VANTA : INFINITY Connect

Decentralized Network for Real-time, Secure, and Private Connectivity

White Paper v0.83
Last updated May 27, 2019

1. VANTA

1.1 What is VANTA?

VANTA is an intelligent network for transmission and processing of real-time data which enables individuals and companies to develop applications without additional infrastructure at lost cost. As a result, creative services will be provided and integrated within the VANTA ecosystem, and VANTA blockchain will be a practical blockchain that will greatly contribute to improving the daily lives of individuals and operations of enterprise businesses.

Real-time networking technology covers a wide range of areas. The technology can be used for messaging / file transfer / voice & video call development, large-scale, real-time video streaming, and transmitting & processing various real-time data collected from IoT sensors. Besides addressing these problems through the VANTA blockchain, VANTA will provide and expand enterprise-level telecommunications network solutions to businesses and enterprise customers.

Using blockchain and cryptoeconomics designed for real-time networking, VANTA creates a system in which nodes participating in the network contribute to real-time data transmission and processing without relying on traditional centralized systems and networks. This system results in a low cost, functional blockchain-based network. Anyone, regardless of existing platforms, can participate and use the network by using an API, an SDK, or modules to integrate with existing applications or platforms in use. VANTA, therefore, can easily expand the ecosystem through modules that integrate applications and platforms that require real-time networking.

1.2 Motivation

The need for this network arises from the fundamental reason that the amount of real-time data exchanged between people and devices is increasing exponentially. In addition to the number of devices connected to the Internet, the amount of data that individuals produce and consume in real-time is exploding. For instance, high-definition broadcast streaming and low latency data processing for VR & AR require efficient and low-cost solution for real-time transmission. Furthermore, as more IoT sensors become utilized in our daily lives, the industry sectors such as traffic information control, factory operation, medical devices, etc. require a real-time networking platform that may handle hundreds of thousands of data points per second without the single point of failure while reducing cost and maintaining efficiency.

1.3 Market

1.3.1 Video streaming
According to global market researcher Research and Markets, the video streaming market in 2016 was $30.29 billion USD in revenue and will double by 2021 to $70.05 billion USD. Cisco also predicts online video to account for 82% of internet traffic by 2022. In particular, the “real-time” video

streaming market provided by Facebook Live, Twitter's sports broadcasting services and video broadcasting services such as YouTube and Hulu, accounted for only 3% of internet video traffic in 2017, but is expected to grow more than four-times to 13% in 2022. As a result, consumers' demand for larger bandwidth and higher quality video will increase dramatically, and the problems regarding inefficient data transfers and expensive central server usage fees will heighten significantly.

1.3.2 IoT data streaming and processing
According to Statista, a market research firm, the size of the IoT industry will grow by 24.4% annually, to $1.7 trillion USD in 2019. Gartner expects global IoT devices to grow to 20 billion by 2020, and BMI Research estimates that by 2050 at least 40 billion "things" will connect to the Internet. As such, all things are coming into the hyper-connected society that connects to the Internet; the emergence of a hyper-connected society will dramatically increase the size of the IoT market.

That is, more data will be generated in real-time by various IoT devices and individuals, and the number of corporations that want to receive such data in real-time will also increase significantly. At some point in time, storing and processing the data produced by IoT devices on a centralized server and delivering it to the users who need it will meet throughput and cost constraints. This will make the IoT sensor or its connected IoT hub more directly connected to the device that requests the data and transmits data in real-time. This means that there will be more devices connected directly to the IoT sensor or IoT hub to receive data in real-time. VANTA's real-time networking is an opportunity for intelligent networks to be integrated into IoT devices and services. VANTA will allow us to reliably and efficiently deliver the data produced by resource-limited IoT devices to more devices.

1.4 Problem and solution

VANTA will aim to solve the following problems through our decentralized intelligent network based on blockchain technology.

1.4.1 Increasing Network Throughput and Cost
Current networks and infrastructures that support various real-time networking are reaching throughput limits. This means that companies will not be able to provide reliable services, since network and server costs will increase along with the increasing amount of data transmitted. VANTA will solve the throughput and cost issues by making the common computers and mobile devices around the world, whose performance rapidly increases each year, contribute to real-time networking.

1.4.2 Real-Time Networking Development Costs and Problems with Centralized Services
Many companies are limited (or even fail) to developing real-time networking services because of the cost, time, and lack of skills required to develop and operate such services. As a result, an increasing number of companies are utilizing centralized API services that help develop real-time networking functions. Yet, there are some problems with centralized APIs. Once a centralized API is used, the fee increases significantly as the usage increases. Moreover, if an API provider suddenly changes policies, stops the API service without notice, or experiences temporary downtime, the company developing the services based on the provided API will be adversely affected. Also, because the data is stored on a centralized server, it cannot be free from hacking or privacy issues. These problems can be solved by building a decentralized network for real-time networking that is not owned or controlled by anyone, and this can be used to provide various real-time networking APIs for companies.

1.4.3 Privacy concerns resulting from transferring and storing personal data
In the future, more diverse personal data will flow within the network to be transferred between devices and will be stored in various centralized servers in order to provide a smooth service experience. However, if users cannot know whether if the data is properly encrypted, transmitted, stored, and deleted from the server, users may become anxious due to various hacks, as well as government & corporate surveillance. At the same time, personal data leakage will cause great damage. With a blockchain, however, it is possible to transparently confirm the process of transmitting / storing / deleting data. Decentralized nodes, in addition, transmit and store real-time data, which prevent hacking and excessive/malicious use of personal data

1.4.4 Access to data generated by devices and the data usage fees
In the future, there will be an increase in the need to send and receive data in real-time between people and devices and between devices. In such a situation, it is necessary to have a system that can operate transparently and accurately according to the rules determined between the devices without human intervention for acquiring the data access permission automatically, configuring the temporary network for receiving the data, and paying the price for the data use. Therefore, VANTA intends to create an efficient system that can quickly and safely send and receive data in real-time by creating a competitive system that instantly configures networks according to each situation.

1.4.5 Trust in the communication between parties and trust in the data transferred from various devices
Currently, various products, stores, and media are evaluated and shared by people. People evaluate the purchase, use, and visitation of products, stores, and media, but there is no evaluation of people or the devices people are communicating with. In the future, there will be more and more real-time communication across people and devices, and credible evaluations will be needed. Whether it is an individual engaged in daily life or a company conducting its business, trust will be achieved in the future.

2. VANTA Positioning & Competition

2.1 Positioning

Unlike the existing blockchains, VANTA is a blockchain focused on real-time communication that both traditional and decentralized applications may utilize the VANTA API to facilitate development in the areas of messaging, call, data / media streaming, etc.

Ethereum or EOS can be classified as platform blockchains while Storj or Golem can be classified as specific-purpose blockchains. Among these blockchains, VANTA is the intelligent network platform that can be classified as both platform blockchain and specific-purpose blockchain. VANTA can be positioned vertically as follows.

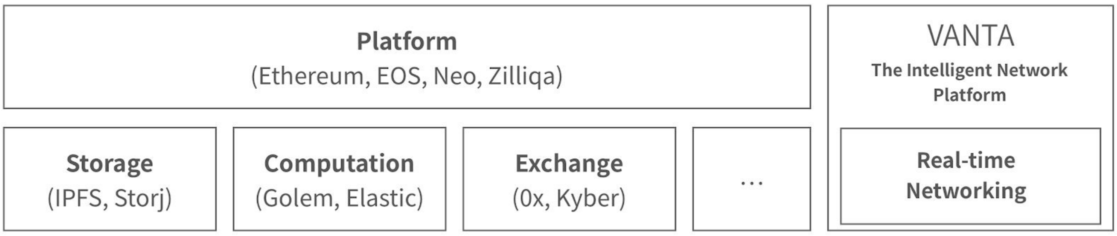

Figure 1. Project Positioning[1]

2.2 Platform & Module

VANTA will build its own ecosystem as a platform blockchain, bringing a variety of real-time networking applications and services. However, VANTA will provide a core module in the form of an SDK and/or API to provide platform-independent access to the VANTA network. Therefore, all platforms and applications that want real-time networking capability can leverage these services, leading to the rapid expansion of the VANTA ecosystem.

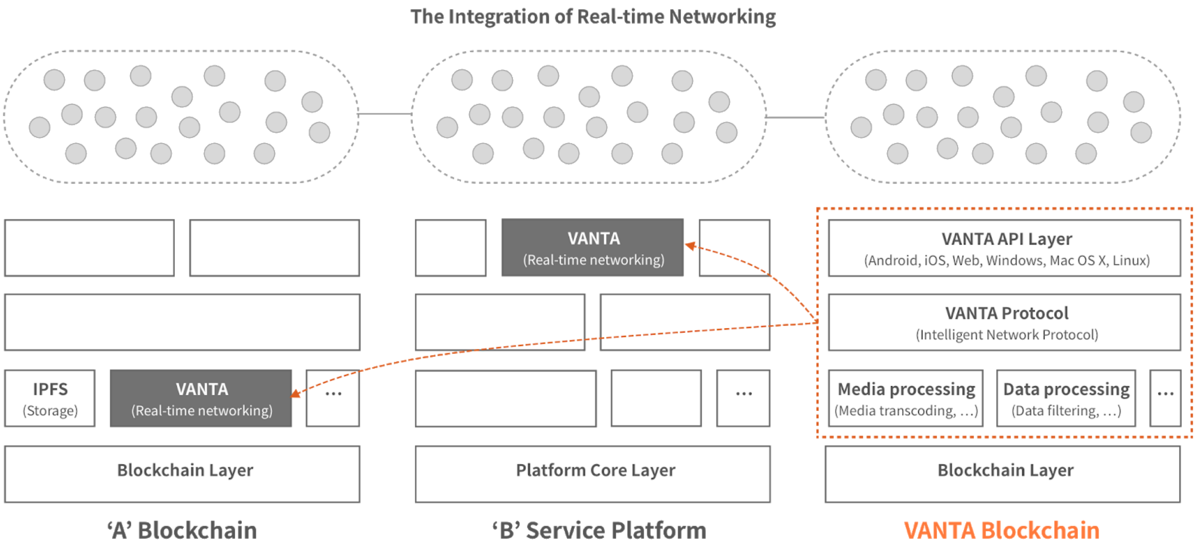

Figure 2. Expandable architecture

2.3 Benefits of using VANTA

2.3.1 VANTA-based service developers

With VANTA, it is possible to develop and operate scalable, stable, and highly secure real-time networking services at low cost. Developers can quickly and inexpensively develop real-time networking capabilities based on VANTA without building up separate server or developing real-time networking from scratch. According to the staking-based token economy, developers may utilize

[1] For descriptive purposes only. VANTA is not related or affiliated with other projects specified in this figure.

VANTA's network resources by staking VNT tokens. It is available at no cost, except for a small fee when VNT tokens are unstaked. If a developer does not have enough VNT tokens to secure the resources it needs for its service, it has the option to create a policy requiring end users to stake VNT tokens for all or a portion of its own resource usage. In other words, developers and users can share staked VNT tokens to run a service. This creates a significant reduction in the development and operational costs of real-time, networking-related services.

Compared to centralized services, services based on the decentralized VANTA network will be highly secure and stable. In addition, it is easy to integrate and combine different services because they communicate over a common standard. Even without a separate payment system, VANTA's VNT token-based payment model can be easily designed and applied to real-time networking services.

By providing those advantages for developers, VANTA can provide a development environment that helps developers build services that benefit the end user. The network can also allow more flexibility for service development to enable creative and innovative applications that are not bound to a typical business model design.

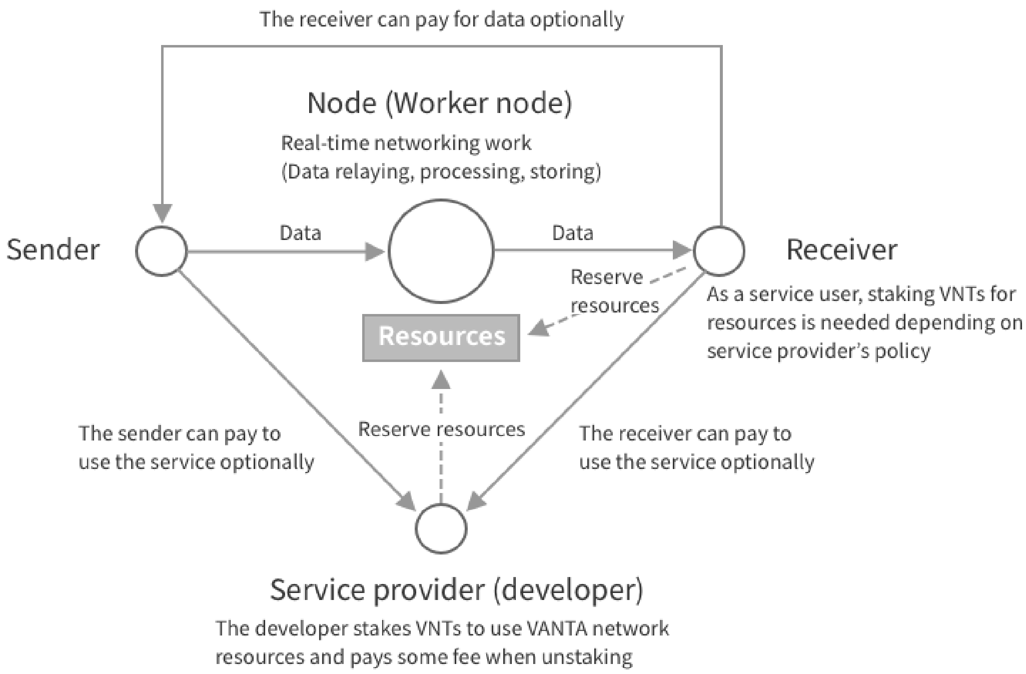

Figure 3. Application business model

2.3.2 VANTA-based service users

End users using VANTA-based services benefit from lower service costs and privacy. When a service developer stakes sufficient VNT tokens for the service's network resources, end users usually do not have to stake VNT tokens for their own resource usage. However, if the service is set up for end users to stake VNT tokens to run the service as explained in the previous sections, each user needs to stake VNT tokens for his/her own resource usage.

Users can also easily create a VANTA account without a separate subscription procedure or authentication. This is possible because network participants communicate through an anonymous hash value that cannot be used to track their identity. Also, users can create a new account at any time, further assuring that an individual cannot be identified. Since there is no central control authority and all data is encrypted and transmitted between peers, it is impossible to provide communication records, data / media, etc. at the request of a central government or authorities. This means that it is possible to use secure, decentralized communication services without privacy problems.

2.3.3 Benefits for organizations from adopting VANTA as a telecommunication network
Because VANTA is specialized in real-time networking and has various communication functions, VANTA blockchain can be used by organizations such as governments, businesses, and schools that want to build their own telecommunication network. The VANTA blockchain telecommunication network can be built quickly and cost-effectively without the need for a separate server or infrastructure.

VANTA will also provide direct consulting and customized development for cases in which the government, company, or school, etc. has technical difficulties using VANTA as a telecommunication network. Therefore, it is possible for each organization to build an optimized blockchain-based network.

2.4 VANTA Blockchain Competitiveness

Existing blockchains don't offer the features necessary in order to develop services with various real-time networking functions such as those offered by Slack, Facebook, and Twitch. These services require various functions such as text messaging, voice / video call, video streaming, and data processing. Current distributed ledger technologies cannot communicate in real-time. To develop and operate such services, real-time networking technology and an infrastructure for transmitting and processing data is essential. The VANTA blockchain is a specialized blockchain for developing and operating these real-time, networking-related services that can be used every day.

2.5 VANTA Team Competitiveness

VANTA is comprised of three teams: (1) researchers who have studied communication networks and have experience in commercializing technology; (2) a university lab that has been conducting research on communication blockchains for the past several years; (3) and a team that has accumulated experience in global IT companies. Combined, they form the VANTA team, dedicated to research and development of a blockchain-based network specialized for real-time networking. This highly competitive team will conduct in-depth research and commercialize VANTA technology to the real economy. The team utilizes the knowledge and results gained from previous research and development of communication networks and brings it to VANTA. This gives VANTA's team a great advantage over other project teams.

3. VANTA Intelligent Network

3.1 Definition of Real-Time Networking

Real-time networking, or real-time communication, is a methodology that lets a device communicate in real-time without transmission delays. In other words, it is a technology that makes it easy for people to quickly find, access, and utilize the necessary information. Real-time networking allows us to share a variety of information, and people in various locations can communicate as if they were facing each other. Online education, audio / video conferencing, file sharing, gaming, collaboration, social networking and machine-to-machine technology are implemented with real-time networking technology. Our team believes that real-time networking technology is essential for everyday life.

VANTA designed the intelligent network to decentralize real-time networking to allow more people to benefit from the technology.

3.2 Definition of Intelligent Network

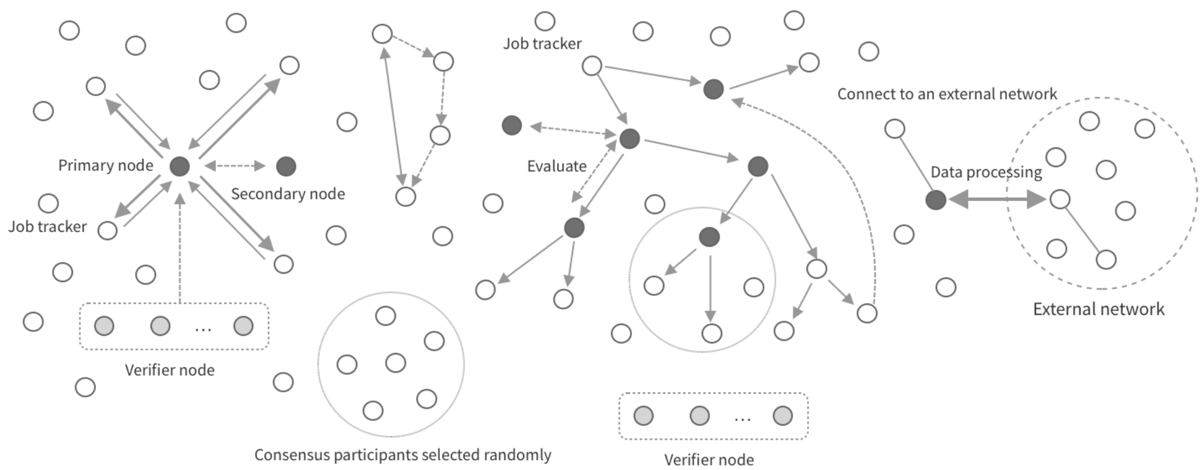

Figure 4. The intelligent network of VANTA - The ARKAS protocol

VANTA's intelligent network is a decentralized network that performs real-time data transmission, processing, and storage functions by selecting and evaluating peers. It is an evolving network that strengthens the scalability, reliability, efficiency, and privacy of real-time networking by creating a competitive system based on resources such as computing power, network bandwidth, memory, and reliability.

3.3 How the Intelligent Network Works

VANTA constitutes an intelligent network by allowing participating nodes to perform data transmission and processing operations accurately and reliably in a competitive manner. The VANTA ARKAS protocol and the consensus algorithm are the keys to this structure. Nodes constituting the intelligent network become intelligent node. In addition, installing the VANTA core client on your own computer or mobile device or installing applications developed on the VANTA API will allow you to participate as an intelligent node. Participants in the network compete with each other in order to receive data transmission / storage / processing tasks requested by the network in real-time, performing the main tasks as described in Figure 5.

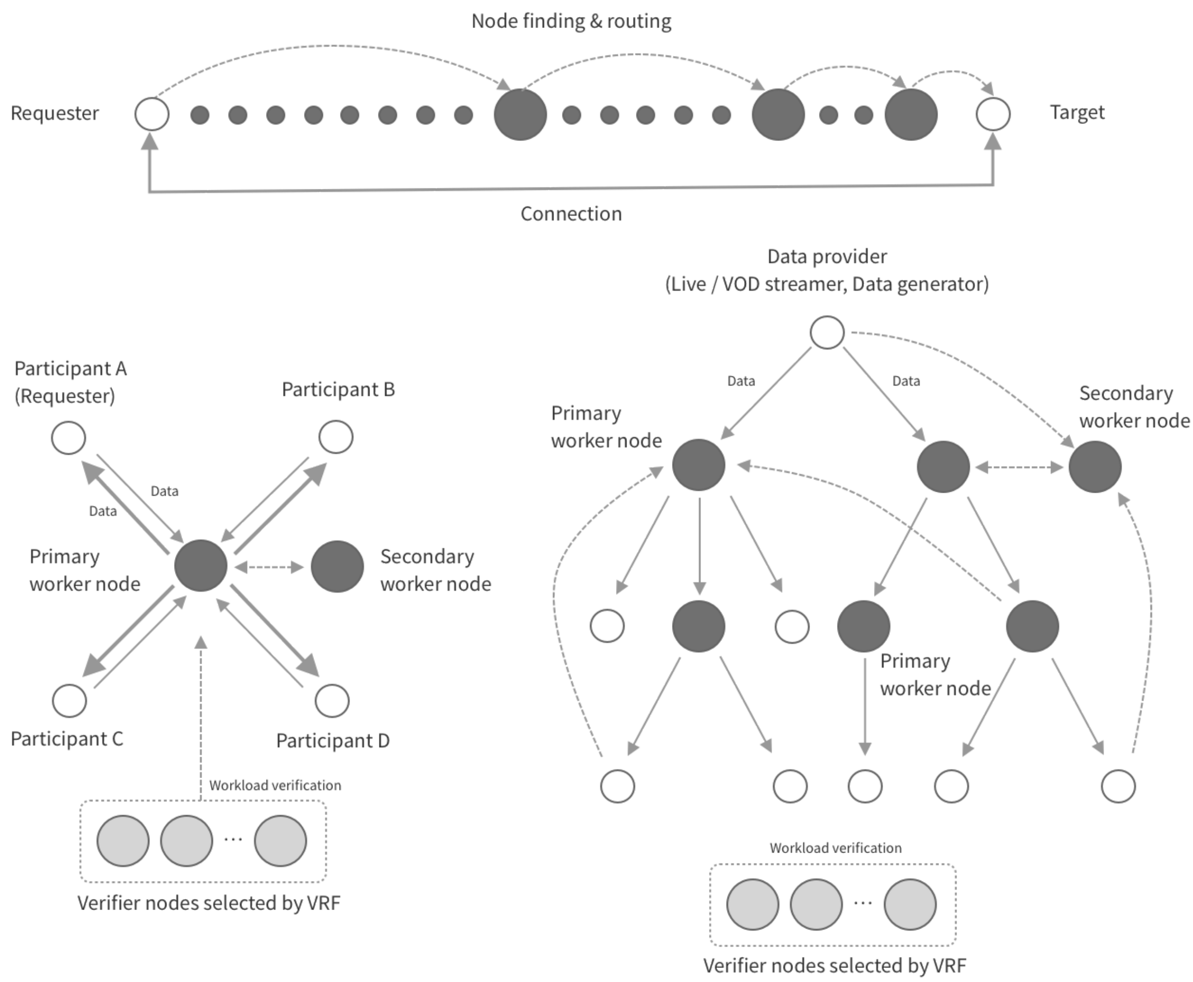

Figure 5. How the intelligent network works

3.3.1 Peer Finding & Connecting

A node finds a specific node in the network and transmits encrypted handshake information so that they can connect to each other in P2P fashion.

3.3.2 Data Relaying

A relaying node receives data from the sender and transmits the data to the receiver accurately and in a stable manner. Depending on the situation, several nodes communicate and collaborate with each other for data relaying. Data relaying plays a critical role for providing group chat, media streaming, video conferencing, and online multi-user games. Its main functions are data multicasting and media streaming.

3.3.3 Data Caching (temporary storage)
To increase efficiency of real-time transmission, a node temporarily stores data for a certain period of time. When the client requests the data, the node effectively delivers it. The node also provides data buffering and temporary storage of the streaming data.

3.3.4 Data Processing
A node processes media by converting the media stream to media format of various resolutions through media mixing or available computing resources of each node. This enables streaming services to be provided in the most suitable format to various smartphone and desktop devices.

3.3.5 Data Verification
A node verifies whether the nodes in the network properly perform the given task. There are various verification tasks, such as verifying the requested job in the network, node selection by a VRF (Verifiable Random Function), the work performed by the node, and various transactions and blocks.

3.4 Verifiable Random Function

A Verifiable Random Function (VRF) is a pseudo-random function that provides a proof that can be used to publicly verify the accuracy of its output. It is widely used within VANTA's real-time networking job competition model and blockchain consensus algorithm. A VRF is composed of three polynomial-time functions G, F, and V, and the details are as follows:

- G is a generator, probabilistic, and accepts one unary string (security parameter k) as an input value. It returns two binary strings each used as public key PK and secret key SK.
- F = (F1, F2) is the evaluator, and is deterministic. It accepts input x for SK and VRF as a binary string, and returns the VRF result value F1 (SK, x) for x and its corresponding proof, F2 (SK, x).
- V is a verifier and probabilistic like the generator. It accepts four binary strings, PK, x, v, and proof as inputs, and returns YES or NO.

Let $a : N -> N \cup \{*\}$ and $b,\ s : N -> N \cup \{*\}$ be any three functions such that a(k), b(k), s(k) are all computable in time poly(k), and a(k) and b(k) are both limited as a polynomial with respect to k (except when a takes value *). (G, F, V) is defined as a verifiable pseudorandom function (VRF) with input length a(k), output length b(k), and security s(k) if it meets the following properties:

1. The two conditions below have a probability of $1 - 2^{-\Omega(k)}$ for $(PK, SK) \leftarrow^{R} G(1^k)$
    a. Domain-Range Correctness
       $\forall\, x \in \{0,1\}^{a(k)}$, $F1(SK,\ x) \in \{0,1\}^{b(k)}$
    b. Complete Probability
       $\forall\, x \in \{0,1\}^{a(k)}$, if (v, proof) = *F(SK, x)*

       $$PROB[(V(PK,\ x,\ v,\ proof)\ =\ YES]\ >\ 1 - 2^{-\Omega(k)}$$

2. Unique Probability: $\forall$ PK, x, v1, v2, proof1 and proof2 when $v_1 \neq v_2$, and i is 1 or 2

a. $PROB[V(PK,\ x,\ v, proof_i) = YES]\ <\ 2^{-\Omega(k)}$

3. Residue Pseudo-randomness: when $T = (T_{E,} T_J)$ and the first input value is 1^k, and $T_E(\cdot,\cdot)$, $T_J(\cdot,\cdot,\cdot)$ are executed at a maximum of s(k) steps, the maximum probability that T succeeds in the following experiment is equal to $\frac{1}{2} + \frac{1}{s(k)}$.
    a. $(PK, SK) \leftarrow G(1^k)$
    b. $(x, state) \leftarrow T_E^{F(SK,\cdot)}(1^k, PK)$
    c. $r \overset{R}{\leftarrow} \{0,1\}$, if $r = 0$, $v = F_1(SK, x)$. if $r = 1$, $v \overset{R}{\leftarrow} \{0,1\}^{b(k)}$
    d. $guess \leftarrow T_J^{F(SK,\cdot)}(1^k, v, state)$
    e. T is successful under the condition that $x \in \{0,1\}^{a(k)}$, $guess = r$ and x are not queried by T.

3.5 Roles of Network Participants within the Intelligent Network

Because the intelligent network is based on P2P communication, nodes cannot trust each other by default and can lead to connection stability issues. Therefore, to ensure fault-tolerant job processing, each node with a specified role is selected based on a predefined set of rules. Data recorded on the blockchain is used to select and verify processing nodes.

The intelligent network uses a new consensus algorithm that selects block producers based on the number of real-time networking jobs a node has processed. We call the process of selecting job processing nodes and verifying workloads as "Proof of Networking", which is a significant part of the network since it is directly related to block generation. Therefore, VANTA needs to improve the distribution and validation of jobs, as well as increase the accuracy of performance measurements and records. The intelligent network uses Verifiable Random Functions to enforce randomness during node selection, and inter-network trust with benchmarks and votes across different nodes. The following is a list of roles assigned to each participant while processing jobs.

3.5.1 Requester
A device/client that requests a job related to real-time data transmission / processing / storage.

3.5.2 Target
The target device of the requester's job. The device receives the data from the requester or sends the data to the requester.

3.5.3 Job Tracker Node
The first node to receive a job request from a requester node becomes the job tracker. The job tracker is valid only for the job request. Job trackers are responsible for verifying and broadcasting job requests, managing nodes selected to process jobs, connecting existing workers and requesters, and more. Job trackers also submit job transactions.

3.5.4 Worker Node
Worker nodes are nodes that actually execute the submitted real-time networking tasks. Because primary workers may be selected based on the size of a VRF hash value (having the job request hash submitted to the job tracker as a seed) being larger than its competitors, verifiable randomness is also incorporated within the process of selecting worker nodes. Depending on the job, the worker is

connected to the sender or another worker, which is the actual data source or relayer. The sender continuously transmits data to the requested receiver or another worker node after processing the data according to the request. Worker nodes are divided into two groups, and more than one node can be selected according to a job.

Primary Worker Node
This is the node that executes the actual task as soon as the processing of the job starts.

Secondary Worker Node
This is the node that waits until the end of the job processing. When the primary worker node experiences a performance problem during processing or a network problem occurs, it takes over the task immediately.

3.5.5 Verifier Node

Verifier nodes verify if the worker node has been correctly selected and the worker node has properly performed the job. Subsequently, the node issues proof of the worker node's workload to the worker node. Using the job request hash as the seed, the VRF function randomly selects different verifiers based on their jobs.

3.6 Competition of Intelligent Nodes

When a job is submitted to the intelligent network and begins to propagate throughout the network, all nodes that are registered for processing the job compete for rewards by processing the job and accumulating proof of workload.

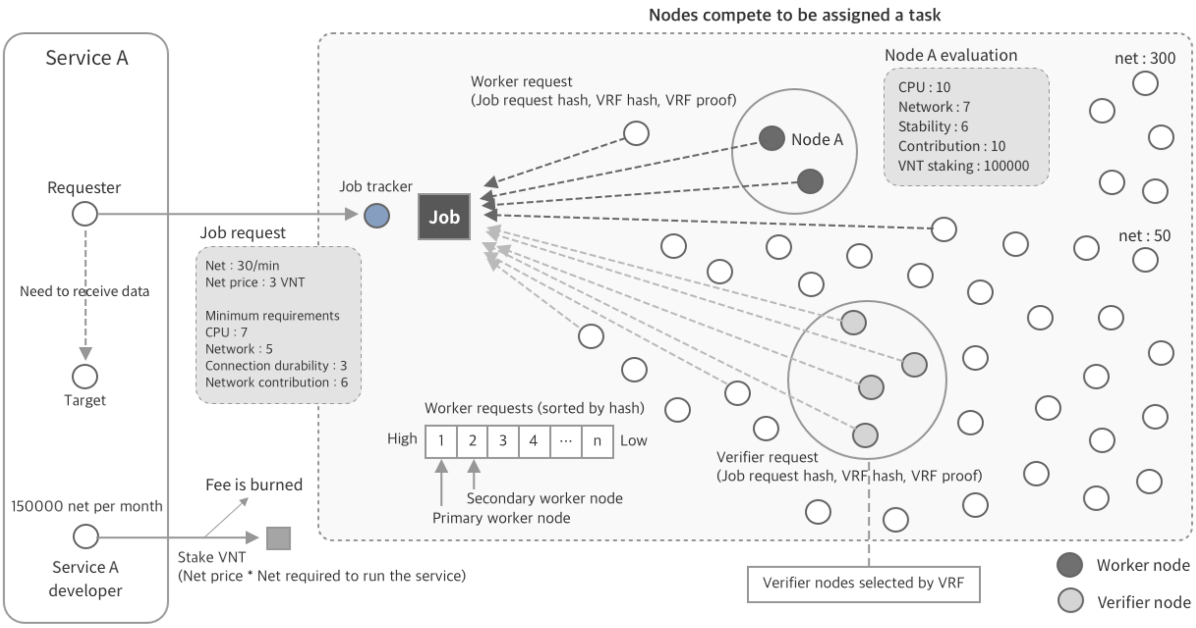

Figure 6. Job competition

3.6.1 Job Processing Requirements

Every job contains the minimum requirement for each criterion set by the developer who developed the service that generated the job. Jobs range from simple text messaging to group video calls, large group video streaming, and data processing. The same jobs may require different computing power, network bandwidth, and processing stability for each service.

3.6.2 Job Requests by Clients

1. A client for service A generates a job request for a real-time networking job and submits it to 1 or more nodes within the VANTA network. The client submitting the job becomes a job requester.
2. A list of job trackers may be managed separately, and in the case of a connection timeout to a node, it is removed from the job tracker candidate list. Another candidate is received and the request is submitted again.

3.6.3 Selecting Job trackers

1. The first node that was assigned to a job request will begin its role as the job tracker. The job tracker reviews job request content and signs it before disseminating it to the network.
2. Depending on certain situations and rules, a job tracker must return another job tracker's list to the job requester instead of performing the role of job tracker themselves.
3. If a requester's target is experiencing data relay because of another worker, the worker list must be returned to the requester.
4. After a job is disseminated, worker request is received by worker node candidates, and verifier request is received by verifier node candidates. A maximum of i, j numbers of worker request and verifier request will be accepted per 1 job. The rest will not be accepted.
5. A job tracker verifies and chooses candidates, then notifies the job requester and disseminates the job transaction to the consensus network to add the job's contents in the blockchain.
6. Lastly, the job tracker combines account information and IP addresses of the selected workers, verifiers, requester, and target and transmits the data to all nodes. The job tracker's role ends here, and the rest of the job processing is performed by the requester, target, worker, and verifier, all communicating with each other.

3.6.4 Selecting Worker Nodes

1. A node receives several job requests at the same time and accumulates jobs in its own queue. Each node judges which job to select based on the job price, which is the processing price of the job specified in the request.
2. A node that participates and wants to compete as a worker node compares the job processing requirements with its current node metrics such as its own computing power and network bandwidth.
3. If the job processing requirements are met, the node will have the basic requirements to process the job. It executes a VRF with the job ID as a seed to generate hash and proof, and sends a signed worker request with the job request to the job tracker.
4. The job tracker should receive at least n worker requests.
5. The worker nodes for N number of worker requests are sorted based on the VRF hash value of the candidates, and then the primary worker node and the secondary worker node are sequentially selected from the node having the highest VRF hash value. For cases where the primary/secondary workers are all malfunctioning, top n number of workers' lists are used as well.

6. *n* number of worker requests are submitted to the verifier nodes to be verified so that the worker node has been correctly picked from the list sorted by VRF hash value.

procedure Worker node selection

// Worker candidate side
if $Qualify(jobRequest, performanceProof_u, reputataionProof_u)$ **then**
$hash_u \leftarrow VRF_{SK_u}(jobRequestHash)$
$proof_u \leftarrow VRF\_Prove_{SK_u}(jobRequestHash)$
$workerRequest_u \leftarrow CreateWorkerRequest(hash_u, proof_u)$
$signature_u \leftarrow Sig_{SK_u}(workerRequest_u)$

// Job tracker side
// Receive and verify worker requests from worker candidates
$< PK_u, proof_u, hash_u, jobRequestHash > \leftarrow workerRequest$
if $VRF\_Verify(PK_u, proof_u, hash_u, jobRequestHash$ **then**
  $workerRequestList \leftarrow AddRequest(workerRequest)$

// Worker selection
$SortByVRFHash(workerRequestList)$
$primaryWorker \leftarrow workerRequestList.get(0)$
$secondaryWorker \leftarrow workerRequestList.get(1)$
$workerList \leftarrow addWorkers(primaryWorker, secondaryWorker, GetSpares(workerRequestList))$
$signature_j \leftarrow Sig_{SK_j}(workerList)$
...

3.6.5 Selecting Verifier Nodes

1. A node that wants to join as a verifier node executes a VRF, judges whether it can join, and sends a signed verifier request with a job request, hash, and proof to the job tracker.
2. The job tracker should receive at least m verifier requests and ignore verifier requests received after m.
3. The top 5 verifiers are chosen for a job based on the VRF hash values of m number of nodes who sent verifier requests.

Each job is measured by the price of the job, which determined by a Net, a work unit of VANTA. The price of a Net is specified by the service developer when staking the VNT to allocate resources for the service. Each node checks the price of the job, and can decide if it wants to compete with other nodes to handle this job. If the Net price is much lower than the current price but there are high requirements, the nodes may decide not to participate in the competition. This will be the selection criteria when jobs that have higher Net prices are requested at the same time. Therefore, when measuring the value of a job, the Net market price can be formed independently of the VNT price.

3.7 Proof of Intelligent Nodes' workload

Because the intelligent network can be joined by anyone, there can be nodes that maliciously behave in order to maximize their own interests. A node in the intelligent network not only receives adequate compensation depending on how many jobs the node processes, but also increases the probability of becoming a block proposer in a specific consensus round. For this reason each node needs to accurately performs its task, and prove it. This is very important because the quality of real-time networking in the network depends on how thoroughly the operation and verification are executed.

Some of the jobs worker nodes do are defined as action. Worker nodes are rewarded based on the workload, which is evaluated based on the amount of data transmitted as well as the duration of peer connection maintained in order to achieve real-time data transmission.

When the first job is created, the nonce value for that job is incremented by 1 every minute starting with 0. The verifier nodes prove that the primary worker node is performing the work on the corresponding nonce value. The verifier monitors the state of the data transmission by communicating with the sender, receiver, and worker every 10 seconds, and the workload verification is written, signed, and sent to the worker in 1 minute intervals.

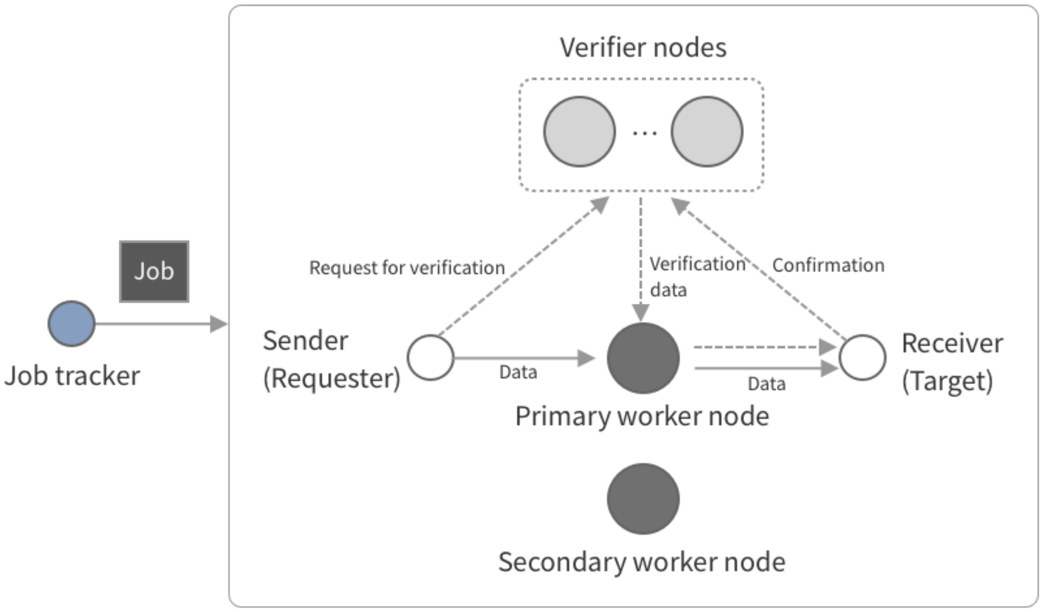

Figure 7. Workload verification

1. The sender signs the verification data, including the nonce value and the amount of data transmitted per 1 minute, as proof indicating that the transmission data for the corresponding nonce is being transmitted to the primary worker node. The sender also transmits it to the verifier node.
2. The verifier node signs again, signifying that it has begun workload verification, and sends it to the primary worker node. The primary worker node sends the verification data with its signature to the data receivers.
3. If the primary worker node correctly transmits the sender's data, the receiver adds its signature to the verification data, including the amount of data received per 1 minute, and sends it back to the verifier node.
4. Each verifier node adds its final confirmation signature to the final collected proof of work data and sends it to the primary worker node.

5. If the proof of work verified by the verifier nodes is secured for ⅔ or more, the primary worker node generates a workload verification transaction including the proof of work in the Confirmed Payload.

The workload verification transaction includes the following data:

$Type$: Value used to classify transaction types (job transaction, workload verification transaction)
$App\ id$: Unique Id value of the application for requested job
$Job\ id$: Unique Id value of committed job
$Data\ id$: Unique Id value of source data
$Action$: Action that must be completed by a worker node
$Nonce$: A unique value at job tx id, starting at the first 0 and incrementing by 1
$Workload$: Workload of the job (Net)
$Net\ Price$: The specified Net price requested by the service developer when staking (VNT)
$Timestamp$: Time to request proof of work; the value to prevent more than two nonce values from being present within one minute
$Primary\ Worker\ Node$: Hash value of primary worker node
$Secondary\ Worker\ Node$: Hash value of secondary worker node
$Verifier\ Node\ List$: List of verifier nodes
$Confirmed\ Payload$:

- Job request signed by a requester
- A bundle of workload verification identified by the verifier node, each of which is the data that the verifier last signed. At least ⅔ verifier nodes for the given nonce must receive the final verified data to be compensated.
- Each workload verification includes a job id, a nonce, and a signature signed by a sender, a primary worker node, and a receiver in sequence with a private key.

There is the possibility that the primary worker node maliciously colludes with the sender and the receiver to only generate the confirmed payload for a long time without actually transmitting the data for the reward. To prevent this situation, the primary worker node is replaced with a standby secondary worker node every 1 hour.

If the proof of work result of the verifier node is not included in the Confirmed Payload, 50% of the ⅓ verifier not included is replaced with a new verifier node via VRF. This means that the verifier nodes must compete with each other and deliver the proof of work results to the primary worker node as soon as possible.

3.8 Fault Detection and Recovery

While processing a job, participating nodes can check the status of each other through a persistent P2P connection. Each node detects status change events when a particular node exits a network or a faulty communication channel caused by an unstable network. When the status event reports a disconnected or failed state, the status of that node is broadcast to the verifier. Each verifiers checks the status of the faulty node and runs a voting process within its verifier group. When more than 50% of verifiers determine that the node was faulty, the node is replaced with a new node that can process its given workload.

3.8.1 Job tracker node

Because a job tracker can be faulty or can leave the network, the job requester submits the job to more than 2 nodes. The first job tracker to compile the list of nodes required to process the requested job processes the submitted job.

3.8.2 Worker node

When the primary worker node is determined to be faulty, the secondary worker establishes a data exchange channel between the sender and receiver and prepares itself to replace the primary worker. When the secondary worker is faulty while the primary node is operating correctly, a new secondary worker is selected from the list of worker candidates.

3.8.3 Verifier node

All verifiers establish a persistent communication channel to determine a faulty verifier, and the verifiers run a vote to decide its final status. When the node is determined to be faulty, a candidate verifier immediately joins the verification process. Because there should be at least 5 verifiers within the processing group to process a job, verifiers should keep a minimum number of verifiers to receive the processing reward.

3.9 Performance Evaluation and Reputation System

All nodes in the network are evaluated against each other for computing power (CPU), network bandwidth, connection stability, and network contribution.

3.9.1 Performance Evaluation

When a node participates in the network, it will be requested to perform a job, such as monitoring the computing power and network bandwidth. Randomly requested for evaluation. CPU-intensive logic is used to evaluate computing power, and file transmission results is used to evaluate network bandwidth. Monitoring results and time stamps are signed off by each node and sent to the requested nodes. Nodes that receive the data turn them into transactions and submit them to the network. The state of each evaluated node is then updated to include their newly evaluated values. The state of each node will represent the average of its performance results.

3.9.2 Classification of performance evaluation results

The performance evaluation result is divided into 10 different levels, based on the distribution of performance results for all nodes. Because the overall performance levels of participating devices can change over time, the performance medium used to calculate a node's level is recalculated every 86400 blocks. Developers and end users can refer to the performance distribution map of participating devices to stake tokens for resource allocation.

3.9.3 Reputation System

Connection stability refers to the ratio of a node not being faulty and actively participating in processing jobs, which includes not leaving the network or not having unstable network connections. This is recorded through a state transition transaction through verifier votes. Network contribution refers to the number of jobs processed by that node and recorded on the net scale with a workload verification transaction.

3.10 Security

VANTA Network is a network of intelligent peers connected by P2P. All peers are directly or indirectly connected to the network, which means that data transmitted over the network may be vulnerable. In order to build a more robust and reliable network from a security perspective, a handshake message for P2P connection is encrypted with the public key of the recipient. And Datagram Transport Layer Security (DTLS) is used to enhance the security of P2P data transmission. In addition, as a protocol for data / media transmission, Stream Control Transmission Protocol (SCTP) and Secure Real-time Transport Protocol (SRTP) for a media stream are used as default. The protocol uses the Privacy Enhanced RTP Conferencing (PERC) method, which is a double SRTP encryption that enables E2E media data encryption when providing the video conferencing function.

3.10.1 Data Transfer

SCTP is used for messages and data transmission. In the case of 1: 1 data transmission, the original data is encrypted with the public key of the receiver so that the intermediate transmitter cannot decrypt the data. For 1: N data transmission, the group creator that creates the first group generates a private key and a public key as group key. The two generated keys are encrypted with the public key of the participants in the group. Each participant encrypts the data using the group public key to transmit data and decrypts the received data with its own group private key.

When a new participant is added, the existing participant encrypts the group key with the public key of the new participant and transfers it. If the existing participant leaves the group, a new group key is generated again and transferred using the same method. Lastly, the message is encrypted with a new group key and transferred.

3.10.2 Media Transfer

In general, a video conference service provided by a centralized service provider transmits a video of a user to a media server, and the media server mixes multiple videos into one and transmits it to other participants. In this process, the media server is able to acquire media data of users in a reproducible form, which means that there is a possibility of privacy problems at any time.

Media servers mainly use the MCU (multipoint control unit) and SFU (Selective Forwarding Unit) methods. The MCU method utilizes Media Mixing processing to make each participant's media stream into one media stream, while the SFU method transmits the media stream of each participant to the other participants as a relay. In both methods, the original media data can be exposed during the process of mixing and transmitting the media data.

The security level of end-to-end media encryption, which makes it essentially impossible to expose media data, is required due to the nature of the VANTA Network that any peer can perform a media mixing function as an intermediary. To achieve this security level, VANTA Network uses the PERC scheme as the concept of SFU-based double encryption SRTP.

The SRTP packet transfer in the conventional SFU method decrypts the encrypted RTP payload in the SRTP packet transmitted from the sender and acquires the data. After acquiring the data, the SSRC (synchronization source) data included in the payload descriptor is modified and transmitted to add the media source of another participant. In this process, the media data contained in the RTP payload is exposed. SRTP ensures that P2P (sender and relay, relay and receiver) security is guaranteed from third parties, but SFU, an intermediary that does not participate in the video conference, is not secure. This method is called Hop By Hop Encryption, and the VANTA network uses the PERC scheme to provide end-to-end encryption that guarantees all security between participants.

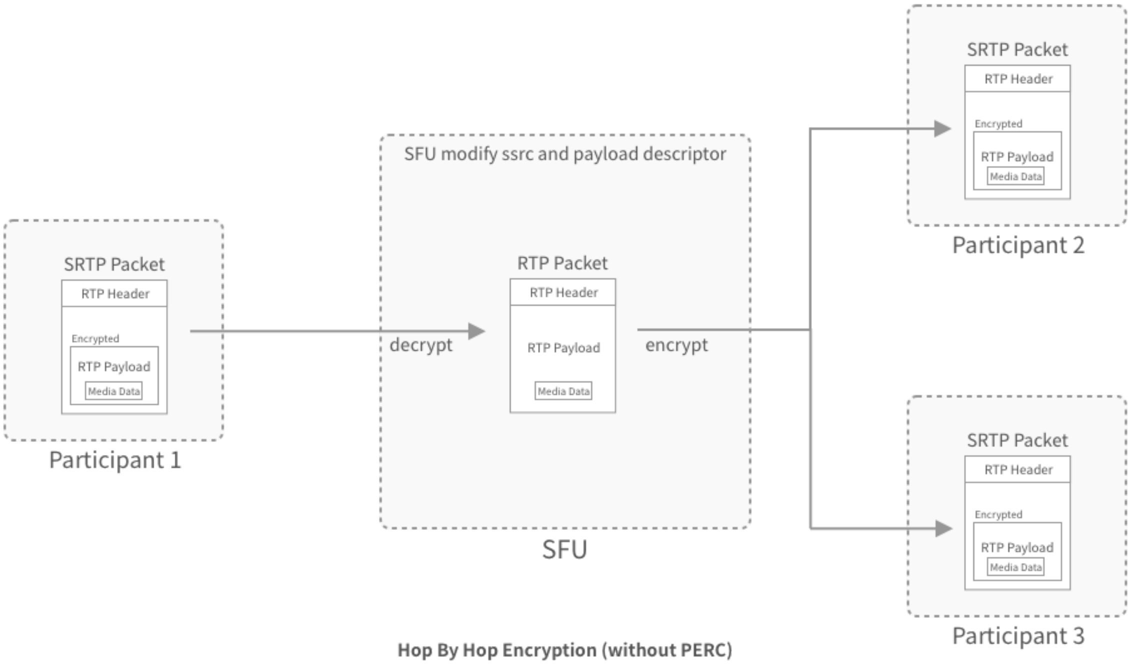

Figure 8. Hop by hop encryption

The PERC scheme encrypts the media metadata once more when generating the SRTP packet so that the SFU cannot acquire the original media metadata. The Advanced Encryption Standard (AES-128) algorithm is used for E2E encryption. To encrypt the media metadata again, the participant needs E2E encryption and decryption keys for his / her one-time use for the conference. They exchange the keys of each other through the key distributor in order to send their own decryption key to other participants. All participants encrypt their E2E decryption key with the public key of the other participant's wallet. Once the E2E decryption key exchange is complete, each participant will have his / her E2E key pair and all other participants' E2E decryption Keys. The decryption key of the other participant is used to decrypt the media metadata encrypted with the participant's encryption key.

When the sender creates the SRTP packet, only the media metadata part of the RTP payload is encrypted with his E2E encryption Key, and then encrypted by SRTP once again with HBH Encryption and transmitted to SFU. SFU executes HBH decryption of the delivered SRTP packet using RTP header and RTP payload and modifies the SSRC in the payload descriptor to add another participant's media source. Again, the SRTP Packet is sent to each receiver after SRTP executes HBH Encryption on the data. The recipients execute HBH Decryption on the received SRTP packet and can acquire and reproduce the original media metadata by decrypting the final media metadata with the E2E decryption Key shared by the sender.

In this process, the media metadata part is encrypted with the E2E key, and no one, including SFU, except the allowed conference participants can restore the original media metadata.

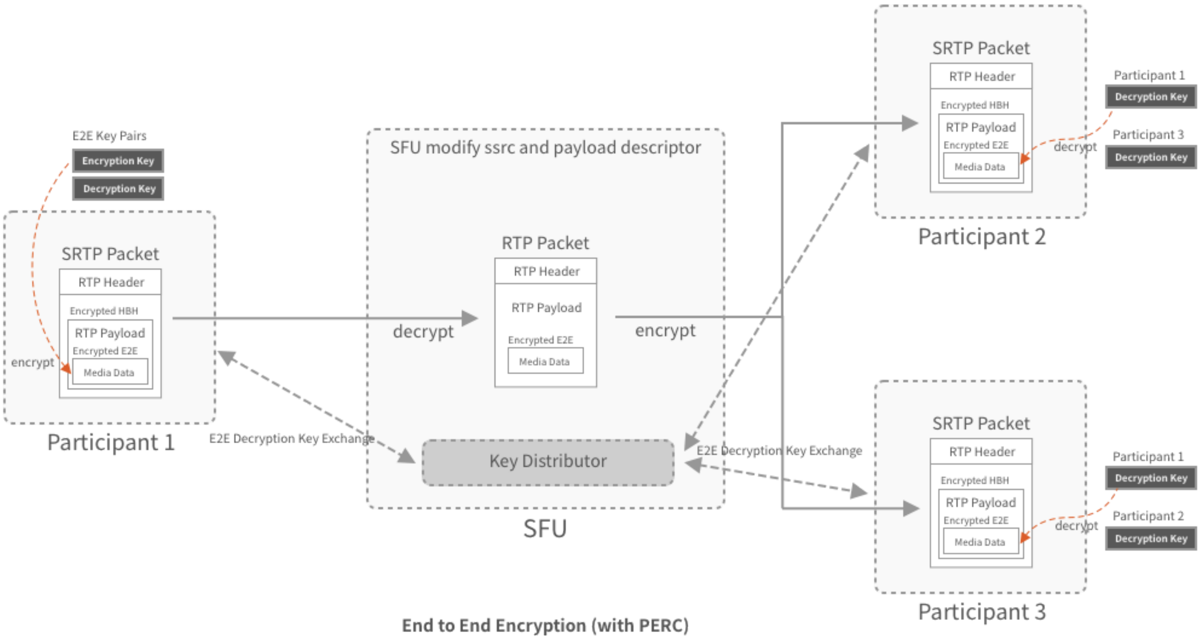

Figure 9. End to end encryption

4. VANTA Blockchain & Consensus Algorithm

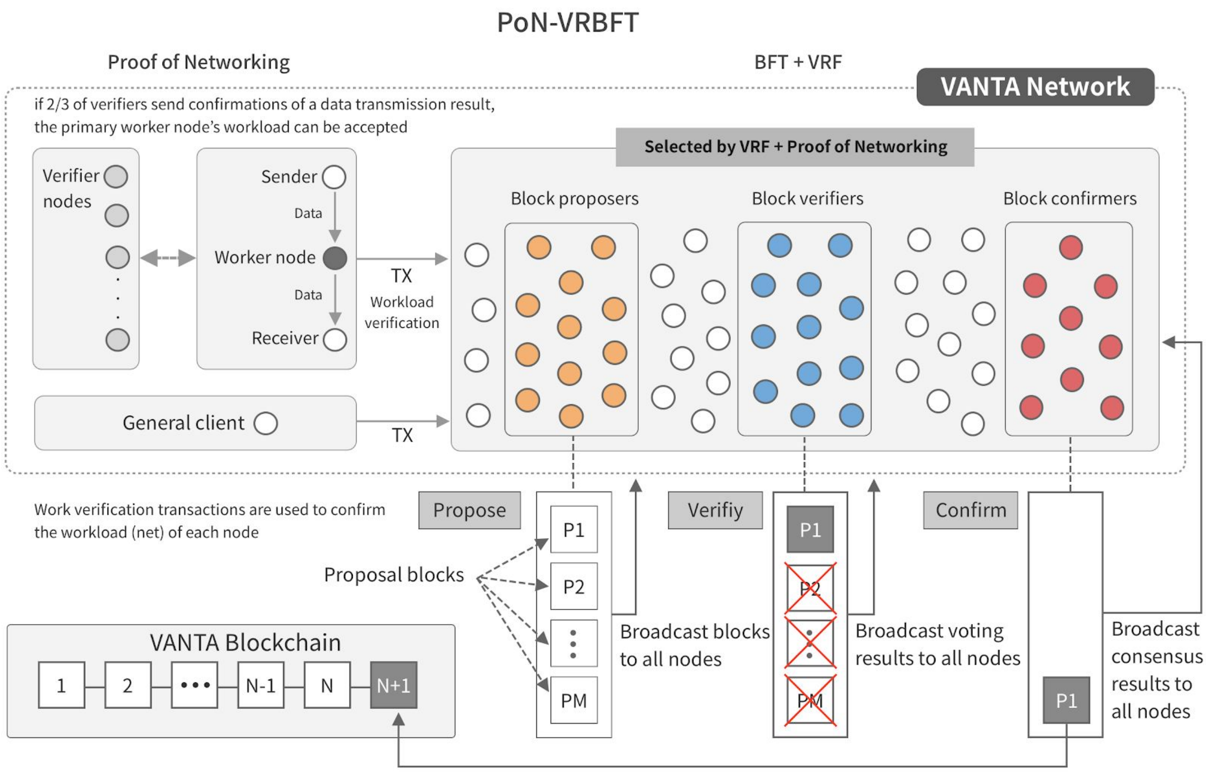

Figure 10. PoN-VRBFT consensus algorithm

4.1 The Need for a New Consensus Algorithm

Because VANTA is a blockchain designed for processing real-time networking tasks, a new consensus algorithm is needed for effectively processing it. Previous consensus algorithms were based on Proof-of-Work or Proof-of-Stake and wasted computer power, and thus were unsuitable for use with VANTA. Therefore, VANTA aims to use the computing power and network resources of network nodes for real-time networking and merge proof for those tasks with block generation and consensus algorithms to create a consensus algorithm optimized for VANTA.

4.2 PoN-VRBFT Consensus Algorithm

VANTA has created an algorithm called Proof of Networking (PoN) that allows each node to contribute competitively to real-time data transmission, processing, and storage in the network. This was combined with Byzantine Fault Tolerance (BFT) and Verifiable Random Functions (VRF) to design a unique consensus algorithm called PoN-VRBFT.

VANTA nodes have a higher probability of generating blocks based on the amount of real-time networking jobs they have performed. However, nodes that have performed the most jobs are not always selected as the block producer. Block proposers, block verifiers, and block confirmers are selected on a random basis through a random function in order to prevent specific nodes from continuously being selected. VRFs are used for the random function, because verification of whether the selected nodes were truly selected randomly cannot be done through typical random functions. The idea of combining BFT and VRF was first proposed by Professor Micali with Algorand, and the idea was also partly borrowed in Ontology for its consensus algorithm. The VANTA Team aims to combine BFT and VRFs to create a new consensus algorithm suitable for the VANTA Network, which equally improves security, scalability and transaction speed of existing consensus algorithms alongside a new networking proof mechanism, PoN.

4.3 Proof of Networking (PoN)

Proof of Networking is an algorithm that mandates each node that has contributed competitively for live data communication, processing, and storage prove its workload and use that proof data when participating in a consensus round. The workload of each node is verified by verifier nodes selected through VRF and recorded using VANTA's unique workload unit called Net and Net price to prove the amount of workload and the actual value of it. This is what differentiates PoN from other consensus algorithms.

The exact mechanism of VANTA processing those workloads on each node and how those tasks can be proved on a decentralized network has been explained in detail within the previous section (section 3). First, the worker node that processed the requested job is verified on whether the job has been properly processed from the verifier nodes. When workload verification is received from ⅔ of all verifier nodes participating in job verification, the worker node generates a workload verification transaction for its own workload including workload verifications. The worker node then immediately propagates the transaction to the network and inserts it into its own transaction pool.

When the consensus round is initialized, all nodes with workload verification data determine whether they will participate in this consensus round. In order to determine participation, each node executes a VRF function by using a hash of the previous block header as a seed. Then, they only select their own workload verification transactions from the obtained hash value and the transactions contained in the current transaction pool. Lastly, they calculate the total work value and use it to execute the consensus participation confirmation function. When a node has processed more jobs with higher value, the node is more likely to be selected as a block proponent.

4.3.1 Transaction Type

There are three types of transactions within the VANTA Network. The first is a general transaction for transferring VNT tokens. The second and third are a job transaction and a workload verification transaction used in PoN for real-time networking job execution.

The workload verification transaction includes the job requester and target, the network and price of the worker node, and the workload verification data from the verifier nodes. This transaction is configured and propagated by the worker node. The Net price is the number of staked tokens required to process a job per hour, set by service developers when they deploy their application. This Net price determines the value of the job on the network, and when block generation rewards are paid, the final reward ratio is determined based on the sum of all of these values.

$$v = \sum_{i=1}^{n} w_i * p_i$$

v : The sum of the workload value of the node (VNT)
w : The workload of the job (Net)
p : The Net price of the job (VNT)
n : Number of the workload verifications for the node that are in the block

4.4 BFT+VRF (VRBFT)

From VANTA's PoN-VRBFT consensus algorithm, VRBFT refers to BFT and VRF. While existing solutions like Algorand and Ontology merged Proof-of-Stake with BFT and VRF, VANTA adds PoN to create a consensus mechanism specialized for real-time networking. Byzantine Fault Tolerance (BFT) combined with VRF is a proven consensus algorithm with many advantages. Unlike conventional PBFT consensus algorithms, VRF that is an unpredictable and verifiable pseudo-random function can be used to randomly select a small number of nodes participating in a consensus round, as explained above. It also allows a network to reach consensus with only a few selected nodes. Conventional PBFT algorithms, where nodes have to communicate with each other twice, have a communication complexity of O(n^2). However, when combined with VRF, blocks can be generated much faster because only a few nodes need to communicate to reach consensus each round.

The random seed for the VRF is determined from the seed of the previous consensus round, so that no one can predict the block proposer, the block verifier, or the block confirmer, thereby preventing a malicious attacker from predicting and attacking the target in advance. In addition, through the verifier function (described with the above definition of VRFs) and the proof value of the evaluator, it increases the reliability of the consensus process because the selected nodes can be easily verified by other nodes on whether the selected nodes are actually the selected nodes in this consensus round.

4.5 Block Proposal

If a node is selected as a block proposer by the VRBFT process, the node puts the transactions into a block in its own transaction pool. The workload verification transactions that it has used to participate in the consensus round are submitted as evidence that it has been selected as the block proposer. The workload verification transactions are first included in the block since they must be verified by other nodes. Next, workload verification transactions and general transactions of other nodes are taken out of the transaction pool in chronological order and included in the block. Finally, the block is signed and then broadcasted to the network.

procedure Propose

1: $hash_u \leftarrow VRF_{SK_u}(CreateSeed(value_{r-1},\ step_{proposal}))$
2: $totalWorkValue \leftarrow 0$
3: **for each** $workloadVerification_i$

$totalWorkValue \leftarrow netPrice_i * netWorkload_i$
if $Eval_{proposal}(hash_u,\ totalWorkValue)$ **then**
$block_u \leftarrow CreateBlock()$
$signature_u \leftarrow Sig_{SK_u}(block_u)$
$Broadcast(block_u, signature_u)$

4.6 Block Verification

To verify a block, the block verifiers select and sign the block with the highest block header hash value among the candidate blocks proposed by the block proposers. Then, they broadcast the message to prove that they are selected as block verifiers, including the workload verification transaction used to determine their participation by the verifier to join as a block verifier.

procedure Verify

$hash_u \leftarrow VRF_{SK_u}(CreateSeed(value_{r-1},\ step_{verification}))$
$totalWorkValue \leftarrow 0$
for each $workloadVerification_i$
$totalWorkValue \leftarrow netPrice_i * netWorkload_i$
if $Eval_{verification}(hash_u,\ totalWorkValue)$ **then**
$maxHash \leftarrow 0$
$selectedBlock \leftarrow null$
for each $proposed\ block_i$
if $\neg VerifyBlock(block_i)$ **then continue**
if $\neg VerifyVRF_{PK_i}(hash_i, proof_i, CreateSeed(value_{r-1}, step_{proposal}))$ **then continue**
$evalHash_i \leftarrow Hash(signature_i)$
if $evalHash_i > maxHash$ **then**
$maxHash \leftarrow evalHash_i$
$selectedBlock \leftarrow block_i$
$signature_u \leftarrow Sig_{SK_u}(selectedBlockHash)$
$Broadcast(selectedBlockHash, signature_u)$

4.7 Block Confirmation

With the confirmation step, the nodes run a Byzantine Agreement based on the voting results. The confirmer nodes count the number of votes for each block. If the vote count exceeds a quorum, a signature is generated and the hash for the block is computed and broadcast.

procedure Confirm

$hash_u \leftarrow VRF_{SK_u}(CreateSeed(value_{r-1},\ step_{confirmation}))$
$totalWorkValue \leftarrow 0$

```
for each workloadVerification_i
    totalWorkValue ← netPrice_i * netWorkload_i
if Eval_confirmation(hash_u, totalWorkValue) then
    voteCounts ← {}
    selectedVoteIndex ← 0
    for each vote_i
        voteCounts[blockHash_i] ++
        if voteCounts[blockHash_i] > quorum then
            break
    signature_u ← Sig_SK_u(vote_selectedVoteIndex)
    Broadcast(selectedBlockHash, signature_u)

…
```

4.8 Block Reward

All nodes that have performed a workload receive a block generation reward in proportion to their total work value. When a workload verification transaction of that node is included with that particular block, or if that node became the final block producer, the compensation received by each node is calculated as follows.

$$R(A) = W(A) + B$$

$$W(A) = \left(\frac{k-1}{k} * \frac{v}{t}\right) * \left(\frac{\sum_{j=0}^{m} w1_j * p1_j}{\sum_{i=0}^{n} w2_i * p2_i}\right)$$

$$B \in \left\{ \frac{1}{k} * \frac{v}{t},\ 0 \mid \textit{if node A selected as a final block producer, B is } \frac{1}{k} * \frac{v}{t}\textit{, else B is 0} \right\}$$

$R(A)$: Total reward for node A at block finalization
$W(A)$: Reward for workloads
B : Reward for block generation
k : Block generation reward ratio
v : Number of new VNT tokens issued this year (VNT)
t : Block generation cycle (sec)
$w1, p1$: Workload (Net) and Net price for node A (VNT)
$w2, p2$: Workload (Net) and Net price for all nodes (VNT)
m : Number of workload verification transactions by node A among the transactions in the block
n : Number of workload verification transactions by all nodes among the transactions in the block

4.9 Penalty

Worker nodes that participate in consensus within the VANTA Network are responsible for performing real-time networking jobs as well as creating and confirming blocks. Thus, if a node does not perform the data transfer and processing roles properly, or if a node does not act properly as a consensus participant, its participation in the network will be limited as a penalty, and the node will be ineligible to receive rewards.

The nodes selected as consensus nodes are worker nodes and will participate in the role of proposing, verifying, and confirming the blocks to receive rewards for their own workload. Even if workload verification transactions of nodes that are selected as verifier or confirmer nodes in the current consensus round are not included in the candidate block, the nodes will verify or confirm the block as soon as possible, so that the next block can contain its own workload verification transaction. Eventually, the nodes that have their workload verification should participate in every consensus round to be rewarded for their workload.

5. VANTA Cryptoeconomics

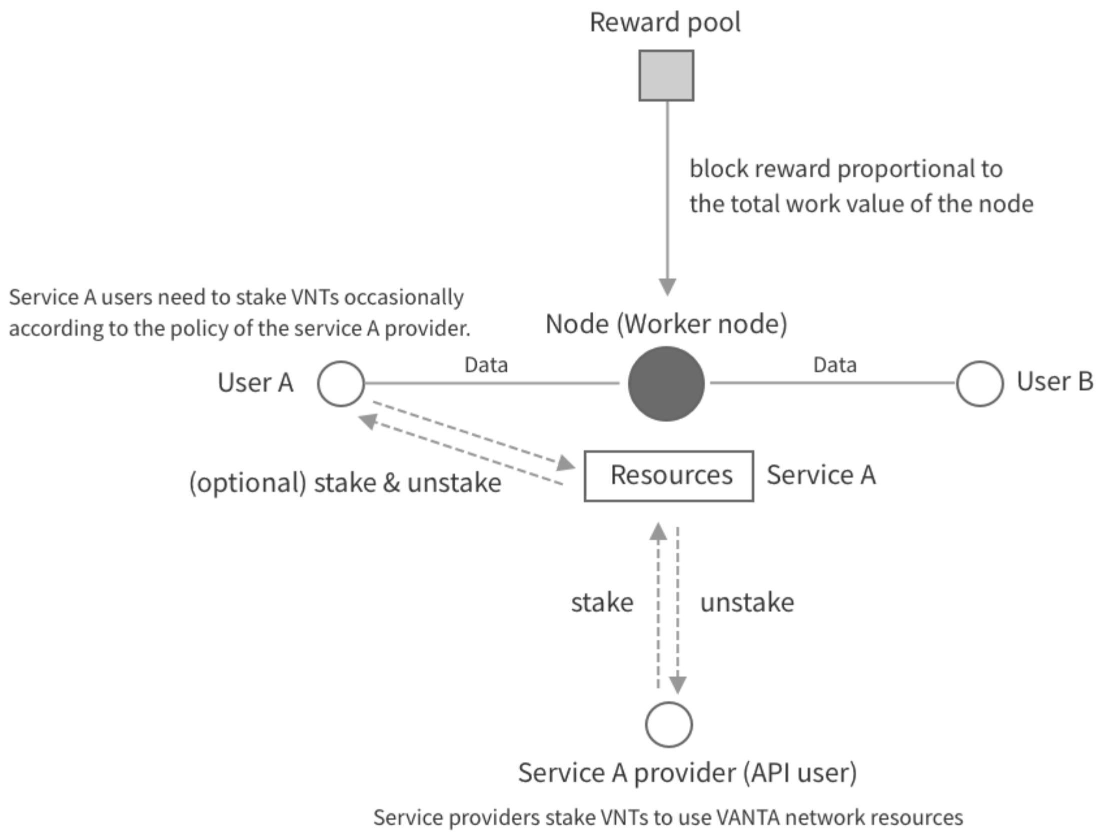

Figure 11. Cryptoeconomics

5.1 Token Issuance

The annual amount of newly issued VNT tokens is determined by a fixed rate of 2 percent, and the variable rate is based on the number of tokens burnt in the previous year. Newly issued tokens are used as incentives for nodes performing real-time networking workloads and participating in block generation. Tokens burnt will go to the zero address, similar to Ethereum.

5.2 Staking Tokens for API Usage (application developers)

Companies that want to develop and operate services based on VANTA must stake VNTs in order to transfer, process, and store data using the VANTA API. There will be an expected amount of workload per month required for each service, and service providers should stake VNTs proportional to it. All of the functions for real-time networking in VANTA are measured by VANTA's work unit called a Net. A service developer should stake VNTs in order to get Net corresponding to monthly resource usage for their service.

$$s = w * p$$

s : total stake required (VNT)
w : workload per month (Net)
p : Net price (VNT) set by developers

For example, if an application developer needs a 500,000-net total of real-time networking resources per month for their application and the current average net price is 3 VNTs, the developer can set the net price to 3 VNTs and stake a total of 1,500,000 VNTs (500,000 net * 3 VNTs). If the developer wants the jobs submitted by its service to be processed faster or wants it to be processed by nodes with higher performance, setting a higher Net price will prioritize processing for that job on the network. When the application generates a job request and the work to be processed by the job is worth 20 Net, 60 VNT (20 Net * 3 VNTs) is set as the price of the job and propagated across the network. Then, the nodes that are willing to process the job for the price may competitively participate and process real-time data transmitting, processing, storing, and other networking tasks. Twenty Net, out of the total available workload request of 500,000 Net for the developer's service, will be deducted for the job from its available workload request, and this deducted workload will be filled to the total available workload after 30 days.

If the price of Net specified by the developer is too low or the service users generate jobs that are worth higher than the assigned workload, the jobs will not be processed by the nodes. In this case, the developer must unstake and stake VNTs for the new Net price again or stake additional VNTs in order to allocate sufficient workload.

Therefore, as more apps are developed for VANTA, more developers will be staking VNTs. And as the VANTA network processes more workloads, the amount of Net required will increase, and each developer will have to stake more VNTs. The efficient market will constantly find an equilibrium between cost of service, performance, and reward.

Finally, when unstaking VNT used to purchase workloads, there may be some tasks that are already being executed and on hold. Therefore, when unstaking VNT is requested, VNT is returned to the developer's account after 24 hours.

5.3 Staking Tokens for API Usage (end users)

In cases when an application developer does not have sufficient funds to continue providing its services, a sudden influx of users, or when required by the service's business model, developers can set staking rules for their end users. When a new user joins the service, or uses the service heavily, the developer can allow the end user to stake the additional number of tokens required for its workload. Also, the end user can set a monthly Net usage limit, which can enable more user-level custom staking models. Thus, the developer can prevent the malicious use of the developer's Net for unintended purposes. Because of these additional preventative measures, developers can choose to stake all the required Net for all users when they have enough funds. In the case of startups or individual developers, they can let the users stake the required VNT tokens to operate the service.

$$v = p_d * w_d + \sum_{i=0}^{n} p_i * w_i$$

v : total value of resources for service A
p_d : Net price (VNT) set by service A developer
w_d : workload per month (Net) shared for all service A users
p_i : Net price (VNT) set by service A user
w_i : workload per month (Net) for service A user
n : number of service A users

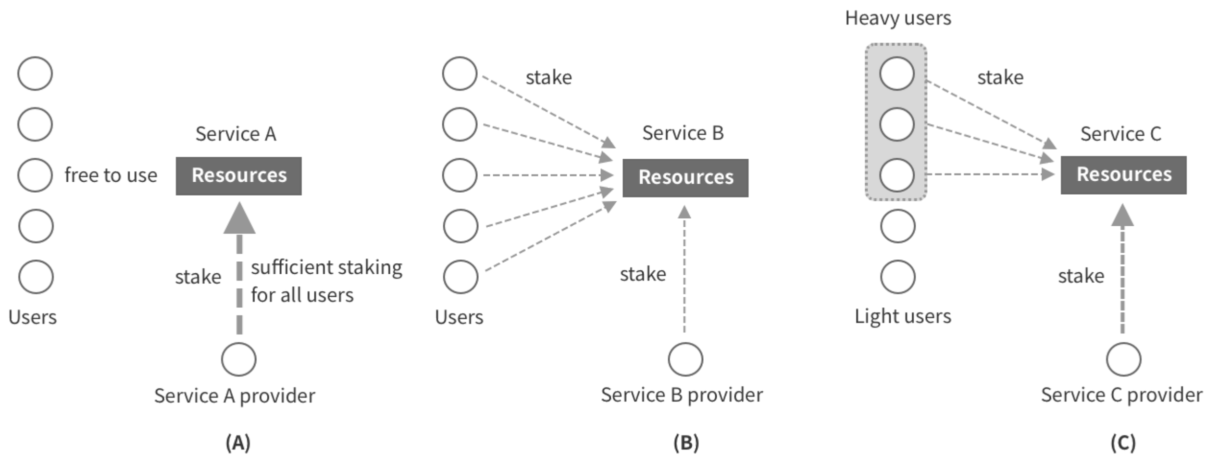

Figure 12. Various staking scenarios based on developer token funds or custom business models

5.4 Staking tokens to join as nodes

Any device can participate in the VANTA network as contributors. They will be working on various real-time networking jobs, verifying each other, generating blocks, and receiving rewards. Participating nodes can be divided into job tracker nodes, worker nodes, or verifier nodes, depending on their roles in the network.

Worker nodes that perform real-time networking jobs and participate in the consensus round are required to stake an amount of VNTs in proportion to its workload.

Verifier nodes act as work verifiers for real-time network processing and can participate by staking fewer VNTs than worker nodes. Therefore, in the VANTA network, smartphones and low-end PCs with low performance or battery-related issues can easily contribute as verifier nodes. In addition, when existing services migrate to VANTA's network and APIs, or when new services are launched on the network, the number of users participating in the network increases. These users' devices can easily contribute to the reliability of the network by participating as verifier nodes.

5.5 Burning Tokens as Fees for Unstaking

Developers must stake VNT tokens to run their services on VANTA. Depending on the developers and their policies, participants/users may be required to stake VNT tokens as well. When staking and unstaking tokens to purchase a workload, VANTA generates a 2% fee, and the entire fee generated is immediately burned.

Staking and unstaking of VNTs may occur when the Net price required for job processing changes. When a developer stakes VNTs, the developer sets the Net price, and the Net price may change depending on the market situation. If the price set at staking time for the workload is too low at execution time and the value of the job is too low, the priority for that workload may be lowered. This may result in a delay in service operation, or nodes may not process that task at all. If the Net price is too low compared to the price at the staking point, the developer may want to restake with a low Net price.

Also, if service users generate a job worth higher than the total workload allocated by the developer, the nodes in the network will not process the job if the workload per purchase is fully used. In this case, the developer will have to stake additional VNTs to gain additional workload capacity.

For instance, when staking is required by participants to use a service, the number of new VNT tokens staked will increase as the number of participants increases.

Eventually, as the ecosystem expands, staking and unstaking behavior will occur more frequently, and the burning rate of the entire VNT token supply will also increase.

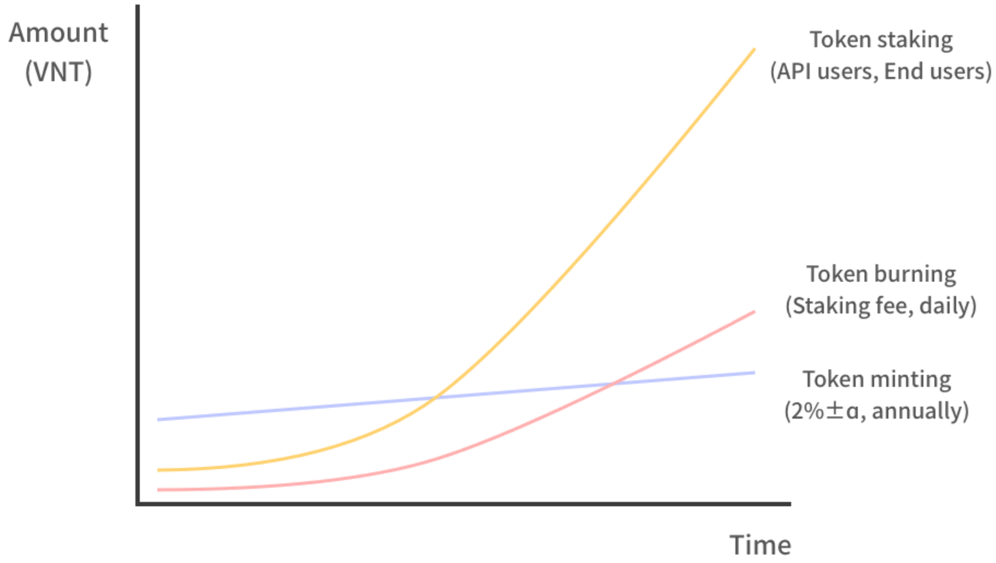

Figure 13. Cryptoeconomics graph

6. VANTA Architecture

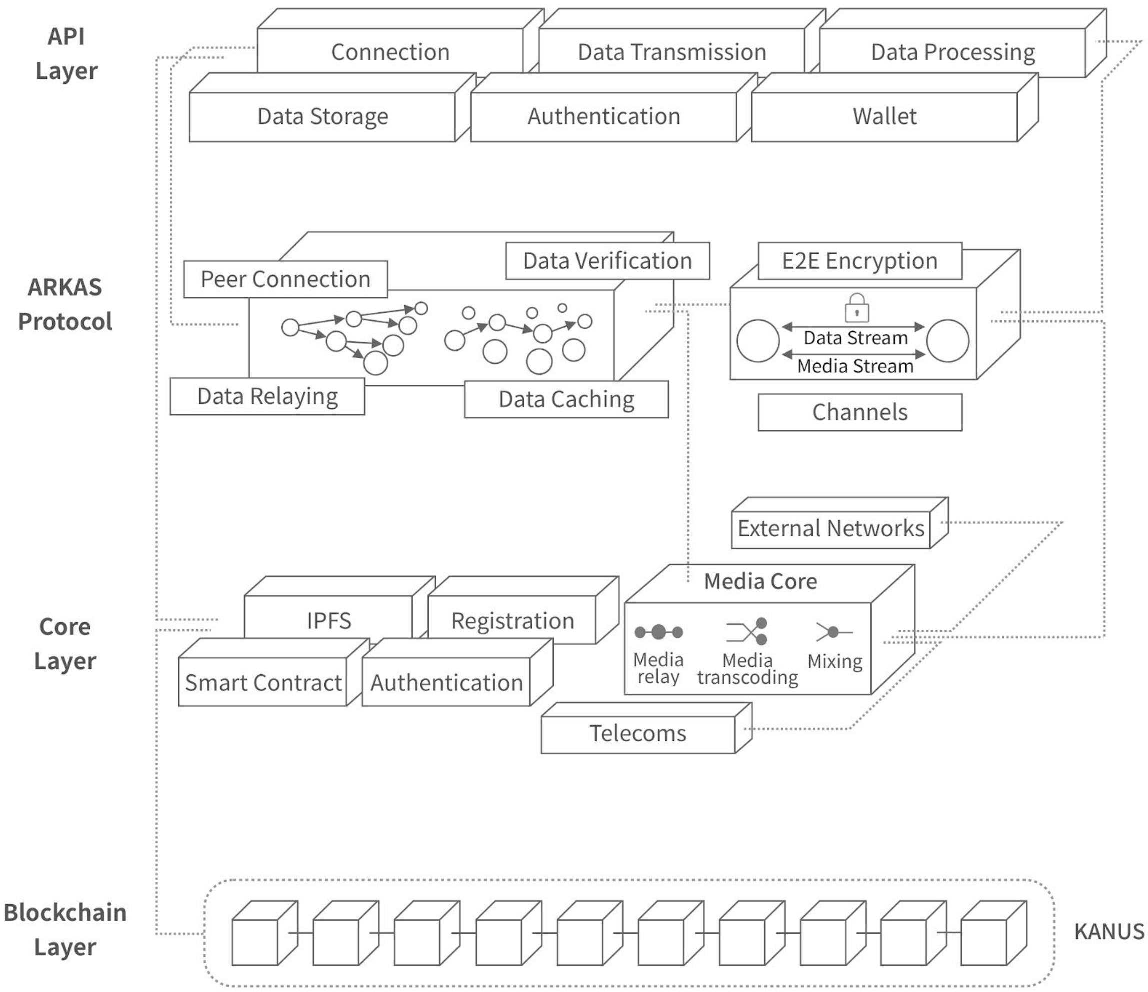

Figure 15. Architecture

7. Use cases

Figure 16. Use cases

VANTA is a platform blockchain to create intelligent networks optimized for real-time communication. For individuals, VANTA can be used to solve real-life problems. For developers, VANTA can be used to create various services that will improve the solutions of those real-life problems. As more devices become connected through the network, more services will be developed for the VANTA ecosystem. The VANTA team is already collaborating with companies that will use VANTA to create diverse business opportunities.

VANTA will allow individuals and corporations to develop real-time communications, games, broadcasting, IoT-related services, and collaborate at low costs. Specifically, universities, hospitals, companies, and public institutions can easily implement private networks in the form of an on-premise private blockchain. It will be easier for services to achieve real-time networking with other services if they also use VANTA's intelligent network protocol, which will result in the expansion of businesses. We will now look into more detail about how VANTA can be used in specific industries.

7.1 Communication

One of the key areas in which VANTA can be integrated is communication. Once corporations begin utilizing the functions in developing their services related to communication, the possibility of widespread usage in this sector will become significant. Customized forms of real-time messenger services can be developed for corporations to use as a method of sending and receiving messages and files, in addition to voice and video calling. A differentiating factor in VANTA is that these functions will operate in real-time. VANTA API can be used to easily create communication services that provide both direct and group chat with voice/video call services. For instances where privacy and real-time communication are critical, such as social dating services, overseas travel reservation services, as well as O2O services that require direct communication between buyers and sellers, these functions can be quickly added. By bringing in the communication happening outside of these services, not only will VANTA be competitive but will gain insight by collecting user data through legitimate means without violating a user's privacy. End users can use the decentralized communication service safely.

Communication services like WhatsApp, Uber, and Airbnb are using centralized API services like Twilio to incorporate communication capabilities into their services. Twilio had around 57,000 corporate customers in 2018, which was a 32% increase compared to 2017. Demand in this area is steadily increasing - Twilio's 2018 sales are growing to be $585 million USD.

7.2 Video streaming (Live & VOD)

Because VANTA is available for use by developers and strategic partners, anyone can develop a P2P-based, decentralized video streaming service that can provide real-time networking between participating devices. This means that it is possible to efficiently deliver high-quality, seamless video streams to the world at low cost. Therefore, using VANTA can lead to more content production because the cost of service development and operation is greatly reduced. Additionally, the costs saved can be reinvested with the content creator or supplier. Live video streaming can be used for online lectures, broadcasting, sports, and game relaying. VANTA will create the next generation video streaming business that will allow Video on Demand (VoD) services, where various content such as movies, entertainment, and music can be produced and supplied.

7.3 Internet of Things

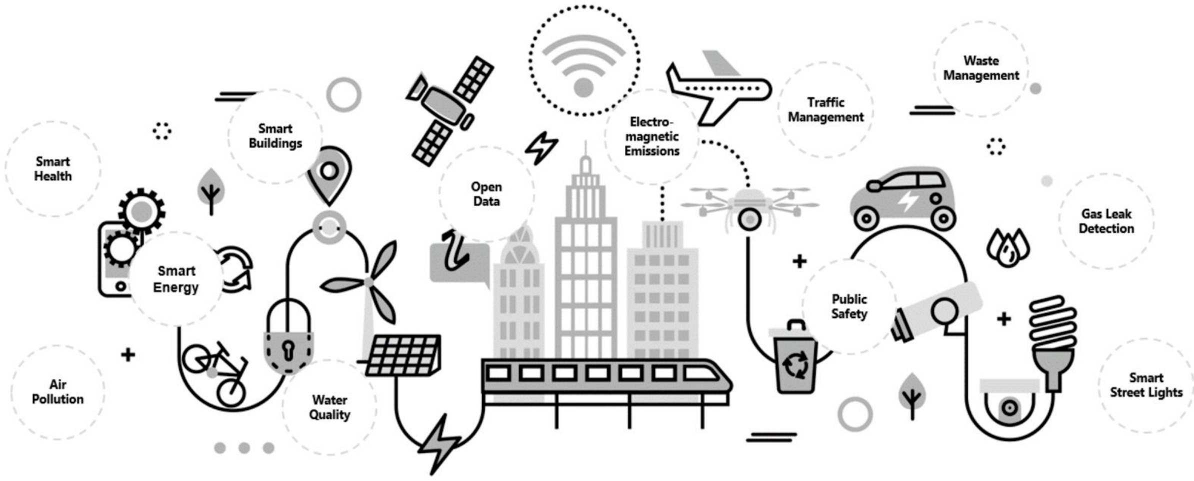

Figure 17. Internet of Things

Because VANTA is a network in which each peer is connected organically, directly connects, and processes data depending on the environment and performance of each other, it is well suited for seamlessly connecting many IoT devices that are scattered everywhere and transferring data. In addition, IoT devices such as smart refrigerators, smart TVs, and smart cars will participate in the VANTA network as work nodes, which will greatly improve the processing performance of the VANTA network.

Many devices can be developed based on VANTA, including processing of CCTV data, data from air pollution or vehicle density measurement sensors, data from sensors of various devices in industry which are distributed in each area, and IoT-related services that can automatically exchange data required between devices.

7.4 Games

VANTA is also applicable to real-time, multiplayer-based games. Generally, in a multiplayer game in which three or more players participate, a game data relay server is indispensable for delivering game data to and between all the players. Developing a multiplayer-based game requires client and server development. In addition, separate game servers need to be operated and managed to provide stable game services. It is therefore necessary to apply the multi-server model considering the various server failure situations that may occur during operation, which means that a lot of costs and development manpower are required for game development.

Through the P2P-based real-time data transfer function provided by the VANTA Network, a multiplayer game without the need of additional back-end infrastructure setup is possible. The developer may effectively share and synchronize game data generated from each player to the entire devices that play the game through the VANTA SDK.

The VANTA network, which includes a large number of peers, will enable more stable multiplayer game services in various network situations.

8. Ecosystem & Business Development

The overall value of the blockchain industry and businesses is increasing. Even though the overall market capitalization of cryptocurrencies can fluctuate greatly, global research groups, financial advisors, and various media channels are forecasting additional growth in blockchain technology's business value

For example, Gartner forecasts that the total market value of blockchain-related businesses will grow to more than $ 176 billion USD by 2025 and will reach more than $ 3.1 trillion USD by 2030. Also, many believe that by 2030, blockchain technology will be implemented in several major government agency systems. Personal information, including government records, credit history, educational background, and medical information, can be easily stored and transferred through blockchain technology. Thus, everyone can have access to useful information by moving away from the centralized social structure seen with the status quo. Blockchain technology is also expected to reduce corruption.

Nobody can be sure about how blockchain technology will advance or blockchain market growth, but it is important to note that blockchain technology will continue to evolve and will continue to grow in size as well.

Efforts to overcome the current limitations of centralized networks will lead to the advancement and growth of the blockchain technology industry. The VANTA platform that is aiming to decentralize real-time networking can be further developed through the global interest on such technologies and efforts in recognition for their demand. In addition, the VANTA team will continue to pursue sustainable development and ecosystem expansion of the VANTA Platform.

8.1 VANTA DApp Ecosystem Expansion

VANTA is a blockchain platform that is aiming to expand its blockchain ecosystem through collaborating with DApps to build on top of VANTA. By focusing on the specialties of real-time networking and allowing them to converge between different DApps, the VANTA team will encourage more individuals and corporations to participate in our ecosystem. In addition, through DApp development competition events targeted at universities and startups, we will promote creative real-time, networking-based DApps to enrich VANTA's ecosystem. VANTA aims to innovate the DApp ecosystem by making it easy to develop DApps that can be used in various fields, such as communications, entertainment, education, Online to Offline, travel, and finance, as well as enterprise-level DApps.

8.2 VANTA Consulting & Blockchain Customizing Strategy

Blockchains and decentralization networks are innovative technologies that are presenting a new paradigm and leading us into the future, and they may gradually replace centralized models found with the status quo. IT technology is rapidly evolving, and its speed is accelerating. However, the speed of those technologies actually being applied to our daily lives has not been fast. For example, IPv6, which is a more advanced technology than the existing and old IPv4 standard, is still taking a lot of time for mainstream adoption. The VANTA Team plans to support the migration of existing systems and applications to the VANTA Network by providing consulting services to allow customizable solutions for enterprise customers in existing industries.

1. PSTN: It is possible to enable communications between a VANTA user and a user outside of the VANTA network by supporting the interworking with the current communication network. In addition, the current PSTN line operators can create a new business model by providing PSTN to VANTA users at a low price through connection with VANTA.
2. SMS: VANTA users can send and receive SMS messages provided by the service provider.
3. VoIP: It supports interworking with IP-based devices such as IP phones, so it is possible to communicate through the VANTA network by using the current system as is.
4. Replacement of communication equipment: By introducing a private VANTA blockchain, it enables the replacement of current hardware / software / cloud-based communication devices such as PBX, SBC, and media gateway.

9. VANTA Team & Partners

9.1 VANTA Team

The VANTA team is specialized in telecommunications & networks, data processing, and blockchain. The team is capable of bringing mass adoption of the VANTA Network via partnerships with global enterprises.

9.2 VANTA Partners

CONNECT

- ORACLE
- aws partner network
- Microsoft
- orange™
- NAVER
- SEJONG TELECOM
- SK telecom
- SK broadband
- BSK Investment
- KODIT 신용보증기금 KOREA CREDIT GUARANTEE FUND
- TIPS KOREA TECH INCUBATOR PROGRAM FOR STARTUP

10. VANTA Token Distribution

The VANTA network consists of 56.2 billion VANTA (VNT) tokens. A total of 35% will be raised[DA1] via token sales. Ten percent of tokens will be given to the team who are core contributors to the VANTA Network. Most of the budget will be dedicated to developing performance optimization and further function development. The VNT tokens shall be distributed as the follows.

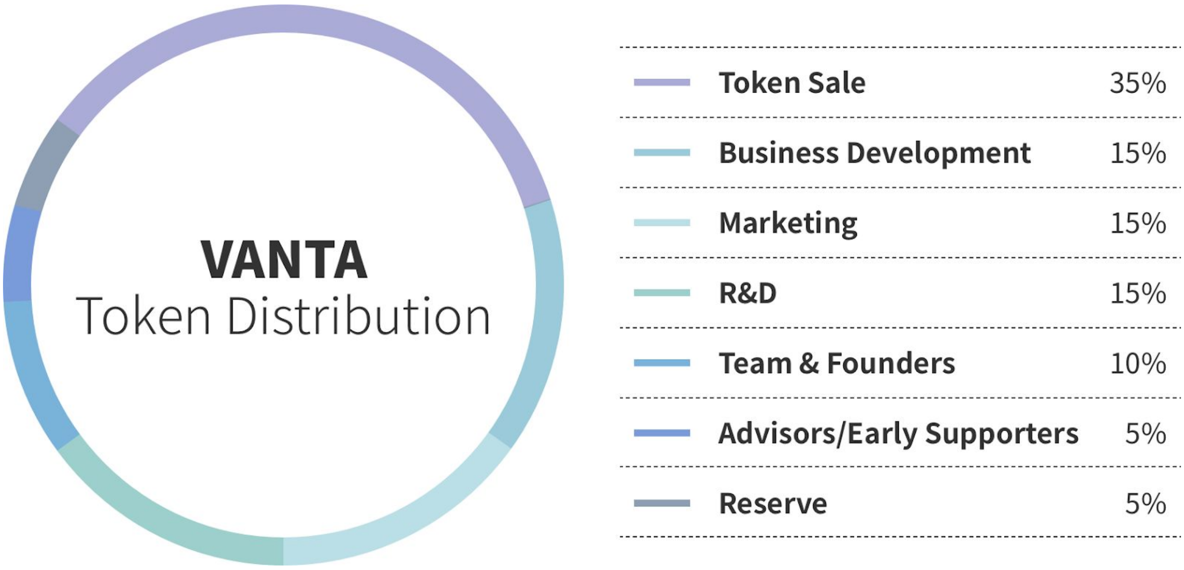

Figure 19. Token Distribution

References

[1] N. Magharei, R. Rejaie, and Y. Guo, “Mesh or multiple-tree: A comparative study of P2P live streaming services,” in INFOCOM, 2007

[2] Micali, Silvio; Rabin, Michael O.; Vadhan, Salil P. (1999). "Verifiable random functions". Proceedings of the 40th IEEE Symposium on Foundations of Computer Science. pp. 120–130.

[3] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson. “RTP: A Transport Protocol for Real-Time Applications”, July 2003, https://tools.ietf.org/html/rfc3550

[4] P. Jones, P. Ellenbogen, N. Ohlmeier. “DTLS Tunnel between a Media Distributor and Key Distributor to Facilitate Key Exchange draft-ietf-perc-dtls-tunnel-04”, October 20, 2018, https://tools.ietf.org/html/draft-ietf-perc-dtls-tunnel-04

[5] C. Jennings, P. Jones, R. Barnes. “SRTP Double Encryption Procedures draft-ietf-perc-double-10”, October 17, 2018, https://tools.ietf.org/html/draft-ietf-perc-double-10

[6] M. Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman. “The Secure Real-time Transport Protocol (SRTP)”, March 2004, https://tools.ietf.org/html/rfc3711

[7] R. Stewart, Ed. “Stream Control Transmission Protocol”, September 2007, https://tools.ietf.org/html/rfc4960

[8] E. Rescorla, N. Modadugu. “Datagram Transport Layer Security”, April 2006, https://tools.ietf.org/html/rfc4347

[9] Ontology, “A new high-performance public multi-chain project & a distributed trust collaboration platform”, 2018, https://ont.io/wp/Ontology-technology-white-paper-EN.pdf

[10] Castro, Miguel, and Barbara Liskov. "Practical Byzantine fault tolerance." operating systems design and implementation (1999):173-186.

[11] Ethereum Foundation. Ethereum, 2016. https://www. ethereum.org/.

[12] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich. Algorand:Scaling Byzantine Agreements for Cryptocurrencies. Cryptology ePrint Archive, Report 2017/454, 2017.

[13] Research and Markets, “Video Streaming Market by Streaming Type - Global Forecast to 2021”, May 2016, https://www.researchandmarkets.com/reports/3715076/video-streaming-market-by-streaming-type-live

[14] Cisco, “Cisco Visual Networking Index: Forecast and Trends, 2017–2022”, November 26, 2018, https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html

[15] Statista, “Size of the global Internet of Things (IoT) market from 2009 to 2019 (in billion U.S. dollars)”, August 2015, https://www.statista.com/statistics/485136/global-internet-of-things-market-size/

[16] Gartner, "Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016", February 7, 2017, https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

[17] BMI Research, “Towards 2050: Megatrends In Industry, Politics And The Global Economy, 2018 Edition”, April 2018.

[18] Gartner, Forecast: Blockchain Business Value, Worldwide, 2017-2030, March 2017, https://www.gartner.com/doc/3627117/forecast-blockchain-business-value-worldwide

Disclaimer

This document is a whitepaper setting out the current and possible future development of the VANTA network Token (“VNT”) and VANTA.

The scope of this disclaimer includes but is not limited to the following:

1. This whitepaper is for informational purposes only and does not constitute an offer or solicitation to sell shares or securities in VANTA or any related or associated VANTA. Any such offer or solicitation would only be made by a confidential offering memorandum and in accordance with applicable securities and other laws. None of the information or analyses presented are intended to form the basis for any investment decision, and no specific recommendations are intended. Accordingly, this whitepaper does not constitute investment advice or counsel or solicitation for investment in any security. This whitepaper does not constitute or form part of, and should not be construed as, any offer for sale or subscription of, or any invitation to offer to buy or subscribe for, any securities, nor should it or any part of it form the basis of, or be relied on in any connection with, any contract or commitment whatsoever. Any information included in this document, such as the VANTA ecosystem, should not be copied, modified, and distributed illegally without prior consent from the VANTA team;

2. Please consult your professional financial, investment, and tax advisers before making any investment in VANTA initial coin offerings. The VANTA Team and VANTA does not provide investment or financial advice. This whitepaper does not constitute any relations between the buyer and the seller;

3. VNT are not an official or legally binding investment of any kind. Due to unforeseen circumstances, the objectives outlined in this whitepaper, may be altered. Despite the fact that VANTA intends to implement all the points outlined in this whitepaper, all persons and parties involved in the purchase of tokens do so at their own risk;

4. This whitepaper includes certain estimates provided by VANTA with respect to the future performance of VANTA. Such estimates reflect various assumptions by the directors concerning the future performance of VANTA. These assumptions may or may not prove to be correct. No representations are made as to the accuracy of such assumptions or the estimates based thereon;

5. VNT are utility tokens that provide access to incentives, rewards system, and exchange data within the VANTA platform. Furthermore, VNT should not be treated as securities, nor do they imply or promise any equity, ownership in, or profit sharing with any part of VANTA. VNT are non-refundable, are not for speculative investment, and they include no promise of future value or performance, on their own, or as a metric of VANTA success;

6. Cryptocurrencies and blockchain technology have been scrutinized by various regulatory bodies around the world. The functioning of the VANTA platform could be impacted by one or more regulatory inquiries or actions, including but not limited to restrictions on the use of cryptocurrencies;

7. This whitepaper shall not legally bind VANTA and its participants. The directors, officers, employees, and advisors of the VANTA shall neither warrant the accuracy and reliability of this whitepaper nor hold any responsibility thereof;

8. VNT do not provide the right to receive profit, income, or other payments or revenues attributable to VNT's acquisition, holding, management, disposal or redemption. Any right, interest, ownership, or privileges on the VANTA platform or any other property on VANTA can expire in whole or in part;

9. The risk of loss in trading or holding cryptocurrencies and tokens can be substantial. Therefore, you should carefully consider whether trading or holding cryptocurrencies is suitable for you in light of your financial condition. Forks and changes in the relevant network may result in significant and sudden changes to the value and/or usability of cryptocurrencies and tokens. VANTA is not responsible for such loss of value of cryptocurrencies and tokens and bears no responsibility for any loss incurred by you while using the VANTA platform or in any direct or indirect connection to the VANTA platform;

10. VNT are issued on the Ethereum blockchain. In this regard, any failure or incorrect operation of the Ethereum Protocol may disrupt the transaction network in unexpected ways;

11. Technologies related to blockchain networks are the subject of supervision and control by various regulatory bodies across the globe. VNT may become subject to regulation, including restrictions on the use or ownership of VNT, slow or limited functionality, or limited possibilities for VNT redemption;

12. Cryptocurrencies, including VNT and other associated and related technologies, are new and untested and outside of your or VANTA's control, and adverse changes in market forces or the technology, broadly construed, will excuse the nonperformance by VANTA, including temporary interruption or permanent termination of your access to the Platform Services;

13. Hackers or other groups or organizations may attempt to interfere with your account or the platform's performance in a number of ways, including, without limitation, denial of service attacks, Sybil attacks, spoofing, smurfing, malware attacks, or consensus-based attacks;

14. There is a risk that VANTA platform may unintentionally include weaknesses or bugs in the source code interfering with the use of or causing the loss of tokens and cryptocurrencies;

15. You are not eligible and you will not be able to purchase any VNT through its token sale if you are citizen or resident (tax or otherwise) of any country or state where the purchase of VNT or similar cryptocurrencies and tokens may be prohibited or the token sale is deemed to be noncompliant with the applicable laws and regulations of your country. Citizens or residents of countries where coin sales are restricted may be subject to penalties for the purchase of coins;

16. The publication, distribution, or dissemination of the VANTA whitepaper does not imply that the applicable laws of any jurisdiction, regulatory requirements, or rules have complied. VANTA and its respective past, present, and future employees, officers, directors, contractors, consultants, equity holders, suppliers, vendors, service providers, parent companies, subsidiaries, affiliates, agents, representatives, predecessors, and successors will not be liable for any damages of any kind, including, but not limited to, direct, consequential, incidental, special or indirect damages (including, but not limited to, lost profits, loss of revenue, or third-party loss whether foreseeable or otherwise,

trading losses or damages that result from the use or loss of use of the website) in tort, contract, or otherwise, arising out of or in connection with any acceptance of, or reliance on, the whitepaper or any part thereof by purchasers of VNT;

17. VANTA may amend, add, or delete any part of the whitepaper for any reason or at any time and will make public, as the case may be, on its website, blog, or otherwise, where any amendment, addition, or deletion is made;

18. This whitepaper and its contents are confidential and should not be distributed, published or reproduced in whole or in part or disclosed by recipient(s) to any other person;

19. VANTA may at any time, refuse the request of a token purchase where the participant, who wishes to be involved in the token transactions in connection with this whitepaper, provides insufficient, inaccurate, or misleading identity information, or the participant is suspicious of being a restricted participant;

In addition, there shall not be allowed any transactions with the fund involving coins or tokens attained from criminal gains such as drug dealing or for the purpose of money laundering or terrorism financing. Where any of Restricted Participants purchases tokens or makes a purchase with illegal and unauthorized funds and purpose, such transactions may be prohibited or restricted at any time, and the purchase of such tokens may be cancelled or invalidated;

20. This whitepaper and related documents may be translated into other languages, and the whitepaper in English shall be given priority in the event of conflicting interpretation.