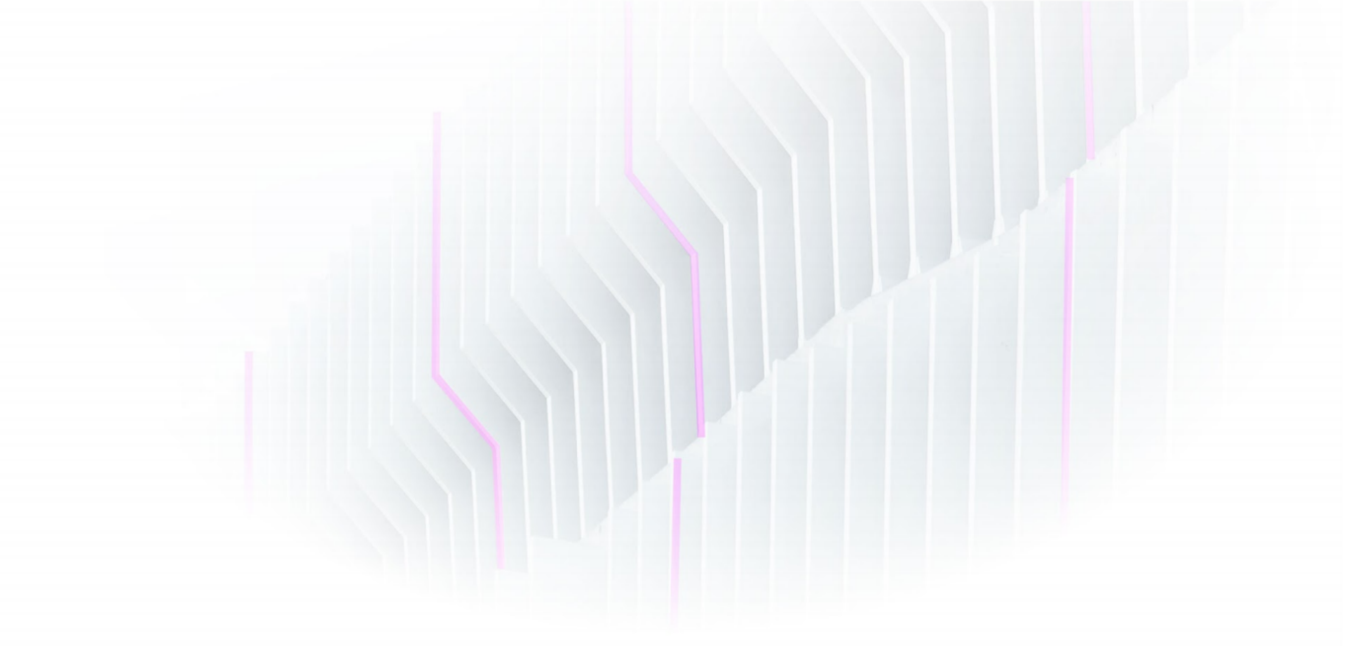
Tachyon

Tachyon Protocol Whitepaper

Internet Libre
The Decentralized Internet Protocol Brings Next-Gen VPN based on Tech Trusted by 50 Million Users



NOTICE AND DISCLAIMER

PLEASE READ THE ENTIRETY OF THIS "NOTICE AND DISCLAIMER" SECTION CAREFULLY. NOTHING HEREIN CONSTITUTES LEGAL, FINANCIAL, BUSINESS OR TAX ADVICE AND YOU SHOULD CONSULT YOUR OWN LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S) BEFORE ENGAGING IN ANY ACTIVITY IN CONNECTION HEREWITH. NEITHER BLOCKSTONE LTD. (THE COMPANY), ANY OF THE PROJECT TEAM MEMBERS (THE TACHYON TEAM) WHO HAVE WORKED ON TACHYON PROTOCOL (AS DEFINED HEREIN) OR PROJECT TO DEVELOP TACHYON PROTOCOL IN ANY WAY WHATSOEVER, ANY DISTRIBUTOR/VENDOR OF IPX TOKENS (THE DISTRIBUTOR), NOR ANY SERVICE PROVIDER SHALL BE LIABLE FOR ANY KIND OF DIRECT OR INDIRECT DAMAGE OR LOSS WHATSOEVER WHICH YOU MAY SUFFER IN CONNECTION WITH ACCESSING THIS WHITEPAPER, THE WEBSITE AT HTTPS://TACHYON.ECO/ (THE WEBSITE) OR ANY OTHER WEBSITES OR MATERIALS PUBLISHED BY THE COMPANY.

All contributions will be applied towards the advancing, promoting the research, design and development of, and advocacy for a viable blockchain-based solution for the aging TCP/IP stack in order to improve fundamental internet infrastructure technologies. The Company, the Distributor and their various affiliates would develop, manage and operate Tachyon Protocol.

The Whitepaper and the Website are intended for general informational purposes only and does not constitute a prospectus, an offer document, an offer of securities, a solicitation for investment, or any offer to sell any product, item or asset (whether digital or otherwise). The information herein may not be exhaustive and does not imply any element of a contractual relationship. There is no assurance as to the accuracy or completeness of such information and no representation, warranty or undertaking is or purported to be provided as to the accuracy or completeness of such information. Where the Whitepaper or the Website includes information that has been obtained from third party sources, the Company, the Distributor, and/or the Tachyon team have not independently verified the accuracy or completion of such information. Further, you acknowledge that circumstances may change and that the Whitepaper or the Website may become outdated as a result; and neither the Company nor the Distributor is under any obligation to update or correct this document in connection therewith.

Nothing in the Whitepaper or the Website constitutes any offer by the Company, the Distributor or the Tachyon team to sell any IPX Token (as defined herein) nor shall it or any part of it nor the fact of its presentation form the basis of, or be relied upon in connection with, any contract or investment decision. Nothing contained in the Whitepaper or the Website is or may be relied upon as a promise, representation or undertaking as to the future performance of Tachyon Protocol. The agreement between the Distributor and you, in relation to any sale and purchase of IPX Token, is to be governed by only the separate terms and conditions of such agreement.

By accessing the Whitepaper or the Website (or any part thereof), you represent and warrant to the Company, the Distributor, its affiliates, and the Tachyon team as follows:

(a) in any decision to purchase any IPX Token, you have not relied on any statement set out in the Whitepaper or the Website;

(b) you will and shall at your own expense ensure compliance with all laws, regulatory requirements and restrictions applicable to you (as the case may be);

(c) you acknowledge, understand and agree that IPX Token may have no value, there is no guarantee or representation of value or liquidity for IPX Token, and IPX Token is not for speculative investment;

(d) none of the Company, the Distributor, its affiliates, and/or the Tachyon team members shall be responsible for or liable for the value of IPX Token, the transferability and/or liquidity of IPX Token and/or the availability of any market for IPX Token through third parties or otherwise; and

(e) you acknowledge, understand and agree that you are not eligible to purchase any IPX Token if you are a citizen, national, resident (tax or otherwise), domiciliary and/or green card holder of a geographic area or country (i) where it is likely that the sale of IPX Token would be construed as the sale of a security (howsoever named), financial service or investment product and/or (ii) where participation in token sales is prohibited by applicable law, decree, regulation, treaty, or administrative act (including without limitation the United States of America, Canada, New Zealand, People's Republic of China (but not including the special administrative regions of Hong Kong and Macau, and the territory of Taiwan), Thailand, and the Socialist Republic of Vietnam).

The Company, the Distributor and the Tachyon team do not and do not purport to make, and hereby disclaims, all representations, warranties or undertaking to any entity or person (including without limitation warranties as to the accuracy, completeness, timeliness or reliability of the contents of the Whitepaper or the Website, or any other materials published by the Company or the Distributor). To the maximum extent permitted by law, the Company, the Distributor, their affiliates and service providers shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including, without limitation, any liability arising from default or negligence on the part of any of them, or any loss of revenue, income or profits, and loss of use or data) arising from the use of the Whitepaper or the Website, or any other materials published, or its contents (including without limitation any errors or omissions) or otherwise arising in connection with the same. Prospective purchasers of IPX Token should carefully consider and evaluate all risks and uncertainties (including financial and legal risks and uncertainties) associated with the IPX Token sale, the Company, the Distributor and the Tachyon team.

The information set out in the Whitepaper and the Website is for community discussion only and is not legally binding. No person is bound to enter into any contract or binding legal commitment in relation to the acquisition of IPX Token, and no virtual currency or other form of payment is to be accepted on the basis of the Whitepaper or the Website. The agreement for sale and purchase of IPX Token and/or continued holding of IPX Token shall be governed by a separate set of Terms and Conditions or Token Purchase Agreement (as the case may be) setting out the terms of such purchase and/or continued holding of IPX Token (the Terms and Conditions), which shall be separately provided to you or made available on the Website. In the event of any inconsistencies between the Terms and Conditions and the Whitepaper or the Website, the Terms and Conditions shall prevail.

No regulatory authority has examined or approved of any of the information set out in the Whitepaper or the Website. No such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of the Whitepaper or the Website does not imply that the applicable laws, regulatory requirements or rules have been complied with.

The information set out herein is only conceptual, and describes the future development goals for Tachyon Protocol to be developed. The Whitepaper or the Website may be amended or replaced from time to time. There are no obligations to update the Whitepaper or the Website, or to provide recipients with access to any information beyond what is provided herein.

All statements contained herein, statements made in press releases or in any place accessible by the public and oral statements that may be made by the Company, the Distributor and/or the Tachyon team, may constitute forward-looking statements (including statements regarding intent, belief or current expectations with respect to market conditions, business strategy and plans, financial condition, specific provisions and risk management practices). You are cautioned not to place undue reliance on these forward-looking statements given that these statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results to be materially different from that described by such forward-looking statements, and no independent third party has reviewed the reasonableness of any such statements or assumptions. These forward-looking statements are applicable only as of the date indicted in the Whitepaper, and the Company, the Distributor as well as the Tachyon team expressly disclaim any responsibility (whether express or implied) to release any revisions to these forward-looking statements to reflect events after such date.

The use of any company and/or platform names or trademarks herein (save for those which relate to the Company, the Distributor or its affiliates) does not imply any affiliation with, or endorsement by, any third party. References in the Whitepaper or the Website to specific companies and platforms are for illustrative purposes only.

The Whitepaper and the Website may be translated into a language other than English and in the event of conflict or ambiguity between the English language version and translated versions of the Whitepaper or the Website, the English language versions shall prevail. You acknowledge that you have read and understood the English language version of the Whitepaper and the Website.

No part of the Whitepaper or the Website is to be copied, reproduced, distributed or disseminated in any way without the prior written consent of the Company or the Distributor.

Abstract

After 36 years of use, TCP/IP-based internet communication is gradually lagging behind contemporary users' increasing demand for stability, security, speed and trust. Tachyon protocol reconstructs TCP/IP network protocol stack by using proven and accepted P2P technologies such as DHT and PPPoIP, self-developed technologies such as UDP and real-time optimal routing, combining end-to-end encryption, traffic hiding, multi-path concurrent routing, and multi-relay forwarding scheme to achieve high security, intractability, availability, and maximum network speed.

The existing lack of trust and security in internet privacy, along with the aging infrastructure, inhibits the internet in providing the speed and reliability required by current network-based, Web 3.0 services such DeFi and other complex applications. To bring a new solution in resolving these issues, Tachyon Protocol utilizes the existing and widely accepted platform, while eliminating the very idea of centralized servers, where proxies, VPNs, cloud storage, CDN's, DeFi or any other services that require a sturdy, secure platform can build their businesses on.

Tachyon Network is built on the V SYSTEMS blockchain with the use of existing and tested technologies to ensure its lasting effectiveness, such as modular design, user-orientation, nodes and versatile application possibilities. Key features of the protocol include:

- Tachyon Booster UDP - adopting techniques from DHT, blockchain, UDP and the real-time Optimal Routing, it is capable of 200%~1000% transmission acceleration and over 90% connection success rate in complex network environment based on experimental data.
- Tachyon Security Protocol - an asymmetric end-to-end encrypted content simulation security protocol that provides real-time protection against man-in-the-middle attacks (MITM), as well as other security issues, when both parties conduct end-to-end communication.
- Tachyon Anti-Content Analysis - enhancing network anti-monitoring capabilities through concurrent multi-routing scheme and multi-relay forwarding scheme.
- Tachyon SDK - combined with blockchain, it can be easily integrated and instantaneously deployed with all popular programming languages.
- IPX Token - which shall be introduced in the Tachyon Protocol to incentivize various participants to contribute to the positive development of the Tachyon ecosystem. The IPX token resides on the V SYSTEMS blockchain.

Keywords: Internet protocol suite, Cybersecurity, Privacy protection, Transmission speed, TCP/IP, Decentralization, Encryption, Blockchain.

Contents

1. Background

1.1 Deterioration in Cybersecurity

Let's recap the major cybersecurity incidents over the past 10 years:

- 2017: PRISM, the program NSA used for collecting various types of data: e-mail, video/voice chat, stored photos, VoIP, file transfers, notifications of target activity, logins, etc;
- 2018: an exchange was exposed for sending sensitive user information in plain text over HTTP. Attacker was able to change the user password without authentication [1];
- May 2018: FBI warned the public of the malware “VPNFilter”, which had infected over 500,000 routers worldwide. The malware is designed for a range of nefarious purposes including monitoring and manipulating the traffic, as well as stealing sensitive data;
- 2019: research by K.U. Leuven suggested that WPA2 encryption flaws can be exploited via KRACK to read, steal, and manipulate the data sent through the WiFi network.

Given that history repeats itself, cyber threats will always be relevant issues for years to come. For more information, please visit https://privacyinternational.org.

Conclusions we can draw from these incidents:

- **Centralized structure cannot protect user data from government surveillance/data requests;**
- **Networks are vulnerable to attacks during transmission;**
- **Security vulnerability is inevitable, regardless of company scale or technical expertise.**

One can never entrust cybersecurity in the hands and technologies of its managers. We need a more practical and elegant solution, especially in the booming DeFi industry where cybersecurity is the primary concern.

1.2 TCP/IP is Becoming Obsolete

As the basis of the modern internet, the TCP/IP model, if it can be improved, is of great significance to the development of the internet. Many companies are working hard to improve TCP/IP, such as Google's QUIC protocol, IBM's Apera and many others.

Next, we will explain why Tachyon would be the one to improve the TCP/IP protocol from practice and experience.

1.2.1 TCP/IP Security Vulnerabilities and Low Transmission Efficiency

It has been 36 years since TCP/IP was officially adopted as the communication protocol on January 1, 1983. The TCP/IP model is segmented into the following parts:

Ethernet as Data Link Layer protocol
Bus topology structure with CSMA/CD would cause congestion in the occurrence of massive numbers of collisions. The star topology is not robust enough. Once the central node fails, the entire network is unavailable.

IP as the internet Layer protocol
IP addresses are often tied to the physical address. Using the social engineering techniques, the hacker may link the address to the individual, profile the person, and commit fraudulent acts. As platforms also use IP address as one of the key identifiers, they track the IPs browsing to serve relevant Ads.

TCP as the Transport Layer protocol
The TCP three-way handshake mechanism, acknowledgment mechanism and congestion control mechanism would result in both bandwidth and time wastage when the network is unstable.

HTTP/HTTPS as the Application Layer protocol
The Hypertext Transfer Protocol (HTTP) is the basis for data transmission of the World Wide Web, but its protocol poses various security risks, vulnerable against penetration & hijacking.

Although TCP/IP provides security components such as TLS 1.3 at the application layer, due to deployment costs and learning costs, some practitioners and even some exchanges still transmit key information (such as passwords) in plain text using HTTP protocol, which is easily intercepted by hackers.

When the network suffers fluctuation, TCP/IP won't be able to manage bandwidth usage properly and cause rapid reduction of the transmission efficiency, and it cannot fully support a massive information broadcasting network such as blockchain, which may cause the miners who haven't synchronized to the newest block to waste time and resources on already mined blocks. In addition, the required deployment & learning expenses of TCP/IP security components may leave potential vulnerability from improper deployment. Further, all blockchain-related communication (such as communication relying on blockchain for verification, security, data storage) will suffer the same issues over TCP/IP.

1.2.2 Trust Issues with the Centralized VPN Providers

Having been working in the industry for many years, Tachyon team have discovered the shortcomings of the business.

- The bandwidth resources are mainly provided by the VPS service provider, and the user data can be arbitrarily obtained and cached, so that the privacy policy claimed by the VPN service provider cannot be completely executed;
- Some VPN service providers themselves ignore the log retention policy and try to capitalize by reselling user data;
- Subject to legal requirements and administrative orders, centralized VPN service providers are susceptible to monitoring by powerful authorities;
- A VPN provider can only provide a certain amount of servers from a few VPS providers. The server node is limited and vulnerable to VPS network. The network is not stable, and the speed cannot be effectively guaranteed.
- Content providers (e.g., Netflix) often use the VPS IP blocking scheme to prevent users from accessing their services with VPNs.

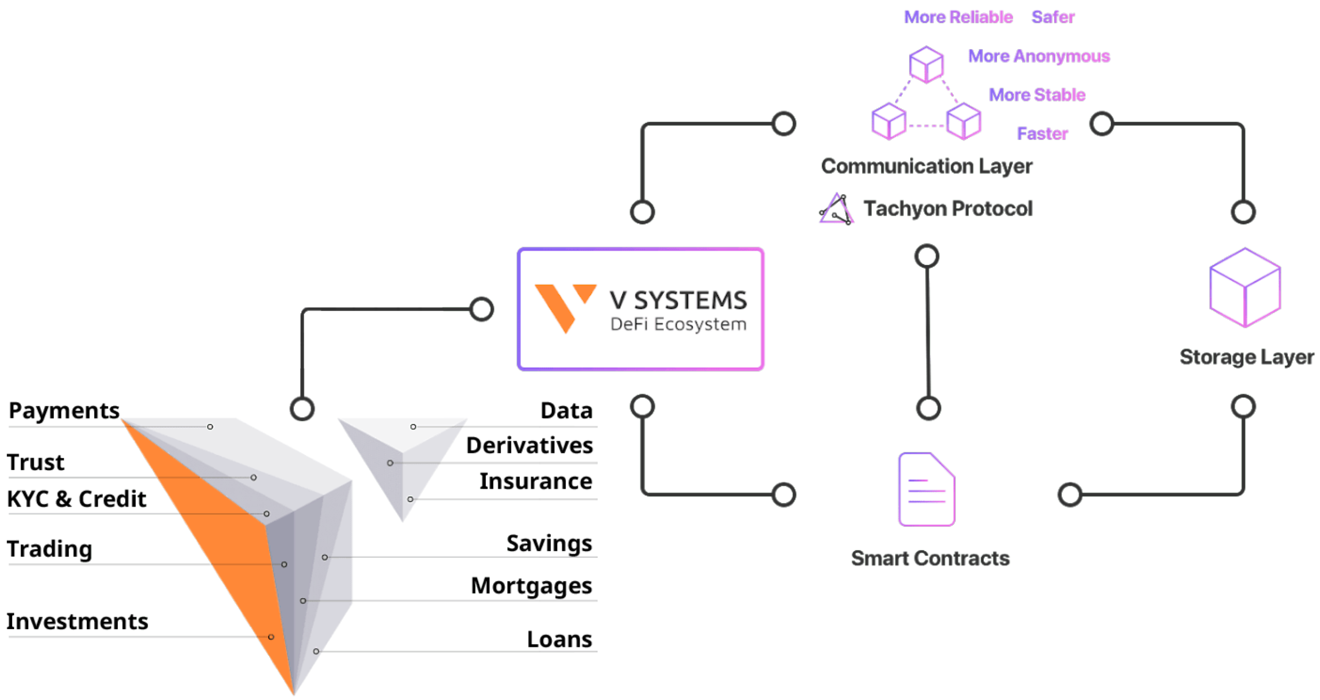
Currently, centralized VPN cannot effectively provide its claimed network security, privacy protection, geo-blocking and network acceleration services.

1.3 Tachyon & V SYSTEMS

The Tachyon team has been on the quest to build a more secure network by revamping the bottom layer protocol. Since 2016, the Tachyon and V SYSTEMS teams have been collaborating and sharing R&D in order to find viable technical solutions for aging TCP/IP stack. We share the same vision: to improve fundamental internet infrastructure technologies. Succeeding in this would mean significant improvement to the internet infrastructure as well as the decentralization of an ever greater number of internet services.

This collaboration marks a great significance to both V SYSTEMS and Tachyon teams. As the first project to be built in the V SYSTEMS ecosystem, Tachyon Protocol will bring millions of users onto the V SYSTEMS network. At the same time, V SYSTEMS will provide Tachyon Protocol the technologies needed to obtain a scalable blockchain DApp [3].

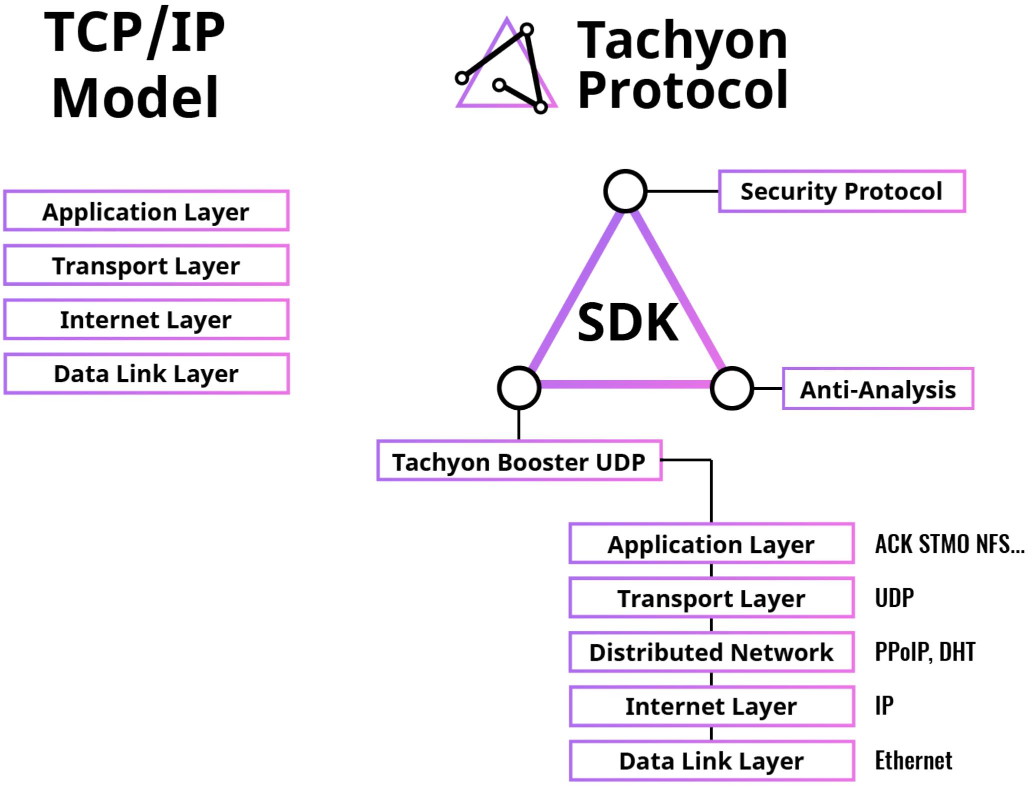
Tachyon Protocol will be released as an open-source library. As more DApp scenarios are realized, network security, privacy protection, and transmission efficiency are still important prerequisites for the success of the project. We will witness the future of Tachyon Protocol.


More Reliable
Safer
More Anonymous
More Stable
Faster
Communication Layer
Tachyon Protocol
V SYSTEMS
DeFi Ecosystem
Storage Layer
Payments
Trust
KYC & Credit
Trading
Investments
Data
Derivatives
Insurance
Savings
Mortgages
Loans
Smart Contracts

2. Tachyon Protocol

2.1 Overview

Tachyon Protocol is a decentralized network stack combining decentralization and encryption techniques; it is designed to reconstruct the TCP/IP stack by means of decentralized structure, end-to-end encryption, traffic concealing, multi-path routing, and multi-relaying scheme.



Tachyon Protocol comprises of:
TBU (Tachyon Booster UDP): Using DHT, blockchain and UDP to reconstruct TCP/IP protocol, coupled with application of real-time optimized routing. The TBU protocol is capable of 200%~1000% transmission acceleration in centralized network with over 90% connection success rate in complex network environment based on experimental data. Independent tests will soon follow to help us further quantify speed improvements.
TSP (Tachyon Security Protocol): Security protocol using a combination of encryption and traffic concealing schemes to protect the connection against relay nodes.
TAA (Tachyon Anti-Analysis): TAA is the security strategy that implements Concurrent Multi-Path Routing and Multi-Relaying to counter traffic monitoring. The difficulty of intercepting the entire communication will increase exponentially with more nodes active on the network.

SDK: Tachyon Protocol offers a standardized API and customizable modules to ensure swift integration & deployment.

2.2 Tachyon Booster UDP (TBU)

TBU is the bottom transport layer protocol which uses DHT, blockchain, and UDP techniques to reconstruct TCP/IP protocol. Coupled with the application of real-time Optimal Routing, it is capable of 200%~1000% transmission acceleration in a centralized network and over 90% connection success rate in a complex network environment.

2.2.1 Revamping TCP/IP with The Blockchain-based Transport Protocol:

We are reconstructing the Internet Layer, Transport Layer and Application Layer of the TCP/IP protocol by using proven technologies such as PPoIP, DHT, UDP and blockchain:

- **Data Link Layer:** In the TCP/IP model this layer includes physical sublayer and logical sublayer, which are the foundation of communication between two points.

    - **Physical Sublayer:** This layer consists of the hardware (e.g., optical fiber, coaxial cable) to be used for the network. As part of the local infrastructure, they are provided by the local internet service providers;
    - **Logical Sublayer:** The modern internet uses Ethernet to build reliable LANs (Local Area Network). Ethernet uses a bus topology with CSMA/CD, where every station must make sure the medium is idle before transmitting. When a collision occurs, the stations will wait for a random amount of time before attempting to re-transmit. The wait time increases as more attempts fail. In the event of a massive number of collisions, the network congestion will last for a long period. With star topology, the central hub failure will result in an inoperable network [4].

    The modern internet is built on the foundation of Ethernet where the structure is already deeply rooted, meaning that Tachyon protocol is unable to make any meaningful optimizations directly.

- **Internet Layer:** In the TCP/IP model, this layer mainly selects nodes and establishes connections. It serves the purposes of host addressing/identification and packet routing, as well as establishing, persisting, and aborting the connection. The primary protocol in this layer is IP protocol.

- Tachyon Protocol takes the concept of PPP (Point-to-Point Protocol) to build PPPoIP on IP Network layer, with complete topology, provide end-to-end connection in the fully connected network. At the same time, blockchain technology is introduced to enable large-scale collaboration of P2P networks.
    - **The elimination of a central server will minimize data centralization and data requests;**
    - **Use of blockchain techniques for sessions and community governance where all nodes are considered equal and free to participate;**
    - **Each node is connected to every other node to strengthen network robustness and stability;**
    - **High capability of anti-filter/censorship with millions of nodes;**

- Route addressing and node matching
    - To ensure the robustness of the P2P network, Tachyon employs a self-developed Tachyon DHT based on Kademlia algorithm for P2P network routing with Trackerless as our objective;
    - DHT (Distributed Hash Table) can be used for distributed storage. IPFS project is one of the examples where DHT is used for distributed data storage [5]. However DHT can also be used for routing and addressing. The nodes and K-bucket can form data structure similar to merkle trees in blockchain, where K-bucket in each node is responsible for the routing of its hashing ring. The combination of the K-buckets makes up the routing table for the entire P2P network;
    - Each newly arrived node will get a Key ID through hashing their location after it passes the V SYSTEMS nodes voting.
    - **Kademlia Message STORE:** Relay uses the XOR operator to look up the node whose Node ID is the closest to Key ID, and requests to store its IP: Port and Active Time to the Key ID of the node.
    - **Kademlia Message FIND_VALUE:** Client receives the Key ID by hashing the connection destination, and looks up the value of the Key ID on the network, which returns a set of IP addresses.
    - **K-bucket data structure:**
        - NodeMap map[NodeID] -> IP: Port, rtt;
        - RouteMap map[KeyID] -> map[NodeID] -> IP: Port, Active Time.
    - **Retriever Store method:**
        - Assuming client A had retrieved the IP list for the USa, A stores this information to its RouteMap;
        - Client B, who is close to Client A, may quickly retrieve the IP information from A;

  - After retrieving the IP information for the US, B also stores it to its K-bucket.
- **Real-time optimal routing system to evaluate transmission efficiency:**
  - Depending on the data type to use different connection strategies: nodes-to-node or node-to-node;
  - Real-time monitoring of latency, packet loss, and bandwidth between nodes to evaluate the transmission Efficiency (i) between nodes;
  - Real-time calculation of node credit.

Lastly sort the Distance(XOR), Efficiency(i), and Credit by priorities to get the available routes.

- **Transport Layer:** In the TCP/IP model, this layer is responsible for process-to-process delivery of the entire message. The three-way handshake, acknowledgment and retransmission mechanisms of TCP ensures reliable deliveries of the information, yet at the cost of speed loss and low throughput.

  - **UDP offers superior throughput and has less overhead. Tachyon Protocol chooses UDP instead of TCP to improve transmission efficiency.**

- **Application Layer:** In the TCP/IP model, this layer is responsible for defining the data format and interpreting the data according to the corresponding format, and can increase the data flow monitoring, encryption and other modules based on the transmission requirements.
  - Since the Tachyon Protocol uses the UDP protocol at the transport layer, **a reliable module needs to be built at the application layer to improve the reliability of the UDP delivery service.**
    - Acknowledgment to improve reliability, bandwidth management, reduce packet loss and data redundancy;
    - FEC (Forward error correction) to minimize the packet loss;
    - Bandwidth auto-scaling to maximize throughput efficiency.

2.2.2 Multi-protocol Smart Circumvent Scheme

There are many influencing factors in the network environment that can cause the network connection to fail. To this end, the Tachyon Protocol selects the available protocols by identifying the current network environment. **Therefore, the connection success rate of the complex network environment is increased to over 90%.**

- We observed in practice how the protocol always fails right before, or right after the connection is initiated, which might cause the firewall to block the remote IP and result in connection failure with other protocols. By categorizing protocols, it will prevent the protocol interference in the connection.
- Prioritizing the protocols with the success connection record will reduce bandwidth wastage.
- Sorting by overhead and handshake will also improve bandwidth utilization and connectivity.

2.3 Tachyon Security Protocol (TSP)

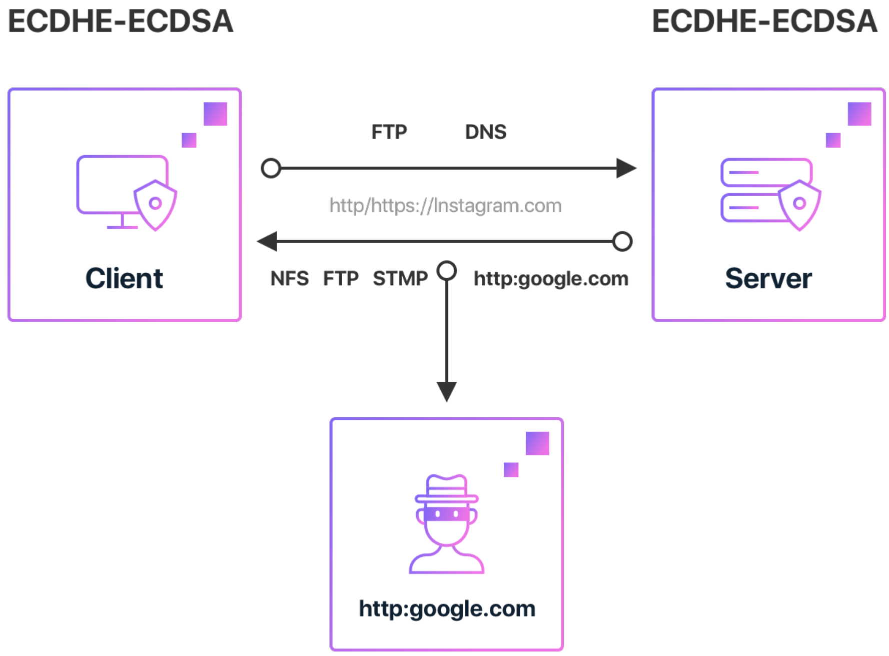
Tachyon Security Protocol is a security component of Tachyon Protocol. **TSP presents asymmetric end-to-end encryption scheme and protocol simulation. The former is mainly used to prevent network sniffing and man-in-the-middle attacks. The latter also plays an important role in preventing attacks, circumventing firewalls and filtering.**

2.3.1 ECDHE-ECDSA End to End Encryption to Protect The Message Being Intercepted by Relays

There are two major threats in point-to-point networking:

- **Network sniffing:** the attacker can analyze the network and intercept the data

    - The P2P network requires TSP to create encryption keys in the insecure channel in which both points do not know each other, so we will implement ECDH - ECDSA and Ephemeral Key to realize forward secrecy;
    - Use AES to encrypt connection, so that the attacker cannot read the content even if the connection is intercepted;
    - Ensure data integrity by using a combination of hash algorithms (HMAC, SHA2, Keccak), so the message would be ignored when communication is altered by the attacker;
    - By using a public symmetric encryption key, adding random data to the transmission, and encrypting the information part such as the frame byte of the transmission content, the third party is prevented from acquiring the statistical feature information;
    - After each connection transmits a certain length of data, the key is automatically renegotiated to avoid multiple reuse of the key.



- **Man-in-the-middle attack (MITM):** the attacker alters communication between parties by pretending to be them
    - The identities of both parties can be verified via ECDH before communication. In theory, as long as the private key is not compromised, the man-in-the-middle attack can be prevented.

2.3.2 Protocol Simulation Scheme

By simulating the feature state of the common protocol, **the real communication content is concealed to avoid information interception and exposure.**

Currently, HTTP/HTTPS is the most common communication protocol of the World Wide Web (WWW), but there are some defects:

- HTTP communication uses clear-text and does not verify the identity of the other end of the connection, which make it easy for the attacker to intercept the message. Also, the HTTP does not check for the integrity of the message.
- TLS 1.3 fixes the certificate exposure issue and HAS a faster handshake, but it exposes hostname through SNI which may lead to blocking [6].

Tachyon Protocol is able to conceal the IP packets and simulate UDP, TCP, HTTP, HTTPS, FTP and SMTP traffic:

- SMTP simulation: The traffic will appear as if the user is sending emails;

- HTTPS simulation: The traffic will appear as if the user is visiting Google/BBC News;
- FTP simulation: The traffic will appear as if the user is transferring data;

The simulation will prevent the attacker in finding the characteristics of Tachyon protocol when intercepting, at the same time disabling the firewall's ability to detect Tachyon traffic.

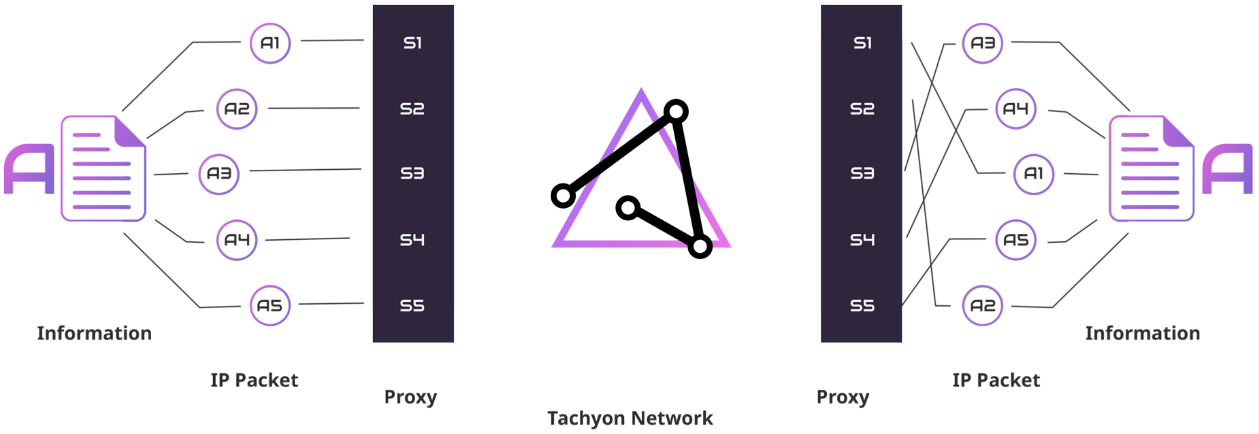
2.4 Tachyon Anti-analysis (TAA)

Decentralized network has, to a certain extent, increased the risk of single node capture attack, as it made easier for the attacker to monitor the communication content in the network. To solve this problem, Tachyon Protocol uses Tachyon Anti-analysis to decompose and forward information. It includes the following two aspects:

- **The concurrent Multi-path routing scheme** separates a piece of information into multiple different IP packets and then forwards them through different paths, so that single-point attacks cannot obtain all the information;
- **The multi-relay forwarding scheme** adopts some ideas from onion routing. The information is forwarded by multiple encryptions, so that the concurrent contribution node cannot know the forwarding content and routing path.

2.4.1 Concurrent Multi-Path Routing

Distribute the data through multiple channels at the same time to obscure the connection route. When a user is communicating with the Tachyon Protocol, the client will assign different exit IPs for UDP/TCP quaternion packets, where each quaternion packet will be sent through a different route.



Concurrent Multi-Path Routing

Assuming the user is sending a message(A):

- The requests of the message(A) will be separated into IP packet(A1), IP packet(A2), IP packet(A3), IP packet(A4), and IP packet(A5); the Head of IP Packet(n) use will the SHA-256 hash result of Information(A) as the IP Packet index to form a tree structure where information A is parent;
- The IP Packet(n) will be routed through Proxy(S1), Proxy(S2), Proxy(S3), Proxy(S4), Proxy(S5) and reach the Client with Tachyon ID;
- After the client receives the entire IP packet, it may use the IP packet index to retrieve the original message(A).

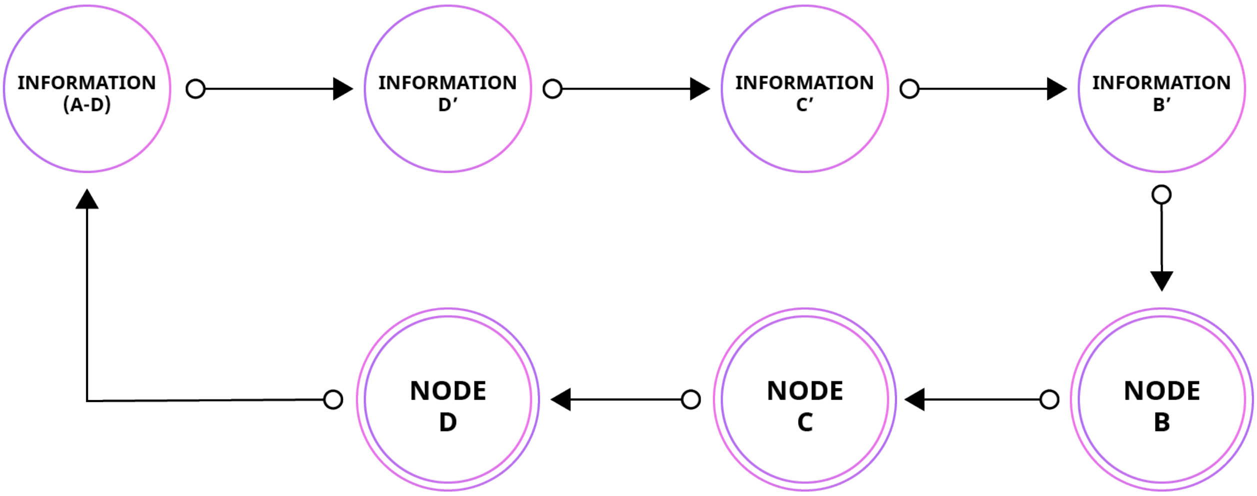
The attacker can only get a part of the message intercepting one channel, with the increase of the nodes in the network, the difficulty of intercepting the entire communication will be increased exponentially.

2.4.2 Multi-relaying Scheme

In a P2P network, no nodes can be trusted. If you were to send only one request, by getting hold of one's public key, attackers would know which nodes you are communicating with and further speculate the route of the traffic. Therefore, a traditional DNS system to look up the destination and relays is not the way to go.

Then how to avoid communication being monitored assuming certain nodes in the network had been compromised?

- A is trying to send a message to D, A encrypts the message with D's public key;
- A puts the encrypted message to D in an envelope to D, then uses C's public keys to encrypt it as a message to C;
- Then A puts the encrypted message to C in an envelope to C, encrypts it with B's public key as a message to B;
- A sends the encrypted message to B. B decrypts it and gets the encrypted envelopes to C;
- B sends the encrypted envelope to C. C decrypts it and gets the encrypted envelopes to D;
- C sends the encrypted envelope to D, D decrypts it and gets the message from A;
- This way, the relays will not be able to know D and A are communicating unless both B and C were compromised.



Unless Node B and Node C are controlled at the same time, it is almost impossible to know that Node A is sending a message to Node D.

This scheme will minimize the possibility of communication monitoring/tracking in the network.

2.5 Tachyon SDK

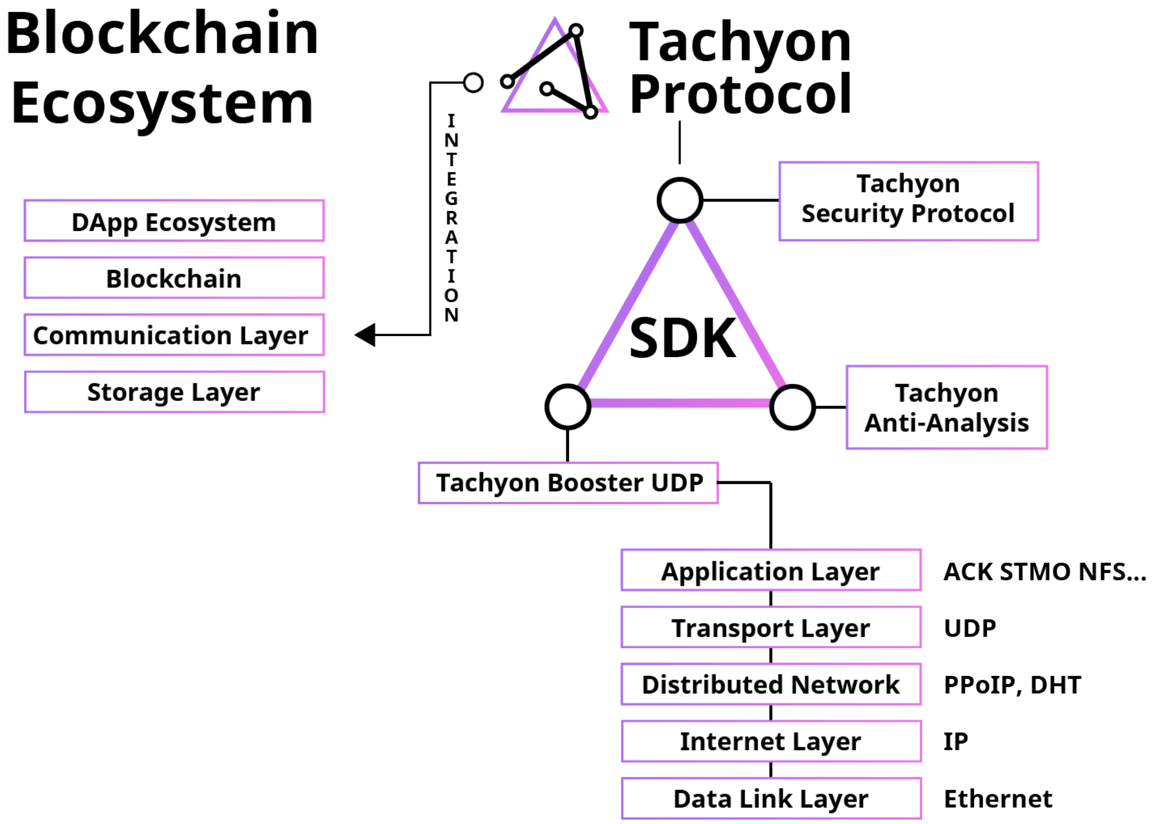
At present, most of the blockchain projects use TCP/IP-based networking. For example, both Bitcoin and Ethereum are using TCP for data broadcasting. If order for Tachyon Protocol to offer an alternative for the TCP/IP protocol, there are a few things that need to be considered: interaction between encryption protocols, data syncing and node interaction. All of these are resource-consuming procedures.

To reduce the integration expense for the blockchains, ensure proper encapsulation and reduce the difficulty of development, Tachyon Protocol shall provide a standard SDK which blockchain networks can easily integrate with their technological stack. After the blockchain is deployed, its nodes can implement automatic proxy and port switching of the transport layer network protocol, and data transmission between nodes can be transmitted through the Tachyon Protocol.

With features of absolute security and privacy, faster speed, No Block and lower cost, Tachyon Protocol will benefit DApp based on blockchain, such as privacy protection, data storage, CDN, DeFi, instant messaging, edge computing, games.

Tachyon offers highly customizable modules for SDK:

- Prioritize per data transmission type, e.g., prioritize low latency/low packet loss/high bandwidth;
- Traffic concealing, e.g., set preferred protocols, request simulation;
- Multi-protocol circumvent, e.g., use certain protocols only;
- Traffic-dispersing, e.g., set maximum/minimum dispersing;
- Multi-relays, e.g. 1~6 relays mode, auto mode.



3. Tachyon Market

Tachyon Protocol is an open, P2P network where nodes provide services to each other and form a market. It is necessary to clarify the roles of each node in the market, delivery services, and potential vulnerabilities:

- Primary roles are client nodes, provider nodes, and business clients.
- Bandwidth is the commodity being traded.
- There are a few potential risks and attacks in the market we need to examine:
    - **Delivering service quality risks:** service providers sell inferior bandwidth at a high price.
    - **Trading volume cheating risks:** both parties to the session lie about the trading volume.
    - **Sybil attacks:** the attacker creates various false identities in a P2P network and uses them to sabotage the reputation of the system, which will damage the interests of the honest node [7].
    - **Man-in-the-middle attacks:** This issue has been addressed by TSP and TAA as discussed above.
    - **Concurrent analysis attacks:** regular concurrent analysis attacks can also be defended by TSP and TAA, but the Tachyon market will introduce new types of attacks, specifically analyzing routing paths through session information to monitor concurrent;

We need to solve the above risks and attacks by means of concurrent contribution node authentication, session target selection, price mechanism design, payment channel design and session record uplink.

3.1 Protocol Specification

Client nodes: The nodes initiate the connection, including consumer-level devices as smartphones, computers, routers or enterprise-level servers, supporting iOS/Android/Windows/Mac/Linux and other operating systems.

Provider nodes: The nodes relay the traffic, including consumer-level devices as computers, routers or enterprise-level devices such as servers and support Windows/Mac/Linux and other operating systems.

Business nodes: The nodes which purchase bandwidth to power their businesses, including blockchains and DApps. Some of the businesses themselves are the collection of many client nodes. While provider nodes have no incentive to pay extra cost, but the client nodes need to access the Tachyon Protocol network for business considerations. At this time, the client nodes can directly pay for the traffic in the network, which is relatively stable.

3.2 Node Verification

3.2.1 Client Node Verification

To provide a smooth user experience, the Tachyon Protocol does not have any hard requirements for the client node.

Proposed client node workflow:

- User downloads client, and the Client generates the Private Key and Public Key.
- The client receives Public key SHA-256 hashed Node-ID as the Tachyon DHT unique ID.
- The client uploads [Node ID, Public Key, and request(Register)] into the registration queue.
- Proceed with V SYSTEMS node verification and log Node ID.

3.2.2 Provider Node Verification

To ensure the node integrity and service operation, provider nodes are required to stake a certain amount of IPX tokens as security deposit. Security deposit minimum amount is yet to be determined but a lock period is proposed to be 7 days at least. Each provider node must be verified on the main net to receive the unique Tachyon ID and become a trusted node, which is done to prevent the Sybil Attack.

Proposed node verification workflow:

- User downloads client, and the client generates the keypair (Private Key and Public Key).
- The client receives Public key SHA-256 hashed Node-ID as the Tachyon DHT unique ID.
- User confirms stake token amount X and initiates lock request
    - Smart contract locks X from user’s wallet
- The client uploads [Node ID, Public Key, Locked(n), request(Register)] into the registration queue.
- Enlist as a trusted node after V SYSTEMS node verification.
    - Verify the node based on function Credit=Locked(n), and put it in trusted list. The more token the node stakes, the bigger session it gets, the credit is in direct ratio with locked stakes. To further protect the market from the malicious node, there will be a lock period of 7 days at least.

- The new verified node receives the Key ID by hashing its location, through XOR operation to look up the node whose Node ID is closed to its' Key ID and send store request to save its' IP: Port and Active time to the location's Key ID.

3.3 Session Economics

Tachyon Protocol is an open, P2P network where nodes provide services to each other and form a market. The cost of a Session is formed by simple laws of supply and demand. We envision the Tachyon protocol to be a large, open bazaar with lots of participating nodes and lots of economic activities.

- Provider node may set a minimum price range to maximize the possibility of getting orders;
- Client node may set a preferred price per unit (MB), and the client's account balance must be higher than the multiplication of preferred price-per-unit × requested amount of bandwidth;
- When the price-per-unit of the client node falls within the price range set by the provider node, it is considered that the two parties agree on the price;

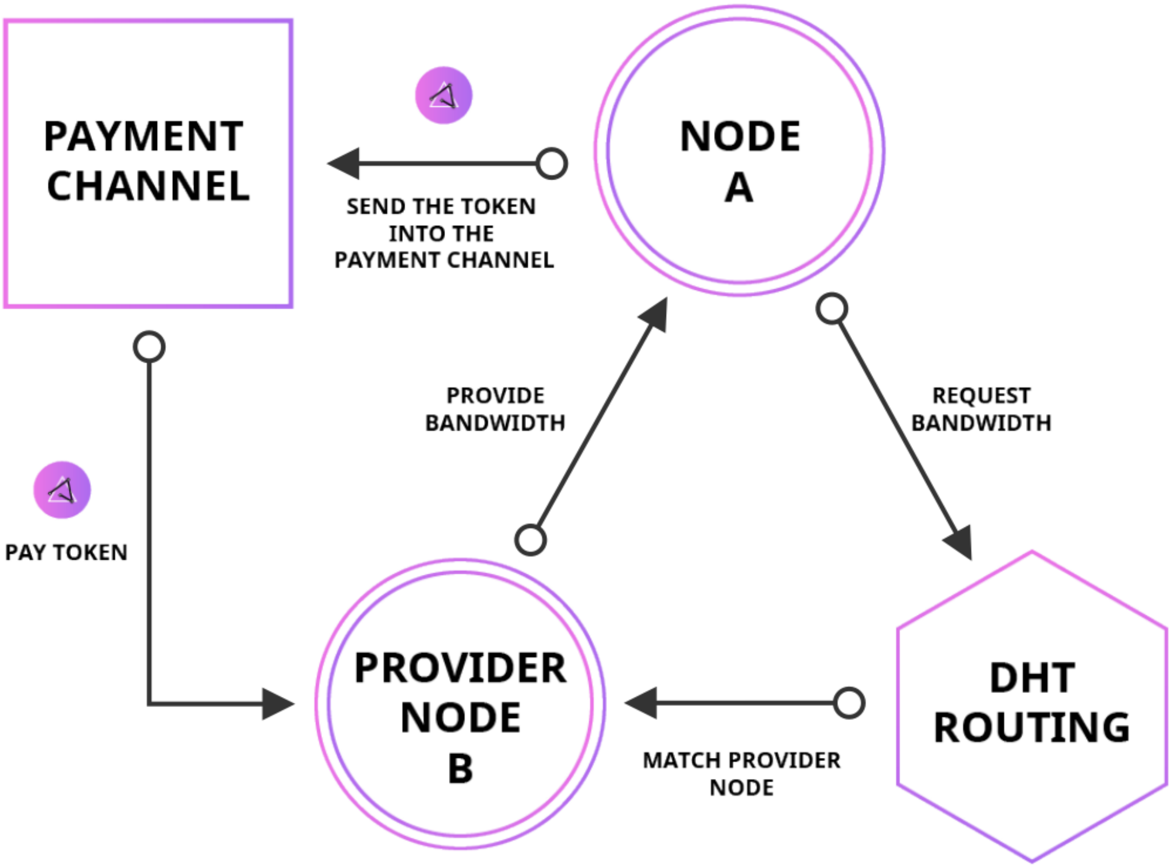
The user interface displays the price index generated by the current market average price for reference by both parties to the session. Both parties may change their pricing according to the price points through following ways:

- Change price for each session;
- Set a price for a specific time period where all sessions occurred within the period will be paid in that price.

3.4 Session Dynamics

Session is the core concept in the Tachyon Protocol. In a session, the client node establishes a transaction with the provider node through the Payment Channel, and the client node uses the traffic of the provider node and pays for it.

Though bandwidth has its standard measurement, bps, it cannot measure the actual quality of the bandwidth. Therefore the Tachyon Protocol will use bytes as the equivalent measurement as bandwidth and introduce payment channel to achieve the confirmation of the delivery service.



Let’s say that A is buying bandwidth and is matched to B by DHT Routing:

- A expects to use traffic
- A and B negotiate the Payment channel, A puts traffic worth of token m as the security deposit, set the bandwidth/token exchange rate and packet loss i;
- A starts using B's bandwidth after the connection is made:
  - Session Unit: A rounds up its TX & RX to B, then signs [Sum(TX, RX, n), Tachyon ID(A), Tachyon ID(B), Timestamp] and sends them to B in the Packet Header;
  - B receives the signed session unit from A, confirms the usage and signs [Sum(TX, RX, n), Tachyon ID(A), Tachyon ID(B), Timestamp] and sends them back to A in the Packet header;
  - A and B may now compare the numbers with other parties usage sign;
  - Every 5MB usage, A's session unit needs to include the hash value of B's last session unit; by doing that, it can ensure that both parties can acknowledge that they have received the session unit of the other party to form a chain of evidence.

- When the session is closed and there is no dispute, both parties can choose not to close the Payment channel but only close the connection.

    - If so, A&B don’t need to renegotiate the Payment channel in the future in order to reestablish the connection.
    - If any party requests to close the Payment channel, the last session signed by both parties will be settled to the main chain as the Payment channel is terminated. The equivalent of the tokens will be transferred to B.

- If the difference of usage from both parties is greater than Packet Loss(i), then B receives the token based on the lower usage count while A pays for the token based on B's usage count; the difference will also be cleared by the system.
- Either party may choose to blacklist the other party in case of distrust, and no connection will be made in the future. At the same time, this information will be broadcast to the network where other nodes may make their own judgment.
- To prevent Sybil Attack, Payment channel can only be initiated by the client nodes. The Provider nodes have the options to either accept or decline, and each provider nodes can only accept 5 Payment channels at the same time.

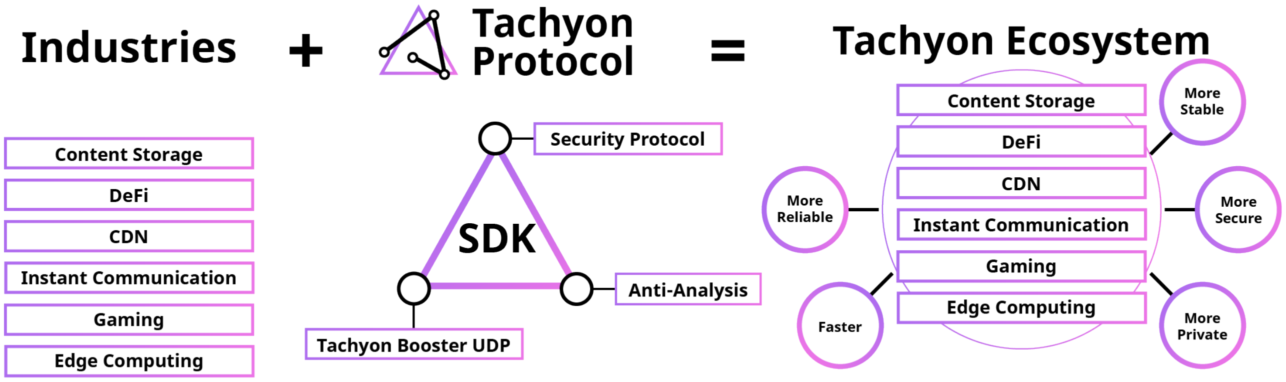
The advantage of this approach is that we can avoid service quality issues by using bytes as an equivalent measurement to bps. The frequent confirmations and information exchanges are the key to prevent fraud between two parties. The planned solution can achieve high frequency trading between A and B without a third party, and can reduce the handling fee in the session process, without writing an enormous amount of transactions to the host chain. For customer A and supplier B, cheating does not grant any financial returns. Assuming both parties are acting in their best interest, fraud shall not occur.

The cheating threshold, ie. the Packet Loss(i) can be negotiated by both parties. If the threshold is relatively low, the cheating party would not cause a serious loss on the other party.

There is no need for third party arbitration. For arbitration commission to work properly, it will require surveillance of the network, which contradicts our privacy-oriented and surveillance-free belief, and it may also introduce security vulnerabilities.

4. Tachyon Ecosystem

As a transport protocol, Tachyon Protocol will support many industries with its protocol stack and SDK, such as data storage, CDN, fast and reliable communication for IoT devices, edge computing and gaming, in building a secure, efficient, and robust Tachyon Ecosystem.



Rome wasn't built in a day. Likewise, Tachyon Protocol will release Tachyon VPN based on V SYSTEMS and Tachyon Protocol to experiment the viability and stability of the protocol stack as our first step of building the Tachyon Ecosystem; then we will integrate Tachyon Protocol into V SYSTEMS as the transport protocol, providing cybersecurity & acceleration solution for the ecosystem to further strengthen its stability. In the future, we envision Tachyon Protocol to be adopted by other blockchains, applying its capabilities in DeFi, gaming, internet surfing, instant communication, data distributing, and other areas.

4.1 Tachyon Protocol Use Cases

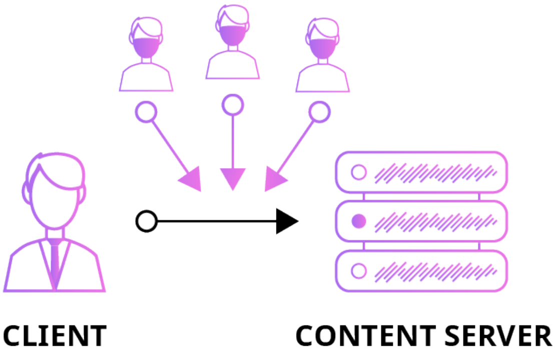
Versatility of the Tachyon Protocol as a transmission protocol allows a vast number of tangible use cases. Considering the technical architecture and advantages of Tachyon, we have put together several application scenarios that are most suitable for Tachyon Protocol.

4.1.1 Tachyon Protocol + VPN

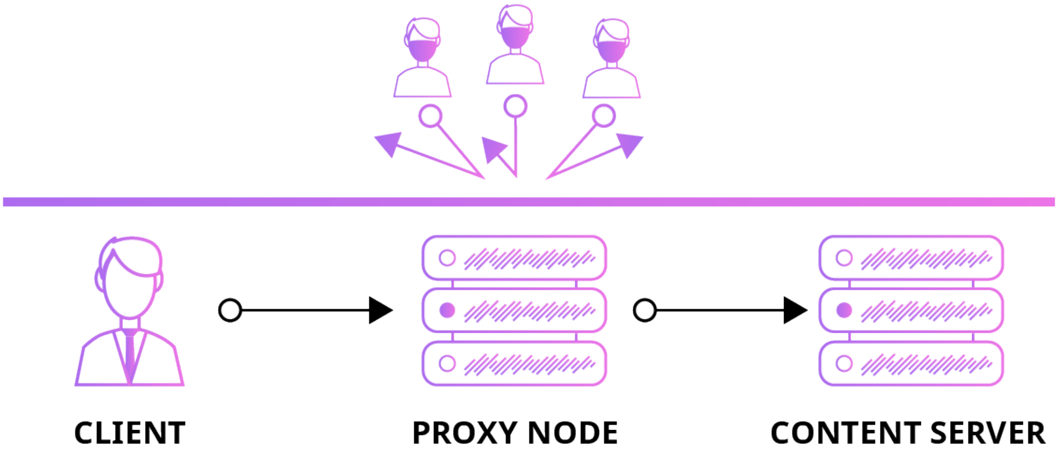
4.1.1.1 Centralized VPN

Mostly, the Client and Content Server are in a direct connection, where Content Server can obtain various information about the Client such as MAC address, IP, and activities. On an insecure LAN the attacker may easily monitor or replace the communication between the Client and Content

Server, which is why we tirelessly tell the internet that it is a bad idea to use public WiFi without protection.



By adding Proxy Node between the Client and the Content Server, as well as encryption on both ends of the VPN tunnel, the Content Server would only receive information from the Proxy Node, at the same protecting the message from the attacker.



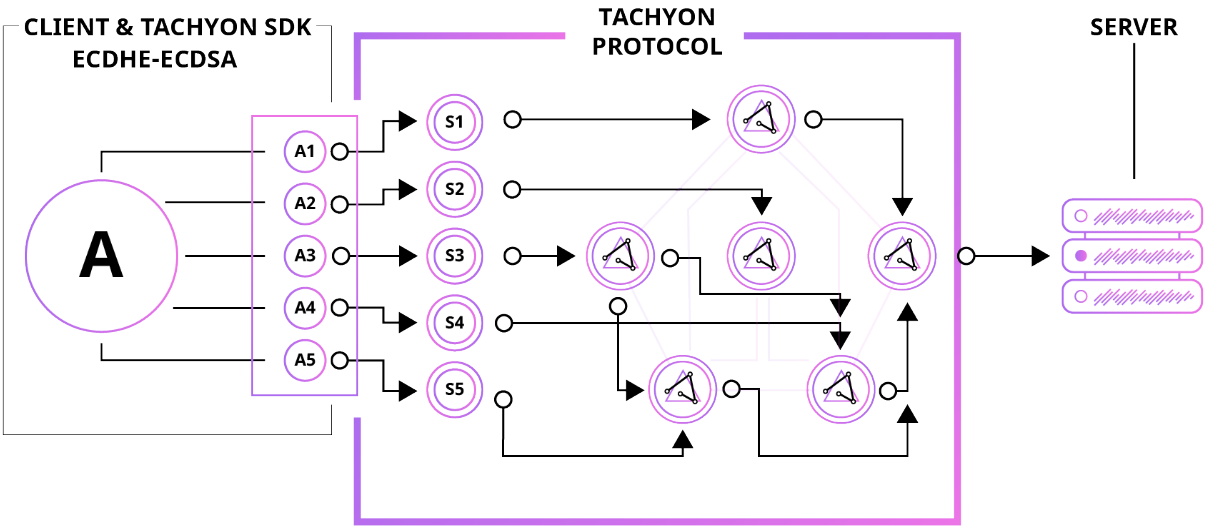
In this model, the Client places all the responsibility for network security and privacy protection on the VPN service provider, relying on it being honest and trustworthy, which is unreliable in the real business environment.

4.1.1.2 Tachyon VPN

Centralized VPN has limited credibility in providing cybersecurity and privacy protection. If we are to replace the Proxy Node between the Client and Content server with Tachyon Protocol network, the aforementioned problem can be perfectly solved.

- Architecturally, network topology is constructed with a number of geographically distributed nodes, which are able to recognize each other and communicate.

- The Tachyon network ensures proper identification of the nodes by using a cryptographic token residing on the established V SYSTEMS blockchain. At the same time, information asymmetry of unfamiliar nodes is reduced, ensuring the smooth operation of the network even on the largest of scales.
- Requirement that node providers “stake” a security deposit, and verify on the V SYSTEMS main chain, bring protection against Sybil and Eclipse attacks and align the interests of the Network with the Provider Node.
- The use of token provides an easy, affordable means of sharing spare bandwidth of not only the nodes, but all the network users.



- Connection workflow
    - The Client wants to use traffic from a certain region to find the nodes that can provide traffic through DHT;
    - The system monitors the latency, packet loss and bandwidth information between Nodes in real time in order to calculate the transmission efficiency between Nodes. Systems always selects the path with the fastest transmission speed;
    - The communication between the Client and each Tachyon Node is end-to-end ECDHE+ECDSA encrypted and authenticated to protect the transmission data;
    - The Client will separate the requests in the encrypted Information (A) into different IP packets, and transmit them through different routing paths;
    - The IP Packet simulation is transmitted as the request to access websites like google.com and BBC News;
    - Content Server receives the requests and then decrypts them.

Tachyon VPN will bring ultra cost-effective blockchain solutions that ensure advanced cybersecurity and privacy protection directly to all users.

4.1.2 Tachyon Protocol + Decentralized Storage

IPFS already uses the same underlying foundations as Tachyon Protocol with DHT as the foundation for storing data indexes. This demonstrates Tachyon's intrinsic ability to be used for data storage, however, unlike IPFS, Tachyon Protocol will have the following advantages:

- **Add an extra layer of protection by encrypting the contents in storage and during transmission;**
- **Accelerate the transmission efficiency as demonstrated in chapter 2.1.**

4.1.3 Tachyon Protocol + CDN

As a content distribution network, CDN network has the advantages of: (1) the number and distribution of edge nodes and; (2) the speed of network synchronization. The decentralized Tachyon network distributes tens of millions of nodes around the world so the quantity and coverage exceed the centralized CDN service. Also, thanks to TBU protocol, **Tachyon CDN's sync speed will be superior to any centralized CDN's sync speed.**

4.1.4 Tachyon Protocol + DeFi

Decentralized Finance (DeFi) uses the blockchain technologies and smart contract to form a machine & algorithm-based trust to replace the human agents and third party-agencies with a goal to provide a transparent, efficient and low-cost financial system. With the use of Tachyon Protocol SDK, exchanges, DApps, wallets and company servers can employ more advanced security and privacy protection to their services as well as provide greater transmission efficiency to their users.

4.1.5 Tachyon Protocol + IoT

As an important part of the new generation information technology, IoT has been widely used in various industries, such as smart home, internet of vehicles, industrial manufacturing, environmental monitoring, environmental sensors, etc. IoT network requires a large number of nodes to interact and cooperate, so it has higher network requirements:

- P2P communication between devices;
- Low latency of transmission between devices;

- Relatively high requirements for information security during the transmission process.
- Safe and fast transfer of data between the nodes.

With the development of 5G, IoT will have a broader application scenario. In the future, Tachyon Protocol can be used as **the IoT communication protocol to provide a more secure and fast information transmission service.**

4.1.6 Tachyon Protocol + DNS

Ever since the start of internet, DNS has been one of the power centers for this new, digital world. Whoever controlled the global DNS records, was able to actively promote or almost completely block any website. Centralization of DNS records presents a global threat to internet freedom and transparency. Decentralized DNS will ensure complete liberalization, and Tachyon protocol is ready for the role. By combining the speed and security improvements already outlined above, as well as using V SYSTEMS chain to immutably store all records, without any fear of privacy issues, or the possibility of censorship by third parties, Tachyon will provide a new-generation, transparent DNS platform for all.

5. Economic System

5.1 The IPX Token

The native digital cryptographically-secured utility token of Tachyon Protocol (IPX Token) is a transferable representation of attributed functions specified in the protocol/code of Tachyon Protocol, designed to play a major role in the functioning of the ecosystem on Tachyon Protocol, and intended to be used solely as the primary utility token on the platform. The IPX token will initially be issued as a digital asset residing on the V SYSTEMS blockchain network. The token provides an easy, affordable means of sharing spare bandwidth for the network users, with the aim to strengthen sustainability and growth in the network. The introduction of an appropriate token economics will promote the positive development of the network, solve major problems with organization of the decentralized Tachyon network and serve as a proxy to valuation of the overall system.

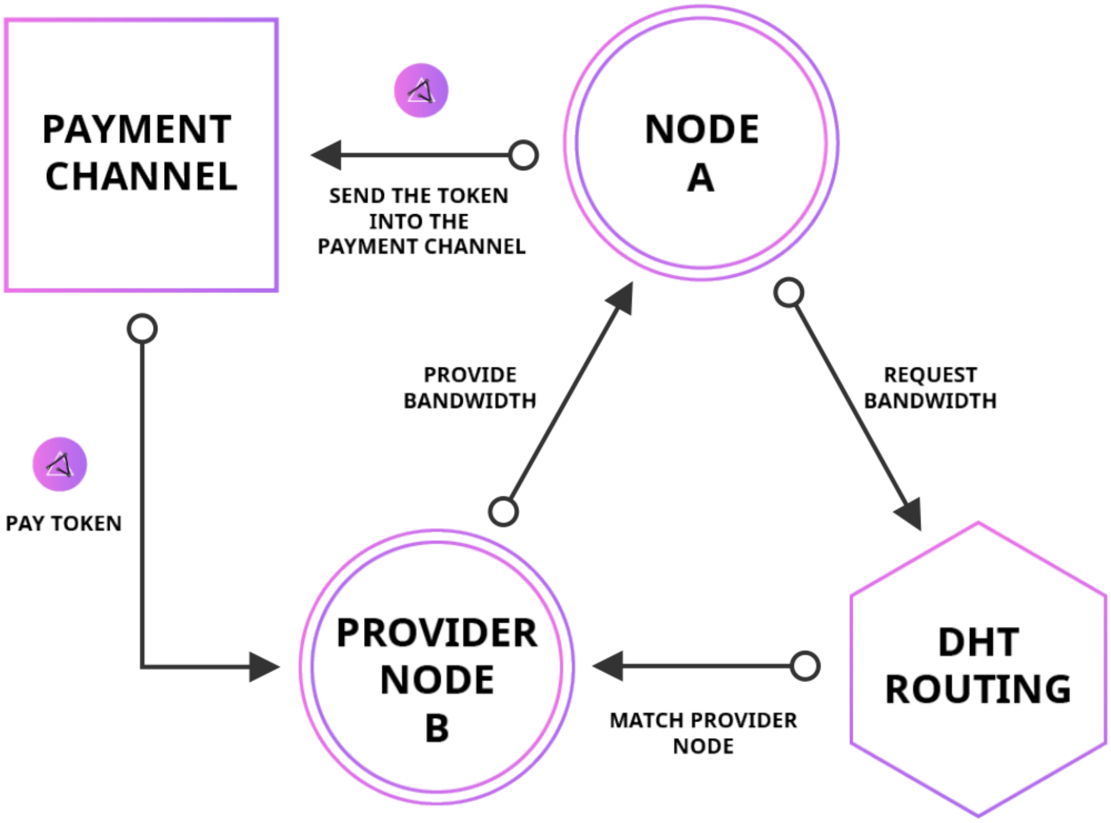
The initial supply of the IPX token is 1,000,000,000 (one billion). As token hosted by the V SYSTEMS blockchain, IPX token serves a clear purpose and utility in the overall Tachyon ecosystem.

IPX Token use cases:

- IPX Token is a non-refundable functional utility token which will be used as the medium of exchange between participants on Tachyon Protocol. The goal of introducing IPX Token is to provide a convenient and secure mode of payment and settlement between participants who interact within the ecosystem on Tachyon Protocol (e.g. users and nodes);
- The IPX token will serve the purpose of identity verification necessary for the ordinary operations of the network. This is essential to the security of Tachyon Protocol Network, as without token for identity verification, the malicious nodes can easily monitor the traffic and undermine the security of the network;
- The IPX token is usable as an indication of commitment of users within the network. The IPX token enables the Tachyon market to operate by means of pre-session locking, instant checkout and session fee collection. Without a token, we cannot resolve Sybil and Eclipse attacks which would result in the whole network being rendered inoperable.
- As an important part of incentive and coordination mechanism, the IPX token is also crucial to the expansion of the network boundary the development of the Tachyon ecosystem. IPX Token provides the economic incentives which will be consumed to encourage participants to contribute and maintain the ecosystem on Tachyon Protocol (users of Tachyon Protocol and/or holders of IPX Token which did not actively participate will not receive any IPX Token incentives). Without token, nodes are not incentivized to join the network, resulting in the inability to produce value for other business scenarios and the settlement.

- Computational resources are required for operating the network, thus providers of these services / resources would require payment for the consumption of these resources to maintain network integrity, and IPX Token will be used as the medium of exchange to quantify and pay the costs of the consumed computational resources. IPX Token is an integral and indispensable part of Tachyon Protocol, because without IPX Token, there would be no incentive for users to expend resources to participate in activities or provide services for the benefit of the entire ecosystem on Tachyon Protocol.
- As an indication of commitment to the system, nodes would be required to place an amount of IPX Token as security deposit before it may participate, so as to ensure service standards and prevent malicious behavior.
- Another purpose is that the token serves to ensure the network is driven by the community participants, and not the Tachyon team, which will prolong the vitality of the project.

5.2 IPX Token Economics



- The User in the network needs to use a certain amount of bandwidth to send its demand and expected transaction price to DHT Routing;
- DHT Routing matches the user with Provider Node based on the latency, packet-loss, bandwidth, and credit of providers in the network;

- The User establishes payment channel with Provider Node, and puts the equivalent token in the Payment channel to be locked, while Provider Node provides bandwidth for the user;
- After the session ends, Payment channel transfers the agreed IPX tokens to the Provider Node as service fee according to the transaction amount confirmed by both parties. For each exchange of services on the Tachyon Protocol, the costs are to be quantified in IPX Token and paid to the Tachyon Protocol and/or the other party providing the service.

IPX Token does not in any way represent any shareholding, participation, right, title, or interest in the Company, the Distributor, its affiliates, or any other company, enterprise or undertaking, nor will IPX Token entitle token holders to any promise of fees, dividends, revenue, profits or investment returns, and are not intended to constitute securities in Singapore or any relevant jurisdiction. IPX Token may only be utilized on Tachyon Protocol, and ownership of IPX Token carries no rights, express or implied, other than the right to use IPX Token as a means to enable usage of and interaction within Tachyon Protocol. IPX Token are designed to be consumed/utilized, and that is the goal of the IPX Token issuance. In fact, the project to develop Tachyon Protocol would fail if all IPX Token holders simply held onto their IPX Token and did nothing with it.

In particular, it is highlighted that IPX Token: (a) is non-refundable and cannot be exchanged for cash (or its equivalent value in any other virtual currency) or any payment obligation by the Company, the Distributor or any affiliate; (b) does not represent or confer on the token holder any right of any form with respect to the Company, the Distributor (or any of its affiliates), or its revenues or assets, including without limitation any right to receive future dividends, revenue, shares, ownership right or stake, share or security, any voting, distribution, redemption, liquidation, proprietary (including all forms of intellectual property or license rights), or other financial or legal rights or equivalent rights, or intellectual property rights or any other form of participation in or relating to Tachyon Protocol, the Company, the Distributor and/or their service providers; (c) is not intended to represent any rights under a contract for differences or under any other contract the purpose or pretended purpose of which is to secure a profit or avoid a loss; (d) is not intended to be a representation of money (including electronic money), security, commodity, bond, debt instrument or any other kind of financial instrument or investment; (e) is not a loan to the Company, the Distributor or any of its affiliates, is not intended to represent a debt owed by the Company, the Distributor or any of its affiliates, and there is no expectation of profit; and (f) does not provide the token holder with any ownership or other interest in the Company, the Distributor or any of its affiliates.

The contributions in the token sale will be held by the Distributor (or its affiliate) after the token sale, and contributors will have no economic or legal right over or beneficial interest in these contributions or the assets of that entity after the token sale. To the extent a secondary market or exchange for trading IPX Token does develop, it would be run and operated wholly independently of the Company, the Distributor, the sale of IPX Token and Tachyon Protocol. Neither the Company nor the Distributor will create such secondary markets nor will either entity act as an exchange for IPX Token.

5.2.1 Provider Node Staking

To ensure the rewards are issued to the provider nodes that actually contribute to the network, the provider nodes must obtain enough IPX Token to become verified. Provider nodes are required to pay a security deposit in the amount of 200,000 IPX tokens after tokens are idle for a minimum of 7 days in order to complete the node verification. This is done in order to prevent the scenario where network is flooded by malicious or inactive nodes. This adjustable period of 7 days is called: “wind up period”, and it is set to align the interests of the network and the potential provider node. However, the speculative value of the IPX token may fluctuate while the tokens are locked in the smart contract. We’ve decided to have inflation based reward system of 5% per annum to encourage the nodes to keep providing the service to the network regardless of the speculative value of the token. The annual reward of 5%, along with mandatory lock-up phase, simulates the Proof of stake “staking” or “minting” found in some blockchain networks. This should help reduce the holding risk and opportunity cost of the operating node.

As we want inflation to happen at provider nodes, we have developed a system which forces the provider nodes to be active in order to get paid. Nodes are required to be active, as well as offer quality service in order to reap both the staking rewards and the session fees. The economic system is set in such a way to generously reward nodes which are active, provide a good service to the customers and to decentralize the nodes which are inactive or provide a poor service.

Trail of successfully completed sessions will be permanently recorded on the V SYSTEMS blockchain, which is used as proof that the provider node is active. That is, we can tell how active the node is by watching the paper trail of receipts left on an immutable public blockchain. A moving average (MA) is to be calculated from the trail left on the blockchain, and if the value of the MA is within the parameters set in the smart contract, the provider node can claim the staking reward from the smart contract based on it’s token balance. The value of the parameter which dictates how many successful monthly sessions should a node complete in order to reap the reward, is still not decided. It shall be decided after additional in-house tests.

In case provider node has been eligible to staking rewards, i.e. there is proof of activity, the node is not allowed to withdraw the tokens from the smart contract lock for a minimum of one week (7 days) after the last completed session. This “unwind” period is set to avoid certain scenarios where malicious provider node has nothing to lose if it tries to harm the network in some way. This is done in order to align the interests of the network and the provider node.

5.2.2 Session Fees

Beside the staking reward, provider nodes are also rewarded in the form of session fees, as we've already explained in chapter 3.4. This economic system creates an economic opportunity for anyone who has access to good internet connection and is willing to participate in the Tachyon network.

5.3 Supply and Demand Dynamics

Supply/demand dynamics of the IPX token revolve around the following factors:

- Demand from new provider nodes which want to join the network;
- Demand from users who want to use the network;
- Supply from the provider nodes who sell their session fee profits;
- Supply from the provider nodes who sell their staking profits;
- Other market dynamics resulting from temporary gaps in supply/demand and speculative activity of traders.

5.4 Community Governance

We believe that in order to successfully transition the project from "rule of the few", that is our team, to "rule of the many", that is our community and project supporters - we must set forth a solid plan for the user governance. A well defined system of governance allows a cryptocurrency network to endure the test of time and grow past its original creators.

While designing the token economics for the Tachyon Protocol we've studied a myriad of tokens and their governing structure and noticed that the trend is to allow for some kind of direct stakeholder governance by forming a DAO. We have looked into a number of DAO solutions, some hosted on Ethereum blockchain and some who run their own respective blockchains, and came to the conclusion that DAO concept would be a great fit for our project.

Specifically, the plan is to have a decentralized system of project support, in the form of grants for various community projects, and always subject to the prevailing regulatory environment. Not all motions must be about project support, motion/grant system can be used to decide upon other important elements or used as an opinion poll.

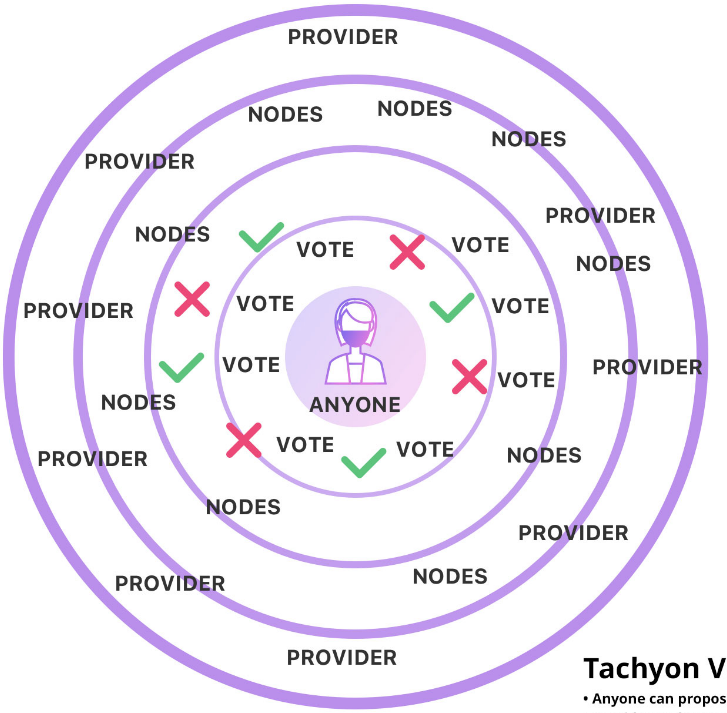
5.4.1 Motions and Grants

Any stakeholders can announce their intentions by publishing a motion. Motions have no direct impact on the network, it is simply a declaration of intention. To pass motions require 50% + one of provider nodes agreeing on the motion. Motion is defined by its organizer, clear goals of the action, requested grant and estimated time of completion. Organizer of the motion must be clear in defining the goals of the action to present the value to the community and come up with a realistic time of delivery in order to improve their reputation. In essence, motions are backed by the reputation of its organizer. Some motions will inevitably be frauds, but community will quickly form an opinion on who is a respected and trusted member of the community and who is a fraudster. In order to minimize the effect of bad motions, it is advised that bigger grants are split into tranches which are judged and voted-in independently. This was demonstrated in past experiments with user governance with other blockchain projects. Communities are agile and wise, if given the right set of tools they can operate the project in decentralized fashion. Each motion, if it passes, is paid directly from the smart contract to the organizer who proposed it. That is, new IPX tokens are created directly from the smart contract in order to facilitate the payment.

To enable all parties to easily explore and decide on the motions, a community hub will be implemented in the form of an easy-to-use website. For the avoidance of doubt, the right to vote is restricted solely to voting on features of Tachyon Protocol; the right to vote does not entitle IPX Token holders to vote on the operation and management of the Company or its affiliates, or their assets, and does not constitute any equity interest in the Company or its affiliates.

5.4.2 Provider Node Voting

Provider nodes vote on motions using the simple set of commands: “vote yes”, “vote no”, or in case they choose not to act: “vote abstain”. The votes are recorded on the host V SYSTEMS blockchain, and are scored according to the staked balance of the provider node.
Only active nodes are eligible to vote on motions, as defined in chapter 5.2.



Tachyon Voting

- Anyone can propose motions
- Provider nodes vote to grant motions
- Community governance

6. Risks

You acknowledge and agree that there are numerous risks associated with purchasing IPX Token, holding IPX Token, and using IPX Token for participation in Tachyon Protocol. In the worst scenario, this could lead to the loss of all or part of the IPX Token which had been purchased. **IF YOU DECIDE TO PURCHASE IPX Token, YOU EXPRESSLY ACKNOWLEDGE, ACCEPT AND ASSUME THE FOLLOWING RISKS:**

6.1 Uncertain Regulations and Enforcement Actions

The regulatory status of IPX Token and distributed ledger technology is unclear or unsettled in many jurisdictions. The regulation of virtual currencies has become a primary target of regulation in all major countries in the world. It is impossible to predict how, when or whether regulatory agencies may apply existing regulations or create new regulations with respect to such technology and its applications, including IPX Token and/or Tachyon Protocol. Regulatory actions could negatively impact IPX Token and/or Tachyon Protocol in various ways. The Company, the Distributor (or its affiliates) may cease operations in a jurisdiction in the event that regulatory actions, or changes to law or regulation, make it illegal to operate in such jurisdiction, or commercially undesirable to obtain the necessary regulatory approval(s) to operate in such jurisdiction. After consulting with a wide range of legal advisors and continuous analysis of the development and legal structure of virtual currencies, a cautious approach will be applied towards the sale of IPX Token. Therefore, for the token sale, the sale strategy may be constantly adjusted in order to avoid relevant legal risks as much as possible. For the token sale, the Company and the Distributor are working with Tzedek Law LLC, a boutique corporate law firm in Singapore with a good reputation in the blockchain space.

6.2 Inadequate disclosure of information

As at the date hereof, Tachyon Protocol is still under development and its design concepts, consensus mechanisms, algorithms, codes, and other technical details and parameters may be constantly and frequently updated and changed. Although this white paper contains the most current information relating to Tachyon Protocol, it is not absolutely complete and may still be adjusted and updated by the Tachyon team from time to time. The Tachyon team has no ability and obligation to keep holders of IPX Token informed of every detail (including development progress and expected milestones) regarding the project to develop Tachyon Protocol, hence insufficient information disclosure is inevitable and reasonable.

6.3 Competitors

Various types of decentralized applications and networks are emerging at a rapid rate, and the industry is increasingly competitive. It is possible that alternative networks could be established that utilize the same or similar code and protocol underlying IPX Token and/or Tachyon Protocol and attempt to re-create similar facilities. Tachyon Protocol may be required to compete with these alternative networks, which could negatively impact IPX Token and/or Tachyon Protocol.

6.4 Loss of Talent

The development of Tachyon Protocol greatly depends on the continued co-operation of the existing technical team and expert consultants, who are highly knowledgeable and experienced in their respective sectors. The loss of any member may adversely affect Tachyon Protocol or its future development. Further, stability and cohesion within the team is critical to the overall development of Tachyon Protocol. There is the possibility that conflict within the team and/or departure of core personnel may occur, resulting in negative influence on the project in the future.

6.5 Failure to develop

There is the risk that the development of Tachyon Protocol will not be executed or implemented as planned, for a variety of reasons, including without limitation the event of a decline in the prices of any digital asset, virtual currency or IPX Token, unforeseen technical difficulties, and shortage of development funds for activities.

6.6 Security weaknesses

Hackers or other malicious groups or organizations may attempt to interfere with IPX Token and/or Tachyon Protocol in a variety of ways, including, but not limited to, malware attacks, denial of service attacks, consensus-based attacks, Sybil attacks, smurfing and spoofing. Furthermore, there is a risk that a third party or a member of the Company, the Distributor or its affiliates may intentionally or unintentionally introduce weaknesses into the core infrastructure of IPX Token and/or Tachyon Protocol, which could negatively affect IPX Token and/or Tachyon Protocol.

Further, the future of cryptography and security innovations are highly unpredictable and advances in cryptography, or technical advances (including without limitation development of quantum computing), could present unknown risks to IPX Token and/or Tachyon Protocol by rendering ineffective the cryptographic consensus mechanism that underpins that blockchain protocol.

6.7 Other risks

In addition, the potential risks briefly mentioned above are not exhaustive and there are other risks (as more particularly set out in the Terms and Conditions) associated with your purchase, holding and use of IPX Token, including those that the Company or the Distributor cannot anticipate. Such risks may further materialize as unanticipated variations or combinations of the aforementioned risks. You should conduct full due diligence on the Company, the Distributor, its affiliates and the Tachyon team, as well as understand the overall framework, mission and vision for Tachyon Protocol prior to purchasing IPX Token.

Glossary

DHT (Distributed Hash Table) - a class of a decentralized distributed system that provides a lookup service similar to a hash table: (key, value) pairs are stored in a DHT, and any participating node can efficiently retrieve the value associated with a given key.

UDP (User Datagram Protocol) - one of the core members of the Internet protocol suite. With UDP, computer applications can send messages - in this case referred to as datagrams - to other hosts on an Internet Protocol (IP) network.

SDK (Software Development Kit) - typically a set of software development tools that allows the creation of applications for a certain software package, software framework, hardware platform, computer system, video game console, operating system, or similar development platform.

CDN (Content Distribution Network) - a geographically distributed network of proxy servers and their data centers. The goal is to provide high availability and high performance by distributing the service spatially relative to end-users.

CSMA (Carrier Sense Multiple Access) - a media access control (MAC) protocol in which a node verifies the absence of other traffic before transmitting on a shared transmission medium, such as an electrical bus or a band of the electromagnetic spectrum.

API (Application Programming Interface) - an interface or communication protocol between a client and a server intended to simplify the building of client-side software. It has been described as a “contract” between the client and the server, such that if the client makes a request in a specific format, it will always get a response in a specific format or initiate a defined action.

FEC (Forward Error Correction) - a technique used for controlling errors in data transmission over unreliable or noisy communication channels. The central idea is that the sender encodes the message in a redundant way, most often by using an error-correcting code (ECC).

SMTP (Simple Mail Transfer Protocol) - a communication protocol for electronic mail transmission. Mail servers and other message transfer agents use SMTP to send and receive mail messages.

Session - the core concept in the Tachyon Protocol. In a session, the client node establishes a transaction with the provider node through the Payment Channel, and the client node uses the traffic of the provider node and pays for it.

Session Unit - a record signed by Node’s private key that records its usage to ensure that the record is approved.

DU (Data Unit) - default unit in which data transfer is measured in MB.

DAO (Decentralized Autonomous Organization) - an organizational form that can be autonomously executed under a series of open and fair rules without intervention and central management.

Bibliography

[1] J. Zeng, *Several vulnerability analysis and evaluation of blockchain Application system*. 2019, pp. 26–28.

[2] S. King, K. Shan, R. Zhang, and S. Nadai, “V SYSTEMS: Blockchain Database and Apps Platform.” [Online]. Available: https://v.systems/static/vsyswhitepaper.pdf. [Accessed: 17-Sep-2019]

[3] Santitoro and Ralph, “Metro Ethernet Services – A Technical Overview.” [Online]. Available: https://www.mef.net/Assets/White_Papers/Metro-Ethernet-Services.pdf. [Accessed: 17-Sep-2019]

[4] Benet and Juan, “IPFS - Content Addressed, Versioned, P2P File System(DRAFT 3).” [Online]. Available: https://github.com/ipfs/papers/raw/master/ipfs-cap2pfs/ipfs-p2p-file-system.pdf. [Accessed: 17-Sep-2019]

[5] R. Eric, O. Kazuho, S. Nick, and W. . Christopher, “Encrypted Server Name Indication for TLS 1.3 draft-ietf-tls-esni-01.” [Online]. Available: https://tools.ietf.org/html/draft-ietf-tls-esni-01. [Accessed: 17-Sep-2019]

[6] D. George and S. Stefan, “On Network formation, (Sybil attacks and Reputation systems).” [Online]. Available: http://archive.dimacs.rutgers.edu/Workshops/InformationSecurity/slides/gamesandreputation.pdf. [Accessed: 17-Sep-2019]