SYSCOIN 4.0

NEVM Code Audit

The Best of Bitcoin
The Best of Ethereum
The Best Scalability
Network-Enhanced Virtual Machine (#NEVM)
will make @Syscoin the perfect #smartcontract
platform for all the #DeFi and #DApps that matter most.
SYSCOIN
PLATFORM

Bryce Weiner, US Blockchain Company, October 2021

TABLE OF CONTENTS

INTRODUCTION

SYSCOIN (SYS) is a 7 year-old proof of work cryptocurrency which continues to stay at the state of the art by continuously integrating new technologies advancing the cryptocurrency space. The most recent innovation, and the subject of this report, is the Network Enhanced Virtual Machine (NEVM). Simply put, the NEVM is an Ethereum blockchain which inherits the security of the SYSCOIN blockchain to provide fast, low-cost, Ethereum compatible smart-contract execution.

This report will focus on five areas: **Tech Stack and Architecture**, **Security Vulnerabilities**, **Code Quality Check**, **Performance and Scalability**, and **Potential Maintenance Issues**.

ABOUT US BLOCKCHAIN COMPANY

Originally founded in 2017 as AltMarket, Inc. the US Blockchain Company has expanded beyond offering monetization services to a full stack cryptocurrency development, regulatory compliance, and monetization consultancy. In addition to the AltMarket exchange, USBC has provided development and consulting services to a variety of cryptocurrency networks, such as Tao (XTO), Unobtanium (UNO), SYSCOIN (SYS), and Bitcoin Cash (BCH). The company website may be found at usblockchain.co.

DISCLOSURE

Nether the author nor US Blockchain Company are holders of the token, securities, or derived assets of the SYSCOIN network or family of corporations and are completely impartial.

TECH STACK AND ARCHITECTURE

SYSCOIN network architecture as of this release defies the standard “layer” paradigm in providing various network functionality through multiple types of node and without creating overly complex topography.

Base Layer

The SYSCOIN codebase is derived from the Bitcoin source code. The proof of work is provided by SHA256 miners, which have the option of merge mining with Bitcoin. This serves to make mining SYS extremely profitable in comparison to Scrypt, Dagger, or non-merged mined SHA-256 coins. The use of SHA256 makes proof of work compatible with all Bitcoin ASIC hardware.

As the primary network being mined is Bitcoin, the proof of work for the SYSCOIN network is essentially environmentally neutral while at the same time supplementing the return on investment with SYS tokens.

Minimum System Requirements: dual core 2.0GHz processor, 8GB RAM, 150GB HDD.

Language: C++

Masternode Layer

The Masternode Layer is a series of smart contracts which require a deposit of 100,000SYS to activate. Upon activation, the SYS Masternodes allow for a fee-based “instant” transaction settlement through a Zero-Confirmation Directed Acyclic Graph (ZDAG). This layer provides the most reliable consensus for the chain tip, and upon Masternode certification blocks are no longer eligible to be re-organized by a chain split, or an alternative chain of block consensus.

Masternodes which process the instant fee-based transactions are awarded a share of the fees, providing a way for users to earn SYS without expensive mining equipment.

Network-Enhanced Virtual Machine

The Network-Enhanced Virtual Machine (NEVM) is an Ethereum-compatible virtual machine for the execution of smart contracts. Consensus for the NEVM layer is provided by the Base Layer via a novel implementation of the Ethereum Virtual Machine. As the NEVM layer is a Base layer independent state machine, it creates its own blockchain which contains the NEVM-specific data on a 1:1 basis with the Base layer.

Minimum System Requirements: quad core 2.0GHz processor, 16GB RAM, 500GB HDD

Language: Go

SECURITY VULNERABILITIES

51% Attack

A 51% attack is when a simple majority of block production is determined by a single entity which then gains the ability to rewrite blocks already confirmed by generating their own version of the blockchain in secret. As the attacker has the most proof of work possible, publishing the secret chain to the network causes a reorganization of the blockchain replacing the “authentic” blocks with the secretly mined blocks. This can be used to reverse transactions resulting in a loss of funds.

At the time of this writing, the SYS blockchain has a hashrate of **27 Exahash per second (EH/s)**. By comparison, the Bitcoin blockchain has a hashrate of **165.68 EH/s**. The latest commercial miners available at the time of writing is the Bitmain S19pro, which tops out at **110 TH/s** for a MSRP of **$9,300**. To achieve 51% of the SYSCOIN network would require around 14 EH/s of mining capacity. Achieving this hashrate would require **127,273 miners**, with an estimated retail cost of **$1,183,636,363.63**. The high cost of the physical machines alone is in the billions and that does not include the ancillary costs of warehousing, environmental conditioning, networking, and personnel. It is worthy to note that the requisite amount of hashpower is not available for rent on services such as NiceHash.

As such, it is the opinion of USBC that at the time of this writing it is economically and technically impractical to attack the SYSCOIN network with 51% hashrate.

Selfish Mining

Selfish mining is similar to a 51% attack, but requires the collusion of several mining entities to execute, reducing the cost of a reorganization attack significantly.

The Masternode Layer of the SYSCOIN network provides the solution to this in what is referred to as a “chainlock”. A block is considered chainlocked after it has been accepted by a quorum of Masternode clients. While originally intended to protect the integrity of the Z-DAG system, it now provides the added benefit of serving as a defense for the NEVM network layer as blocks which are chainlocked may not be reorganized under any circumstances, and any attempt to do so will create orphan blocks.

Distributed Denial of Service

The vast majority of the infrastructure composing the SYSCOIN network topography are Masternodes, with **2,555** in operation at the time of this writing. By comparison, there are only **49** reported nodes which are not Masternodes. As the NEVM network is still only available in testnet, there are no operational statistics provided.

One point of concern with the Masternode layer is that **43%** of nodes are hosted by a single provider, **Digital Ocean**. USBC recommends the SYSCOIN community focus on diversifying server hosting to a variety of other providers to limit potential services outages as a result of the failure of Digital Ocean. However, there is no immanent or existential threat detected in the network topography at this time.

Github

There are currently 15 individuals with organizational access to the SYSCOIN repository on Github, although there is no ability to discern which members have merge access. USBC recommends an audit of the member permissions to verify which have merge access and that it be kept to an absolute minimum.

The Security Policy portion of the repository still retains the original Bitcoin information. USBC recommends that it be replaced with information specific to SYSCOIN.

CODE QUALITY

- ***Convention Consistency*** *- In both the Bitcoin and Geth code base, existing conventions are followed for syntax and variable names.*
- ***Unit Tests*** *- Unit tests are clear and concise, with proper coverage for the additional functionality required by NEVM.*
- ***Compile*** *– SYSCOIN client and Geth client both compile without warnings or errors.*
- ***Libraries*** *– All linked libraries are the latest versions.*

PERFORMANCE AND SCALABILITY

SYSCOIN Client

The SYSCOIN 4.0 client instantiates pruning, which contains the growth rate of the state data store to 50GB per six months, or 100GB per year.

Z-DAG throughput with zero network latency is calculated at upwards of 40,000 transactions per second.

Increased transaction volume does not place an increased burden on the processor, however it is important to maintain sufficient disk space or the client will crash potentially causing network outages.

NEVM Client

The NEVM Geth client requires substantially more processor and hard disk requirements than the SYSCOIN client.

The NEVM client does not instantiate pruning, therefore care must taken to maintain proper disk space.

As NEVM block sizes increase towards the per-block gas limit, processor and memory demands scale accordingly.

POTENTIAL MAINTENANCE ISSUES

The NEVM integration effectively doubles the amount of maintenance, knowledge base required to maintain the network, attack surface, and vulnerability to critical errors in either the Bitcoin or EVM codebases. Due to the specific design implementation of NEVM there is no foreseeable cascade failure potential should either code base become subject of a critical error, respecting that the NEVM state machine relies on the Base Layer of the SYSCOIN network.

The increased prerequisite knowledge will have a curve of community compliance over time, and as such the network should retain stability as it scales.

USBC recommends the SYSCOIN community become conversant in Ethereum Virtual Machine technology, including its flaws and shortcomings, development discussions, news outlets, and influencers.

As the Ethereum VM being used is 1.10.8 as of August 24th 2021, there are no potential flaws or failures as a result of EIP-1155 or the move to proof of stake, known as ETH 2.0. However, this means that future features and enhancements to the Ethereum VM must be painstakingly merged by hand into the NEVM code base, and at times may require significant re-engineering.

Ethereum VM networks require significant infrastructure as compared to Bitcoin networks. NEVM requires the same infrastructure as Ethereum VM networks, including but limited to statistics servers which display real-time NEVM network health and strength, RPC servers for the implementation of Web3.0, wallet providers, and exchanges, and additional blockchain explorers which not only show the contents of NEVM blocks but allow some smart contract visibility if not execution. The NEVM also requires certain infrastructure, such as bridges to allow for the transfer of value between the Base Layer and the NEVM Layer.

CONCLUSION

The specific implementation will mature over time, but the performance is truly impressive. The security of the SYSCOIN Base Layer is nearly unassailable. This provides an amount of reliability and consistency of contract execution which is rivaled only by Ethereum, itself.

The significantly increased technical burden cannot be understated. SYSCOIN engineers must now be experts in two blockchain systems, as well as the specifics of the integration between them. The increased infrastructure requirements may seem daunting, but provide opportunities for commercial solutions resulting in job growth.

The SYSCOIN NEVM integration is a truly remarkable piece of engineering utilizing advanced concepts in cryptocurrency and blockchain engineering. It is unique among cryptocurrencies. The utilization of consensus of a Bitcoin style blockchain to create consensus on an Ethereum VM style blockchain is a first of its kind.

As a result of the code audit, the NEVM integration into the SYSCOIN network is ready for execution.