ATOM's Highwire Act: Balancing Security in a Shared Cosmos

[Figment Capital](#)

[Follow](#)

--

Listen

Share

By:

[VelvetMilkman

](https://twitter.com/VelvetMilkman)

Hub Minimalism

A common tendency of decentralized networks has been to add more features to the base chain. While encouraging experimentation and permissionless innovation in various forms, the Cosmos ecosystem has taken a different approach by rejecting a formal base chain and instead maintaining "Cosmos Hub" minimalism. Minimalism encourages experimentation to take place in separately connected application specific blockchains.

Within the context of the Cosmos ecosystem, "hub minimalism" refers to a design principle that believes the Cosmos Hub should have minimal features and complexity. The purpose of keeping the Cosmos Hub's features minimal is to enhance security, reduce the attack surface, and maintain focus on its core functionality: facilitating inter-blockchain communication and transactions.

By keeping the Cosmos Hub minimal, developers have the freedom to build completely unique features and functionalities on separate chains connected to the Cosmos Hub. These independent blockchains, also known as "zones," have their own applications, execution environments, consensus layers, and governance structures. The Cosmos Hub acts as a common thread across zones, allowing them to exchange information and value while ensuring the security and integrity of its own chain remains intact.

Users can utilize their ATOM to participate in the network's proof-of-stake mechanism, vote on governance proposals, and participate in economic activities.

- Security:

By staking ATOM, users help secure the network and, in return, receive rewards in the form of additional ATOM tokens.

- Governance:

ATOM holders can propose and vote on changes to the network's parameters, upgrades, and funding proposals.

- Economic Activities:

ATOM tokens can be used for various economic activities within the Cosmos Network. The ATOM token is oftentimes used as a medium of exchange. Users can pay transaction fees in ATOM when transacting on the network.

The minimalism movement adopted by the Cosmos Hub (the "Hub") has understandably led many community members and casual observers to question the purpose and utility of the chain (ie, "what is the ATOM token actually supposed to do

?"). You can buy ATOM, spend ATOM, vote with ATOM, and stake ATOM to earn more

ATOM. Beyond those three functions, the Cosmos Hub hasn't historically done much else. It doesn't allow applications to be built on top of it, for example. As the longest standing Cosmos network in existence, ATOM's only semi-utility is its ability to function as a neutral, decentralized, and exportable medium of exchange (ie, "money") throughout the Cosmos ecosystem.

Yet, this use case is at risk. Recently, fiat-backed stablecoins have begun being minted natively in the Cosmos via Noble (USDC) and Kava (USDT); fully collateralized WBTC is being minted on Osmosis. These recent developments are a net positive for the Cosmos ecosystem but risk unseating ATOM's position as the ecosystem's default form of "money." In order for the Cosmos Hub to create utility for the ATOM token and

stay true to its minimalist design philosophy, several value accrual mechanisms have been proposed. The most notable

experimental strategy has been the formation of a shared security alliance between the Hub and various Cosmos chains called Replicated Security. This innovative approach seeks to enhance ATOM's utility while increasing the economic security of Cosmos chains that opt-in to the alliance.

Sharing is Securing

In the broader context of blockchain technology, the term 'shared security' commonly refers to leveraging the security guarantees of one decentralized system to fortify another. Shared security models offer decentralization on demand for emerging networks while offering a greater degree of connectivity to the network they're borrowing security from.

Practically speaking, shared security onboards a subset of an existing, reputable validator set that commits to also securing emerging chains. This arrangement enables these new chains to benefit from the robustness and established trust of the primary network's validator set. Validators are incentivized to opt-in to additional slashing criteria in exchange for maintaining the integrity and security of both the primary chain and its security consumers, effectively spreading their stewardship and trust across multiple networks.

Shared security has the potential to transcend the conventional boundaries of merely offering economic security. Its implications extend into crucial aspects of blockchain such as scalability, economic incentivization, and usability. By implementing shared security, the Cosmos Hub can enhance the Cosmos Hub's ability to help scale its growing ecosystem; it allows smaller, emerging chains to operate without the overhead of developing and maintaining their own security infrastructure. This reduces barriers to entry, unlocking a more vibrant and diverse ecosystem of chains.

Shared security attempts to address critical aspects of economic incentivization. Theoretically, emerging chains can redirect resources (typically allocated for security infrastructure development) towards innovation and growth. This creates a more efficient allocation of resources within the ecosystem. Realistically, the motivation of shared security is to signal social alignment with the security provider's community. Shared security offers an economic benefit to the primary network and its validators and receives kickbacks for extending their security services, creating a symbiotic economic relationship. Once the shared security ecosystem has matured, we expect bootstrapping to streamline and remove several of the bottlenecks that currently exist.

Shared security also simplifies the end-user experience. Users can engage with multiple chains within the ecosystem, assured by the uniformity and reliability of the security model (assuming the entire validator set supports another chain). This not only enhances user confidence but also promotes greater adoption and interaction across the network.

Shared security represents a paradigm shift in the blockchain landscape. Its influence on blockchain architectures will remain a key focus in the coming years. An economically sustainable shared security framework can become a core value proposition of crypto-economies — if properly designed and executed. We believe shared security will realize interchain partnerships, further emphasizing the need for continued research into technical feasibility and economic sustainability. By fostering an interconnected network of chains that support and reinforce each other, shared security paves the way for a more resilient, scalable, and user-friendly blockchain ecosystem.

Replicated Security

The launch of Replicated Security (RS) marked the dawn of the Cosmos Hub's shared security experiment. RS actualizes the theoretical concept of Interchain Security (ICS) by enabling the practical application of shared security across different blockchains within the Cosmos ecosystem. It is the first instance where the security of one blockchain (the Cosmos Hub) is approved through token voting and extended to secure otherwise independent blockchains.[1] The launch of RS operationalizes the idea of interconnected blockchain security. However the RS framework serves as more than just a security feature; it's a strategic initiative to increase the utility of the ATOM token, with the goal to elevate its intrinsic value and importance across the ecosystem.

RS allows the Cosmos Hub to lend its active validator set to other chains within the Cosmos ecosystem. This not only enhances the security of these emerging chains but also solidifies the Cosmos Hub's role as a central, stabilizing economic force in the ecosystem. RS increases the utility of ATOM by enabling other blockchains with lower security guarantees to tap into ATOM's valuable economic security. It also onboards one of the most reputable validator sets in Cosmos.

A "consumer chain" is a blockchain that is secured by the validator set of a "security guarantor," in this case the Cosmos Hub. Generally speaking, consumer chains enter into a service level agreement (SLA)

with the provider chain.[2] In RS's case, the Cosmos Hub (service provider) agrees to provide economic security to the consumer chain (service user) in return for compensation.

RS requires every validator running on the Cosmos Hub to operate a new validator node for the consumer chain, replicating

the active validator set of the Cosmos Hub. Today, the current validator set secures ~$2.7B worth of ATOM across 180 validators.[3] When a new consumer chain is approved, the Cosmos Hub agrees to include additional slashing conditions to the validators securing the Cosmos Hub. If an operator misbehaves or performs poorly on a consumer chain, the responsible validator (and its delegates) have their staked ATOM slashed on the Cosmos Hub.

In return for providing block production services, the consumer chain agrees to compensate the Cosmos Hub. While the terms of each SLA may vary, thus far most proposals have followed a similar playbook. The consumer chain typically proposes to share a minority share of protocol revenue with the Cosmos Hub in exchange for economic security.[4] Protocol revenue typically comes from three main sources: transaction fees, MEV, and inflation (if applicable).[5]

RS creates a new value accrual mechanism for the ATOM token. Its innovative design enables the Cosmos Hub to capitalize on the economic value staked to its validator set and offers a creative new way for blockchains to form economic and social alignment with the Cosmos Hub. In totality, the Cosmos Hub and consumer chains form the Atom Economic Zone (AEZ). The creation of the AEZ and subsequent launch of RS is the first meaningful step taken by the Cosmos Hub community to create utility for the ATOM token. If successful, shared security has the potential to boost the entire ecosystem, improve the ATOM token's utility, and create one of the most valuable services across the Interchain.

In our opinion, the most interesting (and overlooked) aspect of RS is its timing to market. RS is the first of several new shared security frameworks preparing to launch. It offers other teams an opportunity to learn from its early success as well as any missteps and changes subsequently made. Observing its benefits and challenges will have an impact on the future of ICS and shared security more broadly. RS's evolution over the coming months and years can help shape subsequent shared security models in Cosmos (Mesh Security) and in other ecosystems (such as EigenLayer in Ethereum). From economics to technical implementations and governance, the data points and lessons taken away from observing RS can help inform ecosystems designing their own shared security solutions. Should RS succeed, it will have played an integral part in redefining the way in which blockchains are secured.

The remainder of this article serves as a strong endorsement for the concept of shared security through the lens of Replicated Security. We highlight the advantages it offers and identify some of the challenges facing the current version of RS. Addressing these challenges and sharing insights with the broader community is key to identifying and proactively addressing lesser-known obstacles down the road.