early adopters").

The Emerging Decentralized Economy

A number of visionaries in the blockchain and decentralized space believe that we will soon see an ecosystem of "blockchain apps" arise, reimplementing existing services in a decentralized manner. For example, we may one day see a "decentralized facebook", a "blockchain Uber" or "blockchain Airbnb," each with its own app token. In fact, this is already happening with Filecoin reimplementing the Internet's storage layer. See this blog post for a great description of what this broader blockchain economy might look like. Of course, if each blockchain app were to create its own token, there will need to be an interchange system to convert between some "universal token" and all of the different app tokens. We expect that everyone will hold this universal token and pay with it when using a blockchain app. Then, upon payment, the universal token will immediately get converted into the app token at the market rate. This would be similar to having your bank account in USD and using your debit card in a foreign country like Spain, in which case your bank converts your USD into EUR at the market rate every time you make a purchase, without you having to think about it. If this ecosystem of blockchain apps arose, necessitating the need for a universal token, it would be very strange if that universal token were not price-stable. For example, imagine if your daily bus ride to work required USD5 today and USD50 tomorrow. Even more importantly, as we'll elaborate on in the next section, a price-volatile coin is vulnerable to hoarding incentives. If people believe that a coin will appreciate in the future, they are incentivized not to spend their precious appreciating assets. This would kill the blockchain economy before it even got off the ground. In other words, if you believe in the future of blockchain apps, not only should you believe that a

price-stable coin will be needed for interchange—you better hope that a price-stable coin will succeed.

Debt, Credit and Derivatives Markets

Because of their volatility, today's cryptocurrencies are unsuitable for even the most basic financial contracts that our economy relies on. Can you imagine taking a job that pays 1 Bitcoin a month, but still paying your monthly bills in USD—what would happen to you and your family if the price of BTC crashed? What about buying a house with a 30-year mortgage denominated in Bitcoin, but living in a world in which you're probably still paid in dollars? These hypotheticals are unfathomable because credit and debt markets, and in fact markets for any financial contract over time, depend on price stability. As a lender, when you structure a mortgage contract, the biggest risk that you take on is typically the risk of default. But if that mortgage were denominated in a volatile asset like Bitcoin, you're also exposed to extreme price risk. For example, a 30-year home loan denominated in Bitcoin is suddenly worth very little if the price of Bitcoin dropped 90% any day in the next 30 years. To sign the deal, you must either be willing to speculate on the price of Bitcoin in every loan you make, or you must find a speculator who is. Either way, you end up charging the borrower a premium for you or a speculator's willingness to hedge price risk. This adds substantial friction to the simplest of financial contracts. By definition, this friction simply doesn't exist in a price-stable currency. Stable currencies thus reduce costs and increase liquidity for all sorts of financial instruments. At a deeper level, to maintain their stable price, price-stable currencies still require speculators who are willing to trade on expansions and contractions of the money supply. However, instead of operating on individual contracts, speculators operate on the currency itself, creating a pre-hedged, price-stable fungible asset that can be used to structure any deal as a derivative. This is like going from a world in which every home must have its own power generator, to a world in which a power plant leverages economies of scale and generates electricity for whole cities.

As cryptocurrency usage increases, we expect that demand will rise for a cryptocurrency usable for salaries, loans, bets, futures, options and swaps contracts, and more. In a price-volatile cryptocurrency, all contracts that involve payments through time require the friction of a speculator. On the other hand, by offering price stability, ORCS is unique in enabling capital and derivatives markets to form directly on top of its protocol. This is a source of demand that we expect will grow larger and larger as time goes on. Coinship.Trade is the first fully decentralized exchange and trading platform implementing atomic swaps between crypto pairs that will launch cash and derivatives markets with ORCS as the base currency.

Developing Markets with volatile fiat currencies

Developing Markets People living in developed economies take for granted their access to stable currencies. If you're in the US with unfettered access to dollars, or in the EU with access to euros, you may wonder why the world needs a price-stable cryptocurrency. However, in countries with weak institutions and unstable currencies, high rates of inflation and currency devaluation are common. In these markets, we expect a price-stable cryptocurrency will be in high demand. As of publication in Q3 2017, Egypt is suffering 32% annual inflation, Argentina 23%, and Nigeria 16%. And this is just a sampling of countries whose governments are relatively more stable—let's not forget Venezuela, whose annual inflation rate is currently at 741%. What would you do if your savings were disappearing at a rate of 741% a year? Faced with a rapidly devaluing local currency,

people look for other ways to survive, frequently flocking to the USD. This effect is known as dollarization. Generally, it takes three forms: • First, a population might choose to adopt the dollar over local currency without any coordination from the local government. The USD is used as the de facto currency in a number of Central Asian and sub-Saharan African countries, and the rate of adoption can be overwhelmingly fast despite the lack of official coordination. For example, in the 2 years from 2006 to 2008, dollarization in the Seychelles jumped from 20% to 60%. • Second, a country's citizens might demand the dollar in spite of government capital controls that prevent the transfer of USD across its borders. Argentina's black market for dollars, the dolar blue, was an open secret during its reign of capital controls from 2011 to 2015. During these years, $10 million to $40 million per day changed hands under the table at rates that were 25-30% above the official exchange rate. These rates were even published daily in national newspapers, despite it being officially illegal. • Third, currency devaluation could grow so extreme that governments might officially switch to the USD, as happened in Zimbabwe in 2009. Today, the entire country requires routine shipments of physical paper dollars and coins. Isn't there an opportunity here? Whether or not dollarization is officially endorsed, citizens, banks, and governments incur significant costs in importing physical USD. A cryptocurrency solution, by which millions of dollars could be transported on one's phone, seems like a vastly superior alternative to paper dollars in all dollarization scenarios. As a final aside: Existing cryptocurrencies have found some traction off in some hyperinflating economies—for example, Bitcoin usage has been growing in Venezuela as it has faced its currency crisis. However, Bitcoin can never truly free people from their unstable local currencies due to its own lack of price stability. For example, if Bitcoin is going through a cycle of devaluation, users perceive no difference between it and a devaluing local currency. Even if Bitcoin crashes just once, people will want to move to a price-stable alternative—should one exist. A stable coin would thus be the killer app for developing economies experiencing rapid currency devaluation. In the extreme case, instead of switching to importing paper dollars and coins, the next country to switch away from its local currency like Zimbabwe did could instead adopt a price-stable cryptocurrency. Along these lines, in a 2017 speech, the Managing Director of the International Monetary Fund, Christine LaGarde, proposed: [T]hink of countries with weak institutions and unstable national currencies. Instead of adopting the currency of another country—such as the U.S. dollar—some of these economies might see a growing use of virtual currencies. Call it dollarization 2.0. IMF experience shows that there is a tipping point beyond which coordination around a new currency is exponential. In the Seychelles, for example, dollarization jumped from 20 percent in 2006 to 60 percent in 2008. And yet, why might citizens hold virtual currencies rather than physical dollars, euros, or sterling? Because it may one day be easier and safer than obtaining paper bills, especially in remote regions. And because virtual currencies could actually become more stable. For instance, they could be issued one-for-one for dollars, or as table basket of currencies. Issuance could be fully transparent, governed by a credible, pre-defined rule, an algorithm that can be monitored...or even a "smart rule" that might reflect changing macroeconomic circumstances. So in many ways, cryptocurrencies might just give existing currencies and monetary policy a run for their money.

Anti-fragility Insurance and Protection against Blackswan/Tail events

Hedge Fund Managers, Reinsurance companies and sovereign wealth managers are always looking for assets that can act as the most robust hedge instrument against tail risks or so called blackswan events that are by nature unpredictable and highly impactful.

Besides acting as a hedge against negative blackswans, ORCS doubles up as a bridge to expose an institutional investor's portfolio to cryptoassets as ORCS will probably act as the base universal currency for the crypto universe or crypto economy. Allocation of funds to ORCS tokens and ORCS futures/options would allow any institutional or wholesale investors to take exposures in

positive blackswan scenarios with 10x to 100x plus potential payoffs with relatively shorter investment horizons.

Total Addressable Market (TAM)

Total addressable market size or TAM of ORCS could be as high as USD35Trillion to USD50Trillion by 2028 (July 2018 USD value).

How ORCS enforces price-stability?

ORCS implements price stability by leveraging unprecedented power of its underlying realtime unforkable federated blockchain Starcash of Orch Network [1]. Starcash being infinitely-scalable as well as divisible enables ORCS to dynamically expand and contract the total coin supply in response to sharp increase or drop in its price relative to target indices, variables and assets. ORCS subprotocol of Orch implements a coin split (like a stock split) as a mechanism of this dynamic money supply policy. For example, if John holds 1 ORCS and demand for the stablecoin rises, the system would electronically change John's balance to 1.03 ORCS in his ORCS Orch-powered mainnet wallet. For a contraction, a "reverse coin split" would change his balance from 1 ORCS to 0.97 ORCS.

$$\Delta p^i \int_{-100}^{0} \int_{0}^{100} X = f(X)^{i-1th} = \sum_{i=0}^{\infty} \vec{K}[2(a+b) + X^2 - Y]$$

$$\vec{K} = Schelling\ Point\ Vector\ of\ Truth\ Game\ based\ on\ Range - bound\ parameters;$$

$$a = Average\ Transaction\ Fee\ Now;$$

$$b = Hashrate\ of Subprotocol\ ORCS\ Now;$$

$$X = Coinship\ Index\ Level[A\ Subprotocol\ powered\ by\ Orch\ Starcash];$$

$$Y = External\ Datafeed\ of OECD\ CPI\ Data\ Now$$

$$p^i = Price\ of\ ORCS\ at\ i^{th} time;$$

Fig 1.0. A Delta Equation demonstrating referred assets and indices(external and internal) of ORCS stabilization sub-protocol implemented via dynamic coin split/reverse split.

A Post-USD Interplanetary Economy

A Post-USD Interplanetary Economy will be dominated by semi-sovereign networks of corporations and autonomous organizations e.g. space mining companies, organizations operating space-based habitats and worlds and space-based solar farms and Martian colonies as well as Lunar heavy industries and so on.

Initiatives by Blue Origin and SpaceX are already pointing in this direction. Now all these participants will need a universal currency to conduct interplanetary trades. Sovereign fiat currencies of today e.g. USD and Euro are ill-suited for this purpose. ORCS perfectly fits the specification required to run an interplanetary economy.

The Competition

Tether (USDT)

Tether (symbol: USDT) is very interesting, but to us it's not really a cryptocurrency. Tether is run by a company that stores one USD in its reserves for every Tether coin that it mints, and it promises its users the ability to retrieve their USD by returning the Tether coin that accounted for it. In other words, Tether is basically a company taking deposits and issuing their own currency, similar to what eGold was doing in the 1990s—in fact, there is no reason Tether even needs to be a cryptocurrency, rather than a centralized database. While this centralized reserve-based approach can work in the short run, we think there are significant disadvantages overall: • There is a risk that any company taking fiat reserves will be shut down at any time, just like what happened with eGold. The Tether team has been secretive about its banking relationships and restrictive when users want to withdraw their USD. • The owners of Tether have complete control over the money supply, which makes them a single point of failure in general. • Tether can never become independent from fiat because its value fundamentally comes from fiat. In contrast, ORCS has a monetary policy built-in and one which can be evolved as we enter into a space-based interplanetary economy by next decade and beyond.

BitShares

BitShares Below is how BitShares stable coins work. • There are BitShares and BitUSD, a multi-asset system like Basis. • BitShares implements an exchange on its blockchain between the two, so there are always people willing to buy/sell both assets.

People can do two things: They can "go long" BitUSD, which means they make money when it goes up, or they can "go short" BitUSD, which means they make money when it goes down. • If you want to long BitUSD, you just buy a BitUSD for its listed price with dollars. That part's easy. Then, if the price goes up, you can sell it for its listed price later and make money. • If you want to short BitUSD, you give the blockchain $1 in BitShares, as determined by the exchange rate feed, and it'll lock it up for 30 days. Then, there are a few nuances to what happens: ◦ If the price of BitUSD goes up, then you'll get fewer BitShares back after 30 days. ◦ If the price of BitUSD goes up a lot, you might get margin-called and lose all of your BitShares. ◦ If the price of BitUSD goes down, then you'll get more BitShares. Under the hood, when you put your $1 worth of BitShares onto the blockchain, the blockchain does the following: • ◦ It creates 1 BitUSD out of thin air. ◦ It sells that BitUSD to someone, thus effectively increasing the supply of BitUSD. ◦ This is also how shorting works in real life, but you don't have to worry about it as a shorter—you just give it your BitShare and then you get back more/less depending on what happens to the price of BitUSD. • BitUSD only exists because someone decided to enter a short contract. If nobody wanted to short BitUSD using BitShares, then no BitUSD would exist. • When you sell a BitUSD you can either give it to someone else, or you can autoliquidate the person who has the other side of a short contract. If you do the latter, the supply of BitShares increases, driving up the price of BitUSD. Overall, the BitShares protocol has several drawbacks that are deal-breakers for implementing a stable coin: • The BitUSD peg is enforced by a weak self-reinforcement scheme backed by the BitShares company as a lender of last resort, not by the protocol itself. The only reason BitShares

are worth 1 USD is because everyone believes it'll be worth 1 USD, and therefore everyone always shorts and longs in order to keep it there. If everyone one day just decides that BitUSD should be worth $100, then the equilibrium will adjust, and it'll re-peg to $100. The only reason it's even stayed stable this long is likely because the BitShares company acts as lender of last resort to enforce the peg when someone tries to break it. But this will almost certainly get too expensive one day, resulting in the complete breakdown of BitUSD as a price-stable currency.

Incidentally, when we explained this to one of our friends, he immediately suggested we raise a few million dollars and use it to demolish the peg by bidding it up to a new equilibrium, which would be extremely profitable, in the same way George Soros broke the bank of England. Note that this is much different from ORCS protocol, where a negative feedback loop is enforced at a protocol-level to keep the price pegged to USD, Euro and CHF. • BitShares wasn't designed to be a stable coin, it was designed to be a prediction market. Although the above weakness is a complete deal-breaker for a stable coin in our opinion, it's important to remember that BitShares is useful for much more than a stable coin—it's a generalized prediction market that you can use to place bets on anything. For that reason, we would guess (though we don't know for sure) that BitShares wasn't even really designed to implement a stable coin, and the fact that you can have them on its platform is just a happy coincidence, and a testament to how generalizable their platform is.

Dai

MakerDAO is a project that aims to create a stable token, called Dai, backed by decentralized reserves. At a small scale, we think it is relatively easy for any system to remain stable by having early supporters subsidize a stable price for the coin. But we think Dai does not sufficiently balance supply and demand to stay stable in the long-term. Examining the incentives behind the MakerDAO protocol, we've come to believe that: • Dai is unscalable. Dai supply is restricted because there is insufficient incentive for people to lock up collateral in CDPs. CDPs offer collateral holders the opportunity to obtain leverage in a decentralized way. However, the MakerDAO system requires that CDP owners borrow in Dai. Since Dai can spike up in value during collateral crashes, when someone locks up collateral in a CDP, they must either lock up their collateral at a very high collateral-to-debt ratio resulting in low amounts of leverage, or they must bear the risk of having to repurchase Dai at a higher price to close their CDP and avoid liquidation. Neither makes CDPs very competitive with other alternatives for leverage, since centralized futures and other upcoming decentralized lending services arguably offer less risk, more leverage, and a better user experience. • Dai price can easily float up to the liquidation ratio (~$1.50 for example). Aside from the belief that Dai is worth $1, there is no incentive that keeps Dai from wandering up to a higher price. To see this, imagine that there is a collateral crash, say in ETH. On the one hand, people are fleeing ETH and flocking to more stable assets, increasing the demand for Dai. On the other hand, the collateral-to-debt ratio of CDPs is falling, causing Dai to be destroyed as some CDPs are liquidated while some others are closed by their owners to avoid liquidation. The combination of Dai demand increasing just as Dai supply decreases causes Dai price to spike above $1, restricting the usefulness of Dai just as people need it. In these situations, only early supporters who hold large amounts of ETH can be relied upon to subsidize the creation of more Dai by locking up more ETH in CDPs. Absent this artificial force, Dai price is free to rise as high as demand takes it, potentially up until the liquidation ratio, at which point CDPs are allowed to hold less ETH than a Dai is worth, creating a riskless arbitrage. Note that this assumes the system's Target Rate Feedback Mechanism is disabled. • Dai is fundamentally unstable with its Target Rate Feedback Mechanism enabled. This mechanism aims to stabilize the price of Dai by adjusting the rate at which Dai's target price changes. While this creates an incentive for Dai to revert to its target price, it also changes where that target price moves. When triggered, Dai is more stable, but it is "stabilized" against an unstable, unpredictable target. • Dai and MKR devalue under massive crashes in collateral. In the worst of collateral crashes, MakerDAO's auto-liquidation policy means that either Dai devalues or

MKR devalues, and there is no mechanism for restoring prices. • MKR, the investor token for MakerDAO, pays out poorly. It earns very little from stability fees, and it is subject to the risk of occasional dilution. • The MakerDAO stability analysis totally fails to analyze the protocol's economic incentives. From a high level, we find the idea of a reserve-backed cryptocurrency intrinsically appealing. If a reserve-based system can create a rewarding enough incentive for people to deposit reserves, and it can additionally address counterparty risk and the risk of its reserves suffering a black swan crash, then it should be able to remain broadly stable, at least in the short to medium term. However, we think it's very difficult for a project to overcome all of these hurdles. We think that MakerDAO can grow to a small size, subsidized by its early supporters on the supply side and serving fans of decentralized reserve-based currencies on the demand side. However, because MakerDAO doesn't solve the fundamental challenges of building a reserve-backed cryptocurrency, MakerDAO ends up neither widely usable, nor particularly stable.

Conclusion

Imagine a world in which Bitcoin starts competing with the USD in transaction usage. You would get paid in Bitcoin but pay rent in USD, or perhaps vice versa. This just doesn't make sense given Bitcoin's inherent volatility. In this paper, we introduced ORCS, a robust, decentralized implementation of a price-stable cryptocurrency. We believe that if we can just make it so that purchasing power doesn't fluctuate, people will shift from a mindset in which they hold as little cryptocurrency as possible, to a mindset in which they are comfortable holding their savings or revenue in it. We believe this contribution will trigger cryptocurrencies to undergo a virtuous cycle of adoption and help them transition into a mainstream medium of exchange—a result that has eluded every other cryptocurrency thus far.

Contact

If you have any thoughts or want to be involved in the project, feel free to email the author as shown on the title page. For the most up-to-date version of this whitepaper, please visit https://orcs.fund

References:

1. Orch Network: https://orch.network