Omni: Ethereum-Native Interoperability

Omni Labs

March 7, 2024

Abstract

Ethereum's adoption of the rollup-centric roadmap has created isolated execution environments, dividing capital, users, and developers across rollup domains. Addressing these issues, Omni was developed to provide Ethereum-native interoperability in a secure, performant, and globally compatible manner. Omni establishes a new precedent for secure interoperability by deriving its cryptoeconomic security from restaked $ETH. Building on its novel security framework, Omni features a custom network architecture that is capable of verifying cross-rollup messages with sub-second finality. Omni's design facilitates ease of use and development across rollups with its emphasis on minimal integration requirements and the introduction of a universal gas marketplace alongside the Omni EVM. By establishing Ethereum-native rollup interoperability with minimal latency, Omni alleviates the negative externalities associated with rollup fragmentation, enabling Ethereum to return to its role as a unified network for decentralized applications.

1 Fractured Blockchain Scaling

More than three years have elapsed since the Ethereum community endorsed the rollup-centric roadmap, marking the end of a comprehensive search for a scaling solution that would enhance Ethereum's throughput without sacrificing security, performance, or compatibility with the broader ecosystem. This search began during Ethereum's early development stages, which were inherently motivated by a desire to overcome the scalability and efficiency limitations observed in previous blockchain designs. While sharding was part of a long-term vision for scalability, the initial architecture focused on foundational elements that could later accommodate such advanced solutions. Building on this foundation, Ethereum's journey toward enhanced scalability saw the exploration of technologies including payment channels, state channels, and Plasma. This iterative process eventually culminated in the development of rollups, marking a significant advancement in Ethereum's scaling efforts.

By executing transactions off-chain and only storing data and/or proofs on-chain, rollups scale Ethereum in a secure, performant manner while ensuring compatibility with smart contracts and applications. Rollups provide secure off-chain execution environments by relying on Ethereum Layer 1 (L1) for consensus on state updates. Importantly, rollups also provide users with an uncensorable exit mechanism for transferring their capital back to Ethereum L1 in case of emergency. Leveraging Ethereum L1's robust security, rollups are free to optimize their execution environments for performance and compatibility. From a performance perspective, rollups are designed to reduce network congestion on Ethereum and lower transaction costs for users. In terms of compatibility, rollups' Turing-complete nature and support for multiple programming languages empower them to be adaptable to existing developer tooling and infrastructure services. This lowers the barrier to adoption for developers and enables them to create execution environments tailored for different use cases.

Despite these benefits, the rollup-centric approach forces Ethereum to scale via isolated execution environments. This creates a series of negative externalities that degrade Ethereum's network effects. The division of liquidity across multiple rollups diminishes the capital pool accessible to applications, leading to inferior economic properties compared to a unified

Archived copy · cryp2nova.com

system. Consequently, distinct rollup environments force users to interact with multiple application instances across these isolated rollup economies.

For developers, this situation necessitates a shift in focus towards managing distributed state between environments rather than focusing on application functionality and utility. This requirement stands in stark contrast to the original design intentions of the Ethereum Virtual Machine (EVM). The EVM is engineered to abstract away the complexities of distributed state, even though it is operated by hundreds of thousands of nodes on Ethereum L1 [1]. This abstraction empowers developers to program as if they were dealing with a singular CPU and state machine, thereby simplifying application development and minimizing the risk of potential software vulnerabilities. However, the dispersion of users across rollups now requires developers to manage several subcomponents of their applications across independent rollups to access all of Ethereum's users and capital.

On our current trajectory, the expanding variety of rollup designs and their growing adoption will only exacerbate these issues. Consequently, Ethereum is faced with an existential threat that requires a native interoperability protocol purpose-built to realign Ethereum with its original vision of being a single, unified operating system for decentralized applications.

2 Interoperability for Ethereum Rollups

The purpose of any interoperability protocol is to verify the state of a source network and relay state updates to destination networks. To reflect the fundamental properties of its rollup ecosystem, the ideal Ethereum interoperability solution must provide this service in a way that is also secure, performant, and globally compatible with the Ethereum ecosystem. To meet our security standards, the solution should derive its security from the same source as Ethereum rollups: Ethereum L1. To be considered performant, the interoperability protocol must verify and process cross-rollup messages with minimal latency. Finally, for the protocol to be globally compatible, it must enable applications to be Turing-complete across all rollup environments, ensuring that applications are not limited by the resource constraints of any single rollup.

Interoperability protocols offer different security guarantees depending on how they verify the state changes of their supported networks. Existing protocol designs can be broadly classified according to the four categories of verification as defined in Table 1 [2].

Table 1: Interoperability Verification Types

Verification Type	
Native	Security providers of the underlying networks validate the data communicated between networks.
Local	Only the parties involved in a given cross-network interaction verify the interaction.
Optimistic	Every message is assumed to be valid and full verification is only performed if a dispute is raised.
External	A set of third-party security providers is used to validate the data communicated between networks.

Natively verified systems offer the only fully trustless approach to interoperability. However, these systems are the most difficult to implement since they require the security providers of the underlying networks to validate state changes. Given that rollups obtain their security from Ethereum L1, the sole method to establish a natively verified interoperability solution for rollups is to use Ethereum L1 for validating rollup state changes. This can be done with smart contracts that use optimistic or zero-knowledge verification mechanisms. However, the run times of these processes on Ethereum L1 carry high costs and latency with optimistic verification requiring a seven-day challenge period and zero-knowledge verification requiring several hours. As a result, Ethereum L1 does not meet our desired performance criteria and compels us to explore alternative verification mechanisms.

Similar to a strictly native approach, other interoperability solutions also fail to meet our three key criteria. Solutions that rely on local verification provide strong security guarantees and can be applied across various rollups, yet their inability to handle arbitrary messages limits their application compatibility. Optimistic approaches, which incorporate a latency period for potential challenges, inherently do not satisfy our performance requirement.

Externally verified systems are the only solution that can support our desired performance and global compatibility requirements. However, this approach introduces trust assumptions tied to an external verifier set, thereby compromising on our security requirement. To mitigate these trust assumptions, externally verified systems can introduce cryptoeconomic security measures that require the verification set to commit capital that is at risk of being slashed in the event of misconduct. Interoperability protocols that choose to implement this model can be considered game-theoretically secure as long as the staked value of their verifier set is greater than the value that the verifier set can transfer in a single state transition period. However, existing solutions that use this approach derive their cryptoeconomic security from a

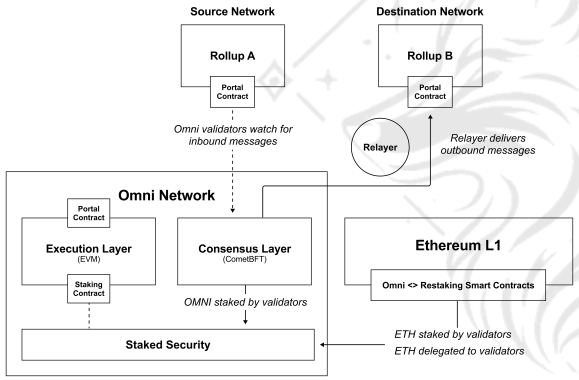
Archived copy · cryp2nova.com

native asset rather than Ethereum L1, making them unfit for our security requirements. By devising a method to extend Ethereum L1's cryptoeconomic security to an external set of verifiers, we can fulfill our security criteria and create a novel interoperability solution that offers all three of our desired properties.

3 Omni

The guiding principle of modular design theory is the separation of a system into distinct, isolated components, each optimized for a specific function. Applying this approach to existing interoperability solutions, we created Omni, a natively secured, externally verified interoperability network that establishes a new precedent in security, performance, and global compatibility for the future of Ethereum's modular ecosystem.

Figure 1: Omni Protocol Overview



Omni realizes this vision by introducing a novel network architecture tailored for low latency cross-rollup communications and global compatibility with Ethereum's entire rollup ecosystem, underpinned by the cryptoeconomic security of restaked $ETH. This design achieves sub-second cross-rollup message verification while harnessing Ethereum's industry-leading cryptoeconomic security budget. Furthermore, Omni is intentionally designed to be easily integrated with any rollup architecture and local rollup application, while also providing a programmable state layer for managing application deployments across rollups. The following sections of this whitepaper will explore the architectural evolution of Omni, detailing how it fulfills our design requirements of security, performance, and global compatibility.

4 Security

Externally verified interoperability systems optimize for performance and compatibility but compromise on security guarantees. Their ability to easily connect with various networks and offer rapid verification allows them to provide a desirable user experience, contributing to their widespread adoption throughout the industry. However, securing these systems has been a persistent challenge, with no clear solution that offers robust and stable security at scale.

The simplest method to secure an externally verified system is to rely on a trusted verifier set. While straightforward to implement, this approach provides minimal security, especially when verifiers remain anonymous, thereby raising the risk of collusion. A marginally better strategy involves using public entities as verifiers, relying on their reputation as a deterrent against collusion. Still, this method remains vulnerable, as these entities can become targets for attacks, particularly if a single entity controls multiple verifiers. As a result, a number of protocols using these trusted verification methods have fallen victim to exploits, cumulatively costing the industry over $1 billion.

Improving upon the trusted verifier model, protocols can use cryptoeconomic security to introduce a new dimension of security to an external verifier set [3]. This approach has been attempted by several prior networks but encounters inherent limitations due to its reliance on the protocol's native asset for security. Under this approach, the scale of the protocol's security is directly tied to the demand for the protocol's asset, introducing reflexive dynamics that result in unstable security guarantees. To establish a security model that is both stable and secure at the scale of the modular ecosystem, it is essential to derive cryptoeconomic security from a broader network.

Prior to the advent of EigenLayer's restaking, a novel primitive that extends Ethereum L1's cryptoeconomic security to external networks by reusing staked $ETH from Ethereum's consensus layer [4], achieving this level of security was unattainable. Now, restaking enables Omni to leverage the cryptoeconomic security of Ethereum L1 for its own validator set.

Archived copy · cryp2nova.com

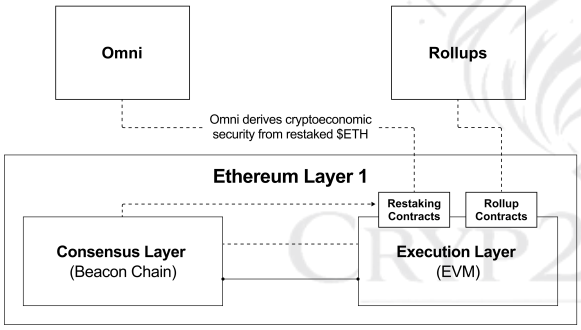
The cryptoeconomic security provided by restaked $ETH, C_e, is given by the formula:

$$C_e = \frac{2}{3} \sum_{v=0}^{n} P(S_v)$$

- S_v = the amount of $ETH restaked by validator v
- P = the function mapping the amount of restaked $ETH to validator power
- n = the total number of validators

With more than $100 billion securing the network, Ethereum's current security budget is an order of magnitude larger than any other Proof of Stake (PoS) network [5]. By leveraging restaked $ETH, a highly liquid, low volatility asset, Omni's security achieves significantly greater stability than its predecessors. Moreover, by deriving security from Ethereum, Omni aligns its security base with the rollups it connects, facilitating a security model that grows in tandem with Ethereum's modular ecosystem. By implementing a cryptoeconomic security model using restaked $ETH, Omni establishes a new paradigm for secure and reliable interoperability across the entire industry.

Figure 2: Security Overview



5 Performance

Having identified restaking as our desired security mechanism, our focus shifts to building a performant protocol architecture. Specifically, our goal is to create an externally verified protocol that minimizes the verification time for cross-rollup messages (XMsgs) and is secured by restaked $ETH. The CometBFT consensus engine (i.e. Tendermint) offers properties that fulfill both of these requirements [6].

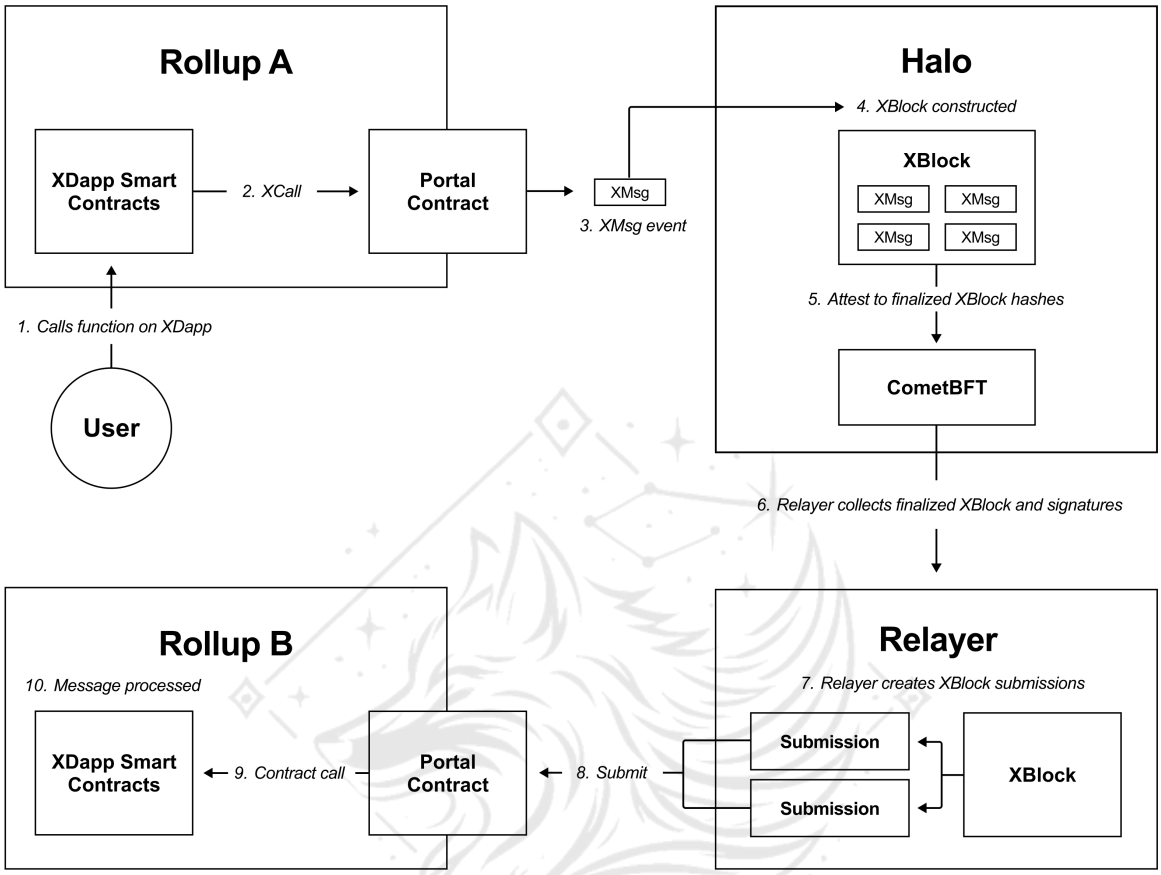
1. CometBFT delivers instant transaction finality, thereby removing the need for additional confirmations or concerns for block reorganizations within Omni. This makes Omni's finality time solely determined by the time it takes for Omni validators to reach consensus.
2. CometBFT also provides support for Delegated Proof of Stake (DPoS) consensus mechanisms, a natural fit for Omni validators to accept restaked $ETH delegations.
3. Finally, CometBFT is one of the most robust and widely tested PoS consensus models that is used in several production blockchain networks that each secure billions of dollars.

Omni uses CometBFT to process XMsgs according to the sequence visualized in Figure 3. First, Omni validators operate full nodes for each rollup virtual machine (VM) to check for XMsg requests. For every rollup VM block that contains XMsg requests, Omni validators build an XBlock containing the corresponding XMsgs. During CometBFT consensus, Omni validators use the vote extension feature from Cosmos' second generation Application Blockchain Interface (ABCI++) to attest to XBlock hashes [7]. Finally, external relayers re-package and deliver finalized XMsgs to their destination rollups. Through this process, Omni achieves sub-second XMsg finality backed by previously unparalleled levels of cryptoeconomic security.

The XMsg verification process is designed with a foundational security standard. Omni validators wait for XMsg requests to finalize on Ethereum L1 (2 epochs, ∼12 minutes) before attesting to their validity in consensus. However, this design is intentionally decoupled from consensus so that low-latency finality mechanisms can be used. Specifically, this can be achieved using transaction insurance mechanisms on a message's source rollup or pre-confirmations from technologies like shared sequencers [[8],[9]]. By supporting these alternative finality mechanisms, Omni will deliver an end-user experience for cross-rollup messaging that mirrors modern cloud-based applications.

Archived copy · cryp2nova.com

Figure 3: XMsg Lifecycle



6 Global Compatibility

To this point, we have established a framework for creating a highly performant cross-network messaging service with unparalleled security guarantees. However, our ultimate goal for Omni is to enable all applications to become Turing complete across all rollup environments. To accomplish this, Omni must be designed to support any rollup architecture. It must also be backward compatible with existing smart contract application instances on rollups, simplifying the complexities associated with contract integrations and gas management. Finally, Omni must be expanded to support a global orchestration layer that alleviates the growing complexities of managing application deployments between rollup environments.

6.1 Rollup Diversity

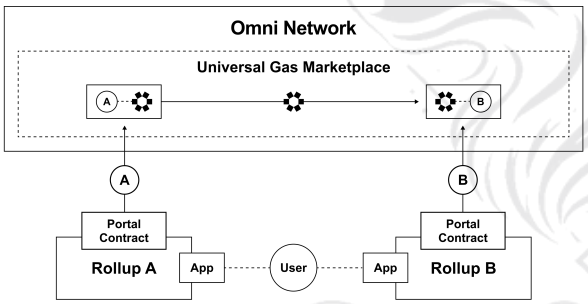
Ethereum is still in the early phases of rollup design development. In the coming years, we anticipate the rollup ecosystem will proliferate in diversity. Projects will develop more customized rollup solutions, each tailored for specific functionalities and performance needs, incorporating unique virtual machines, programming languages, and data availability architectures. Understanding this progression, Omni is intentionally designed with minimal integration requirements to ensure compatibility with any rollup architecture, reflecting the distinct layer separations within the Internet Protocol stack. Thus, Omni promotes innovation at the rollup level while functioning as a global hub that connects the entire rollup ecosystem.

Archived copy · cryp2nova.com

6.2 Universal Gas Marketplace

To support a diverse range of rollup architectures, Omni must be capable of handling gas payments in diverse assets, ensuring that users can interact with any application regardless of where it is deployed. To achieve this, Omni introduces a universal gas marketplace that simplifies the process of gas payments across rollups. A "pay at source" fee model is used to support payments in the native asset of the source network. Internally, these payments are converted into $OMNI, serving as the currency for compensating relayers that facilitate transaction processing on the target rollup on behalf of users. Alternatively, the protocol can accept $OMNI as a gas payment medium across all rollups. This design establishes $OMNI as a gas abstraction primitive, allowing users to obtain $OMNI on any rollup and use it to pay for gas fees anywhere they transact. Using these mechanisms, Omni's universal gas marketplace not only simplifies transactions across rollups but also drives demand for $OMNI, which correlates directly with the volume of cross-network communications facilitated by the protocol.

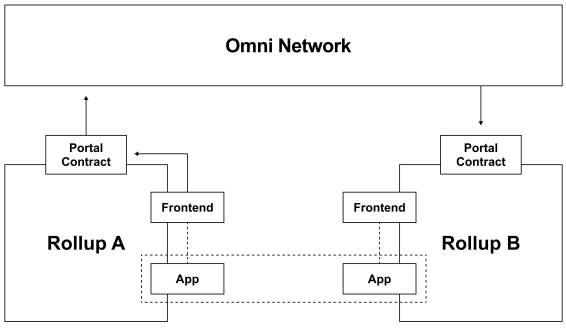
Figure 4: Universal Gas Marketplace



6.3 Backward Compatibility

Building on the foundation of Omni's universal gas marketplace, the protocol is designed to offer backward compatibility with existing rollup applications. Specifically, applications can integrate Omni without modifying their existing contracts. Instead, applications can employ modified frontend instructions to assemble an XMsg that is directed to the Omni Portal contract on the originating network. Subsequently, the Omni protocol takes over, processing XMsg requests and executing their instructions on the target network on behalf of the originating application. As a result, Omni effectively functions as a wrapper around existing applications, allowing them to aggregate users and liquidity across all deployments.

Figure 5: Omni's Backward Compatibility



For developers seeking a higher degree of customization and control, Omni can be integrated directly into applications at the smart contract level using bespoke cross-network function calls. This empowers developers to transmit any type of generic message between rollups, thereby enhancing existing rollup-based applications or enabling entirely new applications with native interoperability.

7 Powering Natively Global Apps with the Omni EVM

While Omni is designed with local rollup applications in mind, the growing diversity within the rollup ecosystem is increasing the complexity associated with managing these application deployments across rollups. Much like how an operating system's kernel abstracts away the intricacies of a CPU's subresources, rollup application developers require a tool responsible for orchestrating application state and configuration across rollups in an efficient manner. This removes the need for developers to think about distributed state management and empowers them to program cross-rollup applications as if they existed within a single state machine.

To satisfy this requirement, Omni must transition from simply facilitating rollup interoperability to providing an abstraction layer that allows developers to program across all rollups from a single environment. From a design perspective, this requires us to expand Omni's current verification layer to offer its own execution environment, the Omni EVM.

7.1 Network Architecture

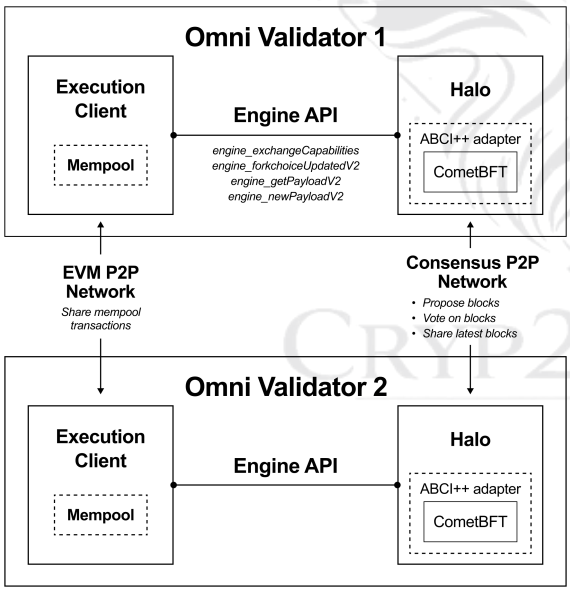
To maintain compatibility with Ethereum's established ecosystem and developer tooling, it is essen-

Archived copy · cryp2nova.com

tial for Omni to adopt the EVM for its execution environment. Additionally, given Omni's reliance on CometBFT consensus for its cross-rollup messaging service, we require a network architecture that combines the EVM with CometBFT consensus without compromising on the protocol's performance or security. However, previous frameworks for integrating the EVM with CometBFT make performance tradeoffs in several areas, with key challenges like mempool congestion and state translations between the EVM and CometBFT impacting consensus efficiency and limiting block times to around multiple seconds, even after optimizations.

We have developed a novel architecture that uses Ethereum's Engine API and ABCI++ to achieve our goal of combining the EVM with CometBFT consensus in a truly scalable manner. Drawing inspiration from Ethereum's PoS architecture, Omni nodes are configured with a new modular framework based on the Engine API. Omni's framework creates a clear separation between its execution and consensus layers, thereby isolating the components that have bottlenecked performance in previous designs.

Figure 6: Omni Node Architecture



Existing approaches use the CometBFT mempool for handling transaction requests. As activity on the network increases, this overloads the CometBFT mempool and compromises the network's consensus speed. Omni uses the Engine API to solve this problem, by moving the transaction mempool to the execution layer, thereby keeping the CometBFT consensus process extremely lightweight. The other major issue with previous design frameworks was the process of translating EVM state to a format that was compatible with CometBFT. We solved this problem by adding an ABCI++ wrapper around the CometBFT engine to handle state translation. Thus Omni's Halo consensus client converts Omni EVM blocks into single CometBFT transactions inserted into consensus blocks. Since Omni EVM blocks are represented as a single consensus layer transaction, the only limiting factor for Omni's throughput is performance of the EVM client itself.

The flexibility provided by the Engine API means execution clients can be substituted or upgraded without breaking the system. As a result, Omni supports any existing Ethererum execution client such as Geth, Besu, Erigon, and others, without specialized modifications. This approach eliminates the risk of introducing new bugs that are common with modified execution clients. Furthermore, Omni nodes can seamlessly adopt upgrades from any EVM client, ensuring ongoing compatibility with the Omni consensus layer. Omni natively supports recent upgrades like dynamic transaction fees and partial fee burning from EIP-1559, as well as future upgrades such as Ethereum's introduction of proposer-builder separation and transient storage. Omni ensures the highest level of EVM equivalence by exactly mirroring the code run by validators on Ethereum L1.

From our research, this novel framework for combining the EVM with CometBFT is capable of subsecond transaction finality at scale. To encourage wider innovation and enable other teams to leverage the best features of both Ethereum and Cosmos, we have open sourced this codebase as a public good for the industry [10].

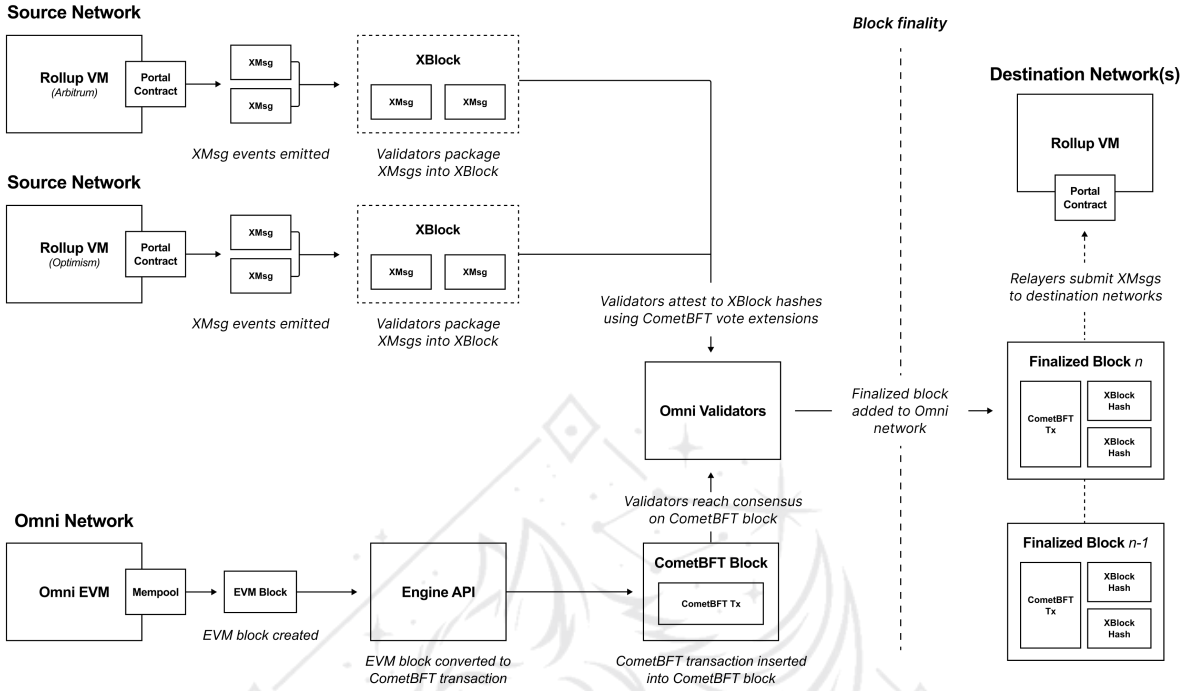
7.2 Integrated Consensus

The addition of the Omni EVM requires Omni validators to simultaneously manage consensus procedures for XBlocks as well as Omni EVM Blocks. To facilitate this, we have created a novel consensus process referred to as Integrated Consensus. This approach represents the culmination of Omni's design objectives, enabling the network to achieve sub-second finality for both XBlock and Omni EVM Block verification in a single process, underpinned by the cryptoeconomic security of Ethereum L1.

Omni implements Integrated Consensus by intentionally decoupling the two consensus sub-processes prior to block finalization. For Omni EVM blocks, consensus is achieved through standard CometBFT procedures. During this process, Omni validators use

Archived copy · cryp2nova.com

Figure 7: Integrated Consensus Process



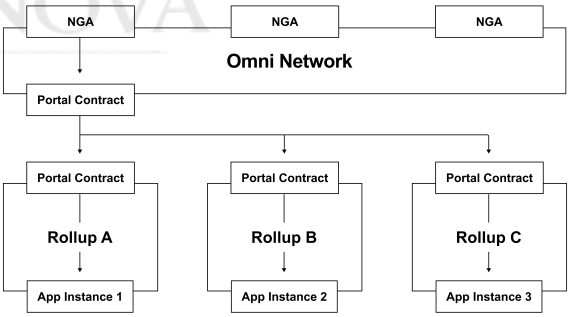
ABCI++ vote extensions to append XBlock attestations to the proposed CometBFT block. By separating these processes, Omni reduces resource overlap for its validators and ensures that Integrated Consensus remains lightweight.

7.3 Natively Global Applications

The Omni EVM reinstates Ethereum's original vision of a unified operating system for decentralized applications by providing a global orchestration layer powered by the full scalability of Ethereum's rollup ecosystem. This equips developers with a new form of infrastructure that simplifies application management across diverse rollup environments and empowers them to build Natively Global Applications (NGAs). This new category of applications functions by dynamically propagating contracts and interfaces to any rollup, allowing them to access all of Ethereum's liquidity and users by default.

This approach to building cross-rollup applications not only streamlines the development process but also minimizes the potential for smart contract vulnerabilities that often arise from the intricacies of working with distributed state. For users, NGAs provide the convenience of interacting with any rollup through a single access point, without the need to navigate between different networks. As the landscape of application management grows increasingly complex, NGAs are positioned to become the new standard application design for Ethereum's modular ecosystem.

Figure 8: Natively Global Applications



Archived copy · cryp2nova.com

8 Reinforced Security

Through the process of making Omni globally compatible with the entire Ethereum ecosystem, we have established two sources of demand for $OMNI. First, $OMNI serves as the universal gas resource for facilitating messages between rollups. Second, $OMNI functions as the gas resource powering NGAs on the Omni EVM. These functionalities present an opportunity to reinforce Omni's cryptoeconomic security model using staked $OMNI in addition to restaked $ETH. Effectively, the total cryptoeconomic security of Omni is determined by the combined staked value of these two assets.

Using this dual staking model, the total cryptoeconomic security C of the system is given by the formula:

$$C = \frac{2}{3} \sum_{a=0}^{m} \sum_{v=0}^{n} P_a(S_{a,v})$$

- $S_{a,v}$ = the amount staked by validator v for asset a v
- P_a = the function mapping the amount of asset a staked to validator power
- n = the total number of validators
- m = the total number of unique staked asset types

The protocol will implement separate functions for mapping existing stake to voting power and for mapping existing stake to staking rewards. The protocol dynamically incentivizes validators to contribute more security from either restaked $ETH or $OMNI depending on market conditions.

By implementing this dual staking model, Omni's security now scales across two dimensions. Restaked $ETH anchors Omni's security to Ethereum L1, enabling it to grow in line with Ethereum's own security budget. The addition of staked $OMNI builds upon this base, expanding Omni's security alongside its own network activity. Collectively, these two complementary mechanisms provide robust and dynamic security guarantees for Omni, setting a new standard for secure interoperability for the Ethereum ecosystem.

9 Summary

The adoption of the rollup-centric roadmap has committed Ethereum to scaling across isolated execution environments. While this approach is actively solving the network's scalability challenges, it has fragmented capital, users, and developers across a growing number of rollup domains. To solve these problems, we created Omni, an Ethereum-native interoperability protocol that establishes low latency communications across Ethereum's rollup ecosystem.

In our quest to build the optimal interoperability solution for Ethereum, we found that existing protocol frameworks failed to meet our criteria for security, performance, and global compatibility. This prompted us to create a new design framework for Omni, prioritizing security as the protocol's foundation. Through restaking, Omni derives cryptoeconomic security from Ethereum L1 and uses it to secure its externally verified network architecture. The integration of a dual staking model further strengthens this security architecture and positions Omni as a new benchmark for secure interoperability.

With a robust security framework in place, we shifted our attention to optimizing Omni's performance. Our goal was to implement a consensus mechanism capable of handling cross-rollup communications with minimal latency. Through the development of a unique protocol architecture, incorporating technologies like CometBFT, ABCI++, and the Engine API, Omni validators achieve this goal by providing sub-second verification for cross-rollup messages.

In terms of global compatibility, Omni was intentionally designed with minimal integration requirements to make it compatible with any rollup architecture and application design. The introduction of a universal gas marketplace simplifies the user experience for cross-network applications, while the addition of the Omni EVM provides developers with a global platform for deploying and managing cross-rollup applications.

Omni represents a comprehensive interoperability solution for Ethereum rollups and is poised to reunify the Ethereum ecosystem. With Omni, Ethereum can once again provide a single, unified operating system for decentralized applications, but this time, at a global scale.

Archived copy · cryp2nova.com

References

[1] Vitalik Buterin. Ethereum white paper: A next generation smart contract & decentralized application platform. 2014. https://github.com/ethereum/wiki/wiki/White-Paper.

[2] Arjun Bhuptani. The interoperability trilemma. 2021. https://medium.com/connext/the-interoperability-trilemma-657c2cf69f17.

[3] Axelar Team. Axelar network: Connecting applications with blockchain ecosystems. 2021. https://axelar.network/axelar$_w hitepaper.pdf$.

[4] EigenLayer Team. Eigenlayer: The restaking collective. 2024. https://docs.eigenlayer.xyz/assets/files/EigenLayer$_W hitePaper$ − 88c47923ca0319870c611$decd$6e562$ad.pdf$.

[5] Bitfly. Beaconcha.in, 2024. https://beaconcha.in/.

[6] Cometbft. 2024. https://docs.cometbft.com/v0.38/.

[7] Abci++. 2024. https://docs.cometbft.com/v0.37/spec/abci/.

[8] Espresso Systems. Analyzing bft proposer-promised preconfirmations. 2023. https://hackmd.io/@EspressoSystems/bft-and-proposer-promised-preconfirmations.

[9] Justin Drake. Based preconfirmations. 2023. https://ethresear.ch/t/based-preconfirmations/17353.

[10] Omni Team. Omni network github, 2024. https://github.com/omni-network/omni.

CRYP2NOVA

Archived copy · cryp2nova.com