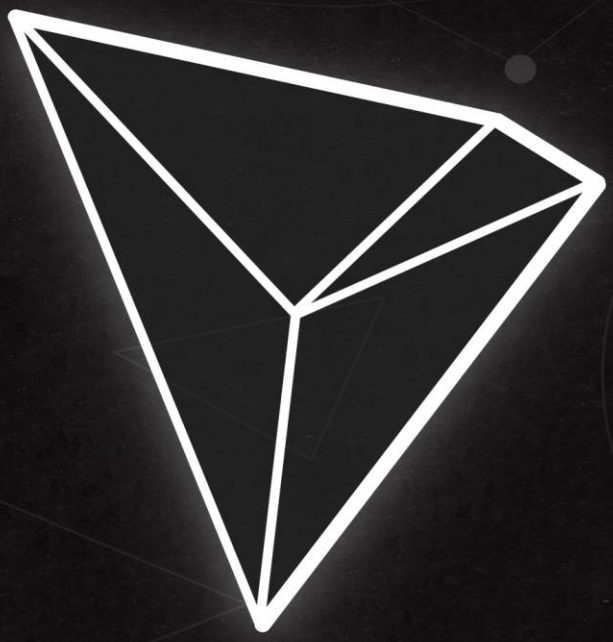


TRON

Whitepaper

Contents in this version V1.7 are subject to change at any time as required for the project progress

Preface | Heal the Internet

Tim Berners-Lee, inventor of the world wide web (WWW) who has been honored with the 2016 Turing Award, issued a statement in 2017, indicating that its invention Internet is deviating from its original intention.

Yes, there has been something wrong with the Internet over the years.

At the time when Tim Berners-Lee invented the Internet initially, Internet was a fully decentralized platform, with which anyone may create contents, webpage and websites and freely interact with others. However, current Internet has developed into a stunner that governs business, communication, entertainment and information from then simple academically researched sharing network.

The Internet's power structure is also changing.

Undoubtedly, the Internet belongs to the corporations of over USD 100 billion each who define the rules of the Internet rather than everyone, which include Amazon, Facebook, Google, Apple, as well as Alibaba and Tencent in China.

With the Internet traffic, data and contents becoming concentrated, there are mainly such giants as Facebook, Messager, Instagram and Snapchat, but China focuses on the Apps including Wechat, Toutiao.com, Taobao and QQ.

Such giants own and benefit from the numerous data created by billions of users throughout the world, with the power to create those read, gained and wished by users.

Giants, other than users themselves, own the ability to control data. The data created by users belong to its owners no longer. Due to the inappropriateness of an attempt to retake data initiatives and the difficulty in building websites and Apps, we have to attempt to accommodate ourselves to the rules of WeChat and Facebook, and presume

the distribution mechanisms of Weibo and Twitter, thus losing our own features. In spite of a self-made App, it is easily withdrawn from Apple.

However, it is never easy to destroy a person, a thing and a cause.

Substantially, Internet has no longer been fully decentralized, and even becomes more centralized than the old forces which have been overturned by it, including newspapers, magazines and records, since newspapers may be collected, but no micro blogs can be backed up.

TRON is an attempt to heal the Internet.

Regardless of the inappropriateness of the attempt in the opinion of giants, or the failure arising out of an overestimation of the ability in the opinion of ordinary people, or success in the thing or not.

We believe, users must have the ownership and power of disposal of the data they create, which will not be assigned to the platform, and users freely own all digital information.

We believe, users must have the final power to make a decision on reading and gaining of contents, and information must be distributed on a free and volunteer basis, at the option of users.

We believe, users must be entitled to the incentives of digital assets using data on a free basis, which will be no longer bound by any platform and will be protected by the decentralized internet.

All of these are subject to a decentralized protocol called TRON.

This is an action against the centralized internet, in which we might fail, but someone is believed to succeed.

This is because decentralized internet is just as it is.

1. What is TRON?

TRON is a blockchain-based decentralized protocol that aims to construct a worldwide free content entertainment system with the blockchain and distributed storage technology. The protocol allows each user to freely publish, store and own data, and in the decentralized autonomous form, decides the distribution, subscription and push of contents and enables content creators by releasing, circulating and dealing with digital assets, thus forming a decentralized content entertainment ecosystem.

With the strengths of social network and value network, TRON is committed to ecological prosperity. In relation to any community, economy and free market economy, an incentive system that fairly and reasonably reflects the contributions made by participants is fundamental. TRON will attempt to accurately and transparently measure and motivate relevant participants and contributors using digital assets for the first time, thus enabling content ecosystem.

2. Value of TRON

In the beginning of designing TRON, the following core values are always adhered to:

1. Date creators (users) will have the fundamental ownership of data, and the internet should be decentralized. This was proposed by doctor Tim Berners-Lee at the time when the internet was born and the original intention for creation of the internet.

2. Those who make a contribution to ecological TRON will be entitled to proportional profits according to rules. A value network has the greatest advantage that may digitally capitalize anything in social and media networks.

3. All forms of contribution should be of equal quantitative value. Substantially, the time invested by participants, excellent contents created and attention are of the measure value as equal as the furnished capitals.

4. The fundamental objective of TRON is to provide services for the public. As an ecology operated by a non-profit foundation, TRON is designed to serve the masses who enjoy content entertainment throughout the world, rather than for the purpose of gaining profits. All TRON participants will benefit from its prosperity.

5. Contents should derive from people rather than capitals which should be used to reward people rather than to control people. Cultural and creative industries should be mainly driven by the pursuit of the quality of art and contents by content creators, artists and scriptwriters rather than the capitalists who consume no contents.

3. Infrastructures Provided by TRON

TRON will provide relevant participants with the following infrastructures:

1. High-quality content platform

2. Social network that allows a link among all people

3. Digital currency as a bridge

4. Payment network

5. Autonomous ecosystem

4. Characteristics of TRON

As a decentralized content protocol, TRON is of the following four basic characteristics compared with the centralized internet:

1. Data liberation: on a free and uncontrolled basis, the contents including characters, pictures, audios and videos may be unloaded, stored and spread.

2. Content enabling: digital assets are obtained through provision and spread of contents, thus economically stimulating the enabling of content ecology.

3. Personal ICO: an individual may freely distribute digital assets in the form of ICO, while others may enjoy the benefits and services brought due to the continuous development of data contributors by purchasing digital assets.

4. Infrastructure: with distributed digital assets will be equipped with a complete set of decentralized infrastructures, including distributed exchange, autonomous gaming, forecast and game system.

5. How to Achieve Stimulation by TRON?

Fundamentally, TRON design requires the monetization of content economy. TRON mechanism is based on economic stimulation contents and monetized in an encrypted manner. Economic stimulation achieved through cryptology may greatly contribute to the growth of a content platform, and it is believed that cryptocurrency could unprecedentedly stimulate content ecology.

TRON will propose a set of improved mechanism to evaluate an individual's

ecological contribution. Most of existing platforms adhere to the principle of one-user one-vote, which easily cause the breaking of limitation of repeated voting and the request for control of junks and attacks. Existing content platforms have been

controlled by profit demands and centralized mechanisms, and the contents we read are those which the centralized platform wish us to read, rather than those which we wish. Due to the unfair algorithm of information flow, Weibo, Toutiao.com, WeChat and Facebook are gradually becoming controlled tools. Advertising platforms are taken as the first profit-gaining mode, among which Phoenix Nest, Ads recommendation algorithm of Toutiao.com, advertising system of WeChat, promotion program of Weibo and ad channel of Taobao are typical cashing modes and unable to enable the contents which attract traffic.

However, with TRON, the economic stimulation system is expected to become a circulatory system in a decentralized manner, enabling users to have a platform to enjoy their favorite contents without conflicting with profit demands. The autonomous system formed by TRON will also unprecedentedly enable ecosystem members, thus forming a autonomous ecosystem rather than current flat user mechanism.

In ecological management and decision-making, TRON only allows the users who involve themselves in the periodical unfreezing of TRX for many years to cast a vote. Under the model, community members will be encouraged to hold TRX for a long term, which will maximize the long-term value of TRON.

6. Realization Path of TRON

It is expected that it takes 8 to 10 years to implement the whole system of TRON, a large program involving 6 steps. Specifically, the realization paths are as follows:

1. Exudos, Data Liberation

A mechanism of upload, storage, and distribution which is based on peer-to-peer and distributed contents.

In the Exodus phase, on the basis of the distributed storage technology represented

by IPFS, TRON will provide users with a completely free and reliable platform for data publication, storage and dissemination.

2. Odyssey, Content Empowerment

Economic incentives, empowerment, content ecology and block chain technology will create a fully competitive economic mechanism with fair returns for content creation, distribution and dissemination. Therefore, individuals can be encouraged and contents can be empowered, thus constantly expanding the boundary of the system.

Of the centralized internet system, in the vast majority of cases, content producers earn cash through advertising models. But the efficiency of obtaining cash has been extremely low due to the fact that the user experience is seriously dampened by the annoyingly strong harassment brought by the existing advertising push mode. Other contents have also confronted with troubles. Despite that cash is gained through tipping and gifting functions for other contents, their profits shall be deducted by 30%-90% due to a lack of paying system. What's worse, hindered by the huge randomness of the tipping model, most content providers cannot break even.

Content creators are in urgent need of a content protocol with a self-paying system. Access to contents can be measured by the payment, and the payment and purchase are based on transparent records of block chain.

TRON protocol is the block chain's entertainment system of free content, in which TRX, the coin of TRON, is circulated. Its native economic system enables an unprecedented one-to-one interaction between providers of digital entertainment contents and ordinary users, and therefore, providers no longer need to pay high channel fees to centralized platforms like Google Play and APP Store. On the other side, providers of contents like text, picture, video and broadcast, will break their curse that popularity and hits cannot create cash. The tipping model focuses on the popularity, and the popularity increases as the tipping rises. The distributed clearing and storage mode will also enable developers and content

providers full freedom of creation, without being restricted by centralized managers.

In the TRON system, content producers can have direct access to TRX, the TRON coin paid by fan users for premium contents. They can also obtain influence and power of spread through creating high-quality contents, thus directly gaining TRX rewards given by the system.

Example of value score of user operation that takes content distribution as major weights:

Calculation formula of V_C^t

$$V_C^t = \sum_{i=1}^{5} \sum_{j=1}^{c_i^t} w_i p_j x_j^t$$

$$p_j = trx_j / \left(d_1 + \frac{ca_j}{1 + e^{d_2 - ca_j}} \right)$$

C = content

w_i = weights of operations such as hit (1), like (2), comment (3), tipping (4), and forward (5)

p_j = user's energy value during the jth operation. User's energy value will constantly decrease when the user frequently operates specific interactions over a certain period; the value will slowly increase when the user stops the operation, thus limiting the click farming.

x_j^t = user's credit score during the jth operation. The score is calculated dynamically on the basis of the status of the user's credit among the community as a whole. User's credit score will be downgraded if he or she is repeatedly reported against or receives complaints.

trx_j = user's available TRX balance during the Jth operation. User's current available TRX balance is obtained by his or her current TRX balance deducting the amount locked by the system. The larger the available TRX balance is, the higher the value score of the user's interactive operation will be. The purpose is to prevent malicious users from registering multiple blank accounts for click farming.

d_1 d_2 = Threshold value of operation

ca_j = the total number of user's various operations during the jth operation

c_i^t = at the moment of t, times of the ith operation

For creators of live-show-like instant contents, the block chain technology can also display the anchor's popularity in a transparent and fair manner and obtain real-time and rapid income through intelligent contract. The technology can avoid problems triggered by the centralized platforms, such as the black box operation, account delay and block for no reason. The problems damage the interests of the anchor and the audience.

Example of anchor's sharecropping of the intelligent contract in the live platform:

```
pragma solidity ^0.4.11;


contract 波场（TRON）AnchorPay {

address platform;     // 平台地址
```

```
function 波场（TRON）AnchorPay() {
        platform = msg.sender;
}

function deposit(address anchor) public payable{
        uint for_anchor = msg.value * 9 / 10;              // 主播拿 90%
        uint for_platform = msg.value - for_anchor;
        anchor.transfer(for_anchor);
        platform.transfer(for_platform);
}

function withdraw() public{
        assert(msg.sender == platform);
        msg.sender.transfer(this.balance);
}

function() payable{}
```

}

With TRON's structure of bottom block chain, TRON can issue their own tokens freely, and thus is equipped with native economic system. Through TRON's official token - TRX, users can easily achieve value distribution, payment and settlement of contents. The system can also motivate users to produce contents with strong power of spread that have clearer copyrights and high quality, which enables the content output system fine self-operation.

3. Great Voyage, Personal ICO

Based on the advantage of block chain, TRON solves three major issues: income measurement, dividend payment and management of supporters, and achieves significant transformation from the "fan economy" to the "fan finance". The autonomous economic system which is on the basis of the block chain and takes TRX as the official token enables that every income and expenditure of the individual content producers in the system are open and transparent and cannot be tampered with. Through intelligent contract, supporters can automatically participate in the purchase of content producers' digital assets, and automatically share dividend growth in accordance with the agreement. All the process can be fairly completed without supervision from any third party.

Example of personal securitization (ICO) financing of content creators:

Tom, a popular anchor of short videos in the TRON system, based on his judgment of his own values, has issued Tom Token, his personal official tokens, and has raised a large amount of TRX. In return, supporters can get a series of privileges for Tom's contents, including free watch of contents requiring premiums, and participation in video making for the top ten owners of TOM Token. In addition, supporters will also obtain the right to use Tom's subsequent income. If in the future, Tom's fame and income substantially increase, then Tom Token's intelligent contract will be used more frequently, its value will rise exponentially, and supporters will gain Tom's growing revenue.

Tom Token can limit the effectiveness period of earnings, such as a week, a month, a year, three years, or indefinite level. Tom Token with different time limits can be issued. The higher the level and the longer the time limit are, the higher the proportion will be.

For example, Tom has 10 thousand fans, and daily average tipping of 1 million TRX, and Tom sells usage right of 20% of his income within three years. Supporter Kevin has spent 300 million TRX for the purchase of the fully issued Tom Token, at a 36.9% static premium. After the purchase, Tom and Kevin signed an intelligent contract, stipulating that Kevin can automatically obtain income that is calculated proportionally from the tipping given by Tom's fan A.

In order to prevent decreasing quality of Tom's creation after the financing, the system will regulate conditions for changing Tom Token into cash. Conditions include the lifting of the ban on a weekly basis, and setting-up of particular indexes to measure the creation quality. The lifting of the ban is not allowed until standards are met, or Kevin, the investor can cancel the contract.

Obviously, the more unfavorable conditions are more conducive for Tom to obtain high valuations. On the other hand, to achieve higher returns, Tom is motivated to improve the quantity and quality of creations, and increase his influence.

4. Apollo, Free Movement of Value—De-centralized Token Trading Exclusively for Individuals

To reach the goal that each content producer in the TRON system can issue their own tokens, the system must have a complete solution for de-centralized tradings,thus realizing the free flow of values.

The platform will face the following challenges:

1. As time passes, the number of tokens issued on the platform is staggering, making it difficult for traders to screen, so they may be easily confused or

even cheated.

2. Despite the very small amount paid by individual supporters, the total number of supporters is huge, who have high requirements for the safety of the platform funds. Especially, the system shall prevent phenomena like hacker attacks and absconding with funds in the trading platform.

3. As the logic of distribution of interests varies from tokens, the platform needs to promptly complete reminders and have quick deliveries.

4. The transaction history needs to be open and transparent, so that participants can understand the whole process of history and have sufficient information, thus reducing transaction risks.

The current centralized exchange cannot respond to the challenges, especially dealing with the rapid-screening trading regarding mass-type tokens and risk management of platform funds, and therefore, de-centralized trading platforms are needed to complete deals. Not all funds are handled by the centralized trading platforms, but instead, they are always stored in traders' accounts, perfectly solving problems like funds being stolen or money being absconded; on the other hand, through the peer-to-peer content-addressable protocol that is de-centralized and distributed, traders can easily and accurately find investment subjects in the mass and exclusive tokens without confusion.

Through the establishment of the de-centralized trading platform, the value, property rights and risks of the system can be freely traded and exchanged, thus increasing the economic vitality of the whole system in geometric multiples.

5. Star Trek, Traffic Monetizing—Gaming of De-centralization and Market Forecast

The size of the global gaming market in 2014 exceeded $450 billion. Traffic brought by the TRON content platform makes it possible to build an online gaming platform

for de-centralization. Developers can freely build online gaming platforms through TRON, providing fully autonomous gamings and predicting market functions.

6. Eternity, Traffic Conversion—De-centralized Game

In 2016, the global video game market amounted to $ 9.66 billion, of which the scale of the phone game market was $ 4.61 billion, accounting for 42%. TRON provides the possibility for establishing an on-line game platform. Developers can freely set up game platforms through TRON, achieve crowd-funding for game development, and make it possible for common investors to invest in games.

7. Technical System of TRON

1. File Storage Protocol

The bottom layer of TRON consists of a group of multi-layer protocol stacks with various implementation models for each layer and is integrated in the form of module. Corresponding interface standards are defined between layers, including the following five levels:

- name layer: a self-certified PKI namespace
- MerkleDAG layer: data structure format
- Exchange layer: block transmission and copy
- Routing layer: locating peer nodes and objects
- Network layer: establishing connection among peer nodes
- Node and identification

1) “TRON node” is the program that can locate, release and copy MerleDAG. TRON network adopts node identification based on PKI (Public Key Infrastructure); the node is shown as NodeId, which is

the Ciphertext Hash of Public Key. Node will store its public and private keys (private key will be protected by password). Users can freely establish and instantiate a “new” node in every boot, which will deprive the network profit achieved from former node running. The system has incentive mechanism to make users maintain the same node.

```
type NodeId Multihash

type Multihash []byte

// self-describing cryptographic hash digest

type PublicKey []byte

type PrivateKey []byte

// self-describing keys

Type Node struct {

    NodeId NodeID

    PubKey PublicKey

    PriKey PrivateKey

}
```

The generation mechanism of NodeId is as follows:

```
difficulty = <integer parameter>

n = Node{}
```

```
do {

    n.PubKey, n.PrivKey = PKI.genKeyPair()
    n.NodeId = hash(n.PubKey)
    p = count_preceding_zero_bits(hash(n.NodeId))
} while (p < difficulty)
```

When the connection is established, the nodes will exchange public keys among each other, check if the hash of node public key is equal to the NodeId hash(other.PublicKey) equals other.NodeId of peer node, if not, the connection will be terminated.

2) Multihash and updatable hash

All hashes in TRON will be encoded with multihash, which is a self-describing hash format. The actually used hash function should be in accordance with specific security requirements. The encryption system is updatable, which means the system can switch to stronger hash algorithm when current hash function cannot meet more strict security requirements. But there is indeed a price to be paid, the object needs to be rehashed and the connection needs to be rebuilt. This way of without defining the length of hash digest in advance allows the tool used today can work normally even if is switched to longer hash function tomorrow.

The hash digest value is stored in multihash format, including a short header, specified hash function and byte length of digest, for instance:

<function code><digest length><digest bytes>

The current TRON node must support the following hash algorithm: sha2-256, sha2-512 and sha3.

3) Network layer

Provide point-to-point reliable and unreliable transmission between two

TRON nodes, and process:

- NAT traversal—punching, port mapping and relaying
- Support various transport protocols—TCP, SCTP, UTP…
- Support encryption and digital signature
- Multiplexing—multiplex connection, stream and protocol…

4) Routing layer: locating peer nodes and data

Routing layer serves for two purposes:

- Node-routing—searching for other nodes
- Content routing—searching for data released to TRON.

Routing layer defines an interface, and all implementations meet or realize the interface can be linked to TRON, for instance: DHTs, mdns, snr, dns. The corresponding interface definition is as follows:

```
    FindPeer(node NodeId)
    // gets a particular peer's network address

    SetValue(key []bytes, value []bytes)
    // stores a small metadata value in DHT

    GetValue(key []bytes)
    // retrieves small metadata value from DHT

    ProvideValue(key Multihash)
    // announces this node can serve a large value

    FindValuePeers(key Multihash, min int)
    // gets a number of peers serving a large value
}
```

5) Block swap: transmitting content-addressable data

TRON block swap layer is responsible for the coordination of data transmission. Once the nodes are aware of each other and establish connection, content-addressable blocks can be transmitted through swap

agreement. Block swap layer is the interface definition, and all implementations meet or realize the interface can achieve seamless access, for instance:

- Bitswap: current implementation, which is the generalization implementation of BitTorrent, supports the swap of any DAG;

- HTTP: simple HTTP implementations can be used between HTTP clients and servers.

BitSwap is a block transmission agreement similar to BitTorrent—where nodes represent the expected block set with want_list, and represent the data block set they can provide with have_list. Unlike BitTorrent, block swapped by BitSwap is not limited to a single torrent. BitSwap serves as a persistent market, nodes exchange blocks through BitSwap market, the node can obtain their favored block sets, and these blocks sets may be completely unrelated files from the file system. Sometimes in exchange, a node may have no blocks needed by other nodes, it will help to find with higher priority than to find block it needs, these are all to get the needed block from each other, and such incentives can help the cache and distribution of rare block.

BitSwap credit

The agreement must urge the nodes to be the seed because the might have blocks not needed by itself but needed by other nodes. Therefore, BitSwap nodes will actively deliver blocks to other peer nodes, and the agreement indeed has to take measures to prevent the existence of greedy nodes that load little and never share their blocks. A simple system similar to credits can solve these problems.

(1) Nodes track its number of bytes exchanged with other nodes.

(2) Nodes transmit blocks to indebted nodes in form of probability, the higher the debt of indebted node is, the lower probability of block

transmission will be.

It should be noticed that if the node decides not to transmit block to opposite end, then it cannot transmit block to the ignored correspondent node within the following ignore_cooldown time. The purpose is to prevent the submitter from escaping from sending bloks repeatedly.

BitSwap strategy

The strategy adopted by the node to send block directly influences the performance of block swapping. It should meet the following objectives:

(1) Maximize the node and the overall transaction performance;

(2) Prevent the greedy nodes from taking advantage of or reducing the swapping performance;

(3) Efficient and exclusive to other strategies;

(4) Be friendly to the credit node.

A practical strategy selection is Sigmoid function, the defined debt ratio *r* is:

$$r = \frac{\texttt{bytes\_sent}}{\texttt{bytes\_recv} + 1}$$

At a given *r*, the probability of sending to indebted node will be calculated as:

$$P\Big(\ send \mid r\ \Big) = 1 - \frac{1}{1 + exp(6 - 3r)}$$

The sending probability drops dramatically with the rising of debt ratio.

Debt ratio is the measurement of credit, which is friendly to previous nodes that have swapped many blocks and unfriendly to unknown or untrusted nodes.

BitSwap accounts

BitSwap node will keep accounts of the block swap, which helps node track history and avoid be cheated. When connection is established, the BitSwap nodes will exchange account information, if the information is not in exact match, the accounts will be deleted and reinitialized, and all profits and debts will be lost. This method seems to have a loophole for malicious nodes to delete debts by the way of intentionally "losing" accounts, but it is impossible because node cannot accumulate enough debts, besides, it will lose all the previously accumulated debts and other nodes will consider it as abnormal behavior and refuse to swap.

```
type Ledger struct {
  owner      NodeId
  partner    NodeId
  bytes_sent int
  bytes_recv int
  timestamp  Timestamp
}
```

The history of account information will not influence the normal operation and only the recent account items are useful. The node can also choose store or not to store historical information.

2. Self-operation of Storage Network

TRON is a centerless storage network, which turns the storage from cloud model to market model based on algorithms and rules. The market is based on blockchain and trade in virtual currency—TRX, namely the miner earns TRX by providing storage for client-side; on the contrary, the client-side expends TRX to hire miner to store and dispatch data. Similar to Bitcoin, miners compete with each other to mine blocks to earn profits, but the mining capacity of TRON is directly proportional to the storage space

offered by miners, which provides a useful service to client-side (unlike Bitcoin, the work of miners is only useful for blockchain consensus) and is a strong incentive to drive miners to contribute as many storage space as possible to rent to client-side. The agreement will integrate these resources into a self-healing storage network for external use, and the network will realize its robustness by copying and dispersing stored contents and automatically detect and repair replication errors. The client-side can choose different replication parameters according to different threat degrees and levels to protect data. The storage network also provides other security guarantees such as end-to-end encryption of contents for client-side while the storage provider cannot obtain the decryption key.

1) Proof-of-Replication (PoRep) algorithm

The server (prover, P) convinces the user (verifier, V) that its data D is replicated and stored in multiple physical storage locations.

Seal operation

Seal operations include: (1) get the public key of verifier's stored data D through asking verifier to prove the pseudorandom and force the data copies to be correctly stored in independent physical storage; (2) force the time required by copying process to be longer than the expected time required by responding to a Challenge.

PoRep algorithm flow

Create a copy: create a copy in Setup algorithm through the Seal operation and provide the proof of successful execution.

Setup
- INPUTS:
  - prover key pair $(\mathsf{pk}_{\mathcal{P}}, \mathsf{sk}_{\mathcal{P}})$
  - prover SEAL key $\mathsf{pk}_{\mathsf{SEAL}}$
  - data $\mathcal{D}$
- OUTPUTS: replica $\mathcal{R}$, Merkle root rt of $\mathcal{R}$, proof π_{SEAL}

Storage verification: The Prove algorithm produces storage verification for the replica. The prover receives a random challenge c and determines one leaf Rc of Merkle Tree R (root is rt), the prover produces the proof of Rc and the Merkle path to rt.

Prove
- INPUTS:
  - prover *Proof-of-Storage* key $\mathsf{pk}_{\mathsf{POS}}$
  - replica $\mathcal{R}$
  - random challenge c
- OUTPUTS: a proof π_{POS}

Verification proof: Verify algorithm checks the validity of the storage verification based on the data copy of the Markel tree root and the hash of the original data. The verification is publicly verifiable: any distributed system node interested in this data can check the validity of the storage verification.

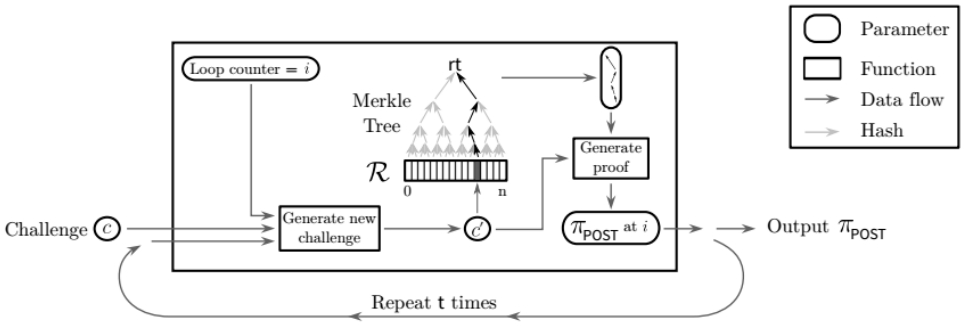
Verify
- INPUTS:
  - prover public key, $\mathsf{pk}_{\mathcal{P}}$
  - verifier SEAL and POS keys $\mathsf{vk}_{\mathsf{SEAL}}$, $\mathsf{vk}_{\mathsf{POS}}$
  - hash of data $\mathcal{D}$, $h_{\mathcal{D}}$
  - Merkle root of replica $\mathcal{R}$, rt
  - random challenge, c
  - tuple of proofs, $(\pi_{\mathsf{SEAL}}, \pi_{\mathsf{POS}})$
- OUTPUTS: bit b, equals 1 if proofs are valid

1) PoSt algorithm flow

The Setup of PoSt is similar to Verify algorithm and PoRep. The Prove algorithm produces Proof-of-Spacetime for data copy.

Prove
- INPUTS:
  - prover PoSt key $\mathsf{pk}_{\mathsf{POST}}$
  - replica $\mathcal{R}$
  - random challenge c
  - time parameter t
- OUTPUTS: a proof π_{POST}

The prover receives random challenge from verifier and orderly generates Proofs-of-Replication, then uses one proof output as the next output until t times of loop iteration, as is shown in the following picture:



PoSt. Prove mechanism displays an iterative proof that is effectively stored for a period of time.

3. Network Implementation of TRON Contents

Through the use of many existing mature technologies, wave field (TRON), as a new content platform, provides security, scalability and privacy, and at the same time by taking incentive mechanism to allow the participants to actively contribute the processing capacity of their machine to build user registration network, give positive contributors the privilege to send advertisements to the whole network to achieve the purpose of incentive, of course this group text messaging will be limited in number.

1) The user registers P2P network

Centerless but secure user registration is implemented through the blockchain mechanism, and the same mechanism has been applied in Bitcoin without the need for central authorization to avoid double payment difficulties. The blockchain ensures no duplicate registered, and the newly registered users must obtain the confirmation of multiple blocks before taking effect, i.e. notarization. Each block is defined as:

$$Block_i = [i, H(Block_{i-1}), Nonce_i, SpamMsg_i, [UserReg_j, UserReg_{j+1}, ...]]$$

H ($Block_i$) provides proof-of-Work to prove that the user gets satisfying Nonce value in $Nonce_i$ space through violent solving; meanwhile occasional hash collision is avoided through verification. The Difficulty of solving is determined by the Difficulty value, and the number of blocks generated per hour is automatically set by the system, which is similar to Bitcoin network.

$$UserReg_j = [Username_j, PUBK_j, Nonce_j]$$

New user j must broadcast $UserReg_j$ when registering online, after receiving the broadcast message, other nodes must prove the proof-of-Work of H ($UserReg_j$), and this will prevent denial of service attacks by false registration. This workload is much smaller than the workload of the blockchain, and a typical few minutes of computation can solve the problem.

The blockchain provides a mapping from the user name $Username_j$ to the user public key $PUBK_j$, a dictionary that can be publicly queried.

The node must verify the uniqueness of $Username_j$ before adding $Username_j$ to the new block, but there is an exception, if the newly registered key is signed by the previously known public and private keys, then it is allowed to be replaced. In addition, the ID_j uniqueness and the proof-of-Work of $UserReg_j$ should be also proved when receiving the new block.

$Username_j$ also has the maximum size and the allowable character limit to protect the ID space from the hash attacks.

$SpamMsg_j$ is a broadcast message (called "Promoted" message) that sends the Promoted message as a reward to those nodes that actively participate in the block generation.

2) Routable DHT overlay network

The second network is a P2P overlay network similar to Kademlia, which is mainly used for resource storage and content search, and also for direct

delivery of notifications between users.

Using the user's ID as the network node ID seems like a good choice, but this leads to the exposure of user identity and location, breaking the privacy of the system. Therefore, by hashing the IP address and port number of the node to identify the node and taking it as the name of the node in the DHT network can also avoid the sybil attack:

$$ID_{node\_j} = H([IP_j, port])$$

The package delivered from ID_{src} to ID_{dst} in DHT network is defined as follows:

$$Packet = [ID_{dst}, ID_{src}, SIG_j(payload), ID_j)]$$

The payload is signed through user ID_j, the ID_j may be different from other users of ID_{src} during package retransmission/refresh.

These functions constitute the third layer function of the concept model of DHT overlay network, and then the above layer is "application layer", which provides the data storage primitive PUT and GET, PUT is defined as follows:

$$payload_{PUT} = [target, value, time, seq] \text{ where}$$
$$target = [owner, resource, restype] \text{ and } ID_{dst} = H(target)$$

Before accepting the storage request, the destination node needs to do the following rule checking:

- ID_{dst} = H（target）：ensure the correct calculation of the destination address;
- ID_{dst} is the neighbor of ID_{node} that actually receives the request;

- ID_j = H（owner）: verify when restype is “single”;

- seq is larger than stored old value seq_{old}, which is also verified when restype is "single".

- time is a valid time (i.e. not a future time value).

restype defines resource types. There are two possible values, "single" and "multi", and single represents resources that can only be updated by key owners; multi represents responses from different users (such as all replies to a post). For a single type, the node stores only a single value, and for the multi type, the new PUT request appends the value to the list. Both types of storage can set expiration time, and the corresponding storage will be deleted from the system after the setting time, so that the expired data will be automatically cleared.Primitive data retrieval GET can also operate on two types of storage resources, other nonstorage resources related to the dynamic content also can achieve similar access operations, so as to share the same API interface.

3) User contents

The k-th message of user j is defined as:

$$UserPost_{jk} = SIG_j([Username_j, k, type, MSG_k, REPLY_k])$$

MSG_k is content, k is a monotone increasing number, possible values of type include: the new posts, replies, retransmission (RT), direct messages (DM), $REPLY_k$ is an optional domain, which provides reference of the original message in response /retransmission and is defined as:

$$REPLY_k = [Username_{j'}, k']$$

representing the original message is the k'-th message of the user j'.

The contents are simultaneously shared in two overlay networks: (1) stored in

DHT as a short-term storage value; (2) archived like files in BitTorrent network. When the new content is created, the client-side must send a PUT request to the following addresses:

$$ID_{UserPost\_jk} = H\left([Username_j, \text{“post”} + k, \text{“single”}]\right) \text{ and}$$
$$ID_{swarm\_j} = H\left([Username_j, \text{“swarm”}, \text{“single”}]\right).$$

$ID_{UserPost\_jk}$ is the address of the destination storage node in the second DHT network, providing the retrieval capability of any content.

ID_{swarm_j} is the gateway address of torrent swarm group related to the content of the user Usernamej in the third network, and this torrent contains all the contents of a given user j, which provides quick distribution and sharing of content based BitTorrent protocol and is independent of the second DHT network. The neighbor node of ID_{swarm_j} needs to join the swarm cluster of user j to help the storage and distribution of content, provide data reliability and better data distribution performance; similarly, the neighbor node of $ID_{UserPost\_jk}$ also needs to store the same values stored by $ID_{UserPost\_jk}$.

The swarm group mechanism solves the problem of fast and efficient notifications and distribution of new content, so that the user's followers don't have to always poll the DHT network address to determine whether new content is generated.

Direct message (DM)

Users posting content can also be delivered by direct message, but only if the message receiver is a follower of user k.

$$UserPost(j \rightarrow l)_k = SIG_j\left([\text{“”}, k, \text{“dm”}, [PUBK_l(DM_k), H(DM_k)]]\right)$$

Except the difference of content (now is $[PUBK_l(DM_k), H(DM_k)]$) , there is no different from regular posts. DM will only be received by user l who has successful decrypted, although other followers can also receive the message,

they cannot decrypt the message, nor they perceive who is the final receiver. Encryption is based on ECIS elliptic curve encryption algorithm.

User content torrent/tracker rule

- In hashing space, the online neighbor nodes within a certain distance from ID_{swarm_j} need to join the corresponding Swarm;

- When ID_{swarm_j}'s neighbor receives new content from the DHT network, it must work as a gateway for BitTorrent network to incorporate content into a file-like archive structure;

- BitTorrent tracker is read-only multi-value list storage. Its hash address is calculated as follows:

$$ID_{tracker\_j} = H\left([Username_j, \text{“tracker”}, \text{“multi”}]\right)$$

- The follower of user j should join in the corresponding swarm to receive real-time update of content, so as to obtain the address of the initial Peer through the primitive GET query of $ID_{tracker\_j}$;

- $ID_{tracker\_j}$ is different from other storage values because it is read-only, which prevents the tracker attack and contains the privacy of the swarm members. The list of IP addresses is obtained through the swarm protocol, which requires the online neighbor node of $ID_{tracker\_j}$ to join the swarm.

- Swarm members can only know each other through IP address, and BitTorrent does not provide any information about the user name.

- There is no need for the hash of all user contents, because the contents (including DM) have been signed to verify the integrity of the content;

- The added value k when generating new content is broadcasted directly through flooding in the Swarm;

- Members of the Swarm will exchange the content list owned by them, where members can choose to save or request only the most recent content;

- The seed node is the node selected to archive the content;

- Content publishers (user j) can choose not to be member of the swarm group (to protect privacy and hide IP address);

- If the publisher chooses to be a swarm member, it does not have to follow the ID_{swarm_j} gateway mechanism, which will of course expose its own IP address;

- Even if the publisher becomes a swarm member, it may not have to act as a seed node;

- The new block generation rate will affect the user's posting speed, and if a new block is generated every 10 minutes, on average, 288 contents can be released daily.

4) User mention mechanism

If the new content refers to user j, the client-side also has to send a notification to ID_j, including the entire message content, to be routed through the DHT network.

The mention mechanism is the only function in the system that needs to be addressed by user ID_j instead of ID_{nodej}, which may expose users' privacy information. An alternative implementation mechanism is as follows:

$$ID_{mention\_j} = H([Username|_j, \text{“mention”}])$$

The user name is hidden by means of hash and a new address for receiving and accumulating all mention is calculated, $ID_{mention\_j}$ neighbor nodes will also participate in the storage of mention, providing maximum reliability

and storage performance. A bad thing about this approach is that the user needs to poll this address periodically to determine if any new mention is received.

The mention mechanism requires the collaboration of the client-side, and if it does not send notification messages to the network, the user will not perceive that he has been mentioned.

5) Explicit message request

User l can request a specific explicit message from user j without joining Swarm group through directly retrieving the corresponding contents from $ID_{UserPost\_jk}$ address of the second DHT network, it supports functions of "message upstream".

6) Message downstream

A downstream trace of the message (such as a reply/RT query for a specific content query) is relatively difficult to resolve, and a possible solution is to send a notification to a storage address of a multi-valued list

$$ID_{replies\_jk} = H\left([Username_j, \text{“replies”} + k, \text{“multi”}]\right)$$

The stored value is the copy of all responses, which also requires the client sides to work together.

7) Hash tag

Like the mention mechanism, the hash tag detects in the context of the new message, and the copy of the message is sent to a specific multi-value list storage address:

$$ID_{hashtag_t} = H\left([hashtag_t, \text{“hashtag”}, \text{“multi”}]\right)$$

This is similar to message downstream mechanism, the difference is: the hash tag creates a new Swarm group; $ID_{hashtagt}$ neighbors must also join this virtual Swarm. It is called virtual because Swarm group do not share any file content and is only used to realize the broadcast function for users who want to monitor the hash tag.

8) Content search

A search for any content that appears can be realized by extending the implementation of the hash tag to build a similar mechanism for the content that appears. In order to reduce overhead and network transmission, corresponding restrictions must be attached, such as restricting content size and excluding prepositions. In addition, it can significantly reduce the storage overhead and the system implementation complexity if the unified storage of content containing the same content is stored in a temporary multi-valued list address. The address calculation is as follows:

$$ID_{word_w} = H([word_w, \text{“word”}, \text{“multi”}])$$

TRON content provides the following security, extensibility and privacy features:

- The architecture itself provides elastic extensions, and no single company, government or organization can close it;
- The distributed user registration mechanism is as secure as Bitcoin transactions, providing non-centralized content authentication;
- To select the favorite user name, users are more eager to register early.
- The common user naming method and discarding the long encryption hash allow users to have a better use experience.
- Public key substitution mechanism allows users to change their key pair when security is threatened;

- The main functions of other blogging systems are included, such as user name search, message tracing, mention, encrypted message, hash tag and content search.

- The ability to send notifications to and request resources from specific user via DHT routing, whether the user is online or not;

- The architecture provides incentives for participating nodes to have the privilege of sending broadcast messages;

- Users' public content and hashtags can be accessed through read-only web interface, which does not break the security of the system;

- Resource-constrained client sides can be optimized, for example, by not storing all blockchains but only the hash values of the blocks. In order to search for a particular user, they can inquire network which block contains the user's registration, and the client-side only have to download the desired block without reducing security and verify data integrity through some branches of the Merkle Tree.

8. TRX—Offical Token of TRON

TRON's official currency is TRONIX. TRON will own the following categories of assets extended from TRONIX:

(1) TRONIX

TRONIX is the basic unit of accounts in TRON's blockchain. The value of all other tokens are derived from the value of TRON. Those who wish to enter or quit TRON must buy or sell TRONIX. TRONIX's total amount of distribution is 100 billion.

(2) TRON Power (TP)

TP is locked TRON. Users can acquire TP by locking their TRONIX. TP, in

nature, is TRONIX with voting right, which means TP holders have more privileges in the ecosystem.

In the world of cryptocurrency, we see speculators constantly seek for fast-appreciating currencies for investment. TRON tries to build an ecology under the full control of TRON holders who is optimistic about TRON on a long-term basis, and we hope TRON could be controlled by those whose values are consistent with TRON's for long.

We'll give TP holders on a long-term basis more TPs as a reward, and the reward will be dynamically allocated. This means those who hold and lock TP for long will be rewarded.

TRON POWER's balance cannot be transferred nor sold, which means TRON POWER is not tradable.

Long-term investment in the direction in which you believe is critical, thus the ecosystem is able to make longer-term plan and will not give up the pursuit of its ideal for short-term interests. Meanwhile, stakeholders enjoy the vigor because of its sustainable growth. Long-term holding of stakeholders can be the benchmark in the ecosystem and better lead the development of the ecology.

(3) TRON 20 TOKEN

Content owner ICO: Content owners (IPs, individuals, and groups) can issue their digital assets freely through TRON 20 standards, while others can enjoy the benefits and services brought by the constant growth of data contributor by buying these digital assets.

Token is a way of defining value in blockchain and is used to benchmark financial or digital assets. On TRON, we suggest all tokens use the same standards TRON 20, which will make it easier for the exchange of tokens and DAPP support.

In TRON's blockchain, one may issue derivatives of content owner ICO through the code provided by the community.

On the basis of TRON's blockchain, the community also will support development of DAPP to some extent, such decentralized exchange, market forecast, random digital sources and other ecological projects.

9. Voting and Community Governance

Blockhead voting mechanism is critical to the system's self-upgrading. When the protocol layer changes, the ecosystem will decide to follow the longest chain. Existing voting mechanism is inefficient and sometimes even fails to make the most vote, leading to the stagnant decision-making of the community.

TRON is the first to propose mixed voting mechanism and set a two-tier voting system,

1. Poll

2. Follow vote

TRON's nodes communicate with each other, but they can confirm the transaction at different times. Blockchain requires the uniformity of sequences, which means every transaction's time sequence must be uniform. To ensure the uniformity of every round of broadcast, TRON's voting system needs to take three steps:

1. Preliminary Preparation

When a user sends an application for transaction, host node will send a message to all verification nodes and wait for a reply.

2. Preparation

A verification node will check this message. If the consensus is reached with two third of affirmative votes or more, the host node will broadcast that the transaction

enters the next stage.

The verification node will have three response options

1) The node approves the transaction

2) The node rejects the transaction

3) The node doesn't reply within the required time

4) Nodes which give no response for many times will be gotten rid of

3. Confirmation

A verification node officially promises to all verifications that information is correct. Then, if a consensus is reached with two third of affirmative votes or more, the transaction will be completed and blockchain will link with cochain and broadcast it to all nodes in the network.

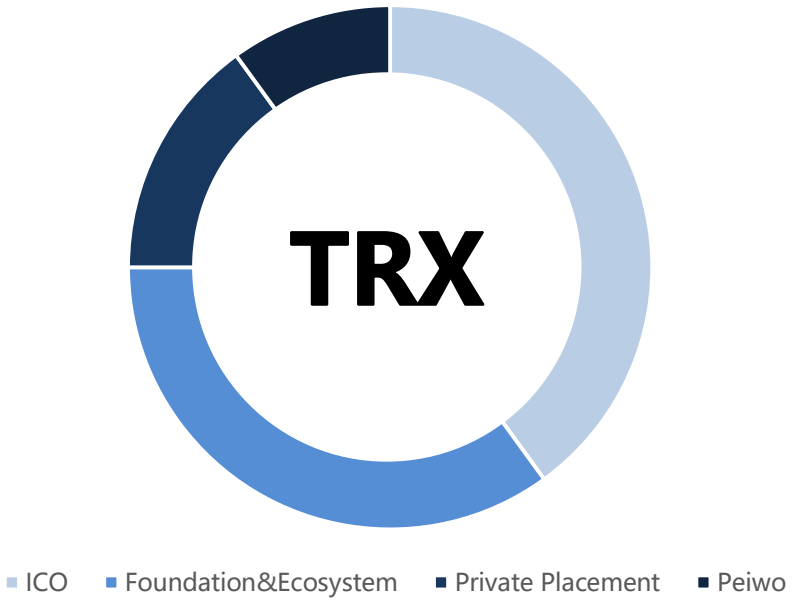
10.TRON ICO PLAN

1. Time: September 9, 2017, Beijing Time

2. Allocation:

Total amount of TRX is 100 billion and will be allocated by the following rules:

- Public offering: 40%
- TRON Foundation and the ecosystem: 35%
- Private offering: 15%
- Pay initial supporter-Peiwo Huanle (Beijing) Technology Co., Ltd.: 10%



11.TRON Schedule

1. Exodus, free data - point-to-point distributive content updating, storing and distribution mechanism, August 2017 to December 2018

2. Odyssey, content empowerment - economic incentive-empowered ecosystem, January 2019 to June 2020

3. Great Voyage, personal ICO, July 2020 to July 2021

4. Apollo, free flow of value-decentralized individual exclusive token transaction, August 2021 to March 2023

5. Start Trek, cash in the flow - decentralized game and market forecast, April 2023 to September 2025

6. Eternity, transformation of the flow – decentralized game, April 2023 to September 2025

12.Compliance

- Operator

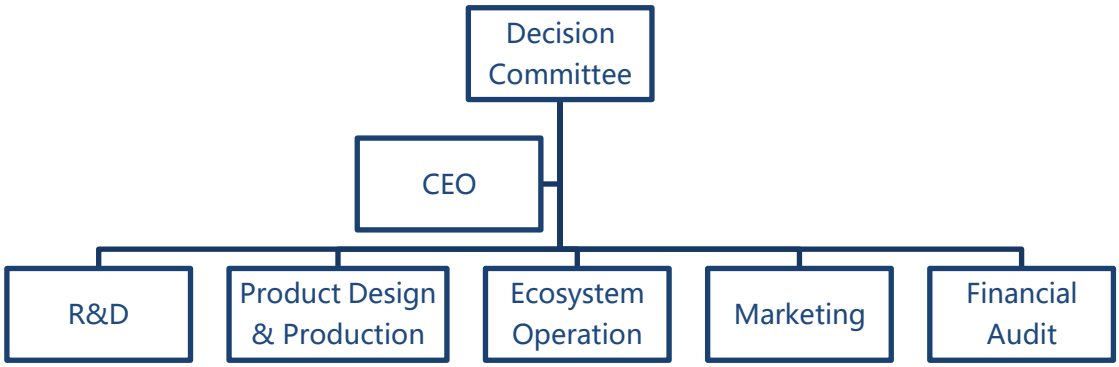
As Sir Tim Berners Lee's a bunch of followers, TRON team firmly believes that it belongs to all humankind since the day the protocol was born, instead of a profitable tool for a fraction of people. Therefore, TRON established Tron Foundation in Singapore, whose primary task is to operate TRON network publicly, fairly, transparently and for no profit, and offer support to TRON's development team.

Tron Foundation was established with the approval of Accounting and Corporate Regulatory Authority (ACRA) and is supervised by Singapore's corporate law. This Foundation is independently managed and run by fiduciary board or management committee and is independent of the government.

Singapore is famous for its stable and sound laws and financial environment. Tron Foundation is a non-profit entity established in Singapore in accordance with Singaporean Laws. This Foundation is a legitimately founded organization without any commercial interests for the purpose of supporting or participating in public interest or private interest activities. The "profit" earned by the Foundation is called surplus and will be kept as outlays for other activities instead of being distributed among its members.

2. Governance structure and voting

To ensure the reasonable use of funds and resources of the Foundation on the premise of openness, justice and transparency, to constantly advance the rapid growth of TRON protocol, to extend the application scenarios of TRON protocol, and to attract more institutions, companies and organizations to enter open-source TRON ecosystem, the Foundation sets up the three-tier organizational structure as follows:



- Decision Commission

  Decision Committee is the supreme decision-making body of TRON Foundation and assumes the final decision. There is no seniority among the Committee members. The Committee is responsible for reviewing and approving the Foundation's major affairs, such as strategic planning, annual plan and budgeting, and vote on major issues in the ecosystem of the TRON protocol on behalf of the Foundation.

- CEO

  CEO is elected by the Decision Committee by voting and is responsible for the Commission. CEO will comprehensively organize to implement the decisions and regulations of the Decision Commission and is responsible for daily operation of TRON, reaching all targets assigned by the Commission, and reporting the implementation to it on a regular basis. Moreover, CEO has the right to establish functional departments when necessary, organize and employ managers. And CEO is responsible for the business of five departments-R&D, product design and production, ecosystem operation, marketing and financial audit, forming a CEO-centered organizational and management system.

- R&D Department

  R&D Department is responsible for the development and audit of underlying technology and is the basic department of the Foundation. To make sure that team members keep information exchanged and act in concert, R&D Department should exchange information with other departments (particularly the department of product design and production) and timely adjust and communicate details of the project, deciding on the research direction for the next stage.

- Department of Product Design and Production

  Department of product design and production is responsible for enriching and perfecting product frameworks provided by technical department, making specific sustainable development strategies, including conducting market research and planning product functions, and TRON's UI design and graphic design and other works. The department staff need to always follow trends, hotspots and feedbacks of the community, proactively communicate with token holders and hold activities like technical seminar from time to time.

- Ecosystem Operation Department

  On the basis of what technical and product departments provide, the Ecosystem Opeartion Department is responsible for "the external and the internal": at first, extend the depth of work, actively develop partners, and link TRON with end users and partners closely, thus building an open, distributive and privacy-protection global entertainment ecosystem; next, build an ecosystem within the user community with benign interaction, free flow of information and utter information symmetry.

- Marketing Department

  Marketing Departmet is responsible for marketing TRON's core and derivative products and services. Its duties include but not limit to

contacting and cooperating with media, advertising, designing user interaction and other tasks. The Department works closely with Ecological Operation Department to formulate the most suitable publicity programme according to the requirements of partners and end users.

- Finance Department

  Finance Department is responsible for financial affairs of the company, including funds management, financial accounting and cost control. Meanwhile, since digital assets feature high risks, this department is also in charge of risk management and control and will cooperate with other departments to analyze and evaluate operational and financial risks of the project. In terms of audit, in view of the particularity of digital assets and tokens, it is hard for existing institution to supervise them in an effective way. So the Decision Committee will engage professional auditors with relevant experience to ensure open and transparent use of TRX.

13. Team Profile

Founder and Chief Executive Officer | Justin Sun

He studied for a bachelor's degree at Peking University and went on to study for a master's degree at University of Pennsylvania, a member of American Ivy League. He is founder of Peiwo APP—China's largest audio content community. In the early days, he joined Ripple where he served as chief representative of Greater China Region of Ripple. He was one of the 2015 Forbes 30 under 30 in China and one of the 2017 Forbes 30 under 30 in Asia. He also won the title of Global Shaper at 2014 Davos Forum (World Economic Forum). He was the only post-90 student of first period of Hupan University founded by Jack Ma. The market value of Ripple has exceeded ten billion US dollars, the number of the Peiwo APP registered users are more than 10 million, and the number of monthly active users has exceeded 1 million.

Chief Operating Officer | Liu Ming

He graduated from School of Philosophy of Peking University with a bachelor's degree. He is a senior practitioner in bitcoin blockchain with more than 5 years of business experience. He has held dozens of professional lectures on bitcoin in well-known institutions like Peking University. As a consultant of many blockchain projects, he who has a good interpersonal network guides the development of the project and has unique in-depth opinions about blockchain. He has written a book called Bitcoin Short-Term Operation Experience.

Technical Supervisor | Yang Kaishan

He graduated from Computer Department of Tsinghua University with a bachelor's degree. With more than 15 years of work experience at front and rear ends, her has worked in UFIDA—a leading provider of enterprise management software, corporate internet services and corporate financial services in the Asia-Pacific region and then in China Roads Information Technology (Beijing) Co., Ltd.—China's provider of leading express highway monitoring system solutions. Yang Kaishan has great attainments in front and rear ends of the system. Since 2013, he has paid close attention to technological development in blockchain.

Senior Rear-End Engineer | Huo Dongdong

He obtained a bachelor's degree in computer and is a senior rear-end engineer. He once served as technical director of rear-end technology of InstNews, one of the largest news information applications in Latin America, and of VnNews, a leading news information application in Southeast Asia. He has rich experience in platform security and high concurrent treatment. Since 2015, he has paid close attention to technology development in blockchain.

Product Supervisor | Deuce Yu

He successively worked on two leading platforms of China's SNS social interaction - Kaixin and RenRen.He served as product manager of Department of Social Interaction and Games, responsible for R&D and promotion of the then very popular social games at the webpage terminal like "vegeteal" and own games at Kaixin's mobile terminal. Then he worked with RenRen, serving as operation principal of games open

platform, responsible for access and combined operation of games from the open platform as well as for R&D and promotion of games at the customized mobile terminal. Ever since 2015, he has paid close attention to blockchain, comprehensively balancing the docking procedure of the TRON protocol entertainment platform with the protocol and their manifestations.

Market Supervisor | Tim Guan

He graduated from Peking University and is a serial entrepreneur. His/her project once obtained investment from Matrix Partners China. He once served as principal of the information strategic system of Global China Group. Since 2016, he has paid close attention to blockchain. He has a unique understanding about markets and brands and is expert in creating high-dissemination brands. He once organized an association of nearly 200 thousand members tied by common values of youngsters.

Operation Supervisor | Zhang Chen

He is a professional practical operator of associations. He once served as co-founder and COO of Elegance Space, secretary-general of Chicago branch of Elegance Space, expert of Zaihang and editorial board member of Association Commerce. He is a founder and operator of an association of 0.1 million high-end women, whose field has covered a dozen aspects like female, training, studying abroad, fund, investment and Internet. He has been invited to give lectures more than one hundred times by Peking University, VBill, Zhongjian Huatong and Internet operating agencies. Since 2016, he has paid close attention to blockchain.

14. Risk

- Systematic risks: They refer to possible changes caused by common factors of overall importance, which will affect the profits of all securities in the same way. Take policy risks for example—at present, the government has not formulated an explicit supervision policy about blockchain projects and ICO financing, so the participators may suffer from losses caused by policies. In the market risks, if the overall value of the digital asset market is

overestimated, the investment risks will be increased. The participators may have an excessive anticipation about growth of ICO projects, but this excessive anticipation may fail to be realized. At the same time, systematic risks also include a series of force majeure factors, which include but are not limited to natural disasters, large-scale breakdowns of computer network globally and political unrests.

- Supervision absence risk: Digital asset transactions including TRX have an extremely high uncertainty. Due to lack of forceful supervision in digital asset transactions, electronic tokens have such risks as sharp rises and falls and being operated by bankers. If an inexperienced individual participator enters the market, he may hardly resist asset impact and mental stress caused by market instability. Though academic experts and official media have given suggestions of prudent participation, there are no written supervision methods and regulations. So at present, these risks cannot be effectively avoided.

- Risks after supervision regulations being formulated: It cannot be denied that in the near future, supervision regulations will be formulated to restrain the fields of blockchain and electronic tokens. If the supervision body performs a standard management over these fields, the electronic tokens purchased during the ICO period may be affected. The impacts include but are not limited to fluctuations and restraints in price and stability.

- Inter-team risks: At present, there are numerous teams and projects in the field of blockchain technology, so the competition is very violent. There are strong pressures about market competition and project operation. Whether the TRON project can stand out of many excellent projects and be widely recognized is not only associated with the capacity and vision planning of its own team but also will be affected by numerous competitors in the market and even oligarchs. There is a likelihood of malicious competition.

- Risks within the team: TRON has gathered a talent team full of vitality and strength and attracted senior practitioners and experienced technical developers in the field of blockchain. As a leading role in the ICO field in

China, stability and cohesion within the team is of vital importance to overall development of TRON. In the future development, there is a likelihood that TRON, as a whole, will be negatively affected by resignations of core personnel or conflicts within the team.

- Risks about project coordination and marketing: The TRON founding team will spare no efforts to realize the development goal proposed in the white paper and expand the growth space of the project. At present, TRON has a relatively mature commercial model analysis. However, due to unpredictable factors occurring in the overall development trend of the industry, the existing commercial models and coordinating thought cannot be well compatible with market demands, thus considerably decreasing the profits. At the same time, this white paper may be revised with the updating of project details. If the ICO participators fail to obtain details after project updating in time or if the public fail to fully understand the project due to information asymmetry, the subsequence development of the project will be affected.

- Risks about project technologies: First of all, this project is constituted based on cryptographic algorithm. The rapid development of cryptology will inevitably bring about risks of being cracked. Second, the development of its core businesses is supported by technologies such as blockchain, distributed ledger, decentration and refusal of falsifying. The TRON team cannot fully guarantee technological fulfillment. Third, loopholes may be found during the process of project upgrading and can be remedied through release of patches. However, the degree of being influenced by loopholes cannot be guaranteed.

- Risks about hacker attacks and crimes: In perspective of safety, the amount of an individual is very small, but the overall number of people is great. This has placed a high requirement upon security assurance of the project. Due to characteristics of anonymity and intraceability, electronic tokens tend to be utilized by criminals or attacked by hackers or may involve criminal behaviors like illegal asset transfer.

- Other risks unknown at present: With continuous development of blockchain

technology and the overall industry, TRON may face some risks that cannot be predicted at present. The participators should fully understand the team background, know about the overall framework and train of thought about the project before making a decision. They should adjust their visions and participate in token crowdfunding reasonably.

15. Disclaimer

- This document serves only for the purpose of conveying information. The contents of this document are for reference only and do not create any suggestions, instigations or invitations of investment about selling stocks or securities in TRON and its relevant companies. These invitations must be made through a confidential memorandum and must conform to corresponding security laws and other laws.

- The contents of this document shall not be interpreted as forced participation in ICO. Any behaviors associated with this white paper shall not be deemed as participation in ICO, including any quests for obtaining the copy of this white paper or sharing this white paper with others.

- Participation in ICO means that the participator has reached the age standard and has full capacity for civil conduct and that the contract signed with TRON is authentic and valid. All participators should sign the contract voluntarily and must have a clear understanding about TRON before signing the contract.

- The TRON team will keep on performing reasonable tests to guarantee authenticity and accuracy of the information in this white paper. During the process of development, the platform may be updated. The updating contents include but are not limited to platform mechanism, electronic tokens and their mechanism and distribution of electronic tokens. Some contents of the document may be adjusted correspondingly in the new white paper with the development of the project. The team will make public the upgraded contents through release of an announcement or the new white paper on the website.

The participators must obtain the latest white paper and adjust their policies in time according to the updated contents. TRON has made a clear statement that it will not assume any losses for the participator caused by (i) the participator relying on the contents of this document, (ii) information inaccuracy in this document or (iii) any behaviors caused by this document.

- The team will spare no efforts to realize the goals mentioned in the document. However, due to existence of force majeure, the team cannot make a full commitment.

- As the official token of TRON, TRX is an important tool for the platform to produce efficiency but it is not an investment commodity. Owning TRX does not mean that its owner has been afforded with the proprietary right, controlling right and policy-making right about the TRON platform. As an encrypted token used in TRON, TRX does not belong to any of the following categories: (a) currents of any types; (b) securities; (c) stock rights of a legal entity; (d) stocks, bonds, bills, warrants, certificates or other instruments affording any rights.

- Whether TRX will appreciate or not is determined by market rules and the demands after application fulfillment. In some cases, TRX may have no value at all. The team will make no commitments about its appreciation and will assume no responsibilities for consequences caused by increase or decrease of its value.

- To the maximum extent allowed by laws, the team shall assume no responsibilities for any damages and risks arising from crowdfunding participation, which include but are not limited to and direct or indirect personal damages, losses of commercial profits, losses of commercial information and any other economic damages.

- The TRON platform will observe supervision regulations in favor of healthy development of the ICO industry and the industry self-discipline statements. Participation means that the participator will completely accept and observe

these inspections. At the same time, the information disclosed by the participator to complete these inspections must be complete and accurate.

- The TRON platform has conveyed possible risks to participators explicitly. Participation in ICO crowdfunding means that the participator has confirmed understanding and recognition of each clause instruction in the detailed rules, accept the potential risks about this platform and will assume consequences by himself.

16. Versions

Date	Version No.	Content
2017/06/03	V1.0	Initial outline
2017/07/08	V1.1	Filling of background contents
2017/07/25	V1.3	Version of global entertainment protocol
2017/08/04	V1.4	Initial version of entertainment system of free contents
2017/08/11	V1.5	Second version of entertainment system of free contents
2017/08/18	V1.6	Initial version of contents

		entertainment protocol
2017/08/22	V1.7	Second version of contents entertainment protocol

17. Contact

Website：tronlab.com

E-mail：service@tronlab.com