HELIOS HIGHLITD FINAL WHITE PAPER

WHITE PAPER OF HELIOS

Abstract:

The launch of the Ethereum blockchain in 2015 demonstrated the ability to deploy Turing complete smart contracts on decentralized, peer-to-peer networks in a transparent and trustless manner. It spawned a multitude of decentralized applications, creating entirely new fields of innovations such as DeFi, AMMs, NFTs, DEXs, etc. In turn, these applications increased demand on the Ethereum network. Due to scalability issues, users faced high transaction fees and long confirmation times, resulting in limited adoption. Other smart contract platforms have been created with higher throughput levels than Ethereum but lack true scalability or decentralization. To address these challenges, we present Helios, a sharded, Ethereum compatible, smart contract platform. Heliosis depends on Horizontal sharding which employs dynamic state sharding, cross-shard atomic composability, auto scaling, linear scaling and many other novel technological innovations designed to solve the scalability trilemma and keep transaction fees low even as adoption increases. We believe sustainably low transaction fees are key to bringing decentralized applications to the masses.

Purpose:

This whitepaper is an evolving document that details Helios current vision, roadmap, technology and future direction. Due to the dynamic nature of our development process, some aspects of our technology are continuously being refined, enhanced and adapted to serve our community better and align with our mission. We deeply value the trust, patience and support the entire community has extended during these foundational phases of development. In collaboration, we aspire to architect a groundbreaking system characterized by enduring reliability, sustainability, low fees and an innate capacity to evolve in alignment with user requirements.

Layer 1 Blockchain

A Layer 1 blockchain is the foundational layer of the blockchain architecture,responsible for fundamental operations and consensus mechanisms. It operates as the primary and autonomous chain on which transactions are directly executed and confirmed, providing essential infrastructure for decentralized applications and smart contracts.

Examples of Layer 1 Blockchain

- **Bitcoin (BTC)**
- **Ethereum (ETH)**
- **Solana (SOL)**
- **Avalanche (AVAX)**
- **Kaspa (KAS)**
- **The Open Network (TON)**
- **Internet Computer Protocol (ICP)**
- **Sei (SEI)**
- **Sui (SUI)**
- **Binance chain**
- **Ripple**
- **Monero**
- **Litecoin**

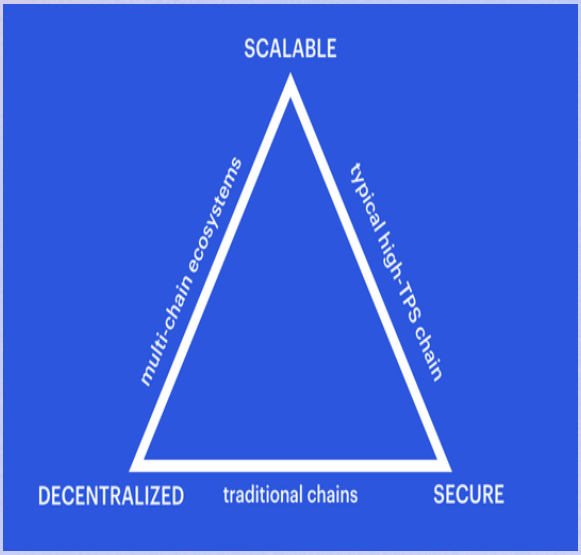
What are the Issues Blockchain Facing Currently ?

Blockchain Trilemma :

The blockchain trilemma refers to a widely held belief that decentralized networks can only provide two of three benefits at any given time with respect to decentralization, security, and scalability

The blockchain trilemma refers to the commonly held notion that, in terms of decentralization, security and scalability, decentralized networks can only provide two of the three benefits at any given time. Computer scientists devised the consistency, availability and partition tolerance (CAP) theorem in the 1980s to express possibly the most significant of these difficulties. The CAP theorem states that decentralized data storage, such as blockchain, can only satisfy two of the three guarantees mentioned above simultaneously.

This theorem has evolved into the blockchain trilemma in the context of the current distributed networks. The widely held notion is that public blockchain infrastructure must sacrifice security, decentralization or scalability.



As a result, the holy grail of blockchain technology is to create a network with impenetrable security over a broadly decentralized network while also handling internet-scale transactional throughput.

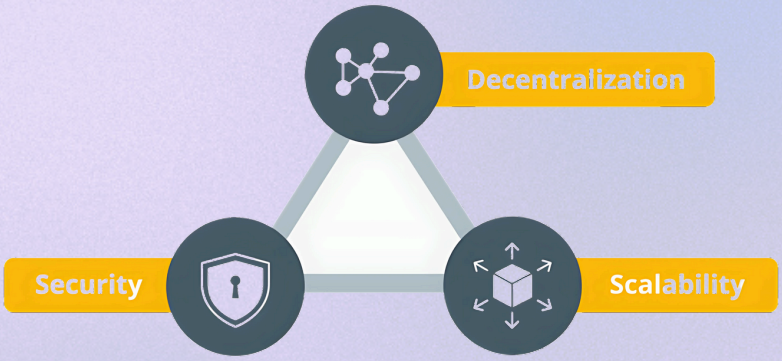
Before delving into the trilemma's dynamics, let's define scalability, security and decentralization in general terms:

The blockchain's scalability refers to its ability to handle a higher volume of transactions.

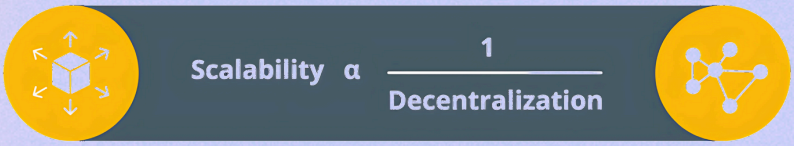
Security refers to the ability to secure data on the blockchain from various types of assaults and the blockchain's defense against double-spending.

Decentralization is a type of network redundancy that ensures that the network is not controlled by fewer entities.

Blockchai Trilemma



The Blockchain Trilemma



Scalabilits Decentralization

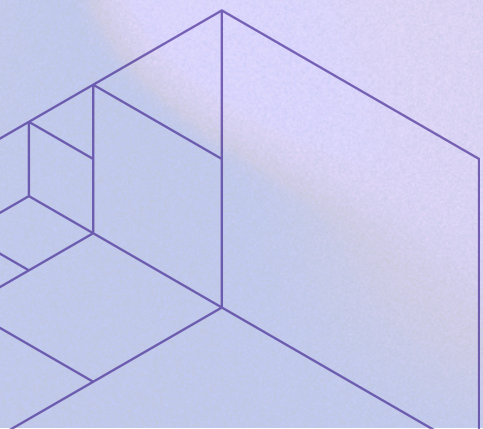
Scalability Vs Security

Consensus :

A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the distributed ledger. In simple terms, it's just a method to decide within a group. Let me clear it up with an example. Imagine a group of ten people that want to make a decision about a project that benefits them all. Every one of them can suggest an idea, but the majority will be in favour of the one that helps them the most. Others have to deal with this decision whether they liked it or not.

Parameters That Define A Consensus Mechanism

- **Decentralized Consensus**
  A single central authority cannot govern a transaction.
- **Quorum Structure**
  Nodes exchange messages in predefined ways, which may include stages or tiers.
- **Authentication**
  Process provides means to verify the participants' identities.
- **Integrity**
  It enforces the validation of the transaction integrity.
- **Non-Repudiation**
  This provides means to verify that the supposed sender really sent the message.
- **Privacy**
  This provides means to verify that the supposed sender really sent the message.
- **Fault Tolerance**
  The network operates efficiently and quickly even if some nodes fail or are slow.
- **Performance**
  It considers throughput, liveness, and latency.



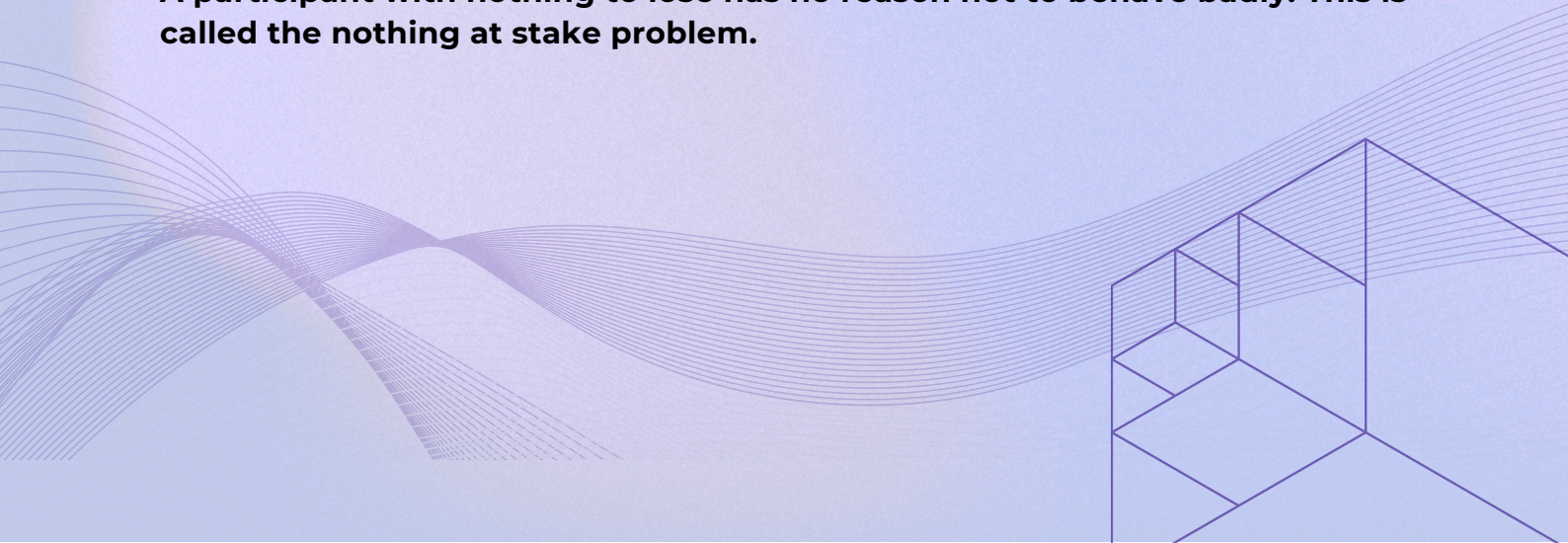
Proof of work (POW)

POW requires nodes on a network to provide evidence that they have expended computational power (i.e., work) in order to achieve consensus in a decentralized manner and to prevent bad actors from overtaking the network. Proof of Work (POW) This idea was first proposed by Dwork and Naor (1992) to combat junk emails. To discourage the attacker from sending junk emails, the sender had to do some work for the validation of email.

The work is given by Service provider to the Service requester.
This work is moderately hard but feasible for the requester and is easy for the provider to validate.
The puzzle friendliness property of cryptographic hash functions makes them useful to be used as POW.
Most implementations of Bitcoin POW use double SHA256 hash function.
The probability of getting a POW is low. It is difficult to say which miner will be able to generate the block. Hence, no single miner will be able to control the network.

Proof-of-Stake

- **Proof-of-Stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also called stake.**
- **No coin creation exists in proof-of-stake, hence a validator invests in the coins of the system.**
- **Your chance of being picked to create the next block depends on the fraction of coins in the system you own.**
- **Different proof-of-stake systems vary in how they handle commitment of the created block to the Blockchain.**
- **A participant with nothing to lose has no reason not to behave badly. This is called the nothing at stake problem.**



What is Helios?

Helios is Layer 1 Blockchain Which solve the Blockchain Trilemma

Decentralization

We are Deploying Nodes in different countries of the world, Our nodes are based in HongKong, USA, UAE, Singapore, China, European Union countries, Middle East, New Zealand.

Security

Given that Helios functions as a sharded network, processing various transaction sets across its multiple shards, its security model diverges from non-sharded Layer 1 architectures: it must defend against both standard Layer 1 threats and those attacks specific to sharded architectures. To this end, we provide an overview of common attacks. The list is non-exhaustive due to the evolving nature of security threats and to maintain a focused and concise document. Readers are encouraged to explore additional resources for a more comprehensive understanding of potential security challenges.

Sybil Attacks Description:

Sybil attacks are a type of attack in which an adversarial actor or group of adversarial actors attempt to gain control of a disproportionate percentage of a network by creating pseudonymous identities that can disrupt the network and compromise its security.

Mitigations

To counter Sybil attacks, DLTs that wish to retain decentralization and secure use a Sybil deterrence mechanism to impose a cost for network participants to join the network as they cannot use typical centralized solutions such as identification authorities. In the case of Helios, nodes must stake a minimum amount of HELT. This imposes an economic burden on the attacker and helps to deter a Sybil attack. Also nodes which misbehave can be slashed and removed from the network. Losing the staked amount makes it harder for an attacker to continue to attempt additional attacks.

Shard Takeover Attack Description

An attack in which an adversary fills a shard with their own nodes in order to control the shard. Once an adversary controls 33% of the nodes they can halt the shard and if they control 66% of the nodes they can forge transactions within the shard.

Mitigations

Helios prevents single-shard takeover attacks by not allowing nodes to select which shard they join. Nodes are randomly selected to be rotated into the active set and prevented from choosing their shard or address range. Thus, to achieve a 66% takeover of a shard would require a 66% takeover of the entire network including active and standby nodes. Since nodes are required to stake even as a standby node, the economic cost of a shard takeover attack would be very high. In addition the rotation of nodes helps to ensure that an adversary cannot build up an attack over a long period of time.

Nothing at Stake Description:

During a network fork, an adversary in the form of a validator node can continue to validate on a fork of a blockchain incurring no cost for validating both chains. On PoW mechanisms, miners are incentivized to not waste network resources mining on the alternate chain, but PoS validators can potentially still earn transaction fees on both versions of the network, meaning they have nothing at stake that incentivizes or disincentivizes them from supporting illegitimate forks unlike on PoW networks.

Mitigations

Helios does not use PoW or PoS as its consensus mechanism, it uses PoQ for consensus and PoS as a Sybil deterrence mechanism so the stake is not part of the consensus. Therefore, the network will not accept a fork based on the longest-chain rule like on PoW or based on overall weight staked like on PoS and an adversary cannot double-sign or equivocate a transaction without getting slashed. Additionally, the digital signatures used to produce a receipt via PoQ can't be forged.

Long Range Attacks Description:

A long-range attack is when an adversary goes back to the genesis block and forks the blockchain.
Mitigations: Long-range attacks on Helios are not possible as we do not use PoW or PoS as a consensus mechanism. Therefore, the network will not accept a fork based on the longest-chain rule like on PoW or based on overall weight staked like on PoS and an adversary cannot double-sign or equivocate a transaction without getting slashed. Additionally, the digital signatures used to produce a receipt via PoQ can't be forged.

Mitigations:

Long-range attacks on Helios are not possible as we do not use PoW or PoS as a consensus mechanism. Therefore, the network will not accept a fork based on the longest-chain rule like on PoW or based on overall weight staked like on PoS and an adversary cannot double-sign or equivocate a transaction without getting slashed. Additionally, the digital signatures used to produce a receipt via PoQ can't be forged.

Censorship Description:

An attack in which a validator has control of the transactions which will be included in a block and uses their status as validator to prevent the transaction going through, possibly via blacklisting.

Mitigations

By having a blockless architecture, Helios prevents validators from altering the order of transactions within blocks and also deciding which transactions are included in a block. Helios also uses leaderless consensus meaning that no validator is elected as leader and so no individual validator can single-handedly prevent transactions being processed. A small group of validators could not put out a vote on specific accounts or transactions, but for an attacker to engage in censorship effectively they would need to control 33% of a shard which is countered by minimum stake requirements, node rotation and disallowing nodes to select which shard they join

DoS or DDoS Attack Description:

Denial of service or distributed denial of service is an attack where nodes are knocked offline and fail to meet liveness requirements. A distributed denial of service is similar but with many nodes taking part to knock a node offline.

Mitigations

Nodes should have DDoS protection by running their node with an ISP with a strong DDoS protection mechanism. If a node is successfully taken down, other nodes in the shard have account range redundancy and can still validate the transaction. Another node or shard will always have an opportunity every cycle to join when nodes are downed. If a shard was knocked down via a form of DoS it would not be able to produce a receipt and the user who submitted a transaction would be informed that their transaction didn’t go through resulting in certain accounts being temporarily unable to process the transaction. Nodes that stay in the network and aren't successfully taken offline will also more likely stay in the network in the long-run due to superior DDoS defenses.

Transaction Flooding Description:

An attack in which an adversary floods the network with valid transactions in an attempt to slow the network.

Mitigations

Helios prevents transaction flooding by imposing economic costs in the form of HELT gas fees. These fees are inexpensive enough to allow a beneficial user experience, but will cost an adversary a large amount should they engage in a transaction flooding attack. Additional measures such as requiring higher fees from excessively active source accounts can impose a burden on an adversary without impacting regular users.

Scalibilty

Scalability Trilemma In order to keep transaction fees low in a sustainable way, a network must be able to scale to accommodate an ever-increasing number of transactions. Of course scalability is not the only important factor. A network must also maintain a high level of decentralization and security. The scalability trilemma says that as a blockchain tries to achieve scalability, decentralization and security, it will only be able to attain any two of these. With security being an essential requirement, this means that there will be a trade-off between scalability and decentralization. A lack of scalability leads to slow processing of transactions and higher transaction fees resulting in a bad user experience. A lack of decentralization is not immediately felt as a bad experience, but puts all the users at risk of losing assets should the lack of decentralization be exploited. Sharding of state data across the many nodes available in a large network can increase parallel processing and also provide a solution to the scalability trilemma.

Current Solutions

Many new networks which provide the exact same or similar smart contract functionality as Ethereum have been developed to fill the gap left by Ethereum. Among these new smart contract platforms a majority of them have sacrificed decentralization to achieve higher TPS. We intentionally use the term “higher TPS” instead of “higher scalability” because these networks are not designed to scale, but rather just raise the bar from Ethereum’s 20 TPS to a higher max TPS. Typically this is about 10000 TPS. The smart contract platforms in this category do not use sharding and include networks such as: BNB Chain, Solana and Algorand, to name a few. As these networks approach their max TPS limit, they too will experience the same high gas fees and slow processing times as Ethereum. These platforms can only increase TPS if each node in the system is upgraded to have more compute, storage and bandwidth. This is referred to as vertical scaling. One of the first smart contract platforms to attempt sharding was Zilliqa. All nodes in this platform stored the complete state and every transaction was received by every node. However, for the purpose of validating transactions the network was sharded into multiple partitions based on the address space of accounts. This is referred to as compute sharding because it divides the work of validating transactions, which is usually compute intensive. But since every node still receives every transaction and updates the state of all accounts, the network bandwidth and storage operations still become a bottleneck. Zilliqa is able to achieve a higher TPS than a system with no compute sharding, but is not truly scalable since the network and storage are not sharded.

A more scalable approach to meet the growing demand for decentralized applications is to have an interconnected system of multiple sub-chains or sidechains. Such an approach is being taken by platforms such as Polkadot, Cosmos and Avalanche. This approach can be referred to as functional sharding, whereby decentralized applications that need to interact with one another can be launched on the same sidechain. In the case of Polkadot, each parachain can process about 1000 TPS.

Even though the TPS of a sidechain may appear low compared to networks like Solana, the ability to have multiple sidechains allows such platforms to scale and the total TPS across all sidechains can surpass that of platforms using only vertical scaling. Transactions between contracts on the same sidechain are fast and easy. However, composability between contracts on different sidechains within the same network is still difficult due to the asynchronous nature of communication between sidechains. Instead assets and messages are expected to be passed between chains to coordinate interactions.

The lack of atomic composability across sidechains can make it difficult to access DeFi liquidity that is fragmented across sidechains. If a sidechain reaches its TPS capacity the only way to deal with the congestion would be to vertically scale the nodes in the sidechain or to migrate some of the popular contracts to other sidechains. The most general approach to sharding is to divide the address space of accounts into multiple fixed size regions called shards and assign subsets of nodes in the network to different shards.

This is referred to as state sharding. Such an approach is being taken by platforms such as Near, Harmony and MultiversX (formerly Elrond). Although Ethereum originally planned to implement state sharding, the new approach, proto-danksharding, shards only the data to achieve higher data availability while execution is done off chain. In a network with state sharding, transactions between contracts in the same shard are fast and easy while transactions across multiple shards require cross shard coordination and are much slower.

Existing state sharded blockchains must execute transactions that affect more than one shard asynchronously and sequentially; passing the transactions to each shard that is involved. That’s because transactions in such networks are grouped into blocks and consensus is done at the block level; therefore, transactions that affect multiple shards risk the possibility of being confirmed in one shard, but not confirmed or rolled back in another shard.

Also, maintaining atomic processing of transactions requires additional layers of complexity. Furthermore, transactions which affect multiple shards will require additional processing time proportional to the number of shards they affect. Even with these complexities state sharding is still beneficial since the TPS of the whole network will increase proportional to the number of shards it has.

Sharding

As Vitalik Buterin, the founder of Ethereum pointed out, sharding is the solution to the scalability trilemma. The most general form of sharding referred to as state sharding divides the nodes in the network into smaller groups which store a subset of the state data and process different sets of transactions to achieve parallel processing. The transaction throughput of the network increases directly proportional to the number of shards in the network. State sharding provides a way to achieve both scalability and decentralization while maintaining security. However, many of the current platforms that employ state sharding do so in limited ways and the grouping of transactions into blocks adds complexity to the sharding protocol. No decentralized network has yet demonstrated linear scaling or auto-scaling. Throughout the rest of this paper we will just use the word “sharding” to mean “state sharding”, unless specified otherwise. Although sharding increases throughput, it introduces additional complexity. Most implementations of sharding break atomic composability which allows multiple smart contracts to be chained together in one transaction. Furthermore, sharding can potentially reduce the network’s security if naively implemented. Adversaries only need to compromise the byzantine fault tolerance limits of a single shard instead of the entirety of the network to halt the shard or engage in arbitrary state changes. Adversaries can also launch other attacks, such as cross-shard takeover attacks, new data availability attacks, sharding-specific replay attacks and other forms of attacks against sharded networks. Therefore, the sharded networks’ architecture must be secure, robust and mitigate existing attack vectors to retain security.

Technology

Design Considerations

A central design goal of Helios is to ensure sustainably low transaction fees. The most popular applications on most smart contract platforms are related to asset trading because the high gas fees during times of network congestion prevent other use cases from being feasible. We believe that to onboard users in developing countries and allow more use cases of decentralized applications to evolve, the smart contract platform must provide sustainably low transaction fees.

User Experience

When a new network is launched, the transaction fees are typically very low because the usage is much less than the capacity of the network. Users are generally happy during this time and get the false impression that fees will continue to remain low. As the popularity of the network grows, the usage begins to approach the capacity of the network and users must bid on how much they are willing to pay to have their transaction processed. At times of peak congestion the transaction fees can increase at an exponential rate. The promise and adoption of smart contract platforms has been severely restricted by the inability of current networks to scale and meet the higher TPS demands of a growing user base

Developer Experience

From a developer's perspective, a lot of time and effort is invested in building decentralized applications. Resources are invested in writing smart contracts, testing them, debugging them, getting them audited, building a friendly user interface, marketing the application, building a community and acquiring a loyal user base. These are resource-intensive endeavors that require a significant investment of time, money and other resources. When a network is new and transaction fees are low, all kinds of decentralized applications are feasible. However, as the network grows in popularity and transaction fees rise, most decentralized applications that depend on low fees will be squeezed out by DeFi applications. A smart contract that gives $1 USD worth of loyalty tokens to customers is not feasible when the transaction fees are in the dollar range. For developers, smart contract platforms that cannot ensure sustainably low transaction fees represent an existential threat to their business model.

Energy Efficiency

The amount of energy used by a network to process a transaction will inevitably need to be paid for by the user. If a network is to achieve sustainable low transaction fees, then the energy used to process the transactions must be kept as low as possible. Therefore, using a consensus algorithm that does not require extreme energy expenditure is a must.

Horizontal Scaling

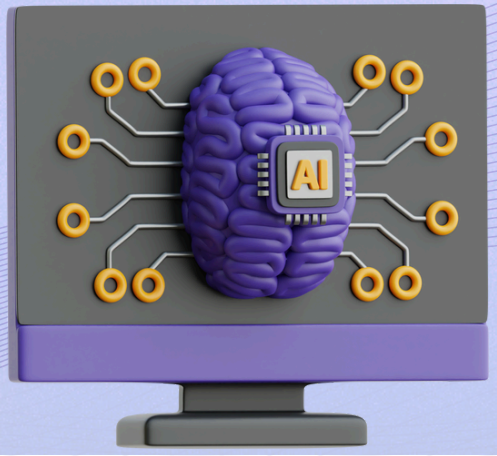
Having more nodes in a network can help to increase the level of decentralization and security of the network, but after a certain point, adding more nodes does not really benefit the network. Many networks don't scale because complexity of consensus and the amount of communication increases as more nodes join the network. In networks where each node must process every transaction, the additional nodes only add to the operating cost of the network once the decentralization and security needs are met. This will eventually result in higher transaction fees for the users. Horizontal scaling through sharding is necessary for a network to optimally use the nodes that are available, keep network operating costs low and ensure low transaction fees for users.

Network Size

All nodes providing resources to a network must be able to operate profitably in the long run. The transaction fees must be able to cover the operating cost of the network if it is to be sustainable in the long run. This means that the number of nodes in the network must be adjustable based on the transaction throughput of the network. At times when the TPS of a network decreases, the network must be able to reduce the number of nodes, otherwise the transaction fees will have to increase to continue paying the extra nodes. This is an important factor not considered by any of the existing networks.

Compatibility

An important design goal of Helios is to not reinvent the wheel when it comes to the programming language used for smart contracts and the virtual machine used to run the smart contracts. A choice was made to have Helios be EVM compatible. This not only reduced the development time, but also made the Helios platform easily accessible to the existing Ethereum smart contracts, developer community and ecosystem.



Shard Security

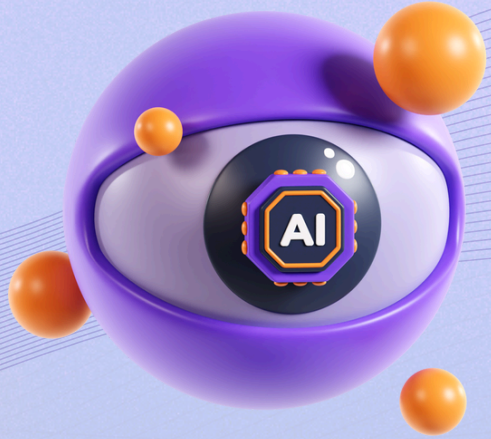
Economic security makes Sybil attacks expensive in unsharded networks such as Ethereum. Sharded networks that are naively designed risk a Sybil attack as the cost of taking over any one shard is much less than taking over a majority of the network. An important design goal of Helios is to ensure that a Sybil attack on a shard has the same economic cost as an attack on the whole network through various mechanisms such as staking, slashing, standby nodes and node rotation.

Architecture

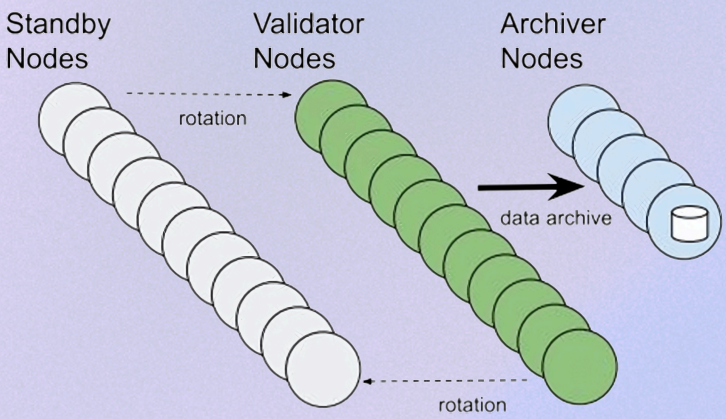
The Helios network was architected based on the above design considerations. In particular, to minimize transaction costs through efficient use of available resources while maximizing network scalability, decentralization and security.

Network Architecture

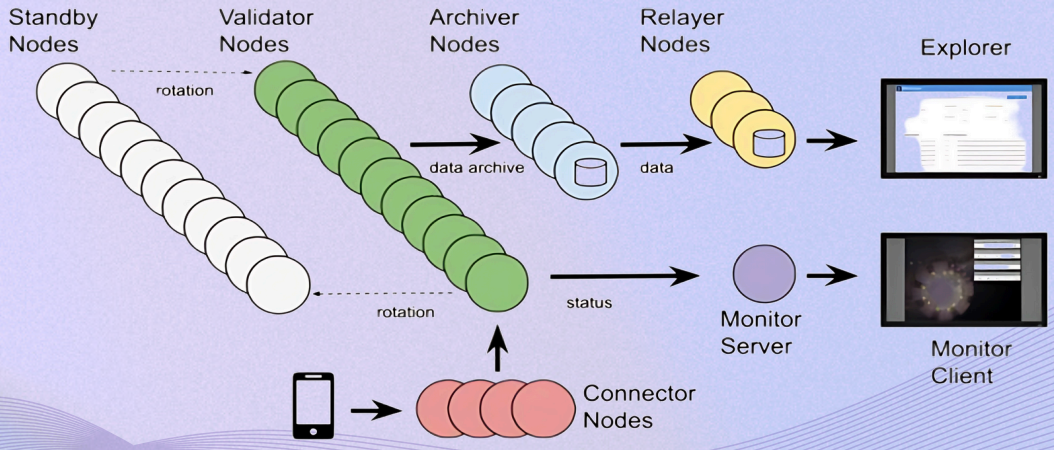
The Helios network is composed of validator nodes and archiver nodes. Validator nodes that are waiting to join the network are referred to as standby nodes. The validator nodes hold the state data of the accounts they are assigned to and process incoming transactions involving the accounts within their address range to change the state. The transaction history is passed on to archiver nodes for permanent storage. The archiver nodes are not involved in any consensus and simply provide the service of storing historical network data such as transactions and receipts. Validator nodes have light storage requirements and fast syncing when joining the network as they only need to sync and store the state of the accounts they are assigned to. Validator nodes which have been active in the network for the longest time are periodically removed from the network and replaced by randomly selected standby nodes. A slow and constant rotation of validator nodes enhances the decentralization level of the network and prevents attacks from slowly adaptive adversaries. Running a validator node requires staking the native Helios coin with ticker HELT. The staked HELT are subject to slashing if the validator does not perform its duties as expected or is misbehaving. However, for honest validators there is sufficient reward to easily cover the cost of operating the node and earn a good profit.



In addition, there are other types of nodes needed to move data and transactions in and out of the Helios network as well as monitor the health of the network. These include connector nodes, relayer nodes and a monitor server. The connector nodes provide an entry point for external wallets and clients to query and submit transactions to the network. These are the same as RPC servers in the Ethereum ecosystem. Relayer nodes communicate with archiver nodes or other relayer nodes to store and stream data produced by the network to downstream services such as the explorer. These are similar to exit nodes in the Ethereum ecosystem which are used by exchanges and explorer services. The monitor server receives status updates from active validator nodes and provides a visual view into the health of the network.



When the Helios mainnet is launched we expect to have a minimum of 1300 validators and 10 archivers. The number of standby validators will depend on various factors, but based on the numbers seen in the testnets we expect at least 20,000 standby validators. The number of nodes per shard will be 128. Based on usage of the network, the number of validators are expected to grow automatically to accommodate demand.



USE CASE OF HELIOS

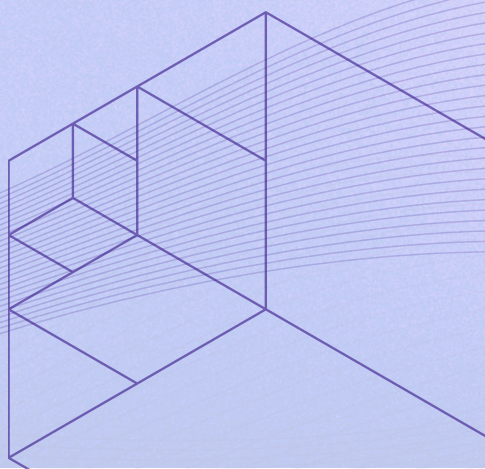
- Supply Chain Management Blockchain can help to track all products in real-time. It can also get rid of tampering issues and improve the transparency of the supply chain. It also allows to locate and isolate any issues faster by tracing the source. Blockchain can reduce the cost and offer verifiable proof of any product's authenticity.

- Digital Identity Blockchain can benefit and help establish a secured digital identity storage system. As blockchain allows users to own and control their data, users can give access to other parties as they need. Users will have a single identity on a blockchain platform, which can be accessed via other platforms if needed. It can also get rid of identity thefts and redundant KYC protocols.

- Asset Tokenization Blockchain makes it possible to tokenize any type of real-world asset. This increases the overall efficiency of asset ownership. It can even tokenize illiquid assets and create a marketplace for buying and owning those assets. This gets rid of the long process of finding a potential buyer or seller and the paperwork for acquiring any asset.

- Energy Blockchain can improve the efficiency of the energy sector by tracking and distributing electricity or other energy sources when needed. It also enables a new type of market for individuals to participate by using their stored-up energy from solar panels. This process can ensure 100% uptime without relying solely on big corporations.

- Healthcare The Healthcare system has to deal with legacy technology that is unable to support doctor-patient confidentiality. Here, patients will have access to their data stored on the blockchain and can give permission to see it when needed. It can also store and facilitate medical research data and offer an easier way to claim health insurance.



- **Real Estate Real estate can highly benefit from blockchain-based smart contracts. It can offer a smoother and safer transaction processing option along with increasing the liquidity of this sector. Blockchain allows the option to partially own real estate, making it possible for global participation. As it gets rid of middlemen, it saves a lot of money for both buyer and seller.**

- **Cyber Security Blockchain is immutable and offers high security against cyber-attacks. This makes it an ideal technology for dealing with cyber threats. It can offer a decentralized storage system and fight against DDoS attacks. It can offer private biometric keys and multi-signature authentication procedures for the users.**

- **Internet of Things Blockchain can offer more security for internet of things devices. As these devices are connected via a centralized cloud network, they are easily vulnerable to cyber-attacks. Blockchain offers them a decentralized environment where these devices can communicate with one another. Also, it helps to keep your data protected and only sharable when needed.**

- **Insurance Blockchain can help to improve the overall insurance claiming process. It's possible to automate the insurance claiming process, which benefits both insurers and the insured. Paperwork in this sector is very time consuming and complicated. With a smart contract that can be facilitated within minutes.**

- **Banking For the banking sector, blockchain can remove the redundant KYC model. Instead, customer KYC information can be exchangeable within banks, which saves a lot of time. It can also offer faster transaction processing time and offer better protection against any cyber-attacks. Users will also get more transparency in using blockchain as a means for the banking sector**

- **Voting Blockchain eliminates the scope of voter fraud. Every data on the blockchain is immutable, so no one can alter it once it's added to the ledger It also provides an option for voting online in a secured channel. Every vote will go through a verification process to see whether it's authentic or not. This allows citizens to have more trust in the voting system and the government.**

- **Food Safety Blockchain can help companies to track food from the source to the end user efficiently. This promotes provenance that the food is coming from quality sources and is not contaminated. This process also gets rid of food waste as timely shipments are achievable. Therefore, blockchain can offer a cost effective and transparent solution to food safety issues.**

- **Data Management Blockchain can streamline a more powerful, faster, and secured network for data management. Once the data gets verified and added to the ledger, no one can alter it. This feature allows blockchain to offer data integrity. Also, blockchain can offer safer and secured storage facilities for Big Data.**

- **Travel In travel, blockchain can offer to track luggage for luggage management. It can also track transportation vehicles and maintain a fixed schedule, getting rid of any delays. Users can use blockchain to store their passports and use that as the official identification when travelling internationally. It can also offer a secure and traceable means of payment.**

- **Gaming Gaming is a great sector where blockchain use cases can really play out. Using blockchain, developers can create decentralized games without needing any centralized servers. It can also help tokenize the e-sports sector by allowing investments in game assets. It can also eliminate counterfeiting of sports merchandise and help users view the authenticity of their purchased products.**

TOKENOMICS

Helios employs dynamic state sharding to attain linear scalability, ensuring that every node added boosts network throughput instantly. As a result, Helios can enhance its TPS capacity and maintain low fees sustainably. Our simulations revealed that the economics of linear scalability required a unique approach to how the native coin HELT is issued.

HELT Coin

The native coin on Helios has HELT as its ticker symbol. HELT is the foundational monetary unit of Helios and serves a wide range of functions. Each HELT is divisible to 18 digits, similar to ETH on the Ethereum network. We will also refer to it as the HELT token, since a tokenized version of the coin is also used by smart contracts and to be consistent with common terminology.

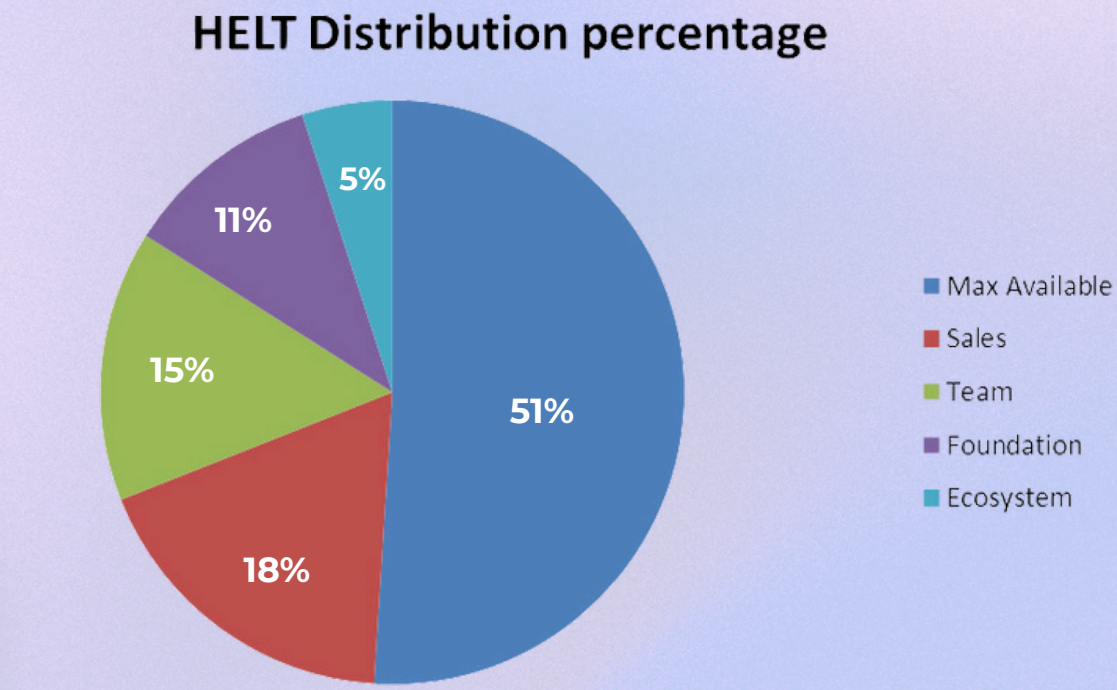
HELT is a utility token with various uses, including:

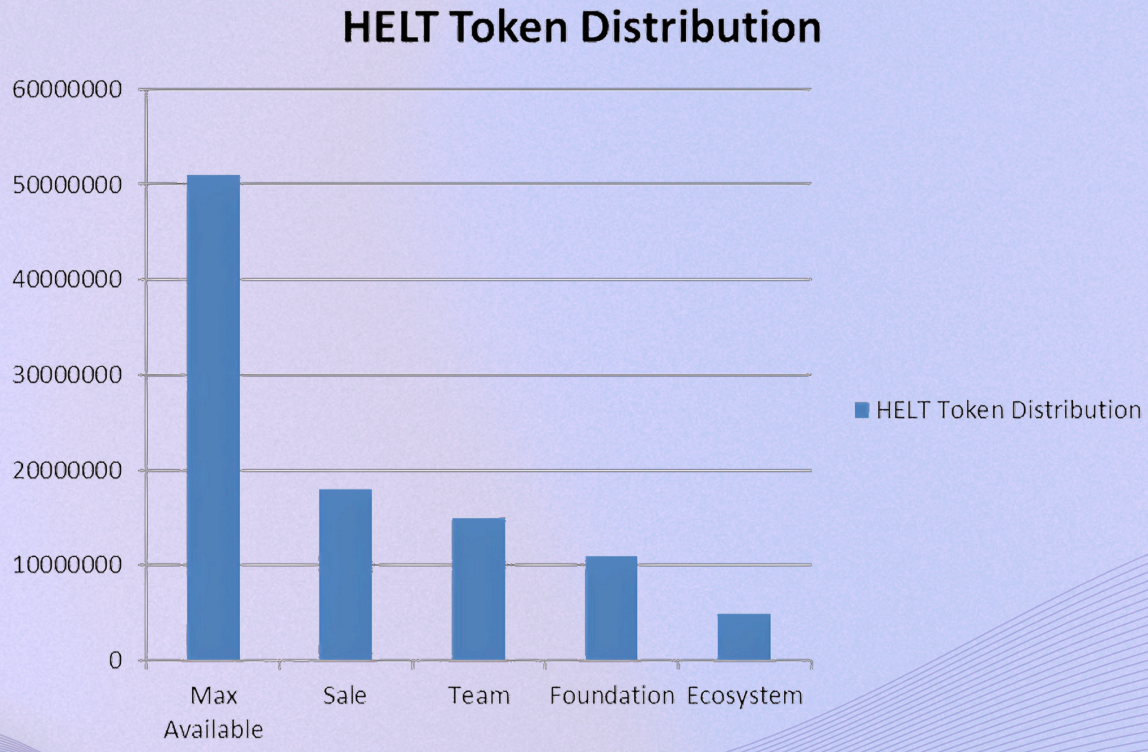
- Staking: Network participants can stake their HELT, increase the network's overall security and earn rewards for their active participation
- Governance: HELT is a governance token conferring stakers governance rights, allowing them to decide and vote on the future of the network. Helios will not use a 1 token 1 vote system
- Reward Token: HELT is given as a reward, for example: via airdrop, ecosystem rewards and network participation
- Gas Token: HELT is a gas token allowing network users to pay fees to execute the required compute units for transactions and other more complex transactions involving smart contracts on the network
- Transaction Fee Burning: All transaction (tx) fees on Helios are burned, allowing the network to remove the HELT from the circulating supply
- User Staking: We are considering the possibility of users staking during deflationary periods. Since Helios is not based on Delegated Proof of Stake (DPoS), there are no delegation pools

HELT Allocation

- Max supply: 100 million
- HELT Distribution:
- 51% Community (51,000,000 HELT) – reward to validator and archiver nodes
- 18% Sale (18,000,000 HELT) – 3 month cliff then 2 year daily linear vesting
- 15% Team (15,000,000 HELT) – 3 month cliff then 2 year daily linear vesting
- 11% Foundation (11,000,000 HELT) – unlocked at Token Generation Event (TGE)
- 5% Ecosystem (5,000,000 HELT) – unlocked at TGE Since transaction fees are burned, the maximum HELT supply of 100 million will never be reached.

The following image shows the HELT distribution as a bar chart and pie graph :





WHY YOU SHOULD CHOOSE HELIOS?

- INITIAL TPS WILL BE 1 LAKH – 3.5 LAKH (WE CAN INCREASE MORE TPS AS WE REQUIRED)
- MULTIPLE LANGUAGE SUPPORT
- LANGUAGES – C+, PYTHON, GO, TYPE SCRIPT, JAWA, RUST,SOLIDITY,MOVE,ETC.
- ·ORACLE WILL BE DECENTRALIZED
- PROVIDE HELIOS NAME SERVICE
- DEVELOPER FRIENDLY
- ONE BLOCK FINALITY
- DAPPS SERVICE
- SMART CONTRACT
- DOCS VERIFICATION
- GESS FEES VARY BETWEEN 0.001 USDT – 0.0001 USDT
- PROPER FUNCTIONING IN NFTS MINTING
- SUPPORT GAMING PROJECTS LIKE WAX BLOCKCHAIN
- HORIZONTAL DYNAMIC SHARDING CONCEPT IS APPLIED ON HELIOS BLOCKCHAIN
- SUPPORT MULTIPLE WALLETS
- INTERBLOCKCHAIN COMMUNICATION WILL BE FAST
- NO. OF NODES WILL BE VARY

ECOSYSTEM

DApps

Decentralized Applications, commonly known as dApps, are applications that operate on smart contract platforms, eliminating the need for centralized intermediaries while providing transparency, security and immutability. In the Helios ecosystem, we encourage and incentivize the development of dApps that are optimized for, or can benefit from, parallel transaction processing. This is particularly beneficial for dApps with high transaction volumes or those that need to execute complex computations that can be broken down into smaller concurrent tasks. Transactions are processed in a first come first served (FCFS) manner; this approach is beneficial as it provides predictability, fairness, prevents higher fees via bidding, offers MEV resistance and opens up a pathway for new types of dApps. For instance:

- **Auction Platforms: In an auction, bids should be processed in the order they're made. FCFS ensures that if two participants place a bid at nearly the same time, the one who bid first gets precedence**
- **Ticketing Systems: For events with limited seats or special editions of items, a FCFS system ensures that early birds get the tickets or items without facing potential delays or out-of-order processing**
- **Queue-based Service Platforms: Any dApp where users queue for a service (like a virtual waiting room) would benefit from FCFS. This ensures fairness and reduces potential disputes**
- **Gaming: Certain online games, especially those where players compete for limited in-game resources, could use FCFS to determine the order of acquiring these resources**
- **Decentralized Domain Registration: As new domains or domain extensions become available, FCFS processing can fairly determine who gets a specific domain name if multiple parties are interested**

Additionally, we are committed to promoting dApps that are predicated on the usage of low transaction fees, opening the door for innovative use cases previously rendered impractical on other platforms due to prohibitive costs. Such dApps include, but are not limited to:

- **Loyalty point systems for merchants**
- **Coupon systems for product businesses**
- **Voting systems for small communities**
- **Crowdfunding platforms akin to Kickstarter**
- **Automated payment solutions**
- **Membership services reminiscent of Patreon**
- **Algorithmic stablecoins**
- **Low investment games such as lotteries**

The rationale for championing this direction is multifaceted. Our incentivization of dApps reliant on low transaction fees is grounded in our commitment to ushering in a broader array of applications that could revolutionize entire existing industries and even spawn entirely new ones. Furthermore, for the first time ever, dApps can scale to levels commonly found in popular web2 services without reaching bottlenecks. Additionally, all dApps within Helios maintain Ethereum compatibility, offering a dual advantage: the vast developer community familiar with Ethereum can easily transition or port their projects to Helios while users benefit from the widespread familiarity and trust associated with Ethereum-based applications.

For the Helios community, these strategies herald a future of increased innovation, interoperability and inclusivity. The Ethereum compatibility not only ensures the seamless portability of dApps between platforms but also amplifies the potential for Helios to integrate with the broader ecosystem, enriching the user experience and fostering a cohesive, interconnected community.

What Are DeFi Protocols?

Decentralized Finance (DeFi) protocols consist of contracts and decentralized applications (dApps) that allow financial transactions to occur without relying on intermediaries such as banks or brokers. These decentralized protocols operate on Helios blockchain network, and offer various financial services like lending, borrowing, trading and investing.

In contrast to conventional financial systems, DeFi protocols are open source. This grants accessibility to these services for anyone with an internet connection, promoting inclusivity and transparency in financial operations.

DeFi protocols are designed to function without the need for trust as they operate independently of an authority. Instead, they rely on the security and transparency provided by blockchain technology . These decentralized finance systems are governed by codes. Often, by communities utilizing governance tokens. This decentralized nature fosters innovation and adaptability, as DeFi development services can be improved over time by their user base.

DEFI

Decentralized finance (DeFi) is a term for financial services that use blockchain technology to operate without traditional intermediaries like banks.

How does DeFi work?

- **DeFi uses smart contracts on a blockchain to enable peer-to-peer payments and financial services.**
- **DeFi users can lend or borrow crypto, trade crypto, and earn interest on savings accounts.**
- **DeFi platforms are built on a layered architecture with composable building blocks.**

Benefits of DeFi :

- **DeFi can offer higher yields than traditional bank accounts.**
- **DeFi can allow users to send money quickly and access funds via digital wallets without paying traditional banking fees.**
- **DeFi protocols rely on blockchain's cryptographic features, making them more resistant to fraud, censorship, and hacking attempts.**

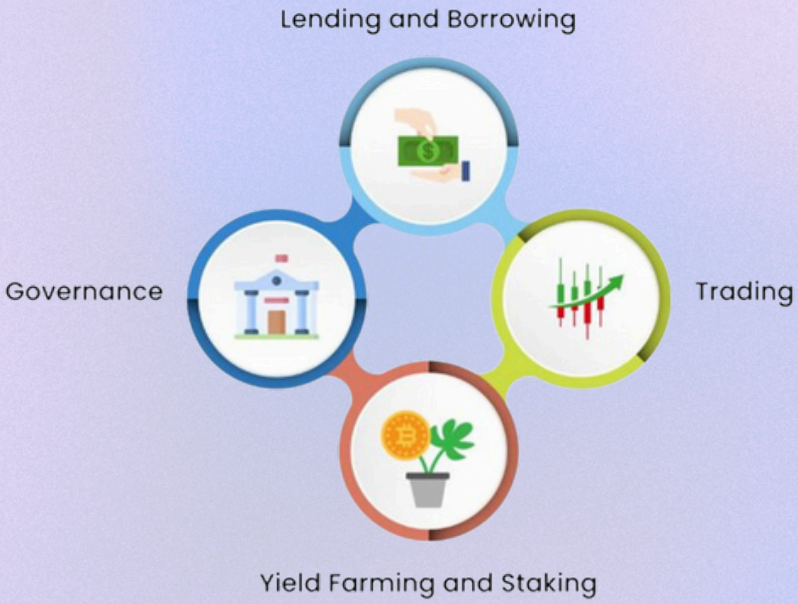
DeFi use cases:

- **Lending crypto**
- **Receiving a loan**
- **Trading and/or exchanging**
- **Saving**
- **Speculating on asset price movements using derivatives**
- **Insuring against risks**

What Are DeFi Protocols?

Decentralized Finance (DeFi) protocols consist of contracts and decentralized applications (dApps) that allow financial transactions to occur without relying on intermediaries such as banks or brokers. These decentralized protocols operate on Helios blockchain network, and offer various financial services like lending, borrowing, trading and investing.
In contrast to conventional financial systems, DeFi protocols are open source. This grants accessibility to these services for anyone with an internet connection, promoting inclusivity and transparency in financial operations. DeFi protocols are designed to unction without the need for trust as they operate independently of an authority. Instead, they rely on the security and transparency provided by blockchain technology . These decentralized finance systems are governed by codes. Often, by communities utilizing governance tokens. This decentralized nature fosters innovation and adaptability, as DeFi development services can be improved over time by their user base.

How Do DeFi Protocols Work?



A DeFi protocol functions through a series of smart contracts—self-executing contracts with the terms of the agreement directly written into code. These smart contracts automate processes such as lending, borrowing, and trading, reducing the need for intermediaries and minimizing the risk of human error.

Lending and Borrowing

In DeFi, users can lend their assets to a decentralized protocol and earn interest, or borrow assets by providing collateral. The interest rates and collateral requirements are usually algorithmically determined based on supply and demand.
For instance, platforms like Aave and Compound, which are leading decentralized finance protocols, enable users to lend their crypto assets and earn interest, while borrowers can access these funds by posting collateral.

Trading

Decentralized exchanges (DEXs) like Uniswap and SushiSwap allow users to trade cryptocurrencies directly from their wallets. These platforms use Automated Market Makers (AMMs) instead of traditional order books to facilitate trades, ensuring liquidity and minimizing slippage.
Liquidity providers contribute their assets to liquidity pools and earn fees in return, making the trading process efficient and decentralized.

Yield Farming and Staking

DeFi protocols often offer yield farming and staking opportunities, where users can earn rewards by locking up their assets in a decentralized protocol. These rewards are typically paid out in the platform's native tokens, incentivizing users to contribute liquidity or secure the network. Yearn.Finance, for example, automates yield farming strategies to maximize returns for its users, demonstrating the power of smart contract development in these protocols.

Governance

In most DeFi protocols, users control the system using governance tokens. These tokens enable holders to vote on crucial matters, like protocol updates, fee adjustments and other significant concerns. This distributed governance approach guarantees community involvement in shaping the protocols growth and trajectory.

Why DeFi Protocols Are Crucial

DeFi protocols are crucial because they represent a paradigm shift in how financial services are delivered and accessed. Here are key reasons why these decentralized protocols are essential:

Financial Inclusion

DeFi protocols are accessible to anyone with an internet connection, removing the barriers imposed by traditional financial institutions. This inclusivity is particularly important for individuals in regions with limited access to banking services, allowing them to participate in the global economy through decentralized application development

Transparency and Security

DeFi protocols operate on blockchain technology, which is inherently transparent and secure. Every transaction is recorded on a public ledger, making it easy to track and audit. Furthermore, the use of smart contracts reduces the risk of fraud and human error, as these contracts execute automatically based on predefined rules.

Elimination of Intermediaries

By removing intermediaries, DeFi protocols reduce costs and increase efficiency. Traditional financial services often involve multiple layers of intermediaries, each taking a fee, which can make transactions more expensive and slower. Decentralized finance protocols streamline these processes, providing faster and cheaper services.

Innovation and Flexibility

The open-source nature of DeFi protocols encourages innovation. Developers around the world can build on top of existing decentralized finance protocols, creating new financial products and services. This continuous innovation ensures that DeFi development remains at the forefront of financial technology, offering users more options and better solutions.

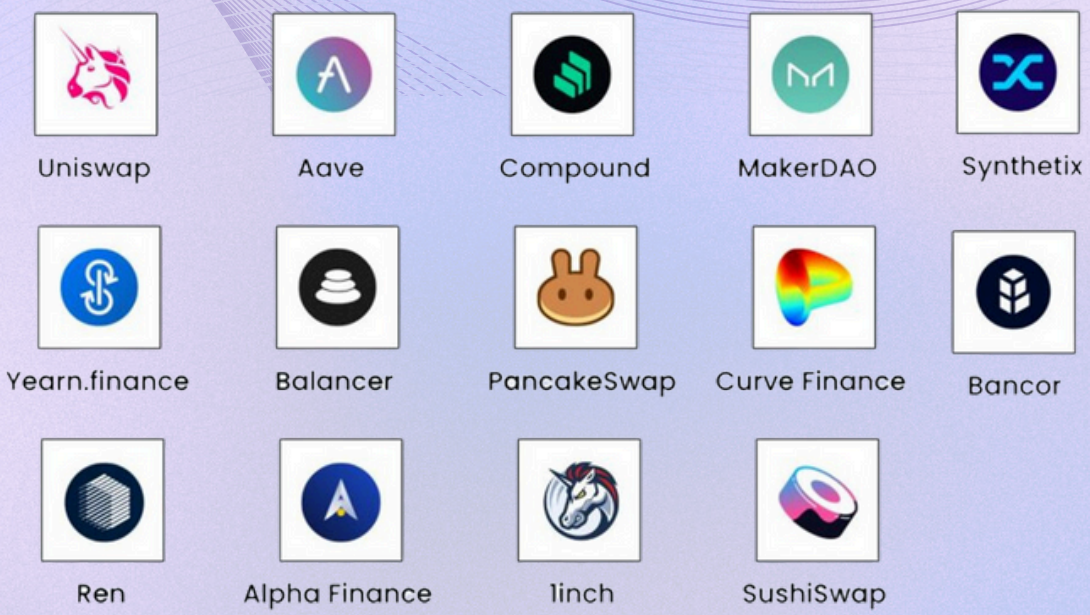
Economic Empowerment

DeFi protocols empower individuals by giving them full control over their assets. In traditional finance, funds are often held and controlled by banks or other institutions. With DeFi, users have direct ownership of their assets and can manage them independently. This empowerment extends to governance as well, where users can influence the direction of the protocols they use through decentralized governance mechanisms.

Resilience and Accessibility

DeFi protocols are designed to be resilient, operating 24/7 without the constraints of traditional banking hours. This round-the-clock availability ensures that users can access financial services whenever they need them. Additionally, the decentralized nature of these protocols means they are less vulnerable to systemic risks that can affect centralized institutions.

TOP 15 DEFI PROTOCOLS



Here are the top DeFi protocols:

Uniswap

Uniswap is a decentralized exchange protocol enabling users to swap various cryptocurrencies directly from their wallets. It operates on the Ethereum blockchain using an automated market maker (AMM) system, which facilitates liquidity without traditional order books. Users provide liquidity to trading pairs and earn fees, contributing to a decentralized trading experience.
Uniswap's innovative design has set a benchmark for AMMs, making it a crucial player in the DeFi ecosystem.

Aave

Aave stands out as a DeFi protocol for lending and borrowing. It also permits users to either lend their assets to earn interest or borrow assets using collateral. It functions on Ethereum and various other blockchains, offering a variety of services without the need for intermediaries.
Aaves standout offerings encompass flash loans, allowing users to borrow assets briefly without collateral and the flexibility to switch between stable interest rates. This makes it an attractive option in the DeFi sector.

Compound

Compound is a decentralized lending protocol that allows users to earn interest on their crypto holdings or take out loans. It operates on the Ethereum blockchain, using smart contracts to facilitate borrowing and lending transactions. Users supply assets to liquidity pools and receive interest, while borrowers pay interest on their loans.
Compound's algorithmically set interest rates and integration with various DeFi platforms make it a key component of the DeFi lending landscape.

MakerDAO

MakerDAO is a decentralized autonomous organization behind the DAI stablecoin, which is pegged to the US dollar. It uses smart contracts on Ethereum to manage the issuance and stability of DAI through collateralized debt positions (CDPs). Users can lock up collateral to mint DAI or repay debt to retrieve their collateral.
MakerDAO's governance structure allows MKR token holders to vote on protocol upgrades and changes, ensuring decentralized control over the stablecoin's stability and functionality.

Synthetix

Synthetix is a decentralized platform for creating and trading synthetic assets on the Ethereum blockchain. It allows users to trade derivatives that mimic the value of real-world assets, such as commodities, currencies, and stocks.
By utilizing a collateralized debt pool, Synthetix enables users to issue synthetic assets and participate in trading activities. Its innovative approach to derivatives trading has made it a significant player in the DeFi sector.

Yearn.finance

Yearn.finance is a yield optimization protocol designed to maximize returns on crypto assets by automatically shifting investments between different DeFi protocols. It uses automated strategies to seek out the highest yields and optimize returns for users.
The protocol includes various products like Vaults and yTokens, which enhance yield farming efficiency. Yearn.finance's ability to automate complex strategies has positioned it as a leading solution in the DeFi yield optimization space.

Balancer

Balancer is a decentralized asset management protocol that allows users to create and manage liquidity pools with multiple tokens and varying weights. It functions as both an automated market maker (AMM) and a portfolio management tool, enabling liquidity providers to earn fees based on their token weights.

Balancer's flexible pool creation and automatic rebalancing features provide users with unique opportunities for liquidity provision and portfolio management in the DeFi ecosystem.

PancakeSwap

PancakeSwap is a decentralized exchange and AMM built on the Binance Smart Chain (BSC). It offers similar functionalities to Uniswap but benefits from lower transaction fees and faster processing times due to BSC's efficiency.
PancakeSwap features a range of services, including token swaps, yield farming, and staking, and utilizes its native token, CAKE, for various incentives. Its integration with BSC has made it a popular choice for DeFi users seeking cost-effective trading solutions.

Curve Finance

Curve Finance is a decentralized exchange optimized for stablecoin trading. It focuses on providing low slippage and efficient swaps between stablecoins, leveraging its specialized AMM algorithm.
Curve's liquidity pools are designed to reduce impermanent loss, making it an attractive option for stablecoin liquidity providers. Its emphasis on stablecoin trading and innovative AMM design have established Curve Finance as a key player in the DeFi stablecoin ecosystem.

Ren

Ren is a decentralized protocol that facilitates cross-chain liquidity by enabling the transfer of assets between different blockchains. It utilizes the RenVM, a network of virtual machines, to enable seamless and private transactions across various chains.
By allowing assets to be transferred and utilized in different DeFi applications, Ren enhances interoperability and liquidity within the DeFi ecosystem. Its cross-chain capabilities make it a valuable tool for users seeking to leverage assets across multiple platforms.

Alpha Finance

Alpha Finance is a DeFi platform offering a suite of products designed to enhance yield farming and asset management. Its primary offerings include Alpha Homora, a leveraged yield farming and lending platform, and Alpha Vaults, which optimize yield strategies.
Alpha Finance aims to provide users with advanced tools and strategies for maximizing returns while managing risk. Its innovative products and focus on yield optimization have made it a notable player in the DeFi space.

1inch

1inch is a decentralized exchange aggregator that sources liquidity from various DEXes to provide users with the best possible trading rates. It uses its proprietary Pathfinder algorithm to find the most efficient routes for trades, minimizing slippage and transaction costs.
1inch's aggregation and routing capabilities enable users to execute trades with optimal efficiency and cost-effectiveness. Its role in aggregating liquidity across different exchanges has established it as a key tool for DeFi traders.

SushiSwap

SushiSwap is a decentralized exchange and AMM platform that originated as a fork of Uniswap. It offers similar functionalities with added features such as governance through the SUSHI token and additional reward mechanisms for liquidity providers.
SushiSwap's commitment to community governance and continuous development has helped it differentiate itself in the DeFi landscape. Its focus on expanding features and engaging the community has made it a prominent player in the decentralized trading space.

Bancor

Bancor is a decentralized liquidity network that allows users to trade tokens directly from their wallets without relying on traditional order books. It uses an automated market maker (AMM) model to facilitate trades and provide liquidity.
Bancor's protocol includes features like single-sided liquidity provision and impermanent loss protection, aiming to enhance user experience and liquidity efficiency. Its innovative approach to liquidity provision and trading has made it a noteworthy player in the DeFi ecosystem.

What are the most common problems DeFi is facing currently ?

- **Regulatory compliance**
- **Smart Contracts**
- **Scalibilty Issues**
- **High Volatility**
- **Security vulnerabilities**
- **Decentralization**
- **liquidity concern**
- **user experience**

How Heliosus is different and advanced from these DeFi Protocols?

Less gas Fees

During the transactions on Helios Blockchain gas fees will be so much cheap, It will connect so many users around the world because anyone can do transactions very fast and cost efficiently on Helios Blockchain

User experience

User experience of Helios Blockchain is very user friendly compared to nowadays DeFi Protocols which deals with the problems currently DeFi Protocol is facing, DeFi protocol is very complex and The Helios Blockchain solve this problem

Liquidity

With the help of Helios blockchain we can connect with any reknown Blockchain liquidity pool with the help of different network and therefore there will be no liquidity issues

Smart Contract audit

We have audit report of our DeFi platform and our Defi Platform is very safe and secure audited by reknown agencies and our project is open source we run bug bounty programs for bug bounty hunters anyone can use our product safely

Scalbilty issues

Our product is support multi blockchain any user from any country and from any reknown blockchain ecosystem can access Helios DeFi product

NFT PLATFORM

Non-fungible tokens or NFTs are a type of digital token where every token is different and hold unique characteristics. Due to the nature of the NFTs, many NFTs have varying rarity and are considered valuable in the digital asset community. Anything from games to painting and even memes can be an NFT.

Fungible Assets

The simple definition of a fungible asset states that any asset can be fungible when the units are easily interchangeable with each other. You cannot distinguish different units of one fungible asset. As a matter of fact, every unit of fungible assets has a similar market value and validity. For example, one ten-dollar bill would be equal to another ten-dollar bill in terms of value and validity. You can find other examples of fungible assets in precious metals, commodities, cryptocurrencies, fiat currencies, and bonds. On the other hand, you will also notice that an equal exchange of fungible assets doesn't mean that you have to exchange two identical units of the asset. When the transaction happens between units of the same asset with similar value and functionality, you can have an equal exchange of fungible assets. For example, you can exchange a ten-dollar bill for ten one-dollar bills. In this case, the units of dollars are involved in the exchange, and the ten one-dollar bills are equal in value to the one ten-dollar bill. Furthermore, the ten one-dollar bills would also have the same validity as the one ten-dollar bill. So, one can clearly notice how the US dollar serves as a fungible asset, with the bills providing representation for underlying value

Are cryptocurrencies fungible? You are likely to come across this question when discussing the basics of NFT. In the general sense, many cryptocurrencies are basically fungible assets. For instance, you can consider Bitcoin as a fungible asset because one unit of BTC is equal to other units. Each BTC unit would have the same functionality and quantity. The order of mining the BTC tokens does not affect the value of BTC units, and they are in the same blockchain. However, if anyone forks the blockchain to create a new type of coin, it would not be similar to Bitcoins.

Non Fungibility

With a detailed understanding of fungible tokens, one could easily ascertain that non fungible tokens would be the opposite of the same. Non fungible assets are not interchangeable with each other and have unique properties that separate them from each other. Even if NFTs may look similar in some aspects, there are many prominent differences between them. Some of the notable examples of non-fungible items in the real world include concert tickets and artwork. Even if two concert tickets are the same in terms of design, a front-row ticket would have more value than a back-row ticket. Similarly, two paintings may look similar, albeit with certain rare elements differentiating them

How NFT Works?

- Blockchain Platform
- oken Standard
- Key Characteristics
- Value Creation
- Marketplace and Wallet

Blockchain Platform

NFTs use public blockchain platforms to function. At this time, Ethereum is the most popular public platform that many of the NFT projects are using for storing or minting NFTs. Other platforms such as NEO, TRON, or EOS blockchain platforms are also capable of creating NFTs. All information regarding NFTs is stored on the ledger. File links, owner's identity, metadata, date of creation, unique characteristics are stored on the ledger. Typically, only the creator of the NFT can select the scarcity level of the NFT. As the blockchain platform is immutable, no one can duplicate or delete NFTs from the ledger once it gets added. Due to using blockchain, transparency regarding NFT ownership is high, as anyone can see the ownership status.

Token Standard -

ERC-721 It's a non-fungible token standard that defines the process of creating an NFT on the Ethereum platform. It allows users to manage, own and trade NFTs and can also represent asset ownership. ERC-721 is one of the common Ethereum token standards used in developing NFTs.

Token Standard -

ERC-1155 ERC-1155 token standard is a multi-token standard, which means developers can use it to develop NFTs, fungible tokens, or any other form of tokens. It allows users to create various tokens using a single contract. This token standard also requires less computational power.

Key Characteristics

- Indivisibility
- Rarity
- Uniqueness
- Ownership
- Transparency
- Interoperability

Indivisibility You can't divide NFTs. It means you can't divide a single token into multiple smaller tokens. Therefore, users can't partially own an NFT or even sell an NFT. Users can only own a full NFT, and only a single person can own that NFT.

- **Rarity Need to be rare. This attribute is necessary as it drives their value in the Marketplace. Creators need to keep in mind that they can develop many NFTs, but they need to maintain a limit to promote scarcity.**

- **Uniqueness NFTs have to be unique. This means that every single token will come with individual characteristics that will differ from one another. Therefore, you can't interchange one NFT with another as they don't have similar traits.**

- **Ownership NFTs come with ownership status. Creators will have full control over the NFTs they are minting. Anyone buying the NFT will own it, but the original creator will remain the copyright. In any case, the owner is free to transfer their NFTs to any other account. In that case, the ownership status will change.**

- **Transparency As NFTs use public blockchain platforms, they are fully transparent. It means every transfer or activity, or ownership status is public on the ledger. This attribute is necessary as it helps the NFTs to create trust.**

- **Interoperability You can create or buy NFTs on various blockchain platforms or even DLT based platforms. Therefore, you can buy NFT from one platform and sell it on another. It improves their interoperability and liquidity.**

- **Value Creation The value of an NFT depends on the uniqueness of that NFT and the creator's profile. Companies with high brand value and famous creators will drive more value to their NFTs. Other than this, the utility of the NFT can also increase the pricing. A creator of an NFT will get sole copyright and can duplicate their work as much as they want. Duplicated NFTs are considered unique but will not have a similar value as the original one. The creator also gets royalties. The buyer of an NFT will get a license to display the NFT and can even resell it. But they can't make changes or duplicate the NFTs.**

Marketplace and Wallet

- To mint or store their NFTs, you will need to have an NFT wallet. Without a blockchain or NFT wallet, you can’t store your NFTs.
- These wallets can safely store all your NFTs in one place. However, you need to choose a wallet that supports your NFTs.
- NFT marketplaces allow users to buy and sell their tokens on the platform. In some cases, users can mint new tokens on the platform.
- Not all marketplaces support every type of NFT. These marketplaces offer lifetime royalties to the creators for every resell.
- NFT marketplaces face many problems, including high fees, fraud, and copyright issues.

Fees

- High and hidden fees: There are many fees associated with NFT marketplaces, including listing, sale, and withdrawal fees.
- Gas fees: These are costs associated with processing transactions on the blockchain.

Fraud

- ·Scams: There is a risk of fraud and scams, including imitations of original NFT stores.
- Asset tokenization: The asset tokenized by the NFT may be nonexistent, duplicated, or tainted.

Copyright

- Defective copyright protection: Images and other tokens can be easily duplicated and spread throughout the internet without the creators' consent.

Scalability

- Congestion: As the number of transactions grows, blockchain networks can become congested, leading to slow transaction processing times and high fees.

Other problems

- Poor user experience: Some NFT marketplaces have poor user experience.
- Limited payment methods: Some NFT marketplaces have limited payment methods.
- Volatile prices: Prices of NFTs can be volatile, leading to fluctuations in value.
- Iliquidity: The illiquidity of the market makes it challenging to participate in the NFT market.

How Helios NFT Marketplace solving this problem

- **Listing and transaction fees**
- **Platform build on our Helios Blockchain can do listing, selling with minimal fees our platform fees is very minimal with comparisons to open sea, raible, sorare.**
- **Multi Blockchain support**
- **Our NFT Marketplace is supported by many Blockchains, Users from different blockchain ecosystem can buy and sell their NFTs No Congestion**
- **We have noticed when big project NFTs comes in market then fees of minting NFTs increases and normal users cant trade their NFTs But Helios blockchain build a Futuristic and secure platform where fees will not rise during Congestion**
- **Copyright protection**

NFTs cant be transferred without the permission of authentic creator

WALLETS

Crypto wallets are a type of digital wallet specifically used for storing digital currencies. These are basically applications that can help you access blockchain platforms and help you retrieve and use your crypto assets. However, crypto wallets technically do not store digital currencies like your physical wallets. It helps to connect to the blockchain platform that stores your assets.

Importance of Crypto Wallets

- **Offers complete ownership of crypto assets**
- **Offers personalized security for asset safekeeping**
- **Provides faster access and transaction**

Crypto wallet security issues
In recent years, crypto wallets have evolved beyond their traditional functionalities — which include storing wallet secrets securely, signing transactions and communicating with dApps — and are now becoming more feature-rich to appeal to their users.
But as their functionalities expand, so do the risks. Specifically, attack surfaces broaden and the sophistication of potential threats to their security increases.

Poor Coding Practices

There is no surprise that poor coding practices can leave the door open to security exploits at that application/implementation level. Risks stemming from poor coding practices can include:
· Cross-site scripting (XSS) attacks
· Man-in-the-middle (MITM) attacks
· Remote code execution vulnerabilities
· Misconfigurations leading to security missteps
· Using unsafe functions or improper error reporting, potentially triggering leaks of sensitive information

Improper Cryptography

Cryptography is a critical component of custodial wallets, providing essential security features. Wallets that fail to implement strong cryptographic practices expose users to significant risks.
Some common cryptographic issues observed in wallet extensions include:

- **·Weak Storage Schemes: Inadequate storage methods for sensitive data expose wallets to significant risks. This applies particularly to browser localStorage, which can be vulnerable to various attacks due to its reliance on web browsers' native storage systems.**
- **Encrypting Multiple Fields with the Same Password: This practice exposes user data if an attacker obtains a single password, as all associated information becomes accessible simultaneously.**
- **Poor or Improper Key Derivation Choices: Weak key derivation methods can compromise wallet security, making it easier for hackers to crack the encryption and access sensitive data.**
- **Allowing Low-Entropy User Passwords: This practice enables attackers to exploit weak passwords, increasing the risk of unauthorized access.**

3Third-Party Vulnerabilities
Denial of Service (DoS) Attacks primarily target third-party sources relied upon by wallet extensions.
4. User Authentication Issues
Aside from cryptographic security measures, user authentication plays the most critical role in maintaining wallet security.
5. Secure Handling of Data
Since non-custodial wallets need to store sensitive data locally, proper handling of this information is crucial for maintaining user privacy and security. Extensions often use localStorage (e.g., LevelDB), a file-based key-value storage system, to save data on users' devices.

6. Platform-Specific Issues
The security of a crypto wallet is closely tied to the platform it runs on — whether web, mobile, or desktop. Ensure that the chosen platform follows best practices and offers robust security features. Regularly review platform-related security updates to stay informed about potential vulnerabilities and fixes.

How Helios wallet is Secure and advanced

Helios solve users authenticated issues
Some important security measusers supported by Helios wallet
· Password Management Policies: Implementing robust policies that govern password usage can help prevent unauthorized access and improve overall account protection.
· Authenticating Critical Actions: Ensuring that essential operations, such as transferring funds or executing smart contracts, require multi-factor authentication (MFA) offers added security.
· Protecting Against Brute Force Attacks: Implementing measures such as account lockouts or delays after multiple failed login attempts can deter attackers from exploiting weak passwords.
· Support for Two-Factor Authentication (2FA) and Hardware Wallets: Encouraging users to adopt these advanced security features can significantly reduce the risk of unauthorized access

Our Helios wallet support secure data encryption practices
Always Encrypt Local Data: Ensure that all critical wallet data, such as mnemonics and private keys, are encrypted using strong cryptographic algorithms. Implementing proper encryption methods helps protect users' financial assets from theft or unauthorized access.
Encryption at Rest: For sensitive information stored on devices, utilize robust encryption mechanisms like AES-GCM to safeguard data both in transit and at rest.

- **Key Management: Implement secure key management practices, such as using strong encryption algorithms, regularly rotating keys, and employing proper access controls for sensitive data.**

- **Secure Backup and Recovery Options: Offer users safe methods to create backups of their wallets without exposing sensitive information or compromising security.**

- **Support for Two-Factor Authentication (2FA) and Hardware Wallets: Encourage users to adopt these advanced security features, which can significantly reduce the risk of unauthorized access.**

- **Our Helios wallet solves supply chain risk .Assess Dependencies Carefully: Manually review dependencies and their transitive dependencies to identify potential vulnerabilities in the codebase. Even devDependencies can cause a lot of damage.**

- **Pin Dependencies: Pinning dependencies helps prevent unauthorized changes that could introduce security flaws or malicious code into the wallet application.**

- **Use Automated Tools for Auditing Dependencies: Implement continuous integration (CI) and continuous delivery (CD) pipelines to automatically scan and audit third-party libraries during development phases, ensuring they are up-to-date and secure.**

How Helios Communicate with DApps

Secure Communication Protocols: Use encryption protocols to protect data in transit, preventing unauthorized access or tampering during transmission.
Authenticating dApp Interactions: Establish robust authentication mechanisms between the wallet and connected dApps to verify their legitimacy and prevent potential phishing attacks.
Regularly Update InteMonitor dApp Activity: Continuously monitor wallet interactions with integrated dApps for suspicious patterns that might indicate fraudulent behavior or attacks targeting user assets
grated dApp Lists: Keep track of known security vulnerabilities in popular dApps — and update your wallet's integration list accordingly — to protect users from exploitation or financial loss due to malicious activities.

HELIOS EXCHANGE

Native Token/Utility:

We Introduced an intrinsic digital token HELT specific to our centralized exchange platform development to increase user engagement and encourage active participation, enhancing the ecosystem's overall life.
Automated Market-Making Bot: With an autonomous market-making bot, we can provide bid-ask spread management around the clock, ensuring trade efficiency and minimizing price slippage. Incorporate this function into creating cryptocurrency exchanges to generate order books with substantial liquidity.

Fiat On/Off-Ramp:

Establish essential channels to enable seamless on-chain fiat to cryptocurrency conversions on our Helios centralized exchange via bank accounts, credit/debit cards, Apple pay, Google Pay, and others.
External Liquidity Module: Helios Exchange Work with a reputable centralized crypto exchange development company to combine order books, liquidity, and pertinent information about various trading pairs from several third-party trading platforms to enable smooth trading.
Airdrop: We can provide strong marketing plan. Utilize airdrop to give out free tokens or virtual currency to numerous people at once for reward schemes and marketing campaigns.

Multilingual Platform:

Enable Helios Exchange users to interact with the platform in the language of their choice, facilitating trade, communication, and navigation for various linguistic backgrounds.

Admin Support:

Helios provide a crucial component that raises clients' confidence in a transaction is customer support. Collaborate with a centralized crypto exchange development business to automate the settlement of issues by utilizing chatbots or human help chat. This will enable users to communicate directly with Helios Exchange platform administrators or support teams.
Multi-Role Access: Provide different user groups with varying levels of privileges and permissions to the platform, such as moderators, sub-administrators, and super administrators.

Crypto Arbitrage Bot

We incorporate a crypto arbritage bot into our platform, we worked with the development team of our centralized cryptocurrency exchange slt allows users to take advantage of price differences between two trading venues by simultaneously buying and selling a digital asset in two different markets.

Staking:

Helios provide a necessary staking module in the creation of your centralized crypto exchange to allow customers to lock their cryptocurrency on the platform and earn passive revenue through both

Fixed and flexible staking.

Prepaid Cards: By providing fiat or cryptocurrency prepaid cards, customers can spend their digital money at both physical and online establishments, replicating the functionality of traditional debit cards.

(OTC) Trading:

To incorporate an OTC trading module into your trading platform, collaborate with a centralized crypto exchange development business. By enabling the immediate execution of sizable orders outside of standard exchange order books, it shields institutional investors from paying for slippage.

Merchant Payment Gateway:

Provide interested entrepreneurs with the ability to accept cryptocurrency payments by adding a payment option to their line of business.
Crypto Loans: The Helios exchange platform, allow customers to borrow money against the cryptocurrency assets they have locked up as collateral. This will enable them to obtain liquidity without having to sell their holdings.

Launchpad

Helios is including many launchpad platform in your centralized crypto exchange, you can open up profitable investment prospects for investors and fundraising opportunities for entrepreneurs.
Copy-Trade: By copying the trading strategies of seasoned traders and automating transactions using a platform that logs and shows trends and performance, copy trading enables users to make more significant gains.
Crypto Betting Module: With a well-designed crypto-betting capability, Helios enable customers to gamble speculatively on price fluctuations and enjoy a simplified, transparent, quick, and safe

betting experience.

User Chat: We Include a user chat feature in our centralized crypto exchange development to allow users to interact and communicate directly with one another via a real-time messaging interface that fosters community building and increases engagement.

Copy-Trade

By copying the trading strategies of seasoned traders and automating transactions using a platform that logs and shows trends and performance, copy trading enables users to make more significant gains.

Crypto Betting Module

With a well-designed crypto-betting capability, Helios enable customers to gamble speculatively on price fluctuations and enjoy a simplified, transparent, quick, and safe betting experience.

User Chat

We Include a user chat feature in our centralized crypto exchange development to allow users to interact and communicate directly with one another via a real-time messaging interface that fosters community building and increases engagement.

Price Alerts

we enable users to set up personalized push alerts for particular cryptocurrency price levels, it may help consumers manage their money and positions more skillfully.

Lending and Borrowing

We Added a lending and borrowing module to our centralized exchange development to enable fast admin-to-user or peer-to-peer crypto loans.

VIP Accounts:

Provide specific clients unique advantages and rights, such as reduced costs, priority support, access to premium services, etc., provided they fulfill certain requirements.

Grid Trading:

By including a grid trading bot in Helios centralized crypto exchange, user may enable traders to automate their trades based on established grid criteria.

Margin Spot Trading Module:

Increase our revenue streams by allowing traders to leverage borrowed money from exchange administrators or other brokers to increase their positions.

Derivatives and Perpetual Futures Trading:

By enabling derivatives and perpetual contract trading, dealers can profit from upward and downward market swings.

Legal Disclaimer

White Paper Disclaimer

This means that the development and roll-out of all the features of the platform as described in this white paper are not guaranteed. Regulatory licenses or approvals may be required in a number of relevant jurisdictions in which relevant activities may take place. It is not possible to guarantee, and no person makes any assurances, that any such licenses or approvals will be obtained within a particular timeframe or at all. This means that features of the Helios platform may not be available in certain markets, or at all. This could require the restructuring of the Helios platform or result in its unavailability in all or certain respects. Helios reserves the right to revise this white paper from time to time at its sole discretion. Any revisions to this white paper will be made available on Helios's website.