An Open Source Initiative Electronic Payment System, a Payment Fulfilment System, and a thesis on the Practical Application of a Mixed Economic Model to Achieve Crypto Coin Stability

By Michael Rossi MBCS CITP / michaelprossi@outlook.com

Narrative: In 2008, an unidentified cryptography enthusiast, decentralisation advocate, and technology visionary, using the pseudonym Satoshi Nakamoto wrote the revolutionary whitepaper, Bitcoin: A peer-to-peer electronic cash system. The paper defined the blueprint for the world's first decentralised electronic currency, Bitcoin, and became a catalyst for an evolution in the practical application of its concepts, namely proof-of-work and coins derived from a chain of digital signatures, cryptographically secured on a digital ledger, which later become known as the blockchain.

The history of Satoshi's Bitcoin can be traced back to the Cypherpunks movement of the late 1980's and 1990's and their philosophies on how to create a more open society using advances in cryptography and computerisation. The movement promoted the use of anonymity through strong cryptography to achieve genuine freedom of speech. This was especially significant in oppressive societies where censorship and monitoring were, and still are common practice.

In 1983, Richard Stallman founded the Freedom of Software movement and the GNU Project. Several other freedom of software initiatives followed, including the Open Source Initiative and its MIT License, which grants users the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the software without restriction. This project is licensed under the Open Source Initiative MIT License.

1. Introduction

The economy for digital currencies has grown 3000% in 2017 and a conservative estimate is that it will double in size in 2018. This has led to a modern day gold rush with prospectors from all walks of life rushing in to stake their claim in any one or more of 1520 active 'Gold mines'. Zero or limited regulation has also led to an influx of dishonest enterprises touting unfeasible roadmaps and the promise of high returns while hiding behind a veil of anonymity*. Founders that have nothing on the line, even if only their identities, are more likely to walk away when the going gets tough. In some circumstances, the founders, unable to establish a crypto currency with any real value, can escape via the project back door, and dump their remaining coins onto the market at the expense of their own investors.

*It ought to be distinguished between the rights to anonymity in open society in the pursuit of freedom of speech, and expecting the same privileges as an anonymous project team asking for investment from the general public. The former is both legally and socially acceptable; the latter is ethically tenuous to say the least.

This paper will define a blueprint for an ethical project based on sound fundamentals, transparency, and an effective economic policy.

2. Blockchain as a Codebase (BaaC)

We define BaaC as Bitcoin or any other alternative currency system that is licensed under the GNU Project General Public License (GPL) or any open source software initiative, that is/can be used as a donor blockchain codebase.

The genesis of Bitcoin has given rise to numerous competing electronic payment systems, many of which use or 'fork' the Bitcoin original codebase, pursuant to the GPL license agreement. Does this mean the forked project is any less legitimate than Bitcoin? The answer, of course lies in the motives of the founders and the problem they aim to address by taking what is essentially Bitcoin in a new direction. If project teams have a genuine motive, an opportunity, and the capabilities to use and improve any freedom of software codebase, this is a perfectly acceptable use case, and no less legitimate than the original codebase. The caveat being that free software should be improved for the benefit of users and the community. Any fork of Bitcoin should aim at being a future fork of another project.

Before investing in any project, the 'investor' should assess the founders' motives, transparency, and capabilities.

3. A Mixed Economic Model for a Cryptocurrency Project

Cryptocurrencies operate in a free market and are subject to the kind of excessive volatility not seen trading any other asset class. This is a clear obstacle in the way of mass adoption and whilst traders and speculators revel with each new market high, price collapses are common, and are a factor limiting mass adoption. A mixed market economy refers to the degree of state interventionism in a market economy, and in the case of a cryptocurrency project, the 'state' would be whoever within the project controls both the treasury fund and the treasury reserve fund.

An important distinction at this point is that of treasury fund and treasury *reserve* fund. A treasury fund is made up entirely of the projects native currency, usually this fund is plentiful. A treasury *reserve* fund is made up of currency from the opposing side of the main trading pair, in most cases this is Bitcoin (BTC).

To understand the financial dynamics and challenges of most cryptocurrency projects, it is important to know where they start out from. Below is a summary of the three funding options available to most projects:

- Initial Coin Offering (ICO) – Ideal situation for any project to start out. Speculators buy the premined or tokenised native currency of the project in exchange for Bitcoin or Ethereum. ICOs usually result in a medium to large treasury reserve fund and a large treasury fund.

- Coin Auctions – Usually coin auctions are the domain of anonymous project teams. The auctions generate a small to medium treasury reserve fund and the founders' premine of between 1.5% and 10% of their native currency makes for a very large treasury fund.

- Direct to Exchange – Direct to exchange cryptocurrencies, unless funded by venture capitalists, start their project life with a small treasury reserve fund and a large treasury fund.

A fourth option is available for an innovative project team:

- Treasury Fund Offering (TFO) – The treasury fund offering is a concept proposed by this paper to build a projects' treasury reserve fund in parallel with an in-flight project. Speculators buy the native currency direct from the treasury fund and their BTC payment is placed, in part, into the reserve fund. The complete mechanism is described in subsequent sections.

As a word to the wise, the downside to any project holding a large treasury fund and a small treasury reserve fund is obvious, in that they have little or no real funding. This is the death zone for most projects and the highest risk investment for the speculator.

4. Treasury Reserve Fund Mechanisms

Treasury Fund Offering (TFO)

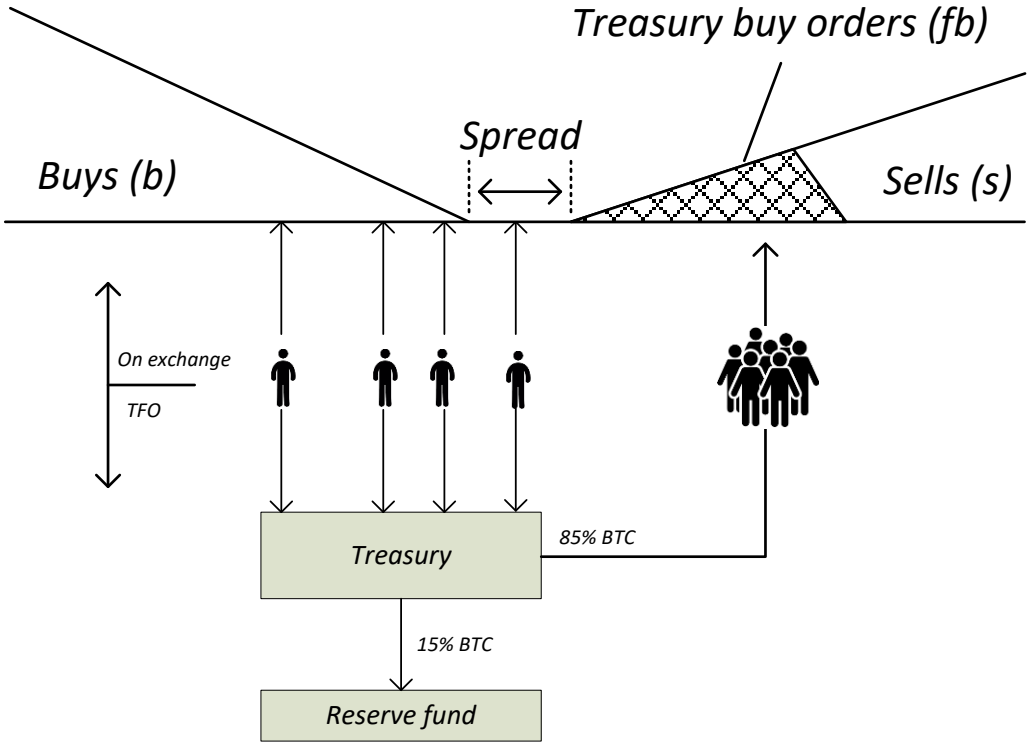
In order to fully participate in a mixed economic model, a project needs a sizable treasury reserve fund. This paper proposes a mechanism for building the reserve fund without risking any reserve capital. The Mechanism is a combination of a Treasury Fund Offering (TFO), the commitment on the part of the Treasury to use up to 85% of the TFO funds to buy back its native coins, and the treasury commitment to buy into buy walls or if under selling pressure, place these funds plus additional reserve funds into buy positions at tactical support levels.

The diagram illustrates four individual traders placing buy orders at varying prices. The buyers are chancing the price will fall into their orders. In a mixed economic project model, buyers are aware of the Reserve Fund Mechanism and the treasury's commitment to support the price at pre-determined support levels, which could result

in intervention at any point. Would the buyers follow the same psychological thought process knowing the treasury may move the price, or are they more likely to buy at a higher price?

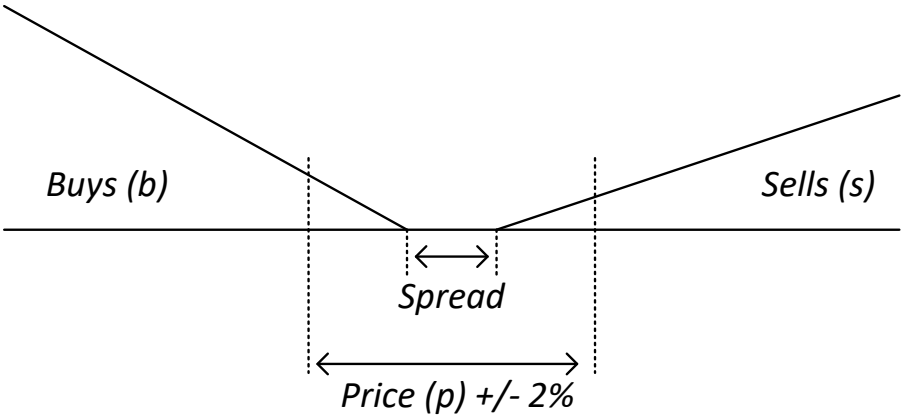
Another supposition is the net effect of consolidating the four individual orders into one larger order would have a greater impact on price than if the four were to left to their own devices. One could surmise that the individual buys would have zero effect on price if the price has to come down for the orders to be fulfilled. Another supposition is that maybe the buyers get bored of waiting and buy into the sell wall anyway, and this would have a greater net effect than 85% of the consolidated treasury reserve fund.

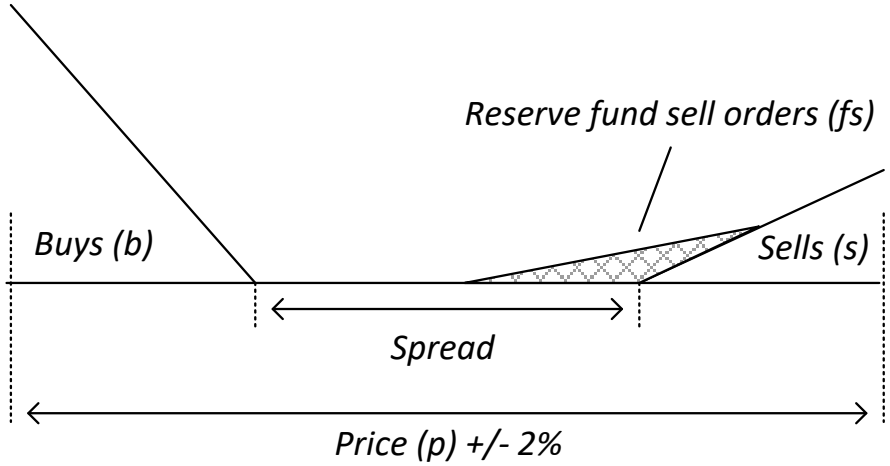
The only guarantee in any of this is that the treasury via the reserve fund will buy into the sell wall. We cannot guarantee the individuals will.



Treasury Fund - Free Market

A secondary method of growing the treasury reserve fund is the sale of treasury funds ethically 'on-exchange' into the free market. The project position on this mechanism should be simple, if the price declines as a result of treasury intervention, the mechanism is not working. Market timing is key, where market sentiment is leaning towards buying. Buy walls will be higher than sell walls at 1% either side of the mid spread price. The treasury will place small sell orders into the spread. The market sentiment will remain in favour of buyers throughout and if the sentiment changes in favour of sellers, the treasury orders will be cancelled. Treasury sell orders will not be entered into sell walls and will have a positive impact on price by way of temping buyers into the spread.





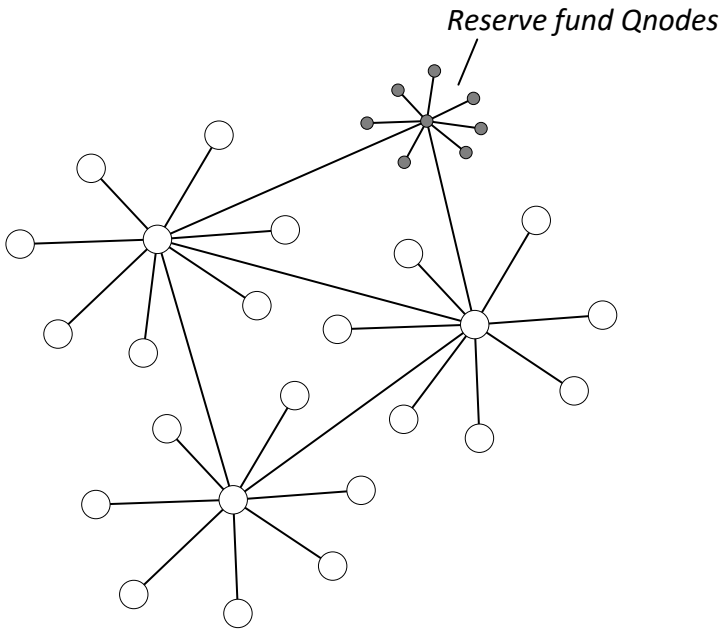
The use of Automation

In order to maximise the timing and effectiveness of exchange market orders, automation should be developed using the exchange(s) proprietary application programming interfaces (API). Automation should be used in all exchange based trading scenarios, from building the treasury reserve fund, providing liquidity, and defending support zones.

Treasury Fund Income

The payment solution allows for speculators to purchase the right to operate a highly incentivised part of the network (Qnodes). In an ethical project, the project team may have chosen to premine an amount of native currency. Whilst the treasury fund is of lesser importance in the early phases of the project than the treasury reserve fund, it is vital for Treasury Fund Offering (TFO) purchases of the native currency. Therefore, the project team should consider a source of perpetual income via their own incentivised network. It would be seen as an ethical position to have access to treasury funding via

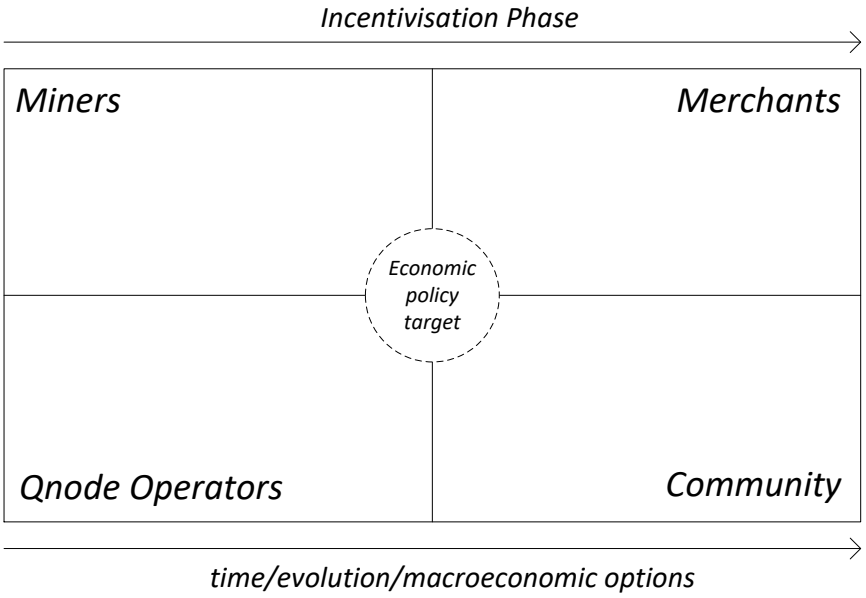
the same income source as your investors. The project team would be more incentivised to ensure the network is operational and efficient if they too participate in it.



Macroeconomic Policy

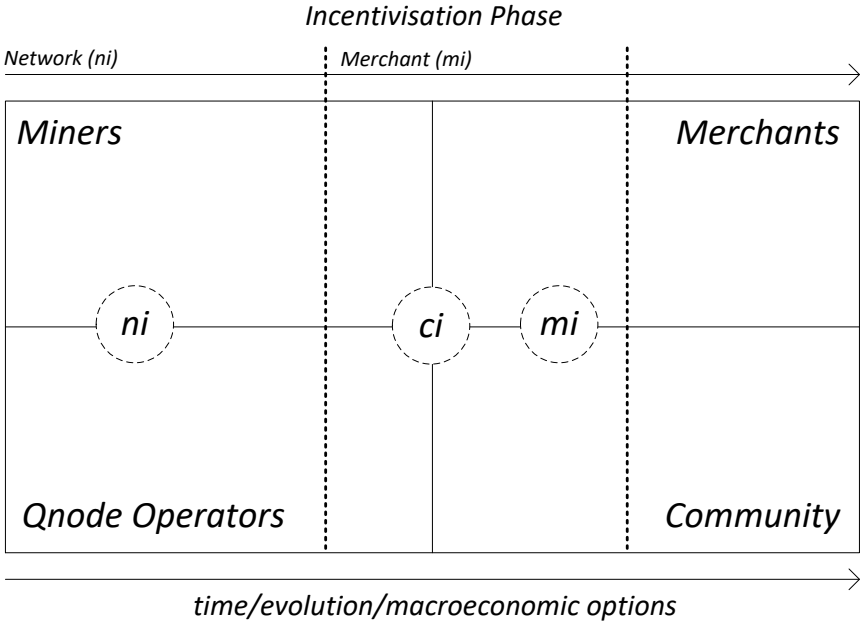
The payment solution defined in this paper has four market participants. These participants are miners, Qnode operators, merchants, and the community/consumers. The objective of macroeconomic policy is to use whatever tools are available to the project team, to control the benefits of participating in the network in favour of those participants that are key to evolutionary phases. Miners and Qnode operators are early evolutionary phase priorities, whereas as the project evolves, the policies must also evolve to address the needs of merchants and consumers. The project team must try to establish a 'sweet spot' of incentivisation at each phase of the project, with the eventual target being a macroeconomic policy that benefits all market participants, fine-tuned in line with economic data.

The early phases of the project will mainly consist of on-chain incentivisation (block time, block rewards distribution split). As the project evolves, microeconomic policy may become a combination of on-chain and off-chain incentivations, with on-chain options evolving, such as the possibility of staking wallets for consumers and merchants.



The figure above shows the market participants and the target sweet spot a project team should seek.

The figure below illustrates the incentivisation biases at different evolutionary phases of the project.



Incentivisation Types - On-Chain/Off-Chain

On-chain incentivisation is that of using the economic tools available to the project team and fine tuning the parameters to meet the needs of market participants. As the illustrations in the previous section show, the aim should be to eventually find a sweet spot of incentives across all participants but, the reality is such that if there is a

confliction of incentives between two or more market participants, the evolution of the project and the most sought after market participant group must always be the priority.

Off-chain incentivisation is the capability of the project team, both in terms of quantifiable results and perceived ability. Typical factors are:

- Capabilities – Strengths, skills.
- Agility – Reaction to events.
- Recruitment – New capabilities.
- Communication – Transparency, Trustworthiness.
- Ideas – Strategy, Innovation.

Mixed Economics – Price Support

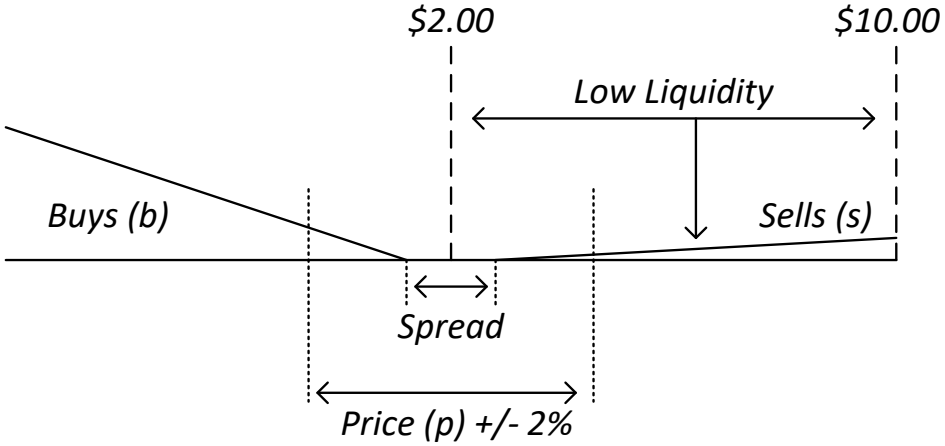
The project, via the treasury reserve fund, will have the ability to intervene in the free market to assist the community at known support levels during periods of bearish sentiment. Technical analysis is a powerful tool if all market participants know the treasury and the reserve fund may enter the market at support levels. The project will grow the treasury reserve fund as ethically as possible. The illustration below is an example of an up-trend (BTC-USD). Support levels can be found along the trend line. Should the price break through the trend line, the logical next support level would be at parallel touch points.

Reserve fund support levels

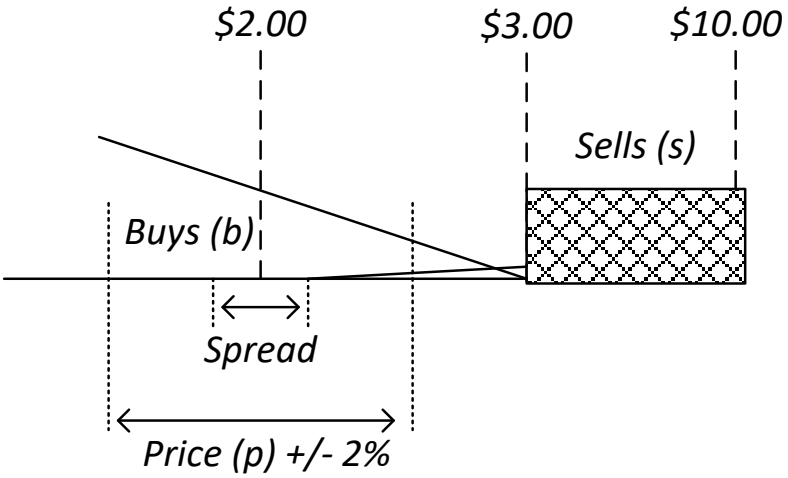
Mixed Economics – Liquidity

In times of low selling liquidity, the project, via the treasury fund will aim to provide resistance on exchanges. Whilst this appears to be at odds with the treasury reserve fund mechanism, it is a deliberate act to quell sharp rises in native currency price. Sharp rises are detrimental to the evolution of the currency because of the equally sharp pull backs that usually accompany them, and prove a hindrance to attracting new investors if they feel they 'missed the opportunity' to invest. With little liquidity in selling positions, a medium size buyer could push the price hundreds of percent, making the currency appear too expensive. This is contrary to popular belief that all 'moons' are great for the crypto economy. It is my belief that a 'moon' should occur over a prolonged period of time and at a steady pace, picking up as many investors as possible along the way.

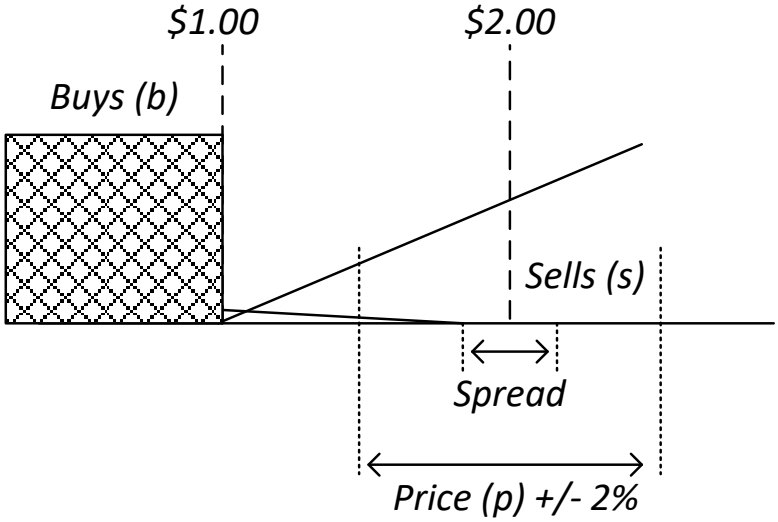
The illustration below is that of the danger of low liquidity in selling positions. On a coin with a daily volume of up to $30,000, a mere $5000 buy order could push the price up 400%.



The treasury must attempt to halt such large rises by providing liquidity, albeit at price level that suits the project, such as between $2.50 and $3.00 mark as illustrated below:



Of course, the reverse of the above scenario is the unhealthiest situation for any currency. Little liquidity on the buying side causes sellers to sell in buy walls and the same $5000 order could have a catastrophic effect on the price. The treasury fund mechanisms, including the quelling of unsustainable price rises, will ensure the projects treasury reserve fund is sufficient enough to prevent price collapses at support levels.



5. An MIT License Electronic Payment System

For the payment system, we intend to implement a BaaC solution and customise the code to suit the needs of all market participants. In selecting a codebase, we first need to select our desired consensus mechanism. This comes down to whether mining (Proof of Work) or staking (Proof of Stake) is the preferred method for adding transactions to new blocks on the network. Whilst both offer incentivisation for network participation, Proof of Stake only pays the transaction fees to the block creator and therefore has not been adopted by many projects to date. Proof of Work, on the other hand, offers the transaction fees and rewards of newly minted coins, and for this reason it is the preferred choice of most new cryptocurrency projects. Therefore, the superior incentivisation of Proof of Work as a consensus mechanism is more suited to the objectives of the project at this time.

Blockchain as a Core (BaaC) Specifications

With Proof of Work selected as the consensus mechanism, we need to select a suitable codebase for the blockchain. Rewarding all market participants is a primary objective of this project and of all codebases, *Dash* offers the most incentivised network solution. Dash nodes, and therefore node operators, receive a share of any mining rewards, in return for performing network functionality beyond that of the Bitcoin core, such as private send transactions and instant send transactions.

For the remainder of the electronic payment system section, only the key differentiators from Dash will be defined.

Dash Reference: ***[3] E. Duffield & D. Diaz "Dash: A Privacy-Centric Crypto-Currency" https://github.com/dashpay/dash/wiki/Whitepaper*** .

ASIC Resistant Mining

Dash uses the X11 algorithm based on Scrypt, which has now reached a hash difficulty uneconomical to mine using commodity GPU hardware. ASIC mining hardware is difficult to attain, and manufactured by only a handful of companies. There is now the argument that ASIC mining is becoming too centralised. The objective of this project is to create a level playing field for all mining participants, free from the constraints of specialist hardware and free to use affordable commodity hardware. For this reason, the ASIC resistant hashing algorithm, Neoscrypt has been selected.

Neoscrypt is also based on Scrypt, and has addressed some of the latter's known security vulnerabilities. Neoscrypt is ASIC resistant whereas Scrypt and X11 are not.

Specifications

Total supply: 52,500,000 coins

Block generation: 2 minutes

Block reward: 20 Qbic

10% decrease in the number of coins per year

Block rewards distribution: 50% Miners, 50% Qnodes

Qnodes

Masternodes will be known as Qnodes going forward. The project wants to differentiate from other 'masternode' coins and aims to add functionality to Qnodes, such as the Treasury Fulfilment Service (TFS), defined in Payment Fulfilment System section.

6. A Payment Fulfilment System

The payment system defined in section 5 of this paper outlines a BaaC payment system, and its differentiators from the original codebase. The system, confined to within its own system boundary, is a mechanism for internal exchange only and has no real use case outside of the mechanism. This is typical of most digital currencies and is the biggest criticism of the industry.

There are a great many projects in the world trying to legitimise digital currencies. Bitcoin, despite its 'first mover' advantage, its huge market capitalisation, and its wide adoption amongst cryptocurrency enthusiasts and traders, has yet to be accepted as a legitimate currency ready for mass adoption. In order to create a genuine alternative token of value for mass adoption, a digital currency must satisfy some key criteria, namely, stability and/or proxy stability, ease of attainability, and ease of exchange.

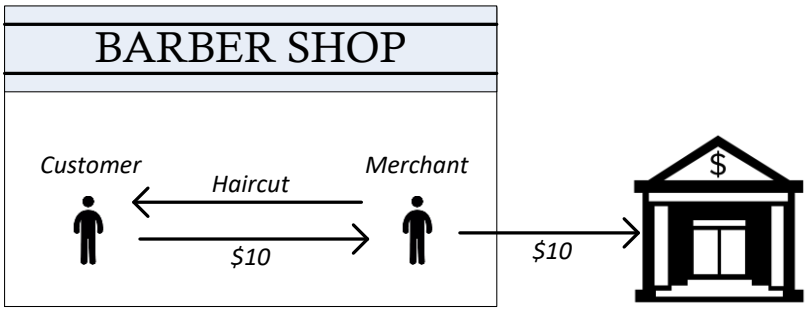
Sections 3 and 4 of this paper define an economic policy for coin stability, and proposes the practicality of two treasury funds, the treasury fund and the treasury reserve fund, and how they may be used for coin stability. In view of the economic principles within this paper, and in analysing the current industry ecosystem, we are able to design a fully functional payment fulfilment solution that could legitimise a digital currency by offering an end to end platform of exchange.

The Merchant Obstacle

Merchants are the last and most difficult market participant in the way of mass adoption. The reason for this is simple, they have bills to pay. Each of the other three participants are speculators, hopefully investing money they can afford to lose, all the while in the knowledge that they have nowhere to spend the digital currency they have just acquired. The merchant obstacle is the key to adoption, and using the existing industry ecosystem, alongside the economic policies on this paper, and the solution defined below, merchants should no longer be such the obstacle.

The Scenario

For this scenario, we are going to use a fictional barber shop. The barber charges $10 for a haircut. The customer pays $10 and we assume the barber then deposits the $10 into his or her bank account. They do, of course, have the inconvenience of walking to the bank but this is a necessary and accepted downside to a cash business. The process is easy, as illustrated below:



Besides the simplicity of the above transaction, the most significant benefit is that the rate of exchange is reliable. $10 is $10 and so long as the $dollar is not subject to

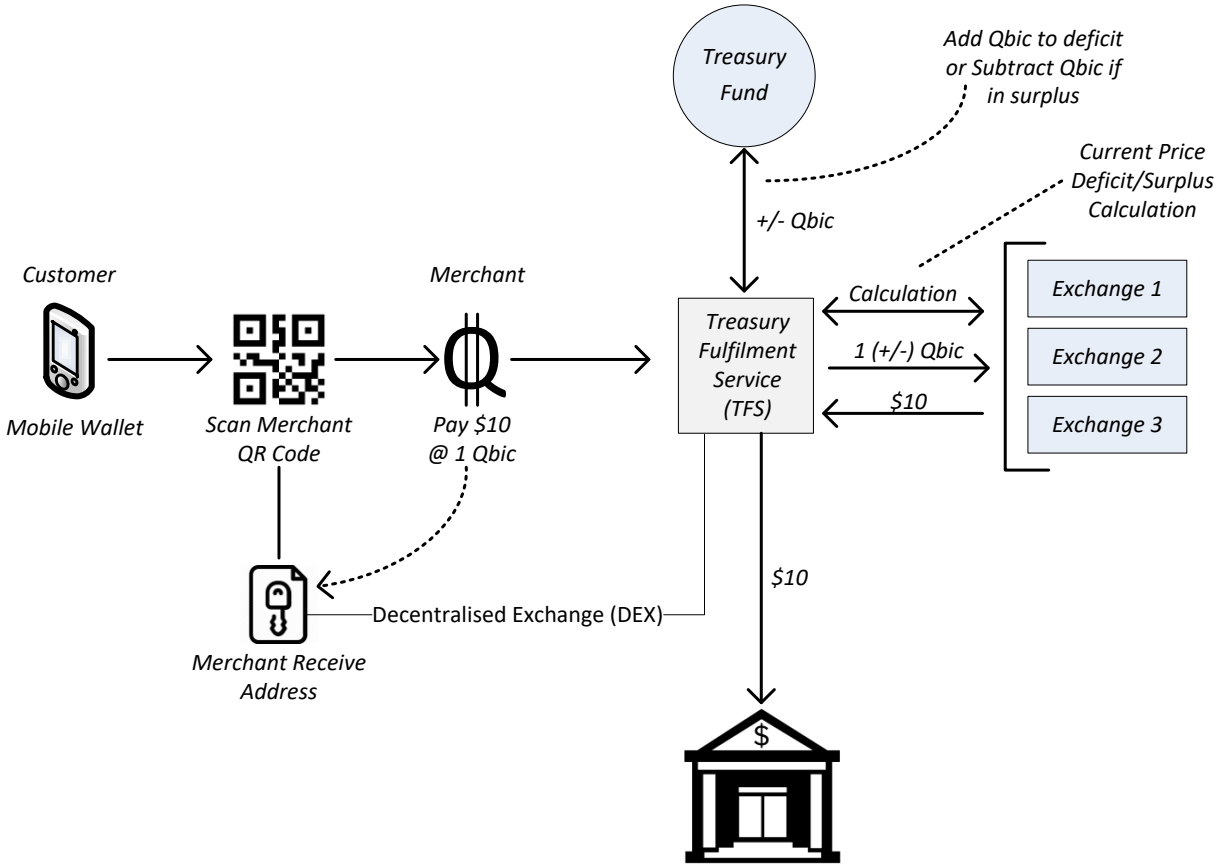
overnight hyperinflation, the $10 is worth the same next week as it was at the time of the customer's haircut.

The Problem Statement

How do we provide the merchant with the same guarantees? Digital currencies experience hyperinflation most days of the week, and any responsible merchant is not going to take a chance on exchanging his digital currency for 10% of the value it was at the time of the haircut. Even if we can guarantee the value, can we, in the current ecosystem, exchange a digital currency for $ and move the $ amount to the merchants bank account seamlessly from the perspective of the merchant, and without the merchant visiting an exchange?

The Proposed Solution

Our solution is to guarantee the value of our digital currency at the time of the payment to the merchant, and to facilitate an automated fulfilment of the payment into the merchant's bank account.



We do this by implementing a 'middle man' component called the Treasury Fulfilment Service (TFS). The TFS is essential a decentralised exchange (DEX) within the projects infrastructure. The merchant, via his mobile app, creates an account on the TFS. He

links his bank account to his TFS account. His mobile now has a connection to his merchant account on the TFS.

A customer, also using the projects mobile app, chooses to pay for his haircut in Qbic and scans the merchants QR code. The app gets a live value for Qbic vs $US dollar (1 Qbic = $10) and an instant send payment is made.

The merchant, in no rush to deposit his Qbic into his bank account as $ Dollars, waits a few days and then, via the app, withdraws the $ Dollar amount to his bank account.

The TFS, leveraging the treasury fund for proxy stability, and with links to various exchanges, exchanges the merchants Qbic for $ Dollars and transfers the money to the merchants bank account.

Proxy Stability

Proxy stability is a mechanism of a future merchant incentivisation policy whereby the treasury provides merchants with a guaranteed future value for the project's native currency. The treasury does this by leveraging the treasury fund within the projects own decentralised exchange, the Treasury Fulfilment Service (TFS). The TFS will be a fully automated trading system with links via APIs into relevant exchanges. The merchant is guaranteed the $ or BTC value at the time of original payment.

As an example;

Using the same scenario as above:

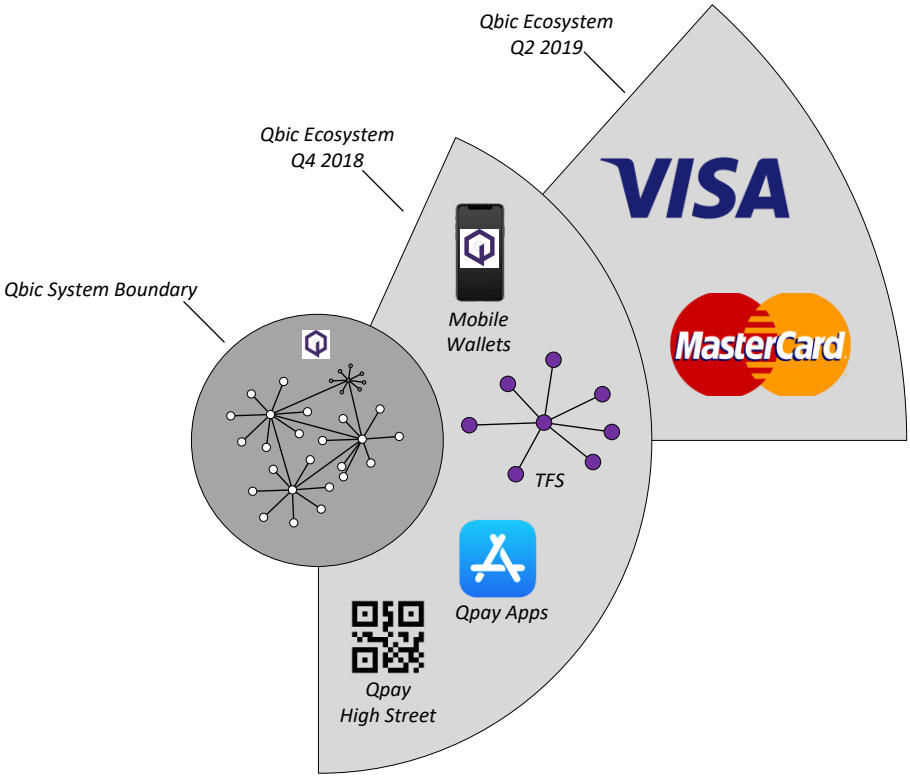
The Qbic price appreciates by 20% during the time between payment and fulfilment, the TFS, having calculated a surplus in the value, exchanges 0.8 Qbic for the equivalent $ value, and earns a profit of 0.2 Qbic.

The Qbic price depreciates by 20% during the time between payment and fulfilment, the TFS, having calculated a deficit in the value, exchanges 1.2 Qbic for the equivalent $ value, and earns a loss of 0.2 Qbic.

This is made possible by a plentiful treasury fund; especially if, by taking advantage of their own incentivisation policies, the project invests in its own infrastructure and earns a perpetual income, in addition to its premined coins.

7. Breaking Through Boundaries: The Qbic Ecosystem

The Qbic ecosystem will follow a three step evolutionary model. The first phase was building the system, its processes, and its network. The second phase is building out the ecosystem to cater for specific use cases and aims at fostering adoption outside of visionaries and enthusiasts. The third phase is that of leveraging the successes of phase two alongside rising adoption rates, and a softening of stances amongst key industry groups, such as banking. Any roadmap has to cater for these phases to be feasible. The illustration below defines the project's evolutionary roadmap (high level).



8. Conclusion

It is my hypothesis that this paper adequately describes a high potential digital currency, an effective economic policy, and a real world use case within the industry ecosystem that could lead to mass adoption. There will be many use cases as the industry evolves, including debit cards, and the quickest and most capable teams to react will become household names. Within 12 months digital currencies will connect to payment networks outside of their own system boundaries and the age of crypto will have arrived.

Cubism - A reaction against traditional modes of representation; to re-construct a subject to represent several different perspectives

References:

[1] S. Nakamato “Bitcoin: A Peer-to-Peer Electronic Cash System” https://bitcoin.org/bitcoin.pdf, 2011

[2] R. Stallman “GNU Manifesto” https://www.gnu.org/gnu/manifesto.html, 1987

[3] E. Duffield & D. Diaz “Dash: A Privacy-Centric Crypto-Currency” https://github.com/dashpay/dash/wiki/Whitepaper

[4] J. Doering “NeoScrypt, a Strong Memory Intensive Key Derivation Function” http://phoenixcoin.org/archive/neoscrypt_v1.pdf