The White Paper of the NETCLOTH - Your Escort

Make You and Your Personal Network Unique

You are your sole raison dêtre of your existence, which is too our raison dêtre to customize an Internet architecture ----Web 3.0---- for your peculiarity.

1. This model is required a particular account which is generated and controlled by our hands. With it, you are entitled with access into all application scenarios and none spams can fly into your inbox without your agreement;
2. Its data is encrypted on our devices instead of the version sent to us after the treatment of a service;
3. Encryption is guaranteed in the process of information transmission, and the key to it is solely to you;
4. The code should be opensource, meanwhile the safety and synchronicity of the running environment are also secured.
5. It provides you with active right to choose, thus more flexible service providers choose for similar services are waiting for you;
6. The network is also required to provide you with a set of secure data storage methods, through which the data you generate online is best controlled by yourselves;
7. Finally, the ownership of this network belongs to you. Based on it, you deserve a corresponding return if your online behavior prospers the entire network.

Our project was founded based on these targets. And we have found technical tools from existed computer technologies that can achieve the above. Asymmetric encryption is a good set of security mechanisms that can be used to generate accounts. Nowadays, there are many asymmetric encryption algorithms, such as RSA, Elgamal, Knapsack Algorithm, Rabin, DH, ECC, etc. Considering both security and cost, as well as compatibility with accounts of existing blockchain projects, we chose ECC as the Algorithm to generate accounts. Since we cannot trust the third party to encrypt data for us, all encryption must be done by ourselves---- our devices. Besides, ECDH can meet the third point----the security in transmission. As for the fourth point, the issues about open source applications can be solved with existing code open source platforms (such as Github), and the operating environment requires virtual machines and smart contracts. Ideally, the front-end of the application should be displayed by the local device and directly interacted with the blockchain, rather than the server; at the same time, the back-end execution environment should be deployed in an overall maintained

and unified virtual machine. After apps open source, service providers cannot cheat users through code cheating. The fifth point can be achieved only with our establishment of an open peer-to-peer network. The sixth point is a bit complicated that it should resort to smart contracts, a trusted computing, and an encryption of the stored data based on the distributed network. The seventh point is that the ownership and benefits ask for insurance through the tunnel of digital assets whose aim initially as an incentive among network nodes run unstable for a long time due to lack of it, which can be reflected in Bitcoin.

1 Version 1.0 of NetCloth----Escort

The first function of the Internet is communication. We named the decentralized communication function in the NetCloth network "Escort", which is also the first version of the NetCloth network. In the following, we will take the decentralized instant messaging scenario as an example to explain what the NetCloth network is.

1.1 Account

On the Internet, we manage and use online identities with the aid of the third party. While through this method, information leakage and traffic competition would occur along with the convenience to users. Now, a new identity system has been introduced, which defines the public key of asymmetric encrypted ECC as the account address that derives from the account secret key generated offline by the users' devices.

Due to offline generation and local parameters, the account secret key is not only unique (the collision probability is extremely low), but also not known to a second person other than the user.

1.2 Establishment of a Connection

The public ledger of the blockchain technology is designated as the "number book", and the user obtains the communication address of the other party by consulting the public ledger. User A informs the Validator of his public key K_A and the selected communication address IP_A, then the validator records this information in the latest block. When user B asks for a connection with A, B retrieves the last communication address (AKA IP_A) claimed by user A and then performs encrypted communication through ECDH.

1.3 Encrypted Transmission

We use ECDH for an assurance of an independent encryption of the data exchange between each other in the network. Supposing user A wants to send a message to user B, K_A, k_A are

respectively the A's public and secret keys, and K_B, k_B the B's, the communication of their information steps as the follow:

1. B informs A of his account address (public key) K_B;
2. A calculates the shared secret key k_A with his secret key and B's public key K_B through ECDH
3. A then uses S to encrypt T with AES into $T^{'}$;
4. User A sends the ciphertext $T^{'}$ to B through the NetCloth network;
5. User B receive the shared key S by his secret key k_B and A's public key K_A;
6. User B obtain raw message T from the ciphertext $T^{'}$ through AES decryption.

1.4 Data Transmission

Data Transmission is performed by the starfish nodes in NetCloth (the service nodes of NetCloth). Any network user can become a starfish node and set up his own communication server. First, users are required for their own account and a server with a public IP address, both for downloading the open source code of the communication service and executing this code. Finally, after the IPAL claim is completed, Data Transmission services can be provided for all users. Because transmitted contents are sent after the user’s local and independent encryption, the difficulty and cost of cracking can scare away the motivation of the starfish node to steal user data.

1.5 Conclusion

Following the above steps, we have reached the decentralized instant communication between users. The application has been open sourced on github and has been listed on the application market(App Store and Google Play). This is the first scenario we developed based on the decentralized security communication problem. We named this version of the NetCloth network "Escort", which will be redeveloping a second and even a third open source application this year based on secure communication functions (check NetCloth Ecological Construction 2020 for details).

2 Network roles

2.1 Client-Account and Wallet

NetCloth network accounts are unified with blockchain wallets. Thus, users can not only enter a variety of future decentralized application scenarios through a pair of ECC public and secret key pairs, but also manage all digital assets by this pair of keys (that is, entering

NetCloth means users of the network can automatically create wallets in most blockchain networks such as BTC, ETH, etc.). Furthermore, they can immediately use the existing decentralized application scenarios of the blockchain.

2.2 Server-Starfish Node

In the NetCloth network, users can easily provide services to others by becoming starfish nodes. Based on open source programs, nodes only need to provide basic hardware for background program operations and register in the network to provide services to other users, eliminating the cost of program development. The relationship between nodes is a parallel starfish organization relationship. Users can switch the nodes that provide services at will. The only thing that can measure the quality of node service is the user.

2.3 Consensus-Validator

The consensus of the NetCloth network is for the stability of the network, mainly including the acquisition and exchange of network credentials NCH, the token of network, and the establishment and maintenance of ecosystems. The NCH is obtained based on the BPoS (BFT and PoS) Consensus, that is, the holders jointly formulate and maintain network rules. The account (public keys) of users and servers are recorded by the Validator in the public ledger to ensure the certainty and immutability of the network relationship. Each of the ecological scenario realized through the side chain is required to complete the founder’s information on the NetCloth main chain and synchronize blocks regularly for a stable operation of the side chain.

The maintainers of the consensus are collectively referred to as validators who come from any starfish node after registration. The top 100 validators who get votes are called active validators and are responsible for network accounting. The total instant increase of active validators is 10 each year, not over the ceiling number of 300.

3 Network Governance

3.1 Network Use Certificate-NCH

Incentives in peer-to-peer networks account for the creation of blockchain network credentials. However, three properties of anonymity, complete autonomy, and selfish rationality of the peer-to-peer network node lead to poor stability and node cheating in the system. Therefore, the credentials in the blockchain is designed to efface the above faults. Since the credential is an incentive model based on the general equivalent, it is also known as digital assets, such as BTC, ETH, etc.

The using certificate in the NetCloth network is NCH with an aim of public information

records, certification of ownership and consensus maintenance.

3.2 Consensus (BPoS)

We believe that the closer stakeholders are less likely to attack the network. The consensus algorithm of the NetCloth network is based on Byzantine fault tolerance and proof of stake, BPoS for short. BPoS, a deterministic consensus, can tolerate 1/3 of offline or faulty of the validators in the network, and can accommodate higher transaction capacity under the same security, accelerating transaction confirmation and diminishing the risk of malicious node forks.

3.3 Governance and Voting

NetCloth network governance is mainly for avoidance of network cheating and ecological autonomy. For users with greater power, their cheating is prevented through NCH collateral and public supervision. For a more flexible ecosystem, a weak-consensus autonomous method is provided, through which eco-builders can set their own consensus, mainly benefiting a chain ecological construction with high performance, safety and stability.

We believe that off-chain governance should be transited to on-chain governance. As a supplement to on-chain governance, off-chain governance is allowed by ecological builders to conduct on the weak-consensus side chain.

We believe that the basic parameters related to the main network, such as the number of validator nodes, the minimum network usage fee, and sidechain mapping standards, need to be governed by on-chain proposals and voting. All NCH holders have the right to participate in proposals and votes. Evaluations such as the quality of specific business services will mainly be done by off-chain governance.

3.4 Ecological Architecture

The above figure is the architecture diagram of the NetCloth network, of which IPAL is a special addressing claim on the main chain, which can be regarded as an addressing protocol. NCH, the token, is between the node layer and the ledger layer to fulfill the disclosure and non-tampering of starfish nodes; while there is no restriction of payment methods between the application layer and users, which can facilitate starfish nodes in different countries and regions. NetCloth being an open blockchain network without any threshold, thus users can become starfish nodes at the lowest cost and any other users in different countries and regions can also enjoy this priority. According to the development roadmap of the NetCloth network, all decentralized application scenarios with different functions can be found.

4 Core Technologies

Each version of the NetCloth network only concentrates on one or two key technologies, and the rest can be learned from the document and open source code on github. Here is the open source address: https://github.com/netcloth

4.1 VM

Bearing an aim of reducing the cost for developers to learn and write smart contracts, the NetCloth network has integrated EVM and will upgrade it to eWASM later.

4.2 IPAL Addressing Protocol

IP Address List is a unique addressing module of NetCloth network. IPAL records such information of starfish nodes as access point IP, node name, and contact information. By searching IPAL list on the chain, users can filter their favorite starfish nodes and enjoy the service.

4.3 C-IPAL Statement

The Client IP Address List (C-IPAL) protocol is an extension of IPAL, facing for client users. Submitting an address through C-IPAL is required by users with a need of enjoying various services. The specific procedure of C-IPAL has been explained in Chapter 1.2.

4.4 Side Chain

The side chain of the NetCloth totally differs its full decentralization from that of the main chain. The side chain with a permission of partial decentralization can dramatically increase transaction processing speed, and is suitable for application scenarios featured with running large-scale and high-concurrency, which can be taken as an extension of the main chain performance. Side-chain token can be issued by users on this chain through a method different from the token issue of the main chain. The issuing way of side chain is presented here: First, make sure the sidechain validator is the main chain Validator, then with the help of smart contract to set the fixed exchange rate between the two sides' token, finally exchange the sidechain token by the operative contract.

5 Roadmap

The NetCloth network will gradually implement decentralized functions through the upgrade of the main network. The upgrade path is divided into four stages, respectively Escort, Container, Bazaar, and Factory.

5.1 Information Interaction-Escort

We named the first version Escort, providing users with open source code in decentralized secure communications, which means users can directly enjoy instant messaging services. Based on this open source code, a secondary development can also be conducted to create other scenarios applications such as social and information interactive games.

5.2 Data Storage-Container

The second version, called Container, offers users safe and reliable decentralized data storage function, consisting of local storage, cluster storage and decentralized storage. Among the three, decentralized storage is to be processed in a form of paying for reading, so as to get those valuable data screened out, that is, “over-reviewed data”, used for a collection of group memory on the network.

5.3 Data Exchange-Bazaar

This version is a function developed based on the fact that users have already kept their own data. Its main purpose is to provides users with various types of smart contracts with data for interaction and exchange to complete the reasonable use and storage of data, ensuring the user's data security and benefits not damaged.

5.4 Trusted Computing-Artificial Intelligence Factory

The last functional version of NetCloth is target to deal with such a property that data are extremely easy-to-replicate. What effort this version make is providing computing space trusted by the third party and then preventing the theft of user data by starfish nodes through three tunnels of time, motivation and cost. Combining the interaction function with the exchange functions of data in the bazaar, we believe that this version will train a large number of artificial intelligence models, which exactly is why we address it as Artificial Intelligence Factory.

6 Community Portal

- Official Website: https://www.netcloth.org
- Open source address: https://github.com/netcloth

- Blog: https://blog.netcloth.org
- Twitter: https://witter.com/NetCloth
- Medium: https://medium.com/@NetCloth