# The Helios protocol - a next generation scalable decentralized blockchain protocol, smart contract, and decentralized application platform

Tommy Mckinnon

(Dated: 21 September 2019)

V 0.2 - Visit http://heliosprotocol.io for the newest version. Note: This whitepaper was originally written in 2018 during the first year of development. Some information may be outdated, and there are a lot of new features that are not included in this document. Please visit our Discord server, blog, or social media platforms for more up to date information. (links at the end of this document)

## I. INTRODUCTION

In 2009, the year Bitcoin was created, a revolution was started. In a world where the financial system, and our money, was controlled by a select few, we had a glimpse of a future where the power would be given back to the masses. Bitcoin was the first decentralized global cryptocurrency that allowed anyone to set up a wallet, get some Bitcoin, and use it to purchase anything anywhere on earth in minutes.

Unlike banks, there are no fees for sending money overseas, no monthly account fees, no fees for having to many withdrawals etc... The only fee that exists is a very small transaction fee, which in 2011 had an average of less than $0.01 USD. The decentralized nature of Bitcoin also means that there is no central authority that can tell you what you are allowed to spend your money on. This results in true freedom to do what you want with your money. It is easy to see why Bitcoin is potentially a much better alternative to the existing banking system for at least 99% of the people on earth.

However, as Bitcoin grew in popularity, it became clear that there were many scaling problems. By the beginning of 2018, transaction fees had increased to an average of over $20.00 USD per transaction.[1] The increased transaction volume also caused transactions to take much longer to be processed. The average confirmation time grew to over 100 minutes[2]. The number of Bitcoin miners also increased in popularity dramatically, which resulted in a massive waste of resources and energy. Bitcoin mining was consuming over 30 Twh per year.[3] It was clear that a new solution was required that could scale far into the future and solve all of these problems.

Today, there are many attempted approaches to solving these scaling problems such as decreasing the interval between blocks, increasing the block size, handling transactions off-chain, using a directed acyclic graph (DAG) architecture, blockchain network sharding etc... However most of these solutions can only handle on the order of 1000's of transactions per second. This is a huge improvement over bitcoin, however, it is still an order of magnitude less than the 24,000 transactions per second that the Visa network can currently process.[4] Furthermore, considering that Visa is only one of many credit card companies, the actual transaction volume of all credit cards is likely in the high 10's of thousands of transactions per second. Therefore, it is unlikely that any of the solutions under current development can even handle the credit card transaction volume of today, let alone scaling into the future. The Helios protocol aims to solve this problem by handling orders of magnitude greater transaction volume, and being infinitely scalable into the future.

Another blockchain innovation was created in 2015 by Vitalik Buterin. It is known as Ethereum, and it is a decentralized blockchain protocol capable of executing turing complete programming languages. This allows developers to create smart contracts and decentralized applications (dApps) stored on the blockchain. dApps are capable of providing decentralization of power not only to currency, but anything we can think of. The most exciting applications are those that replace systems that are especially susceptible to the centralization of power such as: voting, social media, fintech, government, healthcare, legal arbitration, human identification, supply chain, education etc... If Bitcoin was a revolution for the monetary system, Ethereum is a revolution for almost every centralized system in a modern society. However, like Bitcoin, Ethereum is facing the same scaling issues.

## II. THE HELIOS PROTOCOL

The Helios protocol has been developed from the ground up to solve the previously mentioned problems and achieve the following goals:

1. Maintain all of the positive qualities of modern blockchain implementations such as trustlessness, immutability, and decentralization.

2. Be capable of executing the same Turing complete programming languages as Ethereum. This will allow Ethereum dApps to be migrated to the Helios dApp platform without modification which will dramatically accelerate the adoption.

3. Be capable of scaling to handle the transaction volume of the future while maintaining low transaction latency.

4. Have low transaction fees and maintain them into the future.

5. Have a consensus mechanism that doesn't require proof of work (PoW) and uses orders of magnitude less energy while being just as secure. The consensus mechanism also needs to provide the same level of reliability and security as PoW and be highly resistant to centralization of power.

6. Allow the users to choose the order of their own transactions rather than the block miners, and allow them to add a transaction to the blockchain exactly when they wish.

Before getting into the detailed explanation of the Helios protocol, we need to go over some definitions to explain parts of the protocol and language that we will use throughout this paper.

## A. Definitions

### 1. Wallet address (sometimes just called wallet)

A section of the public key portion of the encryption key pair. The wallet address contains a balance of coins and can have transactions to send or receive coins from any other wallet address. In this paper, the wallet address, or wallet, basically means an account on the blockchain that can hold funds.

### 2. Transaction

A transaction is an object that transfers funds from one wallet to another or contains smart contract data. The transaction is also signed by the sender.

### 3. Completed Transaction

A transaction that has a copy on the sender blockchain and receiver blockchain. Both blocks must be completed and have reached consensus on the network.

### 4. Incomplete Transaction

A transaction that only exists within either the sender block or receiver block but not both.

### 5. Block

A block contains a list of transactions. The block is signed by the wallet address of the blockchain to which the block belongs. The block also contains the hash of the previous block in the blockchain.

### 6. Queue Block

A block that is currently being filled up with transactions. It only exists on a local node and has not yet been propagated to the network. It can be changed into a completed block at any time as long as it contains at least 1 transaction.

### 7. Completed Block

A block that contains at least 1 transaction and has all of the required contents of a block. It must be signed by the owning wallet address. As soon as a block has been completed, it must be transmitted to the network to be added to the blockchain database and propagated across the nodes. A completed block that has achieved consensus is never allowed to be modified after being completed.

### 8. Blockchain

A series of blocks that are all linked to each other by the previous hash. Each wallet address has its own blockchain.

### 9. Blockchain database

A complete database of all blockchains from all wallet addresses on the network.

### 10. Fullnode

A computer connected to the network that has a full copy of all of the blockchains, is responsive and actively participating in activities that keep the network healthy. Each node must be associated with at least 1 wallet address that has at least 1 transaction and currently contains a positive balance of coins.

### 11. Masternode

Same as a fullnode except it must contain a specified amount of coins in its wallet address. The exact amount required for a masternode will be decided through testing on the testnet. These nodes are able to gain additional rewards.

### 12. Micronode

A computer connected to the network that can have any fraction of all the blockchains. It will typically only contain the blockchain for its own wallet address. This is for someone who uses the cryptocurrency and simply wants to be able to send and receive transactions but doesn't want to participate in the health of the network. A micronode must be associated with at least 1 wallet address, however, the address doesn't need to have a transaction

### 13. Sender

The wallet address that is sending a transaction to another wallet address.

### 14. Receiver

The wallet address that is receiving a transaction from another wallet address.

## B. Protocol Overview

With traditional blockchain protocols there is a single main blockchain that must hold all of the transactions. However, each block can only hold so many transactions, and there must be a statistically set time interval between blocks. This results in a bottleneck where the blockchain is only being able to process a certain number of transactions per second.

We decided to solve this problem by taking a serialized process and replace it with a parallel process. Instead of having a single blockchain, the Helios protocol has a blockchain for every single wallet address on the network. This is like taking a single lane highway and replacing it with a highway that has a lane for every single car on the road. This completely eliminates the bottleneck caused by requiring all transactions to go onto the same blockchain.

Every wallet on the network owns its own personal blockchain. Each blockchain is only allowed to contain transactions to or from the owner wallet. Each wallet is allowed to add new blocks with new transaction to their own blockchain whenever they wish. When a transaction takes place between two wallets, the transaction is only added to a block on the blockchain of the sender and receiver, see Figs. 1, 2.

This idea is inspired by the way a fully cash-based monetary system works. In that case, each individual has some balance of cash at any given time. If a transaction takes place, the only 2 parties involved are the buyer and seller. They simply exchange cash, and the balance held by each party changes accordingly. As we all know, this system allows transactions to happen all across the planet in parallel because each transaction is entirely independent of the others.

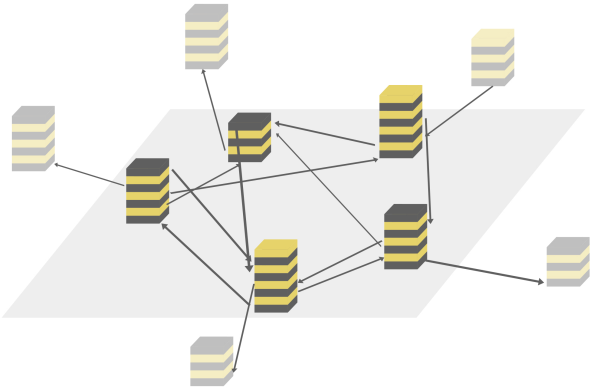

FIG. 1. A group of blockchains on the Helios network, each corresponding to a different wallet address, sending transactions to each other (arrows). When a transaction takes place, it is added to the blockchains of the sender and receiver. All full nodes on the network replicate the entire blockchain database.

Similarly, transactions on the Helios protocol only need to involve the sender and receiver, and transactions between other parties are entirely independent. Just like with the cash-based system, this allows transactions between different parties to occur simultaneously. This also causes the transaction throughput of the protocol to grow linearly with the number of users and means the Helios protocol can scale indefinitely into the future.

## C. Key protocol Properties

- Every wallet address has its own blockchain. Each blockchain contains a series of blocks. Each block contains one or more transactions.
- When a transaction is placed, it is added to a new block at the top of the sender and receiver blockchains.
- A wallet's blockchain can only contain transactions to or from that wallet.

## D. Transaction and Block Creation Process

The block and transaction creation process for 3 wallets, A, B, C are shown schematically in Fig. 2.

1. The sender creates a signed transaction containing all required information.
2. The sender adds the transaction to their local Queue Block. They can add as many transactions

as they wish to their own queueblock. They can also add incoming transactions.

3. The sender then completes the block at any time they choose by signing it and broadcasting it to the network.
4. Eventually the new block is propagated across the network and the receiver sees the transaction.
5. The receiver adds the transaction to their queue block, which can also be completed at any time
6. The transaction is complete when it is present on the sender and receiver blockchains, and the blocks at each end have achieved consensus.

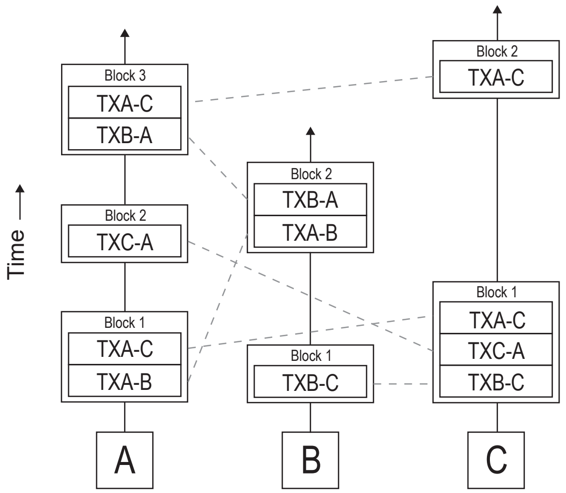

FIG. 2. Showing the blockchains of 3 wallets: A, B, C, within the blockchain database and in chronological order. The wallets are sending transactions to one another by adding transaction containing blocks to their own blockchains. A transaction takes place when it appears on the sender and receiver blockchain. Many transactions can be added per block to reduce the network communication overhead and increases transaction rate.

Unlike a traditional blockchain, since each blockchain belongs to a single wallet, we require that the blocks are signed just like the transactions. This adds a level of security that is not seen in normal PoW systems. Namely, if a transaction or block is changed, the signature will allow everyone to immediately know who is responsible. This will be explained in greater detail later in the paper.

Additionally, instead of having one transaction per block, we are allowing many transactions per block. This dramatically increases the transaction rate for an individual wallet that the protocol can handle because the wallet no longer needs to broadcast each transaction individually and wait for consensus between each one. Instead, the wallet can bundle all transactions into a normal block and broadcast them all at once.

### E. Order of transactions

Each transaction has 2 times associated with it: 1) the time it was sent, and 2) the time it was received. These two times are defined by the block timestamp in the sender and receiver blocks, respectively. The time that the transaction completes is whichever of the two timestamps is latest. If a transaction is in the sender block but not the receiver block, then it is considered incomplete. In order to prevent double spending, the value of any incomplete transactions is subtracted from the spendable funds in a wallet.

In this case it is safe to rely on the timestamp given by the sender and receiver because the time they choose only effects their end of the transaction and nothing else. For example, if wallet A sends a transaction to wallet B, wallet A includes a timestamp for when it was sent. As far as wallet A is concerned, the transaction has already been sent. It doesn't care what time wallet B chooses to add the transaction to their block to receive the funds. So if wallet B chooses a timestamp that is off by any amount of time, it makes no difference to wallet A or anyone else on the network. There are also causally imposed strict bounds on the allowed timestamp of a given block. For example: a block must have a timestamp that is greater than the previous block and less than now. Another example: a block on a receiver blockchain must have a timestamp that is greater than the timestamp on the sender block. Furthermore, just like with Ethereum and Bitcoin, the order of transactions is much more important than the time that they took place. With the Helios protocol, the order of transactions is immutable.

### F. Consensus Mechanism

Proof of stake (PoS) consensus mechanisms are very new and are still an active area of research.[5,6] However, consensus mechanisms already exist in many different areas of nature, from the communication of bees in bee colonies, to the collective behavior of electron spins in a magnetic material. Many of these systems have withstood the test of time and have been continuously improved upon through evolution. Additionally, many of these systems have been studied extensively for hundreds of years and are very well understood. Thus, our approach to developing a consensus mechanism for the blockchain is to combine knowledge from all of the previously done PoS research, with the solutions provided by consensus mechanisms in nature.

We studied many systems in nature and narrowed our focus onto a single one that has many analogies to the blockchain, making it possible to implement the solutions effectively. The natural consensus mechanism system we decided upon is the magnetization dynamics of magnetic dipoles arranged in a lattice within a magnetic material. Under certain conditions, the magnetic dipoles are capable of communicating with each other through the quan-

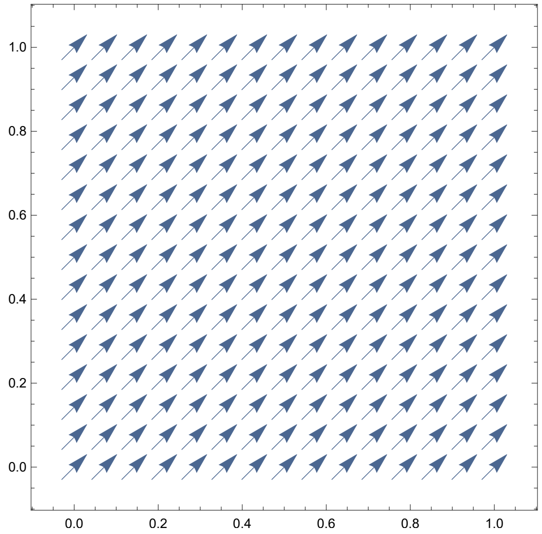

FIG. 3. An array of magnetic dipoles that make up the magnetization of a magnetic material. All of the dipoles are oriented parallel to each other due to the exchange interaction. Each magnetic dipole is analogous to a node in the Helios network. The parallel directions of the magnetic dipoles are analogous to nodes being in agreement and having consensus.

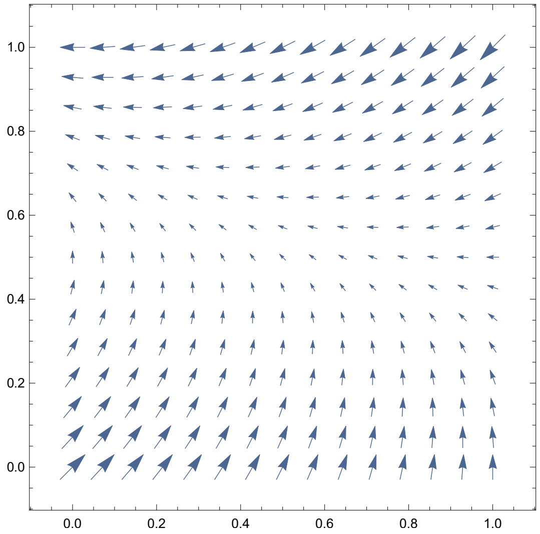

FIG. 4. An array of magnetic dipoles that make up the magnetization of a magnetic material. In this case, the dipoles in the bottom left and top right are pointing in opposite directions causing a magnetic domain wall to form between them. The magnetic domain wall is analogous to a disagreement between nodes on the blockchain.

tum mechanical exchange interaction and achieve consensus about which direction to point. This natural consensus mechanism is an extremely reliable choice for the blockchain because, just like in physics, it is guaranteed to cause the system to reach consensus.

### 1. Theory

A magnetic material is composed of a number of magnetic dipoles arranged in a lattice that can point in any direction in the 2D plane, as shown by arrows in Figs. 3, 4, 5. The magnetic dipoles interact with each other through the quantum mechanical exchange interaction energy, which is given by:[7]

$$E = -\sum_{i,j} J_{i,j} \boldsymbol{M}_i \cdot \boldsymbol{M}_j, \tag{1}$$

where $J_{i,j}$ is the coupling constant between dipoles $i$ and $j$, which drops off exponentially with distance, $\boldsymbol{M}_i$ and $\boldsymbol{M}_j$ are the normalized magnetizations of dipole $i$ and $j$, respectively. The total energy of the magnetic material is found by summing over $i$ and $j$. The system will choose directions of all dipoles that result in a minima of energy. In the case of positive $J_{i,j}$, the minima will occur when all dipoles are parallel.

Now we can imagine forcing the magnetic dipoles at the bottom left and top right corners of the array to point in opposite directions as shown in Fig. 4. This will cause a magnetic domain wall to appear between the bottom left and top right dipoles. If we then let go of the magnetic dipoles at the corners, and let the system reach equilibrium, the interaction energy between the magnetic dipoles will cause them all to align again. This process is shown in from left to right in Fig. 5.

The important thing to understand here, is if any magnetic dipoles are pointing in different directions, the interactions between them will cause them to realign themselves to point in the same direction.

For our analogy with the blockchain, each magnetic dipole (a single arrow) corresponds to a node on the Helios network, and the direction of magnetization corresponds to the state of some blockchain in their blockchain database. If all of the magnetic dipoles are aligned parallel, as they are in Fig. 3, then this corresponds to all of the nodes having the same state for that particular blockchain, are in agreement with one another, and have achieved consensus. If any of the magnetic dipoles are pointing in a different direction, then the corresponding nodes have a disagreement in their blockchain database. If this is the case, the consensus mechanism will realign the magnetic dipoles, which corresponds to the nodes coming to an agreement on a particular blockchain database in order to achieve consensus.

We will now derive the math for a given node to calculate which state has consensus. Lets call this node Node A. We do this by creating a virtual exchange interaction between Node A, and every other node that it is connected to given by:

$$E = -\sum_{j} J_j \boldsymbol{S}_A \cdot \boldsymbol{S}_j, \tag{2}$$

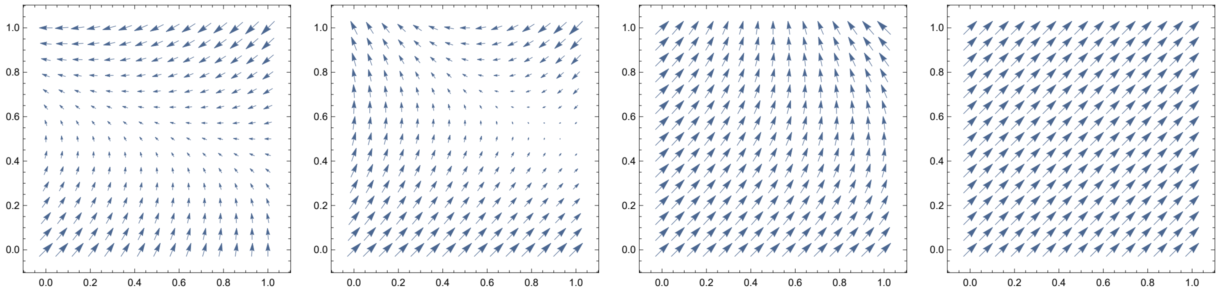

FIG. 5. From left to right the exchange interaction causes the magnetic dipoles to align parallel with each other. This is analogous to the nodes on the network reaching consensus.

where now $J_j$ is the PoS weight of node $j$, $\boldsymbol{S}_A$ is the state of a blockchain on Node A $i$, and $\boldsymbol{S}_j$ is the state of a blockchain on node $j$. $j$ is summed over all nodes that Node A is connected to. If state $\boldsymbol{S}_A$ and state $\boldsymbol{S}_j$ are in agreement, $\boldsymbol{S}_A \cdot \boldsymbol{S}_j = 1$, if they are in disagreement, then $\boldsymbol{S}_A \cdot \boldsymbol{S}_j = -1$. Node A will then choose a state $\boldsymbol{S}_A$ that minimizes $E$, and if that state is different from its previous state, it will convert to the new state. This state that minimized $E$ is the consensus state.

This calculation may seem simple at first glance, however there is a lot of complexity hidden in the dynamics of the system. All nodes are constantly re-calculating Eq 6, which in turn will cause some nodes to decide to change their state. These nodes changing state will then cause other connected nodes to change state. This results in a runaway effect that runs through the entire network until all nodes are in the same state. This is exactly the same process of all the dipoles becoming aligned in Fig. 5. Just like with a magnetic material, this process will always cause the system to reach consensus.

Another reason why this model is very well suited to the blockchain is as follows: The coupling strength between dipoles drops off exponentially with distance. Thus, the dipoles are coupled most strongly to the nearest dipoles around them. So even though most dipoles are too far away and never communicate with each other, the system is still able to achieve a global consensus.

Similarly, in a decentralized network, the combination of network latency and the speed of light means that nodes who are far away from each other will take a long time to communicate. Therefore, if each node had to communicate with all other nodes on the network every time they wanted to reach consensus, the process would be unbelievably slow, and have a large network communication overhead. Thus, for a fast and efficient decentralized network, nodes need to communicate with other nodes within relatively close proximity. Hence, the dipole consensus mechanism shares the same communication properties as a fast and effecient decentralized network allowing it to provide fast and reliable results when applied to the blockchain.

Another point that needs to be made clear is that the dipoles, or nodes, will always align themselves in the direction of the majority stake of the nodes to which they are coupled. Therefore, if a single node or minority of nodes try to alter a blockchain, the network will evolve to take the state of the majority. The result is that the modified blockchain will be ignored. This provides a mechanism for immutability of the blockchain database. The only case where an attacker could modify a blockchain is if they held more than 50% of the stake, just like with all other PoS implementations. However, the Helios protocol has a slashing mechanism to eliminate economic incentive for the modification of a blockchain. See the slashing conditions section later in the paper for more details.

## G. Staking Reward System

The staking reward system is designed to incentivize nodes that actively participate in keeping the network healthy.

Rewards will reward node uptime, network participation, and node performance. All operational nodes with nonzero HLS balance will receive these rewards. Every node will be connected to a group of peer nodes. During this time, the node will keep a log of the uptime and responsiveness of all connected nodes. From this log data, the node will be able to determine the fraction of the time that any peer node was online and working to maintain a healthy network during the time period. Now, we will walk through the process of reaching consensus on the reward amount: Imagine we are node A, and we would like to calculate the amount of reward we get over a time period t.

1. Node A first asks the 10 connected nodes with the highest stake to send a signed message containing their estimation of the fraction of time that node A was online and contributing to network health during time $t$.

2. Node A then calculates the stake-weighted average of all responses. We will call this AVG_UPTIME.

3. Node A calculates the reward amount using Eq. 3.

4. Node A then adds a reward transaction in it's blockchain, along with all 10 signed messages it received from the peer nodes as proof that it calculated the correct reward.
5. Node A broadcasts the new block to the network.
6. The other nodes on the network verify that the reward amount is correct using the 10 signed messages included in the reward transaction. If the calculation is correct, consensus will be achieved.

Node A calculates the amount of reward using

$$A_{R2} = P2 \times \text{AVG\_UPTIME} \times t, \tag{3}$$

where $P2$ is a constant reward multiplier that will be fixed through testing, and $t$ is the time period that the reward is for. The sum of stake of all nodes that responded in part 1 must reach a given threshold to be valid. This will eliminate the possibility of someone creating many different wallets with small stake to increase the number of votes. The scaling factor J will depend on the kind of node. Masternodes will have a larger J than fullnodes, and will receive more rewards.

### H. Slashing Conditions

With any cryptocurrency protocol, users will have economic incentive to break the protocol rules. Slashing is the process of taking money away from a wallet that breaks the rules. The goal of having slashing conditions is to make it expensive to break the rules to reduce or eliminate the economic incentive for breaking the rules. We also have to consider the possibility that a broken rule may be caused by mistake or a bug in the code of software that interacts with the protocol. In most cases, the node that breaks a rule can simply be added to a blacklist and ignored for a given period of time. However, there is one offense that cannot be tolerated and must result in the slashing of a wallet. That offense is the alteration of a transaction or block that had previously reached consensus. The Helios protocol requires that every wallet address has to sign all of the blocks in their blockchain. When a block reaches consensus, then many other nodes on the network will also have a copy of the block. If a wallet decides to alter a block or any transactions within the block, the other nodes will see that there are 2 different blocks with the same block number for the same wallet. The fact that both blocks are signed by the owner wallet offers immediate proof of who tried to change a transaction or block. In this case, the wallet will be slashed for an amount equal to the absolute value of the altered transactions, see Figs. 6, 7. Or in the case of a change in order of the transactions, the wallet will be slashed by 10% of the absolute value of the largest transaction within the block, see Fig. 8.

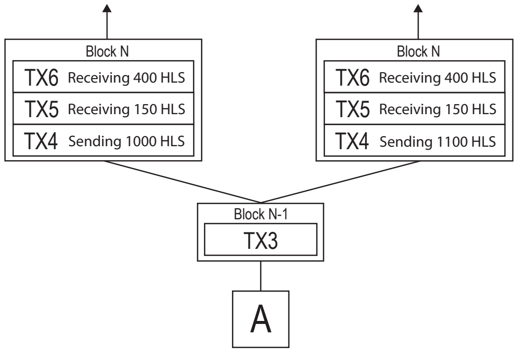

FIG. 6. An example where wallet A produces 2 blocks containing a modified transaction. Wallet A will be slashed by an amount equal to the absolute difference in the two transactions, which is 100 HLS.

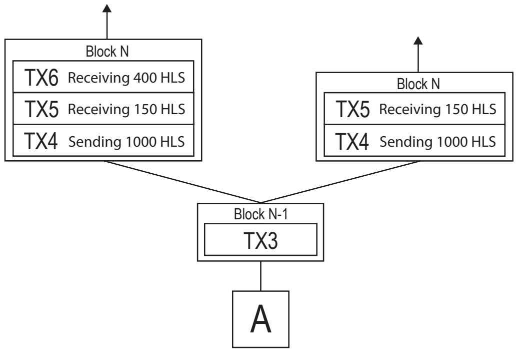

FIG. 7. An example where wallet A produces 2 blocks where a transaction has been added or removed. Wallet A will be slashed by an amount equal to the absolute value of the transaction that is missing in one of the blocks. In this case, wallet A will be slashed by 400 HLS.

There is one case where a wallet will have to create multiple different blocks with the same block number, and must not be slashed. If a wallet creates an invalid block and tries to broadcast it to the network. Consensus will fail, and the wallet will have to fix the block and re-broadcast it resulting in 2 different blocks with the same block number. This will be allowed without slashing under the following 2 conditions: 1) the block must be at the top of the blockchain, and 2) the new block must contain all of the same transactions as the previous block with the same block number, except for any invalid ones.

## III. BENEFITS OF THE HELIOS PROTOCOL

### A. High Speed and Scalable

Every wallet address has its own independent blockchain. Transactions only need to be added to the blockchains of the two parties involved in the transaction,

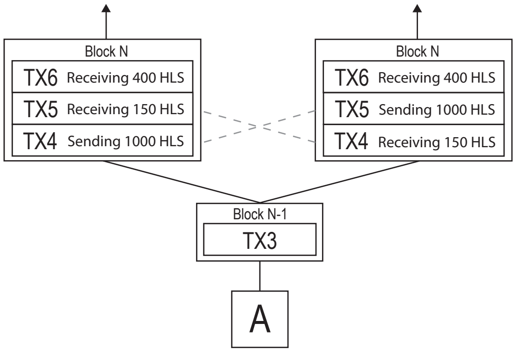

FIG. 8. An example where wallet A produces 2 blocks where the order of transactions has been changed. We can identify that it was an order change by looking at the tx hashes. Wallet A will be slashed by an amount equal to the absolute value of 10% of the largest transaction in the block. In this case, wallet A will be slashed by 100 HLS.

ie. the sender and receiver. This allows transactions between different users to occur independently and simultaneously resulting in a transaction throughput many orders of magnitude greater than current blockchains. If we assume the only bottleneck to transaction throughput is the blockchain architecture, it grows linearly with the number of wallets on the network. Thus, the blockchain architecture of the Helios protocol is infinitely scalable. That said, once we have eliminate the blockchain architecture bottleneck, that limits other blockchain projects, there will inevitably be other bottlenecks that present themselves at higher transaction throughputs. One such bottleneck is the sheer computational power of the nodes. Modern processors can only process so many transactions per second. The exact number depends on the programming language, processor model, and efficiency, but is expected to be in the 1000 to 10,000 tx/sec range with current affordable hardware. However, as computer hardware technology improves, and processors become faster, so will the throughput of our blockchain. We have essentially tied the scaling of the Helios Protocol, with the scaling of computer hardware. If you consider how massive the computer hardware market is, and how much demand there is for faster hardware, it is clear to see that things will reliably scale year after year.

Furthermore, the parallel blockchain architecture is extremely well suited for sharding. This will allow the transaction throughput to approximately scale by the number of shards on the network. If we have just 10 shards, we have no increased the transaction throughput, with current hardware, to between 10,000 and 100,000 tx/sec.

As a brief exercise, let's consider the scenario at some time in the future a few years from now, where computer hardware is no longer the bottleneck. Let us assume and the Helios protocol has 30 million wallets, which is approximately the number of Ethereum wallets as of now, and each blockchain could process 15 tx/sec, which is the approximate speed of a single Ethereum blockchain. The transaction throughput of the Helios protocol for this scenario can be calculated by

$$TX_{\text{throughput}} = 30000000/2 \times 15, \tag{4}$$

where the first term is the number of wallet addresses divided by 2 because there are 2 wallets involved in each transaction, and the second term is the transaction rate of each blockchain. **This results in a Helios protocol transaction throughput of 225 million tx/sec. We can compare this to Bitcoin's 4 tx/sec or Ethereum's 15 tx/sec in which case the Helios protocol is on the order of 50 to 20 million times higher throughput, respectively.**

Secondly, wallets are allowed to add new transactions and blocks to their own blockchain at any time they choose. This allows transactions to take place on demand. There is no longer the need to wait for the next block to be mined like a traditional blockchain. So not only is the transaction throughput increased, the transaction latency is decreased as well.

### B. Low Transaction Fees

Transaction fees are necessary to help fund rewards for full nodes who are required to maintain the Helios network. Without transaction fees, rewards would have to come entirely from newly minted coins which would lead to an increased rate of inflation and devalue the coin. Transaction fees are also necessary to stop a penny-spend attack where users send a very large number of small transactions to overload the network. That said, **the Helios protocol will have many orders of magnitude lower fees as compared to traditional blockchain projects for the following reasons**:

High transaction fees on the traditional blockchain occur because there is a limited number of transactions that can fit into each block. The transactions with highest fees are added before others which causes users to pay higher fees to make sure their transactions are added to a block as quickly as possible. This results in competition amongst users which drives transaction fees upwards. The high transaction throughput of the Helios protocol, and its ability to process transactions concurrently, completely eliminates this competition.

The Helios consensus mechanism, which lacks PoW, allows nodes to run on inexpensive, energy efficient hardware (see the energy efficiency section below). This dramatically reduces the upfront and continuing costs to run a node. So, the rewards required for nodes to generate the same income as they would with other PoW coins are also dramatically lower. This allows Helios to remain lucrative in comparison to PoW coins even much smaller rewards for nodes. The cost savings from having to pay less rewards to nodes is transferred directly to the users of the network via lower transaction fees.

### C. Smart contracts and dApp platform

The Helios platform will be capable of executing smart contracts and dApps programmed in Solidity just like the Ethereum platform. This will allow for accelerated adoption of the Helios platform by existing developers. It will also allow for seamless migration of Ethereum based dApps to the Helios platform. Furthermore, we are allocating a large percentage of HLS tokens to a dApp incubator fund to support new visionary projects built on the Helios platform.

### D. Security and Immutability

The Helios consensus mechanism, which is based on both PoS and the very well understood physics of magnetism, is able to provide security an immutability to the same degree as PoW. It also provides additional measures not seen in PoW that increase security further.

Each wallet address has its own blockchain, and the wallet must sign all blocks on the chain. This makes it impossible for anyone to edit the contents of another wallet's blockchain. Therefore, if a block or transaction is changed after reaching consensus, there is immediate proof that it was changed by the owner wallet. This allows the network to immediately identify the offending wallet and slash their funds. The amount of funds that are slashed are chosen to completely eliminate the economic incentive to break the protocol rules.

See the consensus mechanism section earlier in the paper for more details.

### E. Energy Efficiency

The new Helios consensus mechanism doesn't require mining which dramatically reduces the energy consumption. We can walk through a quick calculation to see just how much more efficient we expect it to be as compared to Bitcoin:

To compare apples to apples, lets assume the Helios network has the same number of fullnodes as Bitcoin, which is approximately 10,000.[8] We will assume each Helios fullnode is running an AMD Ryzen 1700, which is much more than enough processing power, and is not even the most efficient option. In this case, each node will draw around 100 - 130W from the wall.[9] In this case, the annual energy usage of the Helios protocol will be between 0.011 and 0.0087 TWh:

$$100\text{W} \times 10,000\text{Nodes} \times 8760\text{hours} = 0.0087\text{TWh} \quad (5)$$

$$130\text{W} \times 10,000\text{Nodes} \times 8760\text{hours} = 0.011\text{TWh} \quad (6)$$

The annual energy usage of Bitcoin is currently estimated to be 66 TWh.[3] Therefore, the Helios protocol will use approximately **6000 and 9000 times less energy than the Bitcoin network with the same number of fullnodes.**

### F. Truly Decentralized and Democratic

Blockchain technology was originally developed with a guiding principle of decentralization. Decentralization is in the blood of any true blockchain project. The Helios protocol is determined to preserve this principle and provide a truly decentralized blockchain protocol.

The Helios protocol achieves a high level of decentralization by allowing any individual to participate and vote in the consensus process no matter how small their stake may be. Unlike delegated PoS, our consensus mechanism doesn't require electing representatives or delegates to vote on your behalf.

PoW naturally results in some degree of centralization of power because it is more profitable to have a very large mining facility as compared to a single mining rig that an average person might have. Furthermore, the miners have the power to choose which transactions get added to each block. The Helios consensus mechanism eliminates both of these sources of the potential centralization of power.

### G. Transaction Order

With traditional blockchains, the order of transactions is determined by the miner who mines the block. This means the sender and receiver don't know when their transaction will actually take place and just need to wait patiently until it gets added to the blockchain. As mentioned earlier, this can lead to centralization of power, and gas wars. With the Helios blockchain, every wallet is allowed to add a block with transactions to their own blockchain at any time they wish. Effectively, each wallet gets to "mine" a block at any time, and also choose the order of the transactions within the block. This gives the power back to the 2 parties involved with each transaction and eliminates the possibility of a central power choosing the order of transactions. Once the sender and receiver of a transaction has included it in each of their blockchains, the transaction is complete.

### H. No ICO

It is becoming increasingly difficult for normal people to participate in ICO's which are becoming exclusive to a small number of wealthy investors. This also results in a small number of people holding a large stake which reduces the level of decentralization and democracy within the protocol.

In the spirit of decentralization and democracy, we have chosen to not have an ICO. The Helios project is entirely self funded and bootstrapped. We will give away almost all of our tokens as bounty rewards, airdrops, and to fund dApp developers over a period of 3 years. Firstly, this will give everyone equal opportunity to participate in the project and ensure the tokens are distributed to a large number of individuals for improved democracy. Secondly, we will be rewarding, among others, strong community members, hard working developers, and social media influencers who help build the Helios community, project, and dApp ecosystem. These are the individuals who matter most in creating sustainable growth of a decentralized blockchain platform. By rewarding them, we will also accelerate the growth and adoption of the Helios protocol.

## IV. THE HLS ETHEREUM TOKEN

We have created the HLS token on Ethereum to allow people to participate in the Helios community while we develop the mainnet. We are not having an ICO. The Helios project is entirely self funded and bootstrapped. Instead, we will give away almost all of our tokens as airdrops, and to give to DApp developers. We will also take steps to reduce the possibility that any one individual can hold a large amount of stake. One of these steps is to distribute the tokens in small quantities over a five year time period. We will also spread out the airdrop tokens to a large number of accounts. Once the mainnet is launched, we will swap the Ethereum tokens 1:1 for mainnet coins.

### A. Update June 2019

Mainnet went live on June 30, 2019, and the swap finished on Sept 15, 2019. The Ethereum token HLS is no longer in use.

## V. CONCLUSION

We presented a novel blockchain protocol capable of solving all of the scaling problems that exist with current projects, while maintaining all of the positive qualities of the blockchain. The Helios protocol is estimated to be on the order of 50 million times faster than Bitcoin, and manages to increase transaction volume linearly with the number of users who use the protocol. This results in near infinite scaling into the future. The new Helios consensus mechanism is estimated to use 6000 to 9000 times less energy than Bitcoin PoW while maintaining the same high level of immutability and reliability. This, in combination with the massive transaction volume handling, and inexpensive node hardware, will result in orders of magnitude lower transaction fees than Bitcoin or Ethereum. The Helios protocol will also support Solidity based smart contracts and dApps. We believe this will result in accelerated adoption and growth of the Helios dApp platform. Furthermore, we have decided to not have an ICO and are bootstrapping the entire project ourselves. Instead, we will be giving away almost all of the tokens over a five year period to rewarding, among others, strong community members, hard working developers, and social media influencers who help build the Helios community, project, and dApp ecosystem. These are the individuals who matter most in creating sustainable growth of a decentralized blockchain platform. By rewarding them, we will also accelerate the growth and adoption of the Helios protocol. Finally, we will make all code open source and free for anyone to use.

We are true believers in democracy and the decentralization of power, and are developing this protocol to ensure this is the case for now and the future.

## VI. CONTACT

Website: heliosprotocol.io
Blog: heliosprotocol.io/blog
Discord: discord.gg/xXwt2YC
Telegram: t.me/heliosprotocol
Twitter: twitter.com/HeliosPlatform
Github: github.com/Helios-Protocol
Email: contact@heliosprotocol.io

[1] BitInfoCharts, "Bitcoin avg. transaction fee historical chart," (2018).

[2] Blockchain.info, "Average confirmation time," (2018).

[3] Digiconomist, "Bitcoin energy consumption index," (2018).

[4] Visa, "Visa acceptance for retailers," (2018).

[5] V. Zamfir, "Casper the Friendly Ghost A "Correct-by-Construction" Blockchain Consensus Protocol," (2013).

[6] V. Buterin and V. Griffith, CoRR **abs/1710.09437** (2017), arXiv:1710.09437.

[7] D. Griffiths, *Introduction to Quantum Mechanics*, Pearson international edition (Pearson Prentice Hall, 2005).

[8] Bitnodes, "Nodes," (2018).

[9] bit tech, "Amd ryzen 7 1700 review," (2018).