Scalability, Decentralization & Security — What Trilemma?

The blockchain trilemma is a classic idea that truly decentralized blockchains need to choose between security or scalability. Verus offers a different perspective and a new approach. Together we will come to the conclusion that the Verus Protocol solves scalability by neither sacrificing decentralization or security, effectively solving the trilemma.

Max Theyse · Follow
Published in Verus Coin · 10 min read · Feb 12, 2024

285 1

A Closer Look at the Trilemma

Before we dive in, let's examine the current perceived definition of the

> The trilemma is currently looked at from a single-chain standpoint. A false premise that does not scale to the world.

There is truth to the fact that it is very difficult to have a decentralized single blockchain that also has a high tps. The larger the number of validators the harder it is to find consensus among them all, which makes them slower, and makes it more difficult to get them to process large numbers of transactions. To get a high tps blockchain you would need to lower the number of validators so they can find consensus more easily, and raise the hardware requirements for running a node so they can process those transactions quicker too. Yet doing so compromises true decentralization. The lower the number of validators, the less decentralized, the less robust. And the higher the hardware requirements, the less accessible it is for people around the world, the less decentralized.

The trilemma is currently looked at from a single-chain standpoint. A false premise that does not scale to the world. We will show you how Verus offers a new and better approach.

Scalability Does NOT Mean High Tps

> Transactions per second are nothing more than just a performance indicator — like GHz for computers.

Cryptocurrency protocols often boast about how fast their blockchains are (transactions per second) as an indicator of their scalability. Contrary to popular belief this is a false premise. Transactions per second are nothing more than just a performance indicator. Like how we use GHz (CPU clock speed) to indicate how fast a computer is, or an even better example — how fast servers are.

To bring the promise of crypto to billions of people around the globe let's make a comparison with the Internet. The Internet does not run on one single server. All websites and applications that we use daily are **not** connected to one single server. The Internet has not been scaled to the world by constantly upgrading the one server to a faster one. It's millions of servers that are servicing billions of people around the world. These millions of servers are perfectly connected, and completely interoperable so that using the Internet today is a seamless experience.

Now, with this perspective in mind, let's get back to the current situation in crypto land. Most, if not all, crypto protocols are trying to service the world with their one single, monolithic blockchain. The monolithic blockchain becomes a central hub where all smart contracts and applications revolve around. When they notice that it doesn't scale (the transaction fees start ramping up) the industry comes up with solutions that heavily compromise on decentralization and security (e.g. L2s, semi-centralized protocols, master nodes). This is not the answer.

Instead of acknowledging that the Internet today is a giant, interconnected multi-server world where all applications and websites are seamlessly connected, most of the crypto industry thinks we live in a single server (single blockchain) world.

Verus acknowledged that to realize the promise of cryptocurrency and blockchain, it needed to scale for billions of people around the globe and thus it needed to embrace a multi-server, multi-chain world. And that is exactly what the Verus Protocol does today. Without sacrificing decentralization and security.

Unlimited in Scale

Before we start explaining how Verus is truly decentralized and secure, let's start with how Verus embraces the multi-chain world and delivers unlimited scalability.

Most, if not all, current blockchain protocols argue that to have low transaction fees they must achieve higher transactions per second. They try to scale up — increasing the performance of their monolithic blockchains. This only gets them so far. At some point, they will bottleneck again, and in the process, they compromise on decentralization and security.

Verus offers a new approach, one in which each organization or business can launch its own highly capable, rent-free, no-coding-required blockchain. It's called Verus PBaaS (Public Blockchains as a Service). These PBaaS-chains are fully independent, can be customized to the organization's need, inherit all the same features as the Verus blockchain, and most importantly are fully interconnected and interoperable with the complete network and other bridged protocols (e.g. Ethereum). A single PBaaS-chain can do between 75 and 800 tps depending on the options chosen.

There is no upper limit to deploying PBaaS-chains. Just like there is no upper limit to servers being deployed. When we reach a bandwidth limit we don't go out upgrading our single server, we put another server next to it to spread out the usage. The same thing is here, reaching unlimited scalability.

Of course, this only works when those PBaaS-chains are fully interoperable and interconnected, which they are — in a provable, trustless and decentralized way. There is no centralized entity sitting in between the PBaaS-chains regulating everything.

Cross-chain transactions and conversions, cross-chain bridging of identities (VerusID), tokens and basket currencies, even Ethereum (& ERC20/ERC721/ERC1155) — it's all built into the consensus mechanism, trustlessly bridged over by the decentralized network of miners and stakers only. This is all on mainnet now, for everyone to use.

We can conclude that Verus is scalable to billions of people around the world with the unlimited deployment of PBaaS-chains. But does it compromise on decentralization and thus security? Let's dive into it.

Verus lead developer Mike Toutonghi explains how unlimited scalability is achieved.

Built to be Decentralized

There are a few things at play here that work in harmony to achieve decentralization and security — Verus Proof of Power (the hybrid 50% proof-of-work, 50% proof-of-stake consensus mechanism), merge-mining and the Fee Pool.

> Verus had no ICO, had no premine and had and has no developer fee or tax.

Before we jump into the above let's acknowledge some facts that are pivotal to being a true decentralized protocol, to being credibly neutral. Just like Bitcoin before, Verus had no ICO, had no premine and had and has no developer fee or tax. Verus is not a company or a business. Verus is rent-free and all protocol fees go to the block producers. These facts are super important to incentivize decentralization and to be a credibly neutral protocol in the eyes of the world.

A Hybrid Consensus Mechanism

Now let's unpack Verus Proof of Power, the consensus mechanism of the Verus blockchain, and all PBaaS-chains. It's a hybrid of 50% proof-of-work and 50% proof-of-stake, and it's a provable solution to 51% hash attacks. Out of the 1440 daily blocks (on Verus, and when a PBaaS-chain opts for 1-minute block times), half is solved by mining and half by staking.

VerusHash, the proof-of-work mechanism which disincentivizes ASIC & FPGA development, and favors CPUs, mobile phones and ARM-devices for mining. Mining with mobile phones and for example, Orange Pi 5's are the most cost-efficient way to do it. This proves a significant leap towards a more inclusive mining environment. It's accessible to everyone and thus creates a naturally decentralized protocol.

An Orange Pi 5 mining farm by community member DCAL4.

Additionally, to give even more power to miners, they can merge-mine up to 22 PBaaS-chains simultaneously without sacrificing their original hashing power. This dramatically increases efficiency and network security. So, when considering an unlimited number of PBaaS-chains on the network, each miner can choose up to 22 to mine. They can choose for profitability, or choose the ones they want to support.

This approach to mining is environmentally conscious. The protocol's design allows for low-power devices to mine extremely efficiently. It lowers the entry barrier for participation in blockchain validation, especially in low-income countries, yet can also give life to phones that are old or with broken screens. Thus significantly reducing the environmental impact associated with traditional PoW mining.

Then we have the proof-of-stake part of the consensus mechanism. This one is really simple and powerful. Anyone can run a node and start staking. There is no minimum amount of VRSC needed (pretty unique in the world of PoS). Verus solved the "nothing-at-stake"-problem therefore there is no slashing of funds. Funds staking are never locked and running a node can be done with something as cheap as a Raspberry Pi 4. All-in-all proving yet again that Verus is accessible to everyone, creating a naturally decentralized protocol.

We can conclude that Verus is truly a decentralized protocol, naturally emerging from its extremely low-barrier mining and staking. So what does that mean for security?

Protocol Security at Another Level

Seeing as the Verus Protocol is naturally decentralized and provable 51% hash attack resistant, it's extremely secure. PBaaS-chains take these properties with them as they have the same consensus mechanism, and the Verus miners can choose up to 21 of them to merge-mine. It's fair to say that there is no compromise on security given the scalability of the protocol.

Verus Introduces the Fee Pool

Let’s first explain the fees the protocol generates for the miners and stakers:

- PBaaS-chain launches: 10,000 VRSC (5,000 for the block producers of Verus, 5,000 for the block producers of the newly launched chain)
- Currency launches (tokens, basket currencies, liquidity pools, ERC-20 mapped currencies): 200 VRSC
- VerusID registrations: 100, 80, 60, 40 or 20 VRSC
- subID registrations: 0.02 VRSC
- DeFi conversion fees: min. 0.0125%, max. 0.025%
- Transaction fees: 0.0001 VRSC

Builders and users pay these protocol fees for their operations and the fees are directed into the Fee Pool. Then, for each new block, 1% of the Fee Pool is added on top of the regular coinbase reward (currently 6 VRSC).

The Fee Pool is introduced as a security measure to keep the protocol stable. We have seen in other blockchain protocols that when a block has large fees, block producers try to “snipe” the block (putting lots of hash onto the network, then pulling it out of the network, or even trying to reorder the blocks for their own gain). In doing so they destabilize the protocol. Verus mitigates this behavior by spreading the extra fees over many blocks.

Smart Contracts Are Not Secure

Most blockchain protocols use the VM-based application model — smart contracts written with Solidity. It’s full of smart contract hacks and bugs and has insecure and phishing-prone wallet approval mechanisms. On top of that MEV (maximum extractable value) is rampant, due to the serial processing of transactions on the VM-model (it’s easy for a block producer to reorder transactions inside a block for their own gain). We can honestly say that the VM-model is not secure.

The Verus approach is different as it follows the fundamental systems design principle — the most important security layers should be located in the protocol itself, and not coded on top via L2 (smart contracts). All operations on Verus and PBaaS-chains are directly connected to consensus, secured by the miners and stakers of the protocol.

Now you might ask yourself “But can we build dApps that are as capable as building them with the VM-model?”. The answer is yes. Developing dApps with Verus is much more straightforward than building to a VM-based application model and results in inherently more capable, secure and scalable solutions.

Does Verus Solve the Blockchain Trilemma?

A fair question. And hopefully we answered with enough detail. The answer is “yes!”.

Let’s summarize. Verus does not compromise on decentralization and security to reach unlimited scalability. Unlimited scalability is reached by scaling out, not scaling up. It is the equivalent not of upgrading your server but of putting an extra server next to it to spread the bandwidth around.

Decentralization is achieved by making mining and staking accessible for everyone through extremely low hardware requirements. This naturally creates a large number of miners and nodes (stakers), making the network robust against attacks of all sorts.

High security is not only reached through the decentralized nature of the network but also because of the Fee Pool and the fact that all operations are directly connected to consensus and thus the miners and stakers.

Now is the Time to Build with Verus

Without having to rely on smart contracts, builders can develop dApps that are even more powerful, secure and scalable. Builders can use the no-coding-required API commands, together with VerusID and its VDXF (Verus Data Exchange Format) as a controlled public storage system with multiple levels of nesting to create dApps of any kind.

The foundation has been laid for a true Internet of Value. Verus urges all builders to join the community on Discord and to get familiar with the cutting-edge blockchain technology. Go build your project with Verus without having to learn a new programming language. It's here, it's ready, all live on mainnet.

Find Verus at Consensus 2024, May 29–31, Austin, USA. The community is happy to inform you on the dApp building opportunities! Read more here: **Consensus 2024 — Verus Showcases Fully Completed PBaaS Blockchain Technology**

. . .

Try Yourself! ✅

Look up the **complete command list here**. Go to **docs.verus.io** to get guidance on API commands (e.g. **launching currencies, tokens & liquidity pools**).

. . .

Join the community. Learn about the protocol. Use Verus & build.

➡️ Join the community on Discord

Follow on Twitter

Go to verus.io

Blockchain Development Blockchain Cryptocurrency Cryptocurrency News Blockchain Technology

285 1

Written by Max Theyse

149 Followers · Editor for Verus Coin

Follow

More from Max Theyse and Verus Coin

Max Theyse in Verus Coin

Introducing Pure — The Currency 100% Backed by Verus & Bitcoin

Pure is a decentralized currency fully backed by Verus (VRSC) & Bitcoin (tBTC).

8 min read · Mar 16, 2024

196

Max Theyse in Verus Coin

Verus: Profit Generating Protocol for Miners and Stakers

Future and present Verus miners: take notice. Be ready to maximize profit with your...

4 min read · May 12, 2021

304

Oliver in Verus Coin

How to Start CPU Mining Verus Coin VRSC from Your Computer i...

A Dummies Step by Step Guide to Pool Mining Verus Coin with a CPU!

8 min read · Jan 10, 2019

346 1

Max Theyse

How to preconvert into Bridge.vARRR

Participate in the first ever Verus PBaaS-chain launch — vARRR. Learn how to...

4 min read · Mar 20, 2024

259

See all from Max Theyse

See all from Verus Coin

Recommended from Medium

Albert Peter in Cryptocurrency Scripts

Top 5 Crypto Gems Predicted to Reach 100x-1000x Gains in 2024

Discover the top 5 crypto gems poised for 100x-1000x gains in 2024. Don't miss out on...

6 min read · Mar 14, 2024

538 13

Max Theyse in Verus Coin

Introducing Pure — The Currency 100% Backed by Verus & Bitcoin

Pure is a decentralized currency fully backed by Verus (VRSC) & Bitcoin (tBTC).

8 min read · Mar 16, 2024

196

Lists

Modern Marketing

103 stories · 523 saves

Generative AI Recommended Reading

52 stories · 894 saves

My Kind Of Medium (All-Time Faves)

71 stories · 261 saves

N. R. Crowningshield in Kaspa Currency

Kaspa: Accelerating Beyond the Blockchain

From a Concept to a Cutting-Edge Deployment

6 min read · Mar 18, 2024

107

Passive Crypto Mining

My Top 15 Passive Crypto Miners of 2024

I've spent 2 weeks compiling the most profitable Crypto Miners for 2024. You can...

11 min read · Jan 12, 2024

2K 29

Riti Thummalapenta

Is Quantum Computing the End of Blockchain?

An overview of the threats posed by quantum computing, and how we're tackling them.

4 min read · Oct 23, 2023

14 1

KryptoPunk

Bittensor wallet scanner: TensorScan AI (100x gem!)

Discover the revolutionary Bittensor Wallet Scanner: Tensor Scan AI, the ultimate gem i...

3 min read · Mar 22, 2024

122

See more recommendations