OLY: A Time-Stable Cryptocurrency and Self Regulating Network

Aloysious Zziwa
azziwa@olycash.com
www.olycash.org/whitepaper.pdf

May 01, 2019

Abstract

In this paper, a currency is presented that allows proper representation of value in relation to fiat currencies over passage of time. In addition, a self sustaining protocol for communication and processing of transactions in this currency over a network of untrusting, unreliable computing nodes is discussed. This currency, "The OLY", automatically stabilizes value by minimizing contribution of rapidly fluctuating third-party/fiat currencies and increasing contribution of slowly fluctuating currencies to its value. This change of value is nominal and does not attempt to control supply through issuance of new or secondary coins or bonds. Amounts in this currency are always quoted with time, say OLY150.00000000|1556752842 a short form of *150 OLYs on May 1, 2019 4:20PM* or usually read in quick human friendly form as "150 bar 2019". By quoting the amount with time, amounts could be different but equal to the same value due to time difference. As a result of fiat currency inflation tendencies, the earlier amounts will generally be expected as higher in value compared to equal later amounts. Also, since the value of the OLY does not depend on a single currency or asset, trust is not placed in any single government, its creators, organization or asset to ensure stability.

The OLY Network consists of decentralized exchanges to transfer this currency into local fiat currencies, and in return, their activity acts as a feed for the exchange rate distributed database based on completed transactions on the blockchain. Further, the concept of hashtime is introduced to allow parallel processing of transaction blocks by different impromptu "committees" of nodes that are created and disbanded after their block processing is completed. The proposed protocol includes standards for turing-complete scripting, sharding, preparation of smart contracts, self-policing nodes, punishment and appeal processes among others. Using Proof-of-Stake, an approach is proposed where a node's stake is composed of two parts; amount risked and the node's reputation points in the network. These values may be affected by the node's activities and honesty is rewarded while bad behaviour is punished with appropriate severity. Message sending and confirmation among the nodes is achieved using the gossip protocol and recurrent subsampling with Byzantine Fault Tolerance.

It is for this approach that the OLY can be regarded as a true currency as it is a proper representation of value at any point in time in the eyes of whoever is paying or being paid. Instead of guessing or attempting to estimate real-world representation at any time, this task is dynamically coded into the currency by allowing its value to be backed by trust in real, completed and accepted exchange rates.

1.0 The OLY Currency

The need for a time-stable currency is essential for proper exchange of value over a cryptocurrency network. It is unfavorable to one or both parties involved in a transaction if a price of an item or service varied drastically over a very short period of time. If an attempt is made to keep the amount of a currency as equal to its numerical value and representing this as a mere number, it creates a need to award currency holders with a form of compensation for variation in the currency. Proposed compensation schemes include issuing new coins to increase supply or issuing bonds to reduce supply. This becomes complicated to implement in a fair manner, track and maintain, yet runs afoul of some real-world regulations.[1] For the OLY, Since the value of the currency at exchange is tracked at any time in usage, such measures are not necessary to achieve stability. Two dimensions of a currency need to be tracked to maintain a stable value; time and aggregated exchange rate for all third-party currencies interacting with the network.

1.1 Time Stability

It is common in everyday speech to hear phrases similar to "the price of a gallon of milk in 1970 was USD1.15, that is about USD3.27 in 2018 dollars". This means that the same value is represented by different amounts over different times. Therefore, if a version of USD1.15 of 1970 dollars, may be electronic, was presented to a grocer to buy milk in 2018, they would still buy one gallon. In other words,

$V \cong P_1(T_1) \cong P_2(T_2)$

Where:

V = Unit value being tracked

P_1 = Price at a time in consideration, T_1

P_2 = Price at a time in consideration, T_2

To capture this concept of time effect on price, a time stamp is quoted with each amount. This time determines when that amount was set and hence a guarantee of equivalence of value when compared to past or future transactions.

As an example, the price could be quoted as OLY150.00000000|1556752842 a short form of *150 OLYs on May 1, 2019 4:20PM* or usually read in quick human friendly form as "150 bar 2019". Even if amount stays the same, say in a rarely used wallet, the actual purchasing power of the amount is maintained when used in the future as it is then compared at the future aggregate rate prices as discussed in the next section.

1.2 Aggregate Rate Stability

The second dimension of the currency stability is the aggregate rate - tracked internally on the OLY network and used by all transaction processing nodes in completion of their roles. Such node roles include transaction checks and approvals as well as fiat currency exchange rate determination. When computed by a Decentralized Exchange (DEX) it is reported to all other DEXs via gossip protocol which also confirm or propose their own value based on blockchain data available. A node adopts the latest confirmed rate for usage in its computations.

The aggregate-rate is computed by taking an arbitrary time duration, say 24 hours and reading all currency exchange occurrences in this duration reported on the blockchain. If the rate is increased by a nominal value N of 1 OLY per day, the contribution of all known currencies is considered. The most widely fluctuating currencies make the lowest contribution and lowest fluctuating currencies the highest contribution. Hence, the aggregate rate R could be represented as:

Taking C_N as each currency's nominal contribution,

$$C_N = \frac{N}{n}$$

n = Number of non OLY currencies exchanged in the OLY network

N = Nominal value of 1 OLY increased in the standard time duration *t* e.g., *t* = 24 hours.

And the change in currency over this same period as:

$$X_c = X_2 - X_1$$

X_1 is the last recorded exchange rate for the currency before the period *t*

X_2 is the last recorded exchange rate for the currency at the end of the same period *t*

Sum of contributions by all the currencies in the network:

$$S_c = \sum_{c=0}^{c} X_c$$

Then, normalized contribution of each currency would be

$$C_n = \begin{cases} Xc > 0, \frac{Sc}{Xc} \\ Xc = 0, Sc \end{cases}$$

Hence the new aggregate rate for the OLY currency becomes:

$$R_2 = R_1 + C_N \sum_{n=0}^{n} C_n$$

R2 = New aggregate rate

R1 = Previous aggregate rate

For example, if the aggregate rate for the OLY at the beginning of the day is OLY1 = 1,000 points and nominal contribution for four currencies would be C_N = 0.25, the following table tracks changes and computations in currency to bring the new aggregated rate to OLY1 = 1019.28571428 points

Currency, n	Change in Currency, X_c	Normalized Contribution, C_{nn}
1	-10	-8
2	70	1.14285714
3	20	4
4	0	80

Conversion to Fiat Currency:
If a user had 10 OLYs at the beginning of the day, at an exchange rate of
OLY10|[start of day] = 10,000 points = USD20 (at exchange rate of OLY1 = USD2)
At the end of the day they have:

OLY10|[end of day] ≅ 10,193 points ≅ USD20.20 (at exchange rate of OLY1 = USD2.02)

Where the 1,019.3 points = USD2.02 is the USD exchange rate being honored for exchange in complete transactions added to the blockchain at the DEXs. The variation of USD0.20 is compared to other currencies on the aggregate rate scale to determine the point variation.

Another user who had the same balance but is exchanging to a currency that widely fluctuated that same day has the following instead:

OLY10|[start of day] = 10,000 points = VEF100 (at exchange rate of OLY1 = VEF10)
At the end of the day they have:

OLY10|[end of day] ≅ 10,193 points ≅ VEF160 (at exchange rate of OLY1 = VEF16)

Where the 1,019.3 points = VEF16 is the new Venezuelan Bolívar exchange rate being honored for exchange at the DEXs.

Difference in Time:
Using the same example, if over a longer time, say the exchange rate at the DEX changes as follows for the USD:
In 2019: OLY10|[in 2019] = 10,000 points = USD20

In 2025: OLY10|[in 2025] = 12,500 points = USD35

If a user kept the same funds (10 OLYs) in their wallet, their new buying power in 2025 is then USD35

If they wish to spend 20 USD outside the OLY network in fiat currency, their new balance becomes:

```
New Balance      = OLY10|[in 2025] - OLY10|[in 2019]
                 = USD35 - USD20
                 = USD15
                 ≅ OLY4|[in 2025]
```

The user balance shown in OLYs keeps the value of their currency compared to other currencies despite time and rate variations and the user can hence trade in any local currency based on market conditions. Therefore the OLY provides a stable store of value for the wallet owner.

2.0 The OLY Network

In a connected group of untrusting and unreliable computing nodes, to enable reliable exchange of value, without double-spend and in a timely way, a solution is proposed to record transactions in a decentralized ledger on a cryptographically secured network. The following are expectations of such a network:

- A node could be a powerful server, cluster of servers or a hand-held mobile device.
- The node could come online or go offline at any time.
- The previous performance of the node matters in the valuation of its stake.
- For security or convenience, a node could have more than one wallet.
- Processing of one block doesn't need to be completed for another to start.
- A wallet owner may require identification or shared key if withdrawing cash in person.
- Provable bad behaviour on the network may lead to punishment of a node.

Messages sent could be for making a payment, establishing or acting on a smart contract, a network action, role-selection action and so on. They are sent by broadcasting from the sending node and spread by gossip-protocol and recurrent subsampling [2] with Byzantine Fault Tolerance (BFT).

2.1 Node

A node can carry out different roles based on settings made by the installer or maintainer of the OLY Network software on it. Each role has different data, memory and processing requirements. The choice is usually made based on the node specs, reliability and strength of network connection as well as desired sources of earning for the owner. A single node may play more than one role. The following are the roles identified so far:

- A **client**; can initiate a payment, receive a payment, submit a script for processing, submit data for storage, report suspected bad behavior (at risk of loss of stake).
- A **Decentralized Exchange** (DEX); can participate in auctions to sell fiat or third-party cryptocurrency for OLYs in response to exchange buy requests and call committees in response to transaction approval requests.
- A **registry**; paid to maintain a full database on matches of handle-to-wallet-public-address which can be queried by any node just like a DNS server.
- A **processor**; fulfils script or smart contract transactions for a fee.
- An **approver**; can validate transactions within the set lifetime and achieve a share of the user fees and a share of stake lost from wrong "bets".
- An **investigator**; is a node with full network databases that responds to report of suspected behavior by sending query messages and collects responses from a "suspect" node (within limit) for a chance to share stake lost from either the suspect node or reporter node depending on the verdict.
- A **judge**; is a node within 30% of highest reputation on the OLY network which uses judgement codes in network decentralized judgement database (updated based on events) to issue verdict on case using collected investigator query submissions and a chance to share in reputation from stake lost by either the suspect node or reporter node. It risks losing its reputation as well if case is overturned on appeal by another judgement committee.

2.2 Sending a Message

A message can be broadcast or sent to an individual node using its public address or handle. Below is an example of a message packet:

<table>
<tr><td>id</td><td>7af900c022ab01</td></tr>
<tr><td>version</td><td>1.2.1</td></tr>
<tr><td>type</td><td>transfer</td></tr>
<tr><td>from</td><td>9bcb3492924a..</td></tr>
<tr><td>[to]</td><td>888ffe7dcc19d..</td></tr>
<tr><td>[payload]</td><td>
<table>
<tr><td>nonce</td><td>70123378234</td></tr>
<tr><td>process</td><td>transfer();</td></tr>
<tr><td>amount</td><td>50.00000000|155675284</td></tr>
<tr><td>fee</td><td>0.40300023|155675284</td></tr>
<tr><td>stake</td><td>0.40300023|155675284,0</td></tr>
<tr><td>nonce</td><td>70123378235</td></tr>
<tr><td>process</td><td>transfer(_amount/2, task_response);
store(task_response);
wait(‘30 DAYS’);
if(checkApproval(_from)) {
transfer(_amount/2, task_response);
store(task_response);
}</td></tr>
<tr><td>amount</td><td>420.00000000|155675284</td></tr>
<tr><td>fee</td><td>0.70000022|155675284</td></tr>
<tr><td>stake</td><td>0.70000022|155675284,0</td></tr>
</table>
</td></tr>
<tr><td>fee</td><td>1.10300045|155675284</td></tr>
<tr><td>[response]</td><td>boolean</td></tr>
<tr><td>sent</td><td>155676221</td></tr>
<tr><td>[expiry]</td><td>155676604</td></tr>
<tr><td>signature</td><td>4920aQdea34Db10aa89f59f2ceB8125aa21..</td></tr>
</table>

The fields in [square brackets] are optional depending on the message type being transmitted. The message is sent as an OLY object. The message payload could range from a simple transfer request to a

complex smart contract scripted in a way to run on a turing-complete Virtual Machine like Ethereum does [3].

Timed Messages:
These are messages with a specific expiry time. It allows nodes to reject expired messages so that they decay from the network and the sender to resend the message if they do not get a response within 2x(expiry duration). Messages with low fees or priority usually set longer time to expire for a higher chance of being processed before expiry. Any new messages with the same transaction ID and origin are ignored for a message that is already included in a batch for processing - even if a committee has not yet completed approvals.

Proof of Stake:
The stake is always represented as

`(amount in OLYs),(reputation points)`

For some situations, a node can lose points on "reputation". The higher the reputation points, the more likely the node is selected as a judge to earn more in fees and the higher the Stake. These points are gained or lost based on activity in the OLY network. Overall stake is computed as below in relation to others who are participating in the decision:

Part	Weight
OLY amount	60%
Reputation	40%

2.3 Wallets

A node can contain more than one wallet. It is advisable to have a wallet with savings in a secure “cold storage” (not connected to any network) and using a working wallet with only needed funds to avoid loss in case of a breach. A structure of local data stored at a wallet could be as follows:

<table>
<tr><td>address</td><td>9Bbc4r9234892a3E42a..</td><td></td></tr>
<tr><td>version</td><td>1.0.3</td><td></td></tr>
<tr><td>balance_available</td><td>45000230.50106052|155675284</td><td><table><tr><td>block_id</td><td>04ae1a62fe09</td></tr><tr><td>transaction</td><td>d74925bf7bf..</td></tr><tr><td>block_id</td><td>fe09c5f51b139</td></tr><tr><td>transaction</td><td>564d925bf7b..</td></tr></table></td></tr>
<tr><td>balance_pending</td><td>670.00000000|1557809030</td><td></td></tr>
<tr><td>reputation_available</td><td>56002</td><td><table><tr><td>block_id</td><td>04ae1a62fe09</td></tr><tr><td>action</td><td>d74925bf7bf.</td></tr><tr><td>block_id</td><td>fe09c5f51b139</td></tr><tr><td>action</td><td>564d925bf7b..</td></tr></table></td></tr>
<tr><td>reputation_pending</td><td>40</td><td></td></tr>
<tr><td>flags</td><td>1</td><td><table><tr><td>flag</td><td>frozen_stake</td></tr><tr><td>value</td><td>70.00000000|1557809030,40</td></tr><tr><td>timestamp</td><td>1557809030</td></tr></table></td></tr>
<tr><td>active_modes</td><td>client,dex</td><td></td></tr>
<tr><td>generated</td><td>155533290</td><td></td></tr>
</table>

The available amounts reference the transactions causing them on the transactions blockchain and the reputation amount references the reputation actions causing them on the reputation blockchain. This comes in handy for validation proof if queried by an `investigator` node. This info is updated when a node is checking confirmation of its transaction on a blockchain which automatically updates the total amounts.

2.4 Decentralized Exchanges

These are powerful nodes with full databases for the transaction blockchain, and exchange rates. The exchange rates database is extracted from the transactions blockchain by filtering for the transaction type **`exchange_sale`** and noting the final exchange rate amount in the same nonce order as saved on the blockchain. Blockchain data is saved in a standard format popularized by bitcoin [4] with a transaction type field.

Any node can become a DEX. This makes the OLY network not vulnerable to single organization control, censorship or hack. The risk of loss in a hack is limited to the DEX wallet which is in direct control of its owner.

To fulfil an exchange request for fiat currency or other third-party cryptocurrency on the OLY network, a purchaser sends a message of type **`exchange_buy`** by broadcasting (without **`to`** address value) for interested DEXs to bid or to a specific DEX address if already known.

In case of bidding, the lowest bid within the buyer's specified range, received before the expiry period of the message is accepted. On receipt of the acceptance message, which includes the claim code (not known to the DEX node), the purchase amount is frozen from the purchaser's wallet (shows as pending amount) and records the same amount as pending on the DEX's wallet. The purchaser can then provide the claim code in person (for a cash exchange) or enter this code in the seller's third-party app say, to make a PayPal transfer, which then removes the frozen OLY funds from the purchaser's wallet and makes the pending funds available in the DEX's wallet in OLYs. Given the risk of the DEX not honoring the transfer if handed the claim code, it is advisable for the purchaser to deal with a reputable business for remote transfers or in person.

2.5 Block Formation and Validation

The DEXs also perform a very important function of initiating committee formation once a new transaction message is sent out after a certain time T_c or number of pending transactions reaches a preset limit P. Any node can broadcast a **`committee_formation`** message that a DEX is expected to answer by examining pending transactions, discarding those already queued while queuing those not yet processed in a batch and assigning then a **`hashtime`** value (generated from hash of the transaction batch and timestamp) and, based on this value as the seed for randomness, send **`request_to_approve`** messages to nodes whose **`approver`** mode is turned on. This increases throughput of the blockchain network as it does not wait for completion of one block to proceed with the next. The DEX also notifies the client that its message has been received but does not await a response. The size of the processed output is determined by many factors:

- The maximum stake the responding approvers in the committee can stake.
- Whether a quorum has been achieved. A quorum is achieved if, accounting for non/improper responses using BFT, transactions in a block are approved by a majority of the quorum participants (51%).

Hence, given time and uncertainty involved, a decision from the committee is reached by the Las Vegas algorithm[5] where a correct result is expected (list of approved transactions) or a notice of failure to reach quorum in time before disbandment. The DEX does not have to wait for the completion of current

block approvals to call another committee. The number of committees that can be called by the DEX is a minimum of one and a maximum set according to the number of pending batches in queue.

On completion of approval or at expiry of allotted time, the committee is disbanded. If approvals were completed in time, the approved transactions are set in an outgoing queue by the DEX and added to the blockchain after confirming that a) they are not already added b) the blockchain is the latest approved (longest chain).
The DEX and committee participants who submitted their responses before committee expiry time receive a share of the fees. If the message forms multiple transactions (such as a script of a smart contract), the fees are also shared with the processor nodes which pick up approved messages added to the blockchain for further processing. All nodes race to do this and only receive their share if the transaction is finally added to the blockchain. The scheme and amounts received by each role will be set by the network software but changeable via soft fork.

2.6 Network Addresses

The registry nodes maintain a full database on matches of handle-to-wallet-public-address which can be queried by any node. The handles are in a human readable format (e.g., `irs.gov.oly`) and the public addresses returned by a query then point to the actual wallet on the network. The owner of the wallet at the handle's public address has an active smart contract with the registries which share the fee to maintain the handle in their database. The fee is shared in a ratio of the registry uptime on the node and how many registries kept the handle during the period.

2.7 Bad Behavior on the OLY Network

Bad behaviour is expected and people will try to look for ways to game the system. Such ways could include but not limited to attempting double-spends, sending invalid transactions or messages, consistently suppressing committee formation requests and many more.

To discourage intentional bad behavior, it will be coded into the system to punish nodes which engage in such activity. At a trigger of a coded software event or reporting by another node, an investigator node activates its role and sends query messages to the suspect node, checks this response against known data and stores results and the suspect node's response for forwarding to the judge nodes. Nodes can become investigators with the following attributes:

1. Have a reputation at least above 50% of the network.
2. Have the latest full database records from the network including the transaction and reputation blockchains as well as currency exchange rates.
3. Have the `investigator` mode activated

To avoid bias, the investigator node can not be the judge node for the same case. When a sufficient case batch B has been collected or time T_i passes, a judgement committee is called by broadcasting the **`create_judgement_committee`** message for nodes with the judge mode activated to respond and

submit their participation. Inclusion is chosen at random. Receiving the signed case batch from the investigator node is the indication that the judge node is on the committee for that case batch.

Judgement is passed by checking the suspect response/non-response in the investigation and issuing a verdict based on coded violations and respective punishments. A violation could be falsifying balance amounts which do not match available amounts based on wallet records, blockchain data and transaction timestamp. The punishment could include loss of a percent of wallet balance or reputation points (up to a limit).

While an investigation is going on, an investigator is allowed to send a **`freeze_stake`** message to the suspect node after result computation for the expected code violation to avoid spending the stake before judgement. This freeze can only last a time limit T_f dependent on blockchain generation rate.

To avoid abuse of the system, the reporter, investigator and judge are each required to stake a position in line with the violation code requirements which stake is lost to the suspect node if the decision does not go as per their action expectation. However, they stand to win a share of the stake lost by the suspect node if decision is approved.

On receiving a judgement message, a node can send an **`appeal_judgement`** message with the case number within a period T_f for a fresh committee to be called by the previous judges at random. Neither the investigator, nor the first judge in the case can participate in the appeal judgement committee. A decision is made on the same facts without consideration of previous judgement. If the decision is reversed, the judge in the first committee loses their stake on the decision.

To become a judge node, the node has to meet the following requirements:

1. Have reputation points in the top 30% of the network.
2. Have the `judge` mode activated
3. Have the full up-to-date network databases

To avoid suspect nodes escaping judgement, a standing message (without expiry) is broadcast to all nodes about the judgement and even if the node in question goes offline, the stake is removed the next time the node is back online.

Based on events that happen on the network, the violation codes database will be updated through a soft fork. A violation code is considered approved if a majority (51%) of the network implements the fork.

3.0 Conclusion

A currency has been proposed that can be globally used and fluidly exchanged with any other currency without need to trust any central authority. By tracking and maintaining value over time, the proposed currency becomes a more reliable store of value than any fiat currency or that backed by an asset or single organization. Furthermore, using a censor-resistant setup, the currency and network are expected to survive even if its creators are no longer involved in its maintenance.

For this kind of currency to be effective and not abused, a self-policing network is proposed over which the currency can be used. This network reward and punishment schemes are expected to be flexible enough to adapt to real-world changes and strong enough to discourage bad behavior and award good behavior. The proposals in this document have made assumptions that the methods used in implementation of the currency and network are already known or shall be defined later based on current industry best-practices.

References

[1] Ilias Louis Hatzis “Basis shuts down. Will regulation kill crypto?”, December 2018
https://dailyfintech.com/2018/12/17/basis-shuts-down-will-regulation-kill-crypto/

[2] Team Rocket, “Snowflake to Avalanche: A Novel Metastable Consensus Protocol Family for Cryptocurrencies”, May 2018
https://ipfs.io/ipfs/QmUy4jh5mGNZvLkjies1RWM4YuvJh5o2FYopNPVYwrRVGV

[3] Vitalik Buterin, “A Next Generation Smart Contract & Decentralized Application Platform”, 2013
https://whitepaperdatabase.com/ethereum-eth-whitepaper/

[4] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008
https://bitcoin.org/bitcoin.pdf

[5] Steven D. Galbraith, “Las Vegas algorithm” In *Mathematics of Public Key Cryptography*. Cambridge University Press. page. 16, 2012