Zenon Network: Alien Plans For Bitcoin

Zyler9985 · Follow

9 min read · May 20, 2023

Pieter Wuille, one of the chief architects behind the Taproot upgrade of Bitcoin, now famously declared that the real work will be in building wallets/protocols that make use of its advantages. Eerily prophetic, the new use-cases are starting to catch fire, beginning with the Ordinals craze in 2023. But beyond bloating the chain with JPEGs — are there more meaningful ways to leverage the highly anticipated agreed soft fork of November 2021? Are there other ways an integration with Bitcoin could occur? This article discusses Zenon Network's plans for interoperability with

native Bitcoin and how it can work as a scaling solution for the primordial time-chain.

The Premise

Zenon Network is a new layer-1 crypto which since genesis has closely adhered to the same ethos and values as Bitcoin. It is feeless thanks to a novel anti-spam mechanism enabled by its dual-coin economy. Its mainnet

went live in November of 2021 and in April of 2022 its on-chain funding system was released to empower global contributors.

The premise of this piece is that Zenon Network is planning on interoperability with native Bitcoin with a view to scaling it and bringing smart contracts and Defi to the Bitcoin ecosystem. There are 6 ideas currently being discussed and worked now, but two things to cover first:

1. Some of these ideas are based on established tech, others are more on the cutting-edge and can be described as experimental in nature. The probability of success is obviously interesting for speculators, but it is also a chance for devs to make a name for themselves by helping Zenon in its foundational era.
2. Suppose Zenon Network is successful with its tech ambitions; what's to stop another chain from copying its tech? What's to entice Bitcoiners to accept the integration with Zenon? The answer to both of those questions is that Zenon is truly decentralised due to its unique inception and organic growth. In the future you could copy its tech, but you can't copy its decentralisation. See this article here for a discussion of its decentralisation, and be sure to see the links towards the end of the article for further reading.

Idea #1: TSS technology

TSS stands for Threshold Signature Scheme. In practice, TSS allows N participants from a total of T participants to approve the spending of assets, as long as the threshold of N is reached. For example, the signing authority may be distributed amongst 4 parties, and as long as at least 3 agree, the Bitcoin can be spent.

In the context of Zenon, the participants would be Pillars (Zenon nomenclature for validator nodes). They would take on the role of being custodians for the Bitcoin. The ecdsa–TSS could control Native Bitcoin or Bitcoin wrapped on Zenon (zBTC).

Idea #2: Atomic Swaps

HTLC (Hashed Time-Locked Contract) is a smart contract where the assets are locked until a condition is met, such as a time limit or the presentation of a cryptographic proof. PTLC (Point Time-Locked Contract) is a variant which enables greater privacy. MuSig2 is a multi-signature algorithm that allows multiple parties to collaboratively approve a transaction. Combining PTLC with MuSig2 allows for transactions where the control is distributed amongst multiple parties and the permission of all participants is required for it to proceed.

In practice this allows for more complexity with Bitcoin transactions while maintaining a high level of security and reliability. Within the atomic swaps discussion there has been a mention of the xClaim method. In their 2019 research paper, they describe a more efficient implementation for trustless atomic swaps which is cheaper and faster and leverages the concept of cryptocurrency-backed assets (CbAs). Click here for another resource for people exploring something similar.

Idea #3: Layer-2 Solutions (EVM-compatible)

The current consensus amongst the community devs is that the layer-1 should remain feeless, minimalist and efficient; the heavy work and bloat being kept to a separate execution domain. This means the smart contracts will happen on two different types of layer-2 solutions that are currently being worked on. They are not mutually exclusive; 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 will enhance ecosystem growth.

Sidechains enable the transfer of assets between the mainchain and the sidechain, mainly so more complex work can be done while drawing on the security of the underlying layer-1. But because its focus is on extending the

functionality of the mainchain, this layer-2 solution is more accurately described as an extension chain.

ZNN (Zenon) may be bridged to become xZNN (extension Zenon) which will be the gas token for the extension chain. The backing may not be 1:1 because in the extension chain xZNN will be partly burned. One idea for the fee distribution mechanism is 33% to builders/contract deployers, 33% to extension chain validators and 34% burned. ZNN was chosen because relative to QSR it has a high inflation rate and low burn rate. Furthermore, since validators produce ZNN, they can be validators for the extension chain as well and share their inflation to sustain the system subject to demand.

However, these details aren't finalised. It may be that zBTC is bridged from the layer-1 to the extension chain where it will become xBTC and can be used for the fee system instead of xZNN.

Idea #4: Layer-2 Solutions (Zero-knowledge proofs)

A layer-2 which is extremely scalable/fast — this will enable mass-adoption of Zenon as it proves to be practical and robust for real-world use. The design for this layer-2 is a Turing complete zero-knowledge general computation scaling solution that leverages unikernals. It would be written

in a new programming language called Cairo, and the contracts would be called Starknet Contracts. To break down the components:

Turing complete means the computational system can perform any computation that can be described algorithmically; this means absolute competency in executing complex programs and solving a wide range of computational tasks/problems.

The inclusion of zero-knowledge proofs will bring security and privacy, because it allows for something to be verified without requiring the complete information set. The complete information set could include sensitive information that infringes on privacy.

Unikernals 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.

The Taproot upgrade of November 2021 introduced a number of new features to the Bitcoin scripting language. Schnorr signatures and Script path spending allow for more efficient and complex transactions. Taproot outputs is also a key feature, as they can be used for a variety of purposes. Prior to

Taproot, the only way to store data on Bitcoin was with a smart contract, but that is obviously expensive, slow and carries the risk of exploits. Now, Taproot outputs allow for the storage of data on Bitcoin without using smart contracts, meaning it is simple, efficient and secure.

Bitcoin could be used as a data availability layer for zero-knowledge smart contracts. The reference is on-chain on Bitcoin, but instead of referencing a JPEG it will be referencing data stored off-chain (off Bitcoin). For example, suppose a Zenon smart contract is used to store and manage medical records. The medical records could be encrypted using a zero-knowledge proof and stored off-chain. The smart contract could then reference the data on-chain (on Bitcoin) using a cryptographic hash. This would allow the smart contract to prove that it has access to the medical records without revealing the actual records themselves. This would provide an additional layer of privacy for patients.

Zenon could thus use Bitcoin as a data availability layer for smart contracts, meaning the layer-2 would be leveraging the most robust, secure and decentralised database in the world.

Idea #5: Merged Mining

Mining in Bitcoin is the process of solving complex mathematical problems in order to confirm transactions and record them on the blockchain. Miners who successfully do this are rewarded with newly minted Bitcoin as well as with the transaction fees for that block. The intense competition between Miners has led to specialised hardware as well as the formation of mining pools. Essentially, multiple parties combine their computational power to increase their chances of being rewarded, and this reward is shared amongst individual members of the pool in proportion to the hash power they contributed.

Merged mining is a situation where miners can simultaneously mine multiple blockchains using the same hardware. The same hash puzzle is solved to validate both blockchains at the same time. The secondary blockchain (Zenon) would need to be designed to support merged mining. Zenon's consensus would need to recognise and include the proof of work from Bitcoin — and if you read Zenon's whitepaper, the fully realised vision for Zenon is a hybrid of proof of stake and proof of work. Furthermore, Zenon would need to entice the Bitcoin miners to want to merge mine it. The direct incentive for the Bitcoin miners would be the inflationary ZNN rewards and the overall value-add that Zenon brings to Bitcoin's ecosystem. The incentive for Zenon validators is that they stay competitive with earning rewards and can draw from the security of Bitcoin's tremendous hash power.

See here for a more general and indepth discussion of modern merged mining. Rather than a traditional merge-mined sidechain, Zenon could be designed with a BTC relay such that it would be a merge-mined SyncChain. This is more flexible because if Zenon already has a Bitcoin relay, it is easy to transfer value from Bitcoin to Zenon by forwarding the Bitcoin headers and the Bitcoin peg-in transactions from Bitcoin to the Bitcoin relay contract as part of Zenon's consensus.

Idea #6: BRC-20 tokens

Bitcoin Ordinals are created by using the Taproot output to create a transaction that assigns a unique identifier to a satoshi. The identifier makes the satoshi distinguishable from others; it thus classifies as an NFT on Bitcoin. They are indivisible, non-fungible and are being used as NFTs.

BRC-20 tokens are built on Bitcoin. It utilises Ordinal inscriptions of JSON data to deploy token contracts, mint tokens, and transfer tokens. See here for in-depth information about BRC-20 tokens. They are divisible, fungible and are expected to be used in DeFi and in NFTs. They can represent a variety of assets such as Bitcoin, other cryptocurrencies or fiat.

The Zenon devs have suggested that BRC-20 tokens could be ported to become ZTS tokens (tokens issued on Zenon, analogous to erc-20 tokens on

Ethereum) for feeless transactions.

Parting Thoughts

This article has discussed a number of possibilities for integration with Bitcoin and what the future of DeFi with BTC could look like with Zenon. Some of these have already had significant progress made (atomic swaps) while others have only just started to be worked on (both layer-2 solutions). The other possibilities seem to be further down the roadmap (merged mining) or purely experimental in nature (integrations with BRC-20 tokens).

Notably, many of these concepts flow from Taproot. Perhaps Block 709 632 is more historic and significant than the wider Bitcoin community currently realises. The Zenon devs certainly think so, as they signed it with ASC-II art. Arguably this is the real first picture on Bitcoin since that fateful fork …

Links To Learn More

The Main Site

The Official Twitter Account

A community-built site for news, info and education.

A community-run Twitter account for news and updates.

Don’t hesitate to reach out to the Zenon Community on Twitter, Discord, Telegram or the Forum if you have any questions or would like to get involved. For example, Accelerator-Z is an on-chain funding mechanism to

reward contributors who add value to the ecosystem — this applies whether your skills are in tech, marketing or sales.

Thanks for reading. And remember ...

The future is encrypted, it is up to you to decrypt it!

Written by Zyler9985

Follow

53 Followers

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.

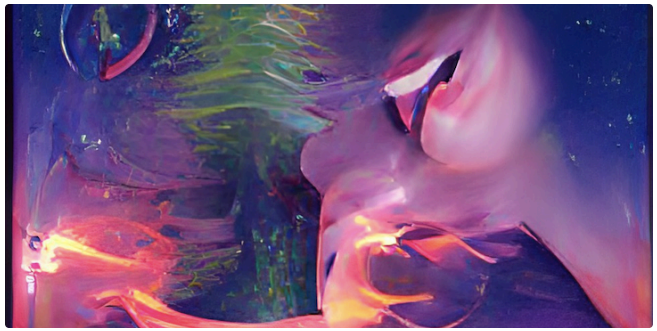
Jun 9 22 3

Zyler9985

Zenon Network: Alien Plans For Bitcoin

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

Software Development Engineer Mar. 2020 – May 2021

- Developed Amazon checkout and payment services to handle traffic of 10 Million daily global transactions
- Integrated Iframes 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

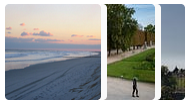
Unbecoming

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

Lists

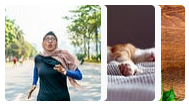


Staff Picks

690 stories · 1145 saves

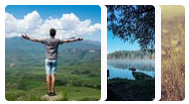
Stories to Help You Level-Up at Work

19 stories · 695 saves



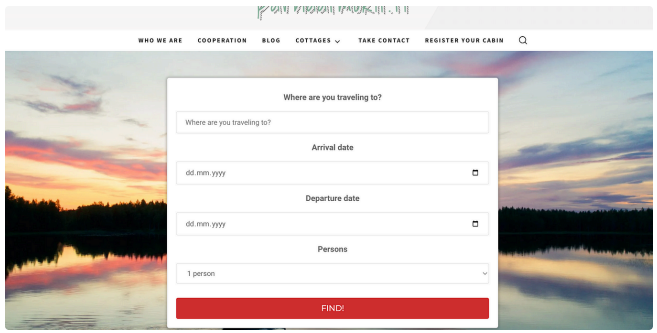
Self-Improvement 101

20 stories · 2334 saves



Productivity 101

20 stories · 2058 saves



Jamil Yousafzay in Coinmonks

Need Money Today? This Crypto App Pays Daily (For Just $1...

A beginner's step-by-step guide to registering your account and starting to ma...

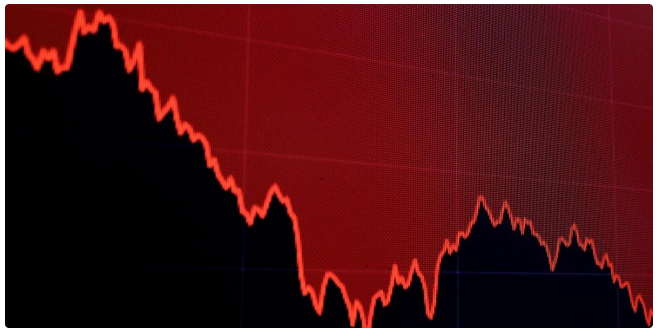
Jul 1 120 7

Artturi Jalli

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

Copy my strategy!

Jan 23 19.8K 210



Derick David in Utopian

Crypto Is Dead.

I've been in crypto for years now, I saw it all—the highs, the lows, and the memes. I worke...

Jan 31 3.4K 233

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