

Be part of a better internet. [Get 20% off membership for a limited time](#)

# Zenon Network: A Blistering Need For Speed

Zyler9985 · [Follow](#)

11 min read · Sep 1, 2023



...

The insatiable demand for kinetic energy is a chorus which repeats itself across time and space. Modern militaries are scrambling to produce hypersonic missiles, internet providers are rolling out powerful 5G networks and Bitcoiners are ever refining their ASICs to compute harder than their rivals. Faster, quicker, sooner — wen instantaneous?!

Speed is the name of the game. It's an inseparable core element of any competitive arena. The dominant players of any such competition know this

and leave nothing to chance. Take the Cheetah for example; mother nature's fastest land animal. Its fast-twitch muscle fibres, flexible spine, aerodynamic shape — every single characteristic it has is geared for breaking Mach 10.

Given Zenon's ambitions for being a scaling solution for Bitcoin as well as a sovereign ecosystem in its own right, an absolute requirement is this: Zenon must achieve peak scalability. If it were a video game, Zenon would need to cheese the game by maxing out its stats to be totally OP. Fortunately, **Zenon's unique design choices have laid the foundation for it to achieve maximal scalability without compromising elsewhere**, and that's what we're going to discuss in this article.

Disclaimer: This article is not financial advice and may contain speculation



Actual footage of a coked-up Mr Kaine designing the NoM.

## What is scalability?

Imagine that Zenon's 100 community members are all using the NoM.

Transactions are fast and cheap — everything is going well. But what if each community member utilises their ten alts? Now we have 1000 people/pseudo-people all trying to transact. Is the system still fast and cheap to use? Can Zenon scale to support a huge number of transactions, and therefore be adopted by a huge number of people? It's a broad question, but there are 3 hard metrics to help us measure this:

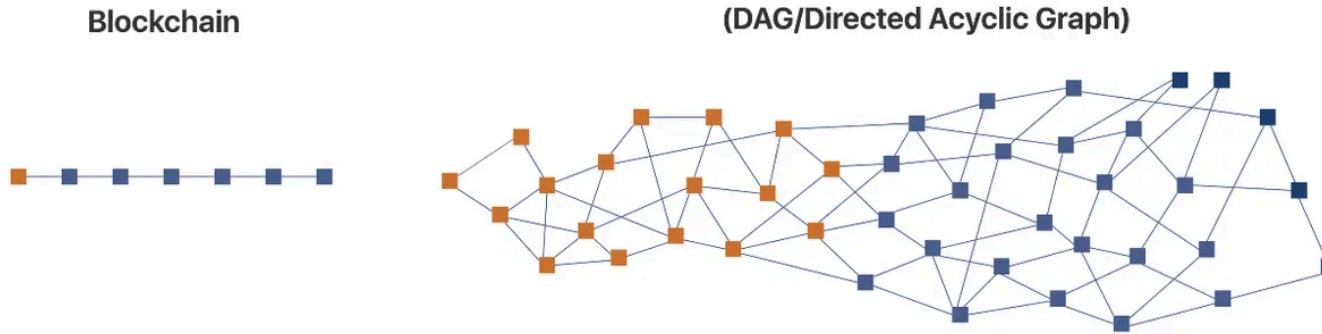
1. **Transaction Throughput.** This is how many transactions per second the network allows for, called the TPS. Traditional blockchains have maybe 100 TPS or 5k TPS, but these are rookie numbers. A 5k TPS means that if 5001 people all wanted to send a transaction at the same time, one guy's parachute wouldn't open.
2. **Transaction Latency.** Those transactions we were just talking about? This is how long it takes for the transaction that was sent to arrive. It's possible to have a high TPS, but what if each participant is waiting ten minutes for their transaction to go through? A KFC drive-thru would become a literal nightmare — a high latency is damn not cool. Typically this is measured in seconds, but projects like Ethereum might want to use minutes instead.
3. **Transaction Fees.** Also called cost efficiency. Are your users getting rekt by fees? In Ethereum it can cost \$100 to send \$100 in times of peak usage. It doesn't take an esteemed Economics professor to see those fees are mutually exclusive with mass-adoption.

As you can see, scalability is a balancing act where you want high throughput, low latency and low transaction fees. But there's another balancing act, one far more notorious ...

**The Blockchain Trilemma.** Derived from the CAP theorem. It describes the difficulties blockchains have historically had with balancing scalability, decentralisation and security. This is why some layer-1s claims of having a high TPS can actually be very misleading, as they might be compromising on their security or decentralisation. Or they might be manipulating their testing conditions so they can report an artificially high TPS. The real question: **Can you scale out in the real-world, without compromising on anything?** Speculators are betting that Zenon will.

## Traditional vs DAG-based Blockchains

A traditional blockchain can't handle many transactions, because it's like being stuck in single-lane traffic. Your car might be capable of going fast, but you're limited by the guy in front of you and you have to go at whatever speed he's going at. DAG-based blockchains however can handle more transactions, because you're not limited in the same way. DAG is like being in a multi-lane highway where you can overtake or drive in parallel to others. See the infographic below for a visual comparison:



As you can see, linear data structures simply don't have the high throughput of non-linear asynchronous structures. For this reason, Zenon is a DAG-based blockchain – but it innovates radically upon this concept.

## The Narwhal & Tusk Research Paper

In mid-2021, a ground-breaking research paper was released. It was called Narwhal & Tusk, and you can find it [here](#) or by googling it. The paper itself is awe-inspiring, but I'm personally more fascinated by the story around the paper. We'll get to that in a moment. Firstly, the findings.

Using a DAG-based blockchain, in a testnet environment they achieved ultra-scalability: **160 000 TPS with a 3-second latency**. Yes, such an achievement means they now have groupies.

For their DAG-based blockchain, they used a **two-layer architecture**. The first layer is the mempool which processes and stores transactions; this is called **Narwhal**. The second layer is the consensus layer which orders transactions and forms blocks; this is called **Tusk**. Tusk uses a Byzantine fault-tolerant (BFT) quorum-based consensus.

The hypothesis was that separating the mempool from the consensus will enable extreme scalability. Their findings supported this intuitive stance. Furthermore, Narwhal can **scale-out** indefinitely. The authors reject the assumption that validators must be limited to one computer; each validator can leverage multiple computers. As validators are given more resources, transaction throughput will also increase linearly **without** hurting the latency. The authors say there is no foreseeable limit with the scale-out; the potential TPS could even reach the millions. The exciting thing is that these numbers are big enough and sexy enough that they **actually support real-world use of the blockchain**.

Now ... for the story around the paper. In the acknowledgement section of the paper, the authors mention that much of their work was done while they were working at Facebook/Meta. Being a company with a market cap bigger than the GDP of most countries means they can obviously hire the best talent money can buy; that's probably why their research is so potent. Of course,

there does exist talent money can't buy. People with ethics and principles might not be a good fit for Facebook/Meta.



For anyone unfamiliar, Facebook/Meta tried to push through their own cryptocurrency called Libra/Diem with their own digital payments wallet called Novi. An American tech giant pushing their own currency? The US government saw this as an immediate threat and swiftly flexed their power to shut the whole thing down. How those vindictive clowns wish they could have done the same thing to Bitcoin; but that's the beauty of the orange coin — you can't stop it.

So where did those Facebook/Meta hires go after that debacle? Crypto is a small world. I wonder if they might one day find Zenon an appealing ecosystem to join. Not only are Zenon devs going to implement their findings, but Zenon's anonymous egalitarian launch, global community-ran status and leaderless nature make it the perfect candidate to avoid regulatory woes. And once we're big, there will be so much momentum no one can stop us anyway. Seeing as though Libra/Diem/Novi got regulated out of existence, joining Zenon would be a nice middle-finger to the centralised bullies they had a previous run-in with.

## Zenon's Unique Consensus Design

As we mentioned above, the premise of Narwhal & Tusk is that the consensus is a bottleneck for transaction throughput, and if you could separate it to a different layer that frees up the mempool to become a mega-

multi-lane highway which can also scale-out. They published this in mid-2021. Interesting, Zenon released a draft whitepaper in early 2020 ... also proposing DAG-based tech with a dual-ledger to separate the consensus. Great minds think alike?

But Narwhal & Tusk was not a conclusive paper. It paired Narwhal with different consensus designs. One was called Hotstuff (between that and one of Zenon's pillars being called bigd\*ckenergy, I can't even deal). But to make it resistant to asynchronicity and faults, they instead used Tusk — the increased latency was negligible and deemed a worthy tradeoff. **The main point of Narwhal & Tusk was not which consensus to use, but that it should be kept on a separate layer, so each layer can be optimised for its specific task.** So how to design the consensus?

Sometimes knowing what to do is the hard part, but executing it is easy. Other times knowing what to do is easy, but executing it is devilishly difficult. In this instance, we know what to do: Separate the consensus. How to do this though? **Let's discuss Zenon's unique consensus design, which is in the process of being built.** Speculators may revel at the thought of betting on its completion, or they may want to sit tight and keep an eye on how its progress is going.

## Pepper your angus, it's tech-talk thyme

With Zenon's dual-ledger architecture, the transaction ledger is a block-lattice. Each user therefore has an independent account chain which again is faster. The second ledger is the meta-DAG which is for the consensus. The novel approach is utilising 2 types of nodes — in Zenon nomenclature they are called sentinels and pillars — to create a **BFT consensus algorithm that is leaderless**. An important key to this is a novel concept known as a '**POW-LINK**', which will be explained below. Also important is that Zenon is designed as a **hybrid of PoW and PoS**.

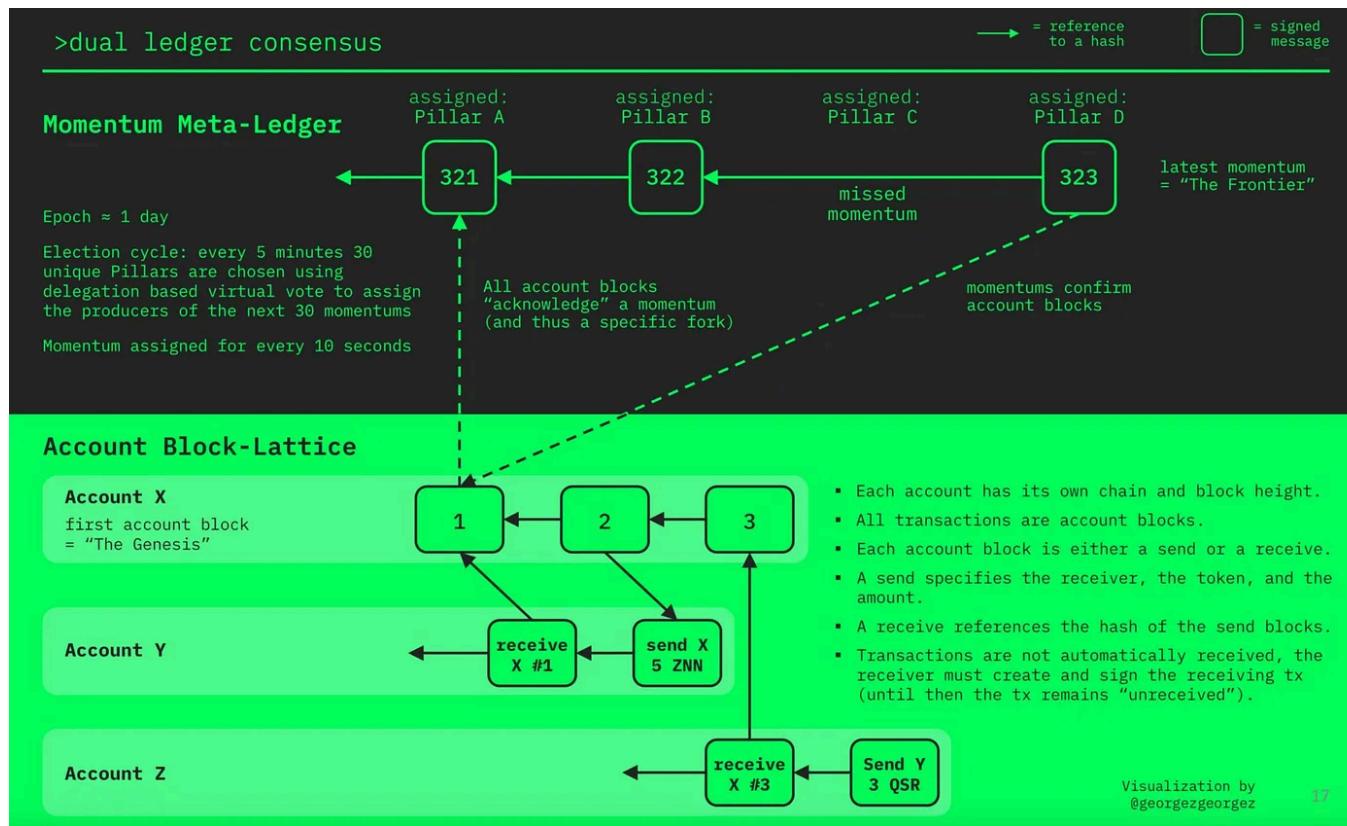
### Stage 1: Sentinels

Sentinels do not participate directly in the consensus, but are considered observers. When a user wants to make a transaction, the message is sent to a random group of sentinels. When this message is received, the sentinels do a proof-of-work computation to generate a receipt of the transaction. This receipt is relayed to a second group of sentinels, forming a chain of sorts. The POW-LINK chain must be at least 3 groups of sentinels long before the network decides the chain has enough weight. The POW-LINK is good for security as it acts as a sybil resistant layer in the network, defends against double-spending attacks and helps participation in the network among other things.



## Stage 2: Pillars

So like we said, the transaction triggers a message which creates a POW-LINK, and once it is of sufficient weight (at least 3 groups of sentinels) then the receipts are sent by the sentinels to random pillars. The pillars perform a PoW computation, and on solving it broadcast the transaction and virtual voting is applied.



Thanks gorgeous Georgez!

## Zenon is a hybrid of PoW & PoS

Classical BFT protocols work in centralised settings; but in a decentralised environment the nodes need a financial incentive to participate. Each epoch, not all pillars receive rewards. It's only the pillars which manage to solve their PoW puzzle before the supermajority does — so pillars are competing against each other. Competition always benefits customers. The competition between pillars will lead to better performance of information propagation.

In typical PoS blockchains, there are concerns with safety and governance because their committees are usually centralised. So even though they have a quorum, their collusion renders this a bit of a joke. A board of 7 people might need a quorum of 4 ‘yes’ votes to pass, but if 4 of the board members are circle-jerking meth goblins (\*cough\* FTX and their cult leader SBF), it’s really only a quorum of 1 because they are a unified group in cahoots with each other. I’ve always wanted to use cahoots in a sentence.

But the Zenon devs have found a way to mitigate this issue with PoS. So in a typical quorum, each node has an equal vote. If there are 80 nodes, each node is 1/80 chance of being chosen. But with Zenon, the pillars are not all equal as their stake weight is variable. ZNNAliens can choose which pillars to delegate their ZNN to. This increases the weight of that pillar, and the top 30 pillars are twice as likely to receive momentums & rewards, which can be shared with delegators. So to counter a bad actor who acquires a bunch of pillars, ZNNAliens can delegate their ZNN to trusted and respected pillars to increase their stake weight and chances of being chosen.

## Smart Contracts on the L2

The current consensus amongst the community devs is the layer-1 should remain feeless, minimalist, secure and efficient; the heavy work and bloat being kept to a separate execution domain. This means the smart contracts

will happen on two different layer-2s which are currently being built. One is for interoperability while the other is for scalability.

The **first solution** is a layer-2 which is EVM compatible/interoperable with existing blockchains — this is to enhance ecosystem growth. Expect some re-skinned racing games and cool NFT collections.

The **second solution** is a layer-2 which is extremely scalable/fast. The design is a Turing complete zero-knowledge general computation scaling solution that leverages unikernels. It would be written in a new programming language called Cairo, and the contracts would be called Starknet Contracts. It may also leverage Bitcoin as a data-availability layer.

The Unikernels are lightweight and optimised for running a single type of program. Their simplicity means they are efficient and fast, and it also makes security easier as there is less of an attack surface to account for. Sometimes less is more.

So not only are the smart contracts being delegated to a layer-2, but Unikernels are being used. **Both of these things are an innovation beyond what most other blockchains do and should further increase Zenon's scalability.**

## Conclusion

Like the Cheetah, every single characteristic Zenon has is intentionally chosen to optimise for ultra scalability:

- Zenon is DAG-based tech, much faster than traditional blockchains and each user has an independent account chain to again be faster
- Zenon is keeping the consensus to a separate layer like in the Narwhal & Tusk implementation for massive throughput that can scale-out without hurting latency
- Zenon has its own unique design for the consensus which is a meta-DAG that is a leaderless BFT protocol and a hybrid of PoW + PoS
- The smart contracts are being deferred to a layer-2 to keep the layer-1 minimalist; this will make both layers faster
- One of the layer-2s is designed for speed. It uses fast unikernels and is written in Cairo, the contracts being called Starknet Contracts
- Each community member finds it culturally acceptable to create ten or more alts, enabling massive community growth

This is the only way for Zenon to one day be the dominant sidechain to scale Bitcoin and bring DeFi to Bitcoin — it must be ultra scalable. It must also be

decentralised; see this article [HERE](#) to read more on that. As for security, the eventual merged mining will allow Zenon to tap into the power of the primordial timechain and you can read more on that [HERE](#). Again, much of this is still being built. The possibility to be early in this vision is appealing to speculators, techies and cypherpunks alike. DYOR ...

## **Thanks for reading!**

- Zyler

### **Sources:**

[Narwhal & Tusk paper from 2021](#) (also just google it)

[Zenon whitepaper from 2020](#) (find it on the main site)

[How to not fracture a layer-1 chain](#)

[What is Zenon Network?](#) and [What is a meta-DAG?](#)

### **Join The Community**

[Zenon.Network](#)

[Twitter/X](#)

[Telegram](#)

[Discord](#)

### **Zenon Community Public Key:**

npub1msvlamqj6j5azykts7sewtzr062a0km0p4hajw2dmchtm5xpz0aqylw09w

## The Zyler Reading List

1. [The Zenon Storybook](#) (updated version coming soon)
2. [Progressive Decentralisation](#)
3. [A Blistering Need For Speed](#)
4. [Alien Plans For Bitcoin](#)
5. [Why Zenon Is Regulation-Proof](#)
6. [Zenon's Synergy With Nostr](#)
7. [Merged Mining Bitcoin](#) (updated version coming soon)
8. [How Zenon Mirrors The Bitcoin Ethos](#)
9. [The Zenon Ethos](#)
10. [Zenon Network: A Noir Story](#)
11. [The Dream of Satoshi's Ethereum](#)
12. Zenostroin (Coming 2024)



## Written by Zyler9985

53 Followers

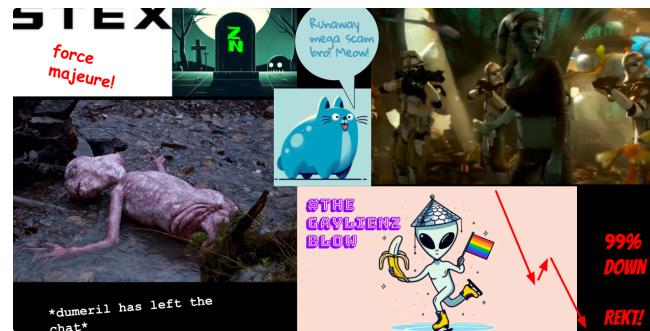
Follow



Please consider supporting me via donation. ZNN address:  
z1qzj03kklg3gvz36khev4rk5k6u0nlctcnn8xmr BTC address:  
bc1qq4qcpzs6euqypqhqu7n79l9yggq5cx3am7z6mq

---

### More from Zyler9985



 Zyler9985

### Why Zenon Is Going To Zero

Bitcoin's early days were fraught with struggle.



 Zyler9985

### Zenon Network: Alien Plans For Bitcoin

Jun 9 👏 22 💬 3

...

The purpose of this article is to explain and outline Zenon's roadmap with specific focus...

Jul 11, 2023 👏 290 💬 2

...



Zyler9985

## Zenon Network: A Zenocracy in Peril

After the events of Zenon Network: A Noir Story, our detective's journey isn't quite over...

Aug 10, 2022 👏 4 💬 1

...

Zyler9985

## Zenon Network: A Noir Story

Disclaimer: This short story is a work of fiction and does not constitute financial advice. It...

Jul 24, 2022 👏 53

...

[See all from Zyler9985](#)

## Recommended from Medium

**ALEXANDER NGUYEN**  
Software Development Engineer Mar. 2020 – May 2021

- Developed Amazon checkout and payment services to handle traffic of 10 Million daily global transactions
- Integrated frames for credit cards and bank accounts to secure 80% of all consumer traffic and prevent CSRF, cross-site scripting, and cookie-jacking
- Led Your Transactions implementation for JavaScript front-end framework to showcase consumer transactions and reduce call center costs by \$25 Million
- Recovered Saudi Arabia checkout failure impacting 4000+ customers due to incorrect GET form redirection

---

**Projects**

**NinjaPrep.io (React)**

- Platform to offer coding problem practice with built in code editor and written + video solutions in React
- Utilized Nginx to reverse proxy IP address on Digital Ocean hosts
- Developed using Styled-Components for 95% CSS styling to ensure proper CSS scoping
- Implemented Docker with Seccomp to safely run user submitted code with < 2.2s runtime

**HeatMap (JavaScript)**

- Visualized Google Takeout location data of location history using Google Maps API and Google Maps heatmap code with React
- Included local file system storage to reliably handle 5mb of location history data
- Implemented Express to include routing between pages and jQuery to parse Google Map and implement heatmap overlay

 Alexander Nguyen in Level Up Coding

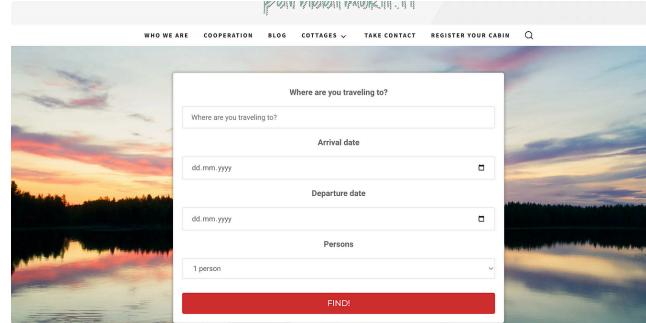
### The resume that got a software engineer a \$300,000 job at Google.

1-page. Well-formatted.

◆ Jun 1  13.4K  200



...



Where are you traveling to?

Arrival date: dd.mm.yyyy

Departure date: dd.mm.yyyy

Persons: 1 person

FIND!

 Artturi Jalli

### I Built an App in 6 Hours that Makes \$1,500/Mo

Copy my strategy!

◆ Jan 23  19.8K  210



...

## Lists



### Staff Picks

690 stories · 1145 saves



### Stories to Help You Level-Up at Work

19 stories · 695 saves



## Self-Improvement 101

20 stories · 2334 saves



## Productivity 101

20 stories · 2058 saves



Derek Johnson

## I'm Unemployed for Over Two Years (as a software engineer)

In 2022, I worked on a contract as a software engineer at Apple. Apple dissolved our entir...



May 31



4.6K



113



Unbecoming

## 10 Seconds That Ended My 20 Year Marriage

It's August in Northern Virginia, hot and humid. I still haven't showered from my...



Feb 16, 2022



83K



1134





 Abhay Parashar in The Pythoneers

## 17 Mindblowing Python Automation Scripts I Use Everyday

Scripts That Increased My Productivity and Performance

 Jul 10  2.9K  21

 ...

 Karolina Kozmana

## Common side effects of not drinking

By rejecting alcohol, you reject something very human, an extra limb that we have...

Jan 21  41K  1083

 ...

[See more recommendations](#)