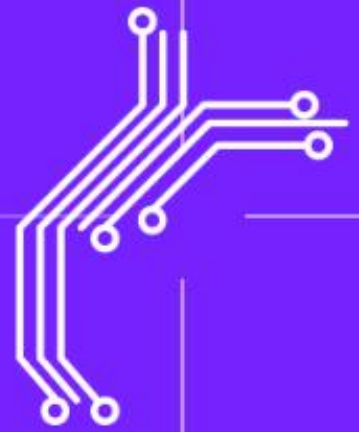
BitcoinZK

Extend Bitcoin with ZK.
Zero knowledge, zero trust, zero wait.

CRYP2NOVA

Archived copy · cryp2nova.com



What is BitcoinZK

BitcoinZK is a revolutionary second layer for Bitcoin. BitcoinZK aims to provide Bitcoin users with the most powerful scaling solution ever: high throughput, native BTC, Turing complete, and modularly built.

BitcoinZK guarantees 100% ZK functionality. Among them, 100% of user actions will be proven by ZK, and 100% of ZK proofs will remain publicly verifiable.

Archived copy · cryp2nova.com

Design philosophy

BitcoinZK

The design of BitcoinZK is mainly driven by the goal of providing better services and expanding Bitcoin (the first layer). It is worth noting that there is currently no clear definition or specification to tell us what Bitcoin's second layer should look like. Therefore, before discussing our solution, it is necessary to first define the exact problem we want to solve.

We believe that the scalability requirements for Bitcoin can be summarized into three aspects: throughput, contract capability, and fewer security compromises.



Handling capacity

Increasing throughput means higher TPS (transactions per second) and lower transaction fees. This will create possibilities for a richer ecosystem of dapps, alternative assets, and usage scenarios.



Smart contract capabilities

We must accept the fact that even after the Taproot upgrade, the scripting functionality of Bitcoin still has significant limitations. Although we can already use the Taproot script to implement complex transaction logic, it is far from being a more universal capability. This limitation confines the application ecosystem of Bitcoin to a very narrow range.
We believe that, considering the simplicity concept of Bitcoin, providing a stronger contract capability (especially for Turing-complete contracts) on the second layer for Bitcoin's first layer is very meaningful, because such a layer can introduce breakthroughs in terms of efficiency and capability boundaries.



Reduce security compromises

Given the limitations of Bitcoin and our goal of achieving breakthroughs in throughput and contract capabilities, we have noticed that a 2nd-layer solution without any compromise in security is impractical. However, a qualified Layer2 solution should clearly define the trust assumptions introduced, explain why they are necessary, and consider ways to minimize them in the future. We will also reserve space in the subsequent chapters to elaborate on our views and solutions regarding this matter.

Archived copy · cryp2nova.com

BitcoinZK

100% zero-knowledge

The fact is that, up to now, Bitcoin cannot natively verify transactions executed on Layer2 in an engineering feasible manner. ZK has become our best option.

ZK is a true game-changer in the Layer2 scenario, as this technology ensures that any action taking place on Layer2 can be verified at a relatively low cost. The mathematics guarantees this.

Therefore, we strive for the "100% * 100%" ZK feature: 100% of user behavior is ZK-provable, and 100% of ZK proofs are publicly verifiable.

Although we have not fully achieved this requirement yet, the essence and characteristics of ZK technology determine that they can be realized. More importantly, ZK technology provides greater flexibility and scalability for our solution, such as interoperability with more blockchains/Layer 2.

Archived copy · cryp2nova.com

Native support for BTC

BitcoinZK

BitcoinZK provides native support for Bitcoin and its users, aiming to reduce entry barriers and enhance usability.

These supports include:

BTC Gas Fee

Users do not need to purchase any other tokens to pay for gasoline fees on the second layer.



Abstract of BTC Wallet

Users do not need to download or use any wallet other than their own Bitcoin wallet.



BTC zkBridge

This is a minimum-trust BTC bridge for depositing and withdrawing BTC.



Furthermore, zkBridge will introduce more alternative assets based on BTC, such as BRC20 and BRC420, etc.

Archived copy · cryp2nova.com

Native support for BTC

Complete EVM compatibility

BitcoinZK is the revolutionary second layer of Bitcoin. BitcoinZK aims to provide Bitcoin users with the most powerful expansion solution ever: high throughput, native BTC, Turing completeness, and modular construction.

BitcoinZK guarantees 100% ZK functionality, where 100% of user behavior will be proven by ZK, and 100% of ZK proofs will be publicly verifiable.

We recognize

Introducing EVM into the Bitcoin ecosystem might cause some controversy, as some people believe that using only the native scripting functionality of Bitcoin is more "orthodox".

We do not make any value judgments; we merely want to bring this fully Turing-complete contract system to Bitcoin.



Archived copy · cryp2nova.com

Modularization and sovereign design

BitcoinZK

As mentioned at the beginning of the previous chapter, we still cannot clearly define what Bitcoin Layer 2 should look like. For us, what is important is how to meet the needs of Bitcoin users and introduce the minimum trust assumption to ensure the security of Layer 2. This design approach has led us to seriously consider a modular, sovereign, and roll-up-like framework.

Sovereign Rollup is a second-layer network that deploys consensus and data availability onto another blockchain (instead of the original first-layer chain). Sovereign Rollup has the ability to determine its own consensus mechanism and how to ensure its resolution. We will discuss later why Layer2 solutions like Sovereign Rollup are a reasonable solution for Bitcoin.

CRYP2NOVA

The advantages of this design will be evident both in the short term and the long term. In the short term, it enables us to leverage the most powerful consensus and data availability to ensure the security of our second layer. In the long term, it provides us with the potential for continuous improvement to maximize the use of the magic verification and privacy features of ZK.

Archived copy · cryp2nova.com

Modularization and sovereign design

BitcoinZK

The second layer of Bitcoin

In order to better illustrate the architecture and design principles of BticoinZK, we need to discuss the concept of "Bitcoin Layer 2" and clearly define the problems we aim to solve.

Layer2 and Rollup

Layer2 and Rollup are concepts within the Ethereum framework, explored by the community to better address the scalability issues of Ethereum. As Ethereum has largely established a "roll-up-centric" expansion roadmap at present, these concepts have been widely accepted by the market.

In the context of Bitcoin, we have been discussing the concept of "scaling" for a long time. For instance, the Lightning Network was an early exploration for expanding Bitcoin payments. From today's perspective, it can be defined as a second-layer solution for Bitcoin.

Although the concept of the second layer has not been clearly described, we have observed that the market has begun to extensively compare Bitcoin's scaling issues with the L2/Rollup solutions of Ethereum. Therefore, for ease of understanding, we also position BitcoinZK as a second-layer solution for Bitcoin.

Archived copy · cryp2nova.com

Modularization and sovereign design

BitcoinZK

It is important to discuss the concept of "Rollup".

By definition, Rollup is not an equivalent expression to Layer2; Rollup is a specific implementation that makes Layer2 work. It is worth noting that we can establish Layer2 without using Rollup; even if we do use Rollup, we can consider several completely different technical solutions to implement Rollup.
Even today, there is still much debate about how to define Rollup and Layer2. For us, what we are more concerned about is expanding Bitcoin, bringing real value to Bitcoin users, and addressing the security issues in Layer2 solutions.
Therefore, we will not attempt to answer questions such as "What is the best Rollup solution" or "Which scaling solution should be considered". Instead, we will try to explain how to use the available technologies to build a complete solution and the future development path for extending Bitcoin using the Layer2 network.

Archived copy · cryp2nova.com

Bottleneck

BitcoinZK

In this chapter, we will discuss why we are here and why we want to use bitcoinZK as a second-layer solution for Bitcoin.

In our philosophy, "scaling Bitcoin" is precisely the goal that helps Bitcoin achieve what users expect (but due to certain limitations, it cannot be accomplished on its own).

From this definition, we can easily list the two main user expectations that Bitcoin has not yet fulfilled:

* Higher throughput

This means higher TPS and lower transaction fees.

* Stronger contract negotiation skills

It is preferably used to build the complete Turing capability of the application ecosystem.

Archived copy · cryp2nova.com

Bottleneck

BitcoinZK

BitcoinZK addresses these two issues here.
We have brought higher transaction throughput and stronger smart contract capabilities to Bitcoin. This is the mission of bitcoinZK.
However, we recognize that by significantly enhancing the throughput and contract capabilities of Bitcoin, we inevitably impose additional trust assumptions on this second layer (which is a negative aspect).

Inevitably, there are two inherent limitations of Bitcoin:

* The current script scheme of Bitcoin is unable to directly verify transactions submitted by the aggregated Layer 2, regardless of the verification style (proof of validity or proof of fraud).

The design of Bitcoin's script and UTXO imposes very strong limitations on its capabilities, making it difficult to support more complex and diverse user scenarios, such as DeFi.

Archived copy · cryp2nova.com

ZK: What and Why

ZK is a cryptographic method that enables one party (the prover) to prove to another party (the verifier) that a statement is true without revealing any other information except for the truthfulness of the statement. Building ZK typically requires satisfying three important attributes:

* Integrity

The prover does possess an answer to a certain assertion and can convince the verifier.

* Soundness

If the witness does not provide an answer that matches the assertion, it will not be able to convince the verifier.

* Zero-knowledge

The verifier only knows the result of the assertion judgment and has no knowledge of any other information.

CRYP2NOVA

In the field of cryptography, ZK has become a relatively mature and widely accepted model, especially in the second-layer scenarios where the second layer needs to prove to the first layer that its execution is correct. We do not overly delve into the technical details of ZK (we do not seek to bring any innovation at the level of ZK algorithms or mathematics), but rather focus on the advantages of ZK and the reasons for using ZK to build this Bitcoin second-layer solution.

Archived copy · cryp2nova.com

Zero-knowledge

BitcoinZK



Theoretically, L2 can submit all transaction data to L1 and let L1 execute all transactions for verification. However, this method consumes a large amount of resources.



The market has widely adopted the verification scheme called "Fraud Proof" (in the Optimism style) to save the resources consumed in on-chain verification.



Here, the advantage of ZK comes into play, because the ZK proof is concise, which means that the verifier only needs to perform much fewer computations (much less than generating the ZK proof) to complete the verification.



This is highly suitable for the L2 solution, as the existence of L2 is to address the performance limitations and resource shortages (primarily execution resources) of L1.



Therefore, having L2 invest more resources to generate the proof, while releasing the L1 validator to verify the validity proof with fewer resources, becomes a win-win situation.

Archived copy · cryp2nova.com

Zero-knowledge

The difference between Bitcoin and Ethereum lies in that Bitcoin shows greater limitations in its ability to execute smart contracts, which results in it being unable to directly verify transactions submitted from the L2.

We have noticed some recent attempts, such as bitVM, which is considering enabling Bitcoin to utilize existing scripts to verify off-chain transactions (EVM).

Therefore, for the sake of rigor, we tend to conclude that "from an engineering perspective, Bitcoin's current scripts cannot feasibly verify the general computing of L1 in a native manner", rather than making an absolute judgment such as "Bitcoin will never have this capability in the future."

To put it briefly, ZK has demonstrated some significant advantages in meeting the basic requirements of Bitcoin L2. Firstly, the limitations of Bitcoin's scripting functionality make non-ZK L2 solutions very unfriendly to operators and validators.

Secondly, the core advantages of ZK, such as simplicity, resource-friendly verification, and privacy protection, make ZK proofs easy for any third party to verify, providing us with a great deal of flexibility and customization space. In the long run, these key features of ZK will better serve L2s and have more potential breakthroughs.

Archived copy · cryp2nova.com

100% ZK Function

BitcoinZK

- ✓ As the name suggests, bitcoinZK is firmly committed to ZK attributes. Specifically, our goal is to achieve 100% ZK provability and 100% ZK verifiability.
- ✓ 100% ZK provability means that all operations that occur on L2, including all operations executed on L2 as well as asset bridging operations between L1 and L2, will be able to generate ZK proofs for their validity.
- ✓ Since Bitcoin miners cannot directly verify the validity of L2 transactions, any smart contract-style Bitcoin L2 cannot inherit the powerful Bitcoin PoW consensus unless we only resort to the existing scripts of Bitcoin to build L2 functions. Based on this fact, we believe that building ZK proofs for all user operations on the L2, combined with the strong and trustworthy verification mechanism of the finality of their states, is the best way to ensure the security of Bitcoin L2.

100% ZK verifiability means that all ZK proofs generated on the L2 can be verified by any third party. The challenge for BitcoinZK lies in how we can manage the verification process in a less trusting manner.

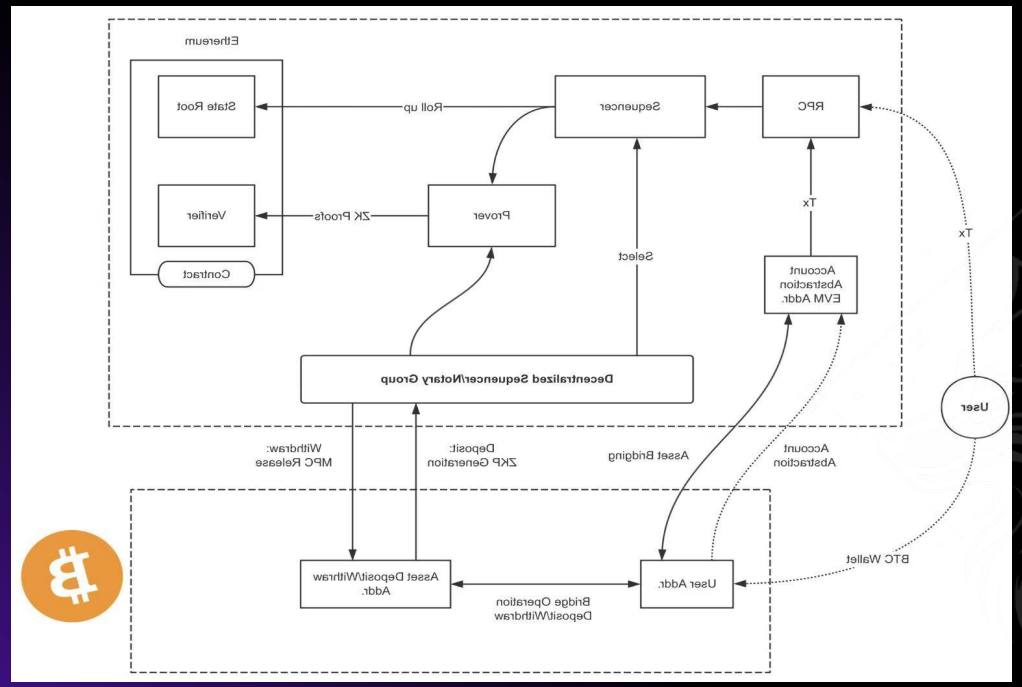
*BitcoinZK avoids introducing the client-side verification (CSV) scheme unless it is absolutely necessary. The drawback of CSV is that it introduces new trust assumptions and a certain degree of authority, which undermines the trust and decentralization level of the L2 network.

* BitcoinZK has introduced a trusted data availability (DA) layer for all L2 transactions and proofs data, namely for Bitcoin and Ethereum. BitcoinZK submits the original ZK proof data to Ethereum for DA and validity proof verification, and submits the highly compressed data to Bitcoin.

Archived copy · cryp2nova.com

Conceptual framework

BitcoinZK



- ✓ This is an important part for understanding the overall design of Bitcoin ZK. Since Sovereign Rollup is a highly abstract concept, we will express our insights into the L2/Rollup architecture and actual design.
- ✓ If defined accurately, Bitcoin ZK represents the ZK characteristics, sovereign style, and rolled-up nature of Layer2 of Bitcoin.
- ✓ In short, the purpose of Bitcoin L2 is to expand Bitcoin (L1) in terms of performance (higher throughput, lower fees) or capacity (L2 achieves what L1 cannot do, such as Turing-complete Bitcoin smart contracts). Any network that meets this purpose can be defined as Bitcoin L2.

However, the concept of Rollup is slightly different. Rolling up is more like a specific implementation method of the L2 network, where L2 nodes execute Txs and submit the data to L1 for final state determination. However, please note that L2 does not necessarily have to be implemented together with Rollup, because apart from Rollup, there are other ways to expand L1. The discussion about rolling up is quite intense because the Ethereum ecosystem has chosen the "roll-centered" development roadmap (compared to previous solutions such as plasma and state channels) for its scaling issues, and this original one has somehow migrated to the Bitcoin scaling solution today.

CRYP2NOVA

Archived copy · cryp2nova.com



Conceptual framework

Furthermore, we prefer to use the terms "sovereign style and similar roll-up" to better describe Bitcoin ZK as the implementation of Bitcoin L2, as we believe they are the closest definitions we can currently find in the market. In fact, the design of Bitcoin ZK is different from any other existing L2.

BitcoinZK Rollup Anatomy

L2 and Rollup Explanation

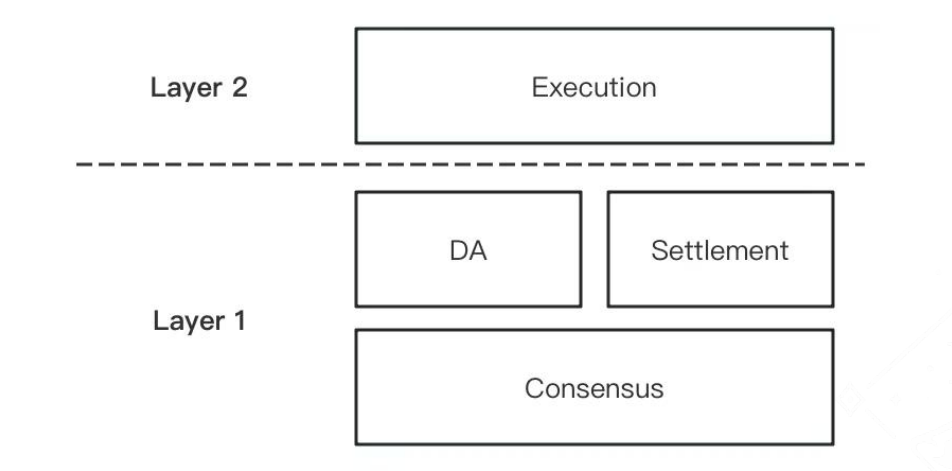
We approach the L2 operations similar to Rollup from two different perspectives.

The first viewpoint is: How does L2 ensure the security and finality of executed transactions?

Archived copy · cryp2nova.com

Conceptual framework

BitcoinZK



L2 (as the Rollup of L1)

It is a partially independent network that retains some of its own components and inherits/borrows the remaining components from L1. Generally speaking, we consider four typical components:

Consensus

The consensus forms the basis and determines the validity of transactions within the network among a group of nodes.

Close an account

The settlement indicates the finality of the transition of the transaction status (so that the transaction can be recorded and callable on the blockchain).

Execute

The node executes the transaction and calculates the transition from the previous state to the new state.

Data availability

DA stands for the release of data (such as transaction data, ZK proofs, etc.). Users or other third parties will be able to verify based on the disclosed data whether the transactions and state transitions executed on the L2 are correct.

CRYP2NOVA

Archived copy · cryp2nova.com

Conceptual framework

BitcoinZK

A very typical summary is an aggregation of smart contracts on the Ethereum platform.



A very typical summary is an aggregation of smart contracts on the Ethereum platform. On L2, the sequencer processes all incoming transactions and "rolls up" the transaction data and state transition results to L1. On L1, all transactions can be re-executed to ensure the validity of the state transitions on L2. In ZK Rollup, we use ZK Proofs to prove the validity of the transactions executed on L2, achieving higher data compression rates and better privacy protection functions.



This type of smart contract aggregation essentially delegates the execution to the L2, thereby alleviating the resource constraints of the Ethereum L1 execution. To ensure the trustworthiness of the execution on the L2, the Ethereum L1 still assumes the responsibility for data availability and settlement (both supported by Ethereum's PoS consensus).

Archived copy · cryp2nova.com

Conceptual framework

BitcoinZK

The bet on Bitcoin

Bitcoin is very different. If we want to achieve Turing-complete smart contract functionality (such as EVM), we need to solve the problem that Bitcoin's L1 cannot natively verify transactions (or ZK proofs) from L2 Rollups. This is a major issue. Some solutions attempt to submit transaction data or ZK proof data commitments to the Bitcoin L1, but at best, this is some kind of data proof. Please note that you cannot even directly obtain this data and verify the transactions on Bitcoin L1; instead, you need to obtain it from the CSV network. This "CSV + data proof" method cannot achieve a satisfactory security level because in this case, Bitcoin L1 hardly provides the four key components for aggregation.

The second viewpoint is more specific, namely, how can we ensure that the user operations for L2 and L1-L2 bridging are carried out in a secure and minimized trust manner?

* From an internal perspective, L2 needs to execute all transactions that occur within L2 and calculate the corresponding state transitions.

* From an external perspective, L2 needs to ensure that the bridging assets from L1 to L2 and their withdrawals are sufficiently secure.

We have found that the external perspective of the security asset bridging between L1 and L2 poses a greater challenge for Bitcoin L2, because the risk of losing L1 assets is a huge disaster for any L2 user, and the security asset bridging on Bitcoin L2 is more difficult than that on Ethereum.

Archived copy · cryp2nova.com

Conceptual framework

BitcoinZK

In the Ethereum aggregation, the challenge of L1-L2 bridging is relatively smaller.

Ethereum L2 will deploy dedicated smart contracts on the L1, which handle the deposit of L1 assets and the redemption of L2 assets. This can be either inherently trustless or very close to it. The only potential drawback might lie in the risk of malicious contract upgrades and the L2 sequencer withholding users' requests. Fortunately, Ethereum L2 has several measures to mitigate these risks, such as contract upgrade waiting periods and mandatory exit/escape hatch mechanisms.

In the Bitcoin L2, the situation becomes complicated.

We are unable to deploy smart contracts on the Bitcoin L1 to handle asset bridging activities, resulting in Bitcoin being completely unaware of the status of the L2. Therefore, in order to address the risks of asset bridging, some additional trust assumptions have inevitably been introduced. This is why BitcoinZK has brought its users a scalable and minimized trust zkBridge, allowing them to safely join their L2 journey securely.

Archived copy · cryp2nova.com

Sovereign-style solutions

BitcoinZK

Based on the challenges outlined by Bitcoin L2, we considered the Sovereign Rollup solution. In fact, we have not yet found an accurate way to describe the Bitcoin ZK solution, but we believe that sovereign aggregation (more precisely, sovereign-style aggregation) is a relatively close definition.

As a sovereign aggregation implementation, L2 can separate several or even all four components from L1.

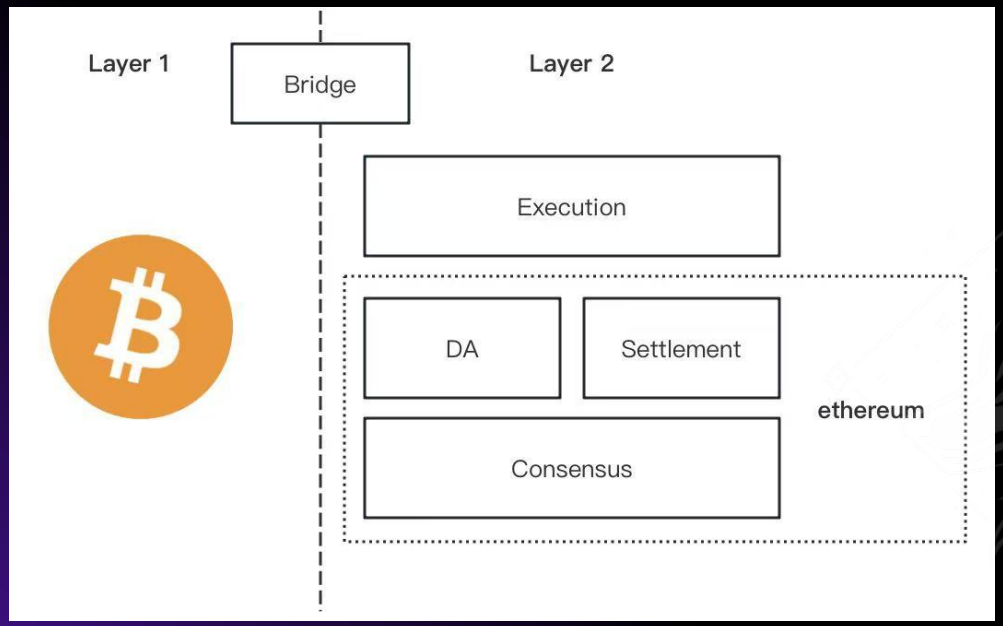
Consensus | **Execute** | **DA** | **Close an account**

The term "sovereignty" implies that L2 can reach an independent consensus and build DA and reconciliation on this basis, rather than relying on the consensus of L1. Therefore, this kind of sovereignty allows L2 to break free from the reliance on the consensus and security of L1, and has greater flexibility in upgrade mechanisms, governance, and customization.

Archived copy · cryp2nova.com

Sovereign-style solutions

BitcoinZK



For ZK Rollup

Sovereign L2 brings additional benefits. ZK proofs can not only be used to verify the results of L2 execution on the chain, but also to verify more states or messages transferred outside the chain or in cross-chain scenarios. This will significantly expand the application potential of our Bitcoin L2.

When we consider Bitcoin from the perspective of L2, the reasons for adopting a sovereign L2 are more concise and sufficient:

* Bitcoin cannot natively support the aggregation of smart contracts.
* L2 cannot directly inherit Bitcoin's powerful PoW consensus.

These are the most important reasons for us to consider a sovereign-style L2, because we can always choose the best alternative for the four key components,

and reserve more space for future upgrades.

Archived copy · cryp2nova.com

Sovereign-style solutions

BitcoinZK

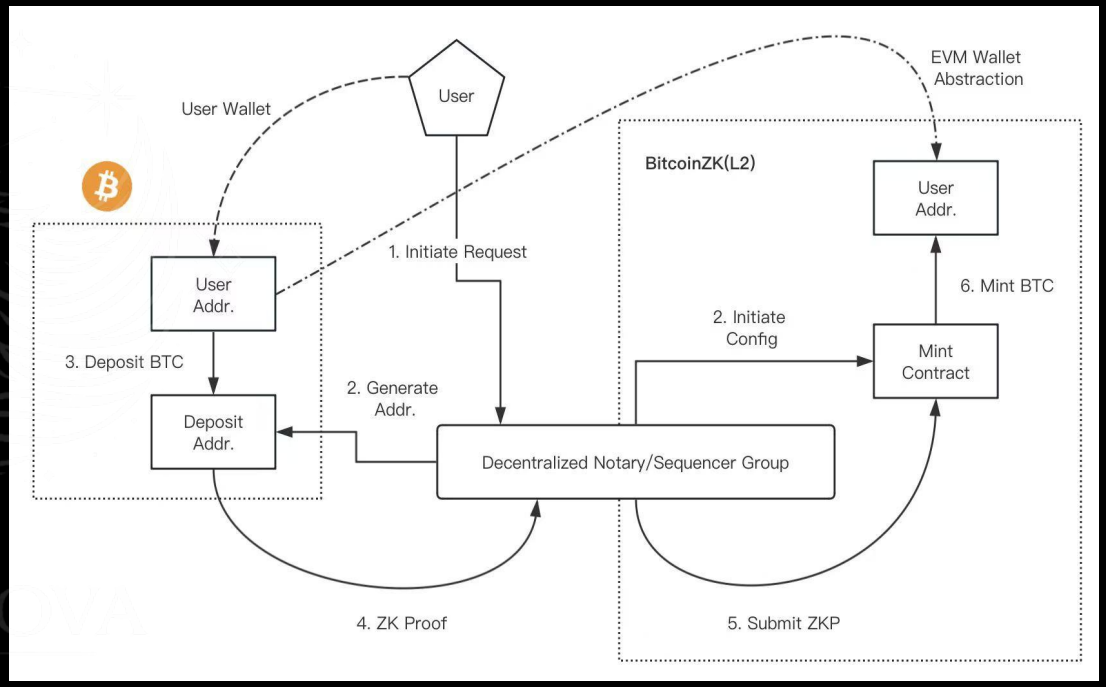
ZK Bridge List

zkBridge is one of the key components of BitcoinZK, as it ensures the transfer of funds between the Bitcoin Layer 1 and the BitcoinZK Layer 2.

The inherent limitations of the Bitcoin script smart contract functionality make it extremely difficult to implement a completely trustless bridging solution between BTC and EVM-compatible chains or Layer 2s. That's why BitcoinZK has built a meticulously designed zkBridge natively, providing a secure way for BTC users or holders to choose to add their assets to our Layer 2 ecosystem.

The key design concept of zkBridge is to ensure that all operations on zkBridge can be proven through zk-SNARKS, and these proofs will be verified by any third party.

By providing ZKP for bridging activities (deposits, minting, burning, and withdrawals), our zkBridge is introducing minimal trust assumptions for asset bridging between Bitcoin (Layer 1) and BitcoinZK (Layer 2). In particular, regardless of the degree of decentralization of the notary group, the BTC deposit-minting activities can be conducted in one assumption.



Bitcoin bridging

We can consider the BTC bridging in two directions separately: from L1 to L2 (deposits and minting), and from L2 to L1 (burning and withdrawals). Regarding the technical nature between Bitcoin scripts and EVM, this makes the bridging solutions slightly different in both directions.

Archived copy · cryp2nova.com

Depository and Coinage Factory

BitcoinZK

01 The user deposits Bitcoin into zkBridge and receives 1:1 amount of Bitcoin tokens on the Bitcoin ZK (L2) platform.

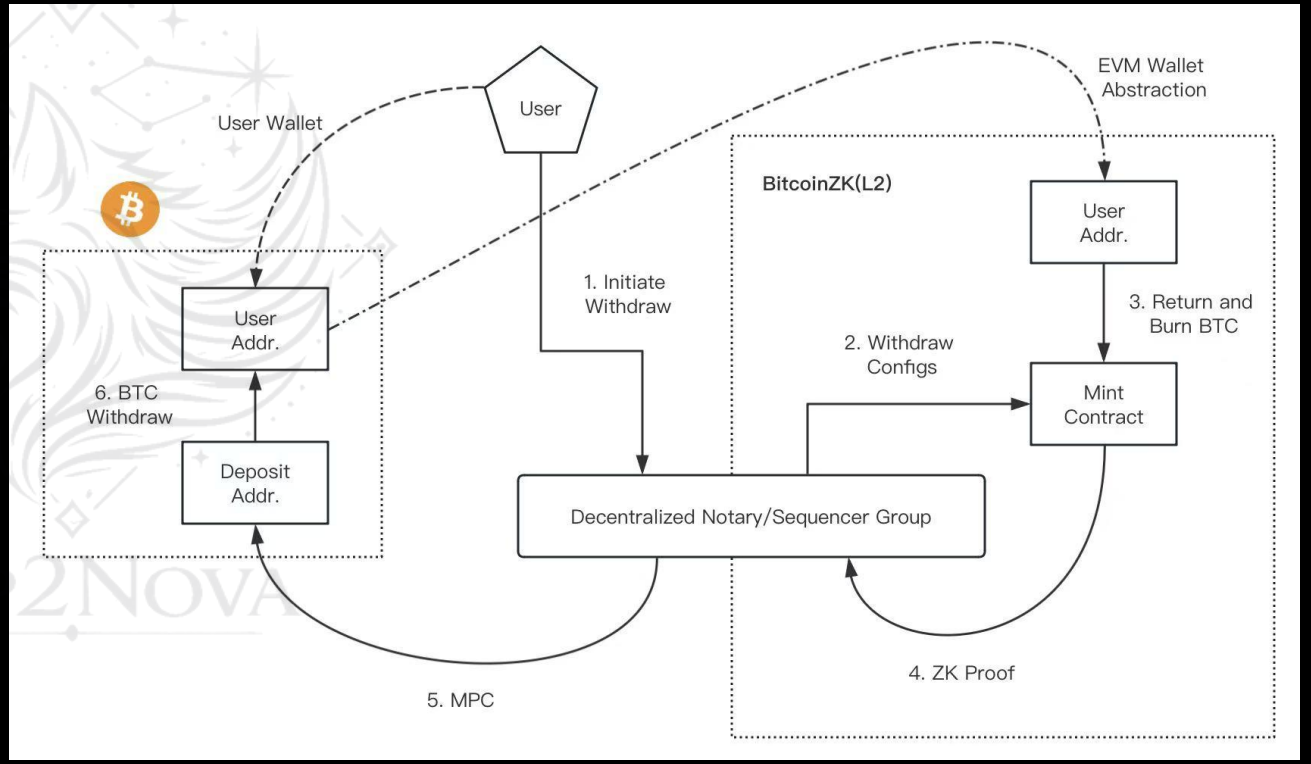
02 The BTC tokens received by the user on Bitcoin ZK are used as the native gas fees.

03 A small portion of the bridged Bitcoin amount will be lost, which will be used as the bridging fee and to cover the bridging costs.

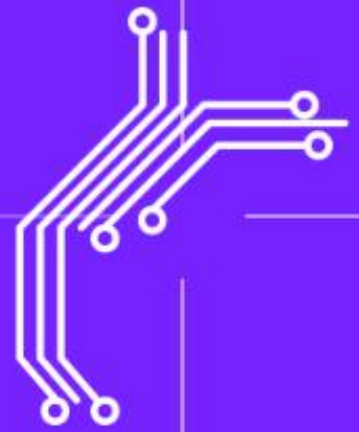
04 When a user generates a bridging request, a BTC deposit address will be created and an EVM address will be indicated to receive the newly minted BTC tokens on the L2.

05 This bridging request uniquely creates an order within the smart contract, which will later be fulfilled by the ZK proof submitted by the notary group as proof of successful deposit.

06 Even if there is only one honest node in the notary group, the deposit and gold-issuing processes will still be protected.



Archived copy · cryp2nova.com



Combustion and Expiration

* Users can withdraw L1 deposits (BTC) from L2 at any time.

* Users receive 1:1 BTC on L1 (the Bitcoin blockchain).

* A small portion of the bridged BTC amount will be lost, which serves as the bridging fee.

* When a user generates a bridging request, an EVM deposit address will be created, and it should represent a BTC address to receive the BTC withdrawal.

* This bridging request is uniquely created in the smart contract as an order, which will later be fulfilled by the ZK proof submitted by the verification group as proof of successful exit.

* The Burn-and-Withdraw process requires 50% or more honest nodes in the verification group. The trustworthiness of the verification group will be strengthened through a combination of several methods, including the Stake-and-Slash plan, shared decentralized sequencer, and ZKP-triggered forced exit.

Archived copy · cryp2nova.com

Threshold BTC integration

BitcoinZK

It should be noted that the complete design of zkBridge is still under development, as suggested by the technical roadmap of BitcoinZK. It is expected to be fully delivered at the end of the launch phase. We are currently leveraging the bridging infrastructure of Threshold Network. It has been proven to be a robust bridge solution that has withstood the test of time, operating between BTC and EVM-compatible chains (such as Ethereum).

The existing solutions that connect Bitcoin and Ethereum require users to send their Bitcoin to an intermediary in exchange for ERC-20 tokens representing the original assets. This centralized model requires you to trust a third party and is vulnerable to censorship, threatening the premise of Bitcoin as a sovereign, secure, and unlicensed digital asset.

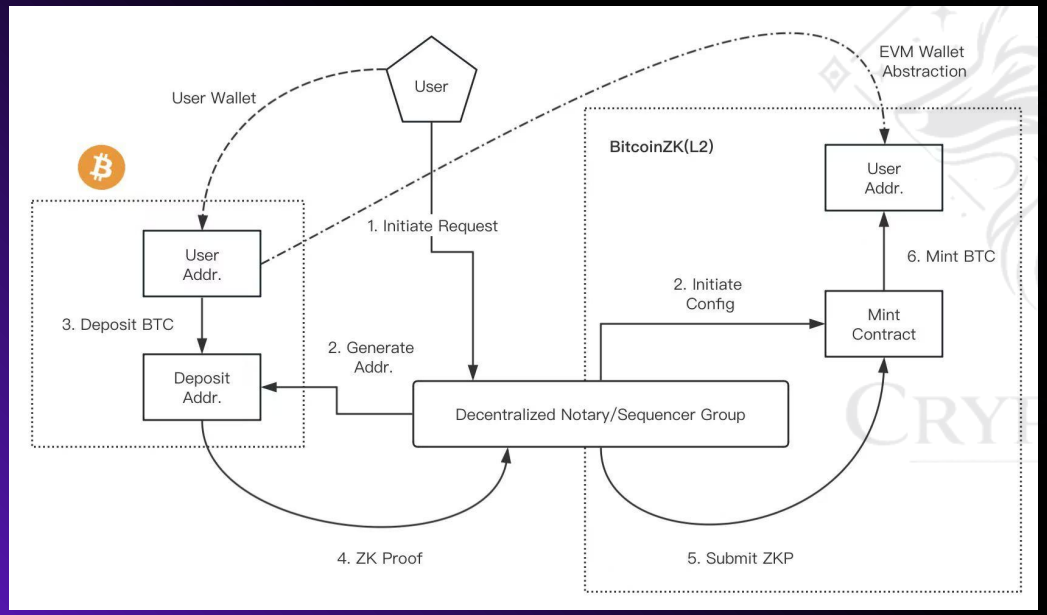
The threshold network tBTC serves as a truly decentralized (and scalable) bridge between Bitcoin and Ethereum. tBTC employs a randomly selected group of operators running nodes on the threshold network instead of relying on a centralized intermediary. It protects the deposited Bitcoin through threshold encryption. This means that tBTC requires a threshold majority protocol before any operation is performed on your Bitcoin by the operators. By rotating the selection of operators weekly, tBTC can prevent any individual or group of operators from colluding to fraudulently seize the deposited funds.

By integrating ZK Proof into the verification process and leveraging the mandatory exit requests initiated by ZK Proof, this bridging solution can even be further enhanced. BitcoinZK will continue to improve the security of BTC bridging based on the current leverage solution and move towards a fully ZK bridging with minimized trust.

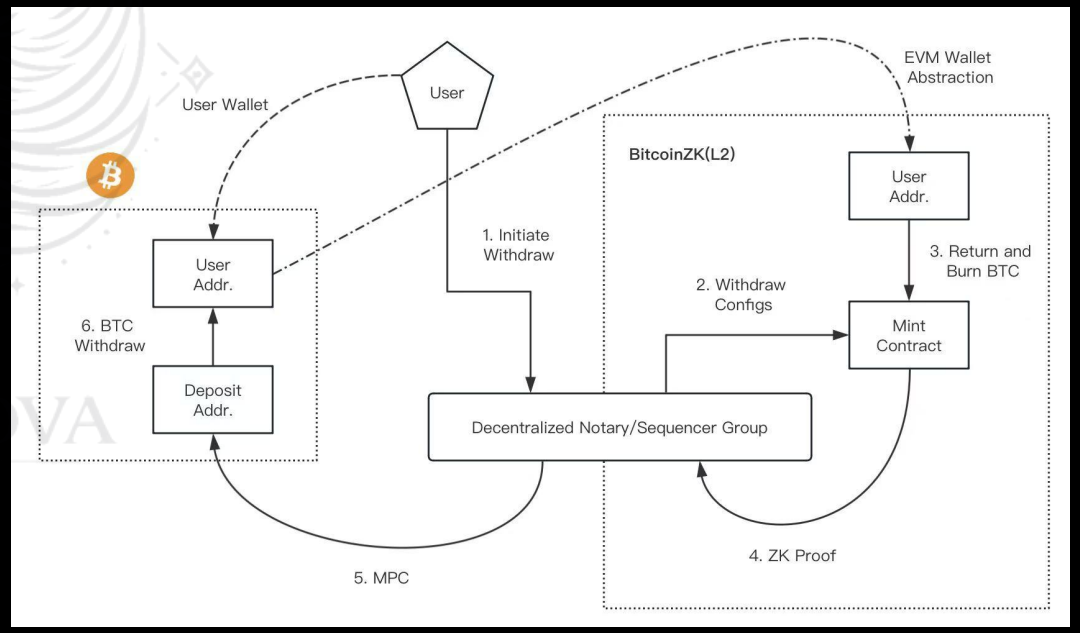
Archived copy · cryp2nova.com

BitcoinZK

Deposit Bitcoin



Extract Bitcoin



Archived copy · cryp2nova.com

Zyra Token economic model

Bitcoin ZK

Token essential information

- Token Name: Zyra Token (ZYRA)
- Total Supply: Fixed total of 1 billion coins
- ZYRA is the native token of the Bitcoinz protocol, used to support the operation and development of its Layer2 solution.

Token allocation and release rules

Token distribution	Proportion	Rules
Miner Incentives	50%	Output from equipment mining over a period of 10 years
Technical Development Team	10%	4-year linear unlocking
Ecological Fund	15%	For equipment subsidies / DApp incentives
Institutional investors	10%	One-year lock-up period + Two-year linear release
Community building	10%	One tenth of the rewards are given to the community each year.
Reserve	5%	For emergency purposes

Archived copy · cryp2nova.com



Bitcoin ZK Chain

* Https://github.com/bitcoinzkio/bitcoinzk-validium-node
* Https://github.com/bitcoinzkio/bitcoinzk-validium-contracts
* Https://github.com/bitcoinzkio/bitcoinzk-prover

Bitcoin ZK Bridge

* Https://github.com/bitcoinzkio/bitcoinzk-bridge-ui
* Https://github.com/bitcoinzkio/bitcoinzk-bridge-service

The network to be deployed

* Network name: BitcoinZK Devnet
* RPC website: https://rpc-devnet.bitcoinzk.io
* Chain ID: 1851
* Currency symbol: BTC
* Block browser website: https://explorer-devnet.bitcoinzk.io

Archived copy · cryp2nova.com

How to through

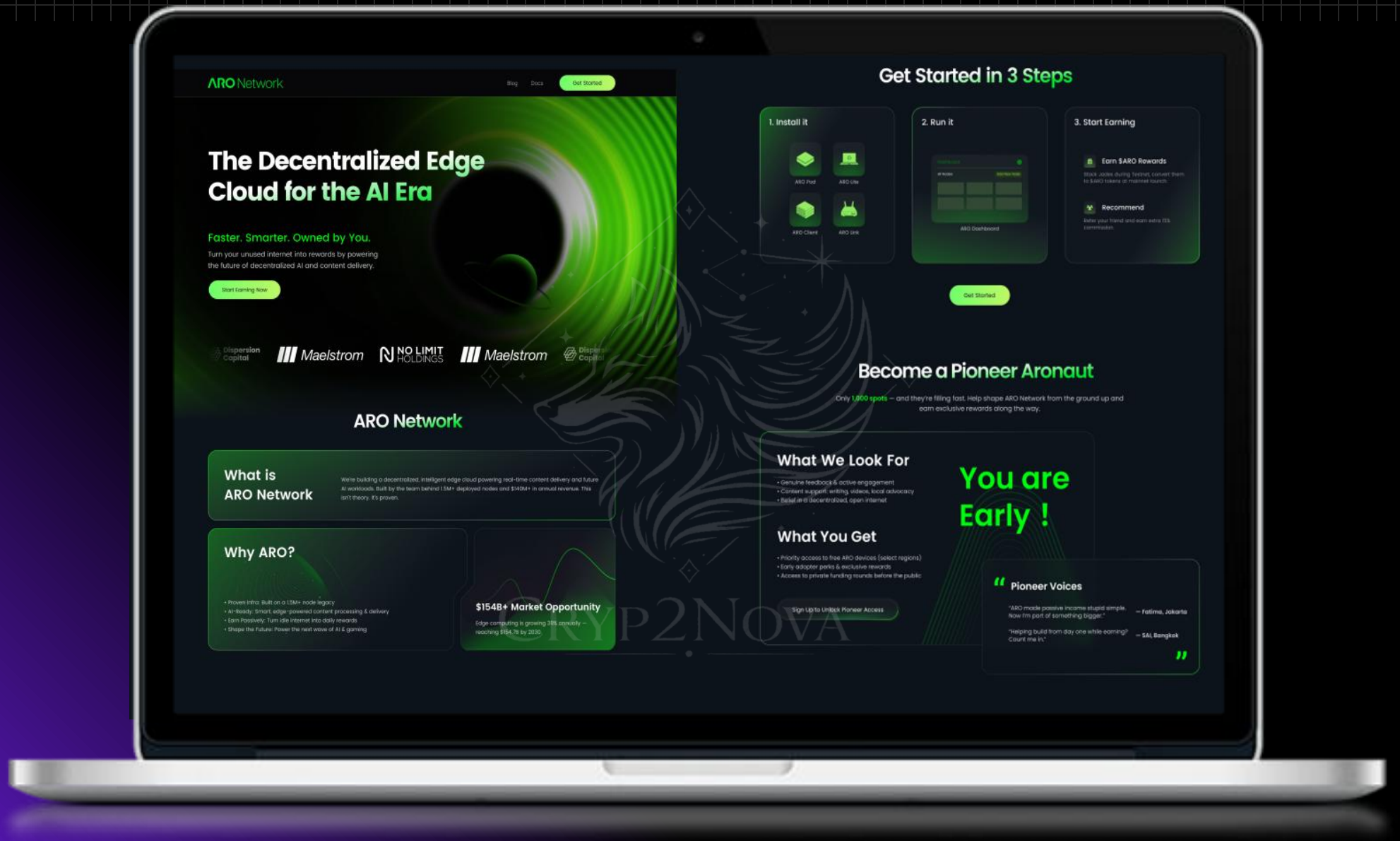
The distributed computing power ensures the computing power of ZK
Long-term and sustainable - build a distributed computing layer for BitcoinZK

Cryp2Nova

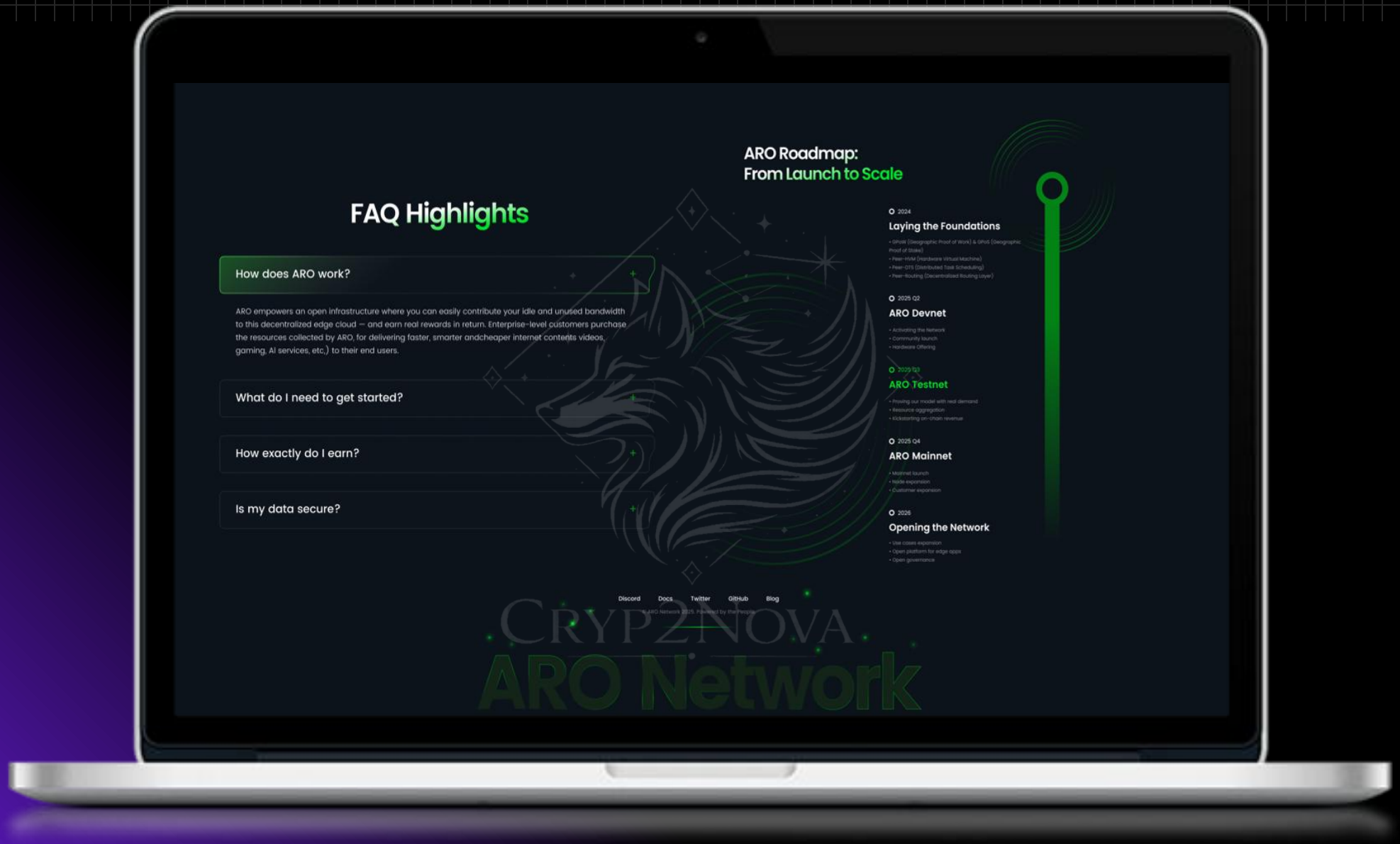
Archived copy · cryp2nova.com

Aro network
Build the distributed physical infrastructure layer
Bitcoin ZK builds the application layer

Archived copy · cryp2nova.com



Archived copy · cryp2nova.com



Archived copy · cryp2nova.com

The world's top depin capital casino has opened.

Maelstrom is a family office investment fund established by Arthur Hayes, the co-founder of the cryptocurrency exchange BitMEX, in 2023. It mainly invests in start-up companies in the blockchain technology field. As of 2024, the fund has invested in 22 enterprises, including projects such as Cytonic, Magma, and Solayer in the cryptocurrency infrastructure sector.

Dispersion Capital is a venture capital firm specializing in investing in decentralized infrastructure. In May 2023, it launched a $40 million fund, focusing on seed rounds and pre-seed rounds of startups. This fund is supported by Web 2.0 and Web3 entities, including WeNade, Circle Ventures, Ripple, Alchemy Ventures, NGC, and individual partners, and has deployed 10% of the fund.

No Limit Holdings (NLH) is a company specializing in global investment in digital assets. Its headquarters is located in the United States. It manages multiple investment funds and continuously pays attention to blockchain infrastructure and emerging fields.

NLH invests in crypto projects through its funds, covering the seed round, pre-seed round and strategic financing stages. Its investment areas include emerging technologies such as DeFi (decentralized finance), Web3 infrastructure and AI data pipelines. For instance, its lead investment in Wynd Labs (a core contributor to the Grass Protocol) and Grass Protocol is one of the most successful DePIN projects at present, allowing users to obtain rewards by sharing unused internet bandwidth.

Archived copy · cryp2nova.com

Summarize

√ ARO Network is building a decentralized, faster and smarter edge cloud for the era of artificial intelligence to redefine human digital experiences.

√ Content drives the Internet. ARO Network provides fast, intelligent, and AI-driven content.

√ ARO Network is not just a vision for the future; it is a scalable platform based on proven technology, now open to everyone.

√ Join the ARO Network. Don't pay for the Internet. Earn rewards through the Internet.

Archived copy · cryp2nova.com

New Edge

Edge Cloud: Closer Cloud

The concept of edge cloud is quite simple: to make cloud servers physically closer to users.
In computer science, physical distance is very important. Running programs closer to the source of the request at the network edge can provide faster responses for the end users. This is the essence of Edge Cloud and also why it is named as such.

You use it every day. Edge Cloud

Edge cloud is a crucial component of modern digital infrastructure, seamlessly supporting services used by billions of people every day. For instance, YouTube does not always directly provide videos from centralized data centers. Instead, it caches high-demand content on edge servers located closer to users, thereby improving speed and reliability. Edge Cloud powers the content-rich internet we have today.

ARO Re-defining the margins

Although the main Web2 platforms rely on edge cloud solutions, ARO Network stands out as a unique decentralized approach. ARO provides content faster and more closely to users. By leveraging the decentralized network, ARO minimizes latency and accelerates content delivery, ensuring seamless access anytime and anywhere. ARO understands content and user preferences. By hosting AI Transformers at the edge, ARO personalizes content based on user requests and behaviors, creating a more intelligent and tailored experience. ARO has transformed the digital experience in the era of artificial intelligence. By combining real-time content delivery with AI-driven functions, ARO makes digital interaction faster, smoother, and smarter.

Archived copy · cryp2nova.com

Architecture

The ARO network uses a three-layer architecture model to build its edge cloud infrastructure:

Resource layer

This is the foundation layer of ARO, consisting of a huge, distributed and unlicensed hardware resource network.
These resources provide the bandwidth, storage and computing capabilities necessary for the edge cloud.

At this level, we focus on addressing two fundamental challenges:

Trust:

How do large-scale distributed nodes verify each other and trust the results of such verification?

Function

In a network with high heterogeneity of nodes, how can we establish a P2P transmission network that can penetrate firewalls and local area networks, while also effectively virtualizing and containerizing these nodes?

Archived copy · cryp2nova.com

Architecture

The ARO network uses a three-layer architecture model to build its edge cloud infrastructure:

Open tier

This is where ARO actively coordinates network resources to optimize the matching of supply and demand.
The foundation of this layer is a trust mechanism for verifying the workload of nodes.
On this basis, we introduce a middleware called Pirrilli.

Pirlich is composed of three core components:

Peer-heterogeneous virtual machines

The abstract P2P network resources provide standardized capability outputs. Through PeerHVM, ARO can deploy functions across distributed nodes, forming a unified interoperable network structure.

PeerDTS

A high-performance P2P transmission protocol that supports the ability to deliver large-scale content across the PeerHVM abstraction layer.

Peer-to-peer routing

A dynamic and proactive response engine intelligently matches resources with the constantly changing user demands.

Archived copy · cryp2nova.com

Architecture

The ARO network uses a three-layer architecture model to build its edge cloud infrastructure:

Application layer

By leveraging the functions provided by the middleware and corresponding chain-on interfaces, this layer offers user-oriented interfaces, service components, and application APIs for third-party CDN, cloud storage, AI inference, runtime transmission, and computing routing services.
As part of our phased approach, this layer is designed to be opened up to facilitate widespread application - achieving the universal acceleration of the ARO vision.

Resources, trust, and services

- This resource-trust-service model provides a clear modular abstraction for ARO on how to organize edge hardware into a powerful edge cloud network, highlighting the key technologies involved.
- This resource layer focuses on virtualization and standardization of large-scale heterogeneous peer nodes to provide distributed computing capabilities. It uses the GPoW (Guaranteed Proof of Work) protocol to offer trusted and verifiable proof of work.
- This trust layer employs the GPO (Guaranteed Interests Proof) protocol to ensure the verification, settlement and governance of these work proofs on the trusted chain.
- This service layer utilizes peer virtual machines, PeerDTS, and peer routing based on these verifiable middleware to deliver services such as CDN, AiDN, and routing to peer nodes.

By integrating these technologies, ARO has created a high-performance and cost-effective artificial intelligence acceleration network based on industry best practices.

CRYP2NOVA

Archived copy · cryp2nova.com

Fringe node

Edge nodes are the basic units of the network. They are usually customers from household devices such as ARO pods, ARO links, laptops, NAS, etc.

The edge nodes operate in segmented areas based on their geographical locations, and provide resources to end users who are geographically close to them.

The edge nodes are interconnected through the PeerDTS protocol in the following manner. This is of vital importance for the distributed edge cloud to meet the requirements of large-scale P2P data transmission.

Detailed explanation of how edge nodes work:

√ Edge nodes provide resources (network, computing, and storage) to the ARO edge cloud. This is particularly beneficial for those who contribute idle devices and network resources.

√ When edge nodes join the network, they are subject to implicit constraints, that is, they are required to provide stable resources and service capabilities for the network. Edge nodes generate work reports to reflect the time basis of their workload ("report period"). Edge nodes cannot profit by simply fabricating work reports because multiple watchdog nodes will later make the final decision through cross-validation from multiple sources (i.e., heartbeats, network traffic tracking, and random challenges).

√ Edge nodes will be connected to a set of randomly assigned keeper nodes that are refreshed for each period. Edge nodes cannot predict the exact set of keeper nodes allocated to them for the next period.

Archived copy · cryp2nova.com

Supporting node

√ The keeper nodes act as guardians of the network, ensuring that the entire system reaches a consensus and remains free from any manipulation, deception, attack, and failure.
√ The keeper nodes operate within segmented areas based on their geographical locations. Each Keeper node should be assigned to the area where its physical location is located to ensure high availability and service quality in that specific area.
√ Keeper nodes typically run in relatively stable and capable network environments, such as server rooms. Keeper nodes need to ensure very high performance and availability of the network.

The main responsibilities of Supporting node

① Maintain the public ledger of the blockchain;
② Ensure the correctness of contract execution;

③ Routine monitoring sessions are maintained on multiple edge nodes within the region, which are used for real-time status tracking and collection of work reports.
④Carry out cross-region random challenges on edge nodes or guard nodes.

Archived copy · cryp2nova.com

Network

Bockchain

The blockchain (EVM) serves as the key state for maintaining the public ledger network, particularly regarding:

- Workload quantification
- Reward calculation and distribution
- $REACH token function
- On-chain governance
- Orders and payments

Geographic area

The ARO network operates geographically divided areas in the following way. This regional approach ensures that edge cloud resources are as close as possible to the end users, which is crucial for maintaining high service quality and competitive costs. Therefore, ARO nodes are essentially "localized".
In the ARO network, all nodes (including edge nodes and watchtower nodes) must register their regional information before starting to provide services and establishing connections with other nodes in the same area.
As a decentralized, blockchain-based protocol, ARO maintains the global state managed by the consensus layer (keeper nodes), which is recorded on the chain.
To balance geographical segmentation with security and distrust, ARO introduces a hybrid verification system on the node workload, with verification mechanisms within the region and across regions.
Within a region, each edge node must maintain persistent websocket connections with multiple Keeper nodes, and these connections are periodically rotated based on a random function on the chain, making collusion difficult.
Considering the challenges and costs of inter-regional communication, ARO uses a random challenge mechanism across regions. This mechanism uses small data packets to distribute randomly assigned challenges, cross-verifying the edge nodes to provide genuine resources.
Finally, all guardian nodes are fully interconnected to support global consensus. On-board radio distance meters.

Archived copy · cryp2nova.com

Certificate of employment

ARO Network

ARO has introduced a new protocol to provide trusted workload proof for heterogeneous edge nodes, which is called GPoW (Guaranteed Proof of Work).

General survey

This GPoW (Guaranteed Work Proof) protocol is the core feature of ARO, aiming to provide trusted resources and workload proofs for heterogeneous edge nodes, including network bandwidth, storage, computing power, etc. Different from traditional systems that only focus on the verification of a single resource type (such as storage), GPoW expands its functions to support various types of workloads, such as CDN traffic and GPU computing tasks, making it a multi-functional proof mechanism suitable for the DePIN network.

Resource virtualization and consolidation

In the first stage, ARO utilized virtualization and containerization technologies to standardize the integration of different hardware resources. This enabled the network to integrate various devices, including enterprise servers, personal computers, mobile devices, and even the WASM environment within browser plugins. Using technologies such as Docker and Kubernetes, these resources were virtualized to create standardized execution environments, allowing them to efficiently perform various tasks.

Work certificate generation

The core of GPoW is to generate trustworthy and verifiable workload proofs for different resource types.
It combines several advanced mechanisms:

- **Trusted Execution Environment (TEE):** By using TEE, GPoW ensures that the resource usage proof is securely generated without being tampered with. The TEE isolates the execution environment and generates workloads for encryption and signature that can be safely verified. This approach guarantees the authenticity of the reporting workloads for tasks such as data storage, network transmission, or computing processing.

- **Zero Knowledge Proof (ZK):** **G**PoW combines a zkVM (zero-knowledge virtual machine) to verify complex computations, such as GPU tasks, without exposing the underlying data. This enables the network to verify the contribution of workloads without exposing sensitive details, thereby ensuring privacy and security.

- **Random challenge mechanism:** To prevent nodes from fabricating workload contributions, GPoW will also employ a random challenge method. The network sends random requests to the nodes, and the nodes must respond promptly with valid workload proofs. This strategy reduces the risks of Sybil attacks and fraudulent reports.

CRYP2NOVA

Archived copy · cryp2nova.com

Certificate of employment

ARO Network

ARO has introduced a new protocol to provide trusted workload proof for heterogeneous edge nodes, which is called GPoW (Guaranteed Proof of Work).

Online verification and settlement

After the workload proof is generated, it will be submitted to the GPoS module of the blockchain for verification. This process includes:
Proof verification: The on-chain logic uses TEE proofs and zk-generated proofs to verify the submitted proof.
Rewards and penalties: Nodes that are verified receive token rewards, while nodes that submit fraudulent or delayed proofs face penalties. This mechanism ensures fair participation and prevents dishonest behavior.
Transparent settlement: All transactions and evidence verification are recorded on the chain, providing transparency and allowing participants to monitor their contributions and returns.

Security and scalability

To prevent potential security threats such as Sybil attacks or forged proofs, GPoW employs TEE and zero-knowledge proofs to integrate multiple layers of verification. This ensures the reliability of the proofs generated by the nodes. Moreover, GPoW is designed to be modular and scalable, allowing the network to support new resource types and adapt to different application scenarios.

CRYP2NOVA

Conclusion

GPoW (Guaranteed Work Proof) is an innovative proof mechanism designed in the ARO network. It utilizes tee, zkVM, and random challenge technologies to verify the workload of heterogeneous resource nodes.
By providing an end-to-end solution from resource virtualization to on-chain verification, GPoW ensures the integrity, transparency, and security of the ARO network, achieving efficient and trustworthy decentralized service delivery.

Archived copy · cryp2nova.com

Consensus

ARO introduced a novel protocol to provide guaranteed consistency and a betting mechanism, which is named GPO (Equity Guarantee Proof).

General survey

This GPO (Equity Pledge Guarantee) agreement integrates the resource verification from GPoW (Proof of Work Guarantee), and is managed by a designated manager. Unlike the traditional PoS mechanism, GPO introduces a guarantee-based block-building model, in which the block-building capabilities of the keeper nodes are directly related to their ability to verify and process the workloads proofs from edge nodes.

The role of the guard node

Guard nodes are crucial intermediary roles in the GPO network, and their core responsibilities include:

√ Proof of Workload Verification: Verify the authenticity and accuracy of the GPoW proofs submitted by various edge nodes (such as CDN endpoints, GPU computing nodes, and storage providers).
√ Consensus Participation: After verification, collaborate with other sentinel nodes to reach a consensus, confirming the legitimacy of the workload proofs, ensuring that only compliant contributions are rewarded and identifying fraudulent activities.
√ Staking Guarantee: Must stake tokens as a guarantee of the reliability of their verification work. The amount staked directly determines the maximum workload scale that the node can verify.

Stake mode and guarantee mechanism

GPO employs a unique GPoS staking mechanism, characterized by a dynamic upper limit for staking and enhanced accountability guarantees:

√ Dynamic Quota Limit: Unlike traditional PoS, the quota limit for the custodian nodes is not fixed or unlimited. Instead, it is dynamically determined based on the node's ability to handle and verify the workload (in terms of quantity and complexity).
√ Reward Mechanism: The rewards are directly proportional to the effective work volume of the custodian nodes (the quality and quantity of the verified proofs) and the amount of质押.
√ Punishment (Penalty) Mechanism： If the custodian nodes fail to correctly verify the proofs (such as negligence) or engage in fraud (such as forging the proofs)， the tokens they have pledged will be partially or fully confiscated. The degree of confiscation is linked to the severity of the violation， in order to ensure accountability and deter malicious behavior.

Archived copy · cryp2nova.com

Consensus

Verification and consensus process

The GPoS verification process consists of several steps to ensure consensus on the proof of work:

√ Submission of proof: Edge nodes submit their workload proofs to the guardian nodes, which are verified by the GPoW mechanism.
√ Initial verification: Each Guardian node performs the initial verification, using cryptographic techniques such as TEE proof and zero-knowledge proof (ZKP) to check the authenticity and correctness of the proof.
√ Cross-validation and consensus: Guardian nodes participate in the cross-validation process, where multiple guardian nodes review the same set of proofs. The network uses a consensus protocol to reach an agreement on the validity of the workload proof.
√ Chain settlement: After reaching consensus, the verified evidence will be recorded on the chain through smart contracts. Then, based on the verification contributions of the edge nodes, rewards will be distributed to the edge nodes, and the guardian nodes will receive a portion of the rewards for their verification services.

Scalability and security

The GPoS mechanism addresses the issues of scalability and security through its structured approach:

√ Scalability: By linking the stacking capability of Keepers nodes with their workload capacity, GPO can dynamically scale with the growth of the network. As the number of edge nodes increases, the number of keeper nodes and their locking capabilities can also be expanded to ensure consistent verification performance.
√ Security: The integration of TEE, ZKPs, and robust pruning mechanisms ensures a high level of security. Dynamic equity caps prevent the concentration of equity and power, reducing the risks of centralization and malicious attacks. Additionally, the strict on-chain consensus process can prevent fraudulent workload verification.

Conclusion

GPO (Guarantee of Profit) constitutes the trust and incentive layer of the ARO network, supporting transparent, secure and efficient verification of decentralized resources. It provides an advanced consensus and bet model, ensuring that the bets of the guardian nodes are consistent with their verification capabilities.
By linking the stack limit with the workload processing capacity and implementing a powerful reduction mechanism, GPoS ensures that the ARO network maintains high standards of security, reliability and decentralization. This innovative approach sets a new benchmark for the stake mechanism in the DePIN network, promoting efficient and trustworthy decentralized service delivery.

CRYP2NOVA

Archived copy · cryp2nova.com

The ARO PeerEdge middleware consists of three core components: Peer Virtual Machines, PeerDTS, and Peer Routing.

ARO PeerHVM

In the ARO network, coordinating and managing distributed heterogeneous resources is of utmost importance. We are confronted with the challenge of efficiently scheduling and adjusting various resources (such as computing, storage, and bandwidth) across different hardware and operating systems. The peer-heterogeneous virtual machine technology of ARO aims to create flexible and efficient resource allocation for various contents by virtualizing and standardizing various hardware and system resources to meet this demand.

Virtualization of heterogeneous resources

Virtualization of heterogeneous resources involves many technical challenges, such as hardware diversity, operating system compatibility, and performance optimization. To achieve this, PeerHVM aims to support a wide range of hardware architectures and operating system environments, from x86 to ARM, WASM, and even browser-based environments. This multi-architecture compatibility gives PeerHVM high adaptability, enabling it to accommodate various devices in distributed networks and providing unprecedented scalability.

Standardization strategies in distributed networks

In a distributed environment, resource standardization requires unified interface and protocol design. The standardization strategy of PeerHVM decomposes resources into standardized modules, and then assembles these modules into customized resource pools tailored to specific business requirements. Different hardware resources are abstracted into unified service interfaces by PeerHVM, allowing the system to seamlessly call these standardized resource units, achieving rapid adaptation and flexible scheduling.

Resource scheduling, monitoring and management

This scheduling layer is responsible for dynamically matching resources based on user requirements, ensuring the efficient utilization of distributed resources. By leveraging advanced load balancing and adaptive adjustments, it can handle various workloads in real time. Customized scheduling algorithms are used to coordinate the unique demands of heterogeneous resources, thereby achieving optimized and responsive allocation.
The reliability monitoring layer that focuses on maintaining resources continuously monitors and identifies the hardware and performance status between nodes. It includes reliable tracking of resource usage, prevention of attacks and false alarms.

Furthermore: Customized containers of ARO

PeerHVM's virtualization goes beyond resource abstraction,
achieving deep optimization of resources. The customized containers developed by ARO can run efficiently in various environments, especially in small and edge devices. PeerHVM achieves low-power operation. The customized virtualization technology enables different hardware architectures to maximize their computing advantages, thereby improving the overall network resource utilization rate and reducing the cost of edge clouds.

Archived copy · cryp2nova.com

PeerEdge

The ARO PeerEdge middleware consists of three core components: Peer Virtual Machines, PeerDTS, and Peer Routing.

ARO agreement

In order to establish a distributed edge cloud to meet the demand for large-scale P2P data transmission across different nodes, ARO developed a proprietary P2P transmission protocol, PeerDTS. This protocol is specifically tailored for the edge environment and optimized for high-speed and reliable data transmission. It utilizes advanced multi-channel transmission capabilities, customized erasure coding technology, and stateful-to-stateless transmission solutions.

Edge optimization

Unlike the standard protocols designed mainly for centralized content delivery networks (CDN), the ARO protocol has been finely tuned for distributed, small-scale P2P and edge environments. Standard P2P protocols often struggle in such situations, as they lack specific edge optimization and their performance is similar to that of CDN. PeerDTS overcomes these limitations by implementing multi-channel and adaptive transmission mechanisms, enabling data to move more efficiently between edge nodes. This customization allows smaller nodes and edge devices to achieve comparable performance to traditional CDN, fully leveraging the advantages of the decentralized architecture.

Static content, dynamic coding

To meet the demand for transmitting large amounts of data through a distributed network, ARO dynamically re-encodes the static content during the transmission process. ARO's protocol does not simply send the static data; instead, it divides the data into blocks, and each block is embedded with unique feature markers that support error correction and recovery. PeerDTS implements low-complexity erasure coding (reduced to O(N) typically from O(N^2)) and is directly installed on edge devices, achieving strong fault tolerance and efficiency without the need for specific chips.

Archived copy · cryp2nova.com

PeerEdge

The ARO PeerEdge middleware consists of three core components: Peer Virtual Machines, PeerDTS, and Peer Routing.

ARO piston engine

The matching algorithm is the holy grail.

This ARO piston engine is an important component of the ARO network, capable of achieving high availability and economic benefits.

Why is the matching algorithm so important? The extent to which users are willing to pay for their needs varies. The needs are classified into high-value and low-value categories. At the same time, the cost of network resources fluctuates constantly. These changes are unpredictable and do not automatically align with the demands. The efficiency of matching directly affects the return on investment for network operators, which is a matter of life and death.
From the perspective of resource scheduling, matching high-value demands with low-cost nodes is the key to success. This is the killer feature of the ARO PeerRouting engine, which has been acquired through nearly a decade of practical service experience.

Perception, before it occurs

The ARO peer routing engine achieves effective matching through a set of mature technologies developed by the ARO team.

High-speed content transmission in P2P networks: This feature has been elaborated on in the previous chapter.
Channel scheduling in transmission: As mentioned earlier, the ARO peer routing engine is proficient in managing and optimizing transmission channels.
A core challenge in P2P networks with channel awareness based on partial information is the ability to infer the overall channel width from limited data (for example, estimating channel capacity based on data fragments over a period of time). The ARO PeerRouting engine integrates a full-chain awareness algorithm, which adjusts the content transmission strategy based on real-time perception results. This enhancement significantly improves handshake efficiency while reducing transmission losses and delays.
Preemptive deployment: In addition to "fragment awareness", the advanced feature of the routing engine lies in preemptive deployment. Traditional network solutions usually handle demands before matching resources, while the peer routing engine uses a packaging algorithm to pre-deploy resources, increasing utilization by more than 50%. This strategic vision can achieve optimal resource allocation before demand surges.

Archived copy · cryp2nova.com

Introduction to Edge Nodes

- The core concept of edge computing is quite simple: to place the servers closer to the users. By doing so, users can experience faster response times and significantly reduced network costs. This means that no matter where the users are located, we must recruit nodes that can serve them nearby - otherwise, the essence of edge computing will collapse.

- We refer to these smaller nodes as edge nodes. Technically, anyone can run an edge node. Even household devices and network resources can be utilized, with minimal impact on daily life. This is entirely in line with the spirit of Depein – contributing idle or surplus resources in exchange for fair compensation.

- That is to say, edge nodes do not necessarily have to be highly miniaturized. In fact, the ARO network is designed as a set of protocols that support interaction between heterogeneous resources and users, and provide users with effective network services.

CRYP2NOVA

Archived copy · cryp2nova.com

Award

ARO Reward Resource Provider

That is, the edge node, by rewarding local tokens, contributes Internet resources such as storage, computing and bandwidth.

These rewards are distributed based on verified contributions, using mechanisms such as work volume verification and random challenges to ensure fairness and trust.

Without any restrictions, any hardware can be connected to the network and idle resources can be converted into profits. To support the early growth, ARO provides subsidies for contributions until the revenue at the application level can sustain the ecosystem, thereby creating a self-reinforcing growth and incentive cycle.

Archived copy · cryp2nova.com

Edge node type

Would you like to know which edge node is the most suitable for you? Here is an overview of the available options to help you make a decision.

01 Hardware Nodes (ARO Pod and ARO Link)

The ARO network is community-driven rather than cloud-controlled. Most importantly, you don't need to be an expert in technology to participate in it - you can directly run a node at home.
Hardware nodes are very suitable for beginners, providing pre-configured, user-friendly devices that have been optimized for efficient operation. They simplify the setup by eliminating the need to configure node clients or adapt to your internet environment.
Currently, there are two hardware node models available: ARO pod and ARO link.
· This ARO pod is a compact plug-and-play device designed for 24/7 operation, with excellent uptime, and is ideal for home use.
· This ARO link can also function as a standard router while generating revenue from your idle internet resources, making it an ideal choice for dual-function business scenarios.

02 Software Node (ARO Client)

The ARO network is an unauthorized edge cloud designed to utilize various resources. To support this, ARO provides software images that the ARO customers can install on various devices, including PCs, workstations, or data centers.
Please note that ARO customers are targeted at advanced users, who require that the devices and operators possess higher professional skills.

03. Lightweight Node (ARO Lightweight)

For those seeking accessible entry points, ARO Jianxing nodes operate browser extensions in a lightweight manner, such as Chrome extensions. These nodes enable anyone to join the ARO network with minimal cost and effort. By deploying ARO Jianxing, ARO promotes exploratory resource construction in new markets and establishes the supply necessary for a strong edge cloud service. This makes ARO Jianxing an ideal way to expand the user base of the network.
During... ARO Jianxing, like other edge nodes, the nodes generate returns. Compared to hardware or software nodes, their lower service capacity results in smaller returns.

CRYP2NOVA

Archived copy · cryp2nova.com

Specification of equipment

ARO Network

Would you like to know which edge node is the most suitable for you? Here is an overview of the available options to help you make a decision.

ARO Pod Specifications

Equipment: ARO Hangar Home Gateway

√ Model: AROP-01
√ CPU: Quad-core ARM processor
√ Memory: 2GB
√ System Storage: 64GB eMMC
√ Network Interface: 1× Ethernet
√ USB Interface: 1× USB Type-C
√ Power: 5V/2A
√ Size: 103×103×20 millimeters
√ Packaging Contents: 1× Manual, 1× Ethernet Cable, 1× Power Cable

ARO Link Specification

Equipment: ARO Link Router

√ Model: AROL-01
√ Chipset: MT7981BA + MT7976C + MT7531AE
√ Memory/Storage: 1GB DDR4, 128GB eMMC
√ Wireless Standards: 802.11a/b/g/n/ac/ax
√ Wireless Speed: 2.4 GHz: 574 Mbps; 5GHz:2402 Mbps
√ Working frequency: 2.4GHz + 5GHz
√ RJ45 ports: 1×Wide Area Network + 4×Local Area Network (10/100/1000 Mbps)
√ Antennas: 6 pieces
√ Operating system: OpenWRT
√ Dimensions: 278×179.1×33 millimeters

The recommended requirements for the software client (ARO client) The ARO client is currently only provided as an x86 virtual machine (VM) image.

To use the client, users must deploy the virtual machine image on a bare-metal server or desktop computer equipped with x86 architecture CPUs using any virtualization solution of their choice.

For detailed installation and usage instructions, please refer to the ARO Client Image Installation Guide..

Archived copy · cryp2nova.com

Pecification of equipment

ARO Network

Bandwidth-based recommendations require

We provide recommended hardware specifications for operation based on your bandwidth. If the bandwidth falls within the listed values, the requirements can be estimated through linear interpolation.

For 100 Mbps or lower

CPU threads: ≥ 2
Memory: 2 GB
Disk:
≥ 50 GB solid-state drive

For 500 Mbps

CPU thread count: ≥ 12
Memory: 12 GB
System disk: ≥ 50 GB (SSD)
Data disk: ≥ 600 GB (SSD)

For 1 Gbps

CPU threads: ≥ 24
Memory: 32 - 48 GB
System drive: ≥ 240 GB SSD
Data drive: ≥ 2 TB SSD

For 5 Gbps

CPU thread count: ≥ 48
Memory: 128 - 192 GB
System disk: ≥ 240 GB SSD
Data disk: ≥ 10 TB SSD

Suggestions for further improving performance

General recommendations: Although ARO customer software (especially for operators with enterprise-level bandwidth)

CRYP2NOVA

Public IP address

NAT type: Full-cone NAT or higher IPv6 support

CPU clock speed: ≥ 2 GHz

Random 4K read IOPS of data disk: ≥ 30,000

Read and write IOPS of system disk: ≥ 15,000/10,00

Archived copy · cryp2nova.com

Common questions regarding edge nodes

ARO Network

Question: Which is better, the hardware node or the software node?

Answer: The capabilities of all edge nodes are the same. The hardware nodes (ARO pods and ARO links) provide a higher level of integration, which makes them easier to install, configure and maintain compared to the software nodes (ARO customers).

estion: Can I run edge nodes anywhere in the world?

Answer: Technically, you can run an edge node anywhere. However, edge nodes perform best when they are close to the end users, as this is the basis for how edge cloud operates. To achieve the best results, we recommend running edge nodes in the regions where the existing ARO services are available, in order to maximize the revenue potential.

Question: Will this device compromise user privacy?

Answer: No. ARO never collects personal data from your daily operations. The only resource ARO utilizes is your idle bandwidth - that's all.

Question: Will joining the ARO network affect my internet usage?

Answer: No. ARO only uses your idle bandwidth, ensuring that it will not interrupt your regular internet activities. You can earn passive income while continuing to use the internet as usual.

The ARO hardware nodes (ARO pods and ARO links) are highly integrated dedicated devices designed to optimize resource allocation without affecting your daily internet experience.

CRYP2NOVA

Archived copy · cryp2nova.com

User Guide - Select Your Node

Things to know before starting

Before running the edge nodes on the ARO network, the following points need to be understood:

ARO is an unauthorized network, which means there is no need for prior permission or qualification to join.

A stable internet connection is of vital importance. Higher bandwidth and connection stability significantly increase the returns for you to operate edge nodes.

Where you operate your edge nodes in this region is very important. Being closer to end users can enhance their access to Internet content, thereby bringing higher returns.

You can exit the network at any time and receive rewards.

Edge nodes mainly utilize your idle Internet resources to provide services for the ARO edge network, having the least impact on your regular Internet experience. The choice is always yours.

You can run a hardware node or a software node (the software solution will be launched soon). Please refer to the next section to learn how to choose the best option.

Archived copy · cryp2nova.com

User Guide - Select Your Node

ARO Network

Which type of ARO node is suitable for me?

Here is a simple guide to quickly find the most suitable node type for you:

ARO HUB:
Specialized plug-and-play device.
Optimized for high uptime and returns.
ARO Jianxing:
Lightweight browser extension. Added with minimal cost and effort.
ARO Customers:
Install on your own device to unlock more functions.
ARO Link:
WiFi router with built-in ARO node.
Selection of business scenarios.

How do I manage my ARO nodes?

This dashboard (currently for Devnet) is an integrated platform for you to manage edge nodes and track rewards.

By creating an ARO account, you can log in and manage your own edge nodes and rewards at any time. For detailed instructions, please refer to the dashboard user guide on this page, including:

01 **Access the dashboard**

02 **Create an ARO account**

03 **Recommend friends to join ARO**

04 **Manage the edge nodes in the dashboard**

05 **Claim your rewards**

CRYP2NOVA

Archived copy · cryp2nova.com

User Guide - ARO Dashboard

ARO Network

General guide

This ARO dashboard is an integrated platform for you to manage edge nodes and rewards. With the ARO dashboard, you can:

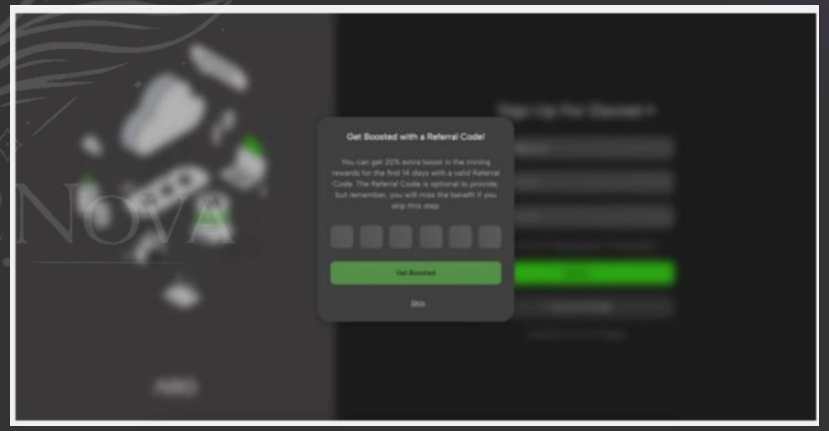
√ Create an ARO account
√ Access your referral code, invite friends to join ARO, and receive referral rewards
√ Manage all your edge nodes
√ Track and manage your rewards
√ Manage your funds

ARO ccount

New users must register an ARO account to get started. After registration, you can log in at any time to manage your edge nodes and related activities.



This is the sign-in page. If you have just arrived at ARO, please click on "Sign Employment Agreement" to create your ARO account. You can register using your email address or Google account. For email registration, you need to set a password and verify your email.



During the registration process, the system will prompt you to enter the referral code. Using the referral code can give you a 20% bonus increase within a limited time after registration. If you don't have the code, you can skip it.

Archived copy · cryp2nova.com

User Guide - What's on the Dashboard?



This top bar provides access to all available pages:

- Edge Nodes: View and manage all the edge nodes linked to your ARO account. You can add new nodes or delete existing ones. Clicking on the device card will display the details of that node.
- Statistics: Monitor the number of edge nodes you are running, their online status, and the total returns obtained by running them.
- Funds: Manage your funds, including claiming token rewards to your wallet. The wallet subscription and token claim functions will be available in a later stage.
- Introduction: Access your referral code, copy the referral link, and track the bonuses obtained through referrals.
- ARO ID: Manage the basic account settings and operations of your ARO account.

Archived copy · cryp2nova.com

User Guide - ARO Hanger and ARO Link Tutorial

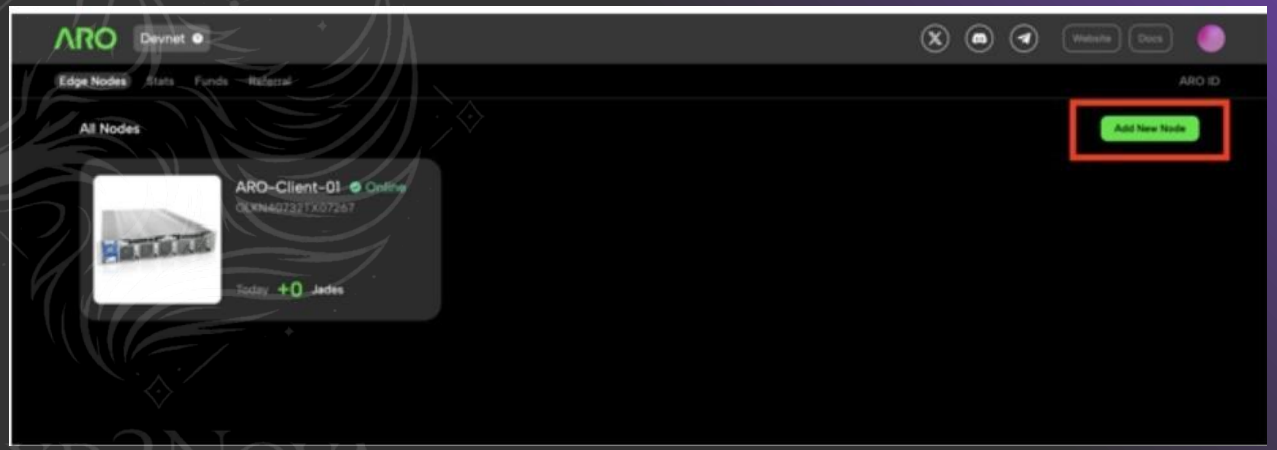
ARO Network

Step 1: Plug in the power supply

Set up hardware nodes, such as ARO pods or ARO links.
The plug-and-play design is simple and intuitive.
Unpack your device, turn on the power, and connect it to the internet using the provided cable. This process will take approximately one minute. Before proceeding to step 2, make sure you have a stable internet connection.

Step 2: Add the device to your dashboard

Make sure you have created an ARO account (ARO ID) and logged in to the dashboard.



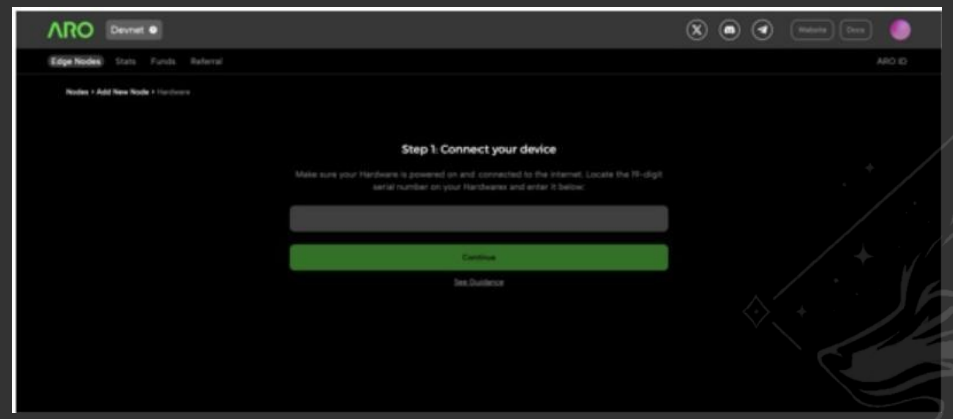
In... On the upper edge node page, find the "Add Your Edge Node" button.
Click on the button and select the hardware node to start the installation process.
Note: The device must remain online throughout this process (powered on and connected to the internet).

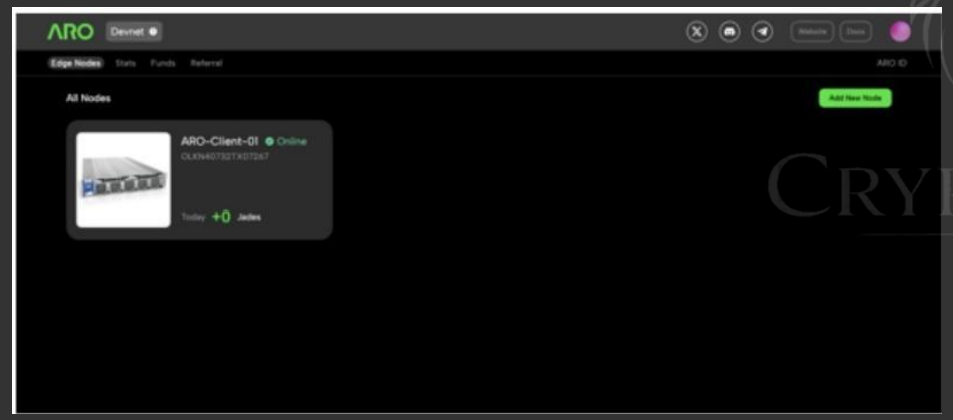
CRYP2NOVA

Archived copy · cryp2nova.com

User Guide - ARO Hanger and ARO Link Tutorial

ARO Network





The system will prompt you to enter the serial number which is printed on the device label.
Please enter carefully to avoid any mistakes.

If successful, the dashboard will identify your device, and you can complete the setup with just a few clicks.

Step 3: Get ready to go!

After adding the device, the device card will be displayed on the edge node page.
Your first ARO edge node is now ready to run!

CRYP2NOVA

Archived copy · cryp2nova.com

User Guide - ARO Client Installation and Initialization Tutorial

ARO Network

Part 1: Prepare the Virtual Machine Environment

To run the ARO client image, you need a virtualization environment. Here are the recommended preparation steps:
Select a virtualization platform
Choose one of the following virtualization platforms (or other Linux-compatible solutions):
Proxmox VE: An open-source virtualization management platform suitable for both enterprises and individuals.
VMware Workstation/Player: Perfect for local testing and development.
VirtualBox: A free and user-friendly virtualization tool.
Install the virtualization platform
Follow the official documentation of the selected platform to complete the installation. For example:
Proxmox VE: Download from the Proxmox website and install.
From the download and installation website of VirtualBox. Ensure that your hardware supports virtualization (VT-x/AMD-V is enabled).
Verify the environment
Ensure sufficient disk space (recommend at least 50GB).
Verify the network connection to allow virtual machines to access the external network (required during initialization).
Note: This tutorial assumes that you are familiar with installing and configuring the virtualization platform you have chosen. If necessary, please refer to the official documentation of the platform for detailed guidance.

CRYP2NOVA

Archived copy · cryp2nova.com

User Guide - ARO Client Installation and Initialization Tutorial

Part 2: Selecting Images and Allocating Resources

After setting up the virtual machine environment, you need to select the ARO client image and allocate the appropriate resources.

Step 1: Obtain and select the ARO client image

Download the image
Download the latest version of ARO customer profile (in .iso format).
Select Image
Proxmox VE: Log in to the Proxmox web interface, navigate to Storage (for example, local), and upload the.iso file.
VirtualBox: Create a new virtual machine, select "Use an existing virtual hard disk file", and point to the ARO Client.iso file.
VMware Workstation/Player: Create a new virtual machine, select "Use an ISO image file", and specify the ARO Client.iso file.
Verify the image
Ensure that the image file is not corrupted by verifying its checksum (such as MD5 or SHA256).

Step 2: Create a virtual machine and allocate resources

Create a virtual machine
In your virtualization platform, create a new virtual machine and select the ARO Client.iso file as the boot medium.
Resource Allocation Proposal
To ensure the smooth operation of the ARO client, this proposal suggests allocating resources based on the following requirements.
Save Configuration
Confirm the virtual machine settings and save them before starting.
Note: Adjust the resource allocation according to your hardware capabilities and the requirements of ARO customers. For complex tasks, you may consider increasing the CPU and memory.

Archived copy · cryp2nova.com

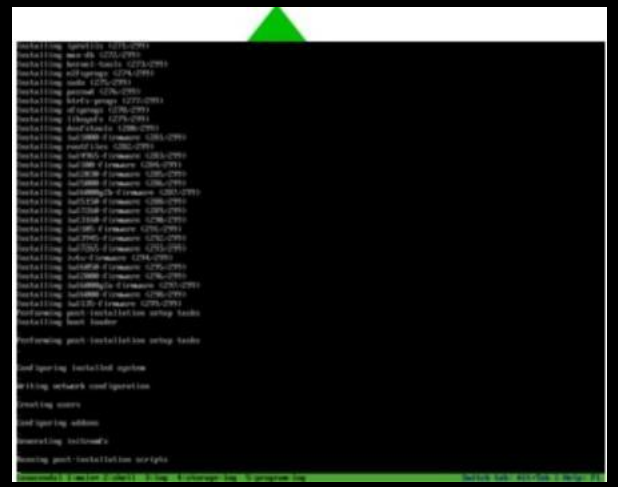
User Guide - ARO Client Installation and Initialization Tutorial

Part 3: Run the image and perform the initial setup of the edge nodes

This section describes how to run the ARO client image and configure the edge nodes for initial use.

1.Start the software image

After setting up the virtual machine, start it to launch the ARO client software image.

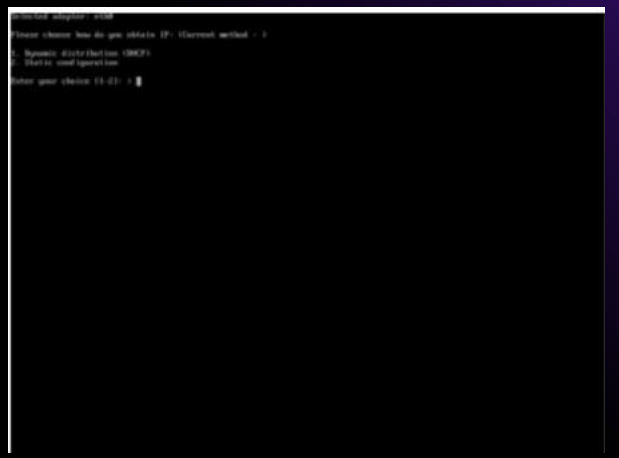


2. Configure the network

After the loading process is completed, the network configuration page will appear.



Select Option 1 (the default option).



Configure IP settings:
Select 1 to have DHCP automatically assign the IP address.
Select 2 for a static IP. If you need to manually configure the network.

Archived copy · cryp2nova.com

User Guide - ARO Client Installation and Initialization Tutorial

ARO Network

3. Initialization activation process

Review the terms of service and privacy policy. Select "Agree" and continue to proceed.

The 19-digit virtual serial number will appear on the screen for this edge node. Please note down this number as it is crucial for activation.





Open the ARO dashboard (accessible via the ARO project website or the designated interface).

Navigate to Edge Node > Add New Node > Software Node, and enter the 19-digit virtual serial number.

Archived copy · cryp2nova.com

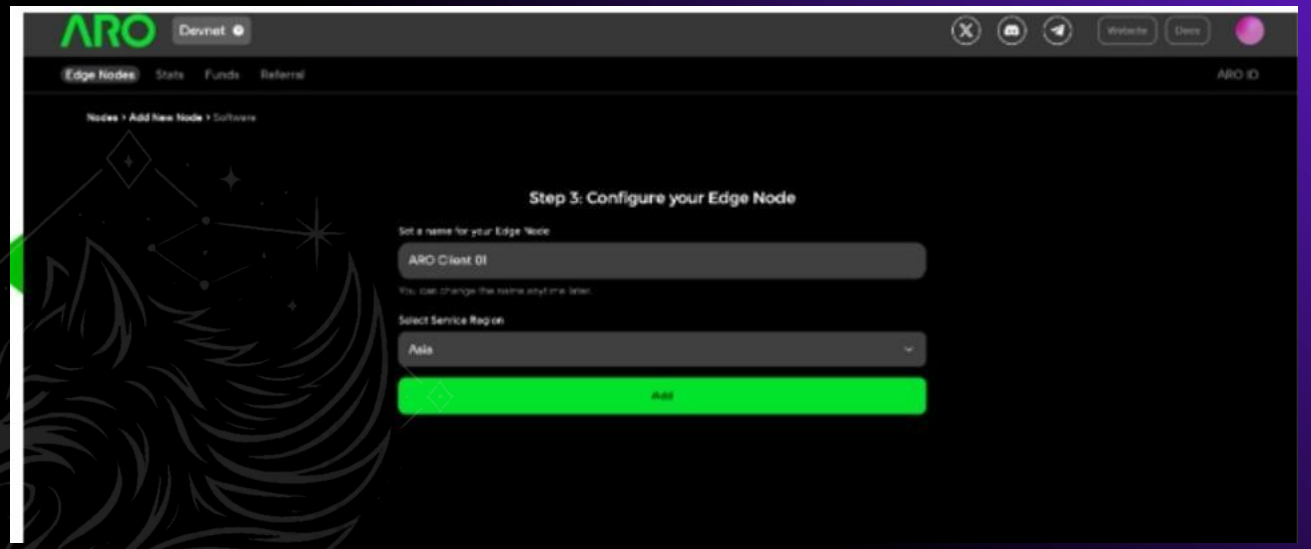
User Guide - ARO Client Installation and Initialization Tutorial

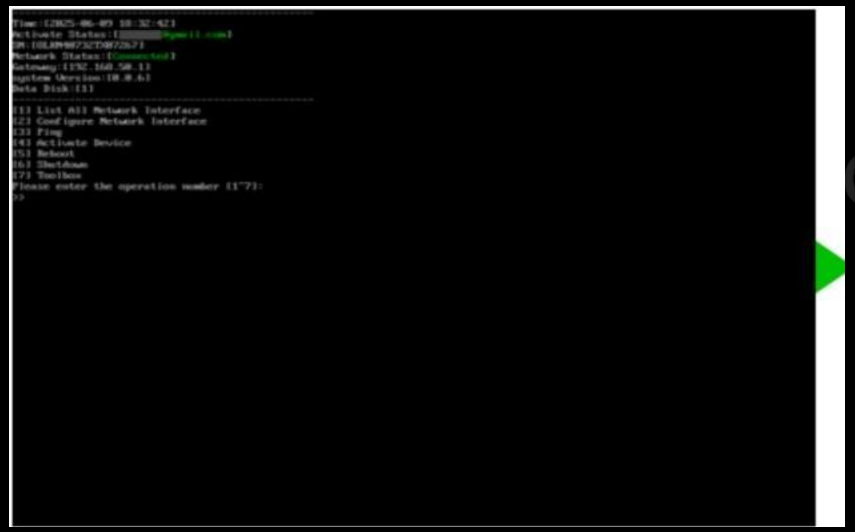
ARO Network

The dashboard will identify the software image instances and display their information.

Important: Ensure that the software image is online during the activation process. If it is offline, the activation or node addition process may fail.

Select the appropriate area and assign a name to the new edge node.





4. Verify the operating status

Congratulations! You have successfully set up your new edge node. The CMD console will return to the main menu, showing the real-time network and activation status. If both statuses are displayed in green, then your edge node is operating successfully.

Cryp2Nova

Archived copy · cryp2nova.com

User Guide - Edge Node's Web Console

ARO Network

The Web console of the hardware node

The dashboard provides access to the web console for managing the devices.

In... On the upper edge node page, find the button in the upper right corner of the "Web Control Console".

View device information in this tab.





Monitor the network status in this tab.
Restart your device directly in this tab.

Configure the IP settings in this tab.

CRYP2NOVA

Archived copy · cryp2nova.com



Our link tree

It's always a good idea to find all the latest links here:

https://linktr.ee/AroNetwork

Official links and entries

Official website:https://aro.network

User Dashboard (for Devnet):https://devnet-dashboard.aro.network/

Open source code repository:https://github.com/aro-network

Official Blog:https://medium.com/@AroNetwork

Hardware sales page

Coming soon.

Social media

Telegram:https://t.me/ARO_Network

Disharmonyhttps://discord.com/invite/Rc4BMUjbNB

Twitter/X:https://x.com/AroNetwork

Archived copy · cryp2nova.com

THANKS

BitcoinZK

CRYP2NOVA

Archived copy · cryp2nova.com