Sphinx Whitepaper

By Ayomide I. Daniels and Damola Akindolire

Version: v1.0

Abstract

This paper provides an architectural overview of the first release of the Sphinx Network, titled “Alpha Superion”, with a native token “NHX”.

Disclosure

The information described in this paper is preliminary and subject to change at any time. Furthermore, this paper may contain forward-looking statements.

Forward-looking statements relates to our future performance. This includes, but is not limited to, Sphinx’s projected performance; the expected development of its business and projects; execution of its vision and growth strategy; and completion of projects that are currently underway, in development or otherwise under consideration. Forward-looking statements represent our management’s beliefs and assumptions only as of the date of this presentation. These statements are not guarantees of future performance and undue reliance should not be placed on them.

Such forward-looking statements necessarily involve known and unknown risks, which may cause actual performance and results in future periods to differ materially from any projections expressed or implied herein. Sphinx undertakes no obligation to update forward-looking statements.

Although forward-looking statements are our best prediction at the time they are made, there can be no assurance that they will prove to be accurate, as actual results and future events could differ materially. The reader is cautioned not to place undue reliance on forward-looking statements.

1. Introduction

Bitcoin and other distributed transaction systems aim to provide a decentralized system for making and verifying transactions. However, for traditional blockchains, including Bitcoin, decentralization comes at the cost of scalability as each node needs to process the entire system history upon joining the network. Bitcoin's blockchain is over 300GB and contains over 550M transactions.

This paper provides an architectural overview of the Sphinx Network. The key focus is on three key differentiators of the platform: the engine, the architectural model, and the governance mechanism. The goal is to design a decentralized technology that offers efficient verification of system history from genesis without relying on connection outside of its subnet. To provide verification time constant (O(1)) in the number of transactions.

2. Goals and Principles

Due to deficits across Africa, especially in Infrastructure and Access, Africa has not really been a major player in the field of Blockchain and/or Decentralization, although it has one of the fastest and highest adoption rates but the West and Asia are the powerhouse of this paradigm shift. To ensure Africa isn't just yet another consumer in this space, we at Sphinx Foundation have been researching and engineering a better way that is able to scale and adapt to the particularity of the African continent, to ensuring Decentralization Technology isn't just put in the right hands but in the hands of every African interested in this tectonic shift.

The Sphinx Network is a really robust network primarily and not limited to handheld devices, Africa can leapfrog web 2.0 (servers requiring lots of energy) to web 3.0 (i.e. devices requiring less CPU to process and/or validate transactions and with equally strong security as with current PoW decentralization technologies) powering the next one million-priority Decentralized Finance and Decentralized Apps built specifically for the 1bn+ people in Africa. The Sphinx Network aims to achieve the scalability, interoperability (including with centralized systems), and sustainability needed for real-world applications. It is designed to be the platform of choice for the large-scale, mission-critical DeFIs and DApps that will drive the economy of the future for the African, and Middle-Eastern Region.

Sphinx is a high-performance, scalable, customizable, and secure blockchain network. It targets three broad use cases:

a. Creation and foolproof of identity information of individuals, organizations, and entities in electronic for.
b. Building highly scalable and decentralized applications.
c. Building complex digital assets with custom rules, agreements, and policies.

The overarching aim of Sphinx is to provide a unifying platform for the creation, transfer, and trade of digital assets.

By intentional design, Sphinx possesses the following properties:

1. **Scalable** Sphinx is designed to be massively scalable, robust, and efficient. The core consensus engine is able to support a global network of potentially hundreds of millions of internet-connected, low and high powered devices that operate seamlessly, with low latencies and very high transactions per second.
2. **Decentralized** Sphinx is designed to provide unprecedented decentralization. This implies a commitment to multiple client implementations and no centralized control of any kind.
3. **Governable and Democratic** Sphinx is a highly inclusive platform, which enables anyone to connect to its network and participate in validation and first-hand in governance. Any token holder can have a vote in selecting key financial parameters and in choosing how the system evolves.

4. **Faster speeds** Because each transaction isn't individually verified, but rather batches of transactions are verified together, Sphinx can process many more transactions in a shorter amount of time. Testing demonstrated that it could handle over 15,000 self-custodial transactions per second, which is orders of magnitude better than native Ethereum, with Sphinx, 15,000 is not the cap limit: in fact, blockchain resources are no longer the bottleneck for Sphinx capacity - rather, it is the magnitude of the prover service in the cloud, which determines its throughput.
5. **Interoperable and Flexible** Sphinx is designed to be a universal and flexible infrastructure for a multitude of blockchains/assets, where the base NHX is used for security and as a unit of account for exchange. The system is intended to support, in a value-neutral fashion. The platform is designed from the ground up to make it easy to connect and interoperate with existing blockchains.
6. **Speeding Up DeFi Transactions** Visa, one of the most popular electronic platforms powering payments, can enable up to 24,000 transactions per second. In contrast, Bitcoin can do around 7 transactions per second and Ethereum can support 15 transactions per second. For decentralized finance (DeFi) and decentralized apps (DApps) to reach the same widespread use and versatility as conventional online payment platforms, it's important that they are capable of scaling in the same way and aren't hindered by speed and efficiency concerns. Particularly for exchanges that support transactions from thousands of users daily, it's important to find secure, efficient ways to record data and broadcast it across the network of nodes. Additionally, exchanges need liquidity in order to support the scale of their operations; slow transaction speeds compromise liquidity, so it's necessary to find a faster alternative. The core underlying reason that slows down networks like Bitcoin and Ethereum is Inclusive Accountability - the principle that says each and every individual connected to the internet must be allowed to verify the integrity of the whole blockchain, using a laptop. This puts a severe limitation on scaling the system (say, 100x), as Visa would easily do (by purchasing larger computers). The problem of blockchain scalability is not novel —– people have been trying to tackle it for a while. Some popular approaches use modified consensus algorithms, but often run into the issue of trading too much security for efficiency. Another popular solution is the Lightning Network, often dubbed a "second-layer" solution, which speeds up transactions with off-chain payment channels and broadcasts a final history of transactions to the entire network after some period of time. Still, the underlying proof and verification protocols for Lightning and other consensus algorithms are computationally expensive, creating delays.

3. The Engine

The Sphinx Network begins with the core component which powers the platform, the consensus engine.

1. **Background** Distributed payments and – more generally – computation, require agreement between a set of machines. Therefore, consensus protocols, which enable a group of nodes to achieve agreement, lie at the heart of blockchains, as well as almost every deployed large-scale industrial distributed system. The topic has received extensive scrutiny for almost five decades, and that effort, to date, has yielded just two families of protocols: classical consensus protocols, which rely on all-to-all communication, and Nakamoto consensus, which relies on proof-of-work mining coupled with the longest-chain-rule. While classical consensus protocols can have low latency and high throughput, they do not scale to large numbers of participants, nor are they robust in the presence of membership changes, which has relegated them mostly to permissioned, mostly static deployments. Nakamoto consensus protocols on the other hand, are robust, but suffer from high confirmation latencies, low throughput, and require constant and high energy expenditure for their security. The Sphinx protocol combines the best properties of classic consensus protocols with the best of Nakamoto consensus. Based on a lightweight network sampling mechanism, they achieve low latency and high throughput without needing to agree on the precise membership of the system. They scale well from hundreds to thousands of participants with direct participation in the consensus protocol. Further, the protocols do not make use of PoW mining, and therefore avoid its exorbitant energy expenditure and subsequent leak of value in the ecosystem, yielding lightweight, green, and quiescent protocols.
2. **Mechanism and Properties** The Sphinx protocols operate by repeated sampling of the network. Each node polls a small, constant-sized, randomly chosen set of neighbors, and switches its proposal if a supermajority supports a different value. Samples are repeated until convergence is reached, which happens rapidly in normal operations. We elucidate the mechanism of operation via a concrete example. First, a transaction is created by a user and sent to a validating node, which is a node participating in the consensus

procedure. It is then propagated out to other nodes in the network via gossiping. What happens if that user also issues a conflicting transaction, that is, a doublespend? To choose amongst the conflicting transactions and prevent the doublespend, every node randomly selects a small subset of nodes and queries which of the conflicting transactions the queried nodes think is the valid one. If the querying node receives a supermajority response in favor of one transaction, then the node changes its own response to that transaction. Every node in the network repeats this procedure until the entire network comes to consensus on one of the conflicting transactions.

3. **Dynamic, and Self-healing** In public PoS (Proof of Stake) systems, if a validator does not produce blocks at their assigned slots, they are generally slashed as a punishment. Also, in public networks the number of validators is relatively large. Even if a couple of them skip their slot, the average block period is not impacted too much. In case of permissioned PoA networks this is a bit tricky as we don't have the concept of slashing (or staking for that matter), and the count of validators is relatively smaller. Even if one of them skips their slot and goes offline, it impacts the block period by quite a bit and that results in latency and bad user experience. The Sphinx protocol solves this problem by removing the offline authorities out of the active set, and then the network would not wait for them to produce blocks. Their slots would be redistributed among other authorities. The average block time would then recover.
4. **Adaptive** Unlike other voting-based systems, Sphinx Protocol achieve higher performance when the adversary is small, and yet highly resilient under large attacks.
5. **Asynchronously** Sphinx Protocol, unlike longest-chain protocols, do not require synchronicity to operate safely, and therefore prevent double-spends even in the face of network partitions. In Bitcoin, for example, if synchronicity assumption is violated, it is possible to operate to independent forks of the Bitcoin network for prolonged periods of time, which would invalidate any transactions once the forks heal.
6. **Low Latency** Most blockchains today are unable to support business applications, such as trading or daily retail payments. It is simply unworkable to wait minutes, or even hours, for confirmation of transactions. Therefore, one of the most important, and yet highly overlooked, properties of consensus protocols is the time to finality. Sphinx Protocol reach finality typically in ≤ 1 second, which is significantly lower than both longest-chain protocols and sharded blockchains, both of which typically span finality to a matter of minutes.
7. **High Throughput** Sphinx Protocol, reach thousands of transactions per second (20,000+ tps), while retaining full decentralization and security. Higher performance results (45,000+

tps) can be achieved through assuming higher bandwidth provisioning for each node and dedicated hardware for signature verification.

4. Architecture

We provide the architectural overview of the network and various implementation details.

1. **Subnets** A subnet, is a dynamic set of validators working together to achieve consensus. A validator may be a member of arbitrarily many subnets. A subnet decides who may enter it, and may require that its constituent validators have certain properties. The Sphinx Network supports the creation and operation of arbitrarily many subnets. In order to create a new subnet or to join a subnet, one must pay a fee denominated in “NHX”. The Sphinx network is made up of subnets that consists nodes, node blocks are stored as a Sphinx-Trinity Tree (a modified version of the Merkle Tree); this is how we are able to create a full proof self-custody distributed and decentralization network that is also independent of other subnets or nodes at the same time should a certain or larger percentage of the network goes offline or down. All subnets are connected to one-another by agents that are delegated by the subgraph itself through the PoS / PoA Consensus Mechanism.

5. Monetary Policy

The native token “NHX” has an unlimited supply with a limit of 19.7m tokens per-year, and has the following but not limited to usecases:

a. **Payments** True decentralized peer-to-peer payments are largely an unrealized dream for the industry due to the current lack of performance from incumbents. “NHX” is as powerful and easy to use as payments, allowing thousands of transactions globally every second, in a fully trustless, decentralized manner with lower fees.
b. **Staking** Securing the System On the Sphinx Network,. In order to validate, a participant must lock up coins, or stake. Validators, sometimes referred to as

stakers, are compensated for their validation services based on staking amount and staking duration, amongst other properties.

c. **Atomic Swaps** Besides providing the core security of the system, the “NHX” token serves as the universal unit of exchange. From there, the Sphinx Network will be able to support trustless atomic swaps natively on the platform enabling truly decentralized exchanges of any type of asset directly on Sphinx.

6. Governance

Governance is critical to the development and adoption of any platform because – as with all other types of systems – Sphinx will also face natural evolution and updates. “NHX” provides on-chain governance for critical parameters of the network where participants are able to vote on changes to the network and settle network upgrade decisions democratically. This includes factors such as the minimum staking amount, minting rate, as well as other economic parameters. This enables the platform to effectively perform dynamic parameter optimization through a crowd oracle. Only a pre-determined number of parameters can be modified via governance, rendering the system more predictable and increasing safety. Further, all governable parameters are subject to limits within specific time bounds, introducing hysteresis, and ensuring that the system remains predictable over short time ranges.

A workable process for finding globally acceptable values for system parameters is critical for decentralized systems without custodians. Sphinx can use its consensus mechanism to build a system that allows anyone to propose special transactions that are, in essence, system-wide polls. Any participating node or subnet(s) may issue such proposals.

7. Pruning

Many blockchain platforms, especially those implementing Nakamoto consensus such as Bitcoin, suffer from perpetual state growth. This is because – by protocol – they have to store the entire history of transactions. However, in order for a blockchain to grow sustainably, it must be able to prune old history. This is especially important for blockchains that support high performance. Pruning is simple in the Sphinx Protocol.

Unlike in Bitcoin (and similar protocols), where pruning is not possible per the algorithmic requirements, Sphinx nodes do not need to maintain parts of the chain that are deep and highly committed. These nodes do not need to prove any past history to new bootstrapping nodes, and therefore simply have to store active state, i.e. the current balances, as well as uncommitted transactions.

8. Clients

Sphinx supports three different types of clients: core, full, and light. Core nodes store the entire history of the Sphinx subnets, the staking subnets, and the smart contract subnest, all the way to genesis, meaning that these nodes serve as bootstrapping nodes for new incoming nodes. Core nodes are typically machines with high storage capabilities that are paid by other nodes when downloading old state.

Full nodes, on the other hand, participate in validation, but instead of storing all history, they simply store the active state (e.g. current UTXO set). Finally, for those that simply need to interact securely with the network using the most minimal amount of resources, Sphinx supports light clients which can prove that some transaction has been committed without needing to download or synchronize history.

Light clients engage in the repeated sampling phase of the protocol to ensure safe commitment and network wide consensus. Therefore, light clients in Sphinx provide the same security guarantees as full nodes.

9. Sharding

Sharding is the process of partitioning various system resources in order to increase performance and reduce load. There are various types of sharding mechanisms. In network sharding, the set of participants is divided into separate subnets as to reduce algorithmic load; in state sharding, participants agree on storing and maintaining only specific subparts of the entire global state; lastly, in transaction sharding, participants agree to separate the processing of incoming transactions.

In Sphinx Protocol, the first form of sharding exists through the subnets functionality. For example, one may launch a gold subnet and another real-estate subnet. These two subnets can exist entirely in parallel. The subnets interact only when a user wishes to buy real-estate contracts using their gold holdings, at which point Sphinx will enable an atomic swap between the two subnets.

10. Platform Usecases

The Sphinx Platform has the following but not limited to usecases (and with the lowest average fee per transaction):

a. **Currency** Make your own cryptocurrency on top of the Sphinx blockchain with your own governance rules and regulations.
b. **Payments** Inter-connected native access to crypto, fiat, and CBDC currencies for ease of cross-border and p2p payments.
c. **Assets Tokenization** Issue digital tokens for either digital or physical assets for the provision a higher level of liquidity via smart contracts.
d. **Digital Identity** Create identity information of individuals, organizations, and entities in electronic form. For efficient functioning of digitization of assets.
e. **Decentralized Apps** Create decentralized applications, contracts, or organizations that operate entirely on the blockchain with Javascript, Solidity and without code with the easy-to-use Sphinx Studio no-code interface for non developers.
f. **Financial Derivatives** Speculate on financial assets at high leverage, or use hedging to protect yourself from volatility.
g. **Non-Fungible Tokens (NFT)** Create NFT applications that allow anyone to mint and trade digital artwork.

11. Conclusion

In this paper, we discussed the architecture of the Sphinx Network. The Sphinx Network is lightweight, interoperable, fast, scalable, secure, and efficient. The native token, which serves for securing the network and paying for various infrastructural costs is simple and backwards compatible. “NHX” has capacity beyond other proposals to achieve higher levels of decentralization, resist attacks, and scale to thousands of nodes without any quorum or committee election, and hence without imposing any limits to participation.

11. Reference

1. Bitcoin: bitcoin/bitcoin (Oct 2018), https://github.com/bitcoin/bitcoin
2. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008).
3. Sam Fisher, Jakob Hautop, and Omri Ross; A Trustless Exchange for Digital Assets (2017).
4. Buttolph, S., Moin, A., Sekniqi, K., Sirer, E.G.: Avalanche white paper (2019).
5. Douceur, J.R.: The sybil attack. In: International Workshop on Peer-to-Peer Systems. pp. 251–260. Springer (2002).
6. OmiseGO Team Joseph Poon: Decenteralized Exchange and Payments Platform (2017).
7. Eyal, I., Gencer, A.E., Sirer, E.G., van Renesse, R.: A scalable blockchain protocol. In: 13th USENIX Symposium on Networked Systems Design and Implementation, NSD (2016), https://www.usenix.org/conference/nsdi16/technical-sessions/presentation/eyal
8. Wood, G.: Ethereum: A secure decentralised generalised transaction ledger (2014)