NEW POWER COIN

Decentralized Global Online Traffic Engine
Based on User Portraits

WHITEPAPER

V1.0

This Whitepaper represents general information about New Power Coin. Please ensure you first read the disclaimer and risk factors at the end of the document to fully understand the purpose, status, and limitations of this Whitepaper.

Table of Contents

I. Vision

Building a new source of internet traffic:

DECENTRALIZED GOLBAL ONLINE TRAFFIC ENGINE BASED ON USER PORTRAITS

II. Introduction

2.1 Background

In 2008, Satoshi Nakamoto published Bitcoin, which opened the gate to the new generation of Web 3.0. Since the advent of Bitcoin, blockchain applications took on many different forms. From distributed ledgers, computing platforms and various financial instruments, blockchain is gradually solving more and more value transfer problems in a decentralized way.

The current blockchain systems are still very primitive, most of them are basically a decentralized ledger, and not yet able to deliver strong and decentralized computation capabilities. However, as people expected, the decentralized computing capability will gradually increase in the future, as the infrastructure of blockchain evolves.

Blockchain is an important foundation of Web3.0. On his blog, Gavin Wood defined Web 3.0 as:

> *Web 3.0, or as might be termed the "post-Snowden" web, is a reimagination of the sorts of things that we already use the Web for, but with a fundamentally different model for the interactions between parties. Information that we assume to be public, we publish. Information that we assume to be agreed, we place on a consensus-ledger. Information that we assume to be private, we keep secret and never reveal. Communication always takes place over encrypted channels and only with pseudonymous identities as endpoints; never with anything traceable (such as IP addresses). In short, we engineer the system to mathematically enforce our prior assumptions, since no government or organisation can reasonably be trusted. [1]*

The Internet has begun to migrate to Web 3.0. The goal of Web 3.0 is to provide features such as value transfer, transparency, trust, privacy protection, and interoperability, while reshaping the Internet.

The user's attentional migration creates traffic. Early internet advocates supported decentralization, interoperability, and openness. However, the internet traffic is gradually concentrated and controlled in the hands of a few people. Under this circumstance, the ecological environment of internet traffic is deteriorating, the intermediate cost is increasing, the user's privacy data is violated, and malicious fraud is rampant. Resulting in damaged interests of participants across the board, with varying degrees of severity.

[1] Wood Gavin 13.09.2018 https://bitcoinmagazine.com/articles/web-3-0-chat-ethereums-gavin-wood-1398455401/

Online advertising is beginning to show a downward trend in traffic. There are several reasons for this:

1. The number of new users is reduced, so that all the apps compete with each other for the existing users, resulting in fewer choices for the user.

2. Intermediaries are increasing their fees for the cost of advertising.

3. The decline of internet marketing, traffic data fraud, internal rebates, and other issues are increasing.

4. In order to reduce costs, publishers have reduced the quality of traffic due to conduct cheating.

5. In order to achieve accurate matching and raise advertising prices, user privacy is seriously affected.

6. The user experience is poor. The users experience suffers greatly, in the way that many applications force users to view the advertisements before they can continue to use the substantive functions. Negatively impacting on the user's impression of the advertisements, and greatly reducing the user's attention span.

Based on the rapid development of the Internet, the NPW development team plan to launch an engine for decentralized Internet traffic exchange on the blockchain. The NPW digital currency is used as an economic support to provide traffic trading services.

2.2 Closed economic model

Bitcoin and blockchain will be a revolution for the online community, but we can only partially agree with Bitcoin's economic model, because Bitcoin's model inevitably creates a problem:
It is impossible for everyone to participate in mining. The economic transmission of Bitcoin is one-way only. If everyone mines, no one will buy Bitcoin. The price of Bitcoin is mainly reflected in the purchase of latecomers. As long as no one buys for a period of time, there will be an inevitable collapse in value, which will economically hurt the latecomers. This scenario has become evident in the history of bitcoin. This is one of the fundamental reasons why many people have doubts about Bitcoin's market value.

This is also the ultimate paradox of all cryptocurrencies currently on the market, resulting in most of the cryptocurrencies being a short-lived, and having do be disbanded before they are able to solve the problems they claimed to solve.

We believe that cryptocurrency should not behave like this. It should have a reasonable economic loop that does not rely entirely on external forces.

If we compare a common product: TV. It has a typical and ancient economic closed loop:

The TV station broadcasts the program to the audience -> **viewers watch the program** -> **the publisher inserts the advertisement in the program** -> **the TV station charges the publisher's advertising fee** -> **the TV station takes out part of the income for the preparation of new programs** ->...

This is a closed-loop economy that everyone is happy with, everyone gets paid, but more than paying, no one gets the short end of the one-way economic chain, and there are no ultimate victims. Although the merchants paid the advertising fee, they gained the attention that will be transformed into purchasing power; the TV station paid the labor and funds for preparing the programs and gained the advertising fee of the merchants; the viewer watched the TV program to get entertained, watched the advertisement and purchased. Therefore, everyone is willing and actively involved in the economic closed loop.

Inspired by this, we also designed an economic closed loop for the NPW network, as shown below:

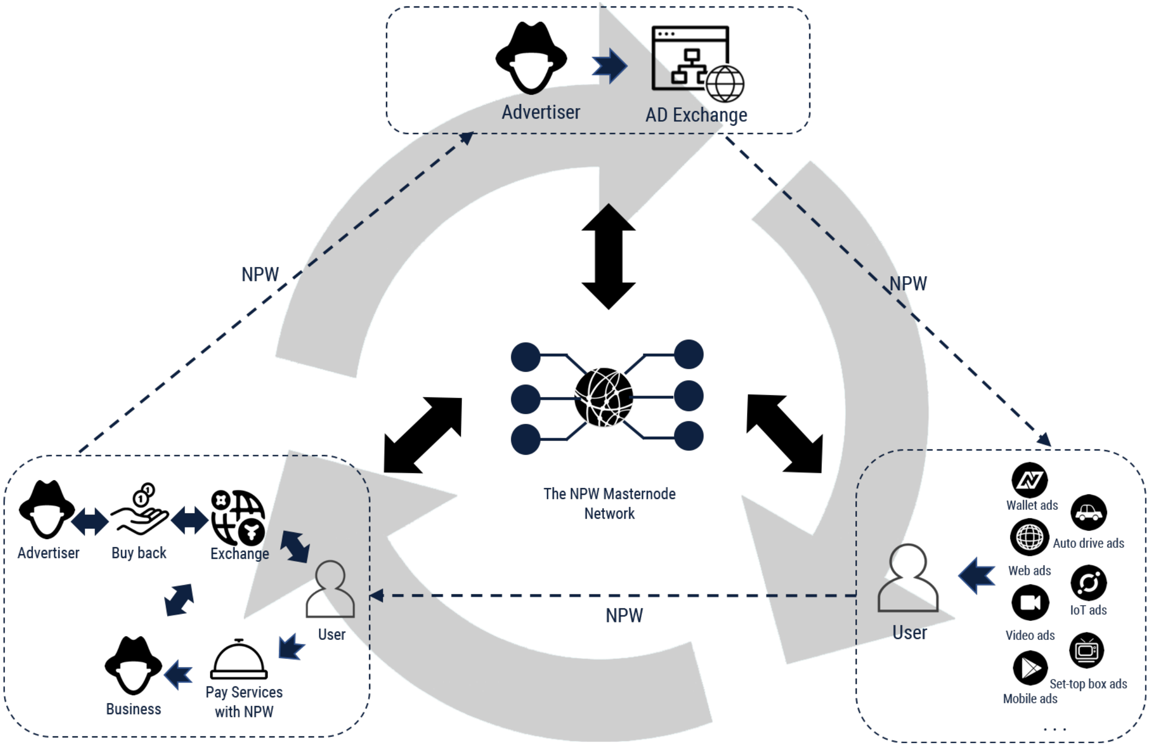


Fig. 1. Closed ecosystem model

In our economic system:

Publishers buy NPW, recharge for advertising -> **users browse or view advertising information in various media to get NPW** -> **users get the NPW used to pay services and goods, or cash in from the platform** -> **publishers buy back NPW for advertising** ->...

In the economic closed-loop of TV stations, the audience indirectly receives spiritual and entertainment benefits, however, NPW end users benefit from direct economic profit.

The above is the core description of the economic system of the NPW network. The detailed implementation principles and mechanisms can be found in the following sections.

2.3 Next generation of platform

As the next generation of advertising traffic platform, we can use the blockchain to achieve the transcendence of traditional propaganda platforms (TV/radio/street billboards, etc.), traditional Internet traffic, and have an opportunity to connect to any source of advertising traffic generated in the future:

- ✓ Both the source and the demand side of the advertisement can be served automatically;
- ✓ Providing a complete on-chain trust mechanism, all parties can ensure that statistics are completely transparent and improve their efficiency;
- ✓ On-chain statistical analysis can ensure that user privacy is not controlled by third parties and the ads can also be accurately matched, so that advertising content can truly help consumers;
- ✓ Remove the intermediary, and all the ad matching work is automatically executed to improve the advertising efficiency;
- ✓ Multi-source automatic price synchronization and real-time bidding;
- ✓ The trust mechanism allows the end user to trust the advertisement itself. The form of advertisement changes from traditional marketing to the end user's real initiative to obtain the source of advertising information as a reference for consumption.

At present, New Power Coin has launched the basic public chain, with features of **masternode support, one-click masternode deployment, private transaction, and instant transaction** capabilities.

↓

On this basis, New Power Coin will also develop a full suite of technical capabilities to gradually support **decentralized traffic transactions, inter-advertisement traffic transactions, multi-platform and multi-advertising presentations, accurate matching based on user portraits, user privacy protection, and avoidance of traffic fraud**.

↓

New Power Coin will serve as the base cryptocurrency for the underlying data stream exchange with network transactions. It will build a large system of **decentralized Internet traffic exchange, providing billing, delivery, statistics, user portraits, tags, and support multiple online decentralized advertising platforms**.

Internet traffic is the core underlying service of the Internet. In this whitepaper, we hope to introduce how to apply New Power Coin for online traffic and describe the development plan of New Power Coin.

III. The challenges

3.1 Sources of traffic

Traditional sources of Internet traffic are often presented in the form of digital ad exchange networks. The roles include:

Advertiser: Digital advertising buyer who wants to promote their products.

Publisher: Software/websites with digital ad traffic that can earn revenue by embedding ads.

Ad network: A platform for connecting multiple advertisers and publishers for ad exchange.

The media of the advertisement includes: Websites, computer software, videos, apps, games, mobile sites, etc. At the same time, modern Internet advertising systems usually mark a variety of attributes and operations for a single user in order to understand the user's customary behavior. Advertisers can usually manage the user's Lifetime Value through this tagging method.

For example: An independent game developer, Valerica Studios, developed a free indie game. The game has been tested and the game retention rate and activity rate are extremely high. Such games are difficult to make profits, therefore, the studio registered as the publisher of NPW, using the game as a medium, using NPW as the advertising platform, earning income, and continuing to develop games for their fans.

3.2 Internet traffic environment

The foundation of the Internet is initially based on the acquisition of content, followed by communication. In the above process, the migration of user interests and attention is turned into traffic. Studies have shown that the user's attention is easily guided and migrated, and it is inferred that having control over Internet traffic is equal to possessing power over the user.

In the past two or three decades, the global Internet has experienced tremendous growth. In the beginning, the Internet's infrastructure has been based on "browser-server", and "client-server" architecture. In the traditional PC Internet era, various browsers serve as the basic entry for traffic, and advertisements use the URL to perform traffic jumps and statistical analysis. In the era of mobile internet, the two giants Apple and Google have built the only two operating system portals of the mobile internet: iOS and Android, forming a substantial monopoly. The mobile Internet no longer has a URL, and the traffic is narrowed down to a form where the user is guided to a respective app, followed by the download of the app's package. Through this method, the giants quickly seized the traffic portal and quickly established a business model based on internet advertising.

Traffic is valuable as a core Internet resource. In the past two decades, more and more companies have gradually segmented Internet traffic. Because of the scarcity of traffic, third-party traffic platforms do not integrate traffic from a higher dimension like the giants do, but they also control the price and propensity of traffic at a certain level.

There will be more new products and services on the market, as well as more sources of traffic. Internet traffic and attention will be a permanent topic, and will always exist in different forms, regardless of changes in technology and business form.

3.3 Current major problems with Internet traffic

3.3.1 Traffic is controlled by giants

Currently, the business models of a few Internet giants are based on Internet advertising. Internet advertising is an important form of driving user traffic, but it is not the only form.

Traffic should be like flowing water, allowing users to flow freely according to their real interests, and should not be limited to a single product or a single service. The internet giants have built a business model on top of Internet advertising, and the potential harm would, if become reality, be enormous. The massive data collecting and storing capabilities of the internet giants mean that users can be analyzed, and the users' attention can be manipulated in the company's favor. These interests belong to the basic interests of users, and the purpose of giant business is to be responsible for shareholders. Therefore, the control and manipulation of interests has created the Internet's advertising environment we have today.

3.3.2 Users are always vulnerable

The centralized-based advertising model will certainly be manipulated to a certain extent, and it is impossible to actually return the ownership of the data to the user.

Whether it is based on the analysis of search behavior, purchase behavior or social behavior of each individual user, the advertising behavior proves to be efficient and an advertising model with a high conversion rate. Results advertised in this way are very easy to manipulate and control, and it is difficult to produce a win-win situation. In the end, users will always remain vulnerable.

The more data the user generates, the more positive the loop turns out to be for the advertising platform. But for the user's rights, it will become a vicious circle. The user's usage behavior is always controlled by the giant's advertising platform, and the user's attention will soon be monopolized by the interests of the biggest advertising platform and progressively guided and manipulated.

3.3.3 User privacy is difficult to protect

The traffic model on the internet makes it difficult for anyone, including a centralized advertising platform, to protect the privacy of users. All of the user's online behavior and information is stored and analyzed centrally.

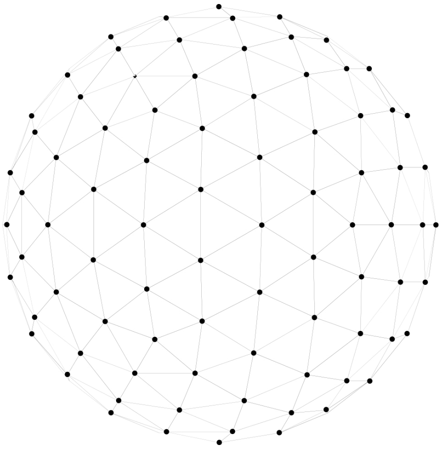
Although various types of regulation emerged, including the emergence of GDPR in Europe, most of the analysis of user data done by the giants is still qualitative analysis. Qualitative analysis is not involving specific users, but ultimately the control of users is individual and independent. At the same time, due to the Matthew effect, the higher the upper-level traffic source, the easier it is to be manipulated, which makes the user's behavior data easily exploited, turning it into a vicious circle, and it can even result in the from of a vicious political event.

3.3.4 Concentration of traffic leads to low technological innovation

Because Internet traffic is easy to manipulate, resulting in low tail value, popular content is an easy prey for the big companies, thus suppressing technological innovation. Because the demographic dividend can be obtained quickly through funds alone, and Internet traffic control continues, no one has the desire for technological innovation in the process.

3.4 New opportunities for existing internet advertising business

Blockchain transforms traditional computer morphologies from centralized computing to decentralized computing. Because of this, for the first time, humans have the ability to make computers automatically calculated without being manipulated. Most digital information flow-based services have the opportunity to migrate to the decentralization of blockchain.



Internet traffic is always a huge market and the underlying basis for the Internet to operate. We have been exploring how to use blockchain technology to find pain points and address the demand for traffic services in a conclusive way.

The existing Internet advertising market has entered a period of rapid decline, and the functions that today's blockchain can achieve are still very limited, mainly reflected in:

- User awareness is limited, and the number of users of blockchain is quite small.
- The underlying technology is relatively simple, and the development depth is low;
- The user experience is poor and it is difficult to benefit ordinary users;
- The blockchain application is too basic and does not yet have refined assets as the pioneer applications of other well known companies in the industry.

In such an early environment, no real benchmarking application can be shown to people, what a real blockchain traffic application should look like.

For the giants, it is difficult to make a real change to their core business by using the blockchain. Because once the blockchain is used, it means complete disruption of the business model. No matter the huge investment in the early stage or the accumulation of vast numbers of users in the later period, it has become a huge burden on the giants.

In this process of transition from the centralized model to the decentralized model, for most giants, it is the most important consideration for combating competitors who are likely to substitute them. Therefore, we also see that today's advertising giants are actively suppressing the advertising of blockchain and digital currency. They use the idea of preventing fraud and prohibit blockchain advertisements from appearing on their platforms.

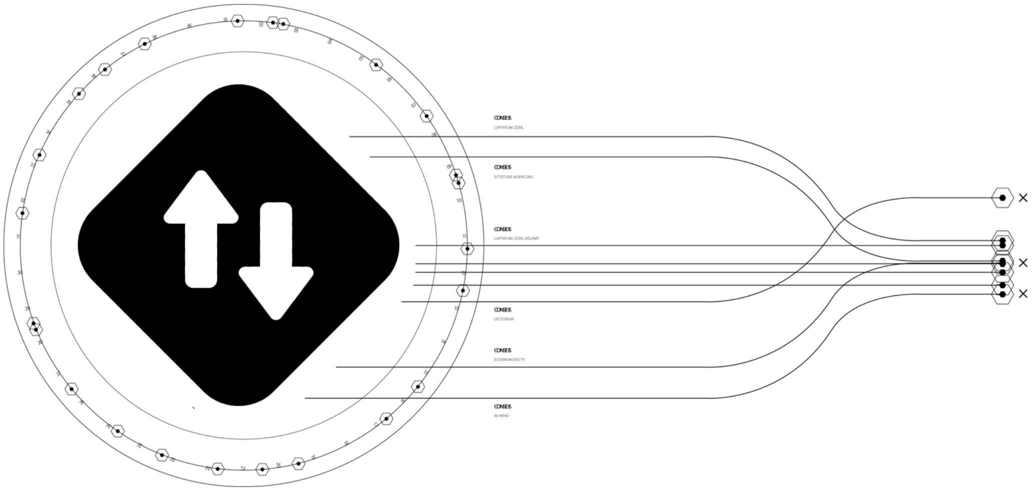
As with all commercial services, the blockchain traffic business also needs an economic cycle. If there is a need, it will generate the provider of the service, which will lead to ecology. With the ecology, the economic system will undergo internal circulation.

Another issue that requires further attention and needs to be solved in the traditional Internet digital advertising industry is that it is a capital-intensive industry. In the process of advertising, funds are heavily occupied, and the payment is easy to generate large debts. The use of blockchain for economic circulation can achieve an efficient, secure, real-time settlement, and large-scale fund management can be achieved without an intermediary.

At the same time, today's various blockchain projects have the need of promotion, and the projects need to accurately find a solid base of more digital currency users and build a lasting community. For the emerging Internet form of blockchain, the demand for traffic is huge.

3.5 Problem New Power Coin hope to solve

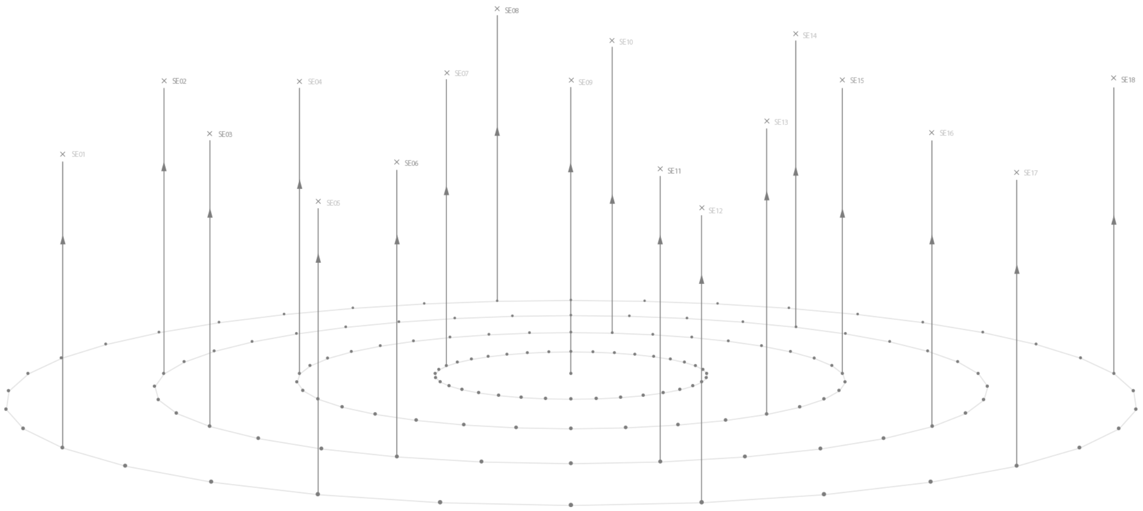
The nature of millions of users on the Internet jumping between different services and content is that it is decentralized and should ideally be transferred according to the true will of the user and not be manipulated in any way. The limitations of the traditional Internet have allowed the control of traffic to gradually gather in the hands of the giants.



The development of blockchain will inevitably undergo a progressive process, just like the development of the internet industry in the past. As the basis of the Internet, traffic should be solved first in the decentralized era of blockchain. The inevitable path of development will be to decentralize traffic first, and gradually get all kinds of blockchain infrastructure on track, and then drive the basic application.

In the next 5-10 years, the application of the Internet will be transformed into decentralization. The new power coin has the opportunity to build a new traffic promotion model that is completely different from the traditional Internet advertising model, allowing users to participate and not be manipulated by a single commercial entity. The overall design of the system is not to serve the centralization benefits, but to let every roles partake in the win-win situation.

The new power coin can not only be used as a basic traffic platform, but in addition to being the best application demonstration, the blockchain itself will serve as a traffic engine, enabling other service providers to build their own traffic applications.



IV. The architecture

Our goal is to build a decentralized online traffic engine, the new power coin is the basis. We will design the blockchain network and business architecture based on the technical requirements of the decentralized online traffic engine, which will be discussed further below.

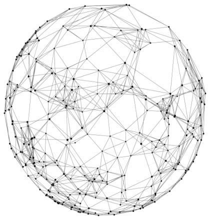
4.1 Technical requirements

In the scenario of decentralized internet traffic, it is necessary to have enough nodes connected to the network, and to have multiple nodes that are online and stable, in order to ensure the continuity and stability of the overall traffic service.

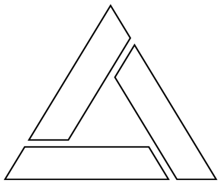
Based on this consideration, on the one hand, we can use PoS consensus, the staking ensures that there are enough online nodes in the network, because the user can only get the return when the wallet is running, which meets our first requirement: to provide enough online nodes on the network.

On the other hand, because masternode service provides a high return, it will also meet our second requirement: someone on the network spontaneously provides a fixed IP address and reliable full-node service support. Through the masternode service, the New Power Coin ad exchange will gradually leverage masternode servers to provide online creative verification, statistics, anti-fraud analysis and decentralized user portrait capabilities.

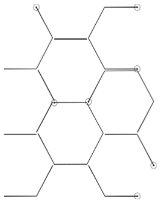
We design the basic objectives of NPW according to the following characteristics:



Decentralization: The underlying blockchain network will be designed to completely eliminate the dependence on the middleman, a completely independent decentralized architecture.



Security and stability: Stability includes two aspects: (1) Blockchain network transactions are stable and safe; (2) The economic system operates stably.



Scalability: The network can be extended according to service requirements, and the second layer network formed by the masternode servers are used to provide extended services

Privacy Protection: Secure and anonymous transactions for specific users and scenarios in a decentralized environment.

On this basis, gradually enriching and improving the traffic platform business will support:

1. The application based on masternodes: enabling masternode gradually supports (1) ad creative resources indexing storage, (2) cross-chain, (3) traffic settlement gateway, and (4) fraud/fake traffic analysis, (5) as future AI-based semi-decentralized data analysis node for user portraits is being introduced.

2. Decentralized storage of assets: Supports cross-chain storage of creative resources for the IPFS and other decentralized file systems.

3. Middle layer support of the traffic engine: Decentralized RTB in a multi-platform, multi-advertising form.

4. Traffic Analysis Smart Contracts: Smart contract scripting and virtual machines designed specifically for decentralized behavioral queries for ad platforms.

5. High performance and low commission: Support faster transaction speed through cross-chain/ sidechain to facilitate on-chain support and statistics of traffic data.

The traffic business will be a process of gradual transformation into decentralization. In the initial stage of business, the digital advertising traffic platform will be mainly implemented in a centralized form to achieve the following objectives:

1. Distributed traffic platform architecture: support sufficient traffic

2. Automatic expansion: volume expansion of statistical analysis according to actual needs

3. Multi-advertising support: text link, banners, mobile ads, video ads, etc.

4. Multi-platform client SDK support: NPW wallet ads, JavaScript embedding, mobile SDK, HTML5 ads SDK and video ads SDK.

5. Coin payment: support NPW recharge and cash-in.

6. Anti-cheat algorithm: Large-scale algorithms guarantee the removal of false data.

4.2 Technical architecture

The overall technical architecture consists of three layers:

1. **Storage layer**: Supports the cross-chain storage of creative resources using the IPFS and other decentralized file systems;

2. **Network layer**: Implements blockchain network, including two-layer network (decentralized value transfer network and semi-centralized masternode network) and cross-chain/sidechain;

3. **Service layer**: Provides users with traffic services, including value transfer services, traffic transaction services, anti-fraud services, privacy protection services, and user portrait analysis services.

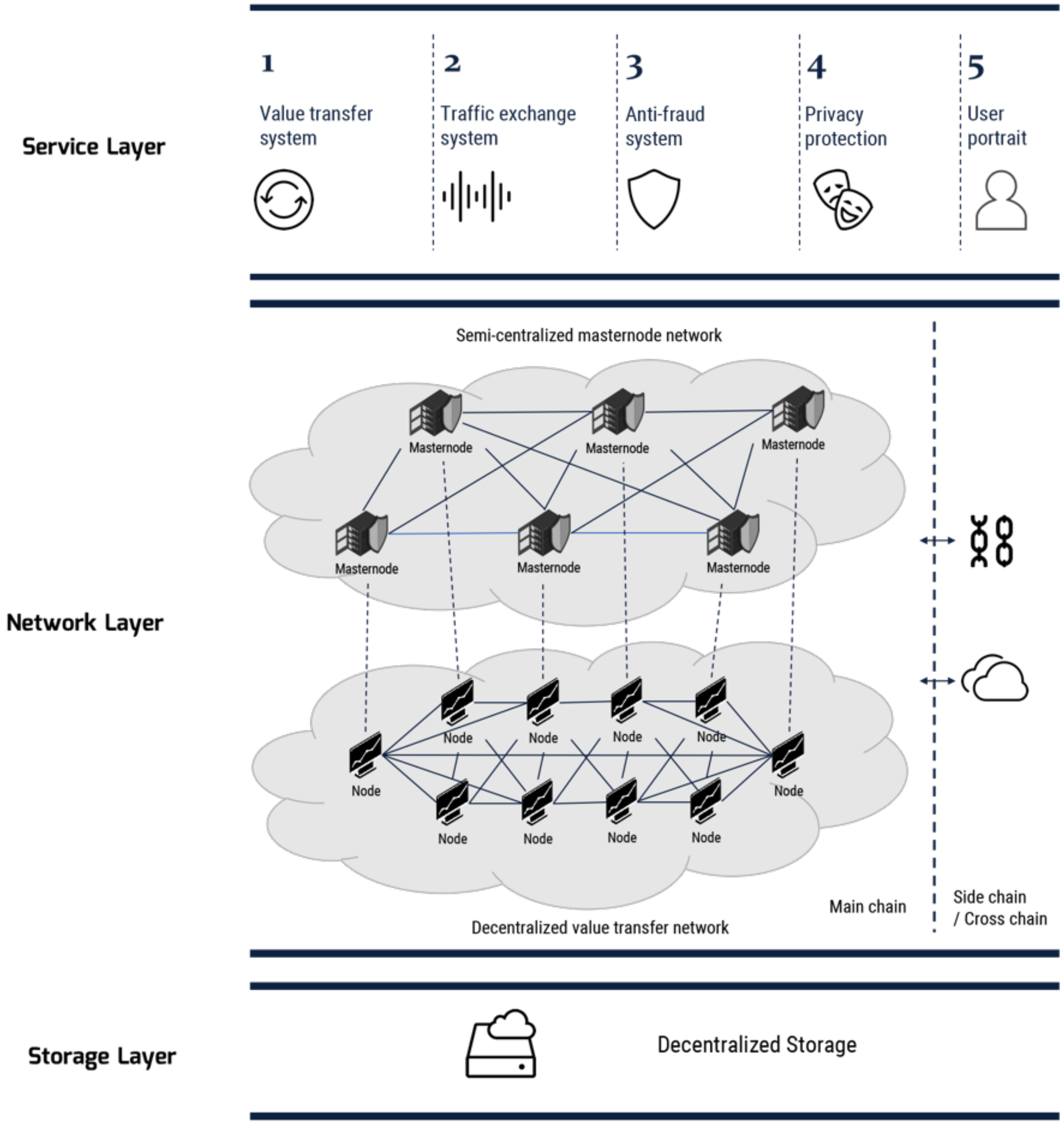


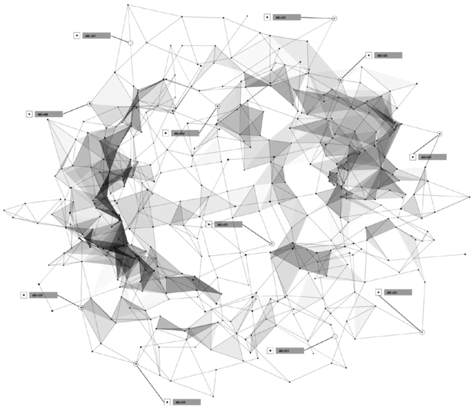
Fig. 2. Network Architecture

4.2.1 Decentralized value transfer network

The decentralized value transfer network is used to ensure the stability of the basic blockchain. It is necessary to increase the number of single nodes as much as possible to ensure the availability, stability and security of the network.

In order to ensure the stability of the main network in the early stage, the basic blockchain used the PoW consensus in the early stage, and from 0-3600 blocks, the rewards were set to 70% from the masternodes and 30% from the miners. In order to encourage more people to use the wallet, after 23,601 blocks, the main network automatically switches to the PoS consensus, rewarding 80% from masternodes and 20% from staking.

4.2.2 Semi-centralized masternode network



The masternode network is relatively stable, and the user needs to lock a certain amount of coins to establish a masternode server and can obtain masternode rewards. Provides essential underlying service support by leveraging a fixed IP address and stable masternode server. Holders of masternodes will get higher rewards.

The masternode network is equivalent to a small network compared with the underlying decentralized value transfer network. It also contains consensus and form a parallel two-layer network structure with the basic blockchain network.

The advantage of this architecture is that a small network composed of masternodes can be used to implement an extended function that is difficult to implement by the underlying decentralized network, thereby ensuring the operational efficiency of the network. Since the ad traffic service conducts intensive transactions, anti-cheating, and statistical analysis, an additional network layer is required to ensure stable operation of the service.

4.2.3 Value transfer service

As the entry point for users to interact with the blockchain network, the wallet provides the most basic value transfer service. The New Power Coin provides a full-featured QT Framework-based full-featured wallet in the early days. The wallet’s features include basic functions such as sending, receiving, zerocoin, transaction history, and masternode settings.

After the QT wallet is released, in order to achieve better scalability to provide more efficient expansion and development to meet business needs, the wallet is completely rebuilt and modified using Vue.js and Electron framework.

The new wallet will greatly improve the user experience by using Vue.js as a basic graphical interface. We’ve built a set of CSS framework for UI effects, and used Electron to support Mac, Windows and Linux.

On the one hand, the new wallet serves as a local node to increase the stability of the network. On the other hand, in the background, the API of the advertising platform is directly connected with the wallet, and the wallet will integrate advertising services.

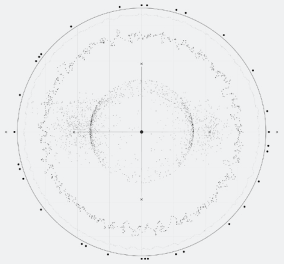
4.2.4 Traffic exchange service

Early traffic exchange services will run in a centralized form and used New Power Coin as an economic support. Subsequently, the entire platform will gradually migrate to be decentralized. At the same time, the traffic platform also integrates with masternodes for click verification, statistical analysis, and acquisition of advertising resources.

In the early stage, traffic platform will run as a centralized 'Demand Side Provider', to serve advertisers. In addition, the ad exchange service will provide ad display and ad platform login to the wallet.

4.3 Blockchain design

The core purpose of the basic blockchain is to ensure the true decentralized operation of the network. Through staking, the support function can be implemented by many traditional blockchain networks.



4.3.1 Consensus mechanism

The network uses a consensus mechanism called Proof-of-Stake (PoS). PoS originates from the Bitcointalk Forum as QuantumMechanic in 2011. The core idea is that "stake" is used to replace the "hash power" to reach a consensus. Compared with Proof-of-Work (PoW), PoS is more environmentally friendly, more decentralized, and more motivating.

From an algorithmic perspective, PoS have two major types: chain-based PoS and BFT-style PoS. In the chain-based PoS, the coin holders mine the new block through a process like PoW and append the new block to the end of the longest chain, such as Peercoin, Nxtcoin, Blackcoin, etc. In the BFT-style PoS, validators are randomly assigned the right to propose blocks, but agreeing on which block is canonical is done through a multi-round process, including Tendermint, Casper, Ouroboros, etc. At present, the BFT-style PoS is still in the theoretical construction stage, and there is still no fully developed implementation. Therefore, this project uses the chain-based PoS as the consensus mechanism for the underlying decentralized value transfer network.

4.3.1.1 Working principle

Assume that the block at the end of the longest chain is B*prev*, and the next new block B that needs to be mined will use B*prev* as its previous block. The coin holders will compete for the new block based on their unspent transaction (UTXO). If the block where the UTXO is located is B*from*, when the following conditions are met:

$$\text{hash}(B_{from}, UTXO, T, M) < V / D$$

Where T is the current timestamp, M is the stake modifier, V is the value of the current UTXO, D is the current mining difficulty, and hash is the SHA-256 function. The coin holder has mined the new block B, then broadcasts it to the whole network, and obtains corresponding economic incentives. The mining difficulty is adjusted with every new block. The adjustment method adopts the moving average correction method. Assume that the difficulty of the previous block is Dold, and the size of the interval range is N, and the theoretical block interval is TS, and the actual block interval is AS, then the adjusted difficulty D*new* is:

$$D_{new} = D_{old} * [(N+1)*TS] / [(N-1)*TS + 2*AS]$$

When the actual block interval AS is larger than the theoretical block interval TS, the difficulty is reduced after the adjustment; otherwise, the difficulty is increased.

The stake modifier is used to prevent a node from constructing a new block in advance as soon as the UTXO is acknowledged. When constructing a new block, the node must select a stake modifier for a specific time interval after the UTXO, to calculate a hash value. The stake modifier is recalculated at regular intervals. In the calculation, the block group is selected according to a certain rule, and a specific bit of the block hash is selected to construct a new stake modifier.

4.3.1.2 Initial distribution

After the main net reaches a stable state, a pure PoS consensus mechanism is adopted. In order to make the PoS run normally, the initial distribution of NPW is required in the whole network. We use the following methods to initially distribute NPW:

1. When the first block in the main net is mined, it will be distributed to the early investors according to the pre-sale of masternodes;
2. Distribute to the miners through PoW mining within about one month after the main net is online;
3. After the main net is online, NPW will be listed on several exchanges around the world, then users can obtain NPW through various ways.

At the block height of 1-23600, the NPW uses the PoW consensus mechanism. The mining algorithm uses NeoScrypt, that replaces SHA-256 with the BLAKE2 hash algorithm. A single NeoScript process will occupy approximately $s(N + 3) * r * 128$ bytes of memory. After the block height of 23600, only the PoS consensus mechanism will be used for mining blocks.

4.3.1.3 Security considerations

Nothing at stake

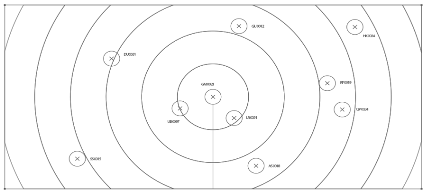
Nothing at stake means that when the blockchain forks, the node will create new blocks on each fork to guarantee the reward due to the lack of punishment. If a node wants to mine blocks at the same time on multiple forks, it will take a lot of time to modify the source code. In contrast, verification in the correct fork requires very little time. Moreover, the NPW held by the coin holder is the most stable incentive. If he continues to make a block on the wrong fork, he will face less incentives and a lower value for the coin. Therefore, there is in fact “something at stake”, and maintaining network stability is closely related to every coin holder.

Long range attacks

Long range attacks refer to: similar to 51% attacks, the attacker rewrites the blockchain by creating a longer chain. Long range attacks can start from blocks that were written at an early stage, or even start from the genesis block. In long-range attacks, if the attacker needs to start from an earlier height, this requires the attacker to get enough old private keys. At present, the sum of the NPW of the top 100 coin holders does not exceed 30% of the total supply. If an attack is launched, the attacker needs to collect private keys that hold more than 50% of the total supply at a certain point in time. At the same time, he also needs enough coins to make the collateral of the master node. Long-range attacks are only theoretically feasible and have great difficulty in the actual attack process.

4.3.2 Masternode network

One of the most important capabilities of the New Power Coin is building a Layer 2 masternode network to provide the traffic service based on the PoS-based decentralized value transmission network. In essence, the masternode is also a full node in the network, but it needs to stay online for a long time and provide additional services to obtain the corresponding incentives. Masternode can make the blockchain network running efficiently and stably.



4.3.2.1 Working principle

The masternode follows the Proof-of-Service protocol, and it gets rewards by providing services. Currently, masternode service requires locking 20,000 NPW in the wallet that can and will broadcast over the entire network. The masternode does not store any coin, and it uses the secondary private key signature to ensure the security of the locked coins instead. The masternode will prove that it is online by sending ping message every 5 minutes. The masternode broadcasts the list of all known masternodes in the network. Other nodes will synchronize all the masternodes and can use their services at any time.

In the masternode network, masternodes use voting arbitration to reach a consensus. Compared with the underlying network, the consensus formed by the masternode network has a higher priority. Since the number of masternodes are relatively stable and remain_ online for a long time, the masternode network can reach a consensus efficiently through voting arbitration.

In the case of instant transactions, traditional transactions typically require waiting for at least 6 blocks to confirm that the transaction is irreversible. But the masternode network can accelerate this process. Users can lock transactions across the network and send funds to specific addresses. When the transaction lock is sent to the masternode network, the masternode locks the input of the transaction and broadcasts the information to the entire network. It can ensure that the transaction is included in the subsequently mined block and does not allow it to be spent while waiting for confirmation.

After receiving the lock request, the masternode generates a lock transaction. By comparing the hash of the lock transaction with the hash of the request lock input, ten masternodes with farthest hash distance constitute the arbitration masternode group. As long as six nodes in this masternode group vote on their validity, the transaction input can be successfully locked. That is, as long as the selected masternode group reaches a consensus, the transaction is completed and has the highest priority. The confirmation time of the transaction is basically equal to the time when the transaction is broadcast to the entire network.

Compared with the consensus mechanism used by the underlying decentralized network, the masternode network provides a more efficient service through the arbitration voting of the masternode group, which greatly enhances the scalability of the underlying network.

4.3.2.2 Incentive system

The New Power Coin hopes to reward the masternode that provides service and utilizes the masternode's server to provide the traffic service at the same time.

By locking a certain amount of coins, the masternode keeps the stable operation of its own server, and the return is 80% of the block reward. It is equivalent to investing in a service similar to "mining machine" to obtain sustainable income. The masternode network ensures the healthy and stable development of the network, and to serve the business.

To run a masternode, 20,000 NPW must be locked in the wallet, and the rewards are issued through the new block. The revenue of a master node for the day is approximately:

$$(n/t) * r * b * a$$

Where n is the number of masternodes controlled by the wallet, t is the total number of masternodes, r is the current block reward (current block reward is 100 NPW), b is the average number of blocks per day (current daily mined blocks are 720), a is the average reward of the masternode (currently 80% of the reward for each block).

The entire network maintains a global list of masternodes. When the masternode is online for more than a certain period of time (about 20 hours), it will be added to the masternode's global queue. When the masternode moves to the end of the global list, other masternodes slowly migrate to the top of the list. Once a masternode reaches the top 10% of the global list, it is eligible to choose from the candidate pool.

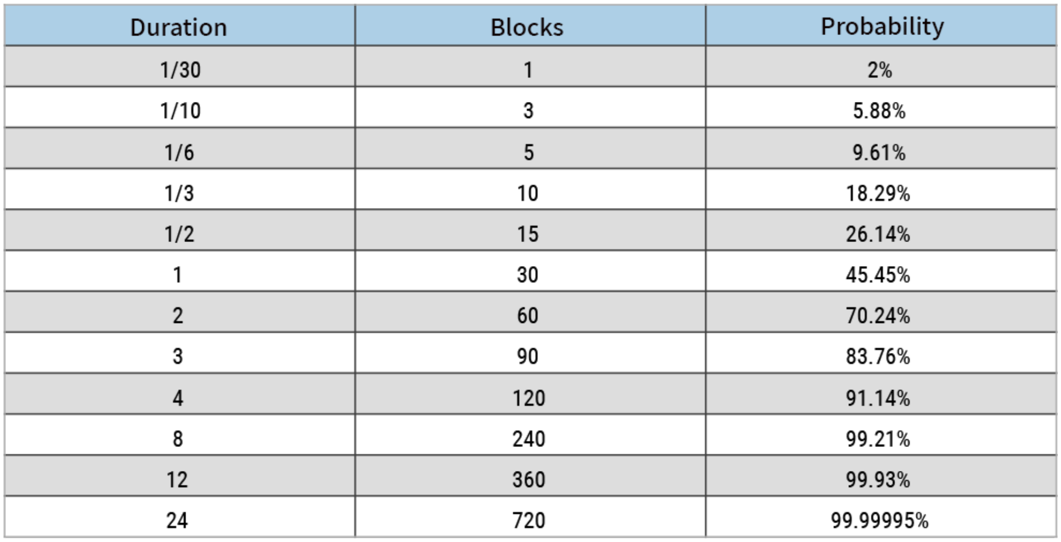
The candidate pool is the top 10% of the global queue. Its size is determined by the total number of masternodes. For example, if there are 450 active masters, the first 45 masters in the global list are available for selection.

Once in the candidate pool, the hash distance will determine which of the masternodes will receive the reward. The hashes of txid and n of the locked transactions of all the masternodes in the candidate pool are compared with the hash of the block that is 100 before the current height. The masternode with the largest hash distance is selected to obtain the reward.

The masternode in the candidate pool has a certain randomness in its choice, so it is impossible to predict when a reward will be awarded. Assuming a size 50 of the current candidate pool (ie a total of 500 masternodes), the probability that nodes in the candidate pool are randomly selected is 1/50.

The table below shows the probability that the masternode will be rewarded during a specific time period. For example, the probability of getting a reward within 12 hours is approximately 99.93%. However, the table does not tell us the probability of getting a reward after a given period of time.

For instance, if you own a masternode and you haven't been rewarded for 24 hours, according to the percentages, you are experiencing a streak of very bad luck. However, the probability of getting rewards in the next block will not increase, it will still be 1/50.



Duration	Blocks	Probability
1/30	1	2%
1/10	3	5.88%
1/6	5	9.61%
1/3	10	18.29%
1/2	15	26.14%
1	30	45.45%
2	60	70.24%
3	90	83.76%
4	120	91.14%
8	240	99.21%
12	360	99.93%
24	720	99.99995%

Fig. 3. Masternode rewards

4.3.2.3 Deployment

In order to make the deployment of the master node easier, we provide an easy-to-use one-click deployment script for the masternode, which allows most people to setup a masternode by simply running the script in the server. The masternode deployment script now only supports a single node deployment. As the script is updated, it will gradually support the automatic startup and automatic update of services.

Each masternode will appear in the global list, and its location in the global list is related to the time when it was last awarded. The new masternode joining the network and the masternode that has been rewarded are placed at the end of the list. The master node can be activated via the wallet interface or using the RPC command:

`masternode start` or `masternode start-alias`

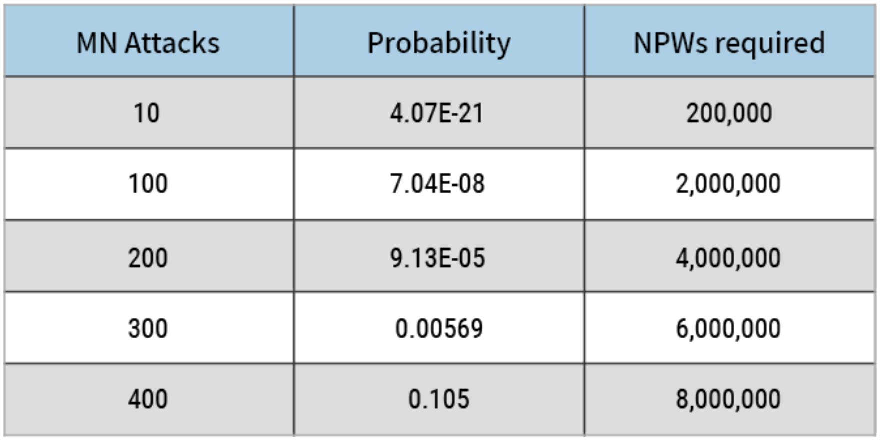
If the masternode that is already running is reactivated, the masternode will be placed at the end of the global list. This can be avoided via the wallet interface or the RPC command:

```
masternode start-missing
```

4.3.2.4 Security considerations

Sybil attack

Assume that the masternode network has a total of N masternodes, the probability of each masternode being selected into the masternode group is 1/N when voting arbitration is performed. When all masternodes in the group are controlled by the attacker, the attacker can attack the masternode network. Assume that the number of masternodes in the network is 500. Under the condition that different number of primary nodes are controlled, the probability of a successful attack by the attacker is:



MN Attacks	Probability	NPWs required
10	4.07E-21	200,000
100	7.04E-08	2,000,000
200	9.13E-05	4,000,000
300	0.00569	6,000,000
400	0.105	8,000,000

Fig. 4. Attack probability

The cost per masternode is 20000 NPW, and the cost of trying attack the masternode network is high. If you want to attack successfully with a probability of about 5.69‰, you need to control about 60% masternodes in the network, which means that you need to purchase 6 million NPW. Considering the limited supply of NPW (about 13 million at the time of writing) and the low liquidity in the market, it is very difficult to implement such an attack.

Finney attack

In a Finney attack, when an attacker successfully finds a block, the block contains a transaction that will be sent to the attacker. Instead of broadcasting the block, he sends a transaction to the merchant to get the goods or services. After the product or service is generated, the attacker immediately broadcasts the previously mined block to achieve a double-spend before the next block is generated by the network.

To prevent Finney attacks, the network must be able to reject blocks that violate the consensus of the masternode, and must be able to distinguish whether a given transaction is successfully locked through the masternode network's consensus system. Only when the selected masternode group broadcasts the message of successful locking, other nodes of the network will consider the locking successful and reject all the blocks that conflict with it.

Race attack

The attacker simultaneously submits two conflicting requests to the masternode network. He submits one request to the specific master node to spoof the receiver, and broadcasts another request to the network to retrieve its own coins. In such an attack, the masternode network will temporarily fork, but will soon reach consensus. The masternode network will only keep one valid transaction, and all nodes on the network will delete invalid transactions and transfer valid transactions to its memory pool.

In another case, when the masternode network does not form a final consensus, due to data loss or the masternode going offline, the client's request will reach a consensus through the underlying network.

4.3.3 Privacy mechanism

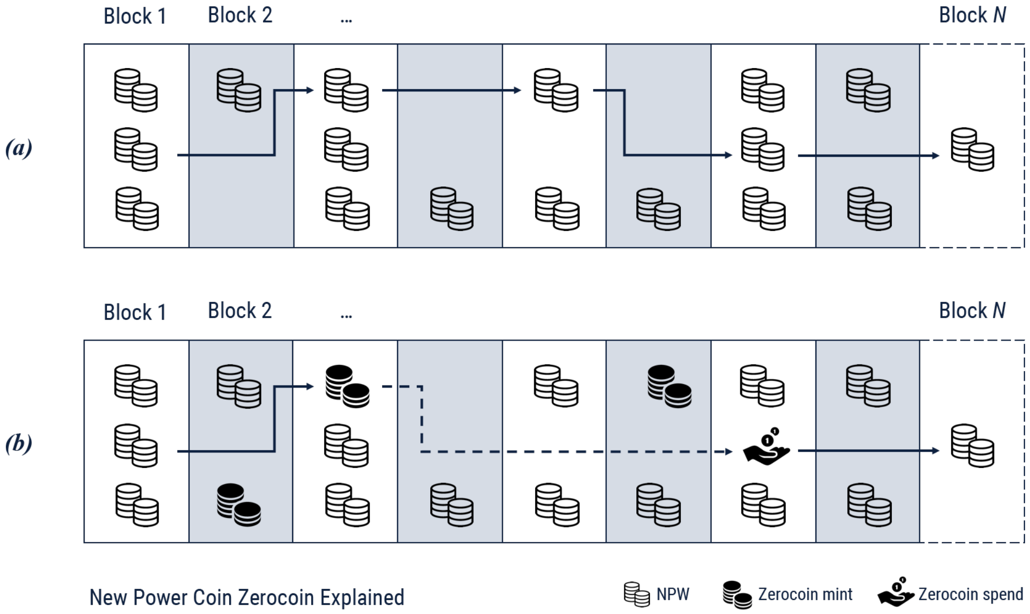
We believe that in the future of traffic services, user privacy is the most important thing to be focused on and guaranteed. The privacy mechanism is the basis for protecting the privacy of users in future traffic transactions, and an important part of the underlying capabilities of the New Power Coin.

4.3.3.1 Working principle

For traditional cryptocurrency transactions, the sender, recipient, and amount for each transaction will be recorded on the blockchain. This poses a great challenge to the user's privacy protection. The address can be associated with the user's real identity through various information on the network and interaction records with the real world. In a private transaction, the sender's association with the recipient should be cut off, making the transaction anonymous.

The New Power Coin uses zerocoin protocol to achieve private transactions based on zero-knowledge proof. Zero-knowledge proof means that the prover (verified person) can convince the verifier that a certain assertion is correct without providing any useful information to the verifier. A zero-knowledge proof is essentially an agreement involving two or more parties, or a series of steps required by two or more parties to complete a task.

In our implementation, the private transaction involves mint process and spend process, in order to hide the relationship between the sender and the receive r of the transaction. Through the zerocoin mint process, the user can convert the NPW into zero coin zNPW into the zerocoin pool. The zerocoin exists in a variety of fixed denominations. Concerning the zerocoin spending process, the user can spend his zerocoins in the zerocoin pool. With the certificate of the corresponding quantity of zerocoins, the zerocoin can be taken out from the zerocoin pool, but the zerocoin does not carry any user address information at all.



This figure shows a schematic diagram of the transaction process based on the UTXO model using the zero-coin protocol. In sub-graph (a), each transaction is associated with the previous transaction, and the association is publicly recorded on the blockchain; in sub-graph (b), there is no one-to-one correspondence between the coin obtained and the coin spent which cuts off the possibility of tracking the source of zerocoins.

When verifying the proof of spending zerocoin, it is needed to ensure that the same zerocoin is not doubled. The node uses the zero-knowledge proof when verifying the transaction, and does not need to know which zerocoin is actually spent. It only needs to verify whether the spend proof has been spent before.

If the coin is spent immediately after the coin is minted, there is a chance that the mint and the spend will be correlated by performing a timing attack. In order to prevent timing attacks, there is a certain time interval between zerocoin mint and spend. At present, the newly minted coin can be spent at least three same denominations of zerocoins are minted.

4.3.3.2 How to use

When users use the zerocoin for private transactions, they first mint zerocoin according to their own needs, and wait for the zerocoins' maturity before sending them to the recipient. In the example shown in the figure below, User 1 needs to send 125NPW anonymously to User 2. User 1 converts the ordinary NPW into zNPW by zerocoin minting, and obtains zerocoins of one 100, two 10 and one 5 respectively. After the minted zerocoins are matured, User 1 sends them to User 2, then completes the entire private transaction process.

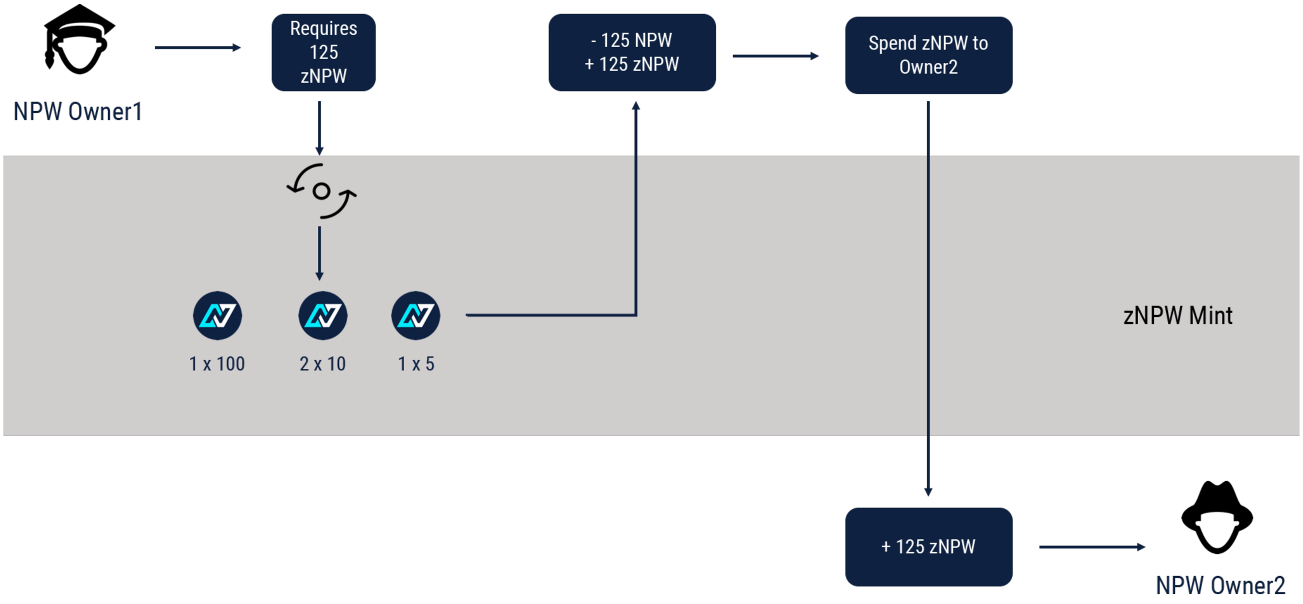


Fig. 6. Anonymous Transaction

In the New Power Coin network, the advertisement transaction can protect the user's privacy through anonymous transactions, thereby hiding the user's transaction record and advertisement access record.

In the process of making user portraits, we will also use the homomorphic encryption algorithm to ensure that the user's private data is computable but invisible. Through anonymization, we can conduct a qualitative analysis of any advertising operation behavior of the user, without affecting the privacy of the user at all. Our network will implement the privacy protection capability in a mathematical manner.

4.4 Traffic platform design

Because of the decentralized stability and the convenience of the masternode network, NPW is no longer limited to the speed of confirmation of traditional blockchains and can guarantee security. Therefore, we will first establish an advertising platform and eventually transition to a decentralized traffic engine.

4.4.1 Business planning

We will gradually build decentralized traffic engine in six phases:

In the first phase, the advertising platform will use NPW as the base currency for traffic purchases and transactions. The advantage of this is that it is instant, self-service, and more efficient without the need for a bank or third-party recharge platform.

The second phase, the masternode server will provide distributed storage indexing of ad resources and migrate to IPFS or other distributed storage resources in the future.

In the third phase, all traceable data will be stored on the blockchain, encrypted and saved, and will serve as the basis for subsequent data analysis.

The fourth phase, provides decentralized user image computing capabilities through cross-chain/ sidechain.

The fifth stage, provide user image query capabilities through smart contracts. Advertisers can precisely match the user community of the demand.

The sixth phase, decentralized customization of personalized matching content, while preserving user privacy.

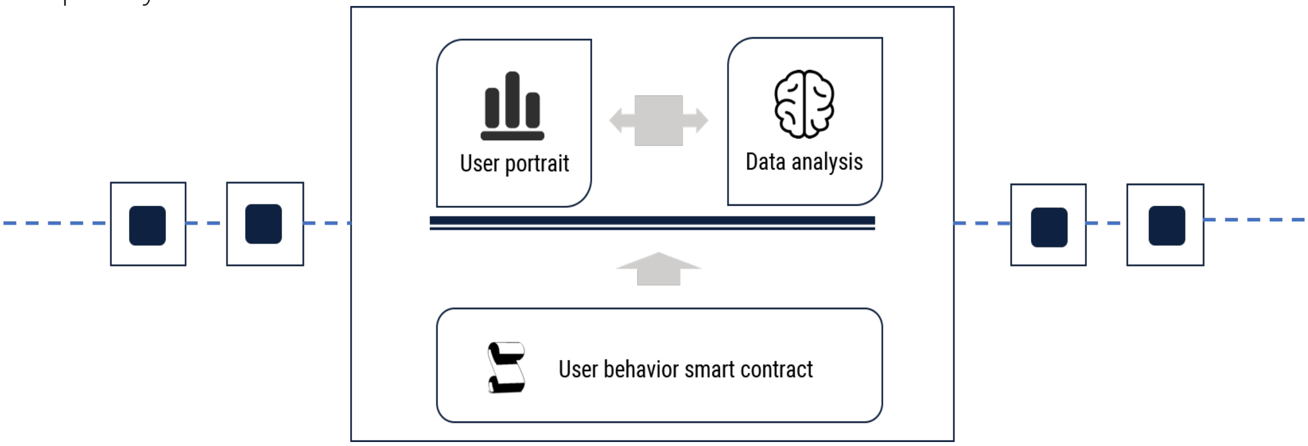


Fig.7. Onchain user portrait

4.4.2 Business logic

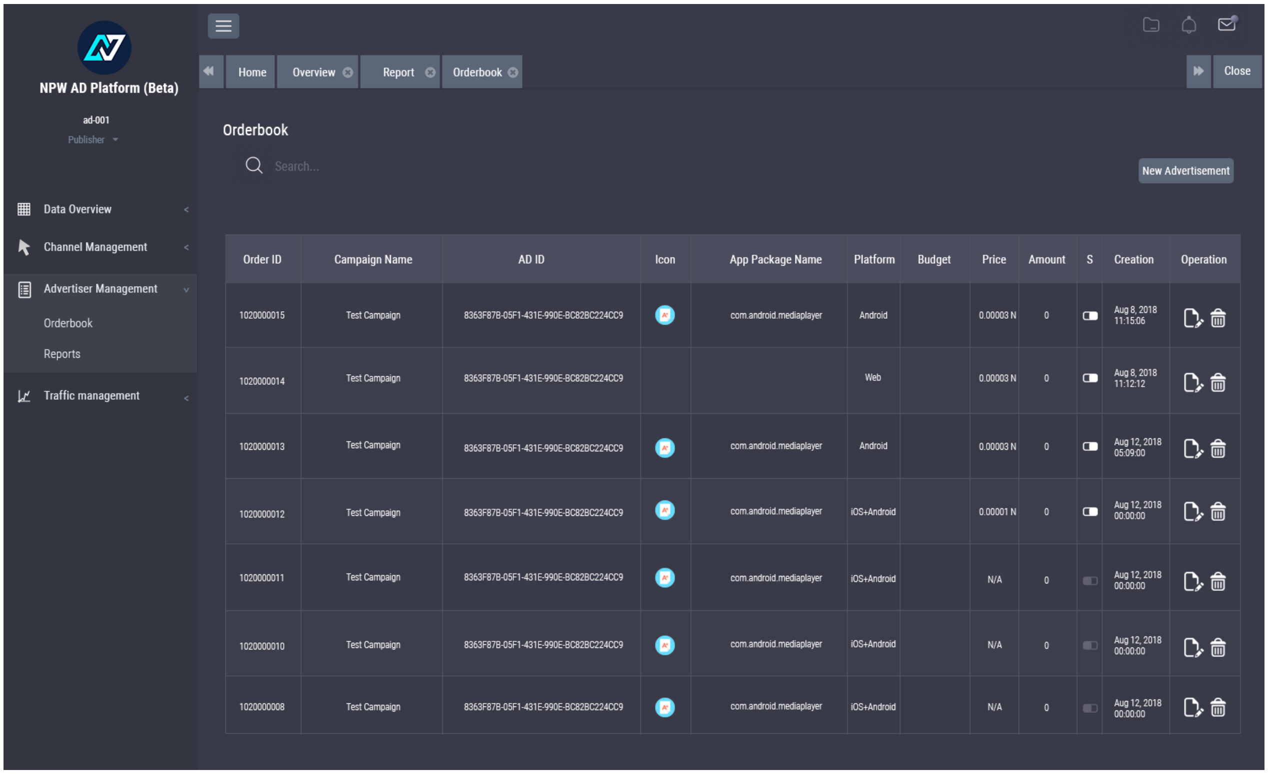
4.4.2.1 Advertising platform

We have developed an early advertising platform that serves as a base platform for applications and as a demonstration of the underlying traffic engine in the future, enabling a variety of the most basic advertising platform features.

The advertising platform supports account registration, advertiser recharge, ad serving, publisher code and SDK acquisition, billing, and wallet ad interface.

All settlements in the advertising backend are based entirely on the blockchain. The functionality of all the underlying chains in the backend of the ad services, the extensions of the masternode, and ad exchange functions will all be developed based on the blockchain of the new power coin.

After the user registers with the advertising platform, the account will automatically create a new power coin wallet locally on the advertising platform server. The wallet and the account are stored separately, and the user's advertising transaction will be stored in the wallet. At the same time, the important click behavior will also be stored on-chain, and the advertising platform provides an operation interface, interacting with the blockchain nodes. The blockchain operation interface implements the advertisement delivery module, the advertisement management module, the anti-cheat module, the billing module, and the settlement module to maintain and manage the entire delivery period of the advertisement. Ads will be displayed through blockchain node interface. The transaction is fast, stable and resistant to cheat.



Orderbook

Order ID	Campaign Name	AD ID	Icon	App Package Name	Platform	Budget	Price	Amount	S	Creation	Operation
1020000015	Test Campaign	8363F87B-05F1-431E-990E-BC82BC224CC9		com.android.mediaplayer	Android		0.00003 N	0		Aug 8, 2018 11:15:06	
1020000014	Test Campaign	8363F87B-05F1-431E-990E-BC82BC224CC9			Web		0.00003 N	0		Aug 8, 2018 11:12:12	
1020000013	Test Campaign	8363F87B-05F1-431E-990E-BC82BC224CC9		com.android.mediaplayer	Android		0.00003 N	0		Aug 12, 2018 05:09:00	
1020000012	Test Campaign	8363F87B-05F1-431E-990E-BC82BC224CC9		com.android.mediaplayer	iOS+Android		0.00001 N	0		Aug 12, 2018 00:00:00	
1020000011	Test Campaign	8363F87B-05F1-431E-990E-BC82BC224CC9		com.android.mediaplayer	iOS+Android		N/A	0		Aug 12, 2018 00:00:00	
1020000010	Test Campaign	8363F87B-05F1-431E-990E-BC82BC224CC9		com.android.mediaplayer	iOS+Android		N/A	0		Aug 12, 2018 00:00:00	
1020000008	Test Campaign	8363F87B-05F1-431E-990E-BC82BC224CC9		com.android.mediaplayer	iOS+Android		N/A	0		Aug 12, 2018 00:00:00	

Fig.8. Ad network

4.4.2.2 Charges

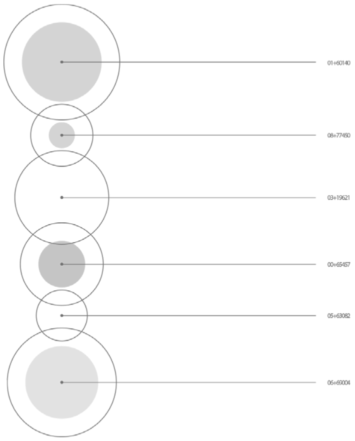
According to different roles, the advertising platform provides different charging strategies.

For advertisers, the system requires the use of NPW to recharge and then consume, the system provides two ways to consume:

> *1. Fixed quota consumption: When setting the advertising campaign, specify the daily consumption of the advertising amount.*
>
> *2. Budget quota consumption: Specify the total budget, the system will customize the fill rate and delivery ratio to achieve the optimal delivery effect.*

Advertiser: Recharge uses NPW, similar to the form of digital currency exchange, the coins directly pass into the NPW recharge address of the traffic exchange platform. The consumption of the advertisement directly uses the NPW balance from the platform wallet, and automatically stops the advertisement from being served and notifies the advertiser after the balance is consumed.

Publisher: By logging into the platform to get the ad code or SDK, the publisher can earn NPW directly by displaying ads on their websites/apps. The advertising platform supports automatic settlement reconciliation every hour, and the settled coins will automatically enter the publisher's wallet and can be withdrawn at any time.



Wallet users: We have designed a new form of advertising that provides advertising services for users who use the wallet for PoS rewards. When the user runs the wallet for staking rewards, he or she can choose whether to display the advertisement provided by the advertisement platform. If the user allows the advertisement to display, the advertisement will automatically send the user's wallet a certain amount of NPW rewards.

The overall settlement of the advertising platform is handled using the blockchain network of NPW, with strict security measures. The charging section provides a risk control module that absolutely guarantees the coin security of large advertisers and traffic owners.

The advertiser and the traffic master's account use cold wallet, and the module docks to the settlement center of the advertising platform to prevent the risk of the private key being stolen. Through multiple certificate signatures to ensure the security and stability of the final settlement.

4.4.2.3 User wallet

In the early stage, New Power Coin provided a Bitcoin QT-based wallet client for functions such as sending, receiving, zerocoin, and masternode settings.

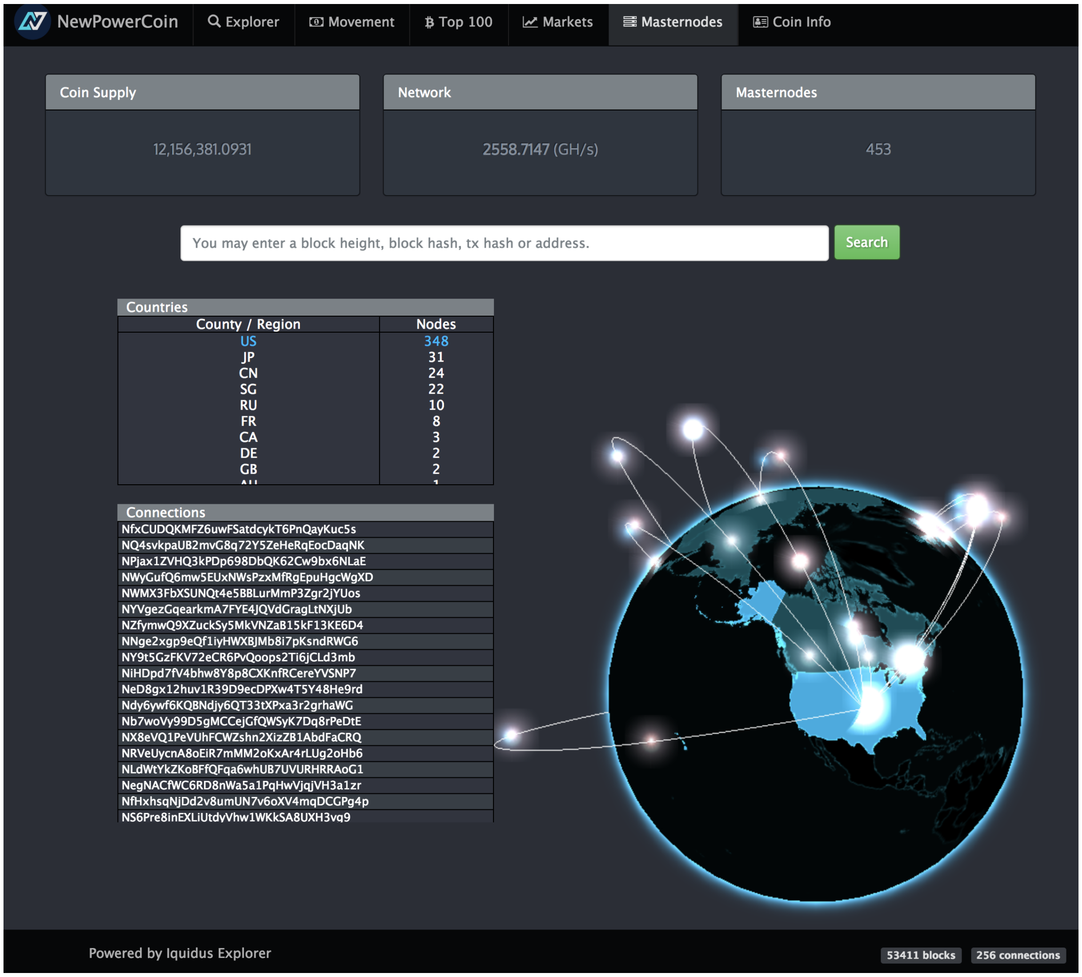
The core wallet is used to provide the basic capabilities of NPW blockchain in the early days. The basic wallet based on a command line client. The settings of the masternode service also depend on the NPW rpc program to provide the overall service to the masternode network. The basic wallet uses port 61472 for communication.

PoS requires users to run the wallet software for rewards, which is also implemented through the core functions of the basic wallet.

Block Explorer

A complete block explorer is built into the wallet to query complete information on all blockchains. The functions of the block explorer include indexing, querying, and viewing transaction details. All transactions will be fully recorded on chain for inquiries and cannot be tampered with.

Anyone can build their own NPW block explorer. As an example, the developer provides a block explorer that can query the masternode network.



Coin Supply: 12,156,381.0931

Network: 2558.7147 (GH/s)

Masternodes: 453

Countries

County / Region	Nodes
US	348
JP	31
CN	24
SG	22
RU	10
FR	8
CA	3
DE	2
GB	2
AU	1

Connections

```
NfxCUDQKMFZ6uwFSatdcykT6PnQayKuc5s
NQ4svkpaUB2mvG8q72Y5ZeHeRqEocDaqNK
NPjax1ZVHQ3kPDp698DbQK62Cw9bx6NLaE
NWyGufQ6mw5EUxNWsPzxMfRgEpuHgcWgXD
NWMX3FbXSUNQt4e5BBLurMmP3Zgr2jYUos
NYVgezGqearkmA7FYE4JQVdGragLtNXjUb
NZfymwQ9XZuckSy5MkVNZaB15kF13KE6D4
NNge2xgp9eQf1iyHWXBJMb8i7pKsndRWG6
NY9t5GzFKV72eCR6PvQoops2Ti6jCLd3mb
NiHDpd7fV4bhw8Y8p8CXKnfRCereYVSNP7
NeD8gx12huv1R39D9ecDPXw4T5Y48He9rd
Ndy6ywf6KQBNdjy6QT33tXPxa3r2grhaWG
Nb7woVy99D5gMCCejGfQWSyK7Dq8rPeDtE
NX8eVQ1PeVUhFCWZshn2XizZB1AbdFaCRQ
NRVeUycnA8oEiR7mMM2oKxAr4rLUg2oHb6
NLdWtYkZKoBFfQFqa6whUB7UVURHRRAoG1
NegNACfWC6RD8nWa5a1PqHwVjqjVH3a1zr
NfHxhsqNjDd2v8umUN7v6oXV4mqDCGPg4p
NS6Pre8inEXLiUtdyVhw1WKkSA8UXH3vq9
```

Powered by Iquidus Explorer

53411 blocks 256 connections

Fig.9. Block explorer

The best way to achieve ad service is to have enough decentralized nodes. Each node can serve as both a service provider for the blockchain and a recipient of the service. This ultimate mode is the shape of the final traffic engine we expect to achieve.

To meet the design needs of this stage, the existing QT-based wallet is difficult to meet the future development needs. So we rewrote the NPW wallet as the bottom layer of the future blockchain traffic engine.

Easy of use

We observed that the vast majority of current blockchain users have insufficient knowledge of programming for this kind of operation. This is being reflected in the low numbers of active cryptocurrency users. (That is why current active cryptocurrency user is not a large number.) Most cryptocurrency application are just technical demos. Therefore, we hope that all users can use our wallet, as both a PoS client and an advertising end-client, benefitting all networks as a whole.

For this reason, our first step was redesigned a new interface based on CSS3, and designed the wallet software based on this interface.

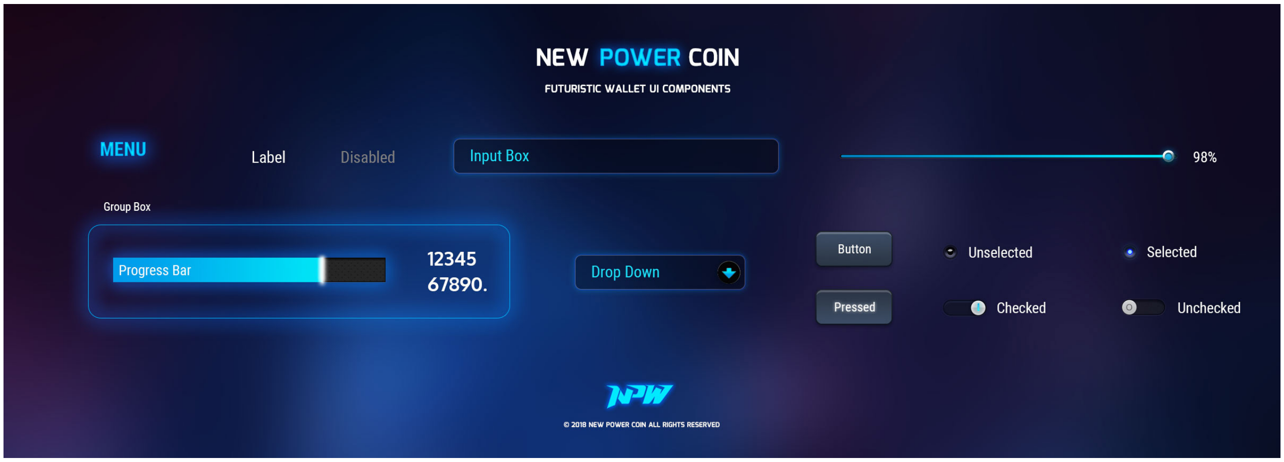


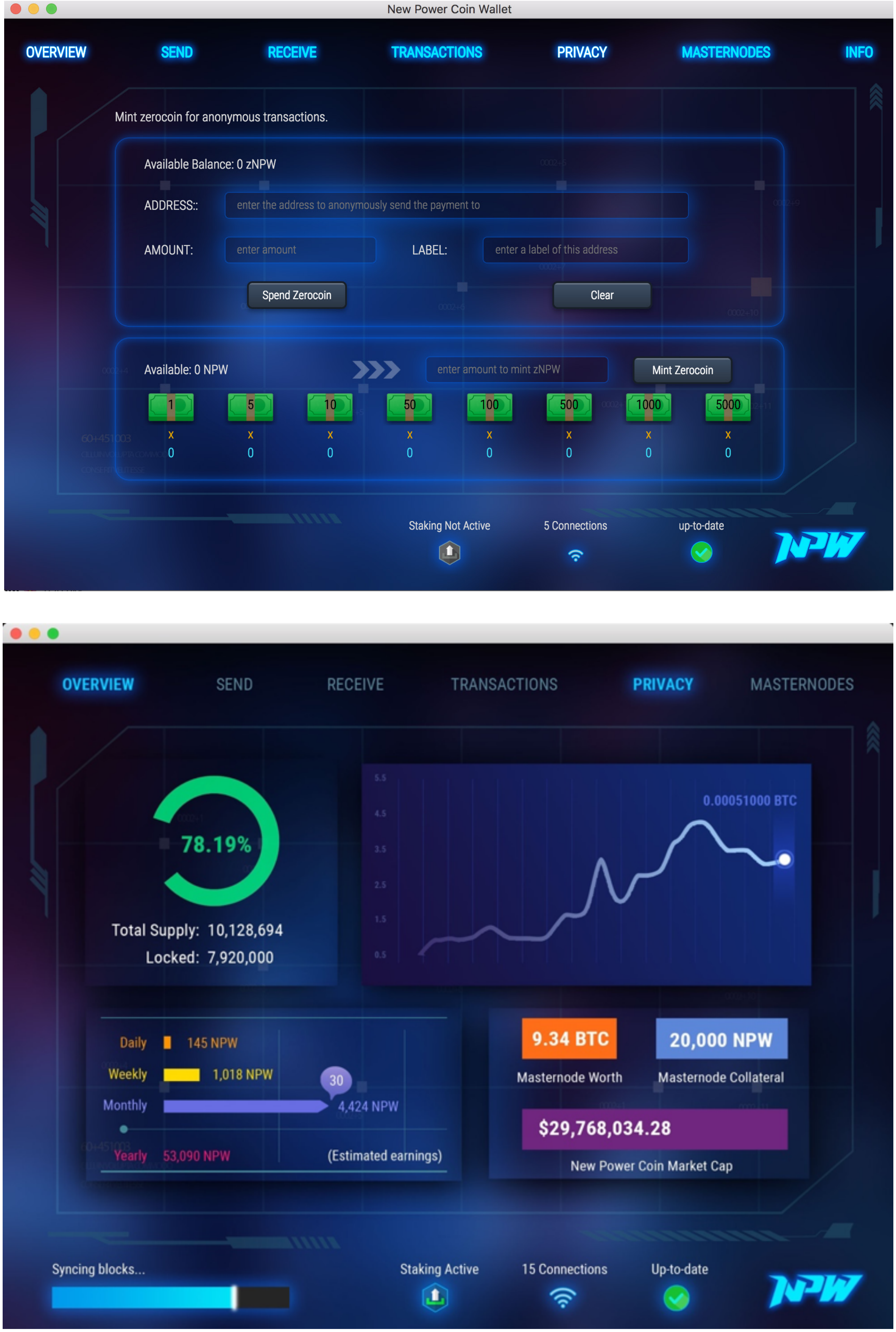
Fig.10. Wallet UI framework

The wallet uses Vue.js as the basic framework to turn all development into front-end development work. With the gradual upgrading of the NPW network, development work will become easier and maintenance can soon be kept to a minimum.

We also use the Electron framework to truly guarantee cross-platform capabilities and scalability.

Vue.js

Electron



Mint zerocoin for anonymous transactions.

Available Balance: 0 zNPW

ADDRESS:: enter the address to anonymously send the payment to

AMOUNT: enter amount LABEL: enter a label of this address

Available: 0 NPW enter amount to mint zNPW

1	5	10	50	100	500	1000	5000
x	x	x	x	x	x	x	x
0	0	0	0	0	0	0	0

Staking Not Active 5 Connections up-to-date

Total Supply: 10,128,694

Locked: 7,920,000

Daily 145 NPW

Weekly 1,018 NPW

Monthly 4,424 NPW

Yearly 53,090 NPW

(Estimated earnings)

9.34 BTC Masternode Worth

20,000 NPW Masternode Collateral

$29,768,034.28 New Power Coin Market Cap

Syncing blocks...

Staking Active 15 Connections Up-to-date

Fig.11. NPW new wallet preview

Scalability

The first expansion capability we implemented in the wallet is an advertising display framework. The back-end provides the blockchain billing through a PoS pool built by the advertising platform. The front-end users can run the wallet for PoS to see the advertisement and obtain the advertising service rewards, which will automatically send them to the user's wallet account address.

The advertising platform management system will also be embedded in the wallet. Both the advertiser and publisher can directly use the private key in the wallet to perform the basic functions of the single-point login, payment, transfer and other traffic services of the advertising platform.

The development of the advertising traffic engine to the ultimate form will no longer have a centralized platform, the wallet is the platform, and the platform is the wallet. Platform features are placed in the wallet for management and execution. Under this premise, due to the decentralized service, the blockchain network does not need to consider the indicators such as advertising concurrency and load balancing and can only be developed as an extended front-end capability.

4.4.2.4 Multi-platform advertising support

The platform supports multiple operating systems and multiple types of advertising formats.

Form of advertising

Scripts support for the ad:
Text link: an advertisement form formed by a URL jump by writing a text link of different content;
Banner ads: advertisements that are usually composed of different sizes of images/dynamic images;
Pop-up ads: web ads that pop up automatically;
Interactive advertising: interactive advertising designed using HTML5 or Flash technology;
Video placement ads: Ad insertions made before/after the video.

Will support:
Audio advertising for Alexa and other voice assistants;
Advertising in the form of a cross-chain blockchain.

Business form

The business forms of advertising include:
CPC: Cost Per Click, charges by click;
CPM: Cost Per Impression is charged according to the amount of impression;
CPA: billing according to user behavior (registration, viewing, etc.);
Point consumption: an advertisement that guides the user's consumption behavior and rewards points;
Community group advertising: community and discussion group promotion;
Word of mouth marketing advertising: bringing new users to growth through recommended methods;
Task-based advertising: An advertisement that can receive rewards after completing a specified task.

Advertising service industry and platform

Digital advertising not only benefits the traditional Internet, but also benefits more industries.

The industries and platforms of the service include:
Traditional Internet;
Mobile internet;

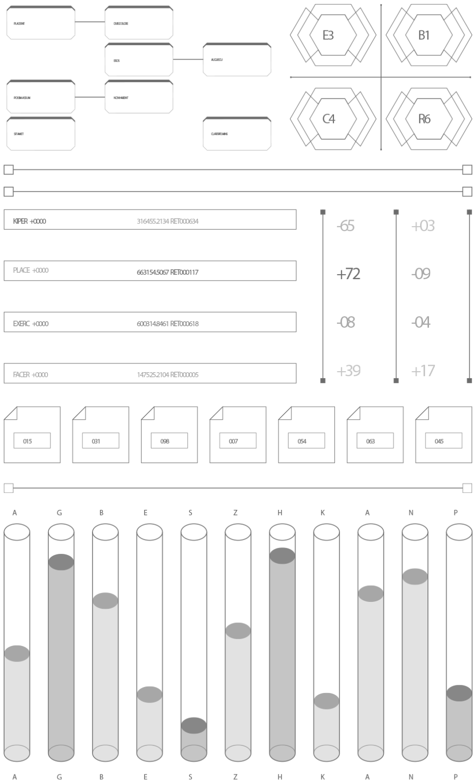
Mobile HTML5 and mini games, Instant Games.

The future will also include:
Blockchain community;
AI, B2C products;
Internet of Things products, wearable and smart home appliances;
Automatic driving.

4.4.2.5 Anti-cheating protection

A more important pain point of internet advertising is that it is very easy to cheat. Traditional large platforms require extremely high human and financial resources for anti-cheating management. The NPW advertising platform handles cheating management in two parts, one is the traditional anti-cheating process, and the other is based on the anti-cheating process of the blockchain wallet.

Anti-cheating of traditional advertising: The traditional way of preventing traffic clashes, usually by limiting the frequency of requests and the number of requests, is limited to a fixed value for a single source. At the same time, the ad is tracked from an impression, click, behavior, etc. through an encrypted fingerprint. If there is no fingerprint or the fingerprint data is incorrect, or the frequency of the advertisement request is too large, the source IP address and the user's behavior identifier are exceeded, and the abnormal traffic is determined. When the log is finally settled, the abnormal traffic will be rejected. This type of click behavior can also be marked by big data machine learning to achieve a large-scale reduction in the rate of cheating.



Anti-cheating of blockchain wallet advertising: the wallet provides uniqueness verification through the encrypted signature, the advertising reward is combined with the wallet's own node binding, and the advertisement is displayed and clicked by the signature to verify that the wallet is displaying the advertisement, then it is considered a legal transaction.

4.4.3 Business Architecture

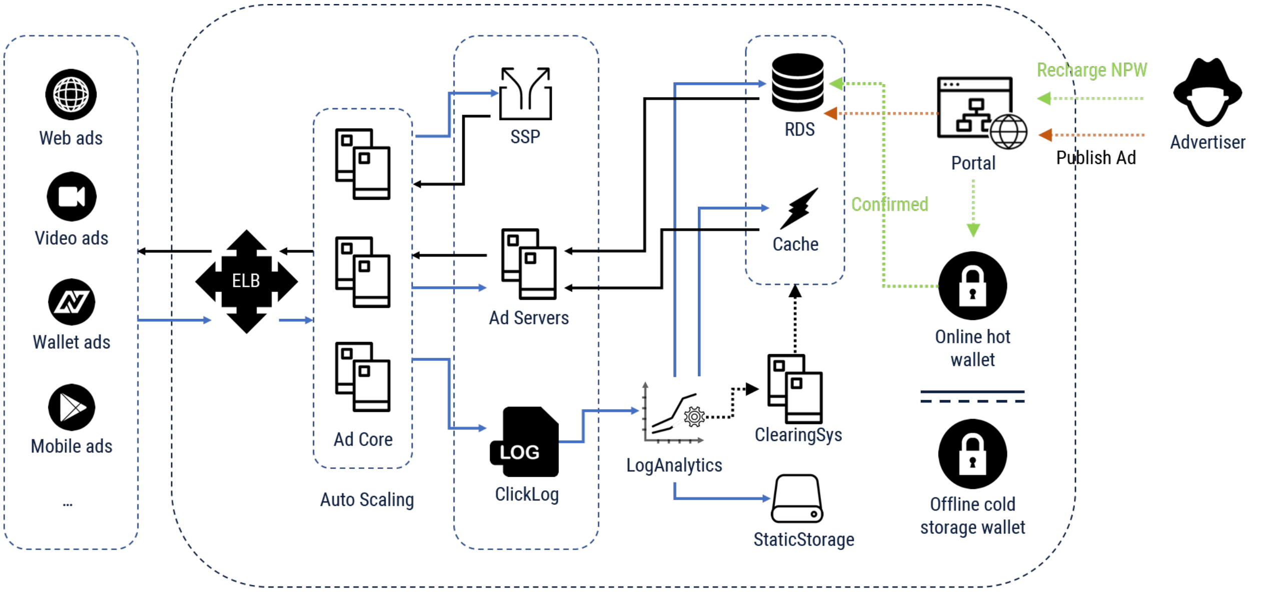


Fig.12. Ad network business architecture

This picture shows the technical architecture of the advertising platform, the content will be explained step by step.

The advertising traffic platform system supports the service of the advertisement traffic application by attaching to the underlying base chain and a single masternode.

By setting up a secure and complete advertising platform, we support multiple advertisers, publishers and systems with large click-through support. The back-end of NPW's main chain serves as the blockchain's settlement support. The advertising platform supports the blockchain part: recharge, settlement, transaction and so on. Similar to a centralized cryptocurrency exchange, the advertising traffic service we will launch in the early stage is also a centralized service.

4.4.3.1 Advertising core system

As the core of the advertising platform, through the underlying blockchain network, the reliability of the nodes and the security of the value transfer are guaranteed, and an incentive mechanism for advertising and display is implemented, rewarding ad display requests and clicks by each node. The reward is sent directly to the node's default wallet address through the settlement module, so that the transaction will be transparent and traceable.

Advertising management module: Using nodes to manage the release of wallet advertisements, including pre-release of advertisements and advertising on-chain display. Anyone can download the wallet to publish their ads.

Ad serving module: Authorizing, matching, targeting and optimizing ad request from wallet nodes. Ensure the legitimacy of the source of the ad request and the verification of the click on the ad.

Anti-cheat module: It is mainly for the detection of the ad serving behavior of the wallet node bypassing or spoofing the delivery module. Punishing the unqualified ad request behavior, and limiting the frequency of the abnormal traffic or reducing the revenue.

Billing module: Billing for CPM and CPC advertising, avoiding excessive or insufficient delivery, and finally charging according to the policy of advertising.

Clearing module: The module that rewards the wallet node. Mainly for the publisher's traffic consumption and the advertiser advertising consumption module for the publisher reward mechanism.

For the traffic platform, the NPW blockchain can be used as a decentralized database. The main role of this advertising service is its data storage function, which stores the most basic settlement data through the blockchain. Both the advertisers and the publishers can perform a series of data query through the interface provided by the system, including display status, click status, user behavior, statistical analysis, settlement, and anti-cheat. The interfaces include socket and HTTP, and developers can also perform quantitative analysis through GraphQL.

In the early stage, all the advertising settlements will be written into the blockchain through the basic chain, to ensure that the advertising revenue settlement is transparent and cannot be tempered with. In the future, through the cross-chain/sidechain method, all display and click data will be gradually analyzed through decentralized distributed storage.

4.4.3.2 Masternode system

The further development of masternodes will be gradual. The current masternode capability only provides two aspects of fast transaction and privacy. The advertising platform itself will gradually carry out a series of expansion and transformation for the mastersnodes.

Since the advertising platform itself is an exchange of self-driven and self-contained loop, the traffic is accepted through NPW, and the structure of the advertising platform itself is inseparable from the blockchain of NPW.

The RPC API in the wallet is mainly used to communicate with advertiser to publish their ads, and for publishers to get rewards. The RPC API consists of an ad management module (AdManagerMod), an ad request module (ImpMod), an ad-click module (ClickMod), an anti-cheating module (AntiCheatingMod), and an RPC authorization module (RPCAuthMod).

Advertising management module: Provides RPC interface for advertisement publishing, advertisement acquisition, advertisement consumption, etc. The advertiser logs in to the Dashboard platform to call the RPC to publish its own advertisement, obtain the consumption data of the advertisement, and the information of the historical advertisement.

Ad request module: RPC API that mainly provides the ad request, obtains the delivery information of the ad core module through the traffic master, and displays the returned ad data in the media to obtain the reward.

Ad click module: Generates a cheat verification algorithm by acquiring the user's ad click behavior and the ad display environment, and forwards the user click behavior to the masternode for verification, and records the user behavior.

Anti-cheat module: A module for cleaning and limiting abnormal traffic. It tracks and fingerprints the advertisements delivered by the wallet nodes to prevent malicious traffic from flowing into the advertising kernel.

4.4.3.3 Advertising management system

The advertising management system has two parts: advertiser management and publisher management. Since the advertising platform uses NPW for settlement, the advertiser must recharge NPW to use the advertising platform for advertising. NPW can be purchased from exchanges or OTC platforms.

Advertiser platform management: mainly provides information inquiry such as advertisement delivery, advertisement delivery history query, and advertisement delivery consumption;

Publisher platform management: mainly provides traffic main traffic consumption, traffic revenue, and payment record query.

4.4.4 Extensions

4.4.4.1 Load balancing

The initial design of the platform is more than one billion transactions per day. It can support various types of ad display, click, video playback, and user behavior advertisements such as installing applications, as well as future expansion of video, smart speakers, and car-based advertising formats. The main pressure of load balancing is from request logs.

Centralized high concurrency scheme

Access layer solution: In the early stage, the access layer connects to the desktop client and SDK through ELB (Elastic load balancing) for advertising. The ad core supports scalable capabilities through stateless design to increase ad serving capacity and high concurrent traffic. This can easily and quickly expand to increase the accessibility of the advertising platform.

Ad serving core solution: The ad core uses an efficient rule matching engine that quickly locates targeted ads, increasing ad conversion rates and traffic revenue.

Data processing layer solution: The log processing engine uses a distributed memory real-time analysis engine combined with a multidimensional analysis data model, easily handle billions of behavioral data, it uses machine learning to quickly identify anomalous logs and restore real traffic and revenue to users.

Decentralized high concurrency scheme

Since decentralized advertising is done through smart contracts, the smart contract runs in memory, which naturally guarantees the performance of the single node for advertising. By expanding the number of masternodes, it can expand infinitely in parallel to support high concurrent access to the advertising platform.

4.4.4.2 Masternode extension

Many of the underlying mechanisms of the traffic engine require various types of extensions for masternodes. Privacy transactions and instant transactions are just a basic case for providing services to masternodes. Based on the ad traffic platform, the expansion plan for the function of the masternode server includes:

1. Decentralized CDN storage and cross-chain IPFS digital creative file index support;
2. Statistical analysis and anti-cheating ad click verification;
3. User data privacy protection
4. User tag and user portrait;
5. Large-scale advertising statistics compression analysis
6. Remote random check of SDK and ad script

These capabilities will gradually expand with the construction of the traffic engine platform. The goal is to gradually build a decentralized traffic engine through the advertising platform.

4.4.4.3 User portrait and privacy protection

In order to accurately deliver advertisements, it is necessary to have user portrait capabilities and label setting capabilities.

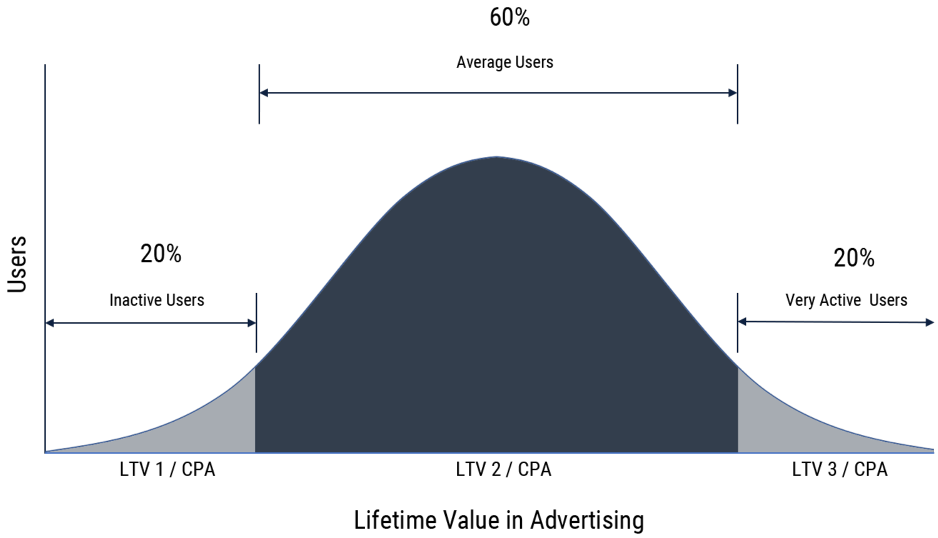


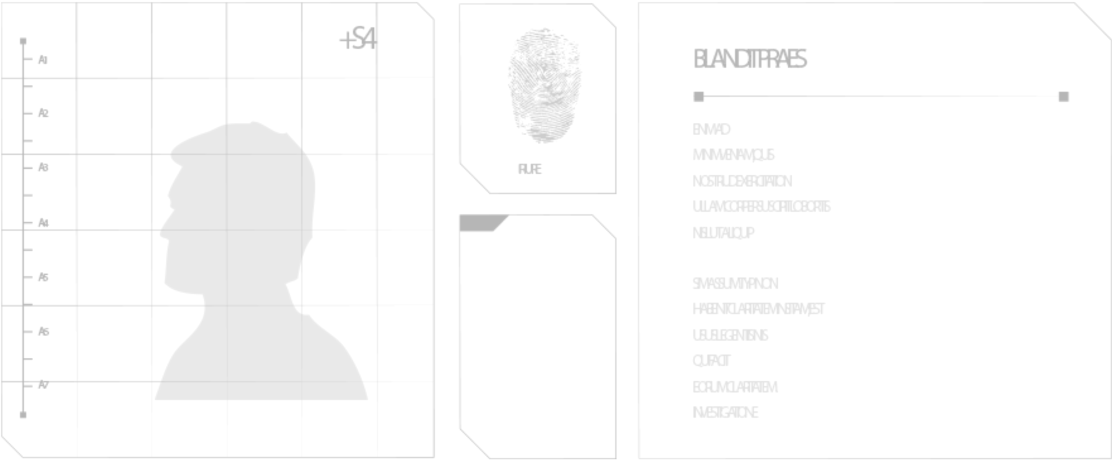
Fig.13. LTV in advertising

LTV analysis is displayed by tags in the advertising platform. Advertisers can choose the user’s age, gender, location, preferences and other details in the process of delivery to achieve accurate results. With LTV, we can understand the true value of users and maximize the value of users. The users benefit by being able to get the exact goods and services they require.

For traditional advertising services, the biggest criticism of LTV-based delivery is that there is no protection for user privacy. In the process of enjoying accurate advertising, the most worrying thing is that their personal information is through little effort acquired by third-party companies.

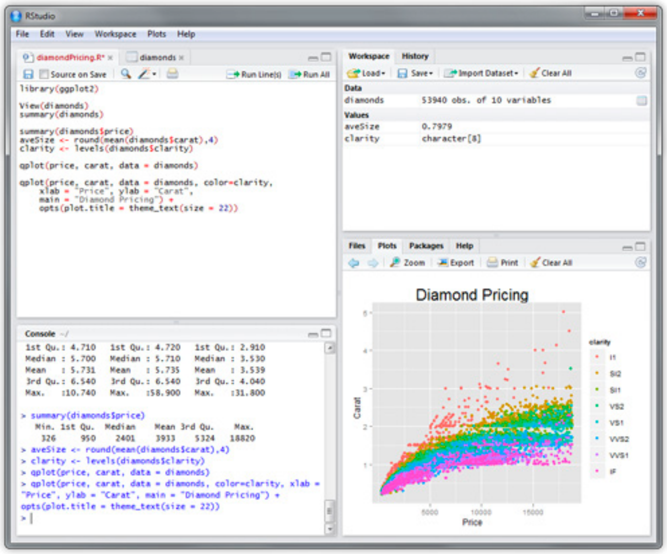
Based on the NPW masternode service, the advertising platform can maximize the analysis of the user’s portrait through the transformation of the masternode, and at the same time, it is possible to ensure that the user’s private data is not controlled by any third party.

For example: Using the principle of zerocoin, the similar browsing behaviors of different users are simultaneous inputs into the masternodes, and the different outputs are returned after being mixed by the masternode service, so that no one can know the true indication of the user at the same time. Zero-knowledge proof allows users to enjoy accurate service, while third-party advertisers maximize the revenue, the user’s data is not owned by any third-party company.



4.4.4.4 Smart contract based on traffic engine

As the underlying engine of the traffic service, it is not only necessary to provide services in terms of advertising traffic support, but also to provide automatic settlement capabilities. NPW will provide a smart contract scripting engine based on ad traffic statistics, user portrait queries, and big data analytics. The scripting mechanism is similar to the R language and is used to perform user analysis and precise matching on the chain.



```
library(ggplot2)

View(diamonds)
summary(diamonds)

summary(diamonds$price)
aveSize <- round(mean(diamonds$carat),4)
clarity <- levels(diamonds$clarity)

qplot(price, carat, data = diamonds)

qplot(price, carat, data = diamonds, color=clarity,
    xlab = "Price", ylab = "Carat",
    main = "Diamond Pricing") +
    opts(plot.title = theme_text(size = 22))
```

```
Data
diamonds        53940 obs. of 10 variables
Values
aveSize         0.7979
clarity         character[8]
```

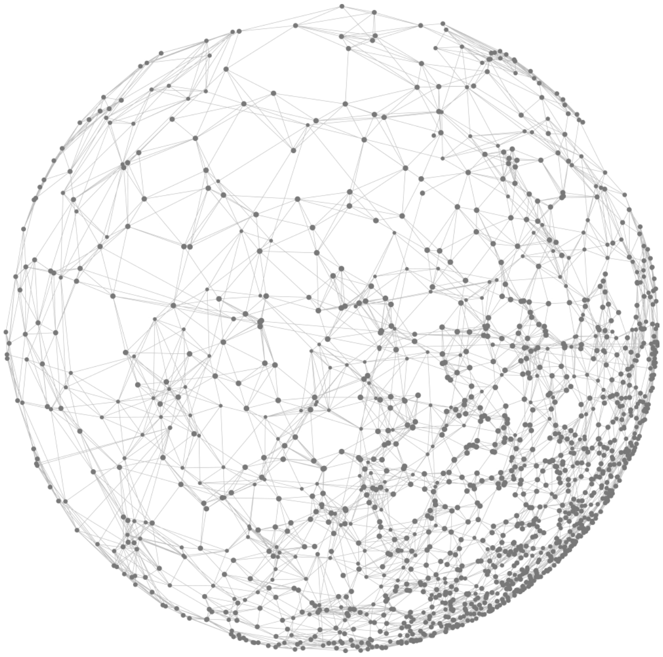
```
 1st Qu.: 4.710   1st Qu.: 4.720   1st Qu.: 2.910
 Median : 5.700   Median : 5.710   Median : 3.530
 Mean   : 5.731   Mean   : 5.735   Mean   : 3.539
 3rd Qu.: 6.540   3rd Qu.: 6.540   3rd Qu.: 4.040
 Max.   :10.740   Max.   :58.900   Max.   :31.800

> summary(diamonds$price)
   Min. 1st Qu.  Median    Mean 3rd Qu.    Max.
    326     950    2401    3933    5324   18820
> aveSize <- round(mean(diamonds$carat),4)
> clarity <- levels(diamonds$clarity)
> qplot(price, carat, data = diamonds)
> qplot(price, carat, data = diamonds, color=clarity, xlab =
"Price", ylab = "Carat", main = "Diamond Pricing") +
opts(plot.title = theme_text(size = 22))
> |
```

Fig.14. RStudio-like smart contract editor (planning)

4.4.4.5 Business globalization

In the early stage, we tried to cut through and improve the advertising business through small-scale marketing trials, and gradually cut into every corner of the world.



V. Economics

We do not recognize the way of tokens today. They are not decentralized economic settings, but the ownership of all rules and warrants still belongs to a centralized system. Therefore, in order to finally construct a decentralized network, we must take the main chain online first, as the basis for the overall implementation.

5.1 Economic design principle

Prior to the release of this white paper, NPW's main network had been launched in advance, running a stable and safe phase, and smoothly passed the initial stage of PoW and entered the PoS phase.

In order to achieve the ultimate goal of decentralized advertising under the premise of improving user experience, economic design is essential.

As we all know, the volatility of digital currency can sometimes be quite serious, because masternode has a strong lock capacity, which is very important to maintain the stability of an NPW price.

At the same time, it is also necessary to consider that with the development of technology, the total value of digital currency will increase greatly.

We hope to consider the development of the Internet as a whole in the process of economic design and achieve the following characteristics:

Self-growth capability of the traffic platform

Business diversity

Multi-participant autonomy and consensus

Coexist with the underlying technology to enhance development

Increase the overall value of the economic closed loop

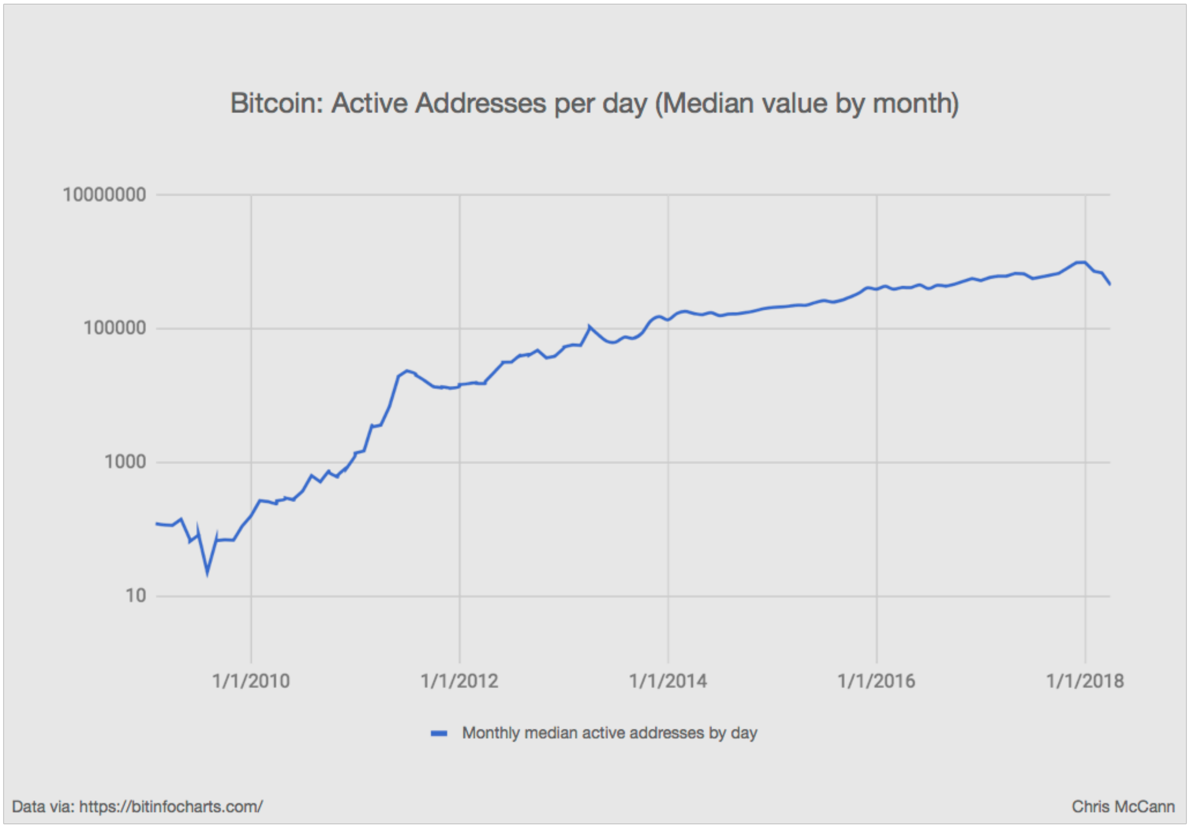


Fig.15. Bitcoin Active Addresses © 2018 Chris McCaan

The above is the growth curve of Bitcoin active users. We can see that users have increased rapidly in the more than one year, shortly after the start of the Bitcoin main network, while the second to fourth years are still in a period of rapid growth, followed by a decline in growth rate. Most well-known blockchain projects have a similar phenomenon, while bitcoin production is fixed at half every four years, that is, its inflation setting is not synchronized with it's respective user growth. Such a setting will cause user who were there from the beginning to expect too much revenue and thus raising their reluctance to sell, leading to deflation, being "over-hyped", by capital, and then once the bubble bursts, the price falls into a state of collapse.

Even the most market-recognized and stable bitcoin, the movement of the Dax or Dow Jones fond are in no comparison to the fluctuations of Bitcoin. This is not conducive to maintaining the stable operation of the overall economic system, and cannot make the cryptocurrency truly effective. Therefore, we came up with our very own economic setting, explained further below.

5.2 Basic economic setting

All NPWs are mined, and the total supply of NPW in four years is about 73 million. The total supply after ten years is about 100 million. The figure below is a predicted line chart of NPW output.

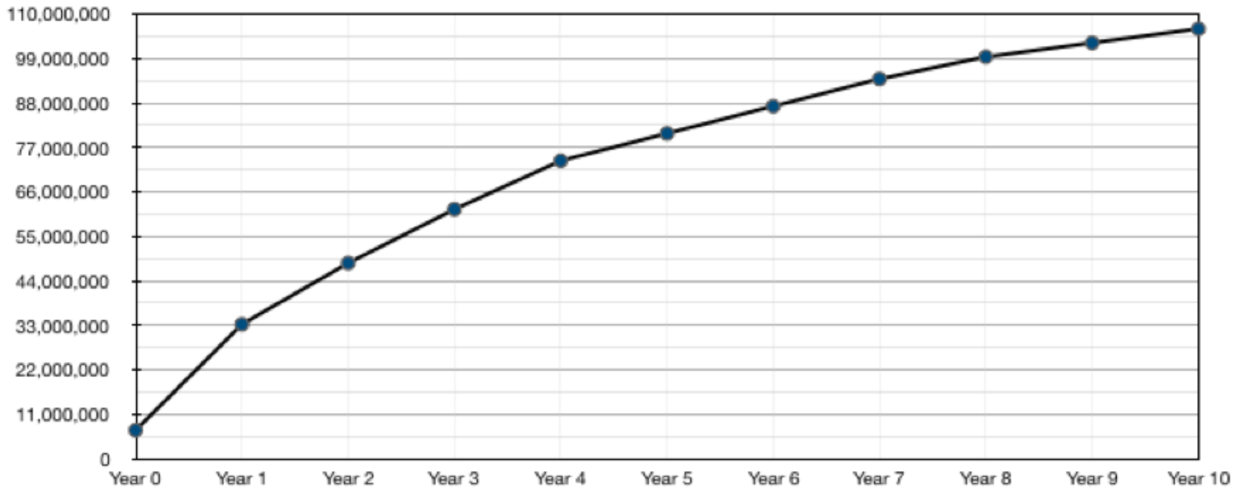


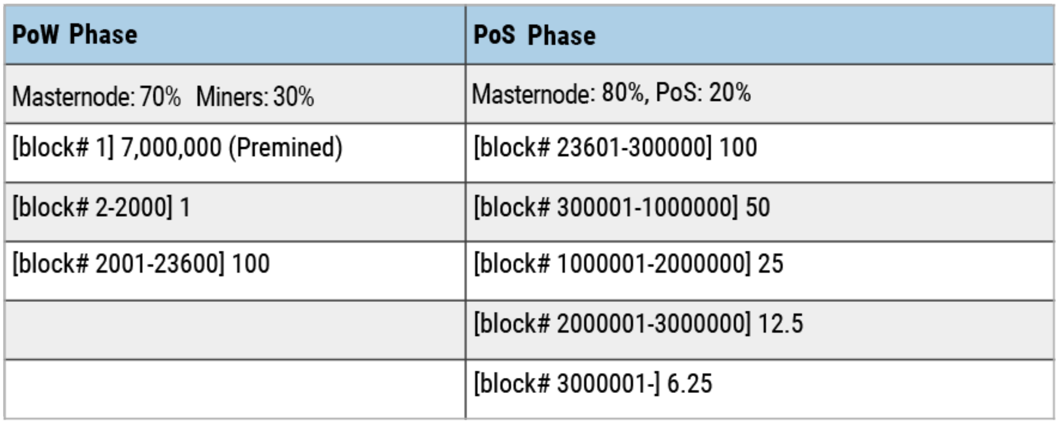
Fig.16. NPW supply prediction

The output of NPW is divided into two stages. The PoW stage is based on the mining stage, and the initial coins are mined through this stage.

The block time of NPW is 2 minutes and the block size is 2M.

Each masternode requires 20,000 NPW Collateral.

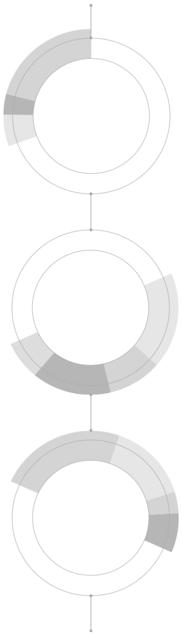
5.3 Block rewards



PoW Phase	PoS Phase
Masternode: 70% Miners: 30%	Masternode: 80%, PoS: 20%
[block# 1] 7,000,000 (Premined)	[block# 23601-300000] 100
[block# 2-2000] 1	[block# 300001-1000000] 50
[block# 2001-23600] 100	[block# 1000001-2000000] 25
	[block# 2000001-3000000] 12.5
	[block# 3000001-] 6.25

Fig.17. NPW block rewards

5.4 Acquisition and consumption



Unlike the ERC20 Token, all NPWs are real application coins rather than securities tokens. In the economic system of the NPW advertising platform, digital currency is obtained through mining and staking, and NPW can be fairly obtained by anyone. All the coins are used for advertising publishing.

In the NPW advertising traffic platform, the NPW is consumed by recharging and advertising. The consumed coins will be offered to the publisher as a reward to re-enter the economic cycle.

When the NPW infrastructure is set up, as the basic traffic engine, NPW will serve as the underlying base cryptocurrency and enter multiple ad platforms for circulation and consumption.

VI. Roadmap

6.1 Business roadmap

6.1.1 Different stages of advertising traffic

Addressing for the eight-year forecast of NPW's overall development, although each stage has its very own challenges, the most difficult part will be the zero-to-one part. A digital currency without real business, although it can portray a beautiful and great prospect when it is announced, will experience difficulties obtaining enough value without a core business.

Since the beginning of the Internet, we believe that the most explicit business model is mainly digital advertising and the online game industry, and advertising traffic is more basic and more versatile than games.

As the business foundation of NPW, we believe that strategically and decentralized advertising is very solid and reliable, and achievable.

6.1.2 Planning for each phase

Business introduction period planning
In the business development phase, the initial business lead-in period is expected to take about 8-10 months, starting with the addition of a small number of participants, KOLs, and enthusiasts.

Therefore, the business plan for the first year includes:
The first three months: from some of the most basic advertising traffic exchange business test, the business model mainly explores the coin->traffic / traffic->coin interchange model. This premise is that NPW already has a certain exchange value. So, we started with the setup of the masternode, which made the NPW have the basic needs in the early stages. Producing actual demand produces a certain value and has the ability to exchange.

Lead-in period: At the same time as the core advertising business tries to start gradually, it is necessary to work not only in the advertising business itself, but also in the product experience of digital currency.

Due to the poor experience of most digital currencies, the difficulty of accepting ordinary users, and the large threshold for many technical work. Therefore, before making the business widespread, we rethink the NPW product experience through the transformation of the wallet. Therefore, enhancing the product experience through the following improvements is also an important task in the lead-in period:

1. Wallet experience optimization and rewriting
2. Cross-platform wallet and light wallet
3. Masternode one-click deployment

At the time the white paper was first written, the above work was basically completed as planned.

The NPW network has a foundation for continuous and stable development, once it has a widely used wallet and an easy-to-deploy masternode server.

Advertisers in the lead-in period not only cover traditional Internet customers (their advertising will not differ from traditional Internet ad serving), but also cover some of the advertisers of blockchain projects from the cryptocurrency community, because these people are more active. As a result, advertisers in blockchain projects can experience more efficient ad serving than traditional traffic sources.

At the same time, due to the strong suppression of cryptocurrencies by the giants, Google and Facebook have introduced a policy of prohibiting cryptocurrency advertisements, and also increased the traffic demand of blockchain advertisers.

Business trial period

The main task of the business trial period is to develop the basic business of advertising and platform construction.

During the business lead-in period, the ad delivery attempt only supports a relatively simple lightweight user interface, and we will develop it into a decentralized platform during the business trial period. The platform form supports both page access through the website and direct ad serving within the wallet, so it’s important to get more wallet users. So we will begin to gradually support the advertising exchange platform at this stage. Since NPW has been listed in some small exchanges, it is also easier to develop more users who have demand for traffic or revenue.

At this stage, the most basic traffic exchange advertising platform will be developed, and various advertising formats and industries will be supported. We will also add a variety of features by extending the wallet, such as:

- Advertising in the wallet
- Commission charged in the wallet
- Advertising self-service in the wallet
- Project development progress query in the wallet

Business transition period

After two to three years of business consolidation, the platform’s actual transaction flow has gradually reached a certain scale. Because no one really “owns” this platform, it means that everyone “owns” a share of the platform, so the platform will be very competitive at this stage, and it is possible to reach or surpass ordinary small-scale advertising companies.

At the same time, during this period, due to the participation of the global NPW community in development and project progress, the business has basically covered most of the mainstream markets. The main work at this stage requires a higher level of optimization of the main chain based on the existing business foundation. At the same time, as the industry becomes more mature, and by that time many of the basic tasks will have become standard procedure in the industry, and development and improvement will be even easier.

Optimization work at this stage includes:

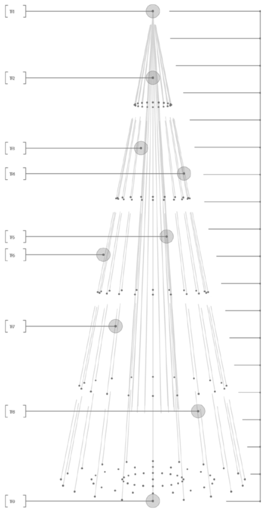
- Higher speed consensus / side chain extension
- Advertising engine-specific delivery smart contract
- Try to work with third-party ad exchanges for RTB
- The algorithm guarantees the user's click behavior and the on-chain privacy of subsequent operation behavior.

Business expansion period

At this stage, the NPW platform has become a more advanced decentralized advertising platform, cutting into the global market and supporting a variety of new advertising businesses.

At this stage, the Internet and technology will usher in a new wave of opportunities, including the Internet of Things, AI, home robots, autonomous driving and the use of new energy sources will gradually enter people's lives. The NPW platform's traffic support capability, at this stage, will be sufficient to span these new business forms, supporting traffic output with more media forms, stronger interactivity, and more scenarios.

Since a sufficient amount of user traffic data has been analyzed during the business transition period, the platform initially has the ability to accurately match the user's portraits. At this stage, we will develop a user portrait engine and selectively open it to third parties for collaborative trials. The analytical computing power of the user's portrait will also be decentralized and analyzed at this time.



At this time, the platform has floated on the Internet like Bitcoin, and is not "owned" by anyone. All users manage the platform in an autonomous manner.

Business growth period

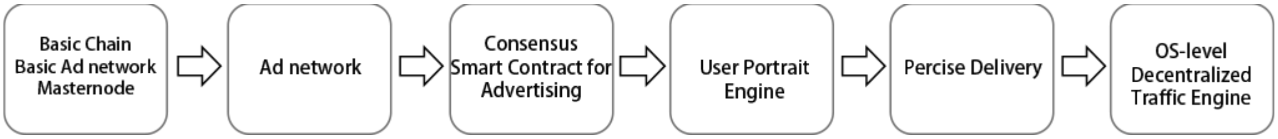
At this stage, the NPW platform has become a traffic platform that no one in the world can ignore, and can affect the top platforms such as Google, Facebook, and Amazon. At this stage, NPW will have the opportunity to support its exchange capabilities without relying on any exchanges, "traffic is as assets".

At this stage, the platform will develop a sense of social responsibility in the process of user autonomy, in order to protect everyone's right to privacy and the right to access services to coexist. It also supports parallel expansion in the form of cross-chain, whether based on IPFS or other storage technologies in the future, or the ability to connect with other main chains.

Business prosperous period

At this time, the development of NPW has gone through the above stages to enter the most prosperous period, becoming a truly decentralized global traffic infrastructure engine, supporting traffic exchange capabilities, serving everyone on the planet, allowing them to obtain any information more quickly. At the same time, user privacy can be free from intrusion. For businesses that need to be promoted, they can use the self-programming method to accurately find the user group that they want to serve on this engine. The entire platform is a self-governing management system for advertisers, advertisement recipients, and all others. There are no owners or managers, and all systems continue to operate through a self-consistent and fair rule.

6.2 R&D roadmap



In terms of technology development, the development roadmap will follow these steps:

1st part:

- The basic chain part: NPW blockchain core development
- Basic advertising network
- Traffic score system, mobile and PC Internet traffic purchase, wallet built-in advertising and other functions
- Blockchain network: including local wallet, masternode service, etc.

Subsequent functional extensions and user experience optimization, including:

- Product experience optimization for light wallets, mobile wallets, etc.
- One-click masternode deployment using wallet client.

Advertising platform begins to support multiple advertising forms.

2nd part:

Provide products and construction of advertising platform; tools for integrating blockchain with NPW, traffic alliance, traffic integration, etc., including:

- The basic version of the decentralized advertising platform
- Advertising display test
- Support NPW payment advertising transactions
- Wallet built-in ad
- Self-service advertising in the wallet
- Traffic score system and user task function

The advertising type meets a variety of industry needs.

3rd part:

Consensus optimization is used to meet transaction and data transfer rates.

Smart Contract Development Based on R-like Statistical Analysis Capability, contains more traffic engine specific Turing-complete API.

- Automatically submit ad content and set ad price
- Advertising self-service
- Real-time onchain settlement
- Active anti-cheating system

This stage of advertising will support a variety of platforms.

4th part:

Basic development of user portraits, user label design based on big data algorithms.

- Safely classify users in real time
- Precise positioning query script
- All queries and data onchain storage
- Zero knowledge proof to protect user privacy from intrusion

5th part:

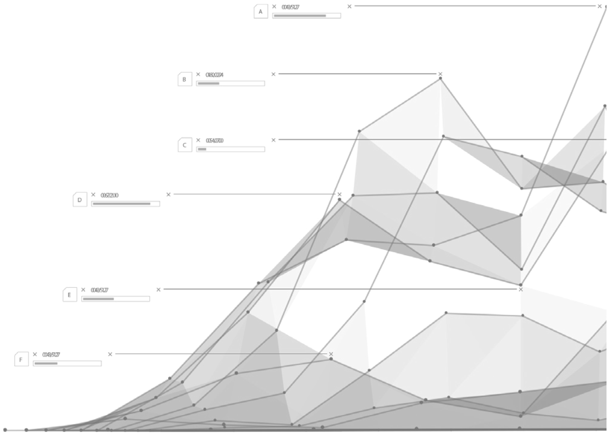
Open smart contract for precise delivery, including:

- Advertisers create their own smart contracts
- User-side task auto-execution and data tracking

6th part:

Eventually it becomes an underlying operating system-level traffic delivery engine that supports the underlying service operating system of multiple advertising platforms with open source__, and decentralized capabilities. Any other platform and application related to traffic can be built on it. Including:

- Connects RTB for a variety of platforms
- NPW exchange connect to multiple ad platforms
- Connecting Multichain smart contract and multiple digital assets.



VII. Summary

From the beginning of the Internet, traffic ability is the eternal power. Giants such as Google, Facebook, and Amazon use traffic capabilities as their business foundation to demonstrate their powerful user control capabilities on the Internet. No single giant can give up centralized traffic capabilities and provide it to third parties. We believe that today's giants are accumulating more and more centralized traffic, while decentralized, new forces are also accumulating.

The decentralization mechanism of the blockchain provides a possibility that the data is no longer controlled by the giants but is truly attributed to the users who use it. In order to help users truly own the data, they can enjoy accurate services without worrying about privacy protection.

NPW has such a foundation that it can use a new force to promote the development of a new era of Internet traffic.

VIII. Disclaimer

This document is a technical Whitepaper carrying out the current and future developments of the NPW ecosystem. This Whitepaper is for information purposes only and is **NOT A STATEMENT OF FUTURE INTENT**.

No person is entitled to rely on the information detailed in this Whitepaper or any inferences drawn from this Whitepaper, including in relation to any interactions with the NPW or the technologies mentioned in this Whitepaper.

ALL PERSONS ASSOCIATED WITH THE PREPARATION AND/OR PUBLICATION OF THIS WHITEPAPER TAKE NO RESPONSIBILITY NOR ASSUME ANY RESPONSIBILITY FOR ANY ERRORS THAT MAY BE CONTAINED IN THE WHITEPAPER.

Nothing in this Whitepaper should be relied upon and shall not confer rights or remedies upon you or any of your employees, creditors, or other holders or any other persons whether related to you or not. The opinions reflected in this Whitepaper may change without notice and the opinions do not necessarily correspond to the opinions of the community of the Whitepaper and/or any persons associated with the preparation and/or publication of this Whitepaper. The community of this Whitepaper do not have any obligation to amend, modify or update this Whitepaper or to otherwise notify any reader or recipient of this Whitepaper in the event that any matter related or stated in this Whitepaper or any opinion, projection, forecast or estimate detailed in this Whitepaper changes or subsequently becomes inaccurate.

By accessing this Whitepaper, the recipient agrees to be bound by the above limitations detailed in this disclaimer.