CONTENT

INTRODUCTION

It is fairly evident that upon analysis and review, humanity's progress and evolution of its societies in technology, science, medicine, industry, communication among others are closely tied to ease, efficiency and effectiveness of transferring wealth between individuals, organizations, and nations. Simply consider, any meaningful effort of coordination that forms the basis of our modern division-of-labor based economy cannot take place without a universal form of currency with which parties can transact and pay for products and services rendered in a safe, secure, and effortless environment.

While recent attempts at creating such a universal currency have resulted in our modern financial system, where several major state-issued national currencies are available to all and can be exchanged among themselves (USD, EUR, CHF, GBP, JPY, etc.), the system inherently relies on the production of debt, inflation, and trust in the centralized authorities that manage the monetary policies behind it. By its very nature, such system will be subject to multiple failure points due to its centralized nature, an innate lack of trust as result of its few-rule-the-many governance structure imposing decisions without consulting its constituents, and an ongoing devaluation of its own coin (the USD, for instance) which causes a continuous erosion of wealth for all of its constituents, as experienced in the 2008 global financial meltdown, among other events.

We start by acknowledging that the first ever solution to truly tackle the aforementioned points of concern was the Bitcoin, devised by its creator(s) Satoshi Nakamoto in 2008. Bitcoin is a true peer-to-peer electronic cash system that allows for direct online payments between end users in a trustless way, i.e., without the need of placing trust in the authority of either party or in a 3rd party intermediary or escrow service, such as a government, bank or credit card company, as a means to verify that the buyer has sufficient purchase funds and the irrevocable intent to do so (eliminate malicious chargebacks despite delivery).

To do so, the Bitcoin network relies on a decentralized, publicly-accessible and cryptographically-secured ledger, called the Blockchain, which stores every balance and transaction carried out on the network and its replica is hosted in its entirety by each of its participants; none of whom can alter its history or undermine the integrity of the ledger or its content in any way.

Launched in 2009 and having amassed a very large number of end users, miners, market participants, merchants with derivative products and services and most importantly a high volume of daily transactions, we recognize that Bitcoin (at its current shape and form) has reached an effective point of stagnation and diminishing returns; as it stands, without any radical infrastructural overhaul, subsequent efforts placed into the system will not allow its community to resolve the primary bottlenecks it is currently facing on its path to universal adoption as a viable global currency.

INTRODUCTION

We recognize its 4 main bottlenecks as being:

1. Centralization

2. Network capacity (transactions per second)

3. Sustainability

4. Governance

We strongly believe that any decentralized payment system that wishes to achieve universal adoption and solidify itself as a viable global currency must be built in such a way that its very infrastructure inherently addresses and solves all aforementioned bottlenecks early on.

Economically speaking, the recent exponential price appreciation of Bitcoin from under $0.01 to over $10k as of writing this paper clearly demonstrates an increasing global market demand for the solution that Bitcoin offers, however, we believe that until a comprehensive solution arises that fully answers the challenges faced by the Bitcoin network, a full capitalization of the global multi-trillion-dollar financial industry cannot be reached.

With this philosophy and unmet market demand in mind, we have decided to create ALQO ("A Liquid Object"). ALQO is a community-driven, open source and fully autonomous cryptocurrency that places a strong emphasis on the very building blocks required to create a complete payment system: it is secure, anonymous, trustless, scarce and fungible with a very low-cost transaction profile. It is designed to embody all that Bitcoin as well as more advanced cryptocurrencies have grown to become as well as to capture the economic value that is thus far inhibited by the systemic constraints outlined above.

We will expand on these 4-main adoption and growth barriers and outline how ALQO's unique architecture seeks to resolve them:

CENTRALIZATION

A network is considered centralized when either vast or absolute decision-making power is vested in the hands of few individuals. We believe that in recent years, the Bitcoin network has taken on a path of evolution that is incompatible with its founders' original vision.

The first is the question of mining. Mining is the process by which individuals dedicate computational resources to solving difficult mathematical problems. Upon solving the aforementioned, a new block is found on the blockchain and with it newly pending transactions are confirmed and cleared through. This process is known as Proof of Work (or PoW) as it forces the miner to prove that they have done the necessary work to verify the block, and the first miner to find a new block is compensated for their efforts. This introduces an element of economic competition between miners and prevents the network from being attacked as attacks become too costly and thus, economically unviable. Consider this process as rolling a die in a casino and needing to roll below a certain number, and the first roller who rolls below said number wins the prize, except that the die does not have 6 facets, but rather an extremely large number of them.

Unfortunately, the Bitcoin protocol has introduced a mining algorithm that allows for ASICs (Application-Specific Integrated Circuit) - devices that can create a very large number of hashes per second (or in our example, roll a die much quicker than other rollers). This has created an unfair status quo whereby those who can afford to purchase ASIC devices have a clear upper hand and those who cannot are effectively excluded from participating in the network. Since every bitcoin protocol enhancement needs to be approved with a 95% majority of miners, the top X% of miners who own 95% of the mining power can either accept or veto any suggestion that is brought before the community. This effectively overrules the democratic nature that a decentralized network should be characterized by and creates a disproportionate centralization of decision-making power.

In order to prevent such an occurrence, ALQO utilizes an advanced and fair hashing algorithm known as Quark. Quark is well known for being a lightweight algorithm that can be mined with very modest hardware devices. This ensures that anyone can participate in the ALQO mining, whether they own a smartphone or a super computer. It further utilizes multiple algorithms, namely Blake, Groestl, Blue midnight wish, Jh, SHA-3 and Skein, which makes the development of a dedicated ASIC device specifically designed to produce a large number of hashes per second virtually impossible as it must work with 6 radically different functions. This property is known as ASIC-resistance, and with it, we seek to eliminate any barrier to entry for the average ALQO end user in terms of network governance and promote absolute decentralization and democracy.

SUSTAINABILITY & GOVERNANCE

A network is considered sustainable (or self-sustaining) if it can grow and maintain itself organically, autonomously and independently of 3rd parties, while being resilient against a wide range of negative external factors. Governance is the set of laws that dictate the function of the network.

This brings the second question of development. As market conditions and needs evolve, a digital currency system must adapt with them in order to survive and thrive. To this end virtually every major digital currency project (Bitcoin, Ethereum, Litecoin, Dash, Ripple) has at least a core team of individuals who maintain and develop the network. Since humans are imperfect, developers tend to shape the direction of the project after their own vision - this has created very heated and unresolved debates within the Bitcoin team and has caused both stagnation and splits (knows as forks) to other derivative and competing projects. Further, developers' cooperation can be bought by a malicious entity, they can be intimidated, or simply lose interest and leave. Any disappearance, broad disagreement and/or sabotage by a core member can have critical consequences for a system that has the potential to serve billions of end users and trillions of transactions.

Since any of these factors detract from the network's ability to sustain itself and exclude the community from participating in governance-related decisions, ALQO has introduced the following:

- **Ad-Hoc Dev Funding**. In recent years, it has become a standard in the cryptocurrency space to create a dedicated dev fund. The dev fund is a special address (similar to a bank account) that is autonomously funded by the network (e.g. Dash, PIVX, etc.). There are typically three events on those networks that trigger a financial compensation in the form of new coins: a miner is rewarded for finding a block, a masternode is rewarded for its services and a staker is rewarded for putting up collateral for securing the network (this process is known as Proof of Stake or PoS, we will expand on the concepts of PoS and masternodes later on). Whenever any such reward is triggered, the network automatically sends a portion of that reward to the fund. While this ensures that development can continue to grow at all times without relying on donations, it is also flawed as the same dev team will always possess the private keys to the dev fund and will be able to use it regardless whether they work in or against the community's and the project's best interests.

  In order for ALQO to ensure that the team behind it always works in the community's interests, the dev fund has been deprecated and instead any funding will only be authorized upon approval of a proposal submitted to the community.

SUSTAINABILITY & GOVERNANCE

The community can then decide whether to grant the team funds on an ad-hoc basis. Further, the team will employ a mining pool and later a staking pool that the community can mine or stake through it, which pays a certain fee to the developers. As it is entirely voluntary, the community can choose to opt in or out of the pools depending on the performance and intentions of the dev team. This is a checks and balances mechanism put in place to ensure the long-term health of the project.

- **Carbon Voting.** While it is imperative that future development funding is guaranteed, it is equally important that the community as a whole has a clear say in how it is being used. To ensure that this is the case, the fund is cryptographically sealed and can only be used if a certain proposal outlining the use of funds and the amount needed is brought before the community for a vote. Some projects (such as Dash and PIVX) have implemented a voting system whereby suggestions are brought masternode operators, however given that masternodes require a collateral of coins in order to operate (1,000 coins in the case of Dash, 10,000 coins in the cases of PIVX and ALQO), such a system has the innate flaw of barring anyone without the necessary funds from voting ("you can only vote if you have a million dollars"). One can argue that such a system only provides with partial decentralization at best.

  ALQO has decided to opt for a system called Carbon Voting, whereby every 1 ALQO is given 1 vote. Utilizing the ALQO protocol, each vote will be conducted via an off-chain channel and sent securely with end-to-end encryption to one of the live masternodes for verification. Voting will be done via our unique in-house wallet called Liberio, compatible with any device, from mobiles to desktops and servers. Each user will see their weighted voting power, represented by their balance rounded down to the nearest integer value (a balance of 8.34 ALQO will grant 8 votes). Upon deadline, the top voted option will be chosen and funds will either be released or not.

  We feel that this is a superior model that eliminates the financial barrier for participation in the voting system and opens the door to anyone who wishes to cast a vote. Much like the public government election system, we strive to achieve a 100% participation rate and believe this system can accomplish that goal.

  These two mechanisms ensure that development can continue indefinitely and are in-line with the community's desires as it can economically depose or elect any development team that best agrees with its views, in a faster and more efficient way than existing solutions.

SCALABILITY AND NETWORK

The bitcoin protocol mandates a maximum block size of 1MB found exactly every 10 minutes. Since only a limited number of transactions can fit into a block and are only produced at this interval, Bitcoin's capacity is rated at ~7 transactions per second. This is a major limitation that cannot sustain an increasing user base and transaction volume, and one that has spawned numerous contentious and hard forks (Bitcoin Cash has forked from Bitcoin to create an 8MB blockchain). If a global cryptocurrency is to take form, it must accommodate any transaction volume.

Furthermore, the blockchain, being a public ledger containing a record of all balances and historical transactions, will only tend to significantly increase in size over time. The larger the blockchain grows, the more expensive it is to maintain, as it requires more powerful machines with faster and more reliable connectivity and larger storage requirements. This inevitably leads to a higher barrier to entry and restrict participation to fewer and fewer individuals and organizations who are willing and able to operate full nodes.

To ensure the long-term health and future-proof its network, ALQO has decided to introduce the following:

- **Larger and Faster Blocks.** ALQO relies on a block size of 4MB and a block time of 60 seconds. This effectively allows ALQO to handle a transaction volume 40x greater than Bitcoin’s.
- **Flexible Blocksize.** Roughly 1 year into ALQO´s life cycle, the network will switch from a consensus algorithm of mining-driven Proof of Work to staking-driven Proof of Stake. Upon this second stage, the protocol will switch to a dynamic blocksize that will adjust in size to any increase in transaction volume. If the network detects that more and more transactions are stuck in the unconfirmed queue (known as the mempool) it will dynamically increase the size of the subsequent blocks to handle the increase in transaction volume. This is the equivalent of a mining difficulty algorithm applied to block sizes.
- **Masternodes.** The ALQO network constitutes a 2-tier architecture, where the first tier is the protocol level, mining and staking and the blockchain itself. The second layer is its masternode array, being a large network of high availability dedicated servers operated by users. These users provide enhanced services to the network (such as faster transactions, anonymous transactions, voting validation and others) as well as contain a full copy of the blockchain.

SCALABILITY AND NETWORK

Masternodes require a collateral of 10,000 ALQO to operate in order to ensure that launching malicious nodes is too costly for a potential attacker, and nodes are paid in ALQO for their services. Since these are dedicated and powerful servers, they can better handle the increasing load of a larger chain than an average desktop machine or smartphone.

- **MVCs on Liberio.** A Minimum Viable Chain (MVC) is the shortest possible blockchain that can still handle incoming transactions, with sufficient history to be compatible with future blocks. The wallet that runs such an MVC is known as a thin client as it doesn't maintain a full copy of the blockchain. This has the utility of being able to provide with chain continuity as well as make each device a full node without sacrificing a significant amount of storage and computational resources. Combined with the Quark algorithm, each device will also be able to mine and create new blocks, allowing for full participation of all end users. We have determined that the ideal size is the 20 most recent blocks, which is sufficient in length and takes up no more than 80MB of local storage, and can dynamically change if needed. In comparison, popular social media and messenger apps often take up hundreds of MBs to entire GBs on a user's mobile device, so we do not expect this to cause any storage bottlenecks. This will be handled by our in-house wallet, Liberio.

We would like to note that this paper deals with the long term challenges many cryptocurrency projects face on their path to global adoption, the solutions ALQO offers and an overview of its features and attributes from both a commercial and technical standpoints. This paper however does not deal with the upcoming Palacio framework, as it is still kept in confidence until its final design can be made public around end of 2017. The Palacio framework will be a major key differentiator and add some beautiful complexity that will facilitate and ensure ALQO's commercial adoption and success in years to come. Given its nature, Palacio will require a separate paper that will follow this one.

Now that we have covered the difficulties we have recognized being faced by Bitcoin and the solutions that the ALQO protocol offers to preempt them, we would like to expand upon the innate properties that will ensure ALQO's far higher likelihood of success at adoption as a global payment system that can address growing market demands.

SCALABILITY AND NETWORK

The architecture and operation of the ALQO network can be summarized as follows:

- New transactions are broadcast to all nodes.
- Each node collects new transactions into a block.
- Each node works on finding a difficult proof-of-work solution to recover its block.
- When a node finds a proof-of-work solution, it broadcasts the block to all other nodes.
- Nodes accept the block only if all transactions in it are valid and not already spent. This critical steps ensures that a double-spend attack cannot occur.

Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash. Given that cryptographic hashing functions are computationally infeasible to reverse, a hash match confirms that the new block refers to the exact current state of the entire blockchain.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work solution is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach a sufficiently large number of nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realize it missed one.

PROOF OF WORK

During its first year of operation, the ALQO network will rely on a Proof of Work consensus algorithm. As mentioned previously, Proof of Work is the process by which miners, individuals who dedicate their computational resources to solve difficult mathematical challenges, prove that they have done the necessary work required by the network to validate blocks, which are data containers for a large list of new transactions. It is referred to as a consensus algorithm because a majority of overall mining processing power is needed in order to enforce any new protocol update proposal.

To motivate miners to participate in the mining process and cover their costs, the first miner to find a new block is compensated for their efforts. This introduces an element of economic competition between miners and prevents the network from being attacked as attacks become too costly and thus, economically unviable. As ALQO uses the ASIC-resistant Quark Algorithm [3] previously mentioned, any party can participate in the mining process regardless of their device type and hardware capabilities, which prevents the concentration and centralization of decision-making power in the hands of the few and enables a true democratic process.

ALQO's block time is set at 60 seconds, meaning the network aims for blocks to be created every 60 seconds. This aim is facilitated by what is known as a difficulty retargeting algorithm, which increases or decreases the difficulty of finding a block in proportion to the total hashing rate (processing power) being contributed to the network. If, for example, the hashing rate suddenly doubles, the difficulty will increase to ensure that blocks are not recovered every 30 seconds and vice versa. This is of extreme importance as we have witnessed the danger of a frozen blockchain with Bitcoin, whose retargeting algorithm adjusts every 2016 blocks, or every 14 days at 10 minutes per blocks. This means that if mining power suddenly drops (due to lowered mining profitability for instance), it will take the network two weeks to lower the difficulty accordingly, during which time the blockchain could grind to a halt. To prevent this from happening, ALQO's algorithm adjusts the difficulty level every block, or every 60 seconds.

PROOF OF WORK

As we have seen, the risks of high inflation and its devaluing implications on national currencies, ALQO attempts to reverse this trend by offering an ever-decreasing emission rate, which ensures it remains a disinflationary currency in nature. This was designed to preserve and protect ALQO's innate coin value. Please refer to the table below to see ALQO's coin emission schedule per stage (or Epoch); the distribution of miners rewards vs. masternode operator rewards are listed next to each stag.

Reward Allocation or PoW Block Rewards (starting on November 10th, 2017):

Block 2 – 86400	200 ALQO	Masternodes 20% / Miners 80%
Block 86401 – 151200	150 ALQO	Masternodes 25% / Miners 75%
Block 151201 – 302400	125 ALQO	Masternodes 30% / Miners 70%
Block 302401 – 345600	100 ALQO	Masternodes 35% / Miners 65%
Block 345601 – 388800	75 ALQO	Masternodes 40% / Miners 60%
Block 388801 - 475200	50 ALQO	Masternodes 40% / Miners 60%

On Block 1 (Genesis Block), 100,001 ALQO were created in order to set up 10 masternodes and support and stabilize the ALQO network (at 10,000 ALQO per node collateral). These are scheduled to be burned later in 2018 and will not be used in any other way.

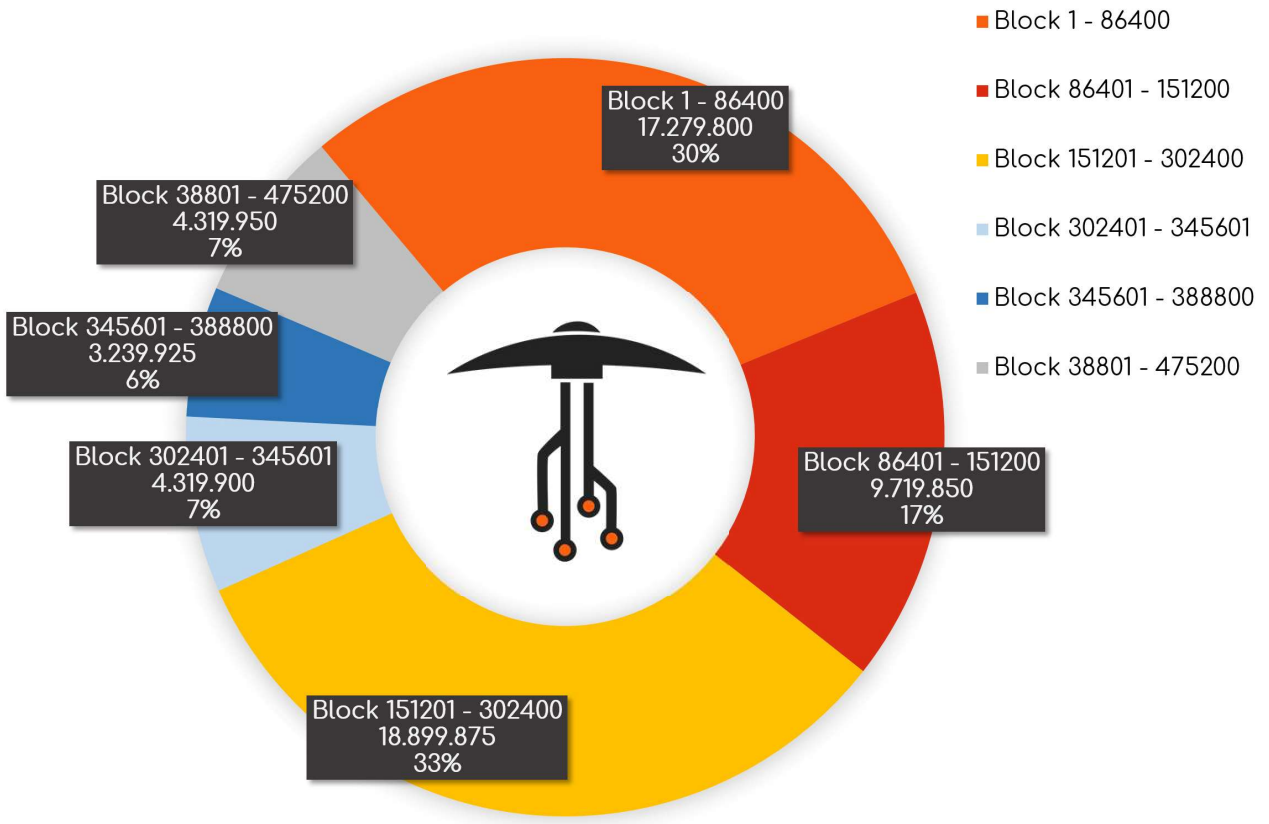
Lastly, block maturity is defined as the minimum age of a block, in terms of blocks rather than standard time units, before it is safely considered to be part of the chain. The logic behind this is that since each block validates all of its predecessors, the more blocks are added on top of a block, the more valid and safe for consideration it becomes. The standard block maturity for Bitcoin is 101 blocks. While ALQO's block maturity is set at 111 blocks, given ALQO's far quicker block time at 1 minute, a block can be considered mature in under 2 hours, giving the network a very solid foundation for security references.

PROOF OF WORK

```
int64_t _nTargetTimespan = CountBlocks * Params().TargetSpacing();

if (nActualTimespan < _nTargetTimespan / 3)
                nActualTimespan = _nTargetTimespan / 3;
if (nActualTimespan > _nTargetTimespan * 3)
                nActualTimespan = _nTargetTimespan * 3;

// Retarget
bnNew *= nActualTimespan;
bnNew /= _nTargetTimespan;
```



PROOF OF STAKE

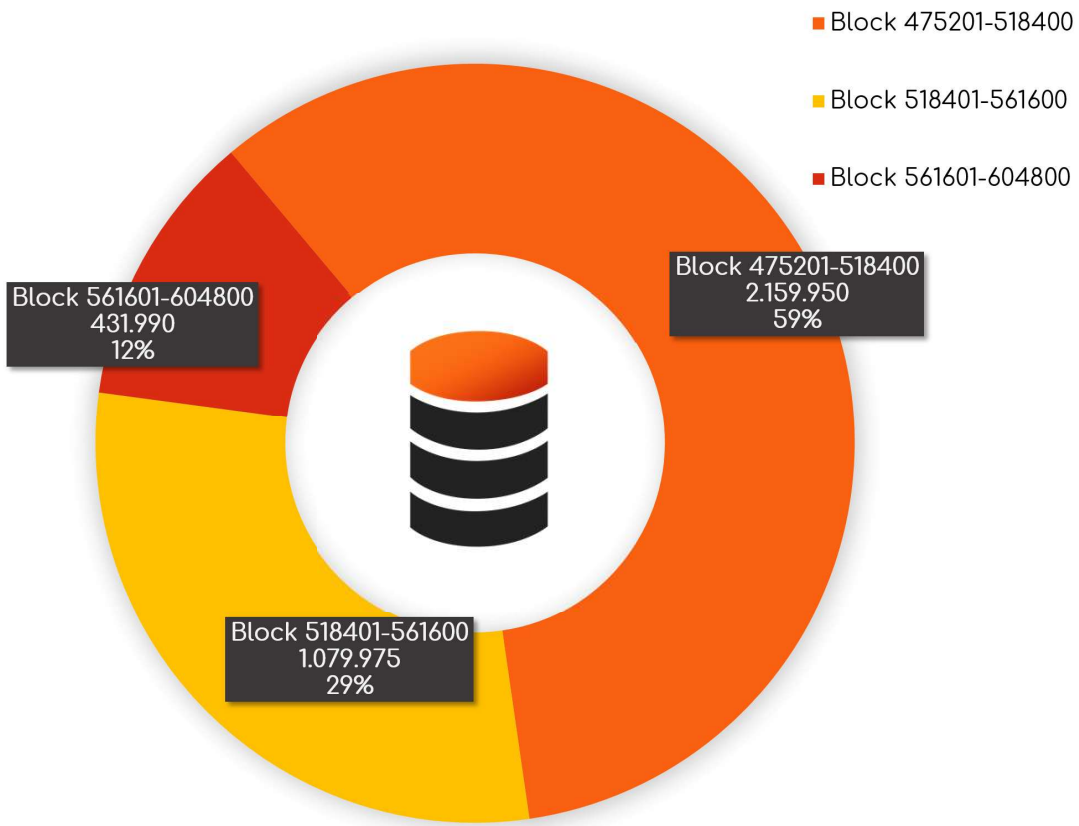
The Proof of Stake (PoS) consensus algorithm is very similar in nature to the Proof of Work algorithm outlined above, rather than devoting computational resources (i.e. work), participants dedicate their ALQO coins as collateral, the more coins one possesses the more likely they are to secure a block. This has two added benefits: first, it is cheaper and more cost effective than PoW as it does not waste nearly as much electricity and real-world resources as PoW does. Second, since the likelihood to find and validate a block is proportional to the stake one owns in the network, the more incentivized they are to ensure its ongoing health and are far less likely to perform malicious attacks against their own wealth. Therefore, it becomes extremely expensive for an external attacker to perform attacks on the network.

ALQO will switch entirely from PoW to PoS in late 2018, effective block #475,201. The following represents the coin emission schedule per block for every stage of operation:

Block 475201 - 518400	50 ALQO
Block 518401 - 561600	25 ALQO
Block 561601 - 604800	10 ALQO
Block 604801 - infinite	5 ALQO

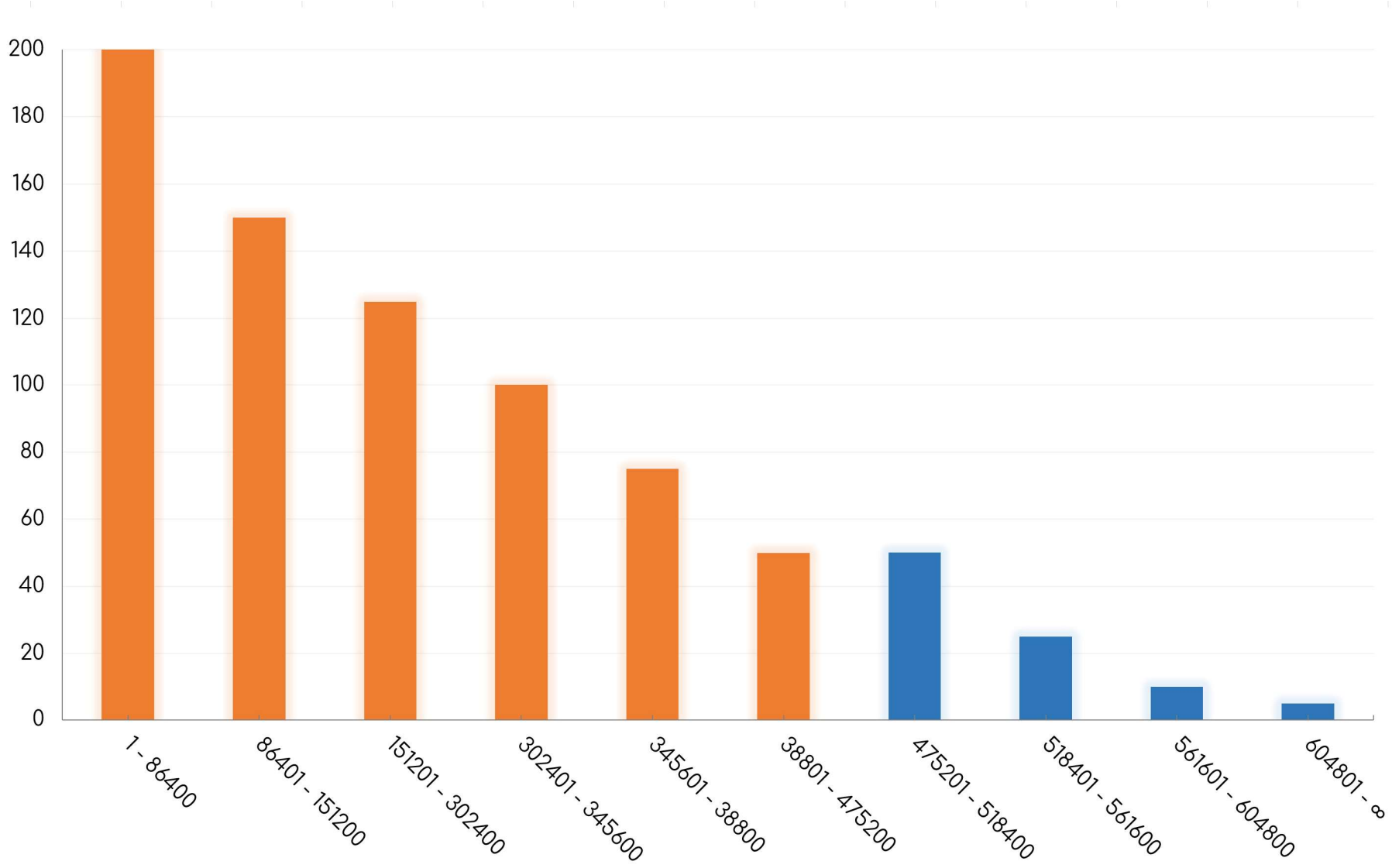
PROOF OF STAKE

Traditionally, staking requires that a user has their device running and continuously connected to the network at all times, otherwise they are skipped by the network for reward distribution. With the groundbreaking Liberio wallet, cold staking is now a reality - users automatically stake and gain rewards for their balances without having to take any actions whatsoever. Think of it as generating passive interest on your bank balance while helping maintain its infrastructure at the same time while incurring no costs at all.



Main Influence : Ethereum [5]

BLOCK REWARDS



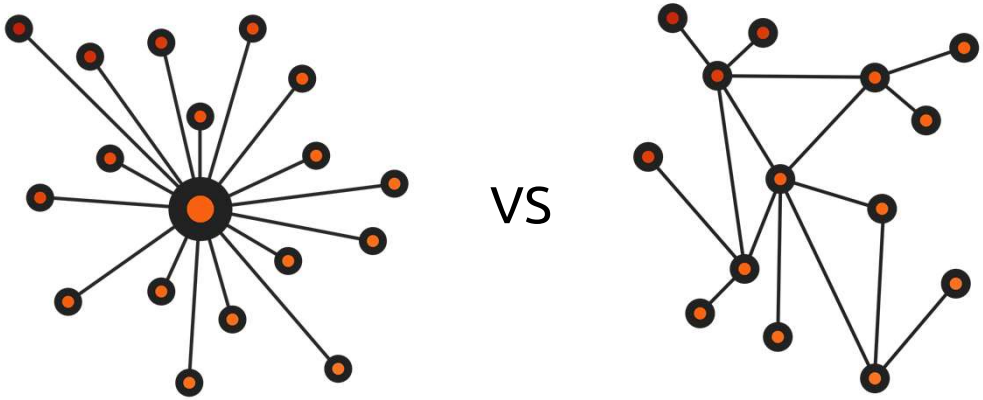
MASTERNODES

As we have mentioned the term masternodes several times in this document and have provided several hints as to its nature, we would like to now offer a more meaningful overview. Masternode are dedicated hardware nodes that sit on worldwide servers connected to the ALQO network, each maintaining an exact replica of the entire ALQO blockchain and providing enhanced services to the network.

As masternodes are essentially continuously-connected nodes that are hosted on dedicated servers, their function is to provide a host of services and guarantee their availability to customers of the ALQO network. To increase the degree of distribution and thus network security, each masternode is required to have its own IP address, to ensure they are hosted on as many servers as possible and guarantee network resilience and redundancy.

Within the context of the ALQO network and as each standard node and thin client (Liberio) is securely connected to one or more masternodes, these services are primarily ALQO HyperSend, ALQO Shroud (will be expanded upon later in later sections) and Carbon Voting, and others to join the ALQO masternode framework.

Masternodes must lock in a large number of coins (exactly 10,000 ALQO as collateral; this is a flexible collateral as it can be withdrawn and moved at any point in time, however, upon doing so, the masternode immediately goes offline) as well as incur hosting costs, they are compensated for their costs and efforts in terms of both a portion of all block rewards and fees for the advanced services outlined above.



Centralized Decentralized

THE LIBRA EFFECT

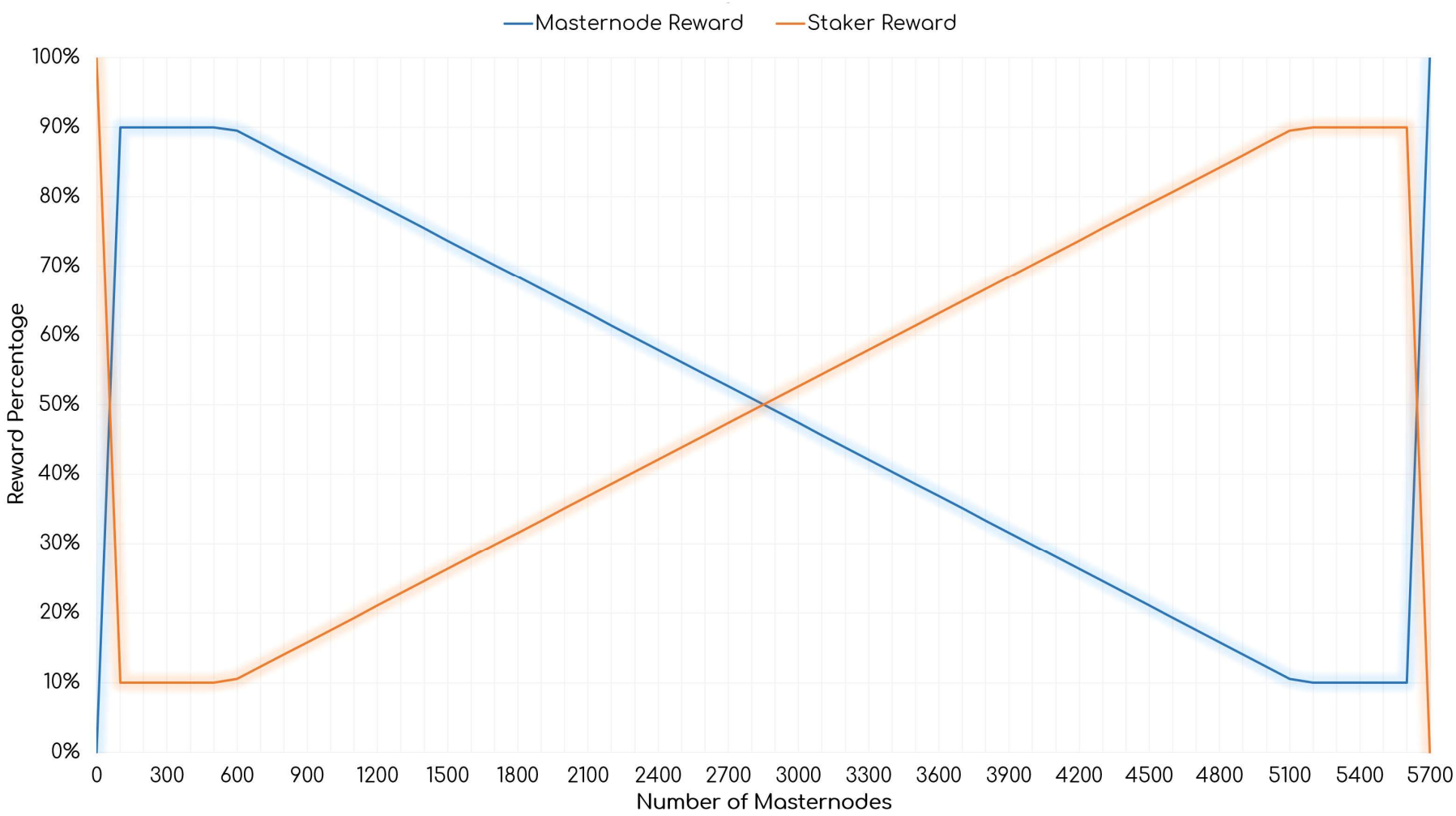
While the exact distribution between the rewards paid out to both miners and masternode operators during each stage of the PoW era is hard-set, ALQO utilizes a more dynamic approach to determine the reward distribution between stakers and masternode operators during the PoS era. The underlying logic is that ALQO strives to strike an ideal balance between the number of masternodes operating on the network and the number of coins being staked at any given time. With too few maternodes, advanced services such as anonymity, voting and instant transaction become less available and difficult to obtain, and with too few coins available for staking, the network as a whole becomes less secure. It also reduces overall market liquidity which will be necessary to power the very large scale commercial applications planned further down the road.

In order to compensate for either of these two scenarios and reach a 50%/50% masternode-locked vs. freely available staking coins equilibrium, we have introduced the Libra Effect. The Libra Effect dynamically increases the block reward paid out to masternodes, the fewer masternodes are available on the network, and reduces it so that more are available, in a precise supplementary relationship. This also occurs to freely available coins for staking.

For example, if 35% of the available supply of coins is locked within masternodes, the total masternode population will receive 65% of the total block rewards and 35% will go to stakers. This inverse relationship between rewards and availability will incentivize more masternodes operators to come forward and lock in their coins, which in turn increases the availability of advanced services provided by and to the network. Unlike similar implementations (see: see saw mechanism; PIVX) that employ sharp 5% step sizes, ALQO employs a smooth variation curve that is rounded to the 8 nearest decimal places. This means that if 12.74% of the total PIVX supply is locked in, the masternode block reward will adjust to 75%. With ALQO, it will adjust to 87.26%, which is the precise supplementary value. This is performed to ensure absolute fairness towards the community and zero room for error.

THE LIBRA EFFECT

Please see the attached Libra yield curve plot to obtain a better visual sense of how it works:



THE LIBRA EFFECT

The following is the code that governs that Libra Effect on a protocol level:

```
int64_t nMoneySupply = chainActive.Tip() - > nMoneySupply;
if (nMasternodeCount < 1) {
  nMasternodeCount = mnodeman.stable_size();
}
int64_t mNodeCoins = nMasternodeCount * 10000 * COIN;
if (mNodeCoins == 0) {
  ret = 0;
} else {
  double lockedCoinValue = mNodeCoins / nMoneySupply;
  double masternodeMultiplier = 1 - lockedCoinValue;

  if (masternodeMultiplier < .1) {
              masternodeMultiplier = .1;
  } else if (masternodeMultiplier > .9) {
              masternodeMultiplier = .9;
  }

  LogPrintf("[LIBRA] Masternode: %d\n", masternodeMultiplier * 100);
  LogPrintf("[LIBRA] Staker: %d\n", (1 - masternodeMultiplier) * 100);

  ret = blockValue * masternodeMultiplier;
}
```

ALQO SHROUD

A very fundamental aspect of the business world is that any business must have intimate knowledge which its competitors do not possess to gain a competitive edge. A core component of that has to do with the commercial relationships it has with its customers, suppliers, vendors, service providers, partners, shareholders, and others. The cost and difficulty of doing business would impossibly increase if competition would gain visibility into a company's financial sheet, its global assets and bank account balances, what each customer is charged and what each service provider and employee is paid.

It goes without saying that in order to ensure the commercial survival and create a solid foundation for a global economy, a robust privacy solution must be put in place, and preferably one that would conceal the transactions made and balances held by each party, as well as their true identities. As long as participants are hesitant to partake in the system, true economic prosperity cannot take place and productivity would greatly diminish as a result.

Recognizing the aforementioned, the ALQO project has introduced the ALQO Shroud service, being a service that is offered by masternodes on the ALQO network. While each user has the option of transacting with transparency, the ALQO Shroud service allows them to significantly obfuscate their activity and cover their tracks by mixing their transactional input with those of other users. This option will be easily and intuitively available to each user within the Liberio wallet framework.

In the future, the ALQO team will also incorporate stealth addresses, which are special addresses that do not list their balances and transactions between two such addresses which are fully opaque on the blockchain.

ALQO HYPERSEND

In addition to above given example, the global financial system relies on the ability to transfer large sums of capital quickly and securely. As every billable project in the world relies on the transfer of funds in order to initiate, the faster funds can be moved and secured, the more productive our global economy becomes and the faster it grows. It is for this very reason that premium transfer services within the global remittance industry are valued in the tens of billions of dollars annually.

To secure ALQO's aspiration of becoming a globally adopted form of currency, ALQO incorporates a service known as ALQO HyperSend. HyperSend allows for a very low-cost transfer of funds in split seconds. It functions by utilizing ALQO's array of masternodes: whenever any entity on the network wishes to transfer funds rapidly via HyperSend, the funds are sent via a list of available masternodes that in turn immediately lock up the sender's funds and are sent to the receiver's address. The payee's funds are guaranteed by the decentralized masternode layer, which makes up for the time gap between the transaction and the next verified block (which could take up to 60 seconds).

The ALQO team will utilize this facet of the ALQO network as part of its commercial applications, ranging from in-store point of sale to major international purchases.

ALQO HOSTING FRAMEWORK

Recognizing the importance of having a broad and established array of masternodes from day 1, the ALQO team has created the ALQO Hosting Framework, being the list of services and practices put in place to create a simple, easy to use, effortless, and cost effective masternode hosting solution with a turnaround time of several minutes. These include a simple hosting service, enhanced security features, a support portal, round the clock monitoring, and easy to follow tutorials. These can be accessed at https://hosting.alqo.org.

While it has proved very successful and has already serviced over 100 satisfied customers, we believe that in order to eliminate any points of failure, the next version of the ALQO Hosting Framework must offer a more decentralized, easier to use, and trustless solution given the mission-criticality of having masternodes with a guaranteed uptime.

THE LIBERIO FRAMEWORK

Having engaged in previous cryptocurrency-related projects, such as coinfolium.com (a web-based portfolio monitoring tool) and the Masternode App (an app which allows you to monitor the status of your masternodes across various coins and incoming payments), and as such have a better appreciation of the needs of the average financially-minded consumer, we would like to put our experience and expertise to use and develop the next generation of cryptocurrency wallet clients.

With this in mind, we have designed the Liberio Framework. Liberio currently acts as a universal semi-thin wallet client designed to run on any device, ranging from dedicated heavy-duty servers down to mobile devices.

Liberio transcends the definition of a simple SPV client and is an entire framework upon which more user-friendly services will be built and offered over time. We can list the array of features and services it currently offers seamless access to as the following:

- **ALQO HyperSend & ALQO Shroud.** Using the Liberio client, users will be able to specify whether their next transaction will be done in a high-speed, high-anonymity fashion utilizing the HyperSend and Shroud services.
- **Infinite Scalability.** Liberio is designed to be a partial SPV, meaning that it'll keep an MVC (minimum viable chain; mentioned previously) version of the chain. This MVC will consist of only the 20 more recent blocks and prune the remainder. Coupled with ALQO's Quark algorithm that's designed for low-end devices, Liberio will allow every single such client to participate in the block and transaction validation process and in turn fortify the decentralization of the network. As Liberio is designed to be compatible with any device, from dedicated services to mobile devices with minimal hardware and network requirements, it'll form the basis of having hundreds of thousands if not million of effective nodes on the network, resolving the scalability issue before it ever arises.
- **Masternode connectivity.** Liberio will allow users to connect and configure their masternodes remotely while maintaining local control of their private keys.
- **ALQO Hosting Framework.** Liberio will grant users seamless access to the ALQO Hosting Framework, launch and monitor their masternodes from the comfort of their wallet. All a user will have to do is connect and/or launch a node with a single click, and ALQO's back-end infrastructure will take care of the rest in a seamless and painless way.

THE LIBERIO FRAMEWORK

- **Offline (Cold) Staking.** Currently, users are required to run a fully synced node and have a mature balance for staking in order to be considered as candidates for block validation by the network and therefore be eligible for staking reward. This places an undue burden on users who do not have the knowledge, inclination or ability to maintain such connectivity. With these users excluded from the network, its overall security level diminishes and rewards are concentrated within the few who can participate. In order to prevent this and create a win-win situation with both the network benefiting from their staking resources as well as users enjoying staking rewards, Liberio will offer a cold staking service, meaning that users who own an ALQO balance will be able to stake even when they're offline, similar to how a bank account works. We believe this will allow for a more decentralized, democratic and fair process overall, while increasing stakeholders value over time.

- **Wallet-To-Wallet Chat.** Using the ALQO cryptographic framework, Liberio will enable secured and end-to-end encrypted p2p chats between any two members on the network in order to increase coordination and economic cooperation, allow for pre-planning and reduce the occurrence of imperfect transactions.

- **Built-In Palacio Framework.** The Palacio Framework is a game changer in the cryptocurrency space with very broad commercial implications, and its design has not yet been finalized and therefore cannot be made public as of yet. As mentioned, more information about Palacio will follow towards the end of 2017.

  We hope that at this point the reader has been able to get a sense of the power of Liberio and its long term mass adoption implications, with further enhancement to be announcement down the road.

  Liberio will be written on top of our custom ALQO Network protocol which utilizes end-to-end encryption and will be compatible not only for desktops, but also for Android, iOS and Windows Mobile.

THE LIBERIO FRAMEWORK

```
public static byte[] Encrypt(string data, string publickey = null) {
  CspParameters cspParams = new CspParameters {
    ProviderType = 1
  };
  RSACryptoServiceProvider rsaProvider = new RSACryptoServiceProvider(cspParams);

  if (publickey == null)
    rsaProvider.ImportCspBlob(Convert.FromBase64String(Settings.HOST_PUBKEY));
  else rsaProvider.ImportCspBlob(Convert.FromBase64String(publickey));

  byte[] plainBytes = Encoding.UTF8.GetBytes(data);
  byte[] encryptedBytes = rsaProvider.Encrypt(plainBytes, false);
  return encryptedBytes;
}

public static string Decrypt(byte[] encryptedBytes) {
  CspParameters cspParams = new CspParameters {
    ProviderType = 1
  };
  RSACryptoServiceProvider rsaProvider = new RSACryptoServiceProvider(cspParams);
  rsaProvider.ImportCspBlob(Convert.FromBase64String(Encryption.PRIVATEKEY));
  byte[] plainBytes = rsaProvider.Decrypt(encryptedBytes, false);
  string plainText = Encoding.UTF8.GetString(plainBytes, 0, plainBytes.Length);
  return plainText;
}
```

ATOMIC SWAPS

We regard the explosive growth of the cryptocurrency space to be indicative of a growing market-wide demand for decentralized and economical solutions across a multitude of industries. As a result, over the past few years, cryptocurrency projects have emerged tending to specific niches, industries and utility sets. There range from the agriculture, construction, health, banking, law, manufacturing, energy, communication industries as others. Rather than hold the belief that there will be one single coin to rule them all, we view the current landscape as rapidly and divergently evolving. Whether coins and tokens will end up form relationship of synergy or competition, one thing is certain and that is that there is a place for all of them in the market.

With this in mind, instead of restricting users' choice of currency, we have decided to accommodate their broad desire by introducing the Atomic Swaps mechanism. An Atomic Swap is the process by which user A who owns coin X can exchange their coin with user B owning coin Y both having separate blockchains, in a fast, secure and trustless way. Once an exchange rate is agreed upon by both parties, a cross-chain swap takes place. It's the decentralized world's equivalent of over-the-counter ("OTC") trades as they don't require a 3rd party. Furthermore, atomic swaps have the added benefit of utilizing a very specific type of smart contract, being hash and time lock. This means that user A sends their funds to a certain address which then locks up the funds. If user B then fails to come through by a certain agreed upon time, the funds are unlocked, the transaction is reversed by the blockchain and user A gets their funds back.

Atomic Swaps will be implemented once the ALQO network reaches the Proof-Of-Stake phase.

In order to perform an on-chain atomic swap between two cryptocurrencies, there are several prerequisites to factor in. Both chains must support:

- **Branched transaction scripts**
- **The same hashing algorithm**
- **Signature checks for transaction scripts**

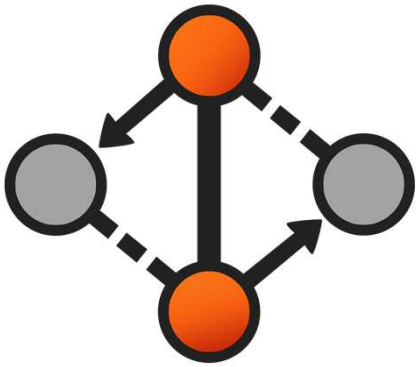
ATOMIC SWAPS

On-Chain atomic swaps are mostly useful in cases where users want to perform an exchange that is characterized by a larger trade that is not subject to a particular time constraint. Since the process involves on-chain transactions, the speed of the process is bound by the mining or staking of blocks on both chains, and the slower of the two at that. This can take roughly an hour when transacting with the Bitcoin blockchain. Additionally, users must pay transaction fees for both the swap and the redemption transaction on each chain, which can have a non-trivial cost with Bitcoin.

Furthermore, since these swaps are on-chain, there are some privacy implications that users should be aware of. The swap transaction on each chain include the same hashed value, meaning that anyone who surveils on the corresponding blockchains can link the coins on one side of the swap to the coins on the other side.

Further down the road, ALQO will implement solutions for off-chain transactions that will eliminate the concerns outlined above.

We hope that by reading this paper the reader has gained a more thorough understanding of the economic growth potential that the near future holds, the solutions currently put in place in order to drive said growth, the inadequacy of their current shape and form as we see them, as well as our approach to providing a complete solution in the form of the secured p2p global payment ecosystem that ALQO protocol and network seek to embody.



REFERENCES

[1] Bitcoin Whitepaper: https://bitcoin.org/bitcoin.pdf

[2] Dash Whitepaper: https://github.com/dashpay/dash/wiki/Whitepaper

[3] Quark vs. Bitcoin: http://www.quarkcoins.com/bitcoin-vs-quarkcoin.html

[4] PIVX Whitepaper: https://pivx.org/what-is-pivx/white-papers/

[5] Ethereum Proof of Stake FAQ: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ

[6] Litecoin Github: https://github.com/litecoin-project