PROOF OF LABOUR IMPROVEMENT PROPOSAL

Julio Moros
jjmorosr@gmail.com

Oscar Olivera
oscarmolivera@gmail.com

February 22, 2016

Abstract

A typical problem on most of cryptocurrency systems is the implicit sternness around the only option for the monetary creation agreement: The proof of (computational / hashing) work. It is the process of money creation in exchange for the service of securing the system's blockchain, but excluding any other possible money creation agreement, involving any human potential of creativity and labor. One hindrance around this exclusivity of the "proof of work" procedure is its low incentive for the cryptocurrency networks to grow and reach the network effect. This document is a preliminary scope for a proposal offering solutions to include in the monetary creation process, new useful alternatives.

1 Introduction

There are already more than 600 cryptocurrencies and another important set of solutions based on these innovations, from which at least 20 % brings important technical breakthroughs. A lot of the code created here is open source and available to everybody. It is very likely that the existing code will be of a great help to develop this proposed improvement. (We have no needs to reinvent the wheel).

This document is the preliminary scope for a work which is intended to expose a set of interdependent solutions around the idea of a simple but new kind of contract which we have named "flow scrip". Also, the proposal will estimate the feasibility of these solutions on the grounds of a conceptual design by finding if the existing open source code is useful to our goals and how much (if needed) are the required changes to them for assembling the proposed system. Nonetheless, this document limits itself to expose the needed arguments and information to give a reasonable idea about the feasibility of this project.

So, in this document are not exposed in deeply many technical details.

2 Why Dash?

Dash system possesses a set of unique advantageous features that enables it to lead important and deep improvements in the cryptocurrency market.

One of most relevant feature for Dash is its voting platform (Dash Whale) which enables it to anybody and in a decentralized fashion, proposes improvements and takes action in a very short time. An example of this was the recent decision made in 24 hours about doubling the size of the Dash block, from 1 Mb to 2 Mb. A similar controversy has lasted months in the case of Bitcoin, without any meaningful progress by the date this document is being written.

Another feature given by this decentralized decision making platform is the politics of Dash community to allocate 10% of mined coins to research and development of new code or technologies, law and public awareness. This gives the opportunity to fund initiatives like this, fostering new changes as no other cryptocurrency does.

There is another feature unique on Dash platform, which places this system ahead to the needed changes towards new options for money creation: The masternode concept itself.

Dash is a tested and functional breakthrough in decentralizing the third party or intermediary for transactions validation, which is only achieved through blockchain miners in other cryptocurrencies. This paves the way toward new monetary creation options based on agreements for useful services, which in this case is verifying transactions making them immediately confirmed, within a decentralized framework.

3 Monetary Design

In an interview with Professor Bernard Lietaer, one of the co-designers of the euro [1], he defines money “as an ***agreement***, within a ***community***, to use something as a medium of exchange... Any monetary agreement is only valid within a given community”.

Then he stated that money is not an object: “If we regard money as a thing, it becomes a given... If you don’t like the quality of rain, you cannot do much about it. If you don’t like your money system, on the other hand, you can do something about it... Currencies can be redesigned to better meet our needs”.

So, in order to find a good agreement for any money system, better is to know well how a good agreement should be. For an agreement to be valid, in the most of world’s jurisdictions, it must regard three main features [2]:

* It must content an offer (By the offerer).
* It must be accepted by another person (Usually a beneficiary).
* And it must involve a mutual exchange of benefits.

The last condition is the guarantee that the offer won't be in the "Godfather's" way. Both parties must win something from the agreement.

A good agreement should avoid any conflict of interests tempting any party to betray the agreement. If it is not possible, a locking must be designed as collateral to warrant the fulfillment of the agreement.

A good way to avoid many conflicts of interests around communities agreements, is keeping a decentralized structure for the community, with the help of the agreements themselves.

Cryptocurrency systems have proven a kind of "rule of thumb" around finding decentralization solutions. It can be say that if any system can work from a centralized o at least distributed structure, then at least one logistic solution exists for that system to work in a new decentralized structure.

4 Flow Scrip

In business field, the concept of flow money [3] is contrasted with the stock concept. As a whole value, the stock money concept is the most acquainted with us, because we deal with currencies or coins on a daily basis, which are money in its stock form. But it is forgotten that familiar concepts such as GDP, is indeed money in its flow form.

A *Flow Scrip* is a contract in terms of *Flow Money*. In order to explain it, let the term "*benefit*" in this context, describe any kind of merchandise, asset, good, product or service with the exception of any kind of monetary payment.

In a flow scrip, the offerer pledges making available to the beneficiary a ***nominal amount of benefits*** (Let it be, the variable N), in a repetitive or periodical way, according to a ***trading period*** (Variable Γ), from a beginning date (D) to an expiring date, or through a ***validity period*** (V), which must be larger than Γ in an positive integer number of times (t): $V = t \times \Gamma$. At the expiring date (D+V), the contract ends, or "matures".

In order to enforce this contract and to be accepted by the beneficiary, a proper escrow mechanism must be incorporated.

In exchange for the benefits offered in the flow scrip, the offerer must receive a fair retribution, which in order to avoid any conflict of interest must take the form of flow money as well. Let's define this retribution as "***Flow Bond***". This is another contract, but it involves a series of money payments, and is the new proposed mechanism for money creation based on ***proof of labour***.

The escrow mechanism, the Flow Bond, and other needed concepts in order to address the system of the Flow Scrip, are described in the next section.

5 Definitions

Since many of the cryptocurrencies have been designed as a fork of the Bitcoin platform, it would be admissible to introduce some definitions in the basis of the architecture of Bitcoin code. It is convenient to consult a good textbook about Bitcoin [4].

+UTXO: A positive unspent transaction output. Is the same regular transaction output, holding "normal" coins [5].

–UTXO: A negative unspent transaction output. Let's suppose we have an improvement in which transactions with negative coin value can be validated by the nodes of a cryptocurrency network. It would require a "hard" fork in the most of the cryptocurrencies on the market.

Nonetheless, this is feasible and relatively easy to code. At least in Bitcoin structure, the transaction output allocates a field with 8 bytes for the value of the coin [6]. 8 bytes are enough to hold $1{,}8\times10^{19}$ different chains of bits, and the total amount of satoshis, expected to come to exist would fill $2{,}1\times10^{15}$ values. It seems more than enough room for the negative values.

Burning Coin Transaction: It is a recommended practice if a system with negative coins is adopted.

If the data in an UTXO pool [7] managed by the nodes of a cryptocurrency network, is well ordered, then it will be easy to verify if any new transaction output, allocating funds to a specific address or public key (henceforth "destination") has the opposite sign to any of the preexistent UTXO related to such destination. If an opposite sign UTXO is found in this pool for the same destination, then the transaction will be invalid.

For a transaction to be valid, the wallet algorithm that create the transaction, must pick as inputs, enough UTXOs to cancel the value of the incoming inputs, in order to end up with an output in which its sign does not contradict those of any of the remaining UTXOs for this destination.

So, this algorithm is a procedure of "burning" coins: Similar quantities of negative and positive coins for a specific destination, must be *destroyed*, or taken out of circulation.

An important corollary here is that the receiver of a –UTXO transaction, must sign an authorization to receive those negative coins, otherwise the transaction should not be valid.

+coinbase: A regular coin creation transaction. It is a transaction in which there is no input, but an output, with new coins [8]. A *+coinbase* can create positive or negative coins.

–coinbase: A special divestiture transaction for coins. It is a transaction in which there is no output but a set of inputs: The coins to be destroyed.

A *Burning Coin* may be seen as a special case of *–coinbase* transaction.

Reputed Wallet: Is a wallet in which the identity of the owner has been thoroughly established before a community.

In communities where the identity is relevant [9], a crucial weakness is the sybil attack [10]. There is not general consensus about how to solve it, even when some proposals exists [11]. But there are reasons to believe in the existence of such solution.

A different option is to use the "Hierarchical Deterministic (HD) Wallet" structures [12], in combination to the proof of existence [13] with the help of the blockchain, and the assessment of a real community (in flesh and bones).

The idea stands from the fact that biometric data are very bad resources as private keys. A long history of identity theft is known. But as long as ***our bio-data*** are attached to ourselves, they ***are excellent as public data***. We don't want anybody being able to manage our accounts with our bios, but only to indicate where to send funds to us.

Biometric data are good to prove that we are living human beings. In an HD wallet, a simple change can be made to incorporate biometric data. One advantage of HD wallets is that its algorithm can create a sequence of public keys without having access to the corresponding private keys. If the first step, after creating the "mother" private key, is to sign the owner's fingerprint hash value, it can be proven that we can incorporate the signed fingerprint hash value into the blockchain as proof of existence of the new reputed wallet linking that user, and would be a way to prove that such user is the owner of all the public keys derived from that wallet.

Of course, it is also the way to deny the reputability of a wallet with the same biometric data of a preexistent one. (Which is the expected solution to a sybil attack).

Although the details must be developed, is easy to see the need of a final step in security: A *census taking* from a decentralized community. People who knows the user as friends, relatives, neighbors, co-workers, who also own a reputed wallet can be part of a smart contract [14] or a signature procedure, triggered by the wallet owner in case of attack, loss of private key or any incident that can happen to the user, to release the funds of the owner to a new reputed wallet.

Decentralized Pools: Decentralized communities, organized around a specific purpose, and where a consensus is reached for giving to this pool the authority to decide over subjects related to that specific purpose.

Electoral Pool: A special kind of blockchain or sidechain [15] related to a procedure in which a community performs an electoral process including argued discussion, in order to achieve consensus in a taking decision process.

There are some existent proposals to carry on these processes [16], and the outcome from such elections could be used for enforcing some instances of smart contracts [14], as long as the data is stored in the referred sidechain.

Reputation: Is a flag associated with all the addresses of a reputed wallet, indicating the level of credibility or past performance due certain kind of *pay it forwards* within a community.

Credit Line: Is a flag, associated with the mother public key in a reputed wallet to indicate the valid maximum amount of negative coins it can hold. The credit line is a proportional function of the reputation. Only the mother addresses belonging to a reputed wallet can own a credit line.

Credit Transaction: Is a kind of +*coinbase* transaction. The mother public key of a reputed wallet can generate a +UTXO to be transferred to another destination, leaving as a valid output for the mother public key, a −UTXO as long as the absolute value of this −UTXO be less or equal to the corresponding credit line.

Credit line is a way to reward reputation, and if executable by the consensus of a community through electoral pools, it is a solution to warrant future behavior. With the execution of a credit transaction, there is a penalty over the reputation value until the payment of the debt is done or a sequence of good deeds, for restoring such reputation are performed within the community. It is important to say, that this debts are not designed to be charged with interests. There is no hurry to pay these debts.

Mapping: In a market, every person has a set of needs and expectations known in the economic jargon as *demands*. Also, every person or group of people may be in position to offer something to the market. Among the cryptocurrency community, there are many initiatives for decentralized and open source e-commerce platforms, such as Open Bazar [17].

Let’s suppose that in a similar platform, users are able to announce either, their offers as their demands. Then it would be easy for a software make matches or at least help people to do matches in order to tie up the loose ends of sets of offers with sets of demands for certain geographical or specific markets. Let’s call this matching process, a mapping.

Of course, such purpose has some hurdles to solve. People need anonymity to honestly announce their real demands. (Some of the demands may be judged as frivolities by some members of a community). But, with the anonymity come the jokers. So, it may be reasonable to organize decentralized pools of people who vote for the price that the announcements of demands should have. The most eccentric demand announcements may be more expensive than other normal announcements. To avoid any conflict of interests, money charged for these announcements may be allocated for projects of research and development for the community sake. The addresses and payment processes for this purpose must be anonymized, using some of the abundant options that cryptocurrencies offer today [18].

If the interests of the majority harmonize with the growth of the community and with knowing reliable data about the demands of it, then it is likely that the average of prices for ads end up being reasonable.

The other problem for mapping is to know the prices: How much the sellers want to get paid, and how much the buyers are willing to pay. Otherwise, mapping a market is not possible. In the next concept this issue is regarded.

Double Auction: Is a game, where buyers and sellers play a tournament, competing in such way that a fair reference price emerges easily. There are many ways for this game to be designed, and there is abundant literature in the field of economics on this subject. [19]

One issue here may be how to decentralize the auctioneer or anonymize participants. However, cryptographic tools provide enough flexibility to publish encrypted data and later expose the decrypted, proving that it correspond to the encrypted and letting the game to go on. So this point is not a real concern.

The relevant feature here is that as participants win, prices are agreed between buyers and sellers, which is a way to be rewarded. But they can also get publicity to the community, which is another kind of prize. All this can be done by decentralized open source software.

Also, double auction tournaments can be games to be really enjoyed by the members of diverse communities. It is an opportunity to socialize, making that you and your business be known. And finally, these games can be organized as events to rising funds to establish a first market, for example, in a new city.

A real concern for double auctions, is to choose a referential commercial activity (some service or product) to establish a reference point for prices. The Flow Scrip can be seen as a special state of existence of money. It is a monetary state of existence without any currency quantification. But it is quantifiable money in terms of flow of benefits. The purpose of these events of double auction is to build a general scale independently of the shadow of any fiat currency.

A benefit delivered by any group of human beings is the same benefit regardless of race, nationality, culture, gender or religion they are, and should be valued independently of these conditions.

Business Wallet: A special kind of a reputed wallet, related to a commercial activity which identifies completely a business. The closing of a Flow Scrip contract is a suggested occasion for the creation of a business wallet. In such case, the mother public address of the wallet, henceforth, ***the charge account*** will be reputed with a credit line of at least the price of the nominal amount of benefits (N).

Let’s suppose the price for this amount N of benefits in a given currency is P. Such price may be the outcome of a negotiation from a reference scale or directly agreed from a double auction tournament.

The Business Wallet then will be linked to a smart contract [14], which will be the programming code form of the referred Flow Scrip. The instructions for this smart contract will include:

1°.- At the beginning of every trading period: Perform a credit transaction over the ***charge account*** for the whole amount P, leaving a –UTXO in this address, for –P coins and transferring the corresponding +UTXO, for +P coins to the first public child address, henceforth, ***the credit account*** of the wallet.

2°.- At the ending of every trading period: Pick all UTXOs corresponding to both the charge and credit accounts, and use them as inputs for a –coinbase transaction, in order to destroy all the involved coins.

As the business wallets will address the operation of groups of partners, several people will access different accounts of the same wallet. Due to that in HD wallets, all the private keys are deductible from the mother private key, all the UTXOs linked to every public address of the wallet, must require additional spending logical conditions besides the corresponding private key, in order to be unlocked. Otherwise everyone would have access to the accounts of all their partners.

One solution may be to request to every partner, an additional signature from a private key of an address of their personal reputed wallet. But as another contract runs besides the flow scrip, there is another logic condition that can be used in order to claim ownership over the coins belonging to the addresses of a business wallet: Shares, [20] from the corresponding Flow Bond.

3°.- A ***business account***, is any business address of the business wallet, different from the credit or charge accounts.

4°.- In order to unlock any UTXO by the owners of a business account, the unlocking script will request at least three conditions, for these kinds of accounts:
A signature from the private key of the business address,
A signature from the mother private key of the personal reputed wallet of the associate
And metadata or a token [20] used as share certificate, provided by the smart contract which executes the flow bond, and which proves the participation of the associate over this bond.

Only UTXOs with a token or metadata of a valid flow bond attached to its unlocking scripts will be accepted as valid coins in the flow scrip system.

The business wallets related to the flow scrip system may operate through side chains, with their ***own transaction rules***, operating in isolation from any main blockchain. This may be convenient for the shake of the lightening of the payment system performance. Let’s suppose the operation on a side chain. Then an additional condition is feasible:

5°.- Transactions in the flow scrip system will be addressed as ***tickets*** [21], or under a tracking event paradigm. And the only events acceptable for valid tickets will be purchase or exchange orders. A proper escrow mechanism is a crucial element for transactions in flow scrip systems.
So, with exception to tickets or transactions generated by the flow bond that handles the flow scrip, those transactions which only transfer money between accounts won't generate valid tickets.

Smart Trust: Usually when a group of corporations agree to work together for a common goal, rewarded by a very generous contract, they hire a trust with a bank. Many lawyers, a lot of paperwork, large fees and taxes are justified by the promised contract. What if this bureaucratic tool is turn into a digital smart contract, for free and without so many paperworks? Cryptographic tools make this feasible today!

A Smart Trust is a smart contract that uses a public side chain to perform its operations. These side chains don't have to use a proof-of-work mining process. Blocks in a side chain may be forged, in a similar way as some alt coins [22] work, but let's discuss this in detailed papers that will be part of this project.

For the smart trust to work, it takes:

1°.- At least, one ***trust address*** (Or trust account) owning a balance of a proven value (Coins, Certificates, Shares, and so on) or UTXOs, which locking conditions are signature structures, made from token's metadata provided by the smart trust.

2°.- An independent token (T) as currency, which the smart trust will create as be needed.

3°.- A private decentralized pool of trading, where users will register their public address, where to redeem their payments.

4°.- A signature structure and a set of private rules in order to validate transactions done with its own private token.

5°.- A ***workshop period***. During the workshop period, a "tasks market" or "benefits market" will be carried on between the users of the pool and in exchange for the private token as coins, in order to meet goals of work and production. The tokens each user "i" receive as result of their work (Let it be T_i) are their ***proof of labour***, which is signed in some way by the smart trust.

At the end of each workshop period, users can claim their corresponding dividends from the trust address or trust account to their registered public address, in exchange of their tokens.

The amount to be transferred to each user is a percentage of the total amount of tokens.
(Dividend % = T_i / Σ T_i)

Flow Bond: Now is easy to see the flow bond as a kind of smart trust.

In this case, the trust address is the credit account of the business wallet related to the Flow Scrip.

The tokens are the shares of the bond. The decentralized pool is integrated by the partners and shareholders of the business, who are going to operate it.

The rules and the signature structure for this kind of contract is a complex and comprehensive subject-matter to be detailed, but which logistics is a feasible solution operated by several real cooperatives [23] in several ways. Also, the rules will depend on the initial agreement for each specific flow scrip contract.

Each user will be related with their business by different functions. Shareholders have a different relation than the associates, and the same user may be a shareholder and an associate. So the same user may have several business accounts in the business wallet. To avoid confusion, let's refer as "user", to the combination of a pool member and a specific business account.

The operation rules for the flow bond will be:

1°.- During the workshop period, the flow bond distributes different tokens among users. The workshop period may vary as the user. For shareholders, the workshop period is zero, because for them it is known in advance their slice.

2°.- Distributed tokens remain inactive until the end of the workshop period.

3°.- At the end of the workshop period, a ***validity lapse*** will be applied to the tokens for activate them and it will last the same that the trading period of the flow scrip, for all the tokens

4°.- The tokens of the previous validity lapse will now have an inactive condition (expire date condition) so the flow bond can now execute them. The flow bond will check the coins in the side chain associated with the flow scrip it handles, looking for expired tokens in all the UTXO's unlocking scripts. It will pick all such coins to create a –coinbase transaction, removing all that old coins that weren't used.

5°.- Then, the flow bond will exchange the active tokens of each user in order to pay their respective dividends, creating transactions that send the money from the credit account to the business accounts of each user.

This process is repeated until the flow scrip expires, and the last unspent coins be removed by the indication of their expired tokens. The flow bond expiration date would usually be at the expiration date of the flow scrip, plus one additional trading period.

A valid question here is: How to save money under the flow scrip system?

Outgoing Transaction: Are the first options to save money coming from the flow scrip system. The most important and necessary of these transactions is a ***paying debt*** transaction.

A transaction which destroys coins from business accounts to create positive coins to the mother address account of the reputed wallet of the same owner. Then a burning coin transaction must be included.

Other options may be to buy cryptocurrencies from regular blockchains in exchange for benefits offered by flow scrip systems, as long as there were agreements to such crypto communities.

And a third way, may be destroying coins from business accounts to create coins in any other cryptocurrency address by some agreement with that crypto-community, if there were an important traffic trade of benefits with some flow script community.

There are many solutions to assess, like colored coins or alliances with other flow scrip communities. The solutions wouldn't need a deep change in the code of any cryptocurrency, just an agreement between communities.

Different flow scrip networks could establish trade alliances no matter the currency they use. Is enough to synchronize their open source protocols, since flow scrip are anchored to the value of the fruits of human labour, not to the value of any currency. So, price scales of different networks should be easily coordinated.

Project Smart Trust: Another useful form for a smart trust is one that helps a team to create a new business, instead of periodically deliver benefits from an existing one.

In this case one of the trust accounts may be the whole *cake of shares*, a unity, and a 100%. And tokens will let the users to get their shares of the new business once incorporated.

Another trust account required, may be some ***fund account*** where investors or backers will fund the project (As in crowdfunding), and the corresponding unlocking metadata will just be used to spend these funds wisely for the sake of the project, and not for the personal pockets of the project team members.

Then, shares coming from projects are the way to get tokens from any future flow bond and claim the dividends coming from any flow script in which the business would get involved. In order to guarantee the rights deriving from these shares, the owners have at least three possible mechanisms:

1°.- Proof of Existence, including in a blockchain the data of the certificate, linked with the proof of existence of the business, which is a necessary condition to create a business wallet.

2°.- All the proper chains of signatures, regarding the processes of creation of tokens from the smart trust of the project, and the signatures claiming the incorporation of the business.

3°.- Electoral pools. If anybody had any problem to claim a fair participation on dividends from a flow bond, he or she may appeal to an electoral pool among the decentralized community to enforce the fulfillment of their shares.

Among the rights that a portfolio of shares should reward to its owner, must be a system of improving reputation, according to some rules to be designed. So, with the ownership of new shares, comes an improvement of the user's personal credit line.

The rules of a *project smart trust* are again a very comprehensive subject to be developed in detail, but the authors of this proposal agree in its feasibility.

In the case of projects, the amount of workshop periods needed and their duration will depend on the project itself. A project trust is not related to any flow scrip.

There are many ways to participate to a project. People can invest money to buy tokens of the project smart trust. But also they may sell their services, advice with their knowledge or help with their assets or intellectual property for the sake of the project in exchange for tokens. (Something important to tell in this point is that if any user in the flow scrip system has a debt in his or her personal reputed wallet, any extra funds to be invested or exchanged for shares in a project, will be directed by the protocols of the system, to pay the debt in first place).

Remember that the tokens are the proof of labour from which money will be created in the flow scrip system. So, a way to save money in the flow scrip system may be in the form of shares of businesses that the community helps to integrate.

A remarkable idea here is that projects for automation of work places in existing businesses are a special form of the incorporation of a new business, because the associates, who work as cooperative members, may end up as shareholders of an automated company.

So, project smart trusts are a way for not to be affected by the automation of our workplaces. Imagine large cities with all its citizens working very motivated, assiduously, to automate and to be released from, their jobs, in a new industrial revolution.

It closely resembles the so-called ***technological singularity***.

Backing Pool: It is the decentralized pool that backs the incorporation of each ***reputed wallet***, and is the group that can help the wallet owner to unblock his or her funds in case of any sinister. This group of people can emerge from double auction tournaments, or from mapping events fostered to create trade groups within local communities or located within the same city. Nonetheless, they may be spread globally. The most important issue about the backing pools is to know well each person incorporated to a reputed wallet.

The higher the number of people backing a reputed wallet the better the security level. Credit line from reputed wallets, will always be collateral for the reputation level of each wallet owner, and can be executed by means of an electoral pool.

Sponsor Pool: Is the equivalent of the backing pool for business entities.

In crowdfunding, every initiative starts with the looking for backers during the project's campaign.

In the flow scrip system, a campaign may be started with the purpose of fund or for backing a project to incorporate a business, but a campaign may also back or even fund an existing business with which to close a flow scrip contract. In both cases, a ***campaign period*** must be proposed, with a goal in reputation (Credit Line) or investment funds.

People who like the business or project proposal will approve the campaign and then will be included into the sponsor pool.

During the campaign period, the sponsor pool may create electoral pools to discuss the relevance of the business or the project, assess the ways to verify the credentials to create the business wallet or the project smart trust, and will discuss about collaterals the business team can offer to warrant the fulfillment of their promises.

The former is a service that the sponsor pool will perform in order to share small dividends (royalties) from the future flow bond (In the case of flow scrip campaign), according to a special smart trust that will reward the members of the pool with reputation quantities that they may exchange later by tokens of that flow bond if they like. In the case of a project's campaign, the royalties are even better: Shares of the newly created business.

Sponsor pools may have the power to decide things like the nominal amount of benefits, the reputation of the business, prices to close the deal, expiring date and the trading period. Among the sponsor pool, is expected to be some of the customers to buy the benefits offered by the flow scrip and so, the pool will be indeed the beneficiary of the flow bond contract. So, the beneficiary to this contract is a decentralized entity.

As the following is a legal subject to be studied in detail, and will depend on the jurisdiction the flow bond is agreed, the sponsor pool should sign with the business entity, a donation agreement or at least a mandate to receive trustee powers over the traded benefits.

Such agreements make the sponsors the owners of future benefits, but only with the purpose of being donated or given to others in a kind of a bartering club, in order to use the benefits as collaterals for the contract, and also to meet conditions for tax avoidance, since the flow scrip is a contract in which the business has resigned from profits in any form of fiat currency and turns it in a kind of non-profit agreement.

Master Pool: A decentralized pool that will play the escrow service role to track and validate the tickets of buying and exchange transactions in flow scrip systems.

The master pool members have similar functions than masternodes in dash platform [24]. As masternodes must exhibit a proof of service, in the flow scrip system there is a very similar paradigm helped by smart trusts (the proof of labour).

But instead of masternodes which need 1000 dash as collateral, master pool members just need to have the enough reputation (credit line) for the responsibilities they expect to afford, as collateral available for a sponsor pool to be executable under specific circumstances by an electoral pool.

Master pools will attend a set of flow scrip contracts, and they will be responsible for the clearance of the charge accounts of business wallets related to those contracts.

The sets of charge accounts they will attend are variable, and will depend on the agreement of each ticket generated by a buyer and a seller, the schedule the pool member that is serving for this case and some pseudo random cryptographic functions.

To initiate or enter into force a flow scrip contract, the business must delegate the clearance of its charge account to a master pool. Then, no selling transaction can be completed by any associate of the business.

Tickets are different from transactions in the way they are a sequence of data structures which must be validated by the corresponding signature. For example a buying transaction ticket:

1°.- Starts from a valid advertisement of selling a benefit of a flow scrip, and is initiated by the buyer who signs it by pushing some “buy” button. This action will sign a data structure, similar to a transaction with only inputs (–coinbase): The spending of the UTXOs to be used to buy the benefit.

2°.- This ticket raise a flag and is broadcasted among the master pool, and some of them will be assigned as authority to clear the ticket.

3°.- The ticket could only involve a simple clearance of a transaction, while at the other end the transaction may be a raffle to hire some trained member of the pool to carry out an inspection work, in person.

4°.- If the transaction is not under any attack, and all parties are honest, the automatic process will then authorize the seller to spend the corresponding –UTXOs of the charge account, and this last signature closes the ticket.

5°.- If any controversy arise, then the on duty pool member will assist the case, as a human being and according to a procedure that will be registered in the ticket, as any regular customer support service would do. If there weren’t enough pool members attending the net, then the decision would rest in some mining network to validate and include (or refuse) the transaction (ticket) on the blockchain or side chain.

As we can see, the master pool performs a service, and is expected to be paid. The way to do this is through a special flow scrip agreement. The pool member is backed by a sponsor pool which activates their business account, but for just one associate.

In this case, the pool member submits their charge account, together with their personal credit line to the sponsor pool, under a smart contract: the flow scrip. But there won't be any flow bond distributing dividends. All the dividends will be available for the pool member from his/her credit account to spend it as he/she pleases.

Every ticket cleared, will use some of the UTXOs to be spent, into the charge account of the master pool member by a burning coin transaction. If there is no incidents, efforts are saved for the pool member. Otherwise, he/she will have to do his/her job.

The most important idea here is that the service of clearing transactions is an exceptional service for the survival of any money system, and it should be regarded as the referential commercial activity mentioned in the definition of the double action concept.

To establish a reference point for prices, let's see how profitable the masternode service in dash is. More or less, it should be the reference "wage" for the master pool service of clearing ticket transactions. By a long period, the profitability (in dash coins) of a masternode has been around 12% per year [25] (A flow money measurement). So the reward of a master pool member for attending similar amount of cases should be around 12% of their credit line, per year.

From this reference, a series of other services may be deductible, using it as a start point for a price scale.

Complete Market Circle: When from a mapping process there is found a sub group of people between which every demand has been completely covered by the offers made by this very same sub group. Then we can call this sub group as a ***complete*** market circle, or complete group.

Finding complete groups may be a part of the decentralized open source software for free markets referred in the definition of "mapping" concept.

6 Rules for the Flow Scrip System

In order to give the best design for the flow scrip agreement, it should meet some suggested criteria, avoiding the most of conflicts of interests possible:

Rule N° 1: Avoid measuring the benefits in terms of time of service or man hours.

The nominal amount of benefits may be measured in physical items (pieces, units, square feet, an so on) or if too complicated in terms of prices of the merchandise, but if it is measured in terms of time of service, the interests of the customer who expects the higher efficiency would be in conflict with the interests of the supplier of maximize profits. Look

for the objectives behind the time of the service in order to find the best way to express the benefits in the best way for the agreement.

Also, by measuring the benefits in terms of time, as technological innovations progress, and the human efforts needed to achieve the same goal decrease, there will be a conflictive interest into a reduced payment for the same benefit delivered, which is not fair and discourages technological progress.

Rule N° 2: Look for formalism in the contract which rewards the capacity of dispatch, instead of the volume of sales while satisfying market needs.

The contract should be fulfilled just with making available the nominal amount of benefits, and never say “NO” if the business is still under commercial commitments. But if the complete nominal amount is not asked within certain trading period, it doesn’t mean that the business breached, provided that it had the ability to dispatch.

The reason for this is the ***planned obsolescence***. This rule encourages precisely the opposite, within the flow scrip systems.

For example, an automobile repair shop. In regular market economy, if you don’t sell there is no income. So, you need flawed cars frequently to survive. But under flow scrip commitments, you may fulfill the contract whether or not customers come to you to fix a car. So, is for your convenience to leave every car in the best possible conditions, so no user come back to “nag” you.

Rule N° 3: Protect the business, placing the productive activity as a priority.

For example, if a burglar goes and steals some pieces of bread to a baker, pieces committed under flow scrip, the baker shouldn’t lose anything. If there was someone who needed his products, and in fact they were “dispatched”, the baker should be properly rewarded.

By the proper evidence and witnesses, the master pool may checks the facts, destroying the value of stolen merchandise (–UTXOs coins) to the baker’s charge account.

In second place, if the burglar is successfully identified, in any way, a reputed wallet may be created by the concerned community, and his credit line executed, waiting for the character to recognize his mistake and restore his reputation.

Rule N° 4: Seize the opportunities the flow scrip gives.

We can see the flow scrip as a capital asset that can be traded. Among the sponsor pools, people may arrange other kind of project campaigns: To arrange composed and, or partial flow scrip contracts.

Composed flow scrip is the combination of several flow scrip not interconnected, in order to create a meta-agreement, between several companies, to produce together in synergy.

Partial flow scrip is the creation of “shares” or chunks of the contract, in order to enable the selling of these rights to individuals or companies.

These projects can be carried on by specific project smart trusts, in order to distribute the profits of the initiative between the community members. An important warning here is that flow bonds should be able to be re-coded, in order to enable the trade of bond shares.

Partial / composed flow scrip contracts may be sold in exchange of shares of the corresponding flow bonds of the buyers (Who are supposed to run business or own bonds in the flow scrip system).

But also partial / composed flow scrip contracts may be sold in exchange for a fiat currency loan, receiving the money to a banking trust that the community must previously created.
The interests from these investments may help every member of the flow scrip communities to pay taxes, as long as their business operate as non profit to the eyes of the revenue authorities, but the business assets will always charge the owners with levies.

Finally, the flow script is a kind of future or derivative which effect, is to stabilize prices in the currency it is traded. And if the automation is fostered, a process of deflation will evolve. The problem is that these currencies have ephemeral existences. But the flow bonds may be a good capital asset.

For example, suppose a partial flow script which gives to the owner the right to take until 20 pounds on fruits and vegetables weekly. That may be $10 per week, $520 per year. Let’s say a typical public bond pay 3% per year. So to get $520 per year, we would need $17.000,oo. A competitive offer would be ask $6.000 in exchange for that flow scrip. We would get $170 per year by buying a very non risky bond with that money. But we would be able to pay the needed taxes. At the maturity term, the investor enjoyed his or her fruits and vegetables by the validity period, and received back the whole $6.000, a great bargain.

7 Action Plan

As project, this proposal must explain a clear objective. This objective is aligned to a new structure for the society, in which everyone has access to the mechanics of money creation, fostering the emergence of decentralized monetary systems as the dominant form of money for all mankind. In order to conceptually explain how to trigger this emerging process, some important concepts are exposed.

Network Effect: Is a positive feedback process [27], which may be described by the help of epidemiologic equations [28], and describes a transformation process in human societies from an initial state of exclusion of a social network, up to another state of plenary use of such network.

People don’t find very attractive the membership to these kinds of networks until a minimum number of people, known as ***critical mass*** is using it. After this point an accelerated positive feedback loop is triggered where a massive migration to the network

happens, which may be called the "***avalanche process***". Lastly, migration decelerates after a point that can be called "***saturation***". These processes may be approximated to the logistic function [29].

Incentives: For the network effect to be feasible, the social dynamics involved must regard a couple of main features:

#1 Alliances: The network design must regard the flexibility to trace bridges or alliances with other competitor networks, for some mutual benefit.

#2 Fledgling Network's Benefit: There must be an intrinsic benefit for any new network user, since the very beginnings of its history. In the design of the decentralized network dynamics, it must be checked: Is there any advantage for a new user, from just becoming a member even if there are too few users?

Mathematic Modeling Conclusions: We developed a simplified mathematic model to simulate a set of social transformation processes. This model was based on the epidemic models, a rectification for the Metcalfe's law due to Odlyzko [30], some conclusions from Zipf's law [31], models for population evolution [32], and others. It is a lot of math, with a set of numeric criteria with which this document will not deal. (If wished, the reader may contact us to share our model details). The important here are the conclusions founded from the simulations:

1°.- ***Social transformations happen in cities***. These transformations don't take place mainly in other geographical bodies, as whole countries or estates. Social transformation processes happening inside cities are quite independent from the spatial-geographical variables. Inside the cities all the social reactions happen in a more or less uniform way.

2°.- ***The bigger the population in a city, the faster and the more intense will be the avalanche process***. Although, in bigger cities the "***critical mass***" event is longer delayed.

3°.- ***Some Simulation Results***: We performed a simulation for a big city, with around ***10 million people*** in age and conditions to produce. It may be a city with around 14 million people like for example, Los Angeles.

The simulation criteria start from the condition to reach at least one complete market circle of, let's say 30 people. This was a moderately pessimistic criterion. Of course, from mapping and double auction tournaments can emerge several complete groups, but is not expected for all to succeed. Let's suppose that the initial condition starts from at leas one successful group.

This complete group impose themselves a challenge: ***Help each other to survive*** without using any fiat money form.

With this and another set of numerical conditions for the equations, we found that the ***critical mass is reached in around 1.200 days***. (A little more than 3 years). It means that,

in regard of any mistakes in calculus, a critical mass in a big city may happen within a period of time of the magnitude order of five years.

But the ***avalanche process lasts around 3 months***!

It means that, accepting several errors in calculus, a massive migration are happening literally suddenly overnight in a big city. In other words, the whole population on a big city is leaving behind the dependence on fiat currency from one day to another. Think of the impact of such event at global scale in a highly interconnected world.

A First Conceptual Action Plan: Based on the above information, we can get a rough idea of a conceptual plan to unleash a process of fully decentralized social transformation.

Step #1: Creating the code for the integrated open source decentralized software for the flow scrip system to work. This implies that all the necessary proof of concept and sandboxes tests have been done.

Step #2: Organize by the means perhaps of a set of independent crowdfundings, a series of tournaments of mapping and double auction events in several big cities (Let's say, around 30 big cities in the world). Best if are done more or less simultaneously. These tournaments must have as one of their goals to reach complete market groups. And the challenge of these complete groups may be:

- Cover the needs of the group members in order to be able to quit their annoying jobs.
- Stop using fiat currency... Or
- Simply to minimize (to almost zero) their costs of production as business, maximizing their capitalization potentials.

So, these complete groups are like (decentralized and open) clubs of mutual support to save money and for creating new businesses, at the beginning. And that's a good ***fledgling benefit***. After network effect, they become in networks of people creating real decentralized money.

But an additional condition must exist to optimize the possibilities to reach the network effect: An alliance to at least one decentralized money system. This is possible, at least thanks to the decentralized democratic platform of Dash Whale, which may let the money created by credit transactions or colored coins for investments, be sold in exchange by dash, if such thing is agreed. But we can bet there will be a lot of other options with other cryptocurrencies.

Step #3: Repeat periodically, by certain term, this recipe (Mapping and double auctions tournaments) in so many cities as possible.

Step #4: Just wait and see how the network effect unfolds spontaneously (May be in an amazing global scale).

Under these circumstances, small complete groups which succeed in establishing themselves in big cities simultaneously will set the conditions to eliciting by itself a network effect reaction.

8 What we Offer

The work under the scope of this proposal is to assemble the document structures to create the code for a decentralized software package which let its users to organize themselves as decentralized and collaborative trading communities. Our compromise will include the following:

1°.- A set of detailed technical whitepapers, explaining how to design and code all the solutions involved by each of the concepts defined in section 5, on this document. However, our biggest priority is how to design the smart trust.

2°.- A main whitepaper describing at least one conceptual design for the creation of a coherent system complying with the objectives proposed by the flow scrip system.

This coherent system will be an ***integrated solution*** on decentralized open source software for anybody to take part of it.

3°.- At this point there should be a lot of doubts about details of this proposal, but the most important is for the reader to have now an own idea about how feasible is this proposal in order to invest on it, given the information shown, even when according to the authors this system is completely feasible.

During the campaign for this proposal on Dash Whale electoral system, all these doubts will be discussed, and then we offer a compilation of such discussions to be shared on a document.

4°.- Detailed technical reports for every solution explained in the whitepapers, compiling the existent open source software that can fit into the flow scrip system. Is very likely that the most code needed already exist, and the rest be already on birth labor. These technical reports will indicate:

- How this code can fit into the flow scrip system.
- How many changes may be needed to make the code be functional in the system.

5°.- Direct communication with the authors, whether by whatsapp, mail, skype, hangouts, and so on. A weekly meeting may be arranged to check progresses.

6°.- Git Hub repositories of all documents to generate the needed synergy, for anybody interested in the project to collaborate in the developing of the code for this integrated solution.

As far as we are just two people, to achieve these goals in a realistic lapse of time, we estimate ***four*** (4) ***months*** to do at least the 80% of the work.

9 Economic Proposal

Given that, as consequence of this proposal people will be able to create their own money in a limitless number of ways, this project has the potential to make EVERYBODY to earn a lot of money. But even best: If it succeed, this project has the potential to transform the human society.

The authors: We are Venezuelan professionals, who have been involved in the monetary design topic for more than four years.

This proposal is a subject we have been discussing for around a couple of years and stumbled upon the cryptocurrency market since then. But only from the last year we realized the huge potential that the decentralized social structures have for unleash all the power of these ideas.

More info about us can be found in our linkedin profiles [26]. The estimated dedication for this project is at least one of us by full time, and the other for part-time. So, we think enough, for two people and in regards to the ambitions of the work schedule we propose, ***a bid of 220 Dashes per month*** by four months.

The progress of our work may be exposed weekly, as the budget must be approved as a monthly basis (As we can see). At the end of the fourth months, progress may be assessed and further proposals for the next steps, like the integrated code to be developed and tests may be discussed.

10 Conclusion

This document has exposed arguments to assess the feasibility of a project, and gave both a technical and economic proposals in order to the authors develop in detail the initial stage of said project.

The technical proposal exposed a set of arguments to give to the reader elements to decide by him, the viability of the project. The project propose the development of a decentralized system as cryptographic tool and software platform, with the aims to be compatible with at least the most of bitcoin forked cryptocurrencies of the market, to multiply the options of the process of money creation, backing this creation processes with proofs of human labor.

It also exposes an action plan for the implementation of the money system through a process based on the network effect.

The economic proposal exposed a work plan to be funded by the democratic decentralized platform “Dash Whale” and a bid of 220 dashes was given.

11 References

[1] Professor Bernard Lietaer. https://en.wikipedia.org/wiki/Bernard_Lietaer
Interview published in his own webpage.
http://www.lietaer.com/2010/09/what-is-money/

[2] For a contract to be valid:
http://www.quickanddirtytips.com/business-career/legal/what-makes-a-contract-valid

[3] Stock and Flow Money concepts: https://en.wikipedia.org/wiki/Stock_and_flow

[4] Antonopoulus Work: Mastering Bitcoin.
http://chimera.labs.oreilly.com/books/1234000001802

[5] UTXO: Transaction Outputs and Inputs.
http://chimera.labs.oreilly.com/books/1234000001802/ch05.html#tx_data_structure
http://chimera.labs.oreilly.com/books/1234000001802/ch05.html#tx_inputs_outputs

[6] Table: The structure of a transaction output.
http://chimera.labs.oreilly.com/books/1234000001802/ch05.html#tx_out_structure

[7] UTXO pool:
http://chimera.labs.oreilly.com/books/1234000001802/ch05.html#tx_outs

[8] Coinbase:
http://chimera.labs.oreilly.com/books/1234000001802/ch08.html#_the_generation_transaction

[9] A community where the ID is relevant: Groupcoin.
http://groupcurrency.org/#AppendixA

[10] Sybil Attack: http://groupcurrency.org/#Sybil

[11] Some proposal about how to address sybil.
https://github.com/d11e9/poi

[12] Wallets: http://chimera.labs.oreilly.com/books/1234000001802/ch04.html#_wallets
Hierarchical Deterministic Wallets:
http://chimera.labs.oreilly.com/books/1234000001802/ch04.html#hd_wallets

[13] Proof of Existence:
http://chimera.labs.oreilly.com/books/1234000001802/ch05.html#op_return

[14] Smart Contract: https://en.wikipedia.org/wiki/Smart_contract

[15] Sidechains: https://en.wikipedia.org/wiki/Block_chain_(database)#Sidechains.
https://bytecoin.org/blog/sidechains/

[16] Democratic decentralized platforms. Bitcongress and Loomio.
http://www.bitcongress.org/BitCongressWhitepaper.pdf
https://www.loomio.org/?locale=en
https://en.wikipedia.org/wiki/Loomio

[17] Decentralized / Open-source e-commerce platforms
https://bitsquare.io/
Open Bazar: https://en.wikipedia.org/wiki/OpenBazaar ; https://openbazaar.org/
Bitmarkets: https://en.wikipedia.org/wiki/Bitmarkets ; https://voluntary.net/bitmarkets/

[18] Secret identity solutions (Monero)

http://chimera.labs.oreilly.com/books/1234000001802/ch09.html#_anonymity_focused_alt_coins_cryptonote_bytecoin_monero_zerocash_zerocoin_darkcoin
https://github.com/bitmonero-project/bitmonero
https://downloads.getmonero.org/whitepaper_review.pdf

[19] About Double Auction.
https://en.wikipedia.org/wiki/Double_auction ;
https://www.youtube.com/watch?v=q2qXM7C8OdM

[20] Colored Coins
http://chimera.labs.oreilly.com/books/1234000001802/ch09.html#_colored_coins

[21] About Tickets Paradigm
https://en.wikipedia.org/wiki/Issue_tracking_system
Open source software: https://en.wikipedia.org/wiki/Request_Tracker

[22] Consensus innovation: Alternatives to proof of work in the blockchain paradigm.

NXT:
http://chimera.labs.oreilly.com/books/1234000001802/ch09.html#_consensus_innovation_peercoin_myriad_blackcoin_vericoin_nxt
https://bitbucket.org/JeanLucPicard/nxt/src
http://nxt.org/developers/whitepaper/

[23] About Cooperatives.
https://www.youtube.com/watch?v=qbZ8ojEuN5I

[24] Masternodes
https://www.dash.org/wp-content/uploads/2015/04/Dash-WhitepaperV1.pdf

[25] Profitability of a masternode:
http://178.254.18.153/~pub/Darkcoin/masternode_payments_stats.html

[26] Author’s Linkedin profiles:

Julio Moros: https://ve.linkedin.com/in/julio-moros-09b39213
Oscar Oliviera: https://ve.linkedin.com/in/oscarmolivera

[27] Network effect: https://en.wikipedia.org/wiki/Network_effect

[28] Epidemic Model: https://en.wikipedia.org/wiki/Epidemic_model

[29] Logistic Function: https://en.wikipedia.org/wiki/Logistic_function

[30] Metcalfe Odlyzko:
Metcalfe Law: https://en.wikipedia.org/wiki/Metcalfe%27s_law
Odlyzko Paper: http://www.dtc.umn.edu/~odlyzko/doc/metcalfe.pdf
Who is Odlyzko: https://en.wikipedia.org/wiki/Andrew_Odlyzko

[31] Zipf's Law: https://en.wikipedia.org/wiki/Zipf%27s_law

[32] Population grow and interaction between species:
https://en.wikipedia.org/wiki/Exponential_growth
https://en.wikipedia.org/wiki/Population_model