Rya: A Trust Based Monetary System

Abstract. Rya is a cryptocurrency and monetary system designed to be both a store of value and a medium of exchange. Using a free, decentralized monetary market, the Rya system tethers money supply to credit without the need for a monopolistic regulatory institution. Money supply is adjusted dynamically depending on economic cycles making for a better medium of exchange. Rya and its Proof of Trust (PoT) model is therefore expected to be a fuller and more complete substitute for Fiat monetary systems than any cryptocurrency yet.

1. Introduction

Bitcoin and other cryptocurrencies have proven the feasibility of peer-to-peer payments over a communication channel without a trusted third party[1]. Blockchain technology is a cryptographic proof designed to be a substitute for a central mint that protects buyers and sellers from fraud (e.g. the double-spending problem). While existing blockchain technology performs this task well, banking institutions and governments still have a monopoly on credit and money supply. This has limited cryptographic currency from bringing about a full monetary revolution.

In today's climate, evolution of new cryptocurrencies stems mainly from the need to deal with technical and methodological problems in existing cryptocurrency systems. Some examples of improvements are better security mechanisms, higher transaction frequency and more efficient use of resources. However, no cryptocurrency system has attempted to incorporate the combination of interest rates and money supply that constitute a full money market. While several cryptocurrencies have been able to create a system of payments sans a trusted third party, not all the features of FIAT monetary systems (debt and fractional-reserve banking) have been fully expressed.

In a traditional monetary system, money's real demand (rather than nominal demand) depends on interest rates and income is in equilibrium with money supply set by the central bank[2]. A decentralized credit and money creation solution should perform as a stable monetary system in which the money market has normal demand and supply curves. It must also have a term spread of interest rates which reflect the risk for credit recipients, the average duration of transactions and the preferences of credit providers.

2. Money Supply

Let us first examine Bitcoin's naïve Proof of Work based model for money supply through the following equation:

$$50\frac{coins}{block} * \frac{0.1block}{minute} * \frac{60minute}{hour} * \frac{24hour}{day} * \frac{365.2425day}{year} * 3.992781year * 2 = 21{,}000{,}000\ Bitcoin$$

[1] Satoshi Nakamoto. Bitcoin: a peer-to-peer electronic cash system, 2009. URL: http://www.bitcoin.org/bitcoin.pdf

[2] Dornbusch, R., S. Fischer, R. Startz, F.J. Atkins, and G.R. Sparks. Macroeconomics, 7th Canadian edition. Toronto: McGraw-Hill Ryerson, 2005

Audited criticism held against Bitcoin is that the structure of the system has a capped money supply which will be maxed out in the long term. The resulting deflationary money trend is bad for the economy.

Now let's examine the FIAT money market. The quantity of money in the FIAT economy is determined as a fixed multiple of the quantity of bank reserves. This number is determined by a central bank (i.e. the US Federal Reserve). The supply curve of money is a vertical line at that quantity. In other words, the money market is monopolistic (both in terms of the basic interest rate and money supply).

We aim to create a monetary system in which money supply is substantively adjusted in order to best serve current economic conditions. To achieve this, the Rya system is built to be a perfectly competitive free money market and money supply is controlled by a decentralized regulatory mechanism. Unlike Bitcoin, which only allows the transfer of present value, Rya allows peers to transfer future value as well (i.e. credit). We aspire to have economic conditions in which the following holds true:

$$D(demand\ for\ money) = I(interest) = MR(marginal\ cost) = AR(average\ revenue)$$

3. The Trust Token

In order to express future value in the Rya system, we propose a double token architecture. While Rya is the cryptocurrency through which transactions can be made (like any other currency), we also establish a token called Trust. Every account has a Trust token balance which cannot be transferred from one account to another.

The primary purpose of the Trust token is to tether money supply to users economic behaviour over time. To this end two key conditions are met. Number one, an account's Trust balance is impacted by his credibility in the system (find out more 'The Trust Token as a Credit Score' below).

Number two, the Trust token plays a key role in money creation in the Rya ecosystem. A users Trust token balance directly impacts their effectiveness at minting new Rya and thus the Trust token represents potential for new money creation.

Before we discuss how peers earn Trust, let's establish some basic terminology:

1. C - Rya coins
2. T - Trust
3. *goodInterestInBlock* - the amount of interest successfully paid back to lenders in the current block in the blockchain.
4. *systemTrust* and *systemCoins* - the total amount of Trust and Rya respectively.
5. *loanSize* – the size of a Rya loan (principal).
6. *loanInterest* - the interest on the loan.
7. *trustReward* - the reward in Trust granted for a successfully returned Rya loan.
8. *trustDeposit* - Trust required to lend Rya.

Trust can be gained just by holding Rya. We suggest that a peer who does not take any action with his money (e.g spend or lend Rya) is equivalent to a person who deposits FIAT money in a savings bank account.

The Trust token enables decentralization by shifting the way interest is set and money is minted. We strive to replace the monopolistic central bank and fractional-reserve banking controlled by governments today. We are progressing to a simple formula which provides a more stable economy and a higher level of transparency to stakeholders.

A peer can gain Trust tokens (and the right to create more Rya in the future) each block by holding Rya coins. Mathematically, this can be described as:

$$\Delta userTrust = \frac{userCoins}{systemCoins * goodInterestInBlock}$$

The second way to gain Trust is by lending/borrowing Rya. Loans in the Rya ecosystem are simple transactions: one peer borrows a set amount of Rya from a second peer for an agreed upon number of blocks. If, by the last block in that time frame the borrower has successfully returned the principle plus interest (in Rya) to the lender, then both parties are rewarded - we will call this a *trustReward*.

In order to loan Rya, a proportionate amount of Trust must be deposit by the lender. Once deposited, this Trust is reduced from his active available Trust token balance, impacting the peer's ability to mint blocks and engage in additional loan transactions. In other words, a peer must risk Trust (in the short term) to gain Trust through a loan transaction:

$$trustDeposit = loanSize * \frac{systemTrust}{systemCoins}$$

The reward component is built in the following way:

$$trustReward = \frac{\sum_F loanInterest}{\sum_S loanInterest} * trustDeposit$$

S is the group of all loan transactions successfully returned in the current block. Correspondingly, F is the group of all loan transactions that were defaulted on in the current block. This reward is divided between the lender and the borrower.

There is an intuitively pleasing side effect to structuring the reward in this fashion. Over time Trust will necessarily be funneled to the group of peers that are involved with successful loan transactions and away from the group of peers that are not. So we can be sure that Trust token balances will function as accurate crypto-credit-scores in the long term.

4. A Crypto Credit Score

The FICO credit score is designed to measure the risk of default by taking into account various factors in a person's financial history. In recent years, it has often been criticized[3]. One of the main arguments is that the rating takes into account factors that are not under the person's full control. Thus, the credit score harms social mobility, fixes and even increases inequality.

The Trust token functions as a crypto-credit-score that will take into consideration only the account's economic activity in the Rya ecosystem without revealing the owner's (or multiple owner's) identity. Essentially, an account's Trust token balance serves as a basic credit score for that account. If an account holder defaults on a loan it impacts both his Trust balance and the balance of the linked account (the lender). This motivates all parties to have a decent relationship.

---

[3] Immergluck, Dan. *Credit to the community: Community reinvestment and fair lending policy in the United States*. Routledge, 2016

Beyond the Trust metric, it is also possible to scan the complete loan transaction history of the network. This enables complete and total transparency to stakeholders in a loan transaction - something not readily available in the FIAT monetary system. In these ways, the Rya system brings blockchain's social values to the traditional credit score, helping accelerate the shift of power from central authorities to non-hierarchical peer-to-peer structures.

It is important to note that we do not expect the Trust token to provide a full credit-score solution. Due to factors such as anonymity and the ability for an untrustworthy person to quickly create a new account with a fresh Trust score, it is clear that no rational lender will engage in a loan transaction on the basis of the Trust balance and transaction history of the potential borrower alone.

We predict that lenders will vet potential borrowers through other means as well - be they traditional credit bureau scores that have been adapted for crypto technology, or new yet to be seen solutions.

5. Proof of Trust: Introduction

Trust is the tool used in the Rya ecosystem to secure the blockchain. This methodology is introduced as Proof of Trust (PoT). Let's compare it to its predecessors.

In the Proof of Work model (pioneered by Bitcoin) security is provided by peers doing work. They expend their resources on computation in order to prevent double-spending transactions. The cost to a malicious peer intent on changing the networks transaction history is prohibitively formidable. Tokens are awarded in exchange for work in the mining process.

Due to the fact that the rate of block generation is typically meant to remain constant, it becomes more difficult for a single peer to earn rewards as the network grows and more mining power becomes available. This creates a sort of arms race among miners – to continue to reap meaningful rewards, miners must invest in ever better computational resources and base themselves in locations with access to cheaper energy sources. Over time this inevitably results in a centralized and exclusive group of miners[4].

In the Proof of Stake model used by Nxt, network security is governed by peers having a stake in the network. The incentives provided by this algorithm do not promote centralization in the same way that Proof of Work algorithms do, and data shows that the Nxt network has remained highly decentralized since its inception: a large number of unique accounts are contributing blocks to the network, and the top five accounts have generated 42% of the total number of blocks[5]. Most importantly, energy consumption is the PoS model is significantly lower than in PoW due to its inherent architecture.

Proof of Trust is based not on a peer's token stake in the network like with PoS, but rather their creditworthiness or *trustworthiness* in the network: their Trust token balance. Beyond the economic benefits we gain from this variation, PoT still maintains many of the inherent advantages PoS has over PoW, low energy consumption amongst them.

6. Proof of Trust: Block Creation and Minting

Rya's underlying blockchain technology is heavily influenced by Nxt. For this reason, we may trivially refer to technology that is well defined in Nxt literature throughout the following sections. We strongly recommend the technical reader acquaint themselves

[4] https://blockchain.info/pools
[5] https://nxtportal.org/monitor/

with the Nxt blockchain (specifically nodes, blocks, transactions and forging) before proceeding so as to have proper context[6].

It's important to note that Nxt has a wider range of features (voting, asset exchange, etc.) than Rya. It's reasonable to assume that if a feature is not at least mentioned in passing in this paper, then the feature is not relevant for Rya at this point in time.

While Nxt has a static number of tokens, Rya has a dynamic money supply. Users working to secure the blockchain are rewarded with both transaction fees and newly created Rya. This is a departure from the forging process in Nxt in which the reward is comprised of nothing but transaction fees. Thus, we replace the term forging seen in Nxt with minting so as to best reflect the fact that when a new block is created new Rya is minted in the system.

In the Rya blockchain, a new block is minted roughly every minute. The block creation and authority selection process is nearly identical to Nxt. We have three parameters which determine whether an account is eligible to create a block, which account actually creates a block and which block is prioritized in case of conflict:

1. Base target value. This parameter is unique to each block and is equal to the previous block's base target value multiplied by the amount of time it took to mint that block.
2. Target value. Unique to each minter. Equivalent to a multiplication of the base target value by the amount of time that passed since the last block was minted (in seconds) and the Trust token balance in the minter's account.
3. Cumulative difficulty. Derived from the cumulative difficulty of the previous block plus a function of the base target value of the block.

Just like Nxt, peers compete to generate *hits*. A hit is the first 8 bytes of the output of a SHA256 hash on an input of the 64-bit signature generated unique block metadata and the accounts public key. If the hit is lower than the accounts target value, then the account can proceed to generating the next block. Because the target value grows quickly over time, blocks are expected to be generated very fast at equilibrium (~1-minute target time) and energy consumption is low.

Because it is possible to view each minters Trust balance, it is theoretically possible to predict which minter will most likely generate the next block (due to having the highest target value). The equivalent scenario in Nxt (with stake) opens the door to a *shuffling attack*, a common threat in PoS systems. The idea is that a malignant user could constantly move stake into an account with the highest chance at generating a block and dominate the network.

Fortunately, this threat does not exist in PoT due to the fact that Trust cannot be transferred from account to account or quickly created in an account. Thus even if an attacker predicts which account will next generate a block, it won't do them any good. Therefore, there is no requirement for stake to be stationary in an account for 1440 blocks before the account can mint in the Rya system as seen in Nxt.

When an account generates a block it broadcasts the new block to the network. Network conflict is resolved by adapting the chain of blocks with the highest cumulative difficulty.

[6] https://bravenewcoin.com/assets/Whitepapers/NxtWhitepaper-v122-rev4.pdf

7. Proof of Trust: Transactions and Rewards

There are three type of transactions in the Rya system:

1. Payment transaction - a transfer of Rya tokens from one account to another.
2. Loan transaction - a transaction containing loan metadata (length, principle, interest).
3. Message transaction - a transaction containing a verbose message.

Both payment and message transactions are equivalent to their Nxt versions while loan transactions are of course unique to Rya (Nxt stake loans serve a totally different purpose). The fee for a payment or message transaction is one Rya minimum, while the fee for loan transaction is one Rya added to one percent of the loan principal (see 'Concerns' for details on why). When an account creates a transaction, it is broadcast to the rest of the network for processing.

A transaction is considered unconfirmed until it has been recorded in a valid block (transactions have a confirmation deadline of 24 hours, just like Nxt). As more blocks are added to the chain it was recorded in, the amount of confirmations grows. We define *feesInBlock* as the sum of transaction fees paid in the current block.

Let's address the coin reward for minting. Tokens are awarded to the minter of a block as a function of *T*, the Trust belonging to the account. The tokens are made up of transaction fees (recirculated Rya) and new Rya created from redeemed loans:

$$Minting(C) = m(T) = \frac{T * (goodInterestInBlock + feesInBlock)}{systemTrust}$$

Note that the component of the reward that actually constitutes new coins in the system is positively influenced by the amount of Trust. This elegantly expresses the idea that in the short term higher system wide Trust will lead to more Rya.

8. Concerns

One of the known threats in PoS systems is the 'nothing at stake' attack. This is a scenario in which a clever attacker generates blocks on every fork in the network for a very low cost, assuring they will get the reward for the fork that becomes dominant. This threat exists in PoT as well (as a function of Trust, of course), and in fact may be more severe due the fact that neither the money supply nor system wide Trust is capped, making it tougher to monitor malicious changes in the system.

We do not anticipate this threat to block the functioning of the system however. Due to the fact that the rewards for an individual block are low, such an attack would likely be damaging for the perpetrator (who necessarily has some level of investment in the system).

Next, we must address the 'self-loan' attack. This is when a malicious peer gains Trust by loaning Rya to themselves or to a co-conspirator. This is possible because both a single peer can own multiple accounts and a single account can be owned by multiple peers. There are a few different aspects to this.

As a basic precaution, we designed the *trustReward* for a loan to be dependent on the success or failure of all other loan transactions in a block. It is therefore impossible to determine how big the reward will be until the block is successfully minted. This element of uncertainty weakens the ability of the attacker to plan ahead.

Let's take a look at both short term and long term ramifications of the self-loan and its impact on the Rya system. In the short term, the Trust reward for a lender and borrower must be smaller than passive Trust that can be gained by simply holding the Rya in one account. Otherwise, the self-loaner will be able to benefit more than an honest user (by earning more Trust and Rya).

We propose two ways to enforce the above. Our current solution is that the fee for a loan transaction is one Rya added to one percent of the actual loan. This enforces high short term loan cost. Another proposal is to postpone the delivery of the Trust reward for a period of time after the loan has been redeemed. This would demotivate the self-loaner, as he would gain less Trust in the short term than the honest user.

In the long term though, it always pays off to loan Rya. Just as it does not pay off to statically hold money in the FIAT economy due to price inflation, so too it's not worthwhile to simply hold Rya in the long term. This is one of the features in the Rya system for encouraging consumption in the short term.

This means that both honest and dishonest loans will be preferable to holding Rya in the long term. However, the *most* preferable action (in a perfect market), is an honest loan because the lender will also enjoy the benefits of interest.

Another threat is the 'history' attack. An attacker can transfer a sum of tokens as payment and then attempt to mint a new chain that does not contain the transaction. If this fork becomes dominant in the system, then he gets his tokens back for free. If it does not, he has lost nothing. In PoS systems this attack is usually limited to attackers with very large stake, but in PoT this attack could be perpetrated by any minter with a high Trust token balance, something which could be achieved with a few well timed self-loans. When the system reaches equilibrium and becomes a common medium of exchange, this scenario will be become less likely as it will be tougher to gain high Trust proportion.

9. Conclusion

We have shown that it is possible to create a fully decentralized and cryptographically secured money capable of fully replacing the FIAT monetary system and banking hegemony. By utilizing a free market to determine the price of money and by binding system wide credit to the creation of new Rya, we provide a substantively adjusted money supply solution and ensure that the amount of currency in circulation will be appropriate for the state of the economy.