2021

RESEARCH PAPER

# Syscoin NEVM

By

## House of Chimera

@HouseofChimera

*All rights reserved*

# DISCLAIMER

*All rights reserved*



# Financial Disclaimer

The content is for informational purposes only, and you should not construe any such information or other material as legal, tax, investment, financial, or other advice. Nothing contained in the research paper constitutes a solicitation, recommendation, endorsement, or offer by House of Chimera or any third party service provider to buy or sell any securities or other financial instruments in this or any other jurisdiction in which such solicitation or offer would be unlawful under the securities laws of such jurisdiction.

All content of the research paper is information of a general nature and does not address the circumstances of any particular individual or entity. Nothing in the research paper constitutes professional and/or financial advice, nor does any information on the research paper constitute a comprehensive or complete statement of the matters discussed or the law relating thereto. House of Chimera is not a fiduciary by any person's use of or access to the research paper. You alone assume the sole responsibility of evaluating the merits and risks associated with the use of any information or other content of the research paper before making any decisions based on such information. In exchange for using the research paper, you agree not to hold House of Chimera, its affiliates, or any third-party service provider liable for any possible claim for damages arising from any decision you make based on information or other content made available to you through the research paper.

## Investment disclaimer

House of Chimera is an independent blockchain research and advisory firm. We value our integrity and transparency as one of our core values. Therefore, we are fully transparent about our holdings and personal interests within Syscoin. House of Chimera is not holding a financial position within the Syscoin ecosystem but has been compensated for our services. The integrity of House of Chimera has not been compromised through the research process, as the Syscoin team did not influence the research outcome at any stage.

All rights reserved

# INTRODUCTION

*All rights reserved*



# Introduction to Syscoin' Network Enhanced Virtual machine (NEVM)

Syscoin is a public decentralized high-performing blockchain network. The ecosystem solves the blockchain trilemma (i.e. the challenge of developing a secure, decentralized, and fast blockchain ecosystem) by having a four-layer tech stack. The implications of these layers will be highlighted in the "Syscoin Tech stack" chapter.

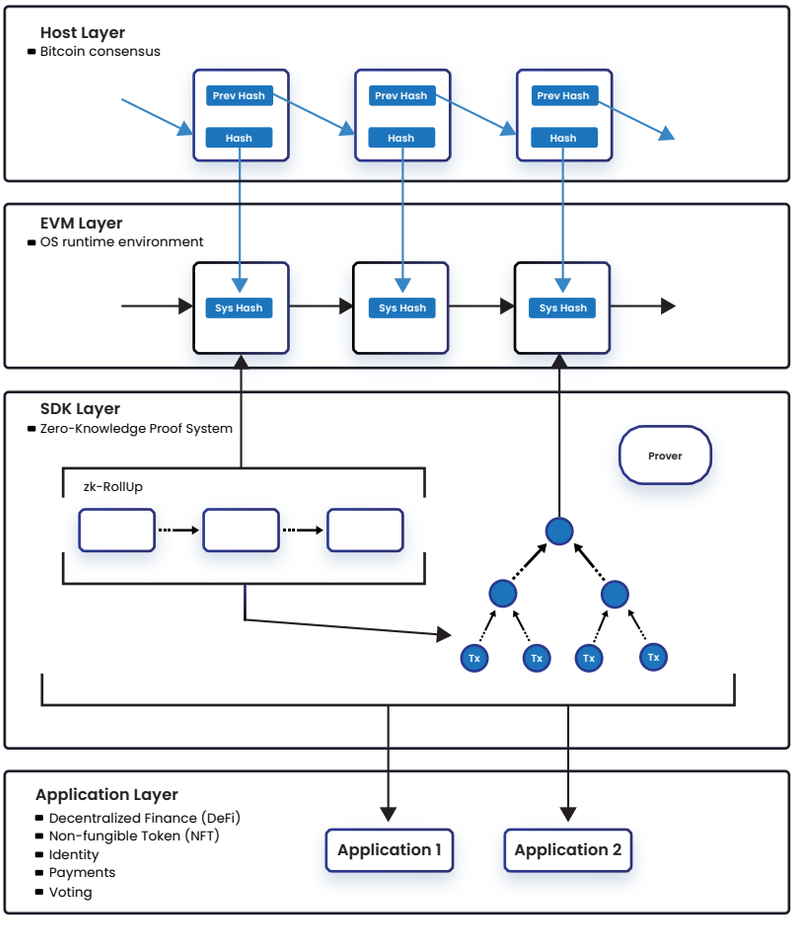
The upcoming NEVM update will have a significant role within the four-layer tech stack and is expected to be one of the most significant updates on the Syscoin ecosystem. The significance of the NEVM release will be highlighted in the "What is NEVM?" chapter. Besides the implications, there are a dozen of capabilities that NEVM will allow developers to capitalize on. Scalability allows developers to deploy more complex products and utilize the ecosystem without any financial constraints. The scalability, security, and interoperability implications of NEVM will be discussed in the chapter "Implications of NEVM".

## Syscoin' Tech Stack

A tech stack is defined as the collection of technologies an organization utilizes to build an application. The Syscoin tech stack consists of 4 layers (Figure 1). Syscoin is being used as the host layer, with Bitcoin as a consensus method, which provides an efficient foundation. On top of that, an EVM layer is being used as the operating layer as Ethereum is widely adopted. The third layer is a software development kit layer (SDK) that will allow Zero-Knowledge proofs. The last layer consists of an application layer, either vertical or applications applying the above SDK to define business goals.

To understand the NEVM and its implications, the four-layer tech stack of Syscoin has to be explained and interpreted. Therefore, Syscoin's four-layer tech stack and its implications will be highlighted in the upcoming chapters.

Figure 1 Proposed Syscoin Techstack




## Merged mining

Syscoin utilizes Bitcoin as a consensus method by utilizing the merged mining mechanism. Miners can mine two or more cryptocurrencies in parallel when they merge mine, without sacrificing any mining performance. Therefore, the miners can use computational power to mine blocks on multiple chains with the same algorithm (i.e. SHA-256 for Bitcoin). Merged mining allows Syscoin to add security to their network by Proof of Work (PoW) by recycling the Bitcoin network's energy. The hash rate of Syscoin is currently around 30 EH/s, which is approximately close to 20% of the total Bitcoin hash rate.

All rights reserved

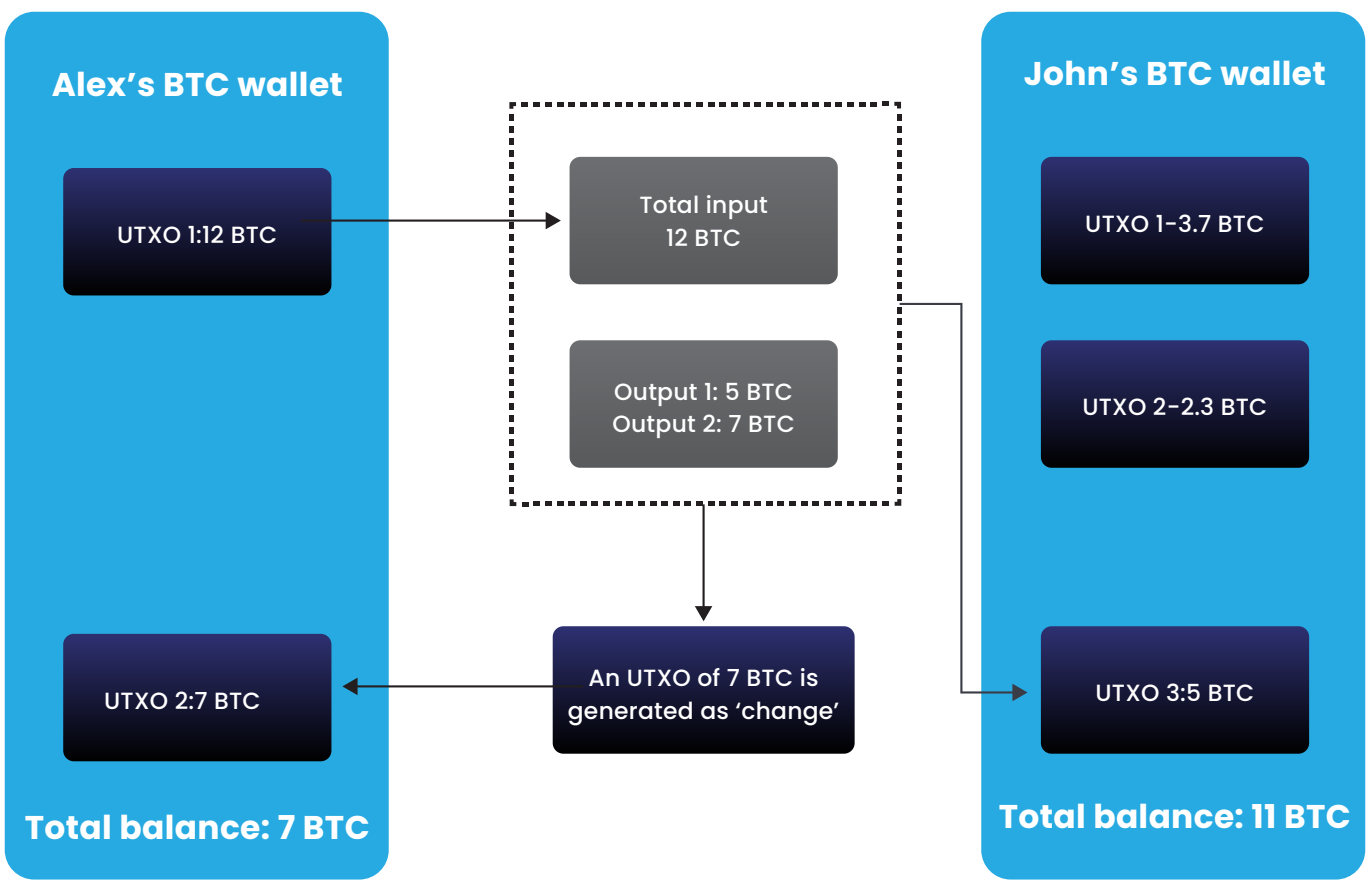
# UTXO model

Syscoin utilizes the Transaction Output (UTXO) model of Bitcoin. The UTXO accounting model works similarly to cash. Whenever a user receives or spends Bitcoin, the transaction is recorded as a UTXO. Therefore, a user's wallet represents the net of all inputs and outputs of the combined Bitcoin UTXOs. The amount left is the amount that is 'unspent.' A bitcoin transaction has both an input and an output. The input is the address where the bitcoin is being sent from, and the output is the address where it is sent to. If an output has been spent, it is impossible to spend it again. However, a UTXO can be used or spent as an input in another transaction. To put this abstract concept into perspective, a simplified example is required (Figure 2).

Assume you would like to send 5 Bitcoin over to a friend. However, you have an input UTXO of 12 BTC. You cannot simply spend these 5 BTC, and you have to spend the entire 12 BTC. Naturally, that is not something you would like to do as you would like to send only 5 BTC. What happens when you send 5 BTC to your friend is that two UTXOs are generated. The first UTXO of 5 BTC will be sent to your friend and the second UTXO is the difference between the input UTXO and the output UTXO, which is 7 BTC.

Syscoin and the Syscoin Platform Tokens (SPT) utilize the UTXO model; therefore, the Syscoin asset model is built on top of the Bitcoin UTXO model. If there are significant innovative breakthroughs of the UTXO model, Syscoin will benefit and capitalize on these innovations. The latest innovation on the Bitcoin network is the Taproot integration. Essentially, taproot increases transaction efficiency, privacy and the potential for smart contracts that can be used to eliminate intermediaries.

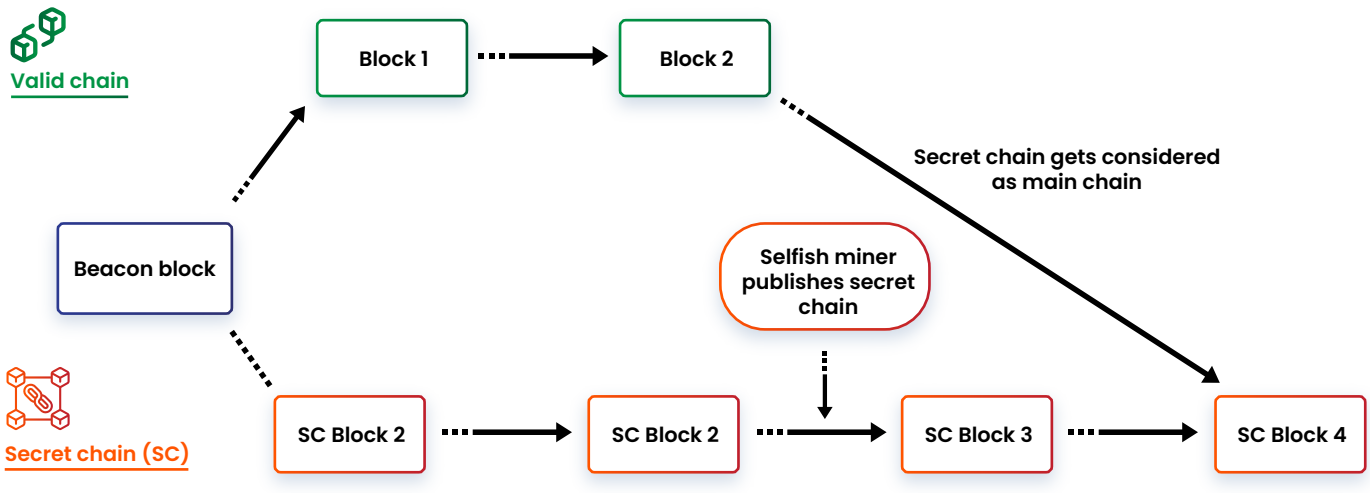
Figure 2 UTXO Transaction process




# Proof of work

Proof of Work has a few significant issues that can be potentially harmful to the Syscoin ecosystem. One of the long-standing security issues of Bitcoin is selfish mining. The design of Bitcoin mining is that miners solve cryptographically complex puzzles and get Bitcoin in exchange. The Bitcoin protocol is designed, so miners get rewarded based on their mining output. However, this assumes that miners will make their newly-generated blocks directly available on the blockchain. According to a study, a miner can increase its mining share; therefore, it rewards by obscuring newly created blocks to reveal them later (Eyal & Sirer, 2018). Via this method, the selfish-miner forms a 'secret' branch (Figure 3). The other non-selfish miners extend the non-secret public blockchain, which eventually becomes longer, assuming that these miners are the majority. The issue is that whenever the secret blockchain is longer than the public blockchain, the selfish miner will publish its blockchain; as it is longer, the other non-selfish miners will assume it is the main chain. The blocks generated by the non-selfish miners are invalid; therefore, they do not get any rewards; instead, the rewards go to the selfish miner. Cryptocurrencies rely on finality, guaranteeing that cryptocurrency transactions cannot be altered, reserved or cancelled whenever they are completed. Due to the complex nature of Decentralized Finance (DeFi) applications and the required level of certainty, selfish mining essentially makes it impossible for DeFi applications to trust the underlying consensus network.

Figure 3 Secret chain visualization




To put this problem into perspective, according to a study (Eyal & Sirer, 2018), selfish mining has the potential to outperform honest mining if the selfish miner has approximately 33% of the global hash rate (Figure 1 appendix). Currently, the biggest BTC pool accounts for 17.10% of the total Bitcoin hash rate. Syscoin does recognize this issue and utilizes chain locks to prevent the selfish mining issue.

*All rights reserved*

# Chain locks

The Syscoin chain lock allows near-instant consensus on the valid chain through long-living master-node quorums (LLMQs). To understand chain locks, it is necessary to comprehend the concept of LLMQs. A quorum is a collection of entities that have voting power with a majority consensus governance system. The quorums are long-living, which highlights the usage period of the quorums; instead of selecting new quorums on demand, the quorums are used for a fixed period.

The reason for the longevity is that quorums perform an M-of-N threshold for signing sessions to gain majority consensus. This means a threshold of M of Masternodes is required out of the total N of Master-nodes to gain consensus and, therefore, sign the session. By leveraging Boneh-Lynn-Shacham (BLS) signatures, multiple signers in a Distributed Key Generation (DKG) event can sign on decisions. The fundamental concept of DKG is built on Shamir's secret sharing paper and is widely used to secure secrets in a distributed way and often used for encryption (Shamir, 1979). DKG events mean that multi-ple parties contribute to the calculation of a shared and private key set by allowing every masternode to contribute to the overall randomness of the key. The Syscoin ecosystem utilizes an M-of-N system, whereby four quorums can participate instead of 1. The system relies on consensus, meaning 3 out of 4 quorums is the threshold for signing a successful chainlock.

The Finality guarantee through the chainlock mechanism is based on the security of validators holding some coins obtained through PoW and participating in consensus. Therefore, the validators are backing the infrastructure with a real cost and have a financial incentive to perform these chainlocks. Addition-ally, Finality will remove some of the roll-ups constraints, such as the waiting period of two weeks, which will be much lower (i.e. hours) with ZK-roll ups.

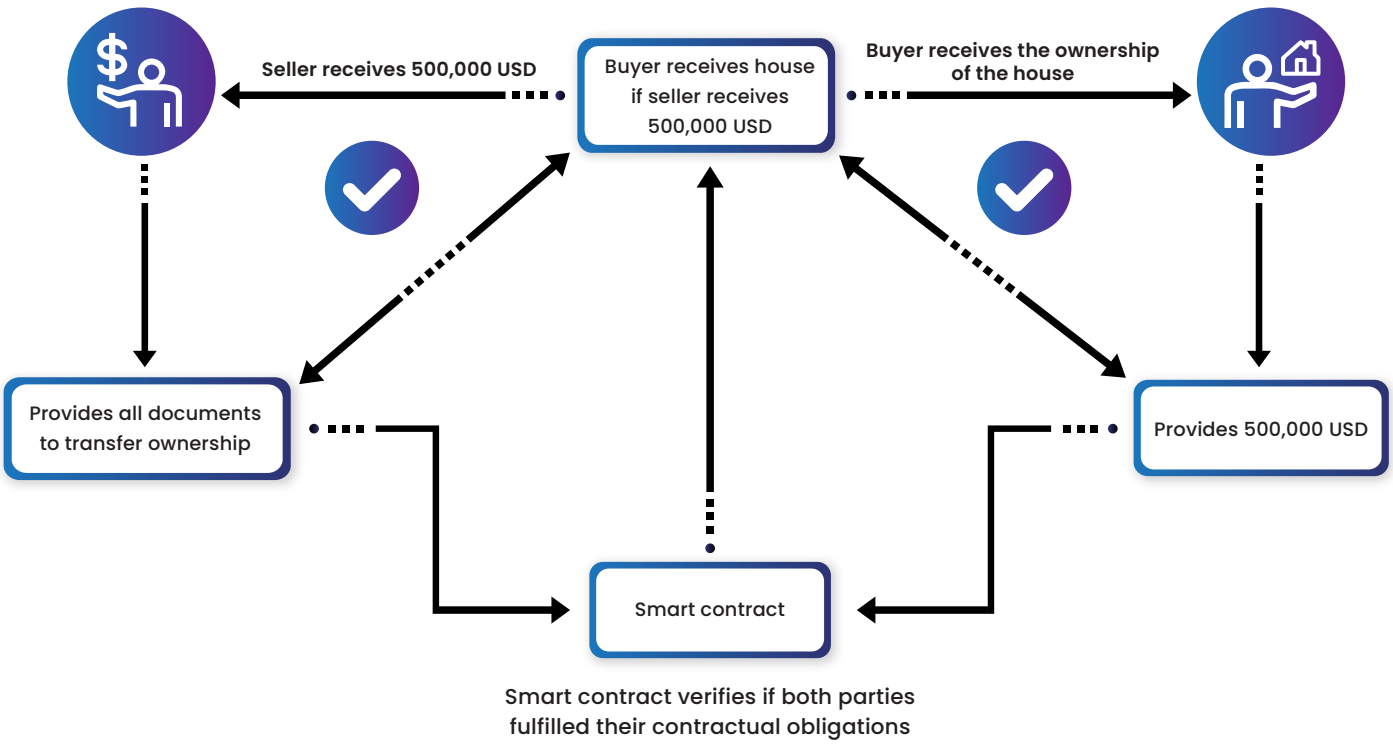
# What is EVM?

An Ethereum virtual machine (EVM) is essentially a machine that mimics a physical computer. The computer is being run by all the full nodes of the Ethereum network. The Ethereum Network is decentralized; meaning, all the full nodes have to agree (i.e. come to a consensus) on how EVM behaves and how computations are made. Therefore, full nodes individually copy and verify transactions on the blockchain. Due to the individual computations, every individual full node has its computation which in the best case is the same as all the other individual computations of every full node.

Developers can run smart contracts within EVM, an isolated environment (i.e. sandbox), which means that every smart contract running inside the EVM has no access to the network, file system, or any other process. Therefore, it does not directly access the full node hardware and cannot disrupt processes and functions (i.e. Ethereum Blockchain operations). To fully comprehend the concept of an EVM, an explanation of smart contracts is required.

A smart contract is a self-executing contract with predetermined rules written in lines of code. When these conditions are met, the contract will run automatically (Figure 4). All participants in the contracts can be certain of the outcome without the need for any intermediary. Smart contracts work by following an "If/when X then Y" structure stored in the blockchain. Whenever the conditions of the smart contract are met, the transaction gets stored in the blockchain. The transaction cannot be changed anymore due to the immutable nature of blockchains.

Figure 4 Schematic visualization of smart contract process




As highlighted in the paragraph above, all contract executions happen on the blockchain run by full nodes. Therefore, a malicious actor could congest the network by creating lots of complex computational smart contracts. A transaction fee (i.e. the computational effort required to execute operations) for deploying or executing smart contracts is required, which leads to higher transaction fees when demand is up. The more complex the requests of the smart contract, the higher the gas fee for executing it. Most smart contracts on the Ethereum network are written in Solidity. However, EVM will provide support for eWasm (Ethereum WebAssembly). WebAssembly is a software format that works across the web and works for multiple software languages. Smart contracts can thus be coded in various languages, including C, C++, and Rust, as eWasm works on all the major browsers.

All rights reserved

# Zero-Knowledge Rollups

The SDK layer of Syscoin will utilize Zero-Knowledge (ZK) roll-ups. ZK Rollups is a layer 2 solution that bundles dozens of transactions off-chain and generates a ZK proof (i.e. SNARK). Layer 2 is a collective term for solutions designed to support the scaling of an application by handling transactions off the Ethereum mainnet (layer 1). The ZK proof is used to prove the validity of transactions, and every batch has its validity proof submitted to the main chain (i.e. Layer 1). The ZK-proofs can be handled off- and on-chain. A significant concern is that transactions could get stuck in the case of off-chain ZK-proofs; however, multiple build-in censorship resistance exiting mechanisms prevent stuck user transactions. Censorship resistance means users can leave layer 2 (i.e. ZK-roll up) without the required coordination of the layer 2 consensus.

The implications of a ZK-proof are highlighted in the chapter "ZK-Proof." The bundling of dozens of transactions leads to a significant decrease in data size and, therefore, a significant increase in scalability. Due to validating the transactions, only the ZK proof is needed instead of all transaction data, which makes validating transactions much more efficient. The amount of stored data can be lowered by indexing instead of transaction addresses. ZK-rollups will drastically increase the scalability of the Syscoin ecosystem and decrease transaction fees. Due to the gas fee market being based on a supply and demand mechanism, the overall cost model will be lowered.

# ZK-Proof

ZK proof is a cryptographic method that allows a party (the prover) to prove to another party (the verifier) that a given statement is true without providing additional information (Figure 5). To make the idea less abstract, there is a relatively simple concept given by Chalkais and Hearn (Demonstrate How Zero-Knowledge Proofs Work without Using Math, 2017).

Your friend is colour-blind and is not able to distinguish the colour red from green. Your friend has a green and a red ball that are otherwise identical. Your job is to convince your friend that the balls differ in colour while revealing nothing else. The concept would go as follows; You ask your friend to show the balls and put them behind his back afterwards. Then he may switch the balls behind his back and shows you a single ball. The question that arises is: Did he switch the ball behind his back? You, as prover, should be able to tell him if he did, assuming you are not colour-blind. Therefore, you could convince him that the balls differ in colour with a high probability of success (i.e. 99%). However, let's assume that the prover has malicious intent, and therefore you are lying to your friend. The two balls are the same colour; according to the Law of Large numbers of Bernoulli (Dekking et al., 2005), the expected probability of you guessing right is approximately 50% after a high amount of games (e.g. 1000 switches). Since a high probability of success by guessing is improbable, your friend can assume that you are stating the truth: the balls differ in colour.

Figure 5 Zero Knowledge Proofs visualization


# Application layer

The application layer is an abstract layer that hides all the complex computations and overall technical details, and it serves as an overall user interface for the network. Therefore, the application layer hides the system's operations to enhance user experience (UX). For example, a decentralized application (dApp) runs on the application layer with an intuitive user interface design, and therefore consumers will not notice the underlying tech.

All rights reserved

# BLOCKCHAIN DESIGN

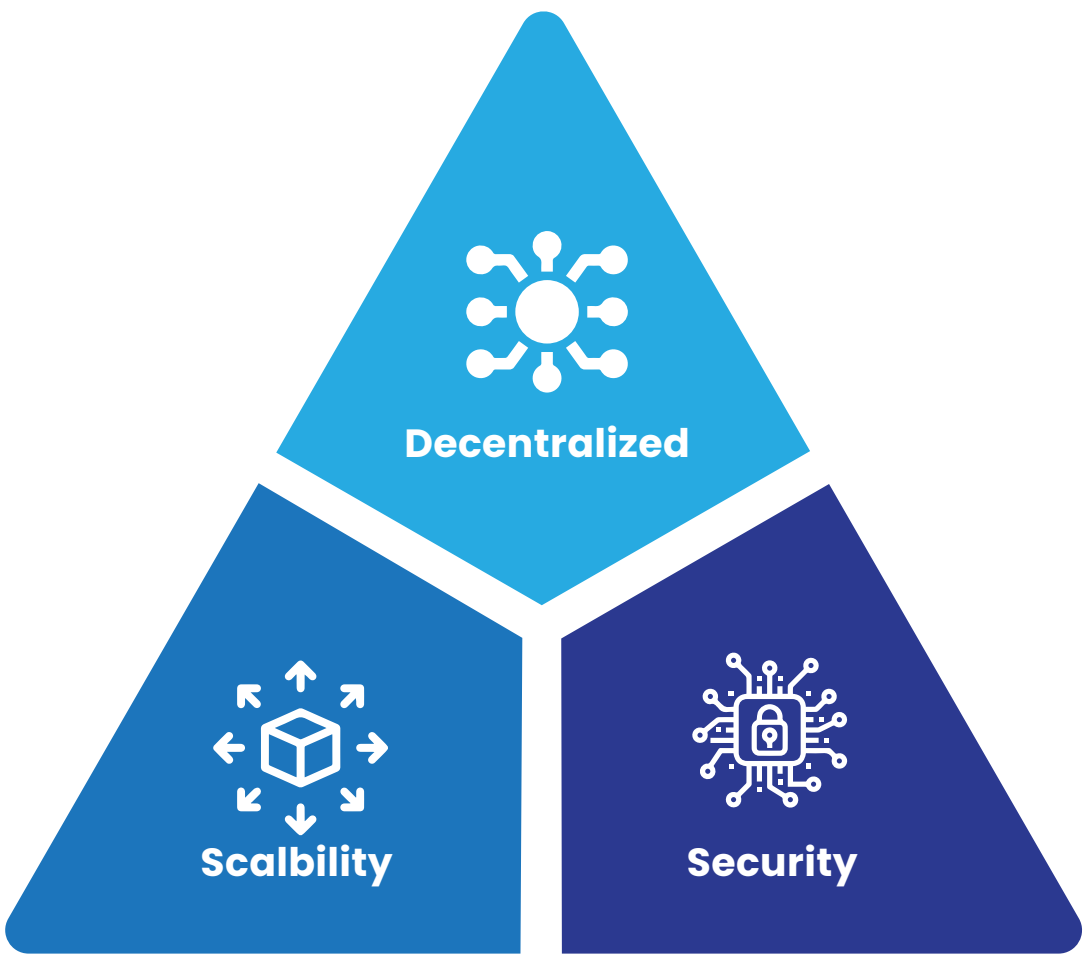
All rights reserved



# Monolithic vs. Modular blockchain design

The scalability issue has been an issue for a relatively long time, and even though a few blockchain networks seem to solve it, there are drawbacks. The blockchain trilemma (Figure 6) comes to mind and is valid for the most part until now. There are quite a few blockchain networks that utilize scalability integrations such as sharding or sidechains, the main problem of most of these integrations is that it is either inherently less secure (i.e. sidechains) or require a particular set of centralized entities (i.e. sharding), which aligns with the blockchain trilemma.

Figure 6 Blockchain trilemma

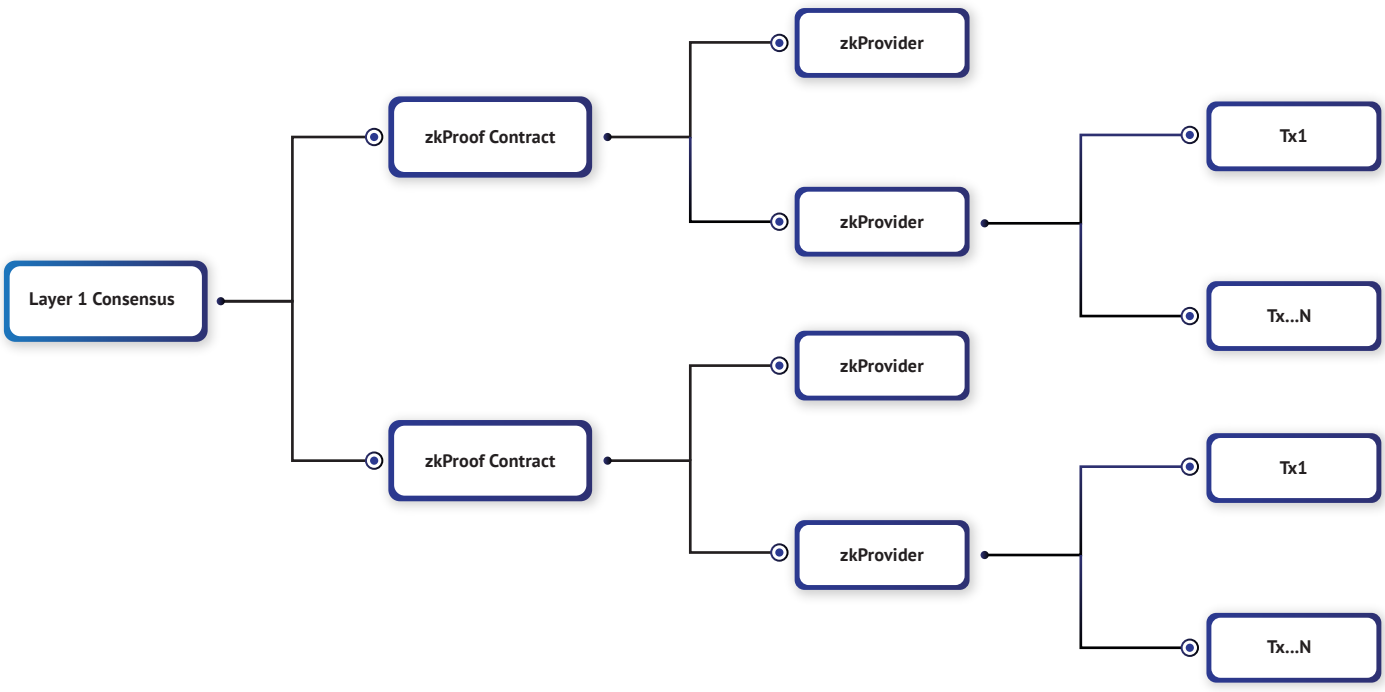



*Source: SEBA BANK AG*

Monolithic chains are blockchain networks that utilize scaling integrations embedded into the client as an in-protocol client. To put this into perspective, if shard fails, this directly impacts the chain, especially on its shared consensus and the other shards. Due to the sharding being integrated into the network, shards are inherently integrated and cannot be separated from the network. An example of a blockchain that will utilize sharding is Ethereum 2.0. The implications of sharding will be highlighted in the upcoming chapter "Sharding as a data layer".

Modular chains utilize ZK-rollups, which can be decoupled from the blockchain network (Figure 7). The ZK-rollups can utilize layer 1 security through smart contracts. Therefore, the layer 1 is decoupled from the scalability integration (i.e. ZK-rollups), and so, if the integration fails, the layer 1 remains operational. The current disadvantage of ZK-rollups is that there is no explicit inter-chain scheme. However, ZK-rollups is a powerful new technology within the blockchain industry; therefore, it is expected that this promising technology will advance and innovate.

Figure 7 Schematic visualization of a modular chain




# Sharding as a data layer

Sharding is a partition technique to spread computational and storage workload across a peer-to-peer (P2P) network. Peers will be responsible for their shard, which is only a portion of the information, instead of the whole network. Therefore, the data will be scattered over shards and hold specific information to relay to other peers but with a much lower computational and storage overhead. A node will handle a certain set of data information in a blockchain network, such as transaction data. The main risk of sharding is that if a shard gets compromised, it could lead to loss of information or malicious intent, false transactions, or malicious programs can be introduced.

By utilizing sharding (i.e. data shards) as a data accessibility layer for ZK-rollups, roll-ups can remain composable while using data from various data shards. Additionally, data shards can be further broadened, allowing quicker and more roll-ups.

All rights reserved

# NEVM EXPLAINED

All rights reserved



# What is NEVM?

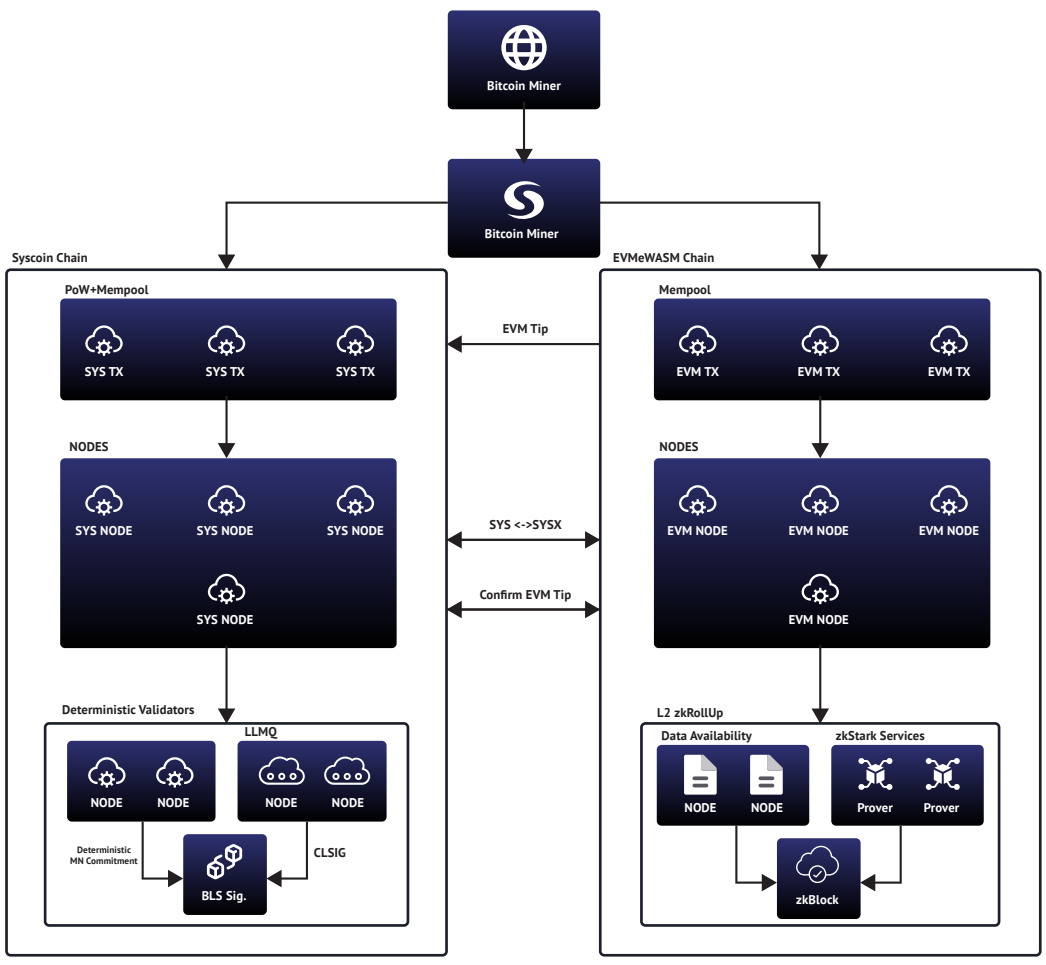
The Network Enhanced Virtual Machine of Syscoin is an adjusted version of an EVM. The main issue with EVM is that the Ethereum network cannot scale as congestion of the ETH network is an issue. Additionally, due to the supply and demand nature of Proof of Work (PoW), congestion will lead to higher transaction fees for users. The NEVM update utilizes aspects of the Ethereum and Bitcoin network and combines these to a coordinated financial computation platform that is secure, decentralized and cheap to use. The ecosystem utilizes the UTXO accounting model of Bitcoin and, as highlighted earlier in this research, utilizes EVM for general acceptance and adoption.

The NEVM update will allow Syscoin to implement security and scalability upgrades such as ZK-rollups and Chainlocks. The implications of these upgrades are highlighted in previous paragraphs. Therefore, the NEVM update is significant for Syscoin users and developers.

# How does NEVM work?

NEVM is a significant development of Syscoin and will be the spearhead for plans of the Syscoin foundation. Understanding how it works is important for potential- and established investors. Figure 8 shows the proposed design of NEVM.  As highlighted before, the Syscoin ecosystem utilizes merged mining; therefore, Bitcoin miners can mine Syscoin while mining Bitcoin without losing processing power. Nodes (e.g. full nodes) run a dual software system, whereby miners execute smart contracts in the node's memory pool running the EVM chain.

Figure 8 NEVM process visualization




A memory pool is an information storing mechanism of unconfirmed transactions for (full) nodes. Essentially, it is a waiting area for transactions that have not been included in a block yet. Nodes verify if the transaction complies with the blockchain rules (i.e. checking signatures, outputs do not exceed the inputs, funds are unspent), and if this is the case, the transaction is accepted. The transaction gets sent from a node to its peers until the transaction is widely picked up, and miners can add it to a block. The buffer zone is significant, considering transactions are not instantly added to a blockchain. Otherwise, these transactions would have gotten cancelled.

The nodes are part of the Syscoin and EVM/eWasm chains, which are kept in sync through an EVM tip hash (i.e. block hash) into the Syscoin block. The nodes will verify if the EVM tip is valid by matching the description stated by the Syscoin block. This can be done locally as nodes run the Syscoin and EVM chain (Figure 8). Additionally, chains can interact through Interprocess Communication (IPC). This means that the chains will be able to 'interact' with each other by sharing, synchronizing, and validating data. To put this into perspective, the interaction in between the chains will be explained in three points. The explanation will utilize figure 8 as a schematic visualization.

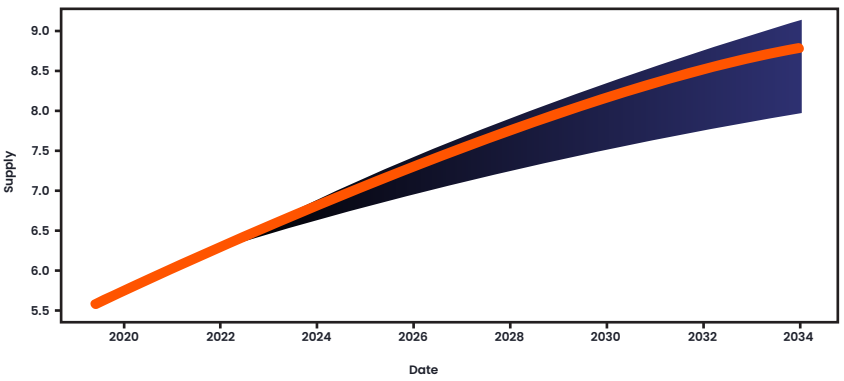
- Miners of the EVM chain collect the latest block hash (i.e. EVM tip) and place that into the Syscoin block.
- When nodes validate these Syscoin blocks, the validity of the block hash will be confirmed by locally verifying through the EVM chain.
- The fees for the EVM chain will flow through an SYSX – SYS bridge. To speed up the whole process, precompiling block hashes and Merkle roots to confirm validity can increase the efficiency of the process.

*All rights reserved*

# Changes to Syscoin

The NEVM release requires a few changes to the Syscoin ecosystem to prevent higher rate inflation and ensure security by adjusting block generation time from 1 minute to every 2.5 minutes. Additionally, the implementation of Ethereum Improvement Proposal-1559 (EIP-1559) will significantly impact the tokenomics of the Syscoin ecosystem.

Figure 9 95% Confidence interval of Syscoin Supply (using ETH Daily TX Fees)




# Ethereum Improvement Proposal-1559

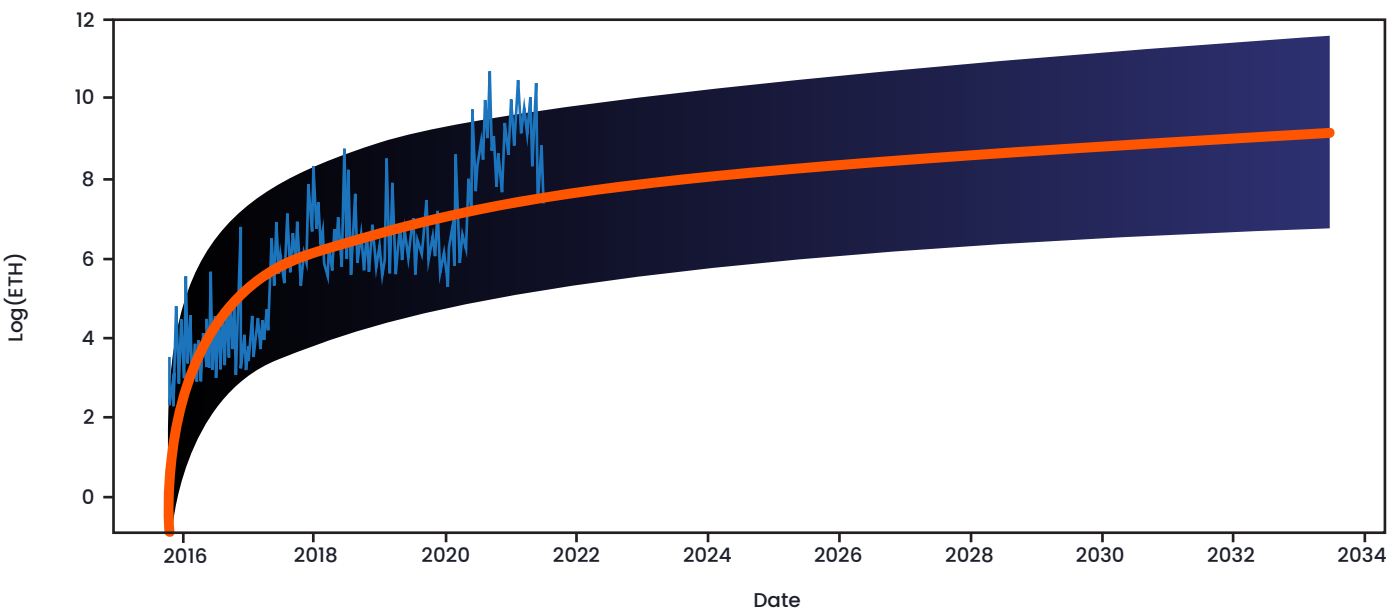
The EIP-1559 was implemented in the London upgrade back on the 5th of august of 2021. The proposal aims to change how transaction fees are estimated by a "dynamic block size" mechanism. The proposal introduces a baseline fee which acts as a minimum transaction fee. Whenever the Ethereum blockchain gets congested, the block size will expand and carry out more transactions. The baseline fee will get burned, therefore having a deflationary impact on the circulating supply of Ethereum.

Syscoin will adopt a similar system, whereby the rewards for masternodes, miners, and governance proposals change. The block generation time will change from 60 seconds to 150 seconds; the current reward for a block is 34.76 Syscoin; this will increase by 86,8, which aligns with the generation time increase of 150%. The baseline fee will be burned, so Syscoin can turn into a deflationary token (Figure 9). The figure utilizes a 95% confidence interval, whereby the blue-green line is the predicted inflation, and the blue area around it is the 95% confidence interval. To fully understand this figure, an explanation of the implications of a confidence interval is required.

A 95% confidence interval is a range of values that returns the population's true mean values with a confidence of 95%. Therefore, there is a 95% confidence level that the unknown parameter is in the interval. In the case of figure 9, it means that there is a probability of 95% that the predicted line (i.e. unknown parameter) falls within the area. Meaning there is a 95% chance that the inflation of the circulating supply of Syscoin falls within the blue area of figure 9, assuming that the model is correctly specified. A confidence interval has the upper bound, the area above the predicted line, and a lower bound below the predicted line.

The confidence interval, in figure 9, relies on the assumption that in the lower bound, all masternodes have less than a year of seniority. In contrast, in the upper bound, the assumption is made that all masternodes have full seniority. The Syscoin ecosystem utilizes a seniority mechanism, whereby masternodes are incentivized to mature their masternode by increasing rewards over time. Due to a full seniority masternode receiving more rewards than a less than a year seniority masternode, the inflation of Syscoin is higher when all masternodes have full seniority. The other variable that impacts inflation is the number of transactions as the baseline fee will be burned and therefore have a deflationary impact on the circulating supply. The predicted line is constructed by utilizing Ethereum historical fee data. Therefore, the prediction assumes that Syscoin will have the number of transaction growth as Ethereum (Figure 10).

Figure 10 Ethereum daily transaction fee burn with projections




# Block time for Chain locks

The block time is raised from 1 minute to 2.5 minutes; besides the inflation argument, the Syscoin ecosystem gets more secure by raising the block time. The full nodes have more time to validate Syscoin blocks by verifying the validity of the block hash, and, additionally, the accuracy of chain locks created by quorums is increased.

Most blockchain networks implement fast block times to increase the scalability of the ecosystem. The more blocks the network produces, the more transactions can be handled. However, Syscoin does not suffer any scalability issues as the ecosystem has an instant-settlement layer (i.e. Z-DAG layer). Therefore, the block time increase does not necessarily hurt the scalability of Syscoin. Additionally, the scalability of Syscoin will drastically increase by the implementation of ZK-Rollups, which will be further highlighted in the upcoming chapter.

All rights reserved

# IMPLICATIONS OF NEVM

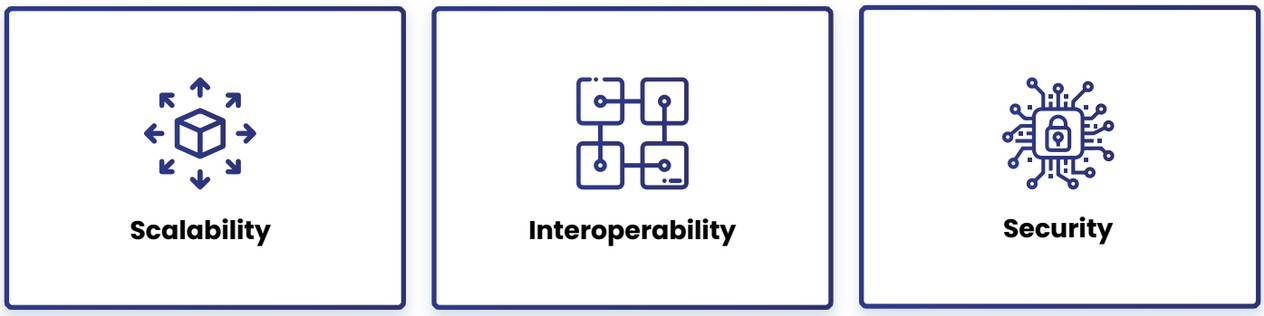
All rights reserved



## Importance of NEVM

NEVM is a cornerstone for the Syscoin ecosystem. It has multiple implications on various aspects of the ecosystem (Figure 11). The implications will be highlighted and explained in this chapter to strengthen the upcoming release's understanding further.

Figure 11 NEVM Implications




## Scalability

The NEVM update will have a direct impact on the scalability of the Syscoin ecosystem. The ZK-rollups integration theoretically allows Syscoin to scale up to approximately 210,000 on-chain Transactions Per Second (TPS) with a gas limit of 10B. To put that into perspective, under normal operating circumstances, Visa processes around 1,700 TP, which can theoretically scale up to 56,000 TPS. However, Syscoin is more than just a payment provider, considering Syscoin is a smart contract platform where developers can build decentralized applications (dApps) for the community. Due to the increase of scalability, developers can create more complex projects that require a considerable amount of smart contracts while being affordable. To put this into perspective, Syscoin can handle 3,100 TPS in its current state while Ethereums TPS is 45. Due to the nature of the supply and demand model combined with the efficiency of an ecosystem, the higher TPS, the lower the transaction fees. The TPS gap will grow in absolute terms with every scalability integration (Figure 12). Therefore, scalable payment and NFTs through Syscoin Platform Tokens (SPT) are more feasible, given that the EVM compliance could increase the number of deployed projects on Syscoin.

Figure 12 Syscoin vs. Ethereum scalability table

| Chain | Gas Limit | Block Time | Mode | Cost 300k Tx | Amortized Cost per Tx | Total TPS | USD / 300K Tx (Mar 20 to Mar 21) | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | median | lwr 5% | upr 95% |
| ETH | 12.5M | 13 sec | L1 | 6.3B gas | 21,000 gas | 45 | 159,328.24 | 10,669.40 | 1,914,394.79 |
| | | | L2 zk-Rollup | 94.47M gas | 315 gas | 3,000* | 2,389.16 | 159.99 | 28,706.81 |
| | | | L2 Validium | 5M gas | 17 gas | 56,000* | 126.45 | 8.47 | 1,519.36 |
| NEVM | 10B | 150 sec | L1 | 6.3B gas | 21,000 gas | 3,100* | 1.92496 | 0.97008 | 4.51653 |
| | | | L2 zk-Rollup | 94.47M gas | 315 gas | 210,000** | 0.02887 | 0.01455 | 0.06773 |
| | | | L2 Validium | 5M gas | 17 gas | 4,000,000 | 0.00153 | 0.00077 | 0.00358 |

## Interoperability

The NEVM update will significantly lower the overhead costs of being interoperable for Syscoin. The current SysEthereum bridge is relatively high in technical overhead. Therefore the overall costs were higher. The main issue with the SysEthereum bridge was the relatively high transaction costs by proposing and approving Superblocks. Running as an agent was not necessarily profitable for the community considering the traffic that went through the SysEthereum bridge was not enough to cover the costs.

## Security

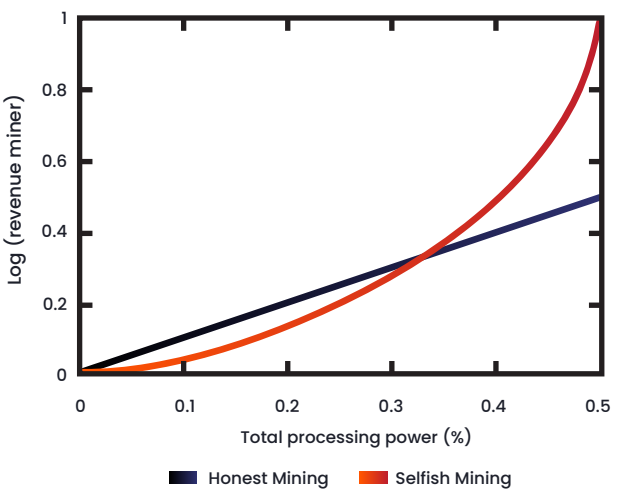
Chainlocks will increase the security of Syscoin by preventing selfish mining, additionally strengthening the overall security against potential re-orgs. As highlighted in the previous chapter, a chainlock is established usually within a minute and therefore does not necessarily slow the ecosystem down by drastically increasing the block producing time. However, the block producing time is increased, but considering the scalability nature of Syscoin, this is not an imminent issue. Additionally, considering scalability is not necessarily a linear relationship. However, more a logarithmic relationship, it is expected that there would be an equilibrium point, whereby the marginal effect of scalability decreases and therefore, more resources can be put into security.

All rights reserved

# APPENDIX

# Appendix

Figure 1 Selfish mining equilibrium




## References:


- Eyal, I., & Sirer, E. G. (2018). Majority is not enough. Communications of the ACM, 61(7), 95–102. https://doi.org/10.1145/3212998
- Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11), 612–613. https://doi.org/10.1145/359168.359176