TSLA Coin

CONTENTS

I Summary

Since the 21st century, the rapid development of a new generation of blockchain technology and the situation of the great development of the e-commerce industry have presented both opportunities and challenges. As long as we can grasp the direction of society's advancement, there will also be a broad prospect and great achievements!

From the DeFi boom in 2020 to the bitcoin price breaking new highs and rising 17-fold in a year's time to the first signs of NFT in early 2021, blockchain has firmly captured the attention of crypto investors. However, as an innovative technology supported by the state, on the road of blockchain from niche to mainstream, many people have tried to explore more "grounded" application scenarios of blockchain while retaining its financial core and stepping out of the financial perspective to make blockchain vivid, imaginative and interesting.

Based on blockchain technology, TSLA Coin has created a blockchain social platform, a DAPP with blockchain

attributes, and a collection of distribution/non-distribution user system, retaining the network structure of friends' relationship, adding a technically mature e-commerce module in combination with the current trend of private domain traffic, laying a good foundation for the transformation of social platform users. TSLA Coin is a social networking platform with a network of distribution/non-distribution users.

TSLA Coin aims to share social networks to open up a highly profitable and viable social media revenue stream for content and followers. Users will be able to leverage the irreplaceable "power" of the platform.

II Overview of TSLA Coin

2.1 Introduction to TSLA Coin

TSLA Coin is developed based on blockchain technology and focuses on creating a decentralised and peer-to-peer transaction ecology serving the global social industry, creating a community chain serving global applications for video, social, gaming, exchanges and wallets, thus promoting the development of its industry chain.

TSLA Coin is a community-based cryptocurrency with an initial issue of 10,000 trillion, which will never be increased and 5% will be destroyed periodically. The goal is to make TSLA Coin a cryptocurrency that can be used by everyone and traded by everyone, so that it can be circulated globally.

TSLA Coin is based on BSC 2.0 and can be mined on mobile phones. You can earn one TSLA Coin for signing in, watching videos and uploading videos every day, plus an additional one for liking a video you upload and two for being retweeted. The video platform is similar to the Tiktok platform, with the subsequent launch of a game section where TSLA Coin can be earned for playing games, and advertisers need to buy TSLA Coin before they can advertise in the game, effectively reducing the cost and increasing the revenue for users!

TSLA Coin opens up a digital ecosystem in the social sphere and supports cryptocurrency transactions with great speed, confidentiality and security.

TSLA Coin fully considers the technical characteristics of IoT and the needs of network ecology construction, and achieves a seamless integration of blockchain underlay and

network ecology in terms of user credit identity management, P2P communication, cryptographic algorithms, consensus algorithms, smart contracts, cross-chain contract mode, decentralisation, and rapid access to new businesses.

TSLA Coin opens up a highly profitable and viable flow of social media content and fans in shared social networks by using smart contracts developed on blockchain for intelligent management of the entire system. TSLA Coin is a universal currency in the virtual world, and moreover a bridge between the virtual world and the real world, by using TSLA Coin, a value pass, real world The digital media sharing platform created by TSLA Coin rewards users for creating, buying and selling digital product content. Empowering creators and fans like never before. With just a few clicks, users can easily access any digital content, including photos, videos and art, and convert that digital content directly from their smartphone or other media device into NFTs. these NFTs use blockchain technology to convert user content into a unique store of value, and users can then share and deliver information across networks and communities worldwide.

2.2 TSLA Coin advantages

1. Reasonable control of users' needs

TSLA Coin provides a reasonable level of control over the needs of its users and offers realistic functionality. In terms of functional design, users can quickly find the products they want through the filtering function. In terms of function application, according to the gender, age and shopping hobbies of enthusiasts, we recommend videos or products of interest to users.

2、Focus on the user's experience

TSLA Coin focuses on user experience. In terms of interface design, the simple page layout can directly poke at the user's psychology and stimulate the user's desire to consume. The rich and perfect consumption mode is one of the keys to attract and retain users. Moreover, personal sharing of product consumption and experience sharing in the community forum can increase the stickiness between users and directly stimulate their psychology to participate in consumption quickly.

3、Transactions are quick and easy

The decentralised TSLA Coin ecosystem is based on blockchain technology development, and it only takes a few seconds to charge coins from the blockchain decentralised wallet to the platform wallet. Other digital currencies when topped up to the platform wallet, the flow within the platform is centralised, which promotes the speed of payment even more. As a result, the TSLA Coin ecosystem works with other platforms to create a new model of decentralisation that provides payment speed and user settlement experience.

4. Open and transparent

TSLA Coin ecosystem is based on blockchain technology and smart contracts, etc., to achieve massive cutting of tenure, traceability of the flow process and management of revenue dividends, etc., which makes TSLA Coin ecosystem asset investment become small and high-end; the process platform of all transactions is contained in the TSLA Coin trading venue built on blockchain technology, and all transaction processes are recorded in the The underlying distributed blockchain ledger avoids black-box operations in the platform's operation process, ensures accurate identification and transmission of rights and values in the

trading session, open and transparent data, and purifies the platform's trading environment.

5、Enhance information privacy protection

TSLA Coin ecosystem absorbs the technology of blockchain, which has the advantages of system security and anti-tampering etc. TSLA Coin ecosystem concludes transactions and automatically generates payment instructions according to the intelligent contract of blockchain. At the same time the block centre to which it belongs records the data of each link one by one and synchronises the updates through the data recorded in the block.

As a result of recording information on users' transactions, exchanges, consumption data and community accounts on the platform, the correspondence between unique mobile phone identification and user tags can be obtained. User data is stored within the block chain, which can be truly anonymous and secure, thus completely protecting users' personal information security and privacy issues.

6、Enhanced information privacy protection

All information about the TSLA Coin funding supply

itself is stored in the blockchain and can be inspected and used by anyone in real time. No individual or organisation can control or manipulate the TSLA Coin protocol, as it is password protected, making the TSLA Coin core believed to be completely neutral, transparent and predictable.

7. Traceability of origin

From production to sale, every product goes through a complex flow. At key points in the process, the platform sets a secret key for that node. The secret key, a string of encrypted addresses, carries the details of the item. People and things alike are tagged by the blockchain secret key, and the platform then sends these keys to all nodes for notarization.

The biggest difference in a traceability system built on blockchain technology is that the information cannot be tampered with. In the traceability chain, neither the enterprises on the chain nor the platform side can make changes to the established information on the chain, enhancing the credibility of traceability information. For enterprises, the traceability chain can not only prevent forgery and traceability, but also chain-based traceability

system will significantly improve the supply chain management level of enterprises, and will enable key nodes in the whole chain to be value-asset-based and asset-digitalized, providing a solid big data foundation for further improving efficiency and reducing supply chain costs.

2.3 TSLA Coin core capabilities

1. Security capability

TSLA Coin will disclose the core random number values used to ensure fairness in all operations on the platform, completely achieving openness and transparency of core data. Compared to the server-side data manipulation in traditional platforms, TSLA Coin transmits data through blockchain decentralized data encryption channels, thus achieving true security and fairness. At the same time, TSLA Coin uses the open and transparent characteristics of the blockchain to export the digital assets in the platform to the blockchain and disclose their integrity and uniqueness to realise the blocking and securing of the digital assets of users.

2. Cryptography-based security

TSLA Coin uses private key security. It only requires the user to enter the Ethernet wallet address, and then it can be used for consumption, transaction and transfer through transfer. The entire transaction process does not require users to provide any private key or password, and no sensitive information of user accounts will remain on your mobile phone or in your browser, not to mention spreading on the network, achieving the best security protection status.

3、Experience smooth capability

TSLA Coin is developed based on blockchain technology, and the platform team gives full play to its rich experience in the field of platform construction, adopting a "deep coupling" approach, processing core data through smart contracts on the blockchain, and seamlessly calling and combining the two, thus achieving the perfect effect of ensuring both fairness and The perfect effect of ensuring both fairness and smooth platform experience.

4. Multiple Token Circulation Capabilities

TSLA Coin uses TSLA Coin as the basic platform circulation currency, and will support other mainstream

Tokens one after another depending on the business development of the platform, TSLA Coin will also establish an access mechanism for new Tokens, and will evaluate the use of its blockchain assets among platform users and fully consider its security before judging Whether or not to enter.

5. Big data analysis basis

The TSLA Coin backend uses data to drive operations, resource allocation, product updates and business development to meet users' needs for products.
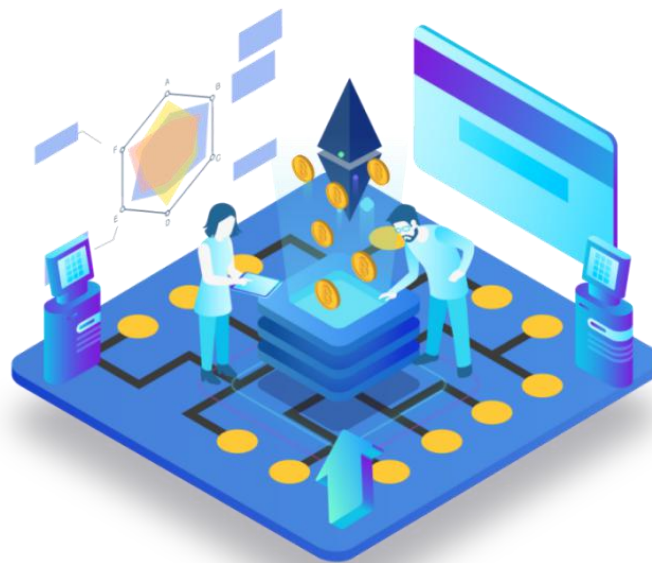
2.4   TSLA   Coin   system framework

1. Access layer

TSLA Coin provides a multi-platform, easy-to-use and beautiful UI interface to meet the needs of users in various scenarios. This includes a PC app, which supports mainstream operating systems such as Windows and MacOS; a mobile app, which supports mainstream operating systems such as iOS and Android; and a web app, which supports mainstream browsers at home and abroad.

2、Front-end UI

The front-end UI consists of interface design, WEB front-end, back-end interface, html code, CSS, JavaScript, etc. It follows the native HTML/CSS/JS writing and organization, which can effectively reduce HTTP requests, reduce DNS lookups, avoid redirects, make Ajax cacheable, delay loading components, reduce the number of DOM elements, slice and dice components into multiple domains, minimising the number of iframes, eliminating http404 errors, etc.

3. Presentation layer

The display layer consists of template engine rendering and Ajax interaction. The template engine rendering can render the APP products and WEB products through the module to show the products in a dazzling way in front of the users

and cooperation. Ajax can adapt to various browser bottoms and server bottoms to a great extent to provide users with smooth and convenient operation requests.

4、System layer

The system layer consists of smart contract, consensus mechanism, stored procedure, consensus mechanism, credit audit, Token exchange, etc. Its function is mainly responsible for database access, which can access database system, data buffer, binary file, text document storage, etc. The business layer is the most direct product presentation of TSLA Coin. Through the development of different products and functions, the practicality, authenticity and legitimacy of TSLA Coin can be effectively improved.

5、Database

The database consists of MS SQL, My SQL, Oracle, etc. The database has basic functions such as storage, interception, security and backup, which are very important in improving the speed of computing and increasing the performance of transportation. User authorization and hierarchical cryptography on top of database usage can fully ensure user privacy and data security.

6、Technology layer

TSLA Coin adopts the latest technology of blockchain, big data and cloud computing. The arithmetic power of cloud computing can drive the blockchain, and the technology of blockchain can make big data traceable and make the data more real and safer; blockchain, big data and cloud computing are mutually influencing and promoting each other.
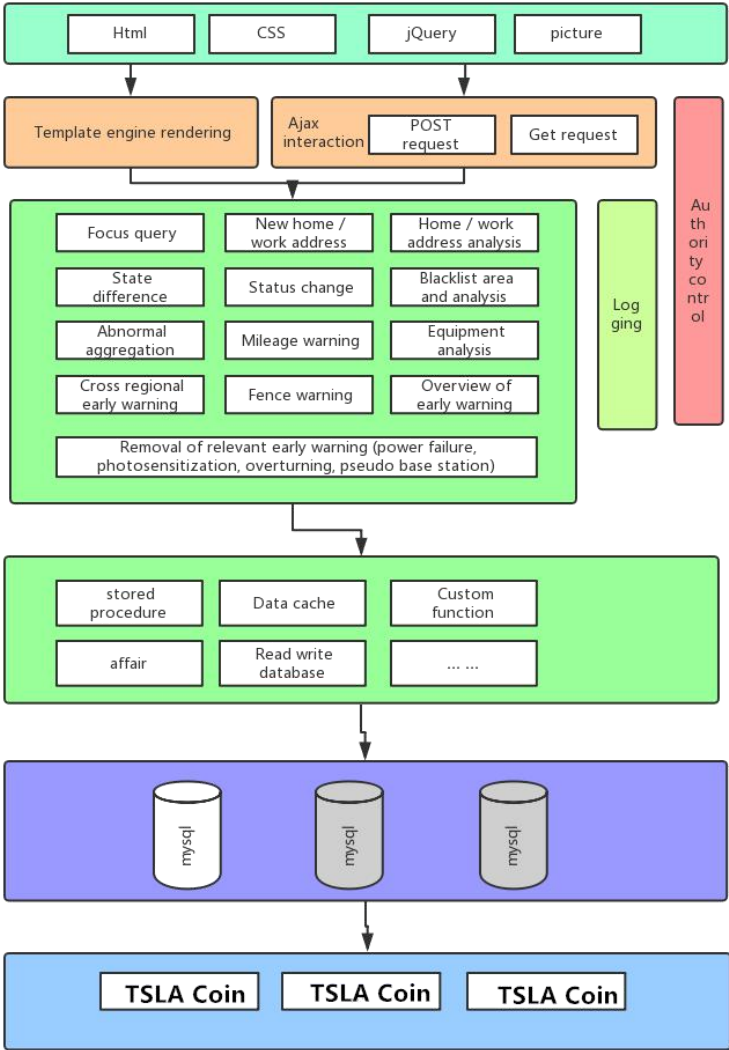
2.5 TSLA Coin features

1、Saving user payment cost

Traditional third-party platforms act as intermediaries between buyers and sellers, holding back money and charging partial service fees for each transaction. TSLA Coin adopts blockchain decentralised technology features, so users can pay with TSLA Coin to improve payment efficiency and save some fees.

2、Multi-currency payment

TSLA Coin system integrates a variety of payment and shopping scenarios of mainstream digital currencies on the market, and can be flexibly configured to support the types of digital currencies according to its own needs, and can realize the function of exchanging digital currencies for coins and digital currencies for digital currencies.

3、Multiple mining modes

TSLA Coin system binds transaction order information, inviting friend information and arithmetic information to the holder, and uses smart contract technology to realize multiple mining modes such as shopping mining, distribution mining and arithmetic mining.

4、Multi-level distribution mode

In order to improve the fit between TSLA Coin platform and users, TSLA Coin Mall has added the contract holder system. Users can invite new users to join the platform through sharing and recommendation, after which they will receive generous reward mechanisms such as shopping rebate value (points) and invitation rewards.

5、Circulability

The TSLA Coin system breaks the traditional centralized operation thinking, allowing points to circulate at the user's fingertips and be consumed in the mall, supporting the withdrawal of coins to the blockchain wallet, giving points value-added attributes, allowing users and the platform to achieve a win-win situation.

6、System security:

TSLA Coin Mall has physical, application dual-level verification, system integration Google verification, token verification, Ukey verification and other multiple verification methods, to protect the safety of user payments.

2.6   TSLA   Coin   technical principles

1. P2P communication

P2P is the core foundation of blockchain, with the characteristics of decentralization, scalability, robustness, privacy and high performance. The block is linked to TSLA Coin's IoT devices and users, and is deeply optimised in terms of session maintenance, address determination, communication mechanisms, storage schemes, and transaction payments. By specifying the physical configuration and size of the user and consensus nodes, and adopting a sharding mechanism and high-speed network connection, the communication, computation and storage burden of the consensus nodes is reduced and the transaction performance of the blockchain is improved, thus achieving the maximum performance of blocking for IoT devices and providing the foundation for the registration, digitization, authentication and security of IoT devices in the future.

2、TSLA Coin encryption algorithm

The encryption and decryption of information is the key link of blockchain, which is mainly the algorithm of hash function and asymmetric encryption.

(1) The hash function part, at present, mainly has a variety of algorithms such as SHA and MD5, and also includes

the use of algorithms in series and in parallel. Since commercial applications generally focus more on performance issues, the TSLA Coin base algorithm is mainly the SHA256 algorithm.

(2) Asymmetric encryption part, there are mainly asymmetric encryption algorithms including RSA, DSA, elliptic curve algorithm, etc. Blockchain generally uses elliptic curve algorithms, including ECDSA and SCHNORR, considering that the verification speed of Schnorr signature is faster than ECDSA signature, and the size of this signature can be smaller, and also natively supports multiple signatures. This is in line with the small size of the Internet of Things, so TSLA Coin has developed its own SDSchnorr algorithm based on Schnorr.

At the same time, TSLA Coin has abstracted the underlying cryptographic algorithm library and interchangeable channels for the algorithms to meet the algorithmic and security needs of different IoT applications. The names of the wallet and the address are interchangeable in the underlying blocks.

3. TSLA Coin Smart Contract

Each Internet-accessible IoT device is given an

"identity" on the blockchain and has a globally unique identifier that can be used to identify a credit identity. Each smart contract has a unique public address, just like a normal wallet. The difference is that the smart contract's private key is discarded when the contract is created, so no one can send the digital assets inside the smart contract after it is created, except for the consensus mechanism. For the IoT's monitoring event-based up-chaining needs, i.e. the IoT device holder sets the smart contract, data storage path and data accounting amount in advance, it can be broadcasted across the network as well as stored in digital records. In the event of a relevant abnormal event that is incorporated into the blockchain's supervision, TSLA Coin's smart contracts require mandatory, strong real-time and fully automated triggering. The data for triggering conditions is also blockchain-protected data, accurate, safe and secure, and cannot be tampered with.

4、TSLA Coin consensus algorithm

TSLA Coin is a comprehensive and complex heterogeneous system, the IoT devices involve a wide range of industries and businesses, and there are various communication protocols, so the security and performance requirements of

the underlying blockchain are high. TSLA Coin solves the security, high performance and trust issues with the following features.

(1) A master node (Leader) is elected from all the nodes of the network based on the blockchain algorithm, and the master node is responsible for generating new blocks.

(2) Each node broadcasts the transactions sent from the user side to the whole network, and the master node sorts the multiple transactions collected from the network to be placed in the new block and puts them into a list, and broadcasts the list to the whole network.

(3) After each node receives the list of transactions, it simulates the execution of these transactions according to the sorting. After all transactions are executed, a hash digest of the new block is calculated based on the transaction results and broadcast to the whole network.

(4) If a node receives 2f (f is the number of tolerable SAFT nodes) digests from all other nodes equal to its own, it broadcasts a commit message to the whole network.

(5) If a node receives 2f+1 commit messages, it can commit the new block and its transactions to the local blockchain and state database.

2.7 TSLA Coin Operations Management

1. TSLA Coin account management and functions

(1) User management. User management mainly addresses the mapping of user identities to blockchain addresses and the confidentiality of user privacy.

(2) Account management. Account management is responsible for user account management, including account registration, login, cancellation, and the irrelevance of account and key processing. When registering an account, the user's customary user name, password and other identity information is mapped to the blockchain address.

(3) Key management. Under the fully managed model, the key management system is responsible for the association of user keys with accounts, key security management and loss recovery. The user key is generated at the user side, and the user can choose to save the key in the key safe or entrust it to an associated account to facilitate key recovery after loss. In order to ensure the reliability of the relationship between the user account and the key, the key management system uses multi-node chain storage for the signature of

the relationship.

(4) Permission management. The permission management module is responsible for the control and management of user accounts, key systems, node joining and exiting, data access and other permissions. It includes account delegation authority, node consensus authority and user data access authority. Audit permissions are used to provide audit functions for the supervisory authority, to strictly control access rights and data scope, and to enable user association for users whose transactions are not relevant on the shared ledger. Account delegation rights are used to control access to user account delegation relationships. The consensus permission is used to manage the consensus permission of participating or newly joined nodes, and the access permission is used to manage the query permission of data on the blockchain from the user side.

(5) User credit risk control management. The risk control module is responsible for risk control of user transaction behavior in the blockchain, which is adopted by the initial users of TSLA Coin.

2. Creation users and user instances

TSLA Coin Genesis users are all community users and enter

the network by means of transactions, so they enter the network with an initial trust relationship with a trust value of 1 on both sides.

User A sets up an auto-contract address in the TSLA Coin user interface that will automatically close 7 days after receipt of the product, posts the product on a social network/web commerce page, assuming a price of $158, and leaves a TSLA Coin auto-contract address.

An unknown user, B, sees this, scans the TSLA Coin auto-contract address on his mobile phone and pays. As no transaction has taken place between them, they must be in different domains. Therefore, User B notifies Verifier C in the Autonomous Domain, who finds Verifier D in User A's Autonomous Domain via a hash table, and sends the transaction message and updates the record. Verifier D sends a paid transaction message to User A's automatic contract address.

User A sees the change in the status of the contract address, ships the goods and updates the automatic contract shipping status. User B receives the goods and can update the status information in the same way as before and the automated contract is executed by A. In the absence of any action by B, the automated contract is executed by A after

7 days. The guaranteed transaction is executed through the automated contract and the validator.

After the transaction is completed, User A and User B form a relational chain and converge to try to establish an autonomous domain. if there is a path in the network that meets the conditions for convergence, both parties enter the new autonomous domain and broadcast the transaction information.

If User B identifies the product as a commodity counterfeit and sends a distrust to the automated contract address, User A deducts the required portion of the purchase price and decreases the trust index. If the trust index drops to 0, the user is permanently disabled from the network.

In summary, TSLA Coin will be a new underlying architecture platform based on e-commerce application scenarios: decentralised, open, secure and efficient. In the ecosystem, participants will be rewarded with appropriate Tokens for their sharing behaviour and effectiveness, and merchants will be able to enjoy the technical services while reducing the cost of entry into the platform and the variable cost of information processing.

As a transparent and open system, TSLA Coin hopes to

facilitate the development of global e-commerce and to drive the reinvention of social commerce through the sharing economy, forming an effective decentralised marketplace.

2.8 TSLA Coin Mining Incentives

1. Reward principle and reward

TSLA Coin introduces the blockchain TSLA Coin to improve the incentive mechanism of the platform and enhance the arithmetic power through transactions, services, learning, activities and material library. Users' login, interaction, release promotion, certification and other behaviors that contribute to the development of the community will be incentivized by TSLA Coin. The opposite effect. The amount each user receives is related to the user's counting power, and miners are ranked according to their counting power, with

the higher their counting power the more they will be rewarded. The TSLA Coin consumed in the ecosystem will be put into a fund pool for the continued development of the platform.

2、Basic mining

The TSLA Coin platform's basic mining arithmetic power is increased in the following ways.

(1) Mining rewards based on users' daily online log-in "punch cards".

(2) Mining rewards based on the number of times a user interacts with friends each day and for how long.

(3) Mining rewards based on the user's viewing of videos, uploading of videos, and other likes on additional uploaded videos.

(3) Receive mining rewards based on the user's top-up of TSLA Coin.

(4) Mining rewards based on the user's authentication of identity information.

(5) Mining rewards based on the user's completion of the task of inviting friends to participate.

(6) Mining rewards based on the completion of the user's advertising bounty task.

3、Shopping mining

When a user purchases a product, the TSLA Coin platform will return to the user the corresponding points rebate according to the coin value. Once the order is completed, users can use the points to bid on products, transfer them out, and buy them for a limited time.

4、Distribution mining

TSLA Coin promotion adopts the self-increasing fission promotion method, i.e. users can get fixed points rewards by inviting members. After a successful invitation, the invitee will be rewarded with points for each order placed by the inviter in the form of step-by-step rebate.

5、Arithmetic mining

Users can obtain points through shopping, distribution, tasks, etc., and also obtain arithmetic power, and after the arithmetic power reaches a specified level, they can participate in the platform sales dividends. Encourage users to participate and grow their loyalty.

6、Task mining

Users can complete various tasks in the TSLA Coin platform to obtain points or arithmetic power. Tasks can be added at will in the background, such as: daily check-in,

product evaluation and other recurring tasks and single tasks such as real name authentication. The user is rewarded for completing the corresponding task.

2.9 TSLA Coin design principles

1. Expansion principle

Each module of TSLA Coin is applied as a smart contract, so it is easy to add new modules to it, and each module itself can be updated without requiring changes to other module interfaces.

2. Scaling principle

TSLA Coin's application access is volatile, if a large number of users access a node, it will inevitably bring the consequences of node service collapse, so the node container itself can be deployed automatically to achieve horizontal expansion when user requests appear under pressure.

3. Security principles

TSLA Coin supports multi-channel feature, and the data between different channels are isolated from each other to improve isolation security, and supports unpluggable architecture, including consensus, authority management, encryption and decryption, ledger mechanism multi-module and other types.

2.10 TSLA Coin application scenarios

1. TSLA Wallet

TSLA Wallet creates a self-sufficient, decentralised wallet. The community contains a large data centre and an exchange based on real user performance. Users can use TSLA Wallet to buy relevant digital assets, reward their favourite content with TSLA Wallet, and video creators will be incentivised to publish and consume content and invite friends to watch it with them under the community. All advertising and revenue generated on the platform will be returned to the Foundation and rewarded to those who have contributed to the community. Users can follow a wide range of fresh and interesting information on the platform.

TSLA Wallet's setup for a decentralised wallet includes the use of immune data anchors as well as existing centralised facilities to cope with the needs of other applications, such as archive storage and scalable computing power. Decentralising all stacks seems unnecessary, inefficient and impractical, so TSLA Wallet has created a modular solution that allows legacy applications to take

advantage of the blockchain. It creates the payment portal solution that developers need, independent and easy to implement on legacy infrastructure. Switching from a centralised to a decentralised portal using this approach is not only easy for developers, but also allows for the consolidation of a minimal amount of resources to maximise convenience for developers.

The TSLA Wallet wallet is based on blockchain technology and develops a mobile TSLA Wallet wallet that integrates a universal wallet, lightning transfer, blockchain exchange and P2P chat in one, with priority support for Android and iOS. the TSLA Wallet wallet will greatly reduce the threshold for using digital assets and accelerate their popularity by providing a universal wallet, a lightning transfers, block-based

III overview of TSLA coin technology

3.1 Distributed control structure

TSLA Coin's digital encryption builds a distributed structure system based on an open source, decentralised protocol determined by the system, allowing information on value exchange to be sent to the entire network through distributed propagation, determining the content of information data through distributed bookkeeping and generating block data after stamping it with a time stamp, and then sending it to each node through distributed propagation to achieve distributed storage. Specifically, the distributed structure is reflected in 3 aspects.

1、Distributed bookkeeping

User behavioural trajectories and transaction data on the platform are recorded by multiple nodes, and their legality is verified. Legitimate transactions are recorded

in the books of all users, avoiding moral risks to the maximum extent and not prone to errors.

2. Distributed dissemination

Each new transaction in digital encryption is propagated in a distributed structure, according to the P2P network layer protocol, the message is sent directly from the delay node to all other nodes in the network.

3. Distributed Storage

Distributed storage allows all data in the database to be stored in all computer nodes of the system and updated in real time. The completely decentralised structure is set up so that data can be recorded in real time and updated in every network node involved in data storage, which greatly improves the security of the database.

In summary, the data storage, transaction verification and information transmission processes within the system are all decentralised through the three main technology modules of distributed bookkeeping, distributed dissemination and distributed storage. Payments are aggregated using a distributed exchange, with the buyer's pending order and the seller's pending order cached in digital encryption. When a consensus node does the bookkeeping, it automatically

triggers the buy-sell pending order, distributes the bill to the network, and completes the transaction after 51% or more of the nodes have validated it. The benefit of distributed aggregated transaction payments is that each transaction is documented and each transaction is confirmed by the widest range of nodes, increasing the security of transaction records while making it more difficult for hackers to manipulate the transaction board.

3.2　Secure encryption algorithm

TSLA digital trading platform selects the encryption mechanism in line with domestic and international standards to encrypt various data of the industry. The transaction data and information between users can only be viewed by both parties and users with corresponding permissions.

1. Private key

Non public, is a 256 bit random number, kept by the user and not open to the outside world. The private key is usually generated randomly by the system, which is the only proof of the user's account use right and the ownership of the assets in the account. Its effective bit length is large
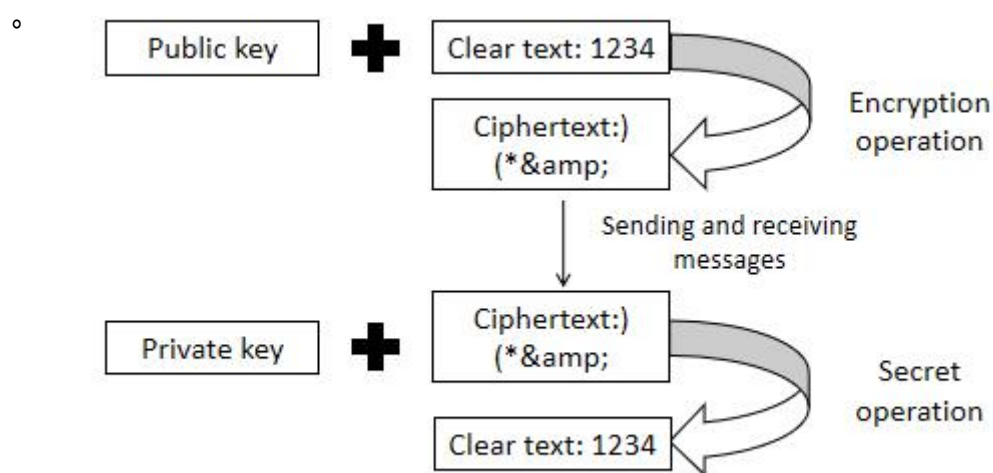
enough, so it is impossible to be broken, and there is no security risk.

2. Public key

Each private key has a matching public key. ECC public key can be generated by private key through one-way and deterministic algorithm. Currently, the common schemes include secp256r1 (International Standard) and secp256k1 (bitcoin standard). The control chain and initial data chain of TSLA digital trading platform choose secp256r1 as the key scheme.

°

```
Public key  +  Clear text: 1234          Encryption
               Ciphertext:)              operation
               (*&amp;
                    Sending and receiving
                         messages
               Ciphertext:)
               (*&amp;                    Secret
Private key +                             operation
               Clear text: 1234
```

3. Encryption

TSLA digital trading platform through asymmetric encryption of digital signature technology, so that the business request in the transmission process is not tampered with, and through the consensus mechanism to ensure that the

data of each node is consistent. The stored data records are checked by self checking system and quasi real-time multi node system to ensure that the stored data records can not be tampered.

The self verification of nodes means that TSLA digital trading platform uses block chain structure to store data records. Tampering with data will destroy the integrity of block chain structure. The system can quickly check out and recover data from other nodes. In addition, each accounting node of TSLA digital trading platform has its own private key. The signature of the private key of the node is recorded in each block, and the modification of the data in the block can be verified by the signature.

Just in time multi node data verification: when the private key of a node is stolen, it is possible for malicious users to modify all the data in the ledger chain. Digital encryption of TSLA digital trading platform provides a data comparison mechanism of just in time multi node, which can discover the situation of a node's ledger data being tampered in time.

## 3.3 Malicious Attack Prevention

and Penalty Mechanism

If a height exceeds 100 from the latest height, all blocks at that height will be considered expired during the consensus process, and all new consensus activity on those blocks will be simply ignored. Therefore it is almost impossible to accomplish a long-rangeattack in PoD, but it is still possible to launch a short-rangeattack within the validity period. The short-range attacker, Attacker, tries to forge chain A to replace chain B as the authoritative chain while the block with high H+1 has not yet expired, and Attacker needs to make block A1 score higher than B1. Since multiple casts will be severely punished, the Attacker will inevitably have to bribe the verifier, otherwise the short-range attack cannot be completed. To demonstrate the security of the PoD consensus algorithm, the following is a separate analysis of the cost to the Attacker when invalidating different numbers of blocks. If Attacker wants to invalidate B1 with the minimum cost as shown in the diagram, it is equivalent to a double payment attack where Attacker is lucky enough to be a block proponent of H+1 height, then at least 1/3 of the verifiers in dynasty D0 need to be bribed

to over vote to bring A1 to finality with a minimum cost of 1/3 of all deposits.
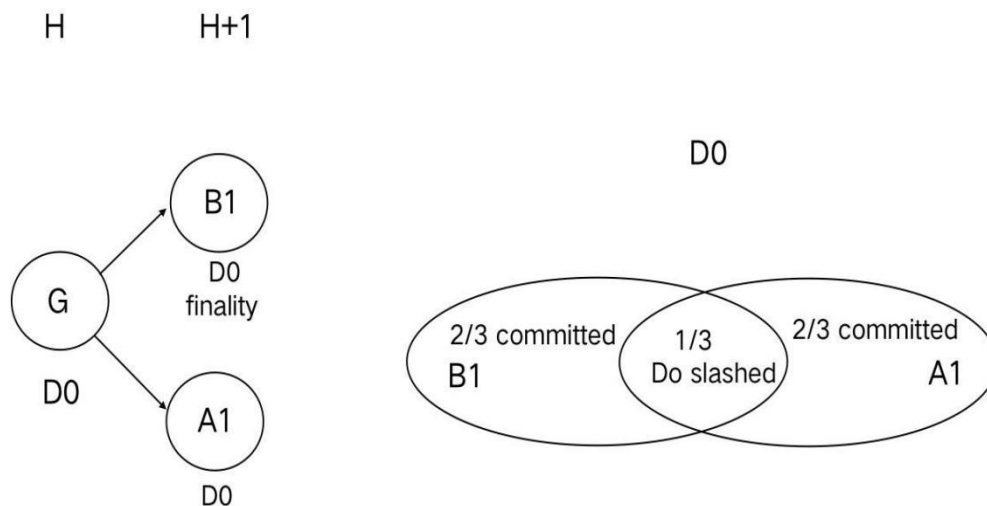
If the Attacker wants to invalidate B1-B2, assuming that both B1 and B2 have reached finality and that the transactions in the block are all valid, in order to invalidate these transactions, two cases are considered here. The first is shown below, where height H+1 and H+2 are in the same Epoch with the same dynasty, then the Attacker first needs to bribe 1/3 of the validators in D0 to make A1 reach finality, at which point this 1/3 of the validators will be penalised and the deposit financed. In A2's validation the overall deposit total is only 2/3 of A1's. At this point, if the Attacker wants A2 to reach the same value as B2's commt ticket, he needs to bribe all the remaining validators who

are not cheating, which together will cost at least 3/3 of the total deposit, and even then there is no guarantee that A1 will score higher than B1, and the risk of the attack failing is high. In the second case, as shown in the diagram below, the heights H+1 and H+2 are in different Epochs with different dynasties, so the Attacker would need to bribe 1/3 of D0 to get A1 to finality and then 1/3 of D1 to get A2 to finality, costing at least 2/3 of the total deposit to complete such an attack. To launch a short-range attack to invalidate two finality blocks would cost at least 2/3 of the total deposit.
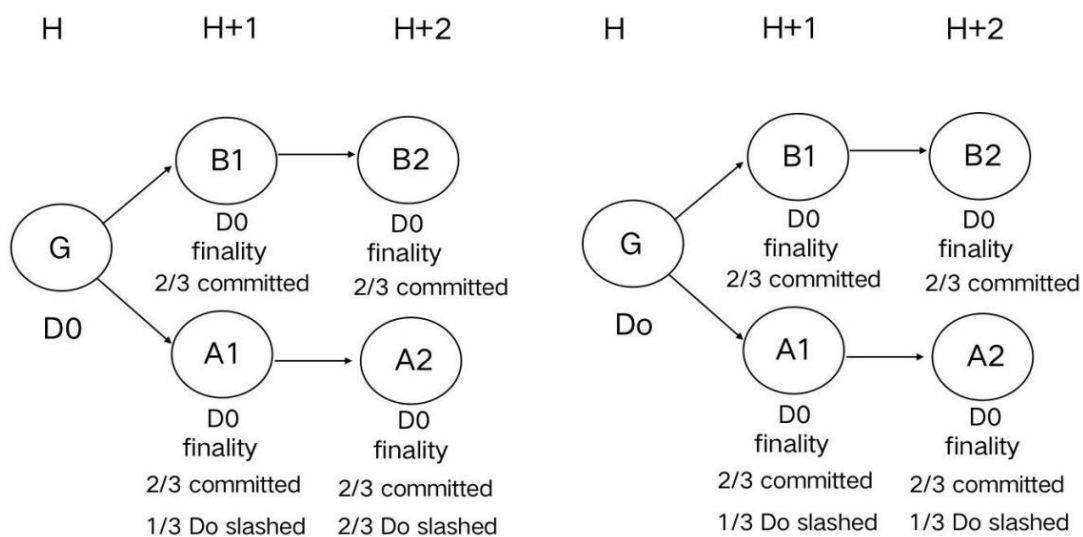
If the Attacker wanted to invalidate B1-B3, as shown below, the Attacker would first need to bribe 1/3 of D0 to complete A1's finality, then 1/3 of D1 to complete A2's finality, and finally 2/3 of D1 to complete A3's finality, resulting in a loss of at least It will be very difficult to prepare for these attacks, and even if we are lucky enough to do so, we may not be able to guarantee a higher score for A1 than B1, and the attack may fail.
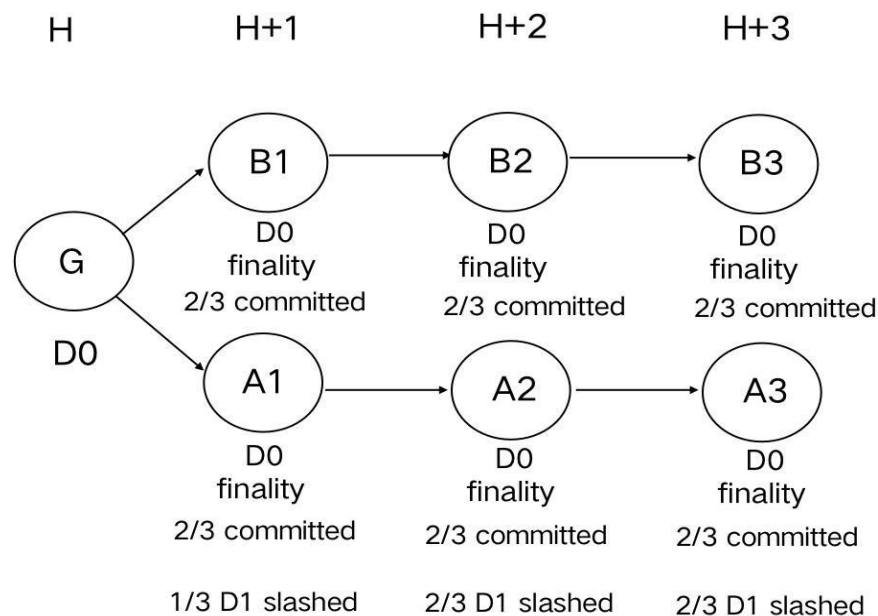

3.4　Resilient　Consensus Mechanisms

A stable and effective block generation mechanism is the cornerstone of the TSLA Coin blockchain ecosystem. The TSLA Coin main chain uses the new IPOS consensus mechanism to ensure high frequency and stable block generation in order

to enhance the user experience. Different sectors and industries require different network operation mechanisms, and TSLA Coin is configured with different consensus algorithms to meet different usage requirements; the consensus under the TSLA Coin protocol uses a pluggable algorithm, and users can choose their own consensus algorithm according to their needs.
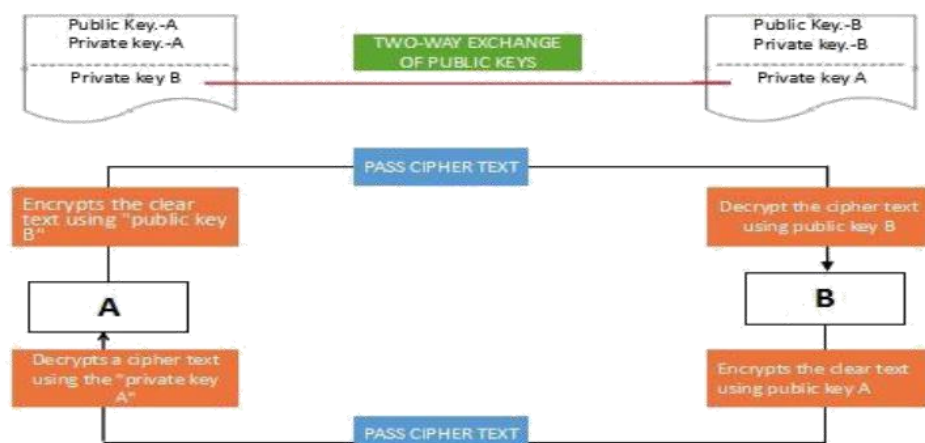
3.5 TSLA + cloud storage

TSLA storage provides a special storage mechanism, which can not only prevent the storage of duplicate data, but also ensure the same security, break the "common sense" of the industry, and achieve both fish and bear. When using this mechanism, in addition to the user permission table, a global metadata table should be maintained to record the corresponding relationship

between plaintext hash and ciphertext hash. When writing data, you should first query whether there is the same hash data, and if there is no such item, save it again

- Hash (data) ➡ hdata to calculate plaintext hash

- If checkdup (hdata) = true goto 11, if the same data already exists, go to step 11

- The symmetric key is randomly generated by randomsym () ➡ STK as the file storage key

- Enc (STK, data) ➡ encdata encrypt files with storage key

- Hash (encdata) ➡ henc to calculate ciphertext hash

- The symmetric key is generated from the plaintext of the data by genkey (data) ➡ sData

- After adding salt, hash value is calculated. The reason for adding salt is that plaintext hash is a public value. If storage blockchain is not added salt to enable partial storage, people who do not have plaintext data can also obtain the key. In order to ensure consistency, the salt value can be a fixed value.

- Enc (hdata, STK) ➡ encstk'encrypts the storage with the symmetric key generated by the data plaintext

● Store the key. This is a very "weird" step. It uses plaintext as the key and the key as plaintext to encrypt. When most people look at this algorithm, they think it is reversed. In fact, it is specially designed in this way, and this step is the core step of de duplication after encryption.

● Putipfs (encdata) stores encrypted data into IPFs

● Putmeta (hdata, henv, encstk) stores encrypted ciphertext hash and plaintext

● The key is recorded in the global metadata table and in the plaintext hash key

● Goto 14

● Get meta (hdata) ➔ henv, encstk'get ciphertext from global metadata table

● Storage key after hash and plaintext encryption

● Genkey (data) ➔ sData uses the same algorithm to generate symmetric key from data plaintext

● The symmetric key is used by Dec (sData, encstk ') ➔ STK to decrypt the storage key

● Enc (spub, STK) ➔ encstk uses the user's encryption public key to encrypt and store the key

- Putpri (hdata, encstk) stores the encrypted storage key of the encrypted public key to the user

- The user permission list is recorded under the clear text hash item

- When getting data, take out the corresponding ciphertext hash from the plaintext hash in the global metadata table, take out the ciphertext hash from the IPFs through the ciphertext hash, take out the encrypted storage key from the permission list, decrypt the encrypted storage key with the user's encryption private key to obtain the storage key, and decrypt the encrypted data with the storage key to obtain the data plaintext.

- It is obtained by getmeta (hdata) ➔ henc from the global metadata table through plaintext hash

- The ciphertext hash getpri (hdata) ➔ encstk obtains the encrypted public key from the permission list through plaintext hash

- Get IPFs (henc) ➔ encdata extract ciphertext from IPFs with ciphertext hash

- Dec (sprv, encstk) ➔ STK encrypts the user's public key with the user's private key

- The encrypted storage key is decrypted to obtain the storage key

- Dec (STK, encdata) ➔ data decryption to obtain file data

- The optimized DSN scheme not only effectively guarantees the security of data, but also realizes encryption and de duplication. In order to achieve better de duplication effect, the data can be divided into blocks according to a fixed length, and each block is de duplicated separately. The above scheme can only be used to store static data. When storing dynamic data, not only the ID that does not change with the content should be used to replace hash as the identification of data, but also the verification of write permission should be added to prevent the data from being covered and tampered by others.

- The creation process is as follows:

- Xun randomasm () ➔ swpub, SwPrv randomly generates asymmetric key as write permission key

- Create (swpub) ➔ ID creates a dynamic data, obtains a unique ID, and records the public key of the write permission corresponding to the ID

● Random sym () ➜ STK randomly generates symmetric key as storage key

● Enc (spub, STK) ➜ encstk uses the user's encryption public key to encrypt and store the key

● Putpri (ID, encstk) stores the encrypted storage key of the encrypted public key into the user permission list, and records it under the ID. the process of each data writing is as follows:

● Get pri (ID) ➜ encstk to retrieve the encrypted storage key from the user permission table

● Dec (sprv, encstk) ➜ STK encrypts the user's public key with the user's private key

● The storage key is obtained by decryption

● Enc (STK, data) ➜ encdata encrypt files with storage key

● Hash (encdata) ➜ henc to calculate ciphertext hash

● Enc (SwPrv, henc) ➜ enchenc uses the public key of the ID's write permission to hash the ciphertext

● autograph

● Putdyn (ID, encdata, enchenc) writes encrypted dynamic data to sign data

- Write authorization on behalf of. When a node storing dynamic data fragments writes dynamic data, it needs to verify the write permission first

- Get key (ID) → swpub get the public key of write permission corresponding to the ID

- Hash (encdata) → henc to calculate ciphertext hash

- If Dec (swpub, enchenc) = henc write (encdata)

- The reading process of writing dynamic data is as follows:

- From the permission list, getpri (ID) → encstk obtains the data encrypted with the encryption public key corresponding to the ID

- Storage key

- Get dyn (ID) → encdata read ciphertext from dynamic data storage area with ID

- Dec (sprv, encstk) → STK encrypts the user's encrypted public key with the user's encrypted private key

- The encrypted storage key is decrypted to obtain the storage key

●Dec (STK, encdata) ➜ data decryption to obtain file data

3.6 TSLA Coin decentralized Wallet

TSLA Coin has the same transaction format as Polkadot for cross chain message transmission.

Address: ss58 code address of the sending account.

Block hash: block hash

Block number: block number

· Genesis hash: Genesis hash

Metadata: submit the scale encoded metadata of the runtime

· nonce: nonce of this transaction

Spec version: the spec version of the current runtime.

Transaction version: the version number of the current transaction format

· era period: effective number of transaction checkpoints

Therefore, Polkadot JS library can be directly compatible with TSLA Coin public chain. Polkadot JS tool contains the command tool for group interaction with the
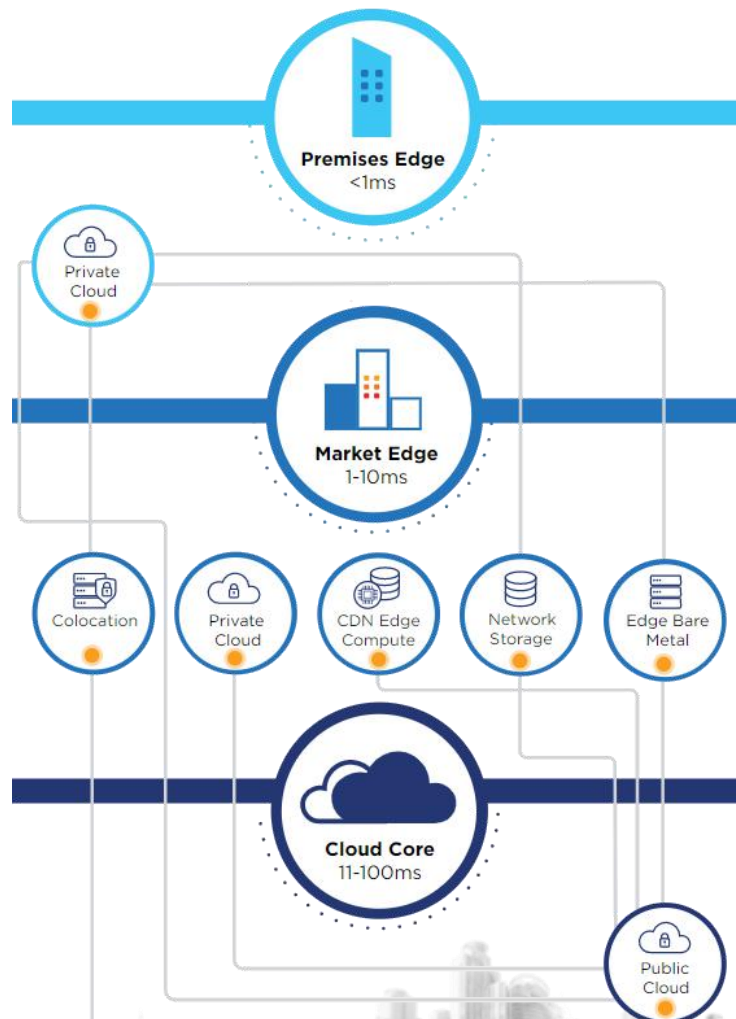
subject client, including a tool named "signer cli" for creating, signing and broadcasting transactions.

(1) To create a transaction:

```
yarn  run:signer sign  --account <from-account-ss58> --seed <seed> --type <sr25519|ed25519> <payload>
```

(2) Submit transaction:

```
yarn        run:signer     submit        --account <from-account-ss58>        --ws      ws://127.0.0.1:9944 balances.transferKeepAlive      <from-account-ss58> 500000000000
```

IV Overview of TSLA Coin

4.1 Introduction to TSLA Coin

In order to accelerate the adoption of blockchain technology and the development of TSLA Coin, TSLA Coin allows members to register. It accepts donations and philanthropic activities related to blockchain technology and the world.

4.2 TSLA Coin Governance Principles

The governance principles of TSLA Coin are to support and coordinate the efforts of the blockchain community, to promote the promotion of blockchain technology and provide better prospects for TSLA Coin through concerted efforts in education and awareness campaigns, to promote the use of blockchain technology and the related technical requirements for enthusiasts, developers, regulators, technicians, practitioners and users worldwide.

4.3 TSLA Coin Budget Plan

TSLA Coin will be issued for a total of 10,000 trillion and will never be increased. TSLA Coin will consist of four components: community incentive, team holdings, foundation and promotion, as a means of promoting a stable and thriving e-commerce ecosystem.

4.4 TSLA Coin Distribution Plan

4.5 Benefits of TSLA Coin

1. The price of TSLA Coin will continue to rise with the operation of TSLA Coin and the development of the project itself. The increase in the number of users and the increase in the exchange power will make TSLA Coin more well-known in the market and the platform itself will rapidly double in value.

2. The TSLA Coin project is open to all users, and the high profitability of the overall project is due to the support of all users, so users holding TSLA Coin will enjoy the project dividends, which is also the TSLA Coin project has been adhering to the concept of win-win cooperation!

3. Voting rights for TSLA Coin holders. The entire TSLA Coin project encourages multi-party financing, and users can also take shares to become shareholders, i.e. users who own TSLA Coin tokens are also a member of the TSLA Coin project, giving users TSLA Coin voting rights and interests, according to the number of TSLA Coin tokens held by users, the more tokens, the higher the level, and the higher the level of the TSLA Coin project. The higher the number of tokens, the higher the level, the more the right to give guidance and make suggestions and comments on the overall operation of the TSLA Coin project.

V TSLA Coin Team

Graduated from Moscow Institute of Engineering Physics with a dual degree in engineering and economics. Currently, he is the architect of TSLA Coin digital ecological data.

CEO

Alcot

She has a master's degree in financial management from the University of Edinburgh. She worked for Morgan Stanley Investment Bank and was mainly responsible for investment consulting at TSLA Coin.

CFO

Prescott

CMO

Worthingto

Sogou is the core development member of big data platform. It takes the lead in TSLA Coin core index calculation, task monitoring, task scheduling and task optimization. It also takes the lead in TSLA Coin product development and blockchain technology

CTO

Garfield

He is a top enterprise architecture master who has designed and diagnosed project level architecture for many famous enterprises such as Google and Amazon.

VI Development Planning

Duration	Development planning content
February-March 2021	Completion of market research and prep work for the TSLA Coin-based project and commencement of the project.
April-May 2021	Completed development of the TSLA Coin based project and released a white paper on the TSLA Coin project.
June-July 2021	Build the Dapp, invite users for internal testing and launch the live TSLA Coin project.
August-September 2021	Applications such as TSLA Wallet and TSLA Exchange are live and ready for smart contract deployment.
October-November 2021	Testing and tuning of the TSLA Coin main chain. Major exchanges go live after completion of tuning

December 2021	TSLA Videa promotional platform, TSLA Game platform, TSLA Shop shopping mall and more ecological applications are implemented.
2022	TSLA Coin is expanded globally.

VII Disclaimers

As expressly set out in this White Paper, the Foundation makes no representations or warranties (in particular as to its merchantability and specific functionality) with respect to TSLA Coin or the availability of the TSLA Coin Glossary. Any consumer participating in the TSLA Coin public sales program and purchasing TSLA Coin is doing so based on his own knowledge of TSLA Coin and TSLA Coin and the information in this White Paper. Subject to the satisfaction of the foregoing, upon the commencement of the TSLA Coin program, all participants will receive TSLA Coin regardless of its specifications, parameters, performance or functionality. TSLA Coin hereby disclaims and denies liability for:

1. any consumer who purchases TSLA Coin in breach of any

national anti-money laundering, counter-terrorist financing or other regulatory requirements.

2. any breach by any consumer of any representation, warranty, obligation, promise or other requirement in connection with the purchase of TSLA Coin and the consequent non-payment or inability to withdraw TSLA Coin;

3. the suspension of the TSLA Coin public sale program for any reason; the unavailability or delayed delivery of TSLA Coin due to a failure or delay in the development of TSLA Coin;

4. any of the risk factors disclosed in this White Paper, and the damages, losses, claims, liabilities, penalties, costs or other adverse effects associated with such risk factors.