White Paper

CAVORITE

A FIAT CRYPTOCURRENCY

Ajai Pratap Singh
3/15/2018

ABSTRACT

The big bang moment for the Blockchain universe happened when BITCOIN was born in 2008-2009, BITCOIN was conceptualized as a peer to peer electronic cash system, free from any centralized governing authority which brought forward the idea of underlying blockchain technology and governance by distributed consensus, Since then blockchain technology has evolved and brought forward its many applications beyond cryptocurrency which is best demonstrated in Ethereum by its use of smart contracts over a blockchain, at present there are many successful and proved crypto currencies are in the market like **BITCOIN,MONERO, ZCASH** etc and the number of crypto assets is growing exponentially day by day.

But in spite of so many solutions being present in the market claiming to be a currency, the real world application for these crypto assets is still limited only to investment and exchange with each other, their exchange with goods and services majorly happens over the black market in need for anonymity, and open market exchange for goods and services is still really limited. Volatility of these asset prices day to day makes them hard to be traded for stable value goods and services. Trading them with goods and services is like old world barter system where buyer and seller both can feel that they received lesser value during the exchange.

With our solution we are trying to address this issue and create a cryptocurrency which is stable in value up to the extant real world currencies are and any upward movements in the currency price comes with assurance that the prices will not fall back below a certain limit so that prices of goods and services can be kept trading in exchange of it with minimum associated risk of value deterrence.

In order to explain our solution further we will first try to look deeper into the fiat currency which in general terms can be called money, We will inspect Fiat Currency from a value perspective to analyze what is underlying value of money and why and how it is easily tradable with goods and services even when the value of money in almost all countries change with respect to each other in international exchange continuously as the cryptocurrencies.

TABLE OF CONTENTS

A look at fiat money from Macroeconomic Perspective

The Evolution of Fiat Money [1]

Money has taken many forms over the centuries. If we loosely define money as a widely accepted medium of exchange, then we can say that there have been thousands of different types of money used globally over the past few thousand years including, but not limited to, cowry shells (used as currency in Africa and China), koko (a unit of rice used in Japan's feudal system), grain, copper, bronze, gold coins and paper notes.

However, our purpose today is not to discuss all the various forms that money has taken, but rather to discuss how money has evolved from commodity money to the fiat money that we use today.

In nearly every society, the first form of money used was some form of commodity money, money that was, quite literally, a basic commodity that had value in that society. Over time, as commerce became more sophisticated and trade became more widespread, the use of perishable commodities (such as grain and rice) as money became less common. Less-perishable commodities, such as copper, silver and gold became the predominant mediums of trade. The acceptance of these metals accelerated when they were issued in coin form.

All of these forms of commodity money derived their value from their physical properties. Early coins were accepted because the metals they were made of were valuable in and of themselves. If a government started debasing their coins, often by reducing the amount of the metal in the coin, then the value of the coin would fall and prices, as measured in terms of that coin, would rise.

Even in the times of the Roman Empire, the principle that the value of money is the denominator of the price level. As the Romans debased the value of their coins (by cutting down on the metal content of each coin), prices began to rise, "Ratio Theory of the Price Level".

The point is that money in ancient societies, commodity money, was a real asset that derived its value from its physical properties.

The problem with commodity money is that it restricts the capability of governments to finance wars and other public expenditures: you can't pay your armies in gold coin if you run out of gold. This problem led to the invention of the first "representative money". Rather than paying the armies in gold, the ancient kings and emperors decided to pay soldiers by issuing pieces of paper that were promises to deliver gold on request.

The first paper money was nothing more than a legal contract: an explicit contract that promised, on request, the delivery of a certain amount of gold or silver from the treasury of the king. The value of this paper money was derived solely from its contractual properties.

Many of the major modern currencies we use today were, at one time, asset-backed currencies. The British Pound and the US Dollar, the two currencies that dominated global trade over the last three hundred years, were both gold-backed currencies for many years. For a long time, the value of both these major currencies depended upon the explicit contract that promised holders that they were convertible into gold.

However, there was one key problem with this arrangement: it limited the amount of money that both governments could create.

At some point, it was decided that we should simply drop the gold convertibility feature. In effect, the explicit contract that promised holders this piece of otherwise worthless paper could be exchange for a real asset was rendered null and void.

So, why did these currencies maintain any value at all? After all, when these paper currencies were first issued, the only reason they were accepted in exchange was because they were "as good as gold".

The popular view is that these paper currencies maintained their value because, after many years, people were accustomed to using them. In the language of an economist, the fiat money maintained its value when the gold convertibility feature was removed because it was already widely accepted as a medium of exchange.

The problem with this argument is that it relies on a circular argument, a form of logical fallacy.

In order for something to act as a medium of exchange it must have value. Benjamin Anderson, in his book "The Value of Money" (1917), states, "The medium of exchange must have value, or else be representative of something which has value. There can be no exchange in the economic sense without a quid pro quo, without value balancing value, at least roughly in the process".

What does this mean? In simple terms, we are not going to part with something of value (a good or service) unless we receive something of value in return. We will not accept money in exchange unless it possesses the property of market value.

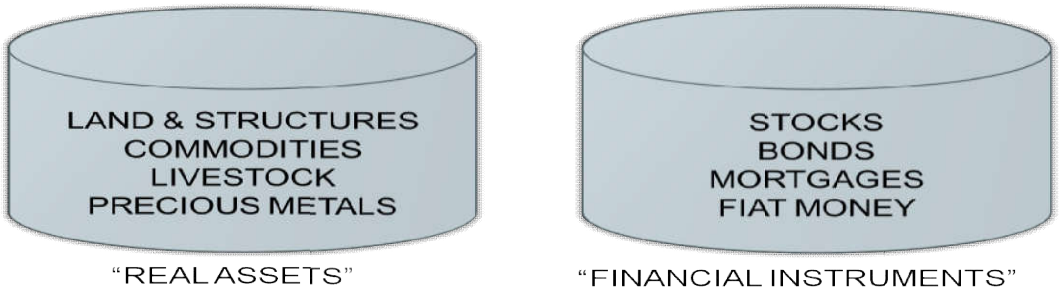
Therefore, money can only serve as a medium of exchange because it has value.

Now, let's ask the question again "why does money have value?" Can you see the problem? Is it reasonable to argue that money has value because it is a medium of exchange if we also recognize that money serves as a medium of exchange because it has value? No, it isn't. What we have created is a circular argument.

We can only resolve this circular argument by breaking one of its legs. Notably, we need another way of thinking about how fiat money derives its value. Fiat money must have value in order to act as a medium of exchange, so how does it derive this value?

Why Does Fiat Money Have Value? [1]

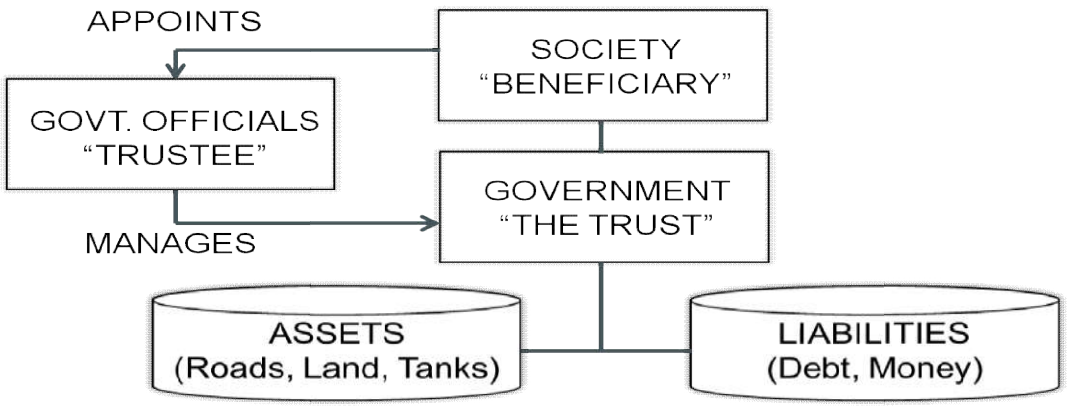
It is generally recognized that all assets derive their value in one of two ways: real assets derive their value from their physical properties, while financial instrument derive their value from their contractual properties.



Fiat money is not a real asset and does not derive its value from its physical properties. Therefore, prima facie, fiat money is a financial instrument and must derive its value from its contractual properties, even if that contract is implied rather than explicit.

Most economists haven't spent much time speculating on the potential nature of the implied contract that money represents. This is unfortunate because such speculation could provide interesting insights into how the value of money is determined.

We can apply at least some elements of traditional finance theory to a theory of money. First, we need to identify the issuer of money. While the legal issuer of base money is the government, the ultimate economic issuer of money is society itself.

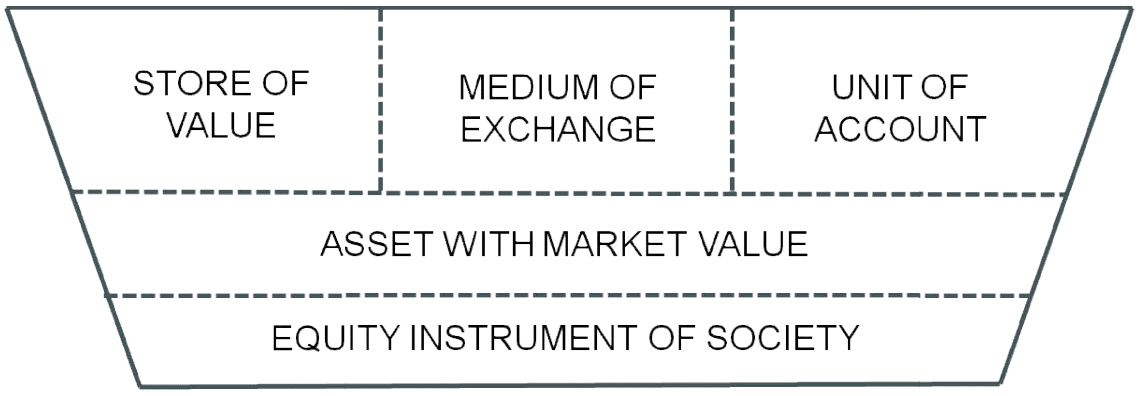


Second, we need to think about what it economic benefit is possessed or created by the issuer that could be promised to the holder of money. In the case of society, the obvious economic benefit that could be promised is future economic output. As the slide below illustrates, society can implicitly authorize government to issue claims against the future output of society. Although fiat money (the monetary base) is *legally* a liability of government, *economically* it is a liability of society itself and a claim against the most valuable economic benefit society produces: its future output.

Third, we need to consider whether the claim represents a fixed or variable entitlement to that future economic output. Our view is that money represents a variable or proportional entitlement to the future economic output of society.

Characteristic feature	Equity	Debt
Fixed payment on the instrument		✔
Fixed term/maturity		✔
Participation in ongoing profits/losses	✔	
Subordination	✔	
Variable claim on repayment	✔	

In this sense, money is a special form of equity instrument: just as a share of common stock represents a proportional claim on the future cash flow of a business, one unit of base money represents a proportional claim on the future economic output of society.



(The Bedrock beneath the Functions of Money)

Money as the Equity of Society [1]

So far it has been established that fiat money is a special-form equity instrument. More specifically, each unit of the fiat monetary base represents a proportional claim on the future output of society, just as a share of common stock represents a proportional claim on the future cash flows of a corporation.

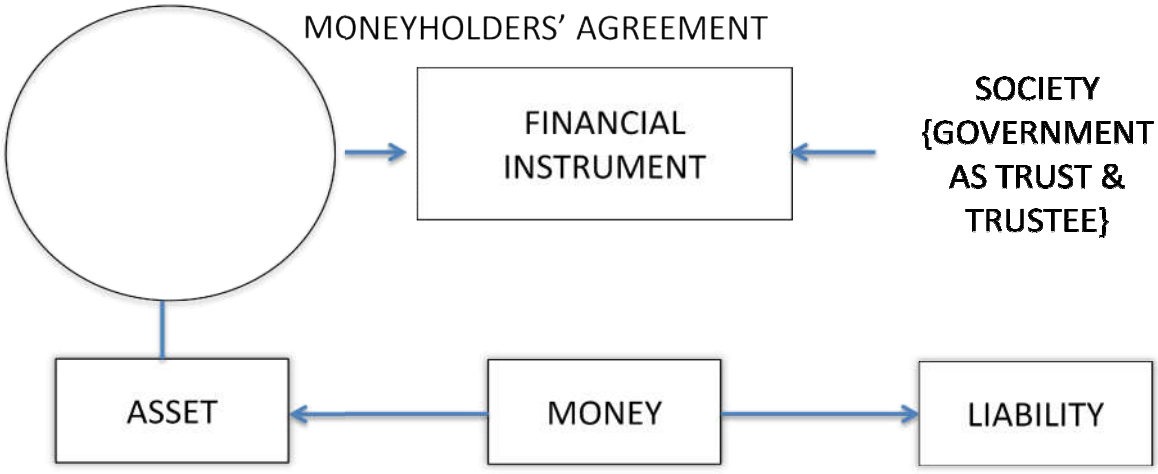
The idea that fiat money is an equity instrument begins with a simple observation: fiat money is a financing tool. Society has three options when it wants to fund public activities: raise taxes, issue debt (government debt) or print money. The monetary base represents a way to fund the public activities that we are not prepared to pay for with current taxes or future taxes (government debt).

We can compare this to the financing options faced by a typical corporation. Most companies face three basic choices when considering the funding of new projects: use existing cash flows, issue debt or issue equity.

The choice of issuing debt or equity for a corporation can be a complicated one, but generally it boils down to one simple issue: does the corporation want to create fixed claims against its future cash flows or variable/proportional claims against its future cash flows?

In the case of a corporation, the equity issued by that corporation has value because it is a proportional claim against the future cash flows of the company. The holder of that equity is party to a shareholders' agreement that promises equity holders a variable entitlement to the future cash flows of that business.

Just as a shareholders' agreement governs the contractual relationship between the issuer of common stock and the holders of that stock, so the implied-in-fact "Moneyholders' Agreement" governs the contractual relationship between the issuer of money and the holders of money.



Since there is no explicit contract, or at least no explicit contract that is meaningful, unraveling the terms of the Moneyholders' Agreement involves a degree of speculation. But we can at least apply the framework that is used for traditional financial instruments so that we know the right questions to ask.

Every financial instrument must possess certain characteristics in order for it to have value. First, it must entitle the holder of the instrument to some future economic benefit, a future economic benefit that the issuer has the capacity to offer. Second, it must entitle the holder to either a fixed or variable (proportional) claim against that future economic benefit.

For example, in the case of shares of common stock, each share entitles the holder to a future economic benefit (future cash flows) that the issuer (the issuing company) has, at least in principle, the capacity to offer. Furthermore, it entitles the holder to a proportional claim against that future economic benefit (the proportion of future residual cash flows each share claims varies in proportion to the number of shares issued).

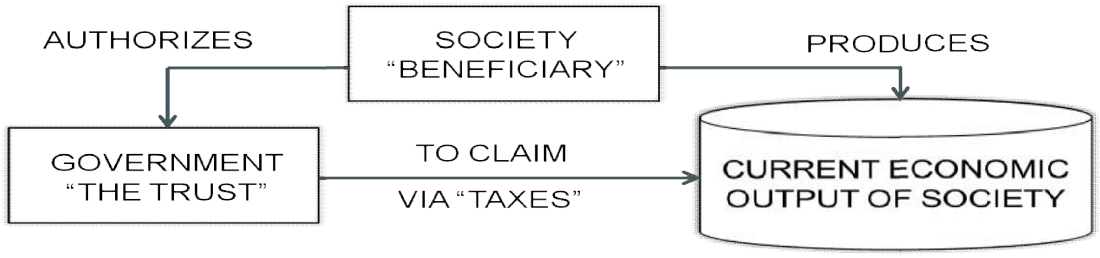
Let's think about these two characteristics and how they apply to the monetary base.

First, if base money is a financial instrument issued by society, then what future economic benefit can society offer to the holder of money? Let's put this question another way. What does society have that it can use to pay its bills?

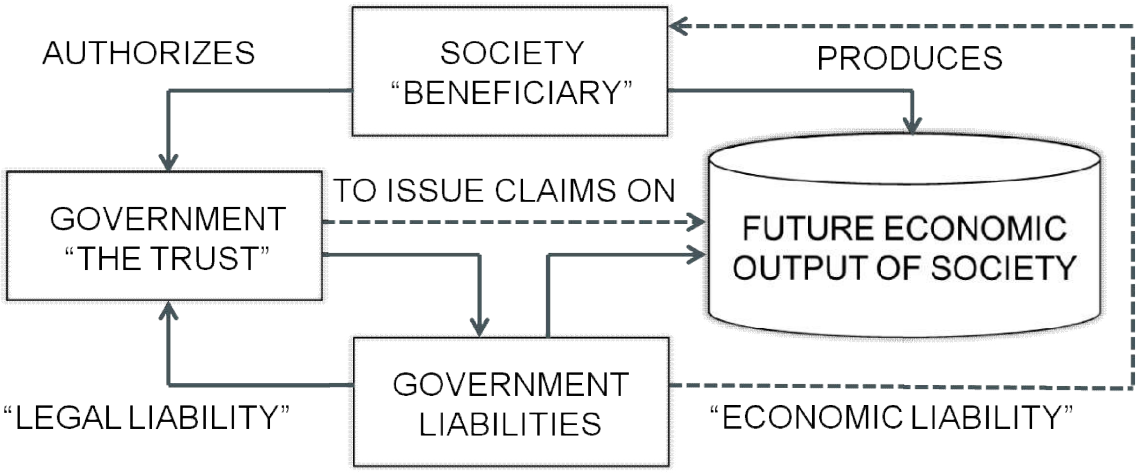
The answer is "economic output".

If we circle back to the beginning of this post, we noted that society has three ways to pay its bills: taxes, debt or money. Taxes are a claim on *current economic output*. Government debt represents a claim on *future economic output*.

If society doesn't wish to pay for current public expenditures by sacrificing current economic output, then it can issue claims against future economic output. Moreover, just as a corporate entity can issue fixed or variable claims against future cash flows, so society can issue fixed or variable claims against future economic output.



(Taxation as a Claim on the Current Output of Society)



(Government Liabilities as a Claim on the Future Output of Society)

It provides us with a framework for thinking about what determines the value of fiat money. If fiat money (the monetary base) is a proportional claim on the future output of society, then the value of fiat money primarily depends upon expectations regarding the long-term economic prospects of society. More specifically, the value of fiat money is positively correlated with expected long-term real output growth and negatively correlated with expected long-term monetary base growth.

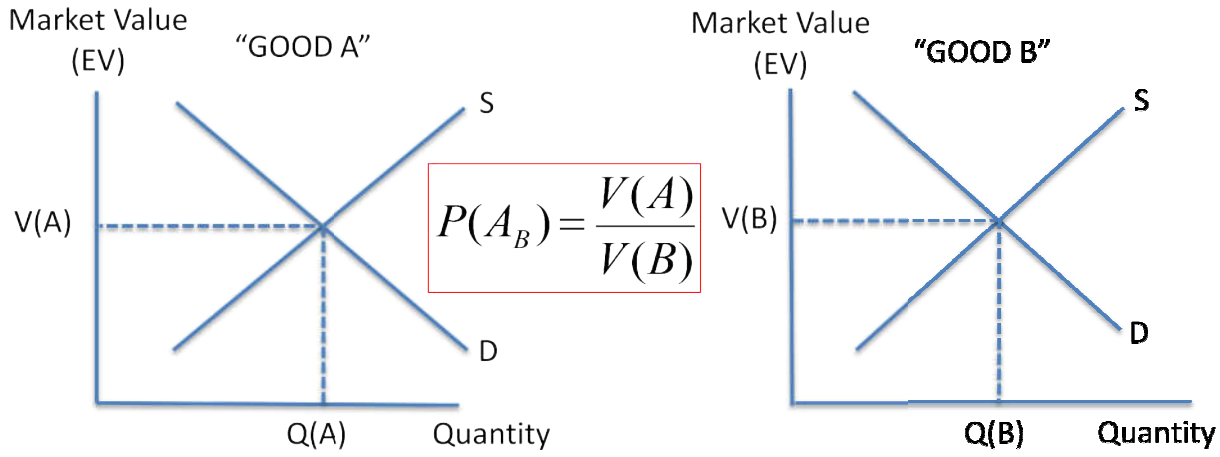
In simple terms, we can think of the value of fiat money as a slice of future output cake. As the expected slice of future output cake gets smaller, the value of fiat money falls. The expected size of our slice of future output cake can shrink either because (a) the expected size of the cake shrinks (expectations for future output growth fall), or (b) we expect that the cake will need to be cut up into more slices (expectations for future monetary base growth rise).

Price Determination [1]

Every price is a function of two sets of supply and demand. More specifically, the price of one good ("the primary good") in terms of another good ("the measurement good"), is determined by *both* supply and demand for the primary good *and* supply and demand for the measurement good.

The traditional microeconomic view is that price is determined by only one set of supply and demand, namely supply and demand for the primary good. For example, the traditional view is that the price of apples is determined by supply and demand for apples.

The problem with this perspective is that it underplays the critical role played by the measurement good. More specifically, in order for the primary good to be priced in terms of the measurement good, both goods must possess the property of market value.

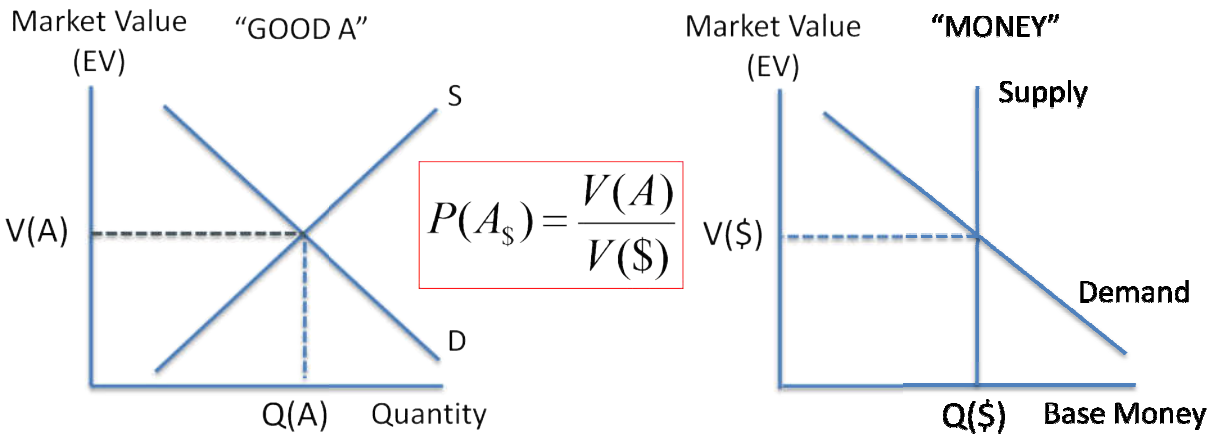


The *market value* of a good is determined by supply and demand for that good. The market value of the primary good is determined by supply and demand for the primary good. The market value of the measurement good is determined by supply and demand for the measurement good.

The *price* of the primary good, in terms of the measurement good, is a relative expression of market value: the market value of the primary good in terms of the market value of the measurement good.

Therefore, the price of the primary good, in terms of the measurement good, is determined by *both* supply and demand for the primary good *and* supply and demand for the measurement good.

This theory represents a *universal theory of price determination*: it applies to the determination of prices in a barter economy ("good/good" prices), prices in a money-based economy ("good/money" prices) and foreign exchange rates ("money/money" prices).



Supply and demand for the monetary base determines the market value of money, the denominator of every money price in the economy. Supply and demand for money (the monetary base) does not determine the interest rate, as suggested by Keynes' liquidity preference theory.

Monetary & Fiscal Policy as a tool to control the value of money [1]

The goal of this final section of the paper is bring together all the work done so far to analyze the impact of monetary and fiscal policy on inflation

Three Basic Scenarios:

- *In order to illustrate the potential impact of monetary and fiscal policy on the price level, three different scenarios arise and need to be analyzed.*
- *In the first scenario, there is no central bank and an increase in society spending is directly financed by base money creation (deficits are monetized).*
- *In the second scenario, there is a central bank and that an increase in base money is used to reduce interest rates via traditional open market operations.*
- *In the third and final scenario, we will analyze the impact on an increase in society spending that is financed by the issuance of debt (no change in base money).*

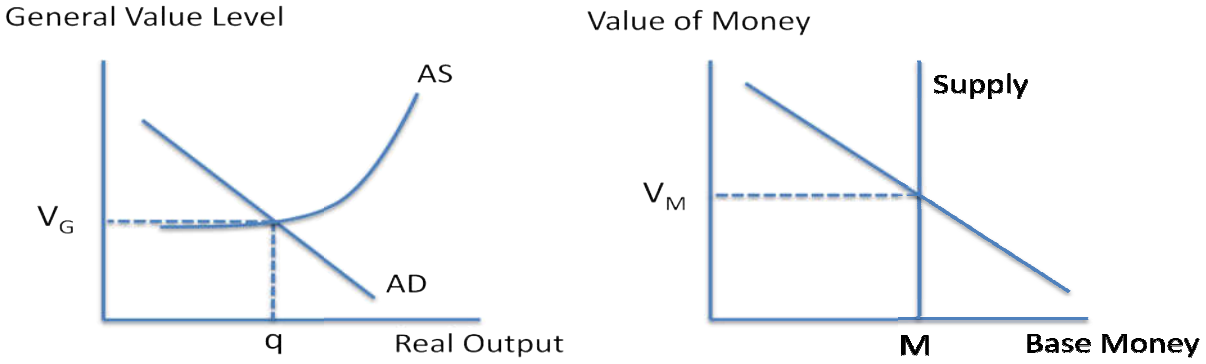
But we will only focus on scenario 1 where there is no bank just like cryptocurrencies, one can point that there are big differences but we will address them latter in this paper

Scenario One: Printing Money Equals Inflation? Not Necessarily

- *What is the response of real output and the price level to an increase in government spending that is directly financed by base money creation? The classical view would be that the price level would rise and there would be no impact on real output (there is no money illusion and no change to real economic outcomes). A Keynesian view might suggest that, in the short-term, there would be an increase in real output due to sticky wages/prices: the short-term impact on the price level would depend on whether the economy is at/near full utilization (the output gap).*
- ***The view of this paper is that the response of real output and the price level will depend largely upon whether the increase in base money is expected to be temporary or permanent, with the output gap acting as a secondary factor.***

Possible Reactions to Money Financed Deficit Spending:

The short-term reaction to money financed deficit spending will vary significantly depending upon specific circumstances and expectations. Let's consider how money financed spending could result in a significant increase in output but only a small change in the price level.



Let's use the long form version of the Discounted Future Benefits Model to consider why the market value of money is stable in this particular scenario. In our current scenario, the only terms that might change in the equation below are the "near future" terms.

$$V_{M,0} = \frac{1}{n}\frac{(V_{G,1}\cdot q_1)}{(M_1\cdot v_k)}\cdot\frac{(1+i)^1}{(1+d)^1} + \frac{1}{n}\frac{(V_{G,2}\cdot q_2)}{(M_2\cdot v_k)}\cdot\frac{(1+i)^2}{(1+d)^2} + \ldots\ldots + \frac{1}{n}\frac{(V_{G,n-1}\cdot q_{n-1})}{(M_{n-1}\cdot v_k)}\cdot\frac{(1+i)^{n-1}}{(1+d)^{n-1}} + \frac{1}{n}\frac{(V_{G,n}\cdot q_n)}{(M_n\cdot v_k)}\cdot\frac{(1+i)^n}{(1+d)^n}$$

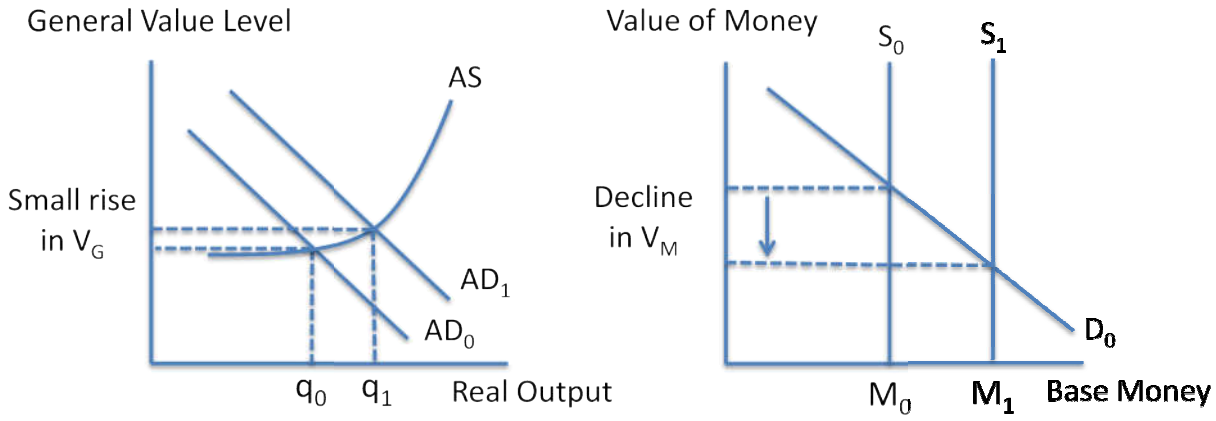
[Note: while this version of the DFB model is not as intuitively appealing as the constant growth version, it is often the better version to use in macroeconomic scenario analysis.]

The "near dated" terms in the DFB model are impacted positively by the increase in real output and negatively by the increase in base money. This might lead to a slight increase or decrease in the value of money. However, the key point is that these "near dated" terms have little overall impact on the absolute market value of the long-duration asset (money).

The "far dated" terms in the DFB model are unlikely to change significantly: both the increase in real output and the increase in base money are generally considered to be "temporary". {There is a possibility here that the rise in current economic activity is extrapolated into higher long-term real output growth rates, an increase in the value of money and a fall in the price level!}

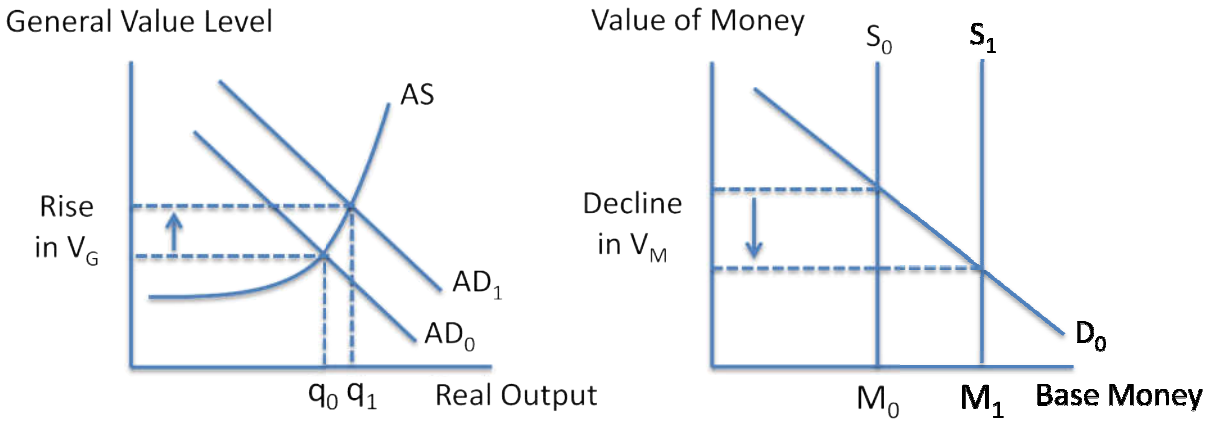
Outcome if Increase in Base Money is expected to be Permanent:

If people believe that money financed deficit spending will lead to a permanent increase in base money (higher future levels of base money), then the absolute market value of money declines. There is an increase in real output but only at the expense of a higher price level.



Worst Case Scenario: Small Increase in Real Output, Big Rise in Price Level

If the economy is operating near "full capacity" and people believe that money financed deficit spending will lead to a permanent increase in base money, then the "perfect storm" is created. There is a large increase in the price level (V_G rises, V_M falls), but a small increase in real output.



Fiscal Policy Plays a Key Role in Preventing Inflation:

- If this view of the world is correct, then one of the important implications is that fiscal policy makers have a critical role to play in preventing inflation and protecting the value of the currency.
- Economics has created a somewhat artificial divide between the liabilities of government and their role in price determination. Ultimately, the future economic prospects of society are beholden to the fixed entitlement liabilities of government (both government debt and unfunded liabilities). In many ways, the absolute market value of money is merely a gauge of market confidence regarding those future prospects and society's ability to "service" the fixed entitlement liabilities from future output.

Lessons from Fiat Currency:

So far it has been established that there is some value hidden inside fiat currency, and what societies must do in order to have a stable and easy to use currency. Now let's try to analyze what features are must in a cryptocurrency in order to be as close as possible to a fiat currency.

We are not going to elaborate on technical must have features like security and decentralization, instead we will emphasize on additional measures which need to be taken to take the decentralized currency systems close to the acceptability of fiat currency and reach a new level of adoption that the existing cryptocurrencies have been unable to achieve so far.

1. **A Targeted & Loyal Community**: As established earlier that a fiat currency is a liability to its issuer, the society itself. Without that there cannot be any value to a currency, any cryptocurrency must have backers who are willing to exchange the currency with the fruits of their labor and not just some other currency. This can only be achieved if the community is inclusive part of the ecosystem and the future benefits generated from the ecosystem are passed to them as in fiat currency.
   In order to be exchangeable with goods and services the currency must have stable value and a secured future which is achieved by the presence of a fiscal policy or monetary policy or combination of both in Fiat Currencies.
2. **Fiscal & Monetary Policy:** Monetary policy is primarily concerned with the management of interest rates and the total supply of money in circulation and is generally carried out by central banks such as the Federal Reserve. While Fiscal policy is the collective term for the taxing and spending actions of society for its benefits and increasing economic output and expansion. Fiscal policy acts as a bridge between the community and monetary policy. This feature is must in order to maintain a loyal following like the fiat currencies.
3. **Controlled Foreign Exchange:** inflow and outflow of currency of one society to other must be controlled to minimize foreign exchange value fluctuations. In real world, countries manage a foreign currency reserve received for exchange of goods and services with other countries in order to manage the escaping of currency outside and be locked out of circulation. The escape of currency can create shortage of currency in the society with respect to production which can pump the values of currency itself.
4. **Risk free to accept:** The value of currency must not lie in holding it but spending, if the benefit of holding is more, then nobody will want to exchange it with goods and services. For free trade to happen both parties need to think that they received more value in the exchange from their viewpoints so only a secure value currency can be counted as risk free to accept.
5. **Fast payments:** Time is of essence, the transactions speed for any currency must be fast to exchange and comparable with fiat money if not. This speed is what makes Fiat much more suitable for exchange with goods and services.

CAVORITE: A Fiat Cryptocurrency

Central Authority as Value Controller:

In order to minimize the value deterioration of currency, CAVORITE consists of a monetary authority, a smart contract whose sole purpose is to controls the value of currency in order to ensure stability.

The monetary authority is the sole issuer of currency similar to a central mint in government banking system, from the first circulation CAVORITE is issued with a set Ceiling and floor price by the monetary authority.

The benefit of having the central authority as the sole currency issuer is that we not only get a stable and secured value currency but also a profit is generated with each new issue.

PROFIT = (SALE PRICE-PURCHASE PRICE) * NO. OF CAVORITE

The role of this authority is to issue and update ceiling and floor price for the currency continuously. It sells CAVORITE at sale price and buys them back at floor price.

If at any time market exchange Rates fall below the floor price decided by the authority, people can start to sell the coins back to the authority instead of selling on exchanges. This in turn will lower the circulation of CAVORITE from the market. This lowered circulation will help CAVORITE prices to move upward again.

Once the prices of CAVORITE in open market reach above floor price people will automatically stop selling to the authority, if the price of CAVORITE rises above the Ceiling rice set by the authority by a certain preset percentage, the authority will start to sell the bought back CAVORITE in the market again, increasing the circulation and lowering the prices of CAVORITE.

During this transition the authority earns a profit again by the formula mentioned earlier,

Even after releasing the bought back coins if the market price of CAVORITE does not fall and each the predefined increase from the decided ceiling price, the monetary authority will generate a short term circulation by creating and selling extra CAVORITE coins and in order to lower the price again and generating some profit again. This is an ever running process so the total number of CAVORITE coins available in the market at a given time is impossible to calculate,

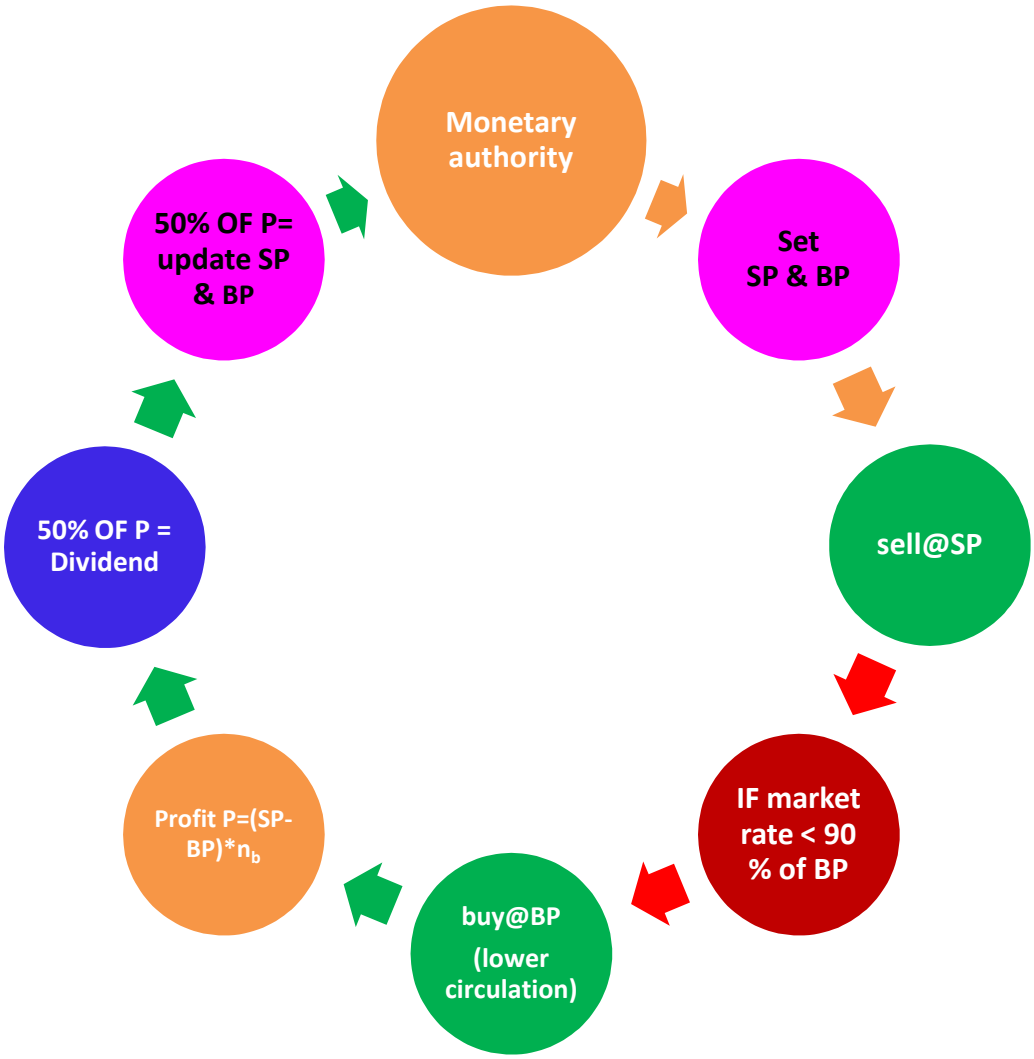
The profit accumulated from the above mentioned continuous selling and a buyback activity over a set period which is currently set at 30 days is used in following activities.

Dividend = 15%

Price Band increase = 25%

Security for New CAVORITE Created as Block Rewards=

The above activities performed by monetary authority results in stable and guaranteed value of CAVORITE which will reduce the effect of speculation on the value of currency.



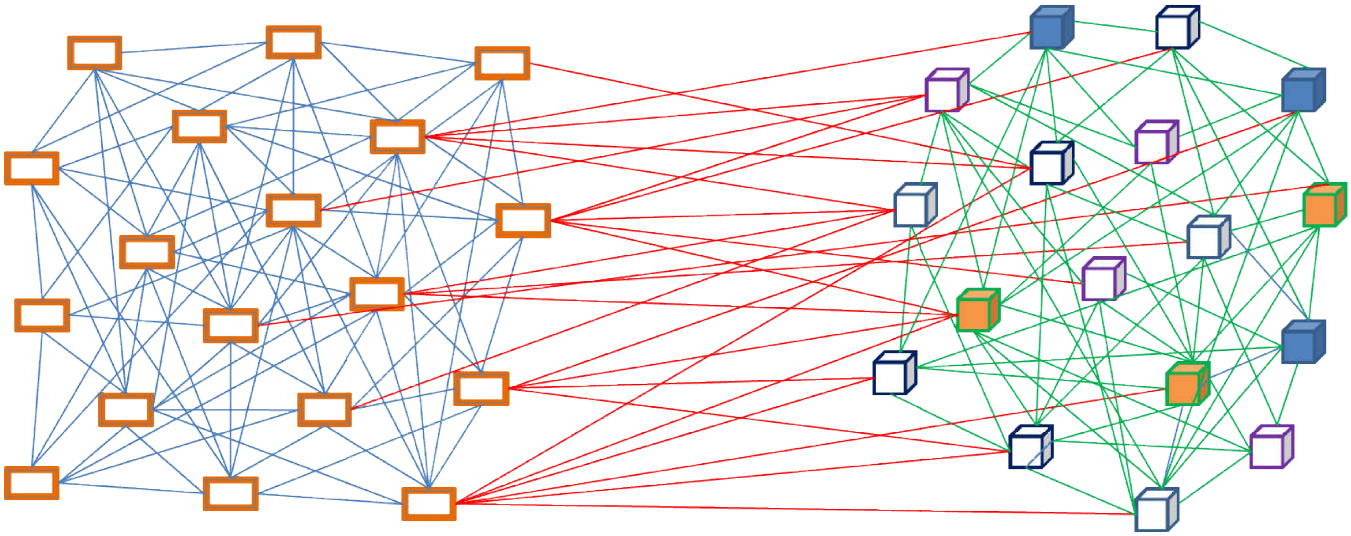
This kind of arrangement is necessary to stop the values of currency falling below a certain level.

The main aim of this authority is to ensure a stable value of CAVORITE, as you can see initially CAVORITE will operate as a full reserve system like the Gold standard adopted initially with fiat currencies. But this full reserve system is only a temporary measure and with increasing adoption the authority will move towards a fractional reserve system just like the fiat systems.

This full reserve system is initially necessary to generate the trust among adopters in the community and as this trust increases only a fraction of CAVORITE will be cashed out for their guaranteed value and that will reduce the burden of maintain full reserve system.

Blockchain Architecture [2]

CAVORITE uses a multi Dimensional Blockchain Architecture in place of generally adopted single dimensional blockchains; both these Dimensions fulfill different responsibilities while improving overall performance of the blockchain in terms of transactions processed per second as well as security.



Processor Nodes **Validator Nodes**

POINT OF SALE TERMINALS
SERVERS

Multi tier structures provide us with various benefits in terms of decentralization and load sharing.

Level 1 consists of real world businesses with CAVORITE point of sale hardware acting as point of service for Level 1 to connect with various Blockchain services offered by CAVORITE, these points of services are known as Processor Nodes in CAVORITE blockchain system.

Level 2 Consists of nodes with high end server hardware which improves the throughput of the system and performs various resource heavy activities that the CAVORITE point of sale hardware cannot perform. Presence of this level not only enhances the performance but also the security of CAVORITE Blockchain.

These Multiple Levels are further described in detail, later in this paper.

Accounts [3]

Account Creation:

CAVORITE implements a multicurrency deterministic wallet with Built in support for CAVORITE decentralized exchange as well as third party exchanges: only CAVORITE accounts and balances are stored on the CAVORITE Blockchain,

Public and Private keys for each CAVORITE account address are generated from combination of **Blake2b** Hash Function and **Schnorr** Signature Algorithm. Each account Address is represented by a 64-bit number which is generated from the further encoding of public key of each account. Each account address consists of CAVORITE as prefix in order to prevent mixing of account address with other assets.

The advantage with providing a multicurrency wallet is that users can transact as well as exchange multiple currencies and assets with each other easily, while mitigating the risk of using different wallets from different currencies.

Account Balance Properties:

For each CAVORITE account, there are multiple values associated and stored on the Blockchain. Each value serves a different purpose, and many of these values are checked as part of transaction validation and processing.

• The Main balance of an account is the total Amount of CAVORITE held by the account owner.

• The flag value of an account represents the current main balance of an account, minus the tokens involved in unconfirmed, sent transactions.

• The fee balance of an account is the total Amount of CAVORITE transactions that has been confirmed but not added to blockchain by any validator quorum yet.[refer “validator nodes”]

• The Fee Multiplier of an account is the number of transactions whose balance is still included in load balance meaning the number of transactions not yet added to the blockchain.

• The Reward balance of an account shows the total quantity of CAVORITE that have been earned as a result of successfully creating blocks that day.

• The Performance Balance of an account is a representative balance which consists of all tokens that have been added through sales over last 30 days and updated every 24 hours only.

• Loan balances lists the CAVORITE balance received from Monetary Authority as Advances.

Transactions: [3]

Multiple types of transactions are possible in CAVORITE apart from the regular payment transactions; each type of transaction has a predefined set of functions and the record of all these transactions is stored on the blockchain.

Transaction types:

Since CAVORITE is based on the **Nxt** code which supports Categorizing transactions into types and subtypes and allows for modular growth and development without creating dependencies on other "base" functions. As some features have been added to the CAVORITE, new transaction types and subtypes have been added to support them.

The following five transaction types and associated subtypes are supported by CAVORITE. Each type dictates a given transaction's required and optional parameters, as well as its processing method.

1. *Payment* Transactions: sending CAVORITE from one account to other.

2. *Messaging*: used by messaging, alias, voting, and account info features.

3. *Colored coins*: To manage and issue assets on Blockchain.

4. *Marketplace Transactions*: Transactions for Decentralized CAVORITE marketplace

5. Decentralized exchange transactions: Transactions carried out on the CAVORITE DEX.

6. *Monetary Authority Transactions*: transactions that involve monetary authority as one party.

- Issue Block Reward
- Sell CAVORITE
- Buy CAVORITE
- Issue Loan
- Issue Dividend
- Announce Exchange Rates

Purchase orders Transactions:

This is a special type of escrow transaction involving 3 or more parties, let's understand by example:

There are 3 parties A, B, C

A issues a purchase order to B for some goods, B is yet to receive CAVORITE from A & he needs to purchase some raw materials for completing the order issued by A, but B does not have CAVORITE to create another escrow with his supplier C.

B creates an escrow with A like a normal escrow,

In CAVORITE purchase orders, B can create a sub escrow to C provided the amount in sub escrow is lower than main escrow amount with A. However C will have to wait till the execution of main escrow in order to receive funds.

Upon fulfillment of order C to B the sub escrow gets executed.

As the main escrow gets confirmed the amount it contained gets distributed according to the terms of sub escrow confirmed earlier between B & C.

Monetary authority Transactions:

Monetary Authority is a contract which acts as an Autonomous Central Bank for CAVORITE currency ecosystem; it interacts with normal CAVORITE accounts through following transactions

Grant Block Rewards: Each time a new block is added to the CAVORITE Blockchain the monetary authority issues the rewards of block creation and the rewards are distributed according to the reward mechanism described earlier in this paper.

Create CAVORITE to increase short term circulation: Monetary authority is like a continuously running ICO. It can create a short term extra circulation to lower the exchange rates and protect currency from volatility.

Buyback Transactions to reduce CAVORITE Circulations: As mentioned above the monetary authority can create extra CAVORITE, likewise it can also buyback if the market exchange value for CAVORITE falls below the guaranteed value, this buyback will lower the circulation of CAVORITE and in turn increasing the exchange rate again.

Issue Loans to Nodes: It can provide credit to validator and processor nodes based on their expected future block rewards and decide a periodical payback; the loaned amount gets displayed in the loan balance of account, upon end of a period the loaned party creates a normal payment transaction back to authority. If at any time the processor willfully tries to

abscond from payment, the processor gets penalized and excluded from future participation in Block Creation.

Issue Dividend to Validators: Monetary authority takes part in various activities by which it generates a profit over time, on regular intervals a percentage of this profit is paid to validator nodes.

Announcement of Exchange rates: Each CAVORITE comes with a guaranteed value, unlike other crypto currencies there is a minimum buyback value associated with each CAVORITE in circulation, this value is guaranteed from the assets received during ICO in other crypto assets.

Transaction fee:

Transaction fee is necessary to mitigate the Denial of service attacks over the network, CAVORITE uses a new method of calculating transaction fee, instead of using flat percentage of transaction amount, CAVORITE uses an incremental transaction fee which starts at zero and increments according to the below given formula.

Transaction Fee = Load Balance*0.05*Fee Multiplier

With CAVORITE we were looking to opt for zero transaction fee but to thwart the risk of DOS attacks over the CAVORITE network, the incremental fee has to be adopted.

Transaction Creation & Processing:

The details of creating and processing a CAVORITE payment transaction are as follows:

1. The sender specifies parameters for the transaction.

Types of transactions vary, and the desired type is specified at transaction creation, but several parameters must be known to the sender for all transactions such as:

- The Private Key for the sending account
- automatically calculated fee for the transaction as described earlier.

2. All values for the transaction inputs are checked. For example, mandatory parameters must be specified;

a) If no exceptions are thrown as a result of parameter checking:
b) The supplied public key for the generating account is retrieved from transaction parameters.
   Account information for the generating account is retrieved from state database, and transaction parameters are further validated:

- The sending account's Main balance cannot be zero.
- Transaction fee ≥ required fee as described above.
- The sending account's Main *balance + Flag value* must not be lower than the transaction amount plus the transaction fee.

3. If the sending account has sufficient funds for the transaction:

a) A new transaction is created, with a type and subtype value set to match the kind of transaction being made.
b) All specified parameters are included. A unique transaction ID is generated with the creation of the object.
c) The transaction is signed using the sending account's private key.
d) The encrypted transaction data is placed within a message instructing network peers to process the transaction
e) The transaction is broadcast to all peers on the network
f) The server responds with a result code:
   - The transaction ID, if the transaction creation was successful.
   - An error code and error message if any of the parameter checks fails by processor Nodes.

Transaction confirmations:

All CAVORITE transactions are considered *unconfirmed* until they are included in a valid network block and a lock is announced on that block by a quorum of validator nodes. Newly-created blocks are distributed to the validator network by the processor node that created the block, and a transaction that is included in a block is considered as having received one confirmation,

Block is further signed by all the validator nodes in the quorum that checked it and announced lock considered as confirmed.

As subsequent blocks are added to the existing blockchain, each additional block adds further confirmation to the number of confirmations for a transaction. All transaction which has been confirmed but not yet added to blockchain show up as load balance in the associated account, this load balance is deducted for each transaction that has been included in the blockchain and 5 further blocks have been added over it.

Processor Nodes:

Who are they? [4]

Processor Nodes consists of point of sale devices with businesses; apart from accepting transactions on our blockchain the devices also have dedicated capabilities for hashing and creating blocks, the devices store only account state database, not the complete blockchain, in order to minimize the storage use. This state database is sync able with the Blockchain.

Role:

Flag value is used as a verification flag in posted transaction to prevent double spending;

When a Processer node receives a transaction it checks whether

Flag Balance ≥ 0

If yes then it propagates the transaction on the network

Verified transactions are included in the blocks and submitted to validator Nodes, as soon as a lock is announced on block by a validator quorum, the transactions stands confirmed and state database in tier 1 gets updated.

Sender A/C Main Balance = Main Balance – Amount;

Receiver A/C Main Balance = Main Balance + Amount;

All the other Balances associated to the accounts involved in the transactions are also updated according to the outcome of the transaction.

Selection & Proof of Adoption:

A special deterministic algorithm is used for instant ordering of the processor nodes per block cycle,

If,

No. of blocks per cycle = n;

Then,

Number of Selected Processor Nodes per cycle = n,

Contrary to POW where all miners compete for generating a block, in order for their block to be selected they all perform a proof of work function and block satisfying the proof of work algorithm gets new coins as rewards,

CAVORITE does not force these block creators to compete with each other and perform some arbitrary and not useful proof of work on every block, instead the creators of blocks are automatically chosen instantly according to the provided algorithm,

The chosen nodes then create blocks and propagate them to validator nodes network for further actions.

Processor Node Communication: [2]

The Processor Nodes are propagated around the network using a series of protocol extensions including a announce message and ping message. These two messages are all that is needed to make a node active on the network, beyond these there are other messages for executing a proof-of-adoption request.

Processor Nodes are originally formed by sending POS HARDWARE SIGNATURE to a specific address in a wallet that will "activate" the node making it capable of being propagated across the network. A Secondary private key is created that is used for signing all further messages. The latter key allows the wallet to be completely locked when running in a standalone mode.

Upon starting, a Processer sends a "Processer Node Announce" message to the network, containing:

Message: (Reachable IP Address, Hardware Signature, Signature Time, Hardware Public Key, Secondary Public Key, secondary Signature)

Every 15 minutes thereafter, a ping message is sent proving the node is still alive.

Message: (Signature (using Hardware key), Signature Time, Stop)

After a time-to-live has expired the network will remove an inactive node from the network, causing the node to not be used or paid. Nodes can also ping the network constantly, but if they do not have their ports open, they will eventually be flagged as inactive and not be paid.

Validator Nodes: [2]

Who are they?

Validator nodes are full nodes, the concept of validator nodes is inspired from MasterNodes in dash, and similarly they must provide a level of service to the network and have a bond of collateral to participate. Collateral is never forfeit and is safe while the node is operating. This allows investors to provide a service to the network, earn interest on their investment and reduce the volatility of the currency as well.

To run a Validator node, the node must store 1,000 CAVORITE. When active, nodes provide services to the network and in return are paid in the form of Block Rewards and

dividend. This allows the users to pay for the services and earn a return on investment. 30% of the total block reward is dedicated for awarding Validator Nodes.

Similar to DASH, Payment on a standard day for running a Validator node can be calculated by using the following formula:

$$(n/t)*r*b*a$$

Where:
n is the number of Validator nodes an operator controls
t is the total number of Validator nodes
r is the current block reward (presently averaging about 5 CAVORITE)
b is blocks in an average day.
a is the average Validator node payment (30% of the Block Reward)

Return on investment for running a Validator node can be calculated as.

$$((n/t)*r*b*a*365)/$$

Variables are same as described earlier.

Trustless Quorums

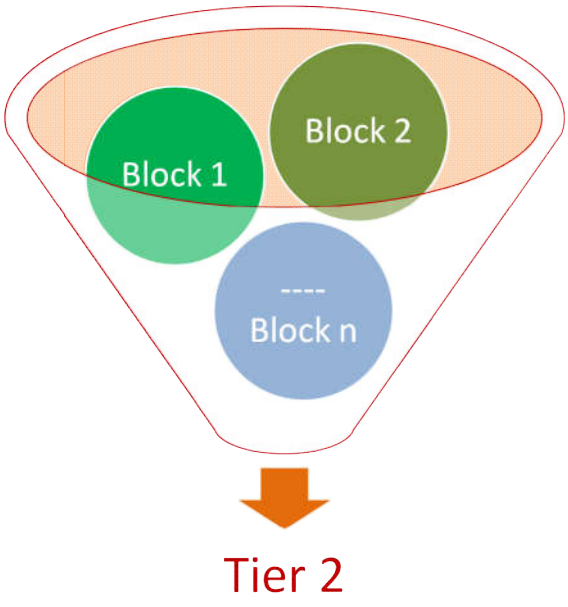
By requiring 1,000 CAVORITE collateral to become an active Validator Node, we create a system in which no one can control the entire network of Validator Nodes. For example, if someone wants to control 50% of the Validator Node network, they would have to buy CAVORITE from the open market. This would raise the price substantially and it would become impossible to acquire the needed CAVORITE.

With the addition of the Validator Node network and the collateral requirements, this secondary network is used to do highly sensitive tasks in a trustless way, where no single entity can control the outcome. By selecting N pseudo random Validator Nodes from the total pool to perform the same task, these nodes can act as an oracle, without having the whole network do the task.

For an example, implementation of a trustless quorum, which uses quorums to approve transactions and lock the inputs or the proof-of-service implementation.

Role and Proof-Of-Service:

Validator Nodes can provide any number of extra services to the network. By utilizing what we is called proof-of-service, we can require that these nodes are online, responding and even at the correct block height.



Validator Node Communication:

The Validator Nodes are propagated around the network using a series of protocol extensions including a Validator Node announce message and Validator Node ping message. These two messages are all that is needed to make a node active on the network, beyond these there are other messages for executing a proof-of-service request.

Validator Nodes are originally formed by sending 1,000CAVORITE to a specific address in a wallet that will “activate” the node making it capable of being propagated across the network. A secondary private key is created that is used for signing all further messages. The latter key allows the wallet to be completely locked when running in a standalone mode.

Upon starting, a Validator Node sends a “Validator Node Announce” message to the network, containing:

Message: (1K CAVORITE Input, Reachable IP Address, Signature, Signature Time, 1K CAVORITE Public Key, Secondary Public Key)

Every 15 minutes thereafter, a ping message is sent proving the node is still alive.

Message: (1K CAVORITE Input, Signature (using secondary key), Signature Time, Stop)

After a time-to-live has expired, the network will remove an inactive node from the network, causing the node to not be used by clients or paid. Nodes can also ping the network constantly, but if they do not have their ports open, they will eventually be flagged as inactive and not be paid.

Propagation of the Validator Node List:

New clients entering the CAVORITE network must be made aware of the currently active Validator Nodes on the network to be able to utilize their services. As soon as they join the mesh network, a command is sent to their peers asking for the known list of Validator Nodes. A cache object is used for clients to record Validator Nodes and their current status, so when clients restart they will simply load this file rather than asking for the full list of Validator Nodes.

Blocks:

The throughput of any blockchain in transactions per second depends on the frequency of block generation, in order to handle large number of transactions per second CAVORITE uses a new strategy of block generation.

Block Cycle:

CAVORITE can support theoretically unlimited number of transactions per second, Contrary to Bitcoin and other cryptocurrencies where a single block is generated every block cycle, in CAVORITE multiple number of blocks are generated each block cycle, the number of blocks per cycle is limited only by number of active validator nodes in second tier of the blockchain, we will explain why it is so, later in this paper in the validator nodes selection section.

Block Cycle = 15 Seconds

Number of blocks per cycle = No. of validator nodes*0.001

Block Creation:

Blocks are created by the processor nodes in first tier of the blockchain and submitted to validator nodes in second tier for final verification and addition to blockchain like other blockchain systems.

Reward Mechanism

As mentioned in monetary Authority section CAVORITE coins are generated by block submission as well in form of dividend from the profit accumulated by monetary authority, the dividend is only payable to the validator nodes as described earlier in this paper, Only the distribution scheme of block rewards is described here.

Block Rewards are also generated in form of payment from the monetary authority. In CAVORITE Blockchain the rewards for a certain block does not completely belong to a single node, instead CAVORITE uses a reward sharing mechanism with the whole CAVORITE community for each block. The rewards will be shared in following way,

1. 15% Monetary Authority for loan issuance
2. 5% Developers with cap on rewards/contribution, unused fund go to authority
3. 30% Validator nodes
4. 40% Processer nodes
5. 10% Users

Processer Node Selection Algorithm

Selection of a Processer node for block creation in any block cycle depends on three parameters

Performance Score (S_P), Time Score (T_D), Reward Score (B_D)

Calculation of Scores:

Performance score S_P: Performance score is awarded for a period of 30 days and recalculated at the end of every 24 hours period by following formula

If for a given node x on a given day D

Current Account Balance = B_{Ax}

No. of coins held at day Start =B_{0x}

Coins received in block rewards this day = B_{Dx}

Value addition V_{Dx} this day D for the given node x = (B_{Ax}) - (B_{0x}) - (B_{Dx});

Total value addition by all nodes for a given day

$$\mathbf{V_D} = \sum_{x=0}^{n} \mathbf{V_{D_X}}$$

Where n = number of total nodes.

Total value addition by given Node x in the defined scoring cycle

$$\boldsymbol{V_{A_X} = \sum_{D=0}^{T} (V_{Dx})}$$

Where T is no. of days in scoring cycle, which is currently 30 DAYS.

Similarly total value addition of all the nodes in the defined cycle

$$\mathbf{V_A} = \sum_{x=0}^{n} \mathbf{V_{A_X}}$$

So the node sore for given node x

$$\mathbf{S_{P_X} = 1\ 00 - [\frac{(V_A - V_{A_X})}{V_A} * 1\ 00]}$$

Time Score T_D: time score is calculated for a given day D for each node and resets after 24 hour period.

If t is time since the node x last took part in block creation and T is the total time elapsed since day start then

Time score for node x $$\boldsymbol{T_{Dx} = 1\ 00 - [\frac{(T-t)}{T} * 1\ 00]}$$

Reward Score B_D: Reward score is also calculated for a given day and resets after 24 hour period as the time score

If R_x is total reward received by node x till the elapsed time in the day and R_{tot} is total reward distributed till that time then

Reward Score for Node x $$B_{Dx} = \frac{(R_{tot} - R_x)}{R_{tot}} * 1\ 00$$

Now all three parameters are available for all the associated processor nodes which are percentages (0-100), nodes can be selected automatically each time a new block is ready to be created based on these scores

Pseudo Code For selection of Processer Nodes:

```
For(Processornode in ProcessorNodes){
    current_score = ProcessorNode.CalculateScore();

    if(current_score > best_score){
         best_score = current_score;
         winning_node = ProcessorNode;
    }
}

CProcessorNode::CalculateScore(){
   S1 = S_P; // get the Performance score for the node
   S2 = T_D; // get the Time score for the node
   S3 = B_D; // get the Reward score for the node
   Score = (2*S1 + S2 + S3)/4;
   Return Score;
}
```

The code can be extended to select multiple processor nodes per block cycle equal to the number of blocks generated in that cycle.

Validator node selection algorithm

A deterministic algorithm is used to create a pseudo-random ordering of the Validator nodes as in DASHPAY. security of this functionality will be provided by the Processer Node network.

Pseudo Code, for selecting a Validator node:

```
For (Validator node in Validator Nodes)
{
    current_score = Validator Node.CalculateScore();

    if(current_score > best_score){
         best_score = current_score;
         winning_node = Validator Node;
    }
}

CValidator Node::CalculateScore(){
   pow_hash = GetHeaderHash(nBlockHeight); // get the hash of this block
   Header_hash_hash = Hash(Header_hash); //hash the header hash to
increase the entropy
   difference = abs(Header_hash_hash - Validator Node_vin);
   return difference;
}
```

The example code can be extended further to provide rankings of Validator Nodes also, a “second”, “third”, “fourth” and further Validator node in the list to be selected equal to the number in quorum.

User reward calculation algorithm:

As mentioned earlier, In CAVORITE 10% of block rewards are awarded to users of the CAVORITE ecosystem

These rewards are distributed weekly among accounts A_1, A_2……..A_n according to following simple algorithm:

If for an account x

All the input CAVORITE to account x over a week = B_{ix}

All the output CAVORITE from account over a week = B_{ox}

Net weekly output B_x for account x = $B_{ox} - B_{ix}$

Weekly Reward score P_x for the given account x will be decided by

$$P_x = \frac{\mathrm{B_x}}{\sum_{\mathrm{x=0}}^{\mathrm{n}} \mathrm{B_x}} * 100$$

Where n = total number of accounts

If total weekly user reward is R, block reward R_x to an account x will be

$$R_x = R * {}^{P_x}/_{100}$$

Processor Node Reward Mechanism:

Processor nodes are paid according to the ratio of their blocks with total created blocks.

IF DURING THE WEEK TOTAL BLOCKS CREATED BY NODE X ARE K_X AND TOTAL BLCK REWARD OVER THE SAME PERIOD BY ALL NODES IS K

REWARD SHARE $RS_x = (K_X/K)*100$

If total weekly processer node reward is R, block reward R_x to x will be

$$R_x = R * {}^{RS_x}/_{100}$$

Validator Node Reward Mechanism:

Validator nodes will be paid similarly according to the services provided in processing blocks.

Cryptographic foundations:

Digital Signature algorithm and Hash Function:

CAVORITE uses **Blake2** [**5**] as Hash function and **Schnorr** [**6**] as digital signature algorithm for their following features:

• ***Very fast signature verification*** **in Schnorr signature**.

• ***Blake2 is a fast and secure hash function.***

• *Multiple* Keys/Signatures can be used generate one Key/Signature Pair of same size in Schnorr signatures.

• Resistant to known attacks in cryptography.

Digital Signature Protocol [6]:

Schnorr Signatures — Signature Generation:

Message M and private key K = (p, q, g, x):
• Choose a random r from {1 . . . q - 1}.
• Compute s = h (Mkgr).
• Compute t = (r + x · s) mod q.
• Attach the signature (s, t) to the message.

Schnorr Signatures — Signature Verification:
Message M and public key K b = (p, q, g, y)
• Accept the signature if h (Mk|gty-s) = s.
• Otherwise reject the signature.

Key Exchange Protocol: [7]

1) **Setup: Schnorr Signcryption parameters:**

p = a large prime number, public to all
q = a large prime factor of p-1, public to all
g = an integer with order q modulo p, in [1,…, p-1], public to all
hash = a one-way hash function
KH = a keyed one-way hash function = KHk(m) = hash(k, m)
(E, D) = the algorithms which are used for encryption and decryption of a private key cipher.

2) **KeyGen sender:**

Alice has the pair of keys (Xa, Ya):
Xa = Alice's private key, chosen randomly from [1, .., q-1]
Ya = Alice's public key = mod p

3) **KeyGen receiver:**

Bob has the pair of keys (Xb, Yb):
Xb = Bob's private key, chosen randomly from [1, .., q-1]
Yb = Bob's public key = mod p.

4) **Signcryption:**

In order to signcrypt a message m to Bob, Alice has to accomplish the following operations:

Calculate

$$k = hash(Yb^X) mod\ p$$

Split k in k_1 and k_2 of appropriate length.

Calculate **r = KHk2 (m) = hash (h2, m)**
Calculate **s = x + (r * Xa) mod q**
Calculate **c = Ek1 (m) = the encryption of the message m with the key k1.**
Alice sends to Bob the values **(r, s, c)**.

5) **Unsigncryption:**

In order to unsigncrypt a message from Alice, Bob has to accomplish the following operations:

Calculate k using r, s, g, p, Ya and Xb

$$\boldsymbol{k = hash((g^s * Ya^r)^{-Xb} mod\ p)}$$

Split k in k1 and k2 of appropriate length.

Calculate m using the decryption algorithm **m = Dk1(c).**
Accept m as a valid message only if **KHk2 (m) = r**.

Summary of CAVORITE Core features

Guaranteed & Stable Value:

Unlike other cryptocurrencies, CAVORITE comes with a minimum guaranteed exchange value which is set by the monetary authority. This makes CAVORITE a form of asset backed currency and it does not derive its value only from market speculation, while depending upon the market demand monetary authority can steadily increase the minimum guaranteed value.

Periodic Dividends:

Since monetary authority is involved in many aspects which are bound to generate extra revenue for monetary authority, this revenue is paid back to validator nodes in terms of dividends periodically on top of the block rewards described earlier in this paper.

Convenient & Fast Payments:

CAVORITE can support theoretically unlimited number of transactions per second as opposed to slow payments in popular cryptocurrencies making it suitable candidate for over the counter purchases and increase adoption.

Device Portability:

Since CAVORITE is based on java code and the cryptographic functions are lightweight as well it can be ported to many less powerful devices like mobile phones etc.

Community Support:

Processor nodes in CAVORITE are going to be real world businesses, who will be handling the processing tasks from their dedicated Point of sales devices optimized to handle the processing tasks associated with CAVORITE and block rewards will create an additional source of income for these businesses. CAVORITE was basically designed to keep the small businesses in mind making it a candidate to enjoy their loyalty and support.

Decentralized Exchange: [3]

CAVORITE blockchain also has a decentralized exchange associated with it where users can issue assets in form of colored coins pegged with digital assets as well as easily exchange CAVORITE for any other crypto asset or fiat currency as well without needing the interference of third party.

Decentralized Marketplace: [3]

As stated above CAVORITE was designed with small businesses in mind, it has a dedicated decentralized marketplace where businesses can perform e commerce transactions without spending any extra fee or commission on sales.

Extendibility: [3]

CAVORITE currently focuses on being a currency but the blockchain is designed as such the hardware in last tier can be made able to support another blockchain as its supporting blockchain performing tasks as required.

Security Overview

Double Spending:

Since the account state is stored with processor nodes and a nonce value is used in each account to determine the volume of total unconfirmed transactions associated with that account. Any double transaction cannot be accepted in CAVORITE; further the fast transaction times minimize the **finney attack** probability as well.

Anonymity:

Anonymity can be achieved using multisignature transactions; Schnorr signatures provide the functionality to generate a single public key and signature of same size from multiple keys and signatures. This feature can be used to mix coins and achieve better performance than the coinjoin.

Pump & Dump:

Pump and Dump caused by holder of large amounts of CAVORITE is not possible since all the coins sold by them would easily be purchased by the authority once the prices fall about the floor price. But the authority will only reissue these bought back coins at ceiling price as described earlier.

Nothing at Stake Attacks:

In a “nothing at stake” attack, forgers attempt to build blocks on top of every fork they see because doing so costs them almost nothing, and because ignoring any fork may mean losing out on the block rewards that would be earned if that fork were to become the chain with the largest cumulative difficulty. While this attack is theoretically possible, it is currently not practical in CAVORITE due to the multi tier architecture of blockchain, as described above any validator node can be dropped after 6 violations of code and probability of a single person controlling large number of validator node comes at substantial cost in form of locked money and hardware costs as well. And as discussed above being dropped from list comes with loss of periodical dividends as well.

Sybil attack in tier 2 [2]:

Bad actors could also run Validator Nodes, but not provide any of the quality service that is required of the rest of the network. To reduce the possibility of people using the system to their advantage nodes must ping the rest of the network to ensure they remain active. This work is done by the Validator Node network by selecting 2 quorums per block. Quorum A checks the service of Quorum B each block. Quorums A are the closest nodes to the current block hash, while Quorum B are the furthest nodes from said hash.

Validator Node A (1) checks Validator Node B (rank 2300)
Validator Node A (2) checks Validator Node B (rank 2299)
Validator Node A (3) checks Validator Node B (rank 2298)

All work done to check the network to prove that nodes are active is done by the Validator Node network itself. A certain part of the network will be checked each block. In order to keep this system trustless, we select nodes randomly via the Quorum system, and then we also require a minimum of six violations in order to deactivate a node.

In order to trick this system, an attacker will need to be selected six times in a row. Otherwise, violations will be cancelled out by the system as other nodes are selected by the quorum system.

Attacker Controlled Validator Nodes / Total Validator Nodes	Required Picked Times In A Row	Probability of success $(n/t)^r$	CAVORITE Required
1/2300	6	6.75e-21	1,000CAVORITE
10/2300	6	6.75e-15	10,000CAVORITE
100/2300	6	6.75e-09	100,000CAVORITE
500/2300	6	0.01055%	500,000CAVORITE
1000/2300	6	0.6755%	1,000,000CAVORITE

Table 1. The probability of tricking the system representing one individual Validator Node as failing proof-of-service

Where:
n is the total number of nodes controlled by the attacker
t is the total number of Validator Nodes in the network
r is the depth of the chain

The selection of Validator Nodes is pseudo random based on the Quorum system

Quantum computing attack:

So far quantum computing threat seems to be at least 10 years away but CAVORITE needs to be prepared and plan in advance for future threats.

A lightweight & quantum resistant Digital signature Protocol known WalnutDSA is currently being evaluated and restructured for use in CAVORITE blockchain in future updates to counter the quantum computing threat, CAVORITE is not in favor of using one time signature algorithms (Merkle Signatures, Winternitz OTS+ etc) at current because of their increasing signature size with transactions and limits with the number of signatures.

CAVORITE basically wants to be ready for the quantum computing threat but it does not want to sacrifice performance at current when there is no visible quantum computing threat.

Economics

Initial Coin Offering:

Total ICO balance with authority = 1 Billion CAVORITE

Initial distribution for fund raising = 1,000,000 CAVORITE

Pre ICO = 99 Million CAVORITE

ICO = 900 Million CAVORITE

Initial Ceiling price = 0.001ETH, Initial Floor Price = 0.0008ETH

ALL 1 BILLION CAVORITE WILL BE FOR SALE DURING THE ICO, WHICH CAN ALSO BE SOLD BACK TO THE AUTHORITY ANY TIME DURING OR AFTER ICO.

50% Profits generated from sale of these coins will be sent to Founders during the ICO, later this amount will be used to expand the reserves with monetary authority.

30% Used by Authority towards increasing the Ceiling and floor price of CAVORITE.

20% Dividend to Validator Nodes

During the ICO ceiling and floor price will be recalculated daily based on outside exchange prices and number of coins sold.

Once The Sale of 1 Billion CAVORITE is Completed, CAVORITE will only be created as Short term circulation, Block Rewards or as Loan In Lieu Of Future Rewards to Processor Nodes by the Authority. These loans will be payable with interest in CAVORITE back to authority.

Inflation Targets:

CAVORITE Maximum supply is unknown and depends upon money velocity. The profits generated by the authority to mint new coins,

As described earlier in this paper CAVORITE starts with a full reserve monetary system and slowly moves toward fractional reserve system based on its adoption as a medium of exchange for goods and services,

Initially 10% inflation per year is allowed per year; however the inflation rate will get adjusted according to the velocity observed by CAVORITE.

Other Related CAVORITE Documentation:

Roadmap: Access it here

CAVORITE Purchase Agreement: Access it here

Website Terms of Use: Access it here

Bibliography

[1] Gervaise R.J. Heddle CFA. (2017, Nov.) The Money Enigma. [Online]. http://www.themoneyenigma.com/theory-of-money/

[2] Daiel Diaz Evan Duffield. (2015, April) Github. [Online]. https://github.com/dashpay/dash/wiki/Whitepaper

[3] Community Nxt. (2014, January) Bravenewcoin. [Online]. https://bravenewcoin.com/assets/Whitepapers/NxtWhitepaper-v122-rev4.pdf

[4] Nakamoto Satoshi. (2008, october) Bitcoin foundation. [Online]. https://bitcoin.org/bitcoin.pdf

[5] Samuel Neves, Zooko Wilcox-O'Hearn, Christian Winnerlein Jean-Philippe Aumasson. (2013, january) Blake 2. [Online]. https://blake2.net/blake2.pdf

[6] Andrew Poelstra, Yannick Seurin, Pieter Wuille Gregory Maxwell, "Simple Schnorr Multi-Signatures," in *Blockstream, ANSSI,* Paris, France, january 2018, p. 35, https://eprint.iacr.org/2018/068.pdf.

[7] Savu Laura, "SIGNCRYPTION SCHEME BASED ON SCHNORR," *International Journal of Peer to Peer Networks (IJP2P)*, vol. 3, no. 1, pp. 1-10, january 2012, https://pdfs.semanticscholar.org/3b28/cdc431efacf126b605f32794a1c9a76770e6.pdf.