GKAN

Whitepaper v1.0

CONTENTS

A. BACKGROUND

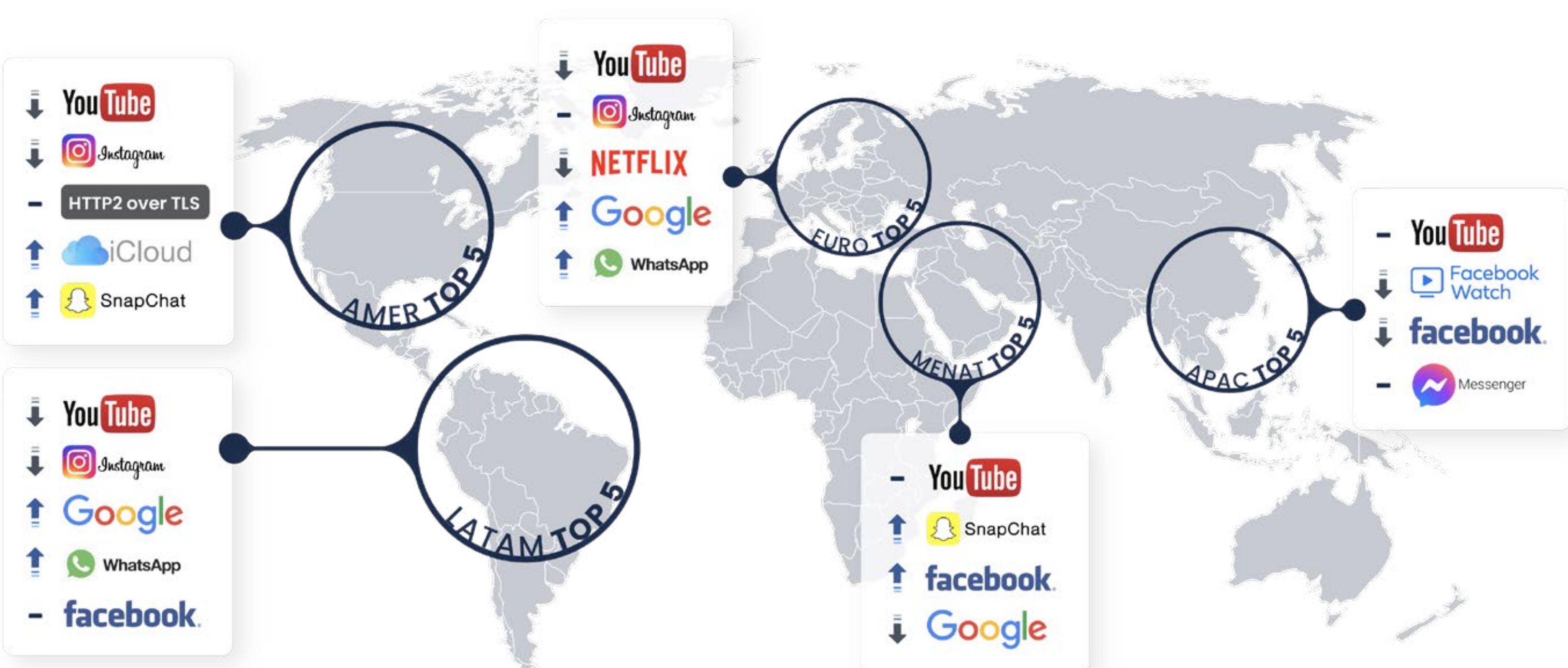
VIDEO STREAMING AND ITS DEVELOPMENT

In today's technological era, streaming has become the norm worldwide, both professionally and personally, to date has fallen short of the mark.

'Streaming' is the activity of listening to audio or watching video directly from the Internet. Thanks to the streaming revolution, people have access to a plethora of online entertainment resources anytime, anywhere, on any device connected to the Internet. Moreover, streaming technologies enable consumers of streamed content to overcome barriers in terms of geographical distance to build connections across geographies as well as widen their horizons.

The music industry first adopted streaming technologies. Consumers soon demanded the same streaming capabilities for movies, technologies, and video games. In the near future, VR and AR will follow. For now, video streaming is the most popular streaming medium and has witnessed phenomenal growth in recent years.

In fact, video streaming technologies have almost replaced broadcasting technologies such as cable and satellite because they offer viewers more significant benefits compared to traditional broadcasting services, for example, a more diverse source of content streamed on any electronic devices. The videos are of high quality and, most importantly, anyone can become a content creator and monetize this as an additional revenue stream. The 2019 Global Internet Phenomena Report cited that video streaming accounts for the highest percentage of total global internet traffic, with the figures for 2018 and 2019 at 57.7% and 60.6%, respectively, and is forecast to account for 82% of total internet traffic by 2022. Revenue obtained from video streaming witnessed a continuous increase from 2017 to 2020 and is expected to reach US$28,1 billion by 2023.



Such rapid development of the video streaming market has led to an increase in the number of video streaming services available. However, the available video streaming platforms, including the most popular ones such as Youtube, Netflix, Hulu, Twitch, are supported by only three predominant centralized content delivery networks (CDN)*: CloudFlare, Amazon Web Services and Akamai. With this imbalance, the global demand for CDNs has risen exponentially over the last few years.

CDN is a highly distributed platform of servers created to provide faster content delivery with minimal delays in loading web page content. This is achieved by reducing physical geographical obstacles between servers and users.

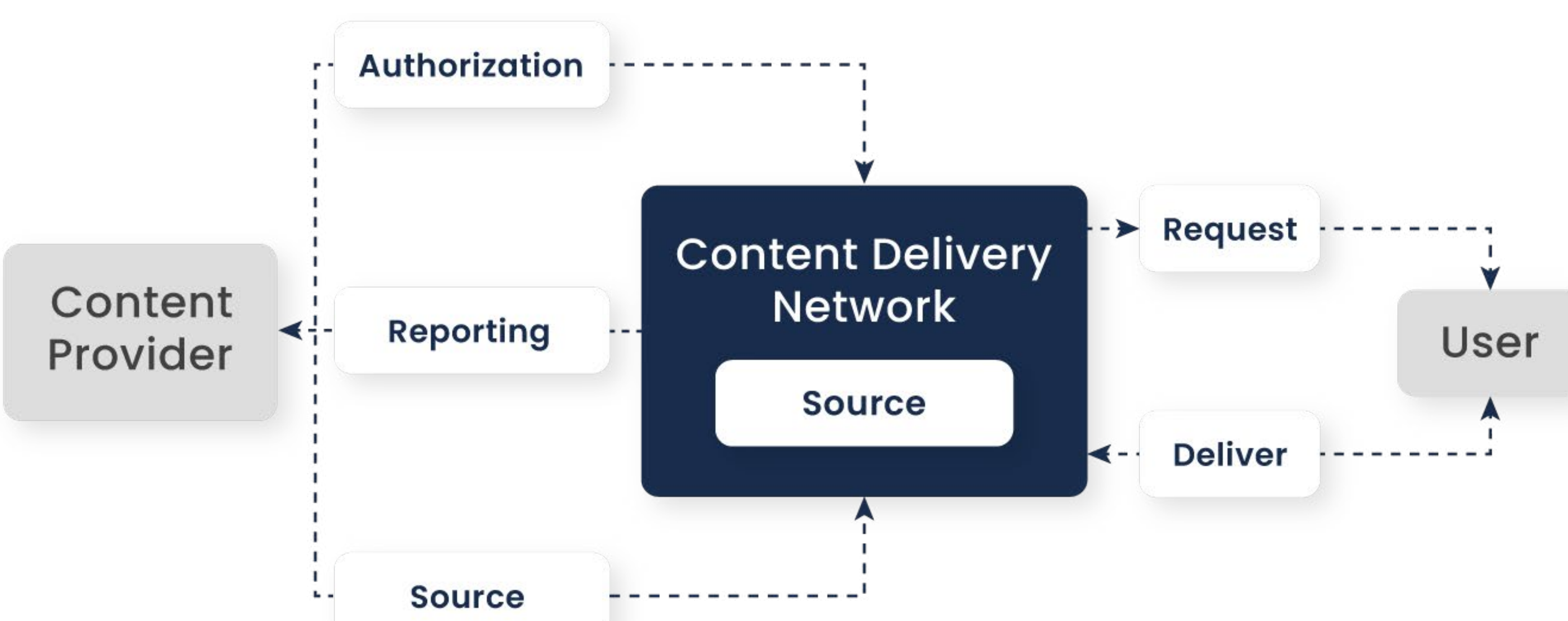


Figure. Model of a typical CDN

— CENTRALIZED AND DECENTRALIZED NETWORKS

A centralized network is built around a single server, called a 'Central server', and a number of less powerful workstations ('Client nodes') directly connecting to the Central server. In such systems, Client nodes will send their requests to the Central server and receive a response.

A decentralized network, on the other hand, is operated by several individual nodes that don't depend on a single central server. The final response is the total of the decisions of the individual nodes on processing requests.

Centralized

Decentralized

Today, conventional centralized networks are the major systems supporting streaming services globally due to their consistency and efficiency. While more video streaming platforms have launched to meet increasing demand, they incur tremendous expenses on construction, as well as operating and maintenance costs. Only a small number of prestigious corporations such as Amazon Web Services, Microsoft and Google Cloud are wealthy enough to develop their own centralized network infrastructure, but even this is in limited supply. As a result, the advantages of centralized network systems have been progressively outweighed by the disadvantages.

The main disadvantages of centralized networks are as follows:

- **Centralized networks can be censored, controlled, or even shut down.**

  If the only central server available was attacked by hackers, enterprises or governments or if client nodes lose connectivity due to some unique technical errors, abrupt failure of the entire system might take place.

- **Centralized networks have limited scaling possibilities.**

  These types of networks operate with 100% dependence on the only master server. The only way to scale the network is to supplement the server with more CPU/GPU cycles for more processing power, more space for storage and more Internet bandwidth.

  Even by increasing the resources of the server node, after a certain threshold, the performance will not rise correspondingly and as such is not a cost-effective measure in the long run.

- **Operations around only a single master can soon experience a bottleneck.**

Streaming services have been developing at a phenomenal rate and users can experience negative outcomes such as poor video quality, slow loading and buffering problems.

- **Centralized networks carry greater risk of data loss.**

  If the server node fails and there is no backup, data is lost.

- **Services delivered from centralized systems are expensive.**

  The high fees paid to corporations that provide cloud services eat into clients' profits and the revenue of content creators/streamers. A clear illustration for the main disadvantage in terms of high cost is YouTube - the most popular streaming platform today.

Decentralized networks, by contrast, provide the solutions for all aforementioned issues and offer many advantages over traditional centralized network systems.

Here are some benefits of decentralization:

- **There is no single point of failure.**

  In decentralized networks, individual nodes work independently. There is no single 'Central server' to control and handle all processes. As a result, it is impossible to shut down the entire network.

- **Decentralized networks can be infinitely scaled.**

  The more individual nodes that are added to the network, the more powerful the network becomes because a lot of new connections are established. The aggregate of resources, including spare processor cycles, storage and Internet bandwidth, would increase dramatically. Therefore, the likelihood of bottlenecks is extremely low.

- **The architecture of decentralized networks offers greater privacy for users.**

  Information is processed by a well-designed algorithm without the need to pass it to any third parties. This makes decentralized networks highly censorship-resistant and more secure against cyberattacks.

- **More autonomy and control over resources.**

  As each node controls its own behavior, it will have better autonomy, which leads to more control over resources.

- **Censorship is less likely to take place.**

  Governments have traditionally had the power to shut down their citizens' access to social media sites by stopping traffic going to the social media platform's central servers. By contrast, it is difficult for governments to censor traffic on a peer-to-peer network, where every single outbound packet being sent could be communicating with another peer on the decentralized network, who can then forward the message along.

- **There is potential for network ownership alignment.**
  In decentralized networks, the people who contribute value will receive ownership or an economic stake in the network, which becomes more valuable as the network grows.
- **Decentralized networks are more likely to be open development platforms.**
  Anyone can build their own tools, products, and services on top of decentralized networks. When more great products and tools are built, the networks will be rapidly widened, and thus business opportunities provided for individuals and companies will rise correspondingly.

Thanks to these various benefits, especially the cost advantage, interest has grown in decentralized networks. More video streaming platforms/applications have been developed and run on decentralized peer-to-peer networks instead of conventional centralized servers. Such platforms/applications are known as 'Decentralized Applications' or as 'dApps'. Currently, dApps are still in their infancy, with more than 3,000 built on Ethereum. Nevertheless, they are forecast to grow exponentially, with the market size being projected to reach USD 21,070.2 million by the end of 2025, according to a study carried out by Blockchain Examiner. The growth of DApps will give rise to the expansion of decentralized networks in the future.

B. GKAN STREAMING NETWORK

GKAN NETWORK ARCHITECTURE

'GKAN Network CDN' is a decentralized peer-to-peer CDN built through the connection of different nodes by a pre-designed protocol of the GKAN Network team. Nodes in the GKAN Network dCDN are categorized as HUB Nodes (a.k.a Satellite Nodes) and Edge Nodes.

GKAN *NETWORK OVERVIEW*

GKAN Network Edge Nodes

Edge Nodes are individual nodes with redundant resources that they can share in exchange for GKAN Network tokens. The monetization process will be determined based on two criteria: the Edge Node's level of contribution and commitment to our protocol.

Edge Nodes are allowed to choose whichever HUB Node to work with that they see as possessing high credibility. They can select as many HUB Nodes as they want to in order to gain more income sources. However, if

Edge Nodes are detected to be non-compliant with requirements listed in the contract agreed with the HUB Node, then, based on the nature and levels of violation, their payments will be partially/fully cut, or they may be permanently eliminated from the GKAN Network dCDN.

Any PC or laptop can become a Edge Node of GKAN Network dCDN simply by installing GKAN Network Edge Node Software. Edge Nodes can opt to handle a combination of one or more of the following: transcoding, storing and delivering.

There are a lot of aspects that must be taken into consideration when selecting which Edge nodes are suitable to store data, including: ping time, latency, throughput, bandwidth caps, sufficient disk space and geographic location.

– GKAN HUB Node

In the GKAN Network dCDN, there are plenty of nodes that hold the responsibility of controlling, assessing and monitoring other Edge Nodes to ensure the smooth operation over the entire network. They are called HUB Nodes.

The main tasks of HUB Nodes are to:

- deal with Edge Nodes on the clients' behalf,
- require Edge Nodes to provide Proof of Transcoding, Proof of Storage and Proof of Delivery in order to keep track of their compliance to the smart contract's terms and conditions,
- reward Edge Nodes after finishing the tasks requested by clients,
- preserve data when there is a lack of resources and
- store technical indexes of each Edge Node.

Most importantly, HUB Nodes are simultaneously technical and video segment indexers that know exactly the locations of segments among a great deal of Edge Nodes as well as the information relating to the storage and bandwidth properties of Edge Nodes.

To avoid duplication error, data controlled by one HUB Node will not be available in the remaining HUB Nodes. Multiple layers of ingress and egress are planned.

Each HUB Node contains the following core items:

- A complete node discovery cache
- A system that manages and authorizes accounts
- A system that stores Edge nodes' reputation, statistics, and audit records
- A service that fixes data
- A service that fulfills payment

HUB Nodes are being developed and will be released as open software.

— GKAN NETWORK OPERATION

In the GKAN Network dCDN, three major redundant resources that Edge Nodes share in exchange for tokens are CPU and/or GPU process cycles, Hard drive space and Internet bandwidth, which are used for Transcoding, Storing and Delivering video content (GKAN Network CDN's three main tasks), respectively.

- **Transcoding video content:** This task transfers the original video resolution into different profile resolutions. Different types of electronic devices have their own requirements in terms of codec, colorspace and resolution; and video content can only be consumed if video properties satisfy all three requirements.
- **Storing video content:** Transcoded videos are moved into storage to make room for other videos being encoded. Videos uploaded onto the Internet are encoded once and stored until there is a request from viewers.
- **Delivering video content:** This task delivers video segments (a.k.a. chunks) to users upon request.

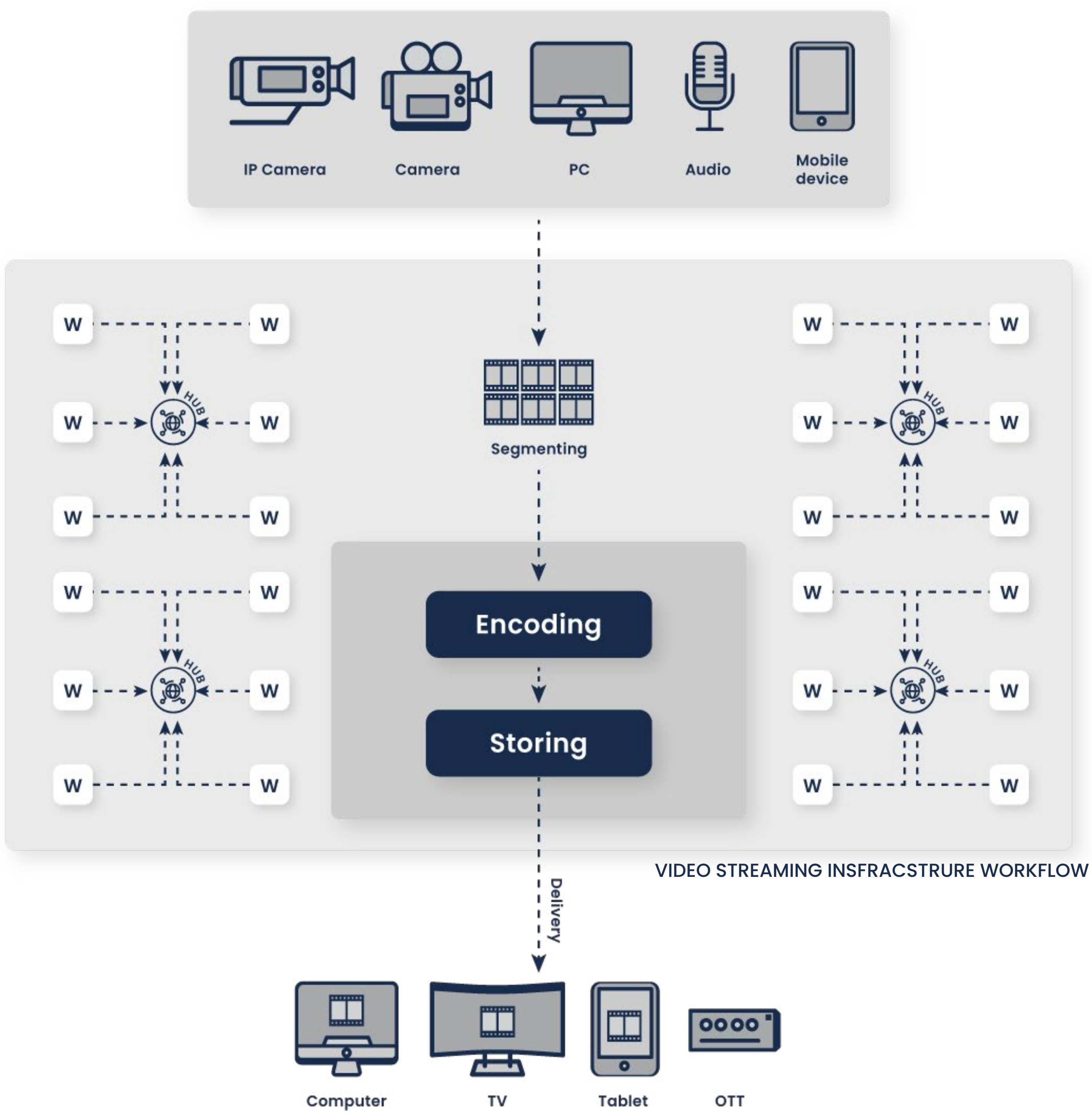
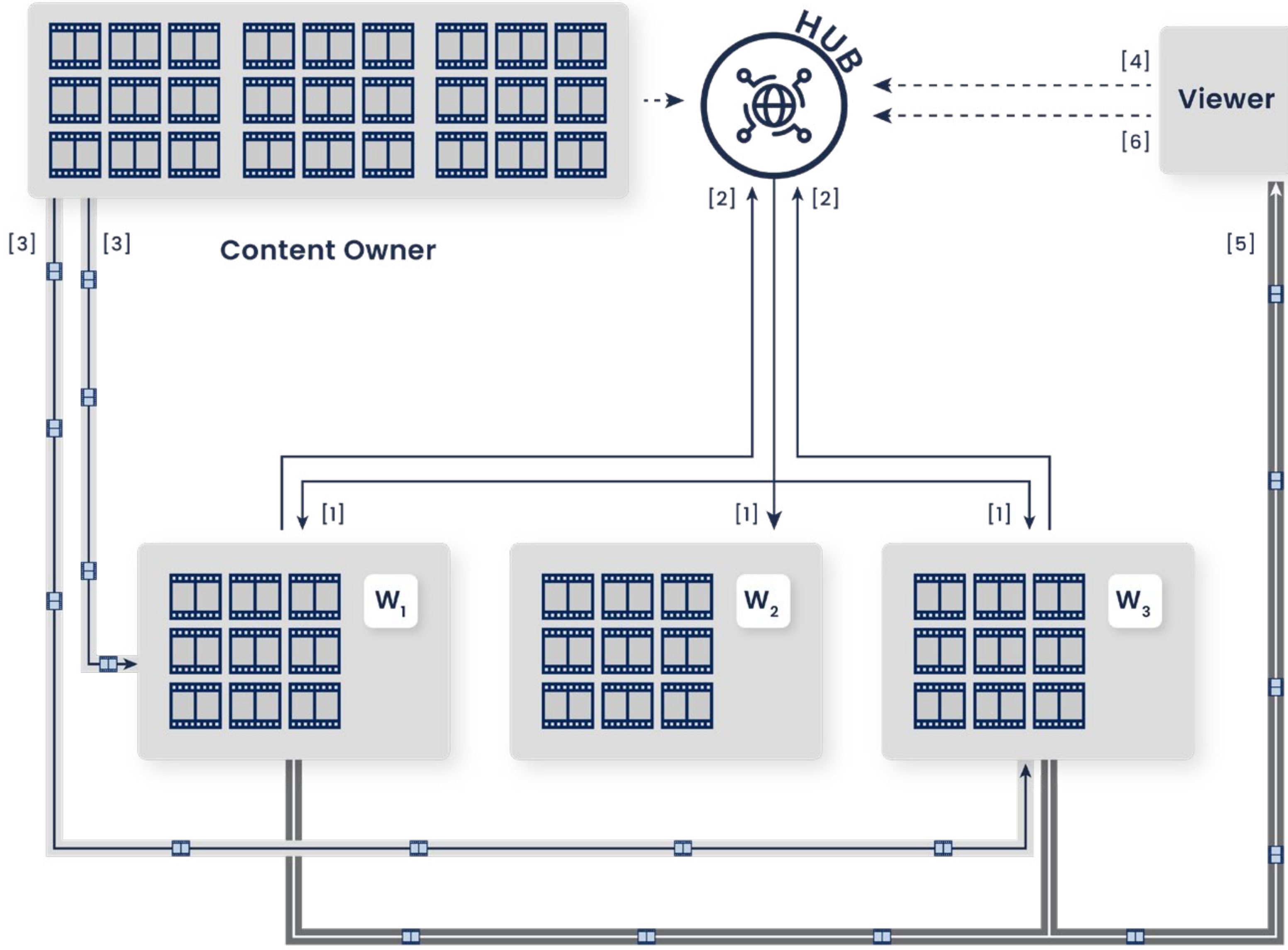


Figure. Overall workflow of GKAN CDN



[1]. **HUB** assigns storage tasks for Edges

[2]. **Edges** approve & sign the storage contract

[3]. **Content Owners** upload video segments to Workers

[4]. **Viewers request** the HUB for Workers to store video chunks

[5]. **Viewers** ask Workers to deliver content

[3]. **Viewers** acknowledge the delivery to the HUB

The detailed operation procedure of the GKAN Network dCDN for video streaming is shown in Figure. The procedure undergoes the following steps:

- Original video content held by the Content Owners (COs) is first split into multiple smaller segments, wherein the checksum of each segment is calculated by the GKAN Network SDK.
- Next, HUB Nodes will determine which Edge Nodes can satisfy the COs' requests (about the type, size, relocation factor of files, duration to store files and the COs' budget) and will connect qualified Edge Nodes to the COs.
- If the COs and Edge Nodes reach a consensus on collaboration, a contract will be sent to GKAN Network Blockchain.
- Thereafter, the COs upload their original video content segments to the Edge Nodes for transcoding.
- The transcoded segments will then be checked for accuracy and completeness compared to their original chunks by the COs by running the **Proof of Transcoding (PoT).**

- All original and transcoded segments will be stored at Edge Nodes that handle the storing task if no errors in the transcoding process are detected. Otherwise, all the work will be reassigned to other Edge Nodes. By nature, video segments could be stored permanently unless they are deleted, which seems to be inconvenient and a waste of resources. Therefore, each video segment will be attached with a 'lifespan time' and automatically deleted after their expiration dates.
- After finishing the storage task, Edge Nodes will provide a **Proof of Storage (PoS).**
- When viewers have a request to view a certain video, HUB Nodes will lead them to Edge Nodes storing segments of that video to receive the complete content. Each segment can be stored in different Edge Nodes. However, HUB Nodes will only recommend to viewers the most optimal Edge Nodes in terms of geographical distance and price.
- After content is delivered, **Proof of Delivery** will be sent back to the HUB Node for verification that the viewers have already received the content. Edge Nodes can then receive their tokens.

Please note that the term 'Content Owners' used in this section refers to providers of video streaming platforms that build their service on top of GKAN *Network dCDN, and 'Viewers' refers to those using the platform of the 'Content Owners' to watch videos.*

1. Proof of Transcoding

Transcoding is the process converting a digital source video file into different formats to match different device requirements. H265, H264, VP9, and VP8 are currently the most utilized codecs because they achieve high degrees of compression. High-quality compression is essential because it reduces video size, while the quality of the video remains nearly consistent. Smaller video files require less storage, which makes it easier to distribute them across many platforms and makes the end-user playback experience seamless.

This section will elaborate on how Edge Nodes receive the transcoding task and how to prevent them from cheating (Figure). To start with, COs who want to have their videos transcoded will send their request and payment to HUB Nodes of GKAN Network dCDN. Next, the HUB Node assesses which Edge Nodes can handle the COs' request and assigns the task to them. Edge Nodes have the right to accept or refuse the task assigned by the HUB Node as well as to freely choose which video segments to handle.

If they agree to carry out the task, the COs will upload their video segments onto corresponding Edge Nodes and wait to get transcoded segments from them. After that, the COs will run a PoT to check whether all original segments and their transcoded counterparts are similar in terms of content. PoT is an algorithm used to check whether all segments are precisely transcoded.

The following process illustrates this clearly and compares an original segment (V1) and its transcoded segment (V2) (Figure):

- Firstly, N indexes (index is a numerical representation of a frame's position in a video segment) are randomly selected **(Indexes = {idx1, idx2 ..., idxN}**, with N, ranging from 0, to the total number of frames contained within V1 and V2).
- Next, N frames from V1 (F1 variable) and N frames from V2 (F2 variable) whose positions match the indexes determined at the previous step are picked out.
- Finally, each pair of frames selected from V1 and V2 is computed for the S Score.

This could be displayed as:

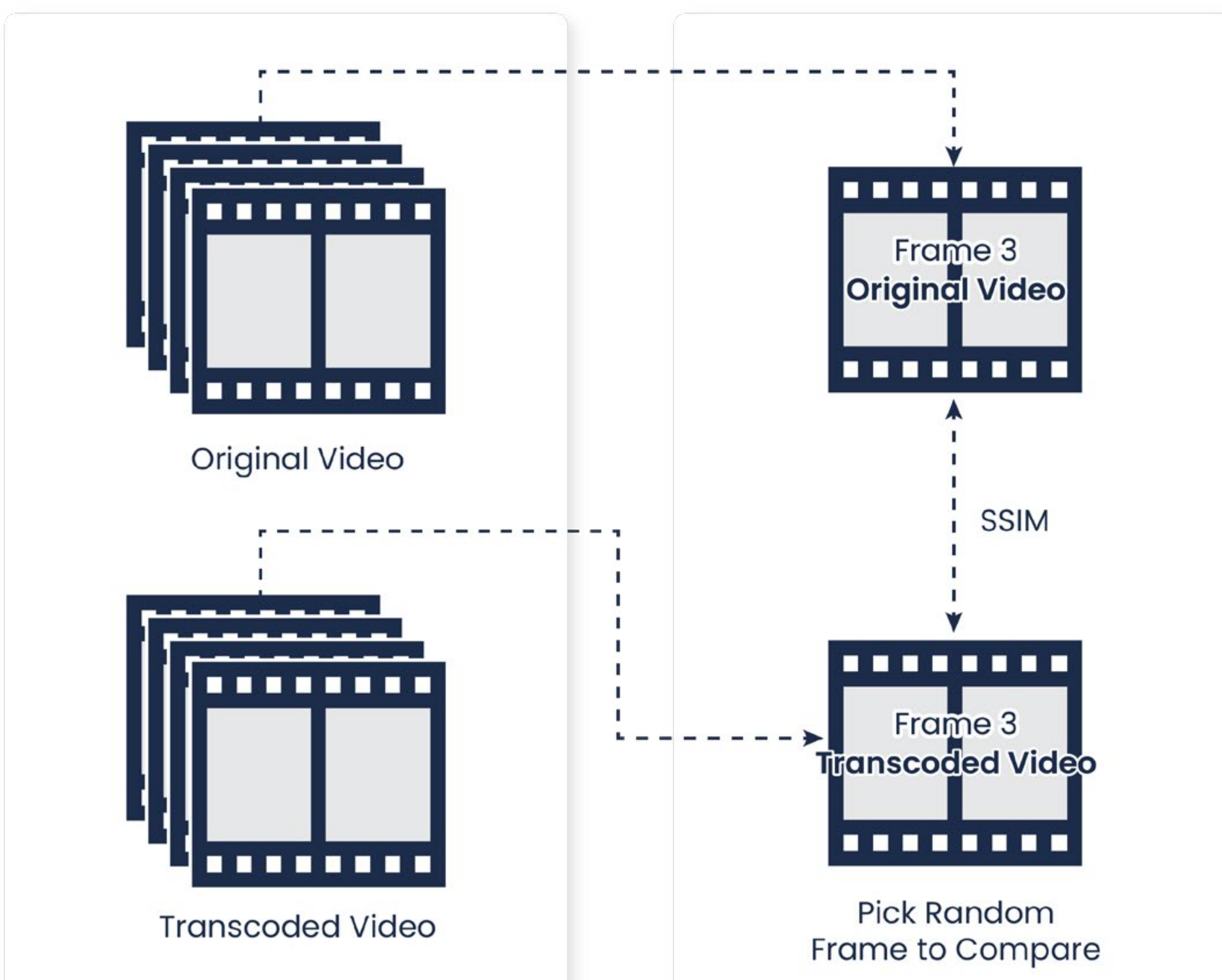
For i in (1..n):

S = S {ssim(F1[i], F2[i]) } (ssim stands for Structural Similarity Index)

By SVM (Support Vector Machine) categorizing algorithm, SSIM and

other indexes are simultaneously used to evaluate the similarity between V1 and V2

Score = svm (S , size(V1), bitrate(V1), size(V2), bitrate(V2))



After the COs run PoT, there are 2 possible outcomes that Edge Nodes will encounter:

- If the COs have no complaints in **all** segments, the entire payment from the escrow account will automatically be sent to the Edge Nodes' GKAN
Network wallet within a certain period of time after they return the transcoded segments to the COs.

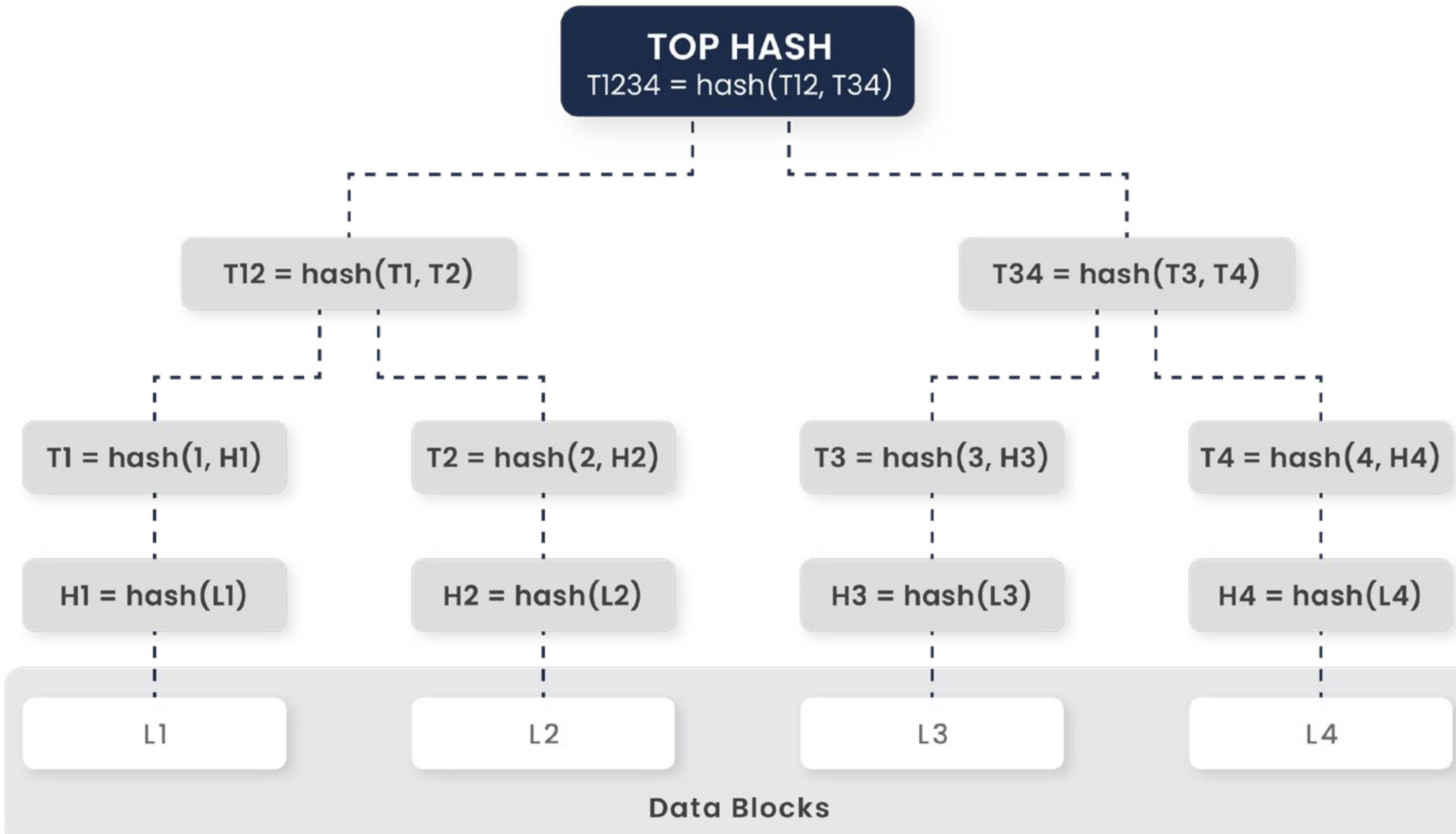
- If the COs detect any flaws in any segments from running the PoT, they must submit both unqualified/broken transcoded segments and the PoT to the HUB Nodes within a certain period of time after the Edge Nodes return the transcoded segments to the COs in order for the HUB Nodes to re-verify these flaws.
    - If these flaws are judged to be the mistakes of a Edge Node, the Edge Node not only cannot receive the rewards for this task but is also given further penalty, depending on the severity of the flaws. For example, they would be assigned fewer tasks moving forward, their prestige on GKAN Network dCDN would decrease, or they might be kicked out from the network. Thereafter, the uncompleted tasks will be reallocated to other Edge Nodes
    - By contrast, Edge Nodes are still able to receive the whole payment from the escrow account.

2. Proof of Storage

It is a fact that storing data brings risks such as data loss, data hacking, data breach or broken data. This is also the case for the task of storing video segments handled by GKAN Network dCDN's Edge Nodes, which might affect the entirety and accuracy of video content. Therefore, before delivering video content to viewers, the HUB Nodes must check the entirety of each video segment stored by the Edge Nodes to ensure the input content and ready-to-be-delivered content are ubiquitously consistent.

In the GKAN Network dCDN, the video segment verification process is designed based on the Merkle root tree principle and put under the supervision of the HUB Nodes. Instead of checking all segments, Merkle root minimizes the amount of video segments being sent back and forth over the Internet by comparing the hashes of these segments. This is obviously a much faster, more resource-efficient and secure solution because hashes of files are much smaller than the actual files themselves. For instance, the hash of a 2,000,000-byte file is around only 544 bytes in size.

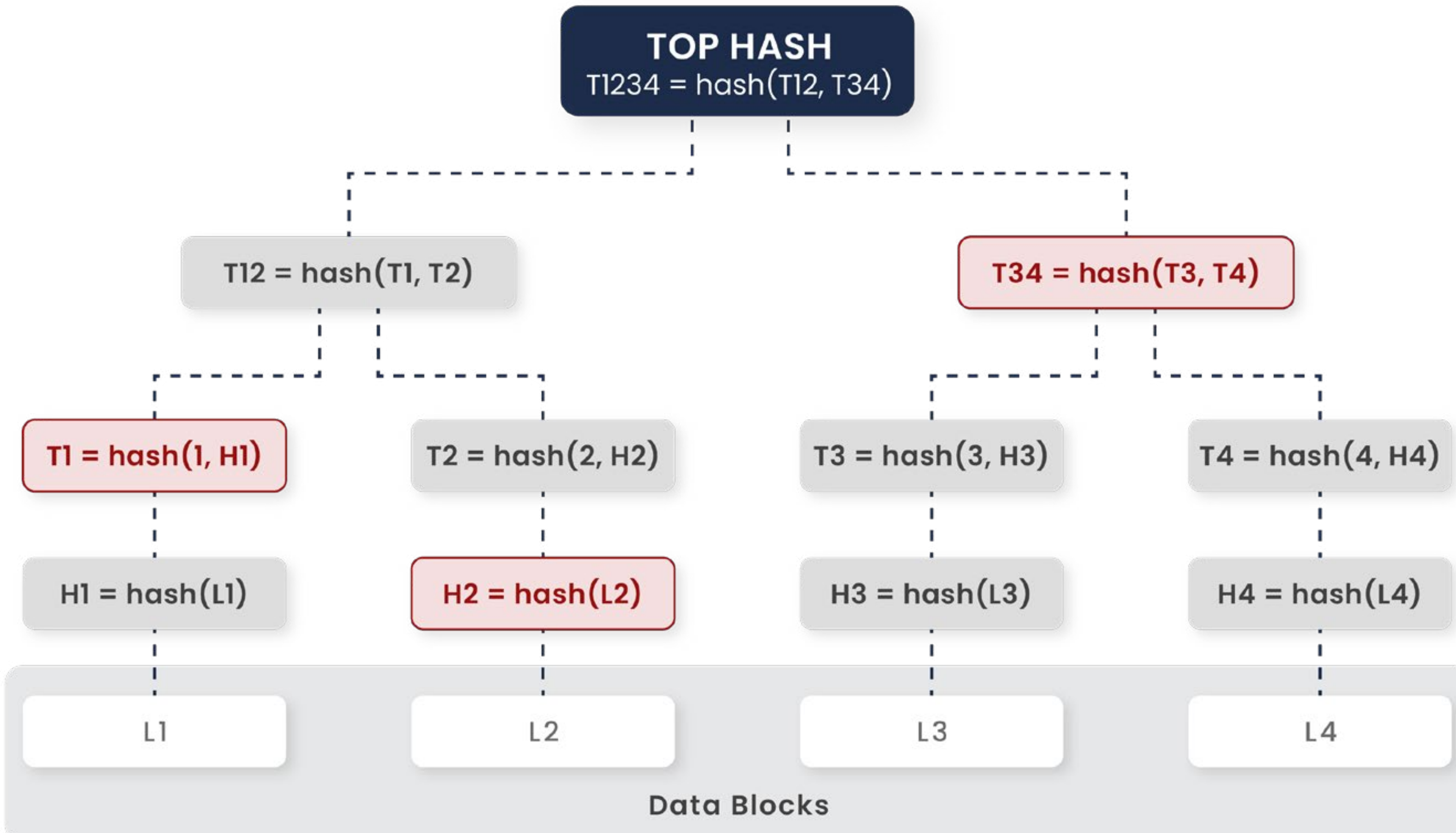
A Merkle tree is a hash-based data structure that is a generalization of the hash list. It is a tree structure in which each leaf node is a hash of a block of data, and each non-leaf node is a hash of its children. Typically, Merkle trees have a branching factor of 2, meaning that each node has up to 2 children. Currently, their main uses are in peer-to-peer networks such as Tor, Bitcoin, and Git and of course, the GKAN Network dCDN.



The illustration for a typical Merkle root in the GKAN Network dCDN is shown in Figure. Instead of only 4 blocks shown in Figure, in reality, a video segment contains n blocks, in which n is computed so that the size of each block ranges from 32 to 64 bits. Via gradual pairing, we will finally achieve a TOP HASH, which is unique for one video segment. In other words, any changes in any blocks or any block disorders of a video segment will lead to a totally different TOP HASH.

Before assigning the task of storing a certain video segment to a Edge Node, the HUB Node will first compute and then save the TOP HASH of that video segment into its memory. This TOP HASH is later used to check whether there is any discrepancy between the original and the stored video segment.

However, if Edge Nodes compute TOP HASHES by themselves and send them back to the HUB Node for verifiction, the verification process cannot ensure 100% reliability. This is because Edge Nodes might compute and save the TOP HASHES as soon as they receive the video segments but then delete all segments or make some changes to these segments. Consequently, the video segments no longer stay the same although TOP HASHES are exactly the same. To avoid this risk, HUB Nodes will also take charge of computing these TOP HASHES of stored video segments.



In the GKAN Network dCDN, a complete Merkle root tree of a video segment which is being stored in Edge Nodes could be constructed from different hashes, with one hash per level being sufficient (Figure). From this tree, the HUB Node will get the final TOP HASH, whose size is log2(X) (X is the number of nodes in the tree).

To do this, the HUB Node will challenge the Edge Node by requesting them to provide random hashes. The block index and location of hashes requested may vary significantly. The HUB Node's request will be coupled with a deadline to eliminate the risk that the Edge Nodes might delay or forget to submit their PoS. If a Edge Node fails to submit the proof within the timeframe given, the storing contract will be cancelled and the Edge Node will be penalized.

3. Proof of Delivery

Delivering content to viewers is the final step in the GKAN Network dCDN. Theoretically, after video content has been delivered to the viewers, Edge Nodes will be rewarded with GKAN Network tokens for completing the assigned tasks. However, in reality, there may be flaws in the process. For example, viewers may not inform the HUB Nodes that they have already received the video content and thus the Edge Nodes are not rewarded; or Edge Nodes can cheat by creating unlimited fake viewers to earn digital tokens. As a result, it is vitally important to strictly control this step with a Proof of Delivery mechanism.

The process of delivering content to viewers in the GKAN Network dCDN is summarized in Figure. Initially, viewers have to send their requests to the HUB Node. After the viewer's request has been approved, the HUB Node will connect the viewer to contact the Edge Node storing the requested content. In order to get the desired Edge Nodes, viewers have to continue sending their requests coupled with a digital signature to the Edge Nodes. This signature acts as evidence which the Edge Nodes can use to claim their tokens from the HUB Node after delivering the content to the viewers.

All transactions between viewers and Edge Nodes are conducted within the ECDH (Elliptic-curve Diffie–Hellman) session - a secure contact channel between 2 parties that absolutely avoids information leaking or hacking. Please note that ECDH sessions can be activated only if viewers are carrying a black box of GKAN Network to ensure that they are real and trusted viewers. Via the ECDH session, the viewer will inform the HUB Node and, therefore, the Edge Node can successfully claim their GKAN Network reward using the initial digital signature of the viewer.

BENEFITS OF THE GKAN NETWORK DCDN

- **The GKAN Network dCDN is a most cost effective solution than centralized CDNs.**

The GKAN Network dCDN's mesh network of resources, by nature, are spare resources contributed by individual nodes in the network, while centralized CDNs have to spend an enormous amount of money building and maintaining their physical servers. Compared to centralized CDNs, the overhead costs of the GKAN Network dCDN are significantly lower, which consequently helps its clients alleviate their financial burden, or, in other words, clients can earn additional revenue through the GKAN Network dCDN.

- **The GKAN Network dCDN ensures high security and privacy.**

By distributing content segments to Edge Nodes within the network, with each node staying in their own location, the risk of losing the entire content is less likely to happen. Meanwhile, centralized CDNs have to encounter the single point of failure issue, as all the data is stored in a central entity.

- **Anyone can earn an income by consenting to participate in the GKAN Network dCDN.**

As a decentralized network, the GKAN Network dCDN also works on the principle that individual nodes participating in the network (Edge Nodes) provide their spare resources to process, store or deliver video services and will receive reward for their contribution in the form of GKAN Network Tokens.

BYZANTINE FAULT TOLERANCE

In any decentralized distributed systems, the participants often communicate with one another in an uncontrolled, open, and permission-less system. Their actions may vary based on their individual interests and can be malicious. Therefore, it is vital for participants in decentralized systems to reach consensus in order to minimize the risk of encountering Byzantine Generals Problem (BGP). This necessity gave birth to the Byzantine Fault Tolerance (BFT) concept. So, ***what is BGP and BFT?***

BGP was firstly defined by Leslie Lamport, Robert Shotak, and Marshall Pease in 1982. To be more understandable, let's imagine that before a battle, a kingdom divides its national army into many different battalions, each of which is situated in different locations and commanded by a Byzantine general. The generals need to reach a consensus on either attacking or retreating to achieve victory. However, the communication among generals has to be conducted via messages delivered by couriers, which might lead to problems. For instance, the messages might be delayed, destroyed or lost, or there might be a possibility that some generals/couriers are traitors who choose to act maliciously or change the message content. As a result, the kingdom is not defended. If we apply BGP to the context of blockchains, each network node will represent a general whereas couriers will be replaced by connections or messaging protocols. Likewise, network nodes also need to reach a secure and efficient consensus to avoid complete failure for the entire network.

Meanwhile, BFT is a property of a network that can still ensure the continuous operation even if up to of the nodes in the network fail or act maliciously. In other words, a network is Byzantine fault tolerant when it can keep operating accurately as long as of network nodes reach consensus.

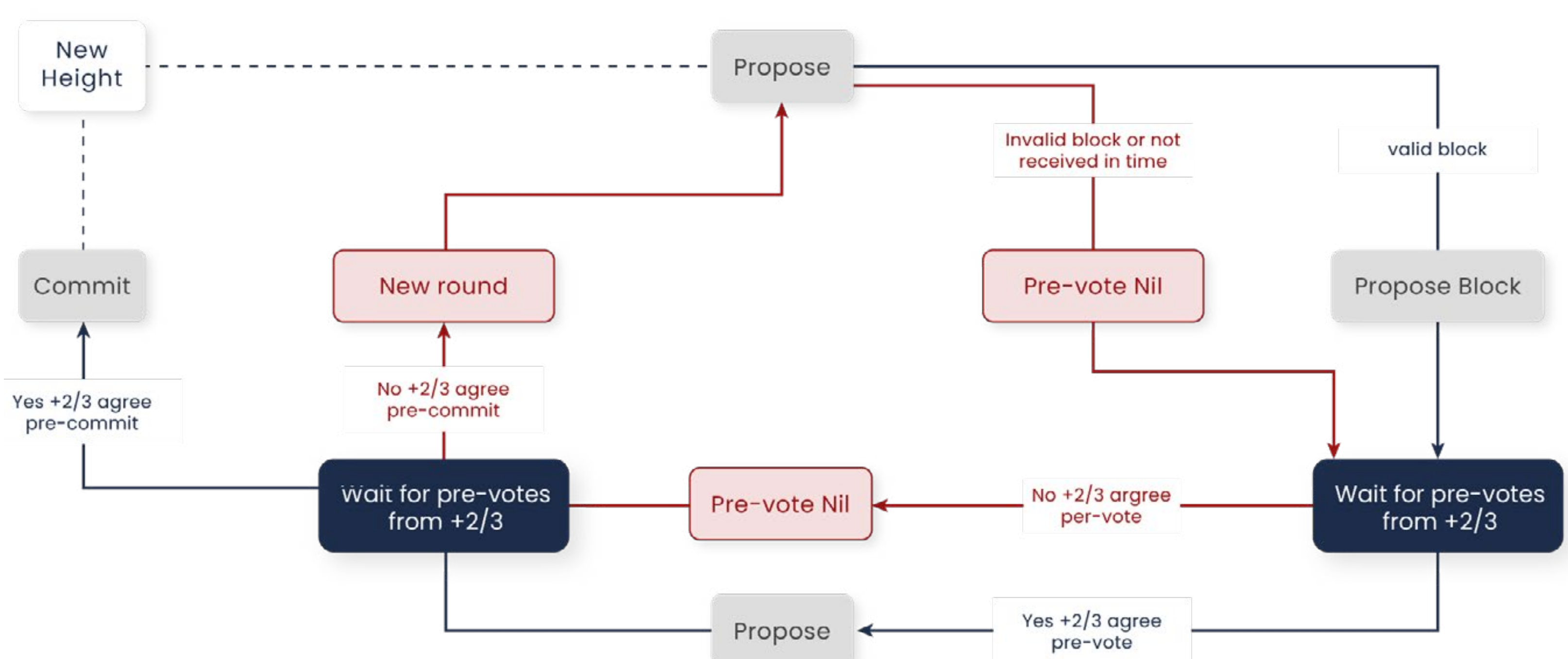
There is more than one approach which could tackle the BGP problem before a true battle and, similarly, in blockchain technology, there are many different consensus algorithms that could be built to achieve BFT. For instance, the consensus mechanisms applied to Bitcoin and Ethereum networks are Proof of Work and Proof of Stake.

GKAN NETWORK DBFT

GKAN Network dBFT is the consensus algorithm developed for the GKAN Network Blockchain on top of Tendermint, wherein “dBFT” stands for “Delegated Byzantine Fault Tolerance”. In GKAN Network Blockchain, there are an enormous number of micro-transactions, such as payment for Edge Nodes or viewers, concurrently taking place. Therefore, it might take validators some time to come to a consensus on verifying all transactions. Among different BFT protocols, dBFT is the algorithm that possesses the highest speed of processing micro-transactions. This is why the GKAN Network team decided to build GKAN Network dBFT.

In GKAN Network dBFT, there are the following two major subjects: 21 **“Validators”** with an unlimited number of “**Witnesses**”:

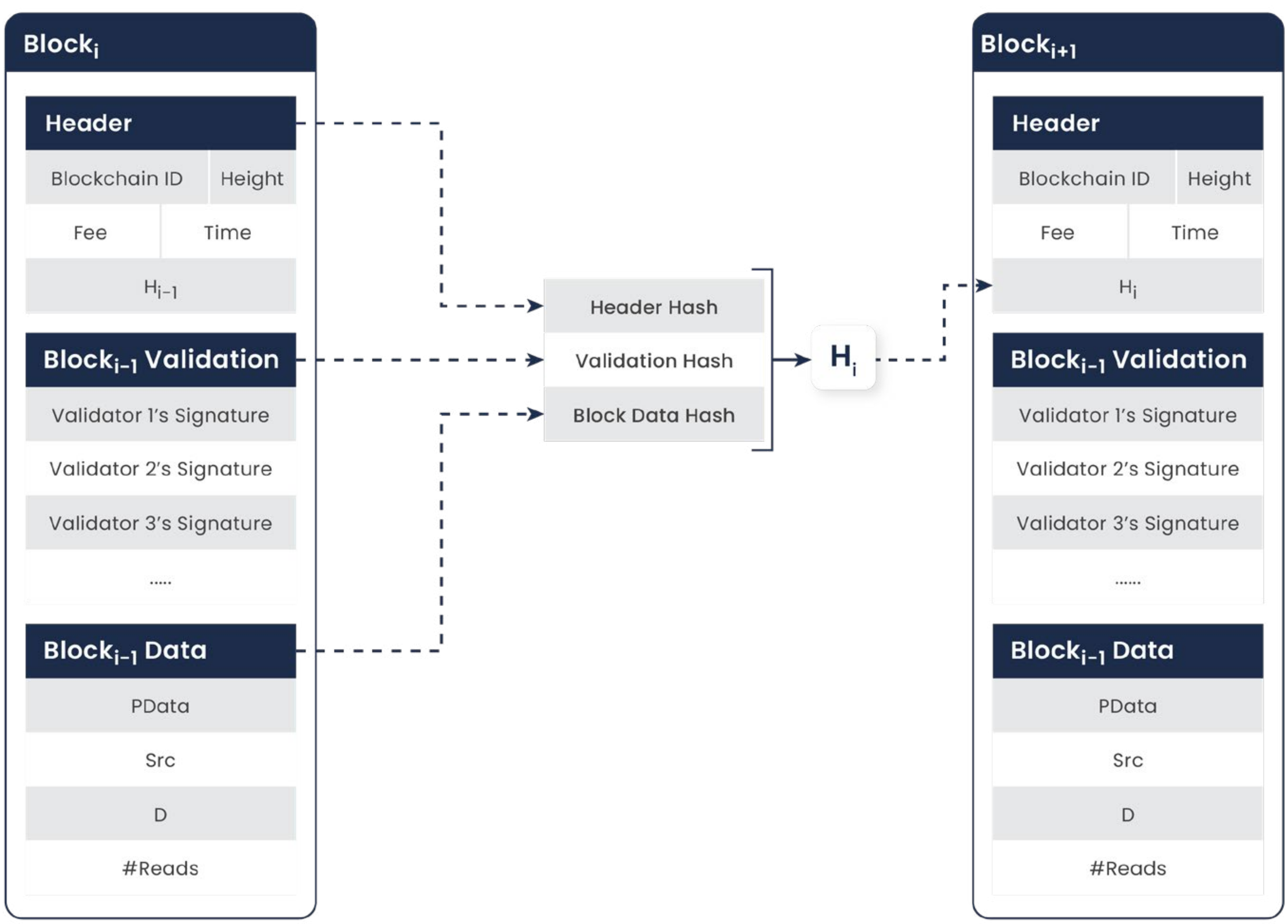
- **Validators** (also known as Delegates): Validators are a group of nodes taking charge of preserving GKAN Network Blockchain data and validating all the transactions. They join the consensus procedure and vote to produce blocks. Validators will take turns proposing blocks of transactions and voting on them. A block is added to the blockchain if more than two-thirds of the validators reach a consensus and validate it. In the GKAN Network Blockchain, the fees are collected and equally allocated among all validators.
- **Witnesses** do not participate in the consensus procedure and block generation, but they (1) take care of the witness consensus process, (2) act as data replicas and help to spread the chain state across the network and (3) receive transactions and broadcast them to all other nodes. Witnesses can become validators by vote.



The block-proposing process is summarized in Figure: Validators take turns proposing blocks for the transaction and voting on the proposed blocks. The blocks are submitted to the chain with each block on the chain at each height. However, the block may fail to submit. In this case, the protocol will select the next certifier to propose a new block at the same height and start voting again.

In order to successfully submit a block, two stages of voting, called a pre-vote and a pre-commit must be undertaken. When more than 2/3 of the certifiers pre-commit the same block in the same round, the block will be submitted. The algorithm that makes 21 validators rotate to propose blocks complies with the round- bin strategy.

Valid transactions are grouped into blocks, the structure of which is illustrated in Figure. The hashes for validation and transactions are Merkle tree root hashes of the signatures and transaction data stored in the block. The state hash (in the header) is the Merkle root hash of the persistent account state after applying the transactions of the block. Finally, the block hash is computed by hashing the header, validation, and transactions hashes. A block is considered to be valid if all the transactions in the block are valid and sufficient signatures are included in the validation.



D. D-APPS ON TOP OF THE GKAN STREAMING NETWORK

Any video streaming platforms/D-apps could be built on top of the GKAN Network dCDN and become a part of the overall GKAN Network Ecosystem in company with 'HUB Nodes' and 'Edge Nodes'. The goal of the GKAN Network dCDN is to become an 'all-win' dCDN, where individual nodes can earn tokens by completing assigned tasks accurately and in a timely manner, while video streaming platforms/D-apps' providers and their partners (content creators, advertisers) as well as their users can benefit as follows:

- **With the GKAN Network dCDN, video streaming platforms/D-providers**

apps' could alleviate their financial burden and increase their profit because the GKAN Network dCDN is remarkably cheaper than commonly used CDNs. As the GKAN Network dCDN grows and expands (more 'HUB Nodes' and 'Edge Nodes' are added), the price would reduce further.

- **Viewers can receive dual benefits while using online streaming platforms built on top of the GKAN Network dCDN.**

In addition to the benefit that viewers will no longer face annoying experiences such as buffering, stuttering, low resolution videos or slow loading, they can also make money just by watching ads inserted into videos on streaming platforms that are the GKAN Network dCDN's partners. After finishing watching a full advertisement, viewers are automatically rewarded with an appropriate number of GKAN Network tokens which are determined based on the property, the length, and the popularity of the advertisement.

- **Content creators can generate more income.**

It is a fact that the average salary of content creators is much lower than what they really deserve because most of today's popular streaming services pay a great amount of money to cloud services for processing raw videos and distributing content to consumers/viewers. This is definitely not the case for platforms collaborating on the GKAN Network dCDN because services offered by the GKAN Network dCDN are inexpensive, as mentioned above. As a result, content creators will be more likely to retain more revenue.

- **Promoting on platforms built on top of the GKAN Network dCDN is a cost-effective solution for advertisers.**

The way advertisers gain advantage from the low price of the GKAN Network dCDN is similar to that for content creators. Furthermore, viewers can earn tokens by watching ads. We believe that the number of viewers who use platforms built on top of the GKAN Network CDN will exponentially increase in the near future. Not only can advertisers approach their targeted audience effectively, but also markedly save costs.

Likewise, the GKAN Network dCDN is a great choice for over-the-top (OTT) services (e.g. Netflix, Hulu, etc.) aiming to expand their business in remote areas or places with limited Internet bandwidth but still maintain the high quality (up to 4K or 8K) of videos delivered to viewers.

The GKAN Network dCDN additionally provides a low-cost cloud solution for a separate audience

whose businesses are not specialized in streaming but who have the demand for storing video content. These are developers of social networking sites or applications such as Tiktok, Instagram, Tinder, that requires digital media content content delivery solutions or developers of electronic newspapers.

E. FUTURE WORK

In the next few years, GKAN Network will continue focusing on research and development activities to increase the number of Edge Nodes and businesses deployed on top of the GKAN Network dCDN. So far, all individual nodes wanting to become our network's Edge Nodes to earn tokens must open TCP/
IP ports, which is a barrier to entry. To eliminate this disadvantage, the GKAN Network team will integrate the WebRTC into the Edge Node Software so that individual nodes can join us easily. The GKAN Network team will also apply AI technology into the content filtering tool to block obscene materials as well as illegal and violent content. The current PoT is not optimal, which necessitates further upgradation of the algorithm built for it. Finally, the GKAN Network team will build and implement a mechanism assessing the 'Reputation Score' of Edge Nodes. The 'Reputation Score' will be determined based on a set of different criteria consisting of Edge Nodes' working status/attitude, working history, number of tasks completed, and duration of participation in the GKAN Network dCDN. The higher the 'Reputation Score' of the Edge Node, the more important tasks and rewards they will receive and vice versa.