Ankr A Shared Cloud Economy Driven by Idle Processing Power

Table of Contents

01 A Brief Introduction to Ankr

As technology continues to advance, so too does the concept of cloud computing, also known as on-demand computer system resources. What began only as mainframes, on-site data centers, and private clouds has evolved into something entirely different: public clouds. Today, companies are reducing costs and speeding up deployment with the help of public clouds and global cloud service providers (CSP's) like Amazon AWS, Microsoft Azure, and even Alibaba. But with so many companies relying on CSP, the power of old-school data centers is being underutilized. Every year, an increasing amount of idle computing power goes unused, untouched–left over.

That's where Ankr comes in.

Ankr believes idle cloud computing power should not go to waste. In fact, at Ankr, we believe idle cloud computing power could replace the need for large CSPs altogether. With Ankr's technology, companies can utilize excess cloud computing power from data centers and edge devices that are not being used to their full potential. As if the idea of recycling computing power wasn't interesting enough, there is much more to be excited about when it comes to Ankr.

First, as trends such as Internet of Things (IoT) technology continue to grow, the need for highly-distributed infrastructure, service, and intelligence increases. With Ankr's ability to repurpose unused cloud computing power from on-site data centers and devices around the world, companies can meet this need by implementing a truly distributed system when it comes to hosting, computing, control, and information. Such a distributed system provides loss avoidance, improves production, and mitigates risk when organizing data and analytics.

On the flip side, Ankr also provides a slew of benefits for owners of unused cloud computing power. Now, consumers and enterprises can monetize their surplus computing power, whether in the form of a device, an on-prem data center, private cloud, or even public cloud.
With the introduction of Ankr, establishing an operational architecture that utilizes distributed computing power becomes easy. Use Ankr to create a production environment that leverages people, processes, and technology in a scalable manner and without getting stuck in a vendor contract. Even enterprise operations that need their legacy systems to fit into a larger framework can use Ankr via virtualized hosts, data management, and open API tools to guarantee a production environment that will stand the test of time.

At Ankr, our solution of a shared, repurposed cloud economy is based on cloud-native and blockchain technology, providing us with abstraction over various types of hardware, operating systems, and unified user interfaces. We define the organizational structure of each participating device based on its condition, taking into consideration aspects like location, bandwidth, CPU, memory, and more.

02 Dynamics of Ankr's Technology

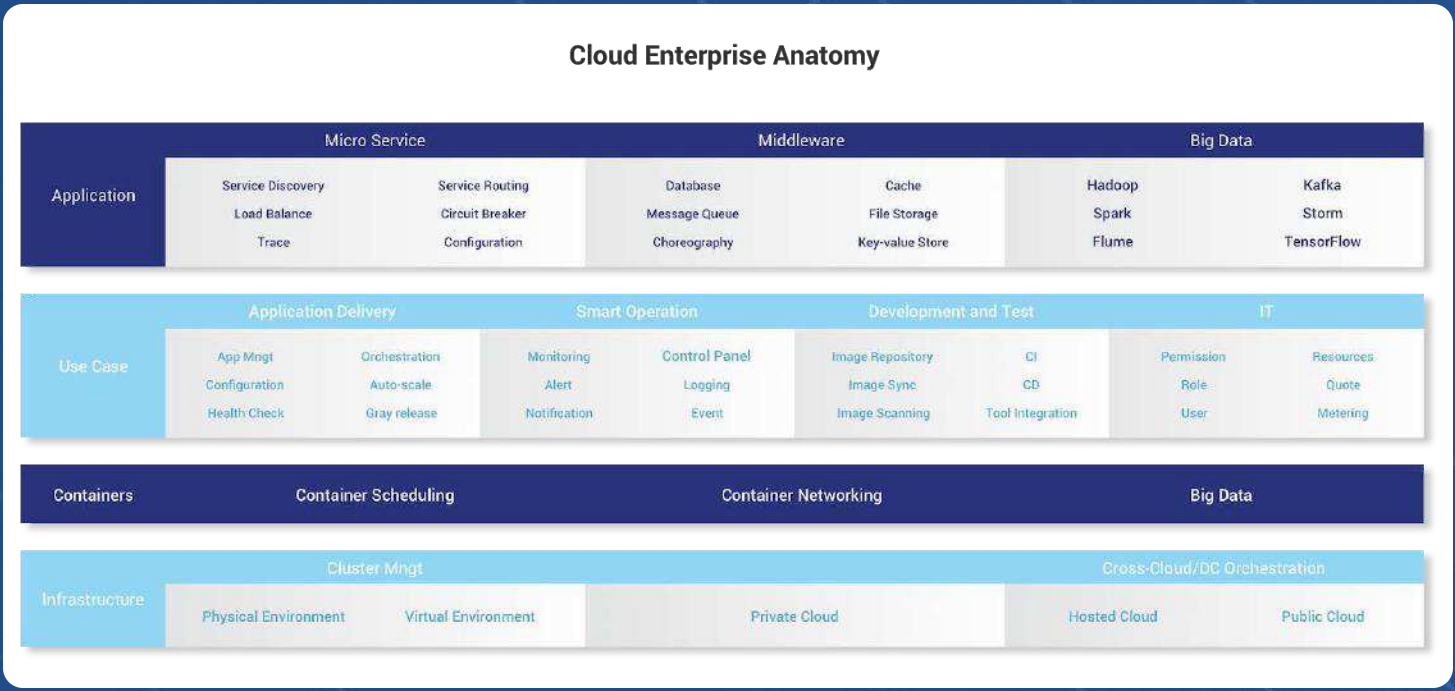
Distributed Cloud Computing Network (DCCN)

In order to build a distributed, shared cloud computing platform, Ankr uses Cloud-Native, container-based environments. Ankr then builds its own architectural and resource allocation algorithm on top of cloud native to include nearly all types of infrastructure resources. This is known as a Distributed Cloud Computing Network (DCCN).

Cloud Native

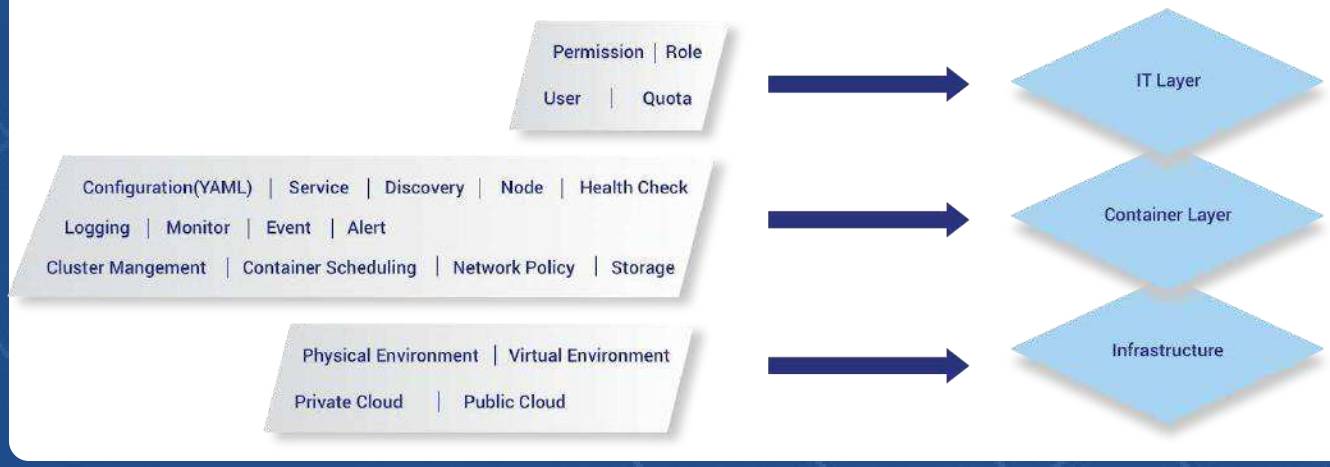
Cloud-Native is a term used to describe container-based environments, which are used to develop applications that have been built with services packaged into containers. These services are deployed as “microservices” and are managed on an elastic infrastructure through agile DevOps processes and continuous delivery workflows.

Where operations teams would normally provision and monitor the infrastructure of resource allocations to applications, cloud-native applications are deployed on an infrastructure that abstracts the underlying computer, storage, and networking primitives.



Using Ankr's DCCN platform, developers and operators using applications do not directly interact with infrastructure providers' APIs. Instead, a local orchestrator will handle resource allocation automatically. The controller and scheduler, which are essential components of the orchestration engine, will handle resource allocation and the life cycle of applications according to Ankr's instructions.

Kubernetes Layers of Concept



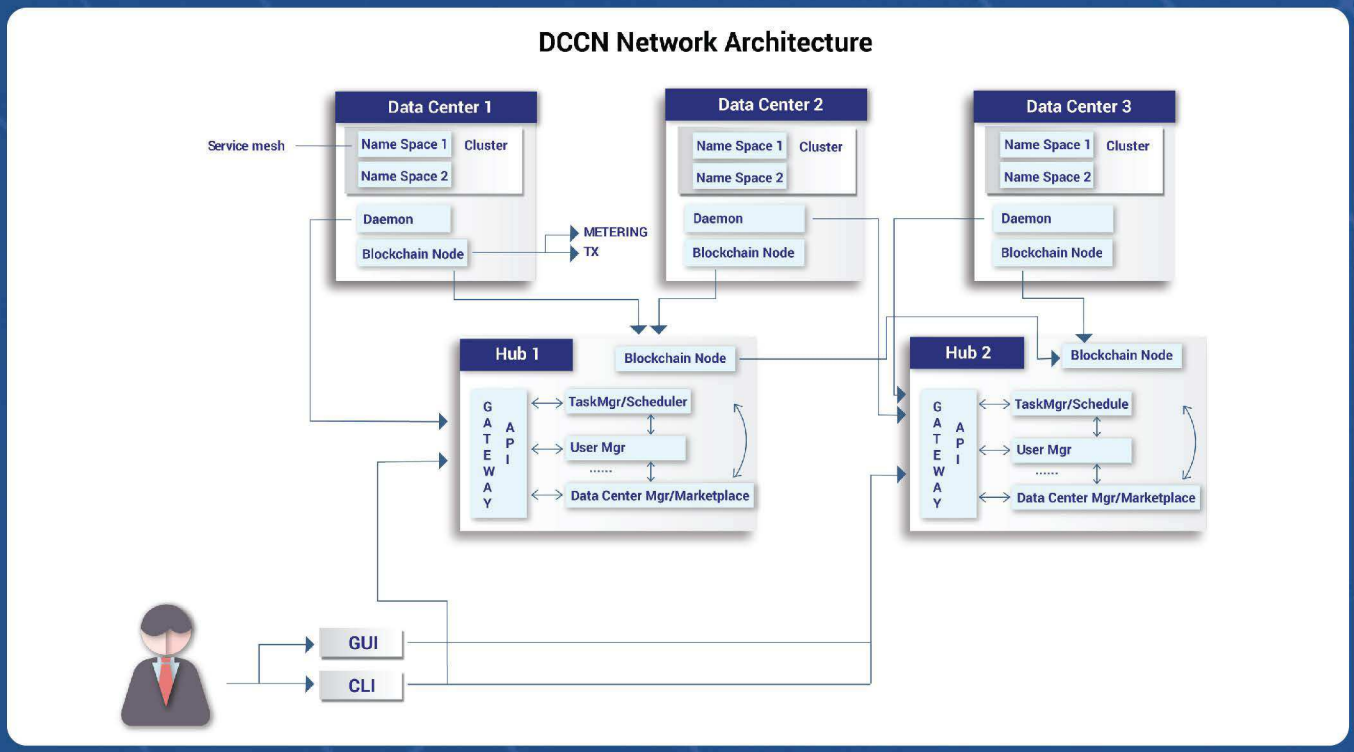
Ankr wants to offer a cloud computing platform for running workloads designed as cloud-native applications in a distributed manner. With the help of Cloud-Native, Ankr is able to focus on its own technical details via integrating with various Cloud-Native solutions such as Observability & Analysis (Prometheus, Fluentd, Jaeger), Service Mesh and Discovery (Envoy, Istio), Streaming (GRPC), Application Definition (Helm), etc.

Ankr Technology Stack

Architecture

Basically, the Ankr DCCN system is deployed and distributed over the computing resources managed by Kubernetes across all geographic locations. Resources configured into clusters in Kubernetes are connected to each other via a specialized type of clusters called Ankr Hub. Hubs at this time are fully set up and controlled by Ankr and serve as key nodes to relay and dispatch the computing tasks to other working clusters. The working clusters are the places or units actually running users' computing jobs.

There are a lot of technical details to be discussed later. But one thing we need to emphasize is that end users of Ankr should use DCCN in a similar manner as other centralized CSP such as AWS or Azure. Through Ankr's GUI or CLI, a user will feel comfortable configuring and deploying their infrastructure, service or applications, which are delivered via Ankr's innovation to gracefully incorporating Cloud Native and Blockchain technology.



Resource Scheduler and Fairness Algorithms

The core task of a resource scheduler is to select and assign tasks to nodes for user applications. These nodes will then run in the desired state.

In our multi-node, multi-user, and multi-task scheduling environment, a weighted dominant resource fairness algorithm (WDRF) evenly distributes the available resources of each node to each task based on resource availability and where services are most needed.

In our WDRF algorithm, there are three main steps:

1. **Filter:** For each resource provider, eligible node instances are filtered according to the specification of the APP resource request. These specifications include definitions of CPU, memory, disk, bandwidth, GPU and so on.

2. **Prioritize:** The final node instance is selected using the weighted sum of the node instance's price score and the resource provider's reputation score. If the node instance is low-cost, it will have a higher price score. The resource provider's reputation score is calculated by the proportion of idle resources, number of resource allocation tasks that have been scheduled, rating score, system stability, and current running status.

Algorithm Filter & Prioritize

$x_{i,j,k}$	The k parameter of node instance j belongs to resource provider i
D	Node instances set of resource providers
w_0	Weight of node instance price
$w_{i,m}$	Weight of node reputation index m of resource provider i
$z_{i,m}$	Value of node reputation index m of resource provider i
y_k	Value of kth parameters of resource requirements
N_i	Node instance of provider i which satisfies resource requirements
$p_{i,j}$	Price of node instance j of resource provider i
$p(x)$	Price of node instances x

$$max\ z = w_0 * (\frac{1}{log(p_{i,j})}) + \sum_{m=1}^{M} w_{i,m} * z_{i,m}\ x(i,j) \in D$$

$$s.t. N_i = \{x_{i,j} : x_{i,j,k} \geq y_k\ i = 1,2,...,ii; j = 1,2,...,jj\}$$

$$p_{i,j} = \{min\ p(x), x \in N_i, i = 1,2,...,ii\}$$

$$w_{i,m} \geq 0\ i = 1,2,...,ii; m = 1,2,...,M$$

3. **WDRFSche Algorithm:** Our WDRFSche algorithm is adopted for resource-request task scheduling for each resource provider. The allocation for each user will be determined by the user's dominant share, which is the maximum share that the user has been allocated of any resource. In addition, each user is associated with a weight vector, which is used to allocate more resources to those users who are running high-importance jobs or who have a high reputation score. The next application task of user with the lowest dominant share will be picked to run, and resources will be allocated to the application task.

WDRFSche Algorithm Pseudocode

$R =< r_1, ..., r_m >$ //total resource capacities of resource provider

$C =< c_1, ..., c_m >$ //consumed resources,initially 0

$s_i (i = 1...n)$ //user i's dominant shares,initially 0

$w_i (i = 1...n)$ //user i's task weight calculated by user reputation,initially 1

$U_i =< u_{i,1}, ..., u_{i,m} > (i = 1...n)$ //resource given to user i, initially 0

pick user i with lowest dominant share s_i

$D_i \leftarrow$ demand of user i's next task

if $C + D < R$ then

$C = C + D$ //update consumed vector

$U_i = U_i + D_i$ //update i's allocation vector

$s_i = max_{j=1}^{m} \{u_{i,j}/r_j\}/w_i$ //calculate user i's dominant share

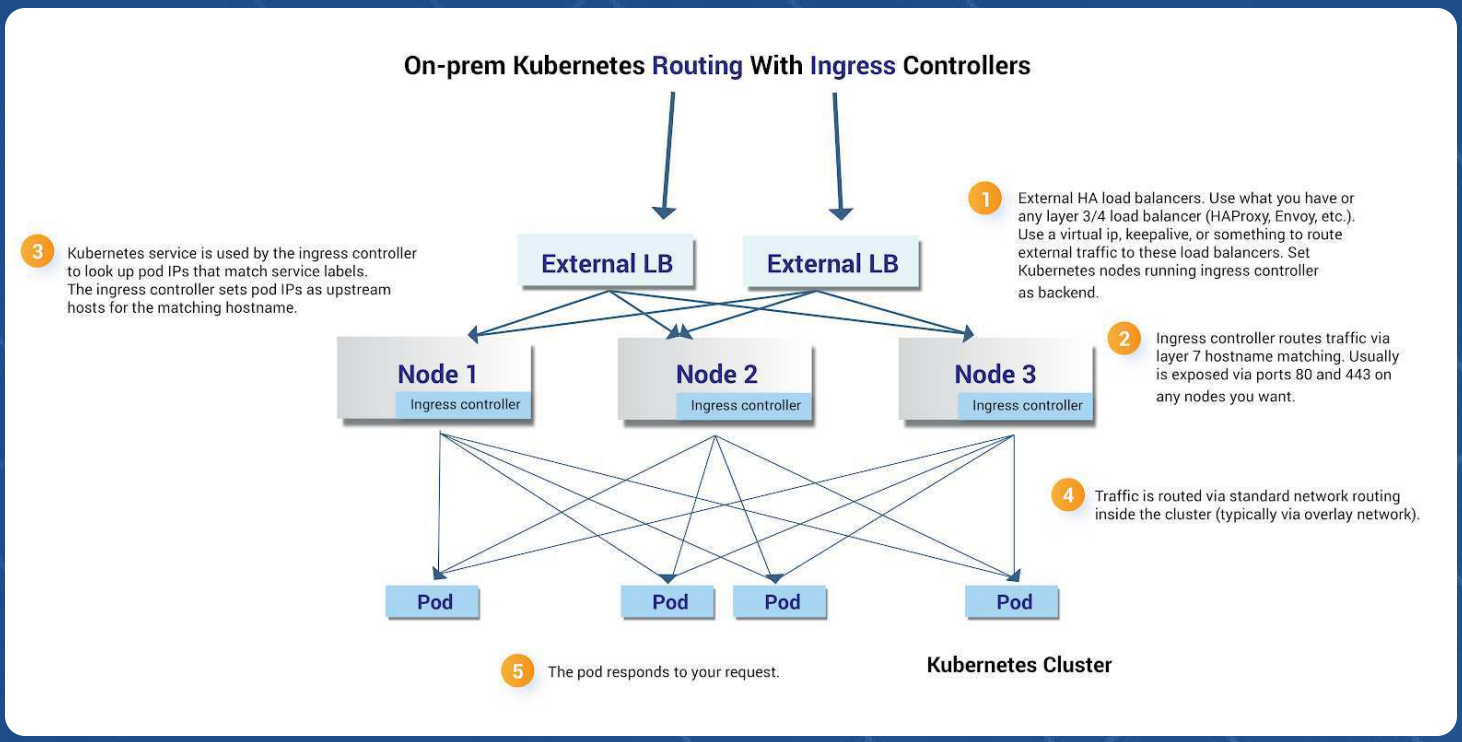
else

return //the resource provider is full

end if

Adoption of Data Center Computing Power

By leveraging the power of Kubernetes, a container orchestration system, Ankr facilitates the deployment and management of client software across entire data centers. Ankr applies Kubernetes to share resources and initiate the deployment of software services depending on hardware conditions. The following workflow shows how Ankr uses highly-available clusters and tools like Kubespray, Kubeadm, Kops, Ansible, and Terraform to adopt the idle cloud computing power of underutilized data centers.



For data centers with dynamic public IP resources, Ankr can provide an external load balancer. This allows the data center to offer load balancing as a service to users and, in turn, increase revenue.

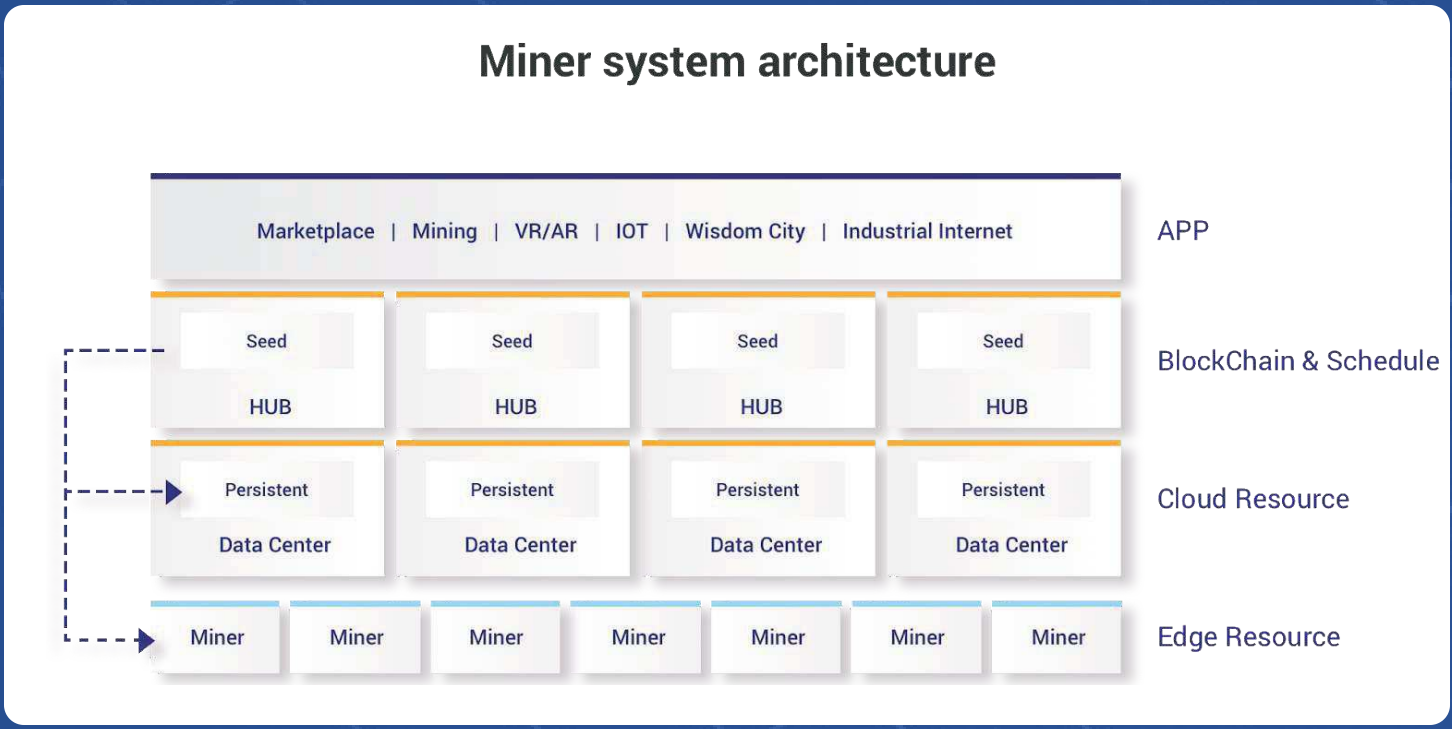
For data centers without public IP resources, Ankr requires only a single virtual IP, which it can use to route all cluster traffic through an Ingress controller. If the data center is able to provide each target server with at least one public IP address, Ankr can utilize an external DNS to resolve the host address with an Ingress controller. This is the configuration used in the Lotte Data Communication case study below.

For data centers that can provide the target server, host the application pod, and provide service through Ingress or a load balancer after an endpoint service has been set up, Ankr will provide a TLS certificate manager for the secure connection.

Edge Node Design

In our blockchain network, there are three types of nodes, including:

- **Seed Peer:** Generates new blocks, and is deployed in Ankr Hub.
- **Persistent Peer:** Synchronize blockchain, and is deployed in data center.
- **Access Peer (or Ankr Miner):** Access Persistent Peer and report the workload. Ankr Miner also provides computing services as an additional edge computing node to the data center.



Since the mining equipment is also used for resource sharing and calculation, the graphics card mining machines with CPU, disk, and memory are selected to deploy.

With the ever-growing development of 5G technology, the modern network has much higher bandwidth and much lower latency. This allows for the implementation of a variety of real-time coordination applications using Ankr Miner, such as IoT, machine learning, distributed storage systems, and VR/AR.

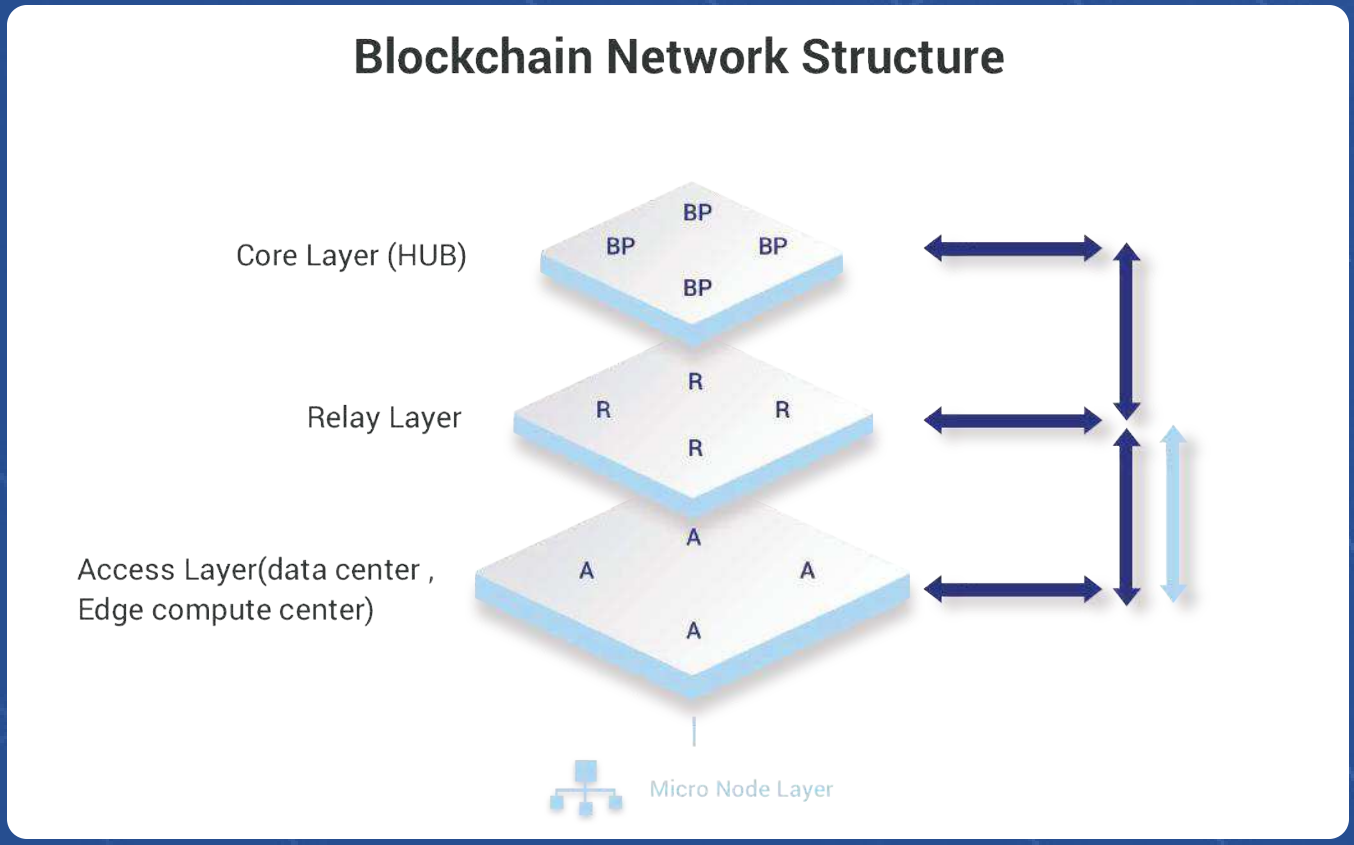
03 Ankr DCCN Blockchain

Ankr's shared cloud economy uses blockchain for metering, international micro-payments, and smart-contract-based service level agreements (SLA). To keep track of all of these moving parts, all usage data and transaction data are recorded in the blocks. This allows organizations to easily verify their records, prevent backtracking and manipulation, and establish a user account reputation system.

Ankr blockchain is a public chain aimed at DCCNs. The blockchain's network is multi-layered, expandable, and freely organizable.

The Ankr blockchain also features a smart contract system, which supports multiple programming languages such as C/C++, JavaScript, Rust, Python, and more.

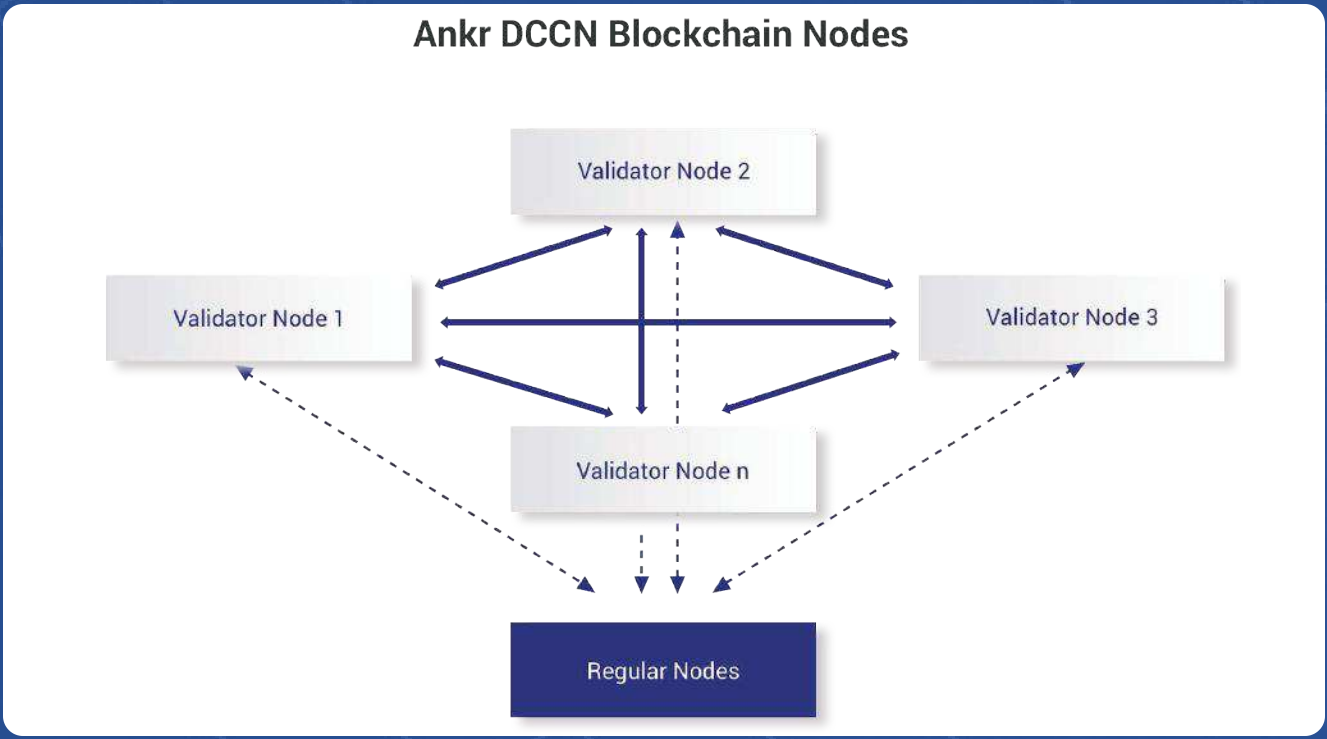
Blockchain Network Structure



Ankr's blockchain network is divided into four layers:

1. **Core Layer:** This is the core consensus layer. Here, all nodes are full nodes on the layer. The consensus calculation this layer uses is the Proof of Service Level and Stake Byzantine Fault Tolerance (SLSBFT), which defines the service quality of bandwidth, computation, and storing in the distributed cloud computing service market. Within this layer, blocks will be produced until a consensus is reached by the Block Producer (BP) nodes.

From the user's point of view, the core layer consists of validator nodes and regular nodes. The validator nodes are currently being approved by Ankr DCCN, and will be voted on by the community in the future. The regular nodes are open to the public.

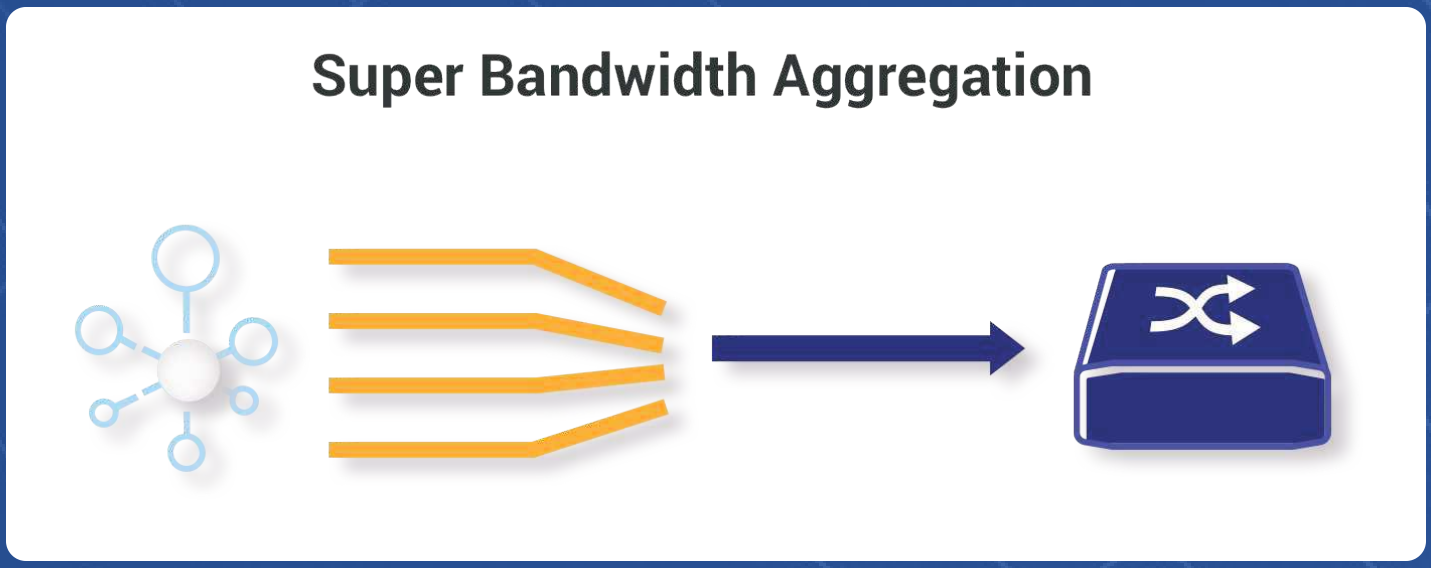


2. **Relay Layer:** The relay layer is for fast network routing. All nodes in this layer are also full nodes, but they will not produce blocks or take part in the consensus. Users have the ability to add a better network on top of the layer, and they can earn an ANKR coin reward based on proof of a network contribution (PNC). The PNC calculation is based on the node's relayed packet number, network steadiness, network bandwidth, and the node's quality of service.

3. **Access Layer:** The access layer contains data center nodes, mining nodes, and edge computing nodes. All of these are light nodes and can control illegal node access.

4. **Micro-Node Layer:** The micro-node layer contains device nodes and some transaction hashes. If a micro-node needs to retrieve network proof, it will ask the access-layer node. If the access-layer node can't provide a proof, the request will pass through the relay layer to the core layer.

The provider of the network, the computation, and the store will provide proof periodically to the access layer. The access layer will then verify the proof, and the result will be passed to the core layer. If the proofs are verified, the resource provider's service level will be increased, which in turn increases the probability that the provider will be elected as a BP node.



Using supernetting technology, Ankr's blockchain network can aggregate the idle network and produce more bandwidth, thus providing better service. To do this, a supernetwork IP is formed by routing two or more networks into a larger network. The new routing prefix for the combined network represents each constituent network as a single routing table entry. This process is often referred to as "supernetting," but is also known as "prefix aggregation," "route aggregation," or "route summarization."

Expandable and Freely Organizable Network

The Ankr blockchain network imports distributed sloppy hash tables based on the traditional Kademlia DHT.

The node can retrieve physical neighbor nodes, allowing packets to be transmitted faster and more nodes to join the Ankr blockchain network.

Ankr has also expanded network organization by using the tag model, in which nodes with the same tag are clustered into the network organization.

High Security

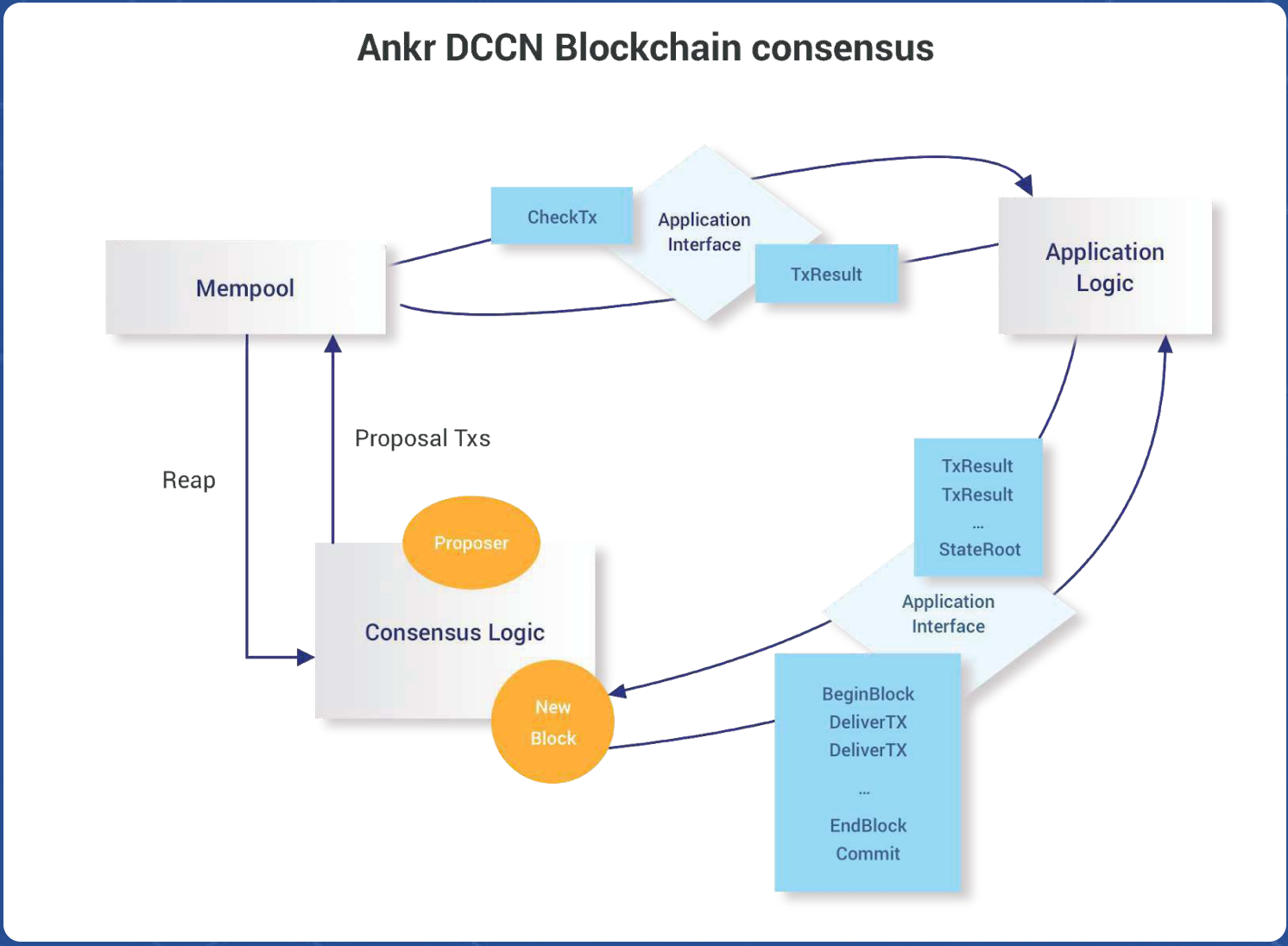
Using a Proof of Work (POW) node ID generation calculation, Ankr's blockchain network avoids Eclipse and Sybil attacks. The blockchain network also avoids hostile routing attacks by using disjoint path-finding algorithms.

Consensus

Ankr's blockchain consensus is called Proof of Service Level and Stake Byzantine Fault Tolerance (SLSBFT). For verification, the consensus also has three phrases:

1. Propose
2. Prevote
3. Pre-commit

Ankr's blockchain consensus sequence can be visualized in the following diagram.



The difference between SLSBFT consensus and standard BFT is the BP node election. BP node election is based on service level and stake, such that if a user has a specific ANKR token, they can take part in the BP node election.

The user's service level is calculated by the DCCN resource provider's Quality of Service (QOS) and the resource consumer's credit. The first step for all satisfied account nodes is to become a candidate node.

For security, all of the validator nodes are randomly selected from a pool of candidate nodes. During each cycle, the proposal node is randomly selected from all validator nodes.

Smart Contract

The history of smart contracts begins in the 1990s, when they were first invented by computer scientist Nick Szabo.

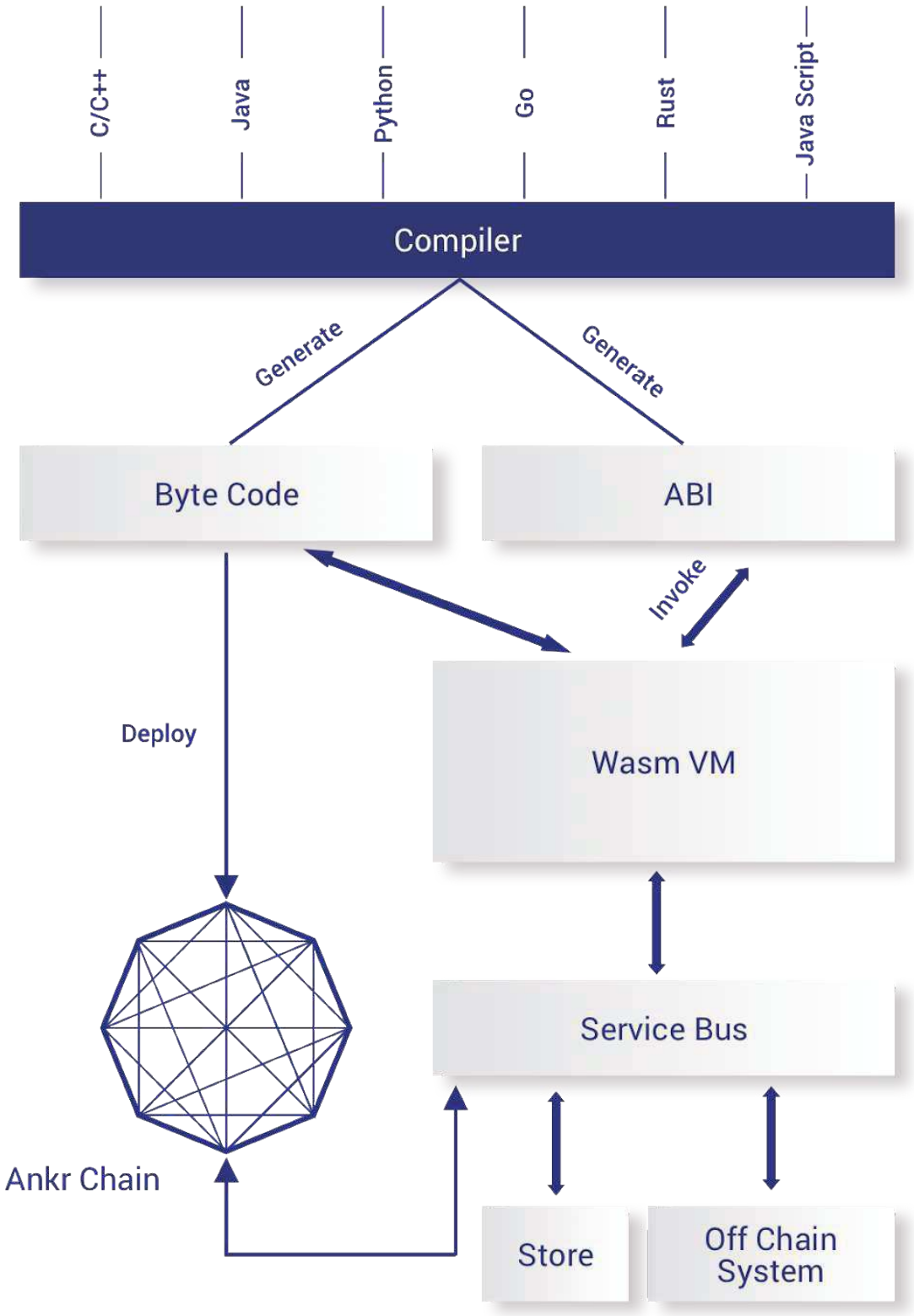
Smart contracts are "self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code." (Investopedia)

Although smart contracts aren't born from blockchain, they can provide a convenient way to automate blockchain further.

Smart contracts are not only executable computer programs, but also active participants in the blockchain system. They can receive, store, and reply to received messages, as well as make the message and its value external.

The diagram below is a visualization of how smart contracts work in Ankr's blockchain.

Ankr Smart Contracts System Architecture



Ankr's smart contract blockchain system is characterized by the following traits:

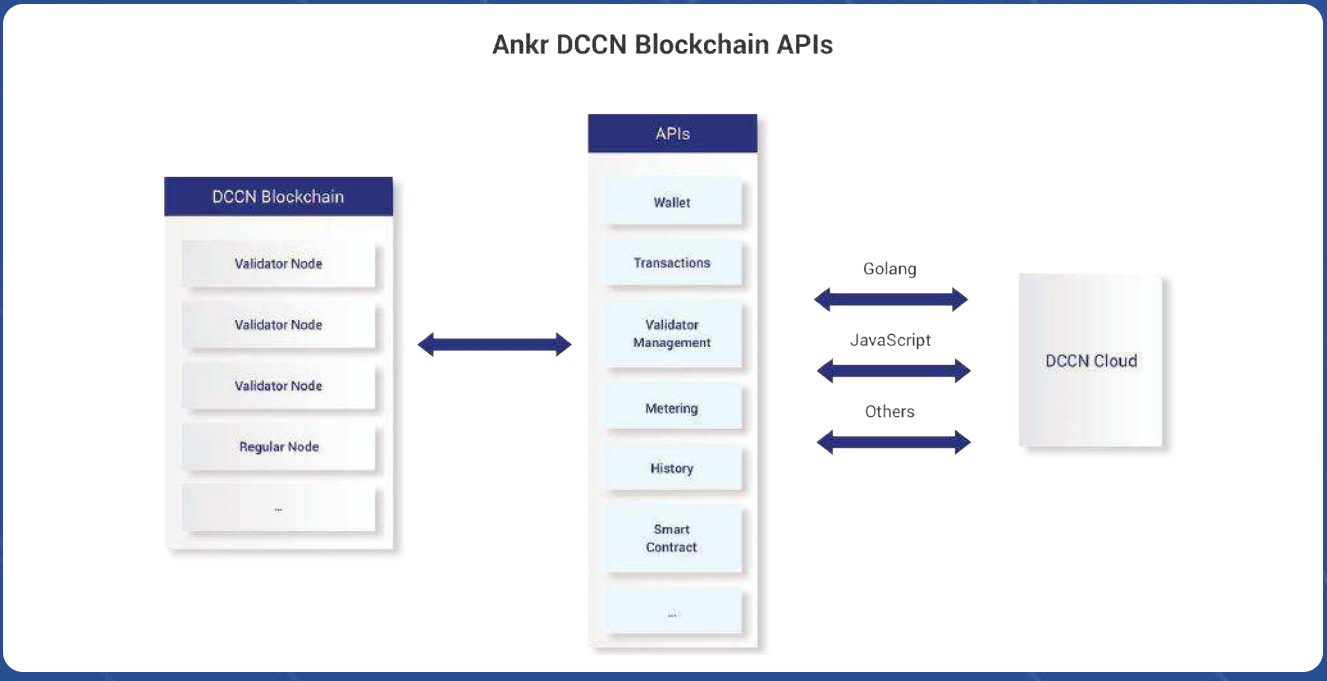
- It supports multiple programming languages, such as C/C++, JavaScript, Rust, Python, and more.
- The virtual machine (VM) of the smart contract complies with WebAssembly 1.0.
- During the execution of smart contracts, Ankr's blockchain can invoke the contracts API via a service bus.
- In the smart contract development tool, the responding language's IDE plugin will be supported.Ankr's blockchain will charge transaction fees based on the smart contract instructions.
- It supports the smart contract's communication with Ankr blockchain.It supports the smart contract's direct communication with the off chain system. For example, the DCCN's edge node.

Incorporation with DCCN

The Ankr DCCN blockchain serves Ankr's DCCN in several ways, including:

- It provides the payment interface for cloud users and providers.It rewards resource providers and computing users when they successfully finish their computing tasks.
- It rewards validators when they help maintain the blockchain and handle transactions.
- It provides smart contract functionality.
- The relay network secures communication between DCCN hub and DCCN daemon.
- The resource provider can provide proof to Ankr DCCN blockchain, and the Ankr DCCN blockchain can verify it.

In addition, the Ankr blockchain provides APIs to DCCN services and frontends. These APIs include wallets, transactions, history, validator management, metering, and smart contracts.



04 Operating Model

Stakeholders and Incentive Mechanism

There are four stakeholders in the circulation ecosystem.

On the supply side, there are Enterprise-Grade Data Center Providers and Edge Node Owners.

On the demand side, there are Infrastructure Consumers and Application End Users.

These stakeholders can be defined as follows:

Enterprise-Grade Data Center Providers: Ankr's open marketplace enables providers to sell surplus cloud computing power, allowing them to monetize their depreciating assets. These providers can be colocation data centers (e.g. NTT), on-site server clusters (e.g. Intuit) and public cloud providers (e.g. Amazon Web Services, DigitalOcean).

Edge Node Owners: Anyone can purchase an Ankr-manufactured edge mini-server. These edge nodes should have a DCCN hub and daemon pre-installed in order to share resources, monitor status, and earn rewards. These hardware devices must be purchased. Ankr will announce the price of these devices in the very near future.

Infrastructure Consumers: Ankr's open marketplace allows for a dynamic pricing model when it comes to infrastructure cost. This provides the market with an equilibrium to match the supply and demand.

Application End Users: Users select applications through the marketplace and run APP tasks through data centers and edge nodes.

Ankr's staking mechanism ensures individuals within the ecosystem act honestly and with integrity. To do this, the Ankr provides a monetary incentive to individuals that participate in the network and have a good reputation. The risk of fraudulent behavior is highest when new, unknown providers join our network. Still, rather than requiring a centralized or federated approval process for new accounts, Ankr allows anyone to join.

When a new edge node owner (miner) chooses to offer their resources to the network, they are not immediately approved. First, they must stake a meaningful value on the network in the form of ANKR tokens.

There is no minimum stake amount, but participation in Ankr's network is proportional to the provider's stake, and is thus a fraction of the sum of all stakes. Additionally, stake contribution is factored into the provider's reputation score. Tenants may use this score as a deployment criterion, as the score of the edge node provider will be visible.

In order to promote the healthy development of the Ankr cloud computing platform and to provide customers with high-quality services, an advanced incentive mechanism is provided to all relevant participants in the ecosystem.

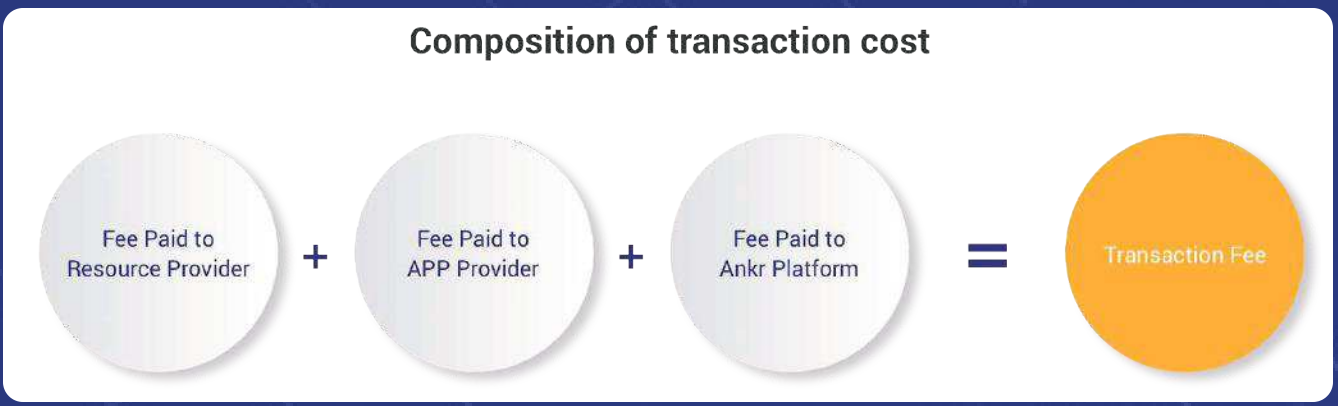
Rewards for participants are calculated using several factors, including:

- Rewards for Ankr stakeholding
- Rewards for Ankr stake consumption (ANKR tokens)
- Rewards for resources and services provision
- Rewards for reputation

Reward Calculation Formula	
w_i weights of rewards p_i factors of rewards $Rewards = \sum w_i * p_i \; i = 0...3$ //total rewards of platform participants	
$w_0 = 0.00005$	weight of Ankr stake holding, e.g. holding 10w ankr token, get 50 Ankr token/day
p_0	the amount of Ankr stake holding,calculated daily
$w_1 = 0.002$	weight of Ankr stake consumption, e.g. consumed 1w ankr token, get 20 Ankr token
p_1	the amount of Ankr stake consumption,calculated on each transaction
$w_2 = 0.002$	weight of resources and services provision
p_2	the amount of resources and services provision, represented by earned fee
$w_3 = 100$	weight of reputation, e.g. participant with 0.5 reputation get 50 Ankr token/month
$0 \le p_3 \le 1$	reputation score,calculated monthly

Ankr Platform Revenue Model

Ankr charges some percent (e.g. 5 percent) of every deal. This fee is made up of three parts: a fee paid to the resource provider, a fee paid to the Application provider, and a fee paid to Ankr.



Financial Incentive to Reward Demand

The demand of service are encouraged to make full use of our platform. Reward tokens are paid according to consumption history and stake-holding records.

SN	Parameters	w_i	p_i	Calculation Period
$score = \Sigma w_i \star p_i \; i = 1...7$				
1	PayFee	0.002	Transaction fee	Every transaction
2	CompletedDeals	10	Number of deals completed	Every transaction
3	InvitationNum	100	Number of guests invited	Individual invitation
4	OnlineTime	0.0001	Time spent online (s)	Login to logout
5	RatingTimes	50	Number of user evaluations	Each evaluation
6	StakeHolding	0.00005	Stake holding	Every day
7	Reputation	100	The weighted sum of TotalPayFee, TotalCompletedDeals, CompletedDealsRatio, ServiceLevel, RatingScore	Every month
8	TotalPayFee	0.4	$p_t = \psi * (log_{10}^{p}/1000) + (1-\psi)p_{t-1}$	/
9	TotalCompletedDeals	0.2	$p_t = \psi * (log_{10}^{p}/1000) + (1-\psi)p_{t-1}$	/
10	CompletedDeals Ratio	0.2	Ratio of completed deals to all deals	/
11	ServiceLevel	0.1	p/p_{max}	/
12	RatingScore	0.1	$p/100$	/

Financial Incentive to Reward Application Supply

Application suppliers are encouraged to continue providing high-quality applications. Reward tokens are paid to them according to completed deals, rating score, earned fees, stake holding records, etc.

SN	Parameters	w_i	p_i	Calculation Period
$score = \Sigma w_i \star p_i \; i = 1...6$				
1	EarnedFee	0.002	Earned Fee	Every transaction
2	CompletedDeals	10	Number of deals completed	Every transaction
3	InvitationNum	100	Number of guests Invited	Individual invitation
4	RatingTimes	50	Number of provider evaluations	Each evaluation
5	StakeHolding	0.00005	Stake holding	Every day
6	Reputation	100	The weighted sum of TotalEarnedFee, TotalCompletedDeals, CompletedDealsRatio, ServiceLevel, RatingScore.	Every month
7	TotalEarnedFee	0.4	$p_t = \psi * (log_{10}^{p}/1000) + (1-\psi)p_{t-1}$	/
8	TotalCompletedDeals	0.2	$p_t = \psi * (log_{10}^{p}/1000) + (1-\psi)p_{t-1}$	/
9	CompletedDeals Ratio	0.2	Ratio of completed deals to all deals	/
10	ServiceLevel	0.1	p/p_{max}	/
11	RatingScore	0.1	$p/100$	/

Financial Incentive to Reward Resource Supply

Resource providers are encouraged to provide more abundant and appropriate resources. Reward tokens are paid to them according to completed deals, reputation, earned fees, stake holding records etc.

SN	Parameters	w_i	p_i	Calculation Period
$score = \Sigma w_i * p_i \; i = 1...5$				
1	EarnedFee	0.002	Earned Fee	Every transaction
2	CompletedDeals	10	Number of deals completed	Every
				transaction
3	RatingTimes	50	Number of providers evaluations	Each evaluation
4	StakeHolding	0.00005	Stake holding	Every day
5	Reputation	100	The weighted sum of TotalEarnedFee, TotalCompletedDeals, CompletedDealsRatio, ServiceLevel, RatingScore	Every month
6	TotalPayFee	0.4	$p_i = \psi * (log_{10}^{p}/1000) + (1-\psi)p_{i-1}$	/
7	TotalCompletedDeals	0.2	$p_i = \psi * (log_{10}^{p}/1000) + (1-\psi)p_{i-1}$	/
8	CompletedDeals Ratio	0.2	Ratio of completed deals to all deals	/
9	ServiceLevel	0.1	p/p_{max}	/
10	RatingScore	0.1	$p/100$	/

05 DCCN Security Guidelines

The Ankr Cloud is a decentralized network platform for provisioning and scaling cloud workloads at the highest security standards. Confidentiality, integrity, and availability are the Ankr team's highest concerns, and Ankr has taken measures to maintain the highest level of security for its providers and consumers.

Security Principles

Immune to Malicious Software

As an infrastructure, Ankr Cloud has no control over software running on it, but Ankr Cloud can minimize any damage through strategies such as damage to itself (if a user damages their own space, they will not affect their neighbor), stake penalty (if a user doesn't behave, their stakes will be affected), and application signatures.

Trust Level and Security Level

Ankr Cloud has varying trust levels for different applications. For example, publicly-known and long-tested applications have higher trust levels. Custom software normally has a lower trust level. For sensitive applications, the consumer can choose a higher security level, and Ankr Cloud will use the highest standard of security measures.

Minimal Customer Responsibility

In a regular cloud platform, responsibility for security is shared by both parties. In Ankr Cloud, customers have a lower risk of danger than in other platforms, since Ankr Cloud has systems in place to automate security operations for customers.

No Single Point of Failure

If any component fails, it will not stop the entire system from working.

Authentication and Authorization

Strong authentication and authorization is used everywhere in Ankr cloud.

High Level Encryption for Storage

High level encryption standard is used for Ankr cloud storage.

High Level Encryption for Data Transmission

The high-level encryption standard is used for Ankr cloud data transmission.

Role and Services

Access control is applied to role level and service level.

Fault-Tolerant

The Ankr Cloud will continue operating properly in the event that some of its components fail.

Development Principles

Throughout every step of software development, Ankr's CircleCI CI/CD process has considered, implemented and tested potential security requirements, security review, threat modeling, risk assessment, and static code analysis.

Security Boundary

Ankr Cloud has components such as Ankr Daemons, Ankr Hubs, and CLI/GUI clients. Each component communicates to each other via encrypted traffic, and each component defines its own security boundary.

Ankr Daemons, especially, can co-exist with old applications, servers, and networks within the data center. Ankr also uses segregation to separate the Ankr Cloud from the old network.

Compliance Program

To maintain security and data protection in Ankr Cloud, the infrastructure of Ankr Cloud adheres to security best practices and security standards, including compliance with FIPS 140-2 security standard. Ankr is actively working on implementing FIPS 140-2 certification, which will be introduced in the near future.

Hardware and Environnment Security

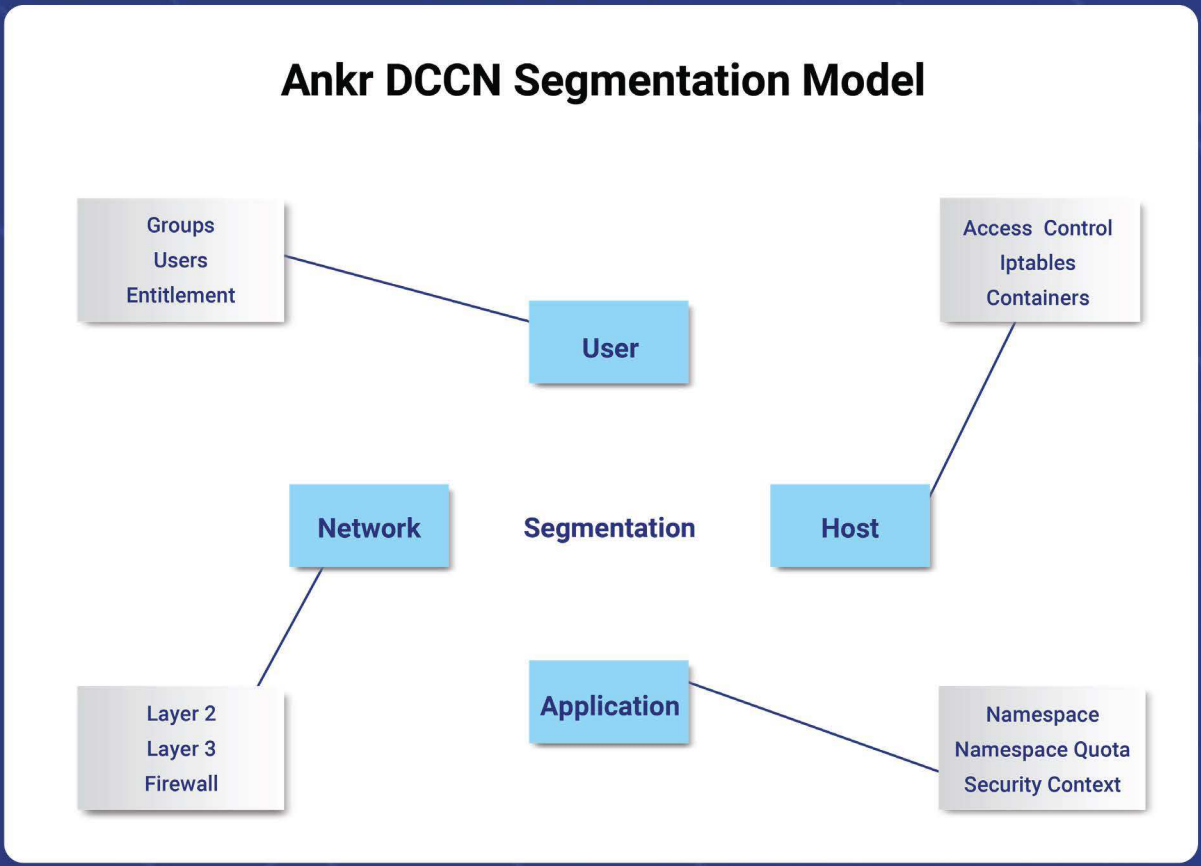
Typically, Ankr Cloud would have no control over the hardware and data center environment. However, Ankr is working to ensure each host machine meets security standards and is segregated from the networks that are not part of Ankr Cloud.

Ankr can tolerate hardware and data center failures with minimal impact. Important applications will be re-deployed in different data centers, and Ankr will maintain sufficient capacity for these applications to be fully re-scheduled at other data centers.

Network Segregation

The Ankr Cloud supports almost all kinds of data centers and uses different methods to segregate itself from the data center network.

Because Ankr Cloud is using the idle computing power of data centers, Ankr Cloud is typically only part of the data center network.



Application-Level Segregation

In Ankr Cloud, an application is run under a single cluster namespace with no access to other cluster namespaces. Clusters have their own private IP ranges and will never conflict with other networks.

Host-Level Segregation

By default, the host can gain access to both internal networks and public networks. Ankr Cloud uses IPtables to disable either the data center network from visiting Ankr Cloud, or Ankr Cloud from visiting the data center network.

Strict Access to Host

Applications run on Ankr Cloud are in a virtual application layer and will therefore never visit the host machine directly. The admin must explicitly request access with the Ankr authorization system to perform this action.

Layer2 Segregation

The network can assign a unique VLAN for the cloud network.

Layer3 Segregation

The network can assign a unique IP range for the cloud network.

Firewall Segregation

A firewall restricts ingress/egress for the Ankr Cloud network.

Hypervisor Layer Segregation

Ankr Cloud supports functionality of hypervisors like VMware ESX/NSX to segregate the network.

Other Tools

Illumio micro-segmentation can be used together with Ankr Cloud.

Internal Segregation

- Cross-cluster communication is prevented by Ankr Cloud platform.
- Cross-namespace communication is prevented by Ankr Cloud platform.
- Network Special Interest Group (SIG) is used for pod-to-pod communication policies, which can create access control rules to limit network access around pods, no matter if it's a flat sharing network or an overly network. For example, a rule can allow only front-end pods access to the gateway pod.
- Resources in one namespace are invisible to other namespaces.
- Authorization policies can segregate access to namespace resources between users.
- Namespace quotes are defined to limit resource usage and avoid "noisy neighbor" scenarios.
- Ankr's security context is used for pod, containers, and volumes. It can control capabilities for containers and other security parameters.

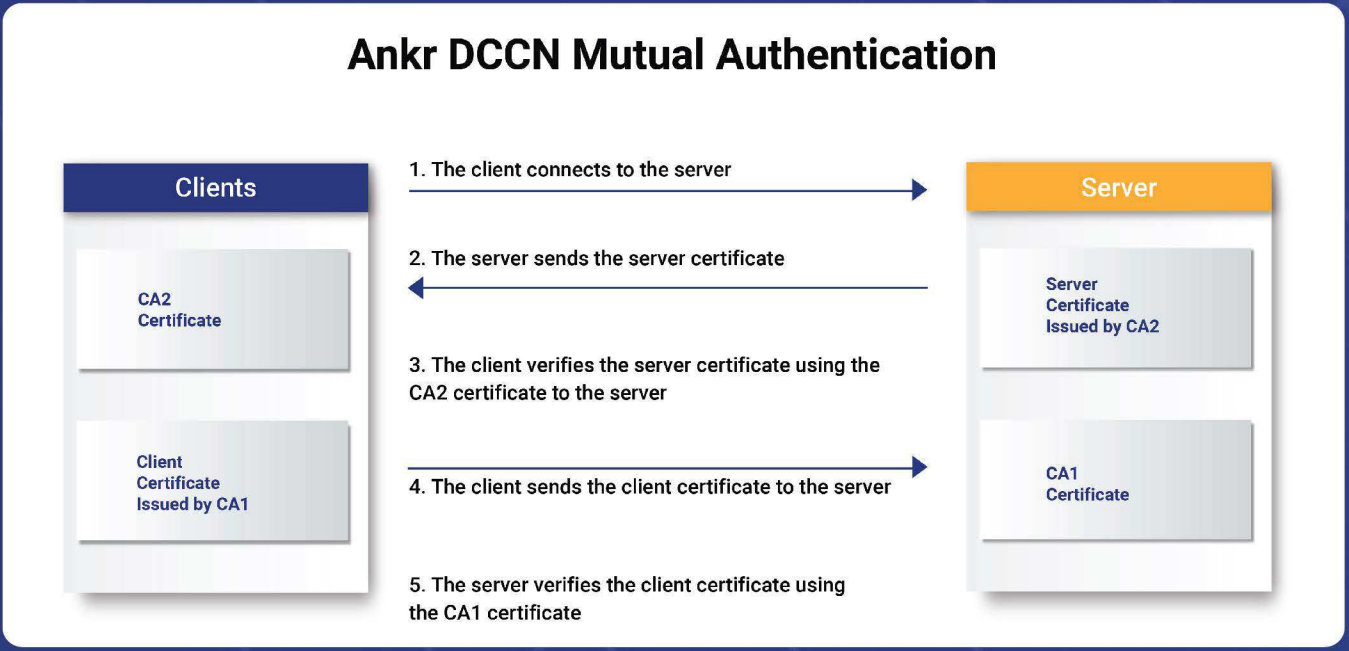
Authentication

User Authentication

Ankr uses multi-factor authentication. Users have to present at least two pieces of evidence to the authentication server in order to gain access. These pieces of evidence can be a username/password, a cell phone text, or Google authentication.

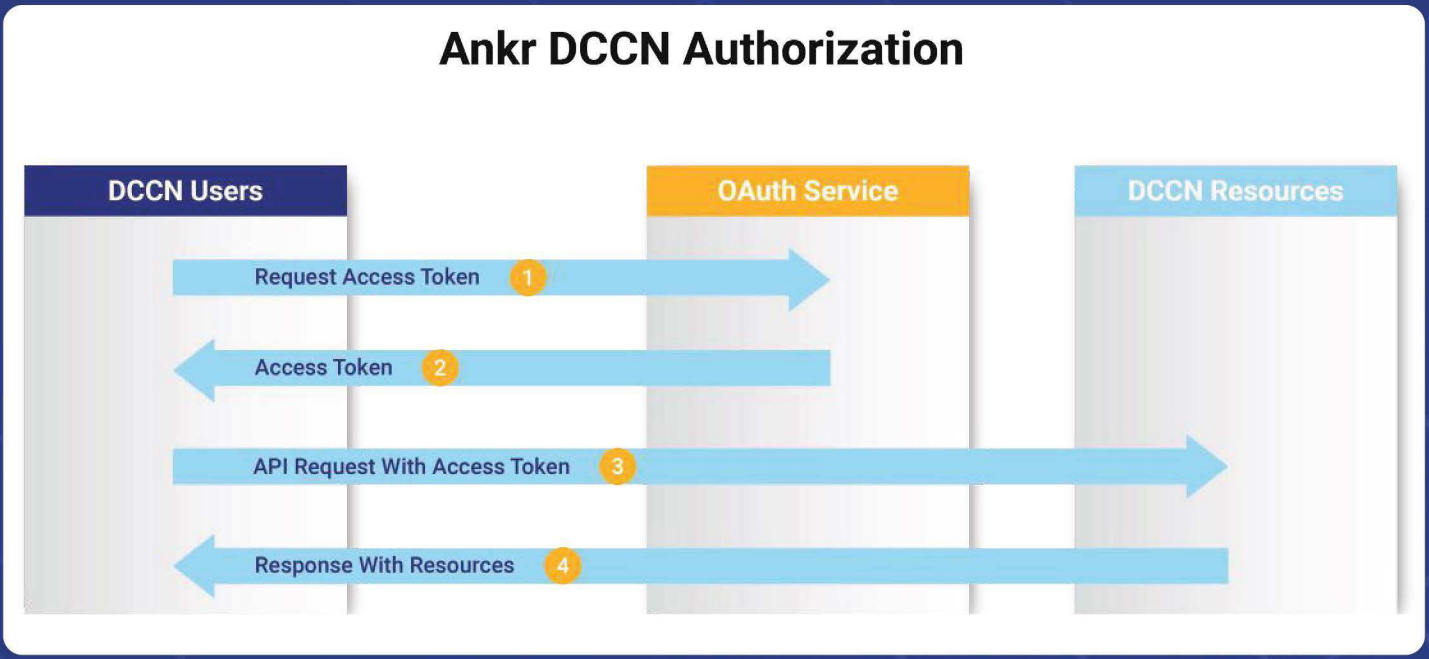
Communication Authentication

When a user talks to a server, Ankr supports one-way and two-way authentication. For a higher level of security, two-way authentication is required. As such, the client certificate is necessary. Ankr's authentication includes RSA and ECDSA algorithms. RSA is at least 2048-bit security strength, and in ECDSA, 256-bit EC curve is the minimum.



Authorization

Ankr Cloud uses OAuth-2 to grant applications access to resources on the behalf of the resource owner. Without sharing credentials, the resource owner can authorize third-party access to their resources.



Roles and Users

The Ankr Cloud supports four different roles:

1. Administrator
2. Operator
3. Regular User
4. Monitor User

Ankr Cloud enforces the separation of roles using identity authentication.

Login Methods

To log in, a user must create a username and password. The user's password must consist of:

- At least 8 characters, up to 32 characters
- At least 1 uppercase character
- At least 1 lowercase character
- At least 1 special character

A randomly generated password complies with the FIPS 140-2 requirement of 1 in 1,000,000.The module also locks out the user for 60 seconds after 5 incorrect attempts. The user will be frozen for one hour after 15 incorrect attempts.

Admin SSH Login

An admin user needs a private key to log in to the server. Currently, we use a RSA 2048-bit (or higher) private key for this purpose.

Key Management

Critical Security Parameters

- User password
- Wallet private keys
- SSH certs
- ERC20 private keys
- Datastorer

Service	Algorithms
User password	HMAC-SHA256
Wallet private keys	ED25519
SSH certs	RSA 2048-bit and over ECDSA 256-bit and over
ERC20 private keys	ECDSA secp256k1
Local Data Encryption	AES-256-GCM
Data Traffic	ECDHE-ECDSA, ECDHE-RSA
Datastore	HMAC-SHA256

Key Zeroization

After a key is deleted or reaches the end of its cycle, key zeroization ensures that the key cannot be recovered or reused, even if the key was in encryption or hash mode.

Payment Security

Private Keys

In Ankr DCCN, the native ANKR tokens can be used for payment. Ankr has two kinds of tokens: ERC20 tokens and native tokens, which are in 1-to-1 relationship. In total, the circulation is 10 billion, as announced publicly.

The ERC20 token is maintained in the Ethereum blockchain, and users' private keys are kept by users themselves.

Ankr will never ask for private keys from users. If a user uses exchanges (e.g. Bittrex, Huobi, etc.), the exchanges will manage private keys for users.

Ankr will not manage private keys for users. The key generation algorithm is ED25519, which is a public algorithm, and users can generate keys and addresses without the help of Ankr.

When users need to transfer tokens or make payments, a private key is needed to sign the transaction, but the private key will never be revealed to Ankr. Also, private keys will never be transmitted in any network or Internet.

Blockchain

Ankr's blockchain follows the nature of regular blockchain, and uses consensus protocol to make decisions for each block.

Traffic can be encrypted optionally, because blockchain is already used for untrusted networks. Illegal information will be removed by consensus protocol.

Like Bitcoin, Tor can be used together with Ankr blockchain if the user is very cautious about privacy.

Ankr performs regular planned attacks on its blockchain as part of its penetration test to ensure the usability and stablity.

Monitoring and Auditing

The Ankr Cloud is carefully monitored by an automated monitoring system that detects unusual or unauthorized activities. Metric thresholds can be set for unusual activities.

Alarms and warnings are configured to notify operations and users, and Ankr Cloud GUI has configuration and events for this purpose.

06 Conclusion

In recent years, the use of public clouds for computing power has not only grown, it has become the norm. With this change of the status quo, organizations have found alternative ways to power their systems, while the powerful mainframes, data centers, and private clouds go unused or underutilized.

Ankr is creating a new future with its shared cloud economy–one that balances a demand for cloud computing power and a surplus of untapped, globally-distributed data.

Between Ankr's cloud, blockchain, token economy, and state-of-the-art security protocols, organizations now have a way to utilize idle computing power, a function that benefits both the organization and the owner of the computing power. No longer do organizations need to agree to financially disadvantageous contracts with service providers, and data centers can finally make use of under-used servers, increasing revenue along the way. The applications of Ankr's technology are infinite, and we anticipate an operations revolution to take place once the smartest minds in technology get hold of Ankr and learn to leverage its shared cloud economy to their benefit.

We believe Ankr's progressive technology will change the landscape of cloud sharing in the modern technological age.