WenQuanYi Micro Hei [Scale=0.9]WenQuanYi Micro Hei Mono song-WenQuanYi Micro Hei sfWenQuanYi Micro Hei "zh" = 0pt plus 1pt

nebulas wiki Documentation

åŔŚåÿČ 1.0

nebulas

8ælJĹ 29, 2018

Table of Contents:

CHAPTER 1

Category

Here is all you need to dive into Nebulas.

1.1 NebulasIO

- WebsiteïijŽhttps://nebulas.io
- Non-Tech WhitepaperïijŽhttps://nebulas.io/docs/NebulasWhitepaperZh.pdf
- Tech WhitepaperïijŽhttps://nebulas.io/docs/NebulasTechnicalWhitepaperZh.pdf

1.2 Go-Nebulas

- Wiki: https://github.com/nebulasio/wiki
- Join Testnet: https://github.com/nebulasio/wiki/blob/master/testnet.md
- Join Mainnet: https://github.com/nebulasio/wiki/blob/master/mainnet.md
- Explorer: https://explorer.nebulas.io
- Tutorials:
  - English 101
    - Installation (thanks Victor)
    - Sending a Transaction (thanks Victor)
    - Writing Smart Contract in JavaScript (thanks otto)
    - Introducing Smart Contract Storage (thanks Victor)

        * Interacting with Nebulas by RPC API (thanks Victor)
    - äÿ■æŰĞ - åĚěéŮÍæŢŹçÍŃ
        * çijŰèŕŚåőL'èčĚåŔŁè£Řèą Ňneb
        * åIJÍæŸ§äžŚéŞ¿äÿŁåŔŚéĂĄäžd'æŸŞ
        * ä¡£çŤÍJavaScriptçijŰåĘŹæŹžèČ¡åŘĹçžę
        * æŹžèČ¡åŘĹçžęå■ŸåĆÍåŇžäżŃçż■
        * éĂŽè£ĞRPCæŐěåŕčäÿŐæŸ§äžŚéŞ¿äžd'äžŠ

1.3 Wallet

- Web Wallet: https://github.com/nebulasio/web-wallet
    - English
        * Creating A NAS Wallet
        * Sending NAS from your Wallet
        * Signing a Transaction Offline
        * View Wallet Information
        * Check TX Status
        * Deploy a Smart Contract
    - äÿ■æŰĞ
        * éŠśåŇĚæŢŹçÍŃ|æŸ§äžŚWebéŠśåŇĚæŢŹçÍŃ1ïijŽåĹŻåžžNASéŠśåŇĚ
        * éŠśåŇĚæŢŹçÍŃ|æŸ§äžŚWebéŠśåŇĚæŢŹçÍŃ2ïijŽåŔŚèţůè¡ňèť'ę
        * éŠśåŇĚæŢŹçÍŃ|æŸ§äžŚWebéŠśåŇĚæŢŹçÍŃ3ïijŽçężçž£ç■¿åŘ■äžd'æŸŞ
        * éŠśåŇĚæŢŹçÍŃ|æŸ§äžŚWebéŠśåŇĚæŢŹçÍŃ4ïijŽæ§ěçIJŃéŠśåŇĚä£ąæĄŕ
        * éŠśåŇĚæŢŹçÍŃ|æŸ§äžŚWebéŠśåŇĚæŢŹçÍŃ5ïijŽæ§ěçIJŃäžd'æŸŞçŁűæĂĄ
        * éŠśåŇĚæŢŹçÍŃ|æŸ§äžŚWebéŠśåŇĚæŢŹçÍŃ6ïijŽéČÍç¡šæŹžèČ¡åŘĹçžę

1.4 DApp

- Web SDK: https://github.com/nebulasio/neb.js
- Smart Contract: https://github.com/nebulasio/wiki/blob/master/smart_contract.md
- Standard Protocol:
    - NRC20: https://github.com/nebulasio/wiki/blob/master/NRC20.md

1.5 Community Tools

- Nebulearn: https://nebulearn.com/official-docs/go-nebulas (thanks to Tehjr)
- Demo DApp: https://github.com/15010159959/super-dictionary (thanks to ChengOrangeJu, yupnano, Kurry)
- Chrome Extension: https://github.com/ChengOrangeJu/WebExtensionWallet (thanks to ChengOrangeJu, yupnano)

1.6 Contribution

We are very glad that you are considering to write tutorials or documents of Nebulas. If you did write something, please submit a issue to let us know, we will add your name and url to this page soon.

CHAPTER 2

WhatâĂŹs Nebulas

2.1 Nebulas: Next Generation Public Blockchain

2.2 Nebulas is aiming to build a continuously improving ecosystem.

Nebulas is a next-generation public blockchain. It introduces Nebulas Rank (NR), a new measure of value for every unit of the blockchain universe, like addresses, DApps and smart contracts. Based on NR, it involves Nebulas Incentive (NI), which incentives developers with Developer Incentive Protocol, and users with the Proof of Devotion consensus algorithm. Moreover, it proposes Nebulas Force (NF), which gives the blockchain and smart contracts within it a self-evolving capacity. In unison, NR, NI, and NF produce a continuously improving and expanding blockchain ecosystem.

There are three technical features: value ranking, self-evolution, and native incentive.

Facing the opportunity and challenge as above, we aim to create a self-evolving blockchain system based on value incentive.

2.3 Principles

The Nebulas blockchain has three major principles:

2.3.1 Nebulas Rank (NR)

Nebulas Rank (NR) is an open sourced ranking algorithm used to measure the influence of relationships among addresses, smart contracts, and distributed applications (DApps). It helps both users utilize information among the ever-increasing amount of data on all blockchains & developers to use our search framework directly in their own applications.

In Nebulas, we measure value regarding:

- **Liquidity**

Finance essentially is the social activities which optimize social resources via capital liquidity and promote economic development. Blockchains establish a value network in which the financial assets can flow. Daily volume of Bitcoin and Ethereum, which are most familiar to us, already exceeds $1 billion. From these data, we can see that the more transaction volume and transaction scale, the higher liquidity. In turn, higher liquidity will increase the quantity of transaction and enhance the value. That will further strengthen financial assetsâĂŹ value, creating a complete positive feedback mechanism. Therefore liquidity, i.e. transaction frequency and scale, is the first dimension that NR measures.

- **Propagation**

Social platforms like WeChat and Facebook have almost 3 billion active users per month. Social platformsâĂŹ rapid user growth is a result of the reflection of existing social network and stronger viral growth. In particular, viral transmission, i.e. speed, scope, depth of information transmission and linkage, is the key index to monitor social networkâĂŹs quality and user growth. In blockchain world, we can see the same pattern. Powerful viral propagation indicates scope and depth of asset liquidity, which can promote the blockchain worldâĂŹs asset quality and asset scale. Thus, viral transmission, i.e. scope and depth of asset liquidity, is the second dimension that NR measures.

- **Interoperability**

At InternetâĂŹs early stage, there are only basic websites and private information. Now, information on different platforms can be forwarded on the network, and isolated data silos are gradually being broken. This trend is the process of identifying higher dimensional information. In our point of view, the world of blockchains shall follow a similar pattern, but its speed will be faster. The information on usersâĂŹ assets, smart contracts, and DApps will become richer, and the interaction of higher dimensional information shall be more frequent, thus better interoperability shall become more and more important. Therefore, NRâĂŹs third measure dimension is interoperability.

Based on above-stated dimensions, we start to construct NebulasâĂŹ NR system by drawing from richer data, building a better model, digging up more diversified value dimensions, and establishing a measure of value in blockchain world.

2.3.2 Nebulas Force (NF)

A series of basic protocols such as NR, PoD, DIP shall become a part of blockchain data. With the growth of data on Nebulas, these basic protocols will upgrade, and this will avoid frac-

ture between developers and community as well as the âĂIJforkâĂİ. We call this fundamental capability of blockchain âĂIJNebulas ForceâĂİ (NF).

As Nebulas community grows, NF and basic protocolsâĂŹ update ability shall be open to the community. According to usersâĂŹ NR weight and community voting mechanism, the community determines NebulasâĂŹ evolution direction and its update objectives. With the help of NFâĂŹs core technology and its openness, Nebulas will have ever-growing evolving potential and infinite evolving possibilities endlessly.

{#7746}

2.3.3 Nebulas Incentive (NI)

Nebulas Incentive include Proof of Devotion (PoD) and Developer Incentive Protocol (DIP).

Proof-of-Devotion (PoD)

Based on NebulasâĂŹ NR system, we shall adopt PoD (Proof-of-Devotion) consensus algorithm. PoD gives an âĂIJinfluentialâĂİ user of Nebulas Blockchain an opportunity to become a bookkeeper and receive NebulasâĂŹ block rewards and transaction fee as revenues, which will encourage them to contribute to NebulasâĂŹ stability and security continuously.

Developer Incentive Protocol (DIP)

In Nebulas, we propose the concept of DIP (Developer Incentive Protocol) for developers of smart contracts and DApps. DIPâĂŹs core concept: in pre-specified blocksâĂŹ interval, for those developers whose smart contracts and DApps deploy online in the most recent interval with NR value higher than a specified threshold, DIP shall reward them corresponding developer incentives (NAS token), and these incentives shall be recorded on blocks by bookkeepers. With DIPâĂŹs positive incentive mechanism, more and more developers get incentives to create valuable smart contracts and DApps, which helps to build a positive feedback ecosystem for the developersâĂŹ community.

2.3.4 Value ranking

To enable value discovery in blockchain, **Nebulas Rank** measures multidimensional data in the blockchain world and powers the decentralized search framework.

2.3.5 Native incentives

To avoid the damage caused by forking to the blockchain, **Nebulas Force** enables rapid iteration and upgradability to its blockchain without the need for hard forks.

2.3.6 Nebulas Incentives

With forward-looking incentive and consensus mechanisms, the **Nebulas Incentive** rewards developers and users who contribute to the sustainability and growth of the ecosystem.

This is the except of Nebulas Non-technical Whitepaper.

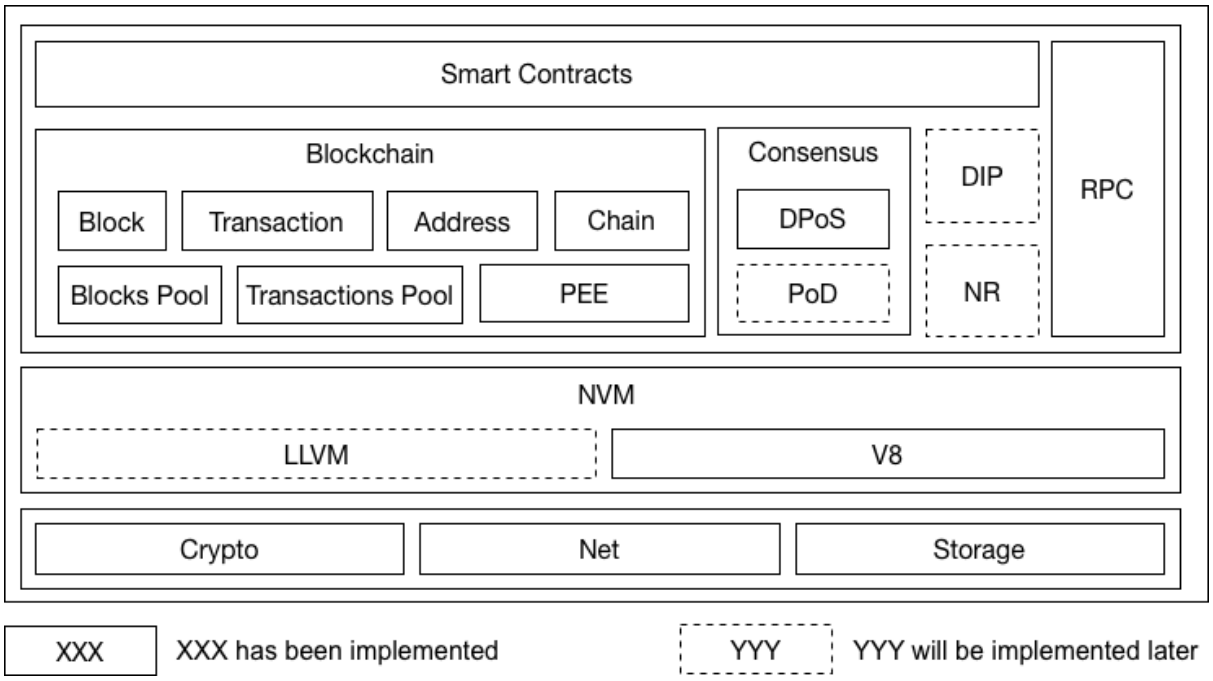
If you want to know more about Nebulas, please subscribe this official blog, or visit our website: nebulas.io. Read our Non-technical White Paper (English), Technical White Paper (English).

Thank you.

CHAPTER 3

Go-Nebulas

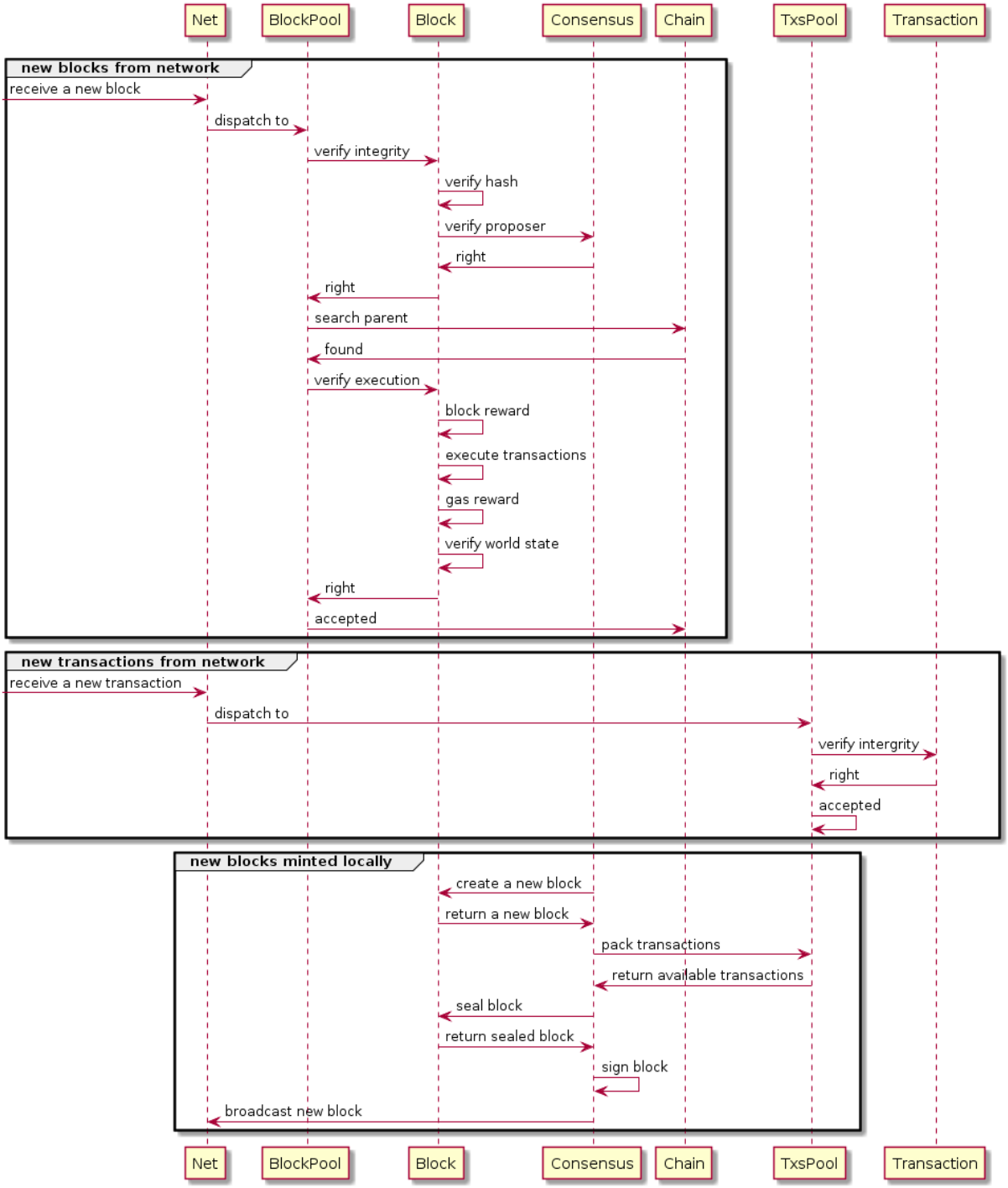
3.1 Design Overview



TODO: More features described in our whitepaper, such as NR, PoD, DIP and NF, will be integrated into the framework in later versions very soon.

3.1.1 Core Dataflow

Here is a core workflow example to explain how Nebulas works in current version. For each Nebulas node, it keeps receiving blocks or transactions from network and mining new block locally.



3.1.2 More Details

Blockchain

Model

Nebulas use accounts model instead of UTXO model. The execution of transactions will consume gas.

Data Structure

```
Block Structure
+---------------+----------------+--------------+
|  blockHeader  |  transactions  |  dependency  |
+---------------+----------------+--------------+
blockHeader: header info
transactions: transactions array
dependency: the dependency relationship among transactions

Block Header Structure
+-----------+--------+--------------+------------+-------------+----
 ↪---+--------+
|  chainid  |  hash  |  parentHash  |  coinbase  |  timestamp  | ␣
 ↪alg  |  sign  |
+-----------+--------+--------------+------------+-------------+----
 ↪---+--------+
+-------------+-----------+--------------+-----------------+
|  stateRoot  |  txsRoot  |  eventsRoot  |  consensusRoot  |
+-------------+-----------+--------------+-----------------+
chainid: chain identity the block belongs to
hash: block hash
parentHash: parent block hash
coinbase: account to receive the mint reward
timestamp: the number of nanoseconds elapsed since January 1, 1970␣
 ↪UTC
alg: the type of signature algorithm
sign: the signature of block hash
stateRoot: account state root hash
txsRoot: transactions state root hash
eventsRoot: events state root hash
consensusRoot: consensus state, including proposer and the dynasty␣
 ↪of validators


Transaction Structure
+-----------+--------+--------+------+---------+---------+----------
 ↪---+
|  chainid  |  hash  |  from  |  to  |  value  |  nonce  | ␣
 ↪timestamp  |
```

```
+-----------+--------+--------+------+---------+---------+----------
 ↪---+
+--------+------------+------------+
|  data  |  gasPrice  |  gasLimit  |
+--------+------------+------------+
chainid: chain identity the block belongs to
hash: transaction hash
from: sender's wallet address
to: receiver's wallet address
value: transfer value
nonce: transaction nonce
timestamp: the number of seconds elapsed since January 1, 1970 UTC
alg: the type of signature algorithm
sign: the signature of block hash
data: transaction data, including the type of transaction(binary␣
 ↪transfer/deploy smart contracts/call smart contracts) and payload
gasPrice: the price of each gas consumed by the transaction
gasLimit: the max gas that can be consumed by the transaction
```

Blockchain Update

In our opinion, **Blockchain** only needs to care about how to process new blocks to grow up safely and efficiently. What's more, **Blockchain** can only get new blocks in the following two channels.

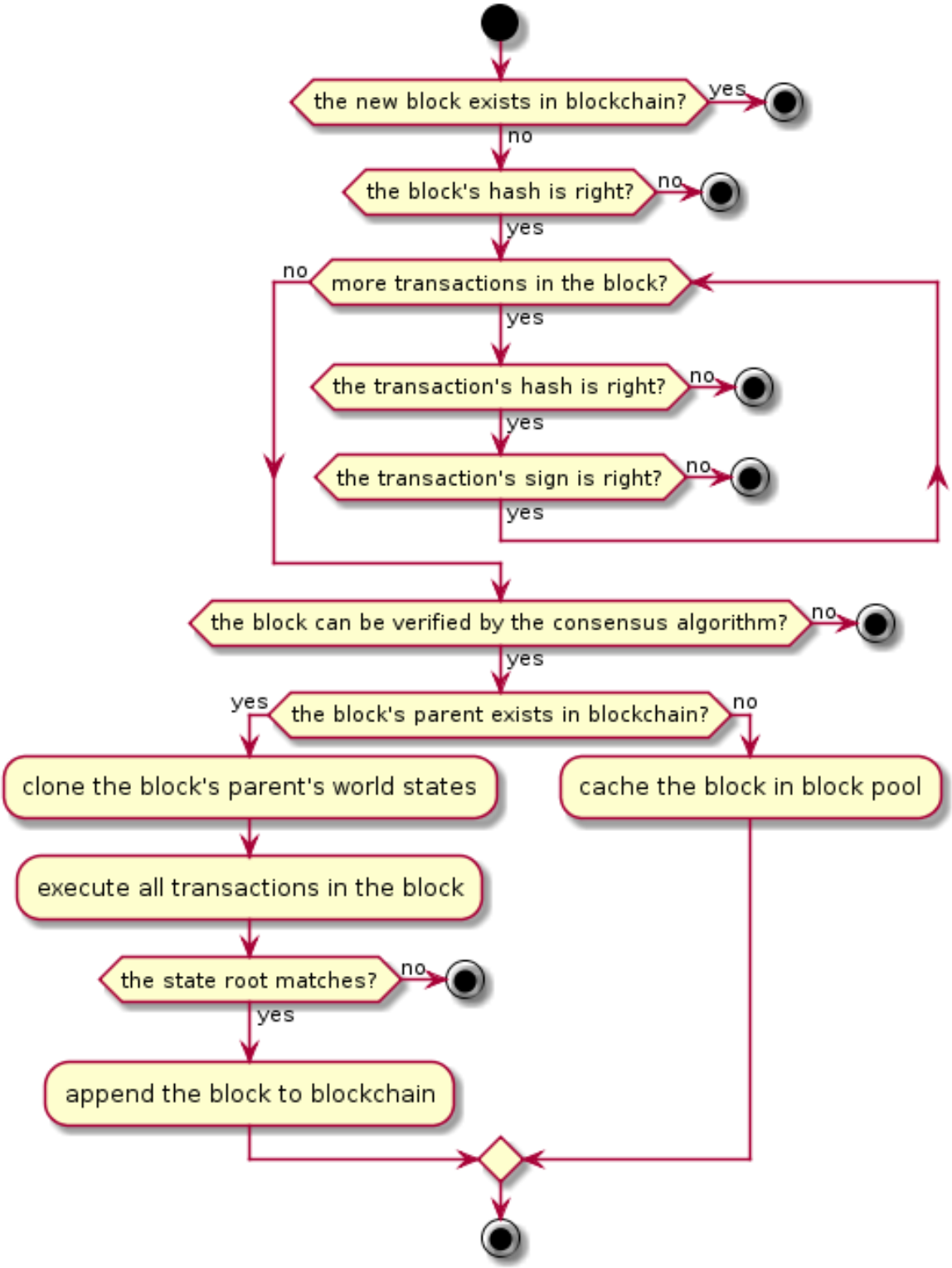
A new block from network

Because of the unstable network latency, we cannot make sure any new block received can be linked to our current **Chain** directly. Thus, we need the **Blocks Pool** to cache new blocks.

A new block from local miner

At first, we need the **Transactions Pool** to cache transactions from network. Then, we wait for a new block created by local **Consensus** component, such as DPoS.

No matter where a new block comes from, we use the same steps to process it as following.



World State

Every block contains the current world state, consist of following four states. They are all maintained as Merkle Trees.

Accounts State

All accounts in current block are stored in Accounts State. Accounts are divided into two kinds, normal account & smart contract account.

Normal Account, including

- **wallet address**
- **balance**
- **nonce**: account's nonce, it will increment in steps of 1

Smart Contract AccountïijŇ including

- **contract address**
- **balance**
- **birth place**: the transaction hash where the contract is deployed
- **variables**: contains all variables' values in the contract

Transactions State

All transactions submitted on chain are storage in Transactions State.

Events State

While transactions are executed, many events will be triggered. All events triggered by transactions on chain are stored in Events State.

Consensus State

The context of consensus algorithm is stored in consensus state.

As for DPoS, the consensus state includes

- **timestamp**: current slot of timestamp
- **proposer**: current proposer
- **dynasty**: current dynasty of validators

Serialization

We choose Protocol Buffers to do general serialization in consideration of the following benefits:

- Large scale proven.

- Efficiency. It omits key literals and use varints encoding.
- Multi types and multilangue client support. Easy to use API.
- Schema is good format for communication.
- Schema is good for versioning/extension, i.e., adding new message fields or deprecating unused ones.

Specially, we use json to do serialization in smart contract codes instead of protobuf for the sake of readability.

Synchronization

Sometimes we will receive a block with height much higher than its current tail block. When the gap appears, we need to sync blocks from peer nodes to catch up with them.

Nebulas provides two method to sync blocks from peers: Chunks Downloader and Block Downloader. If the gap is bigger than 32 blocks, we'll choose Chunk Downloader to download a lot of blocks in chunks. Otherwise, we choose Block Downloader to download block one by one.

Chunks Downloader

Chunk is a collection of 32 successive blocks. Chunks Downloader allows us to download at most 10 chunks following our current tail block each time. This chunk-based mechanism could help us minimize the number of network packets and achieve better safety.

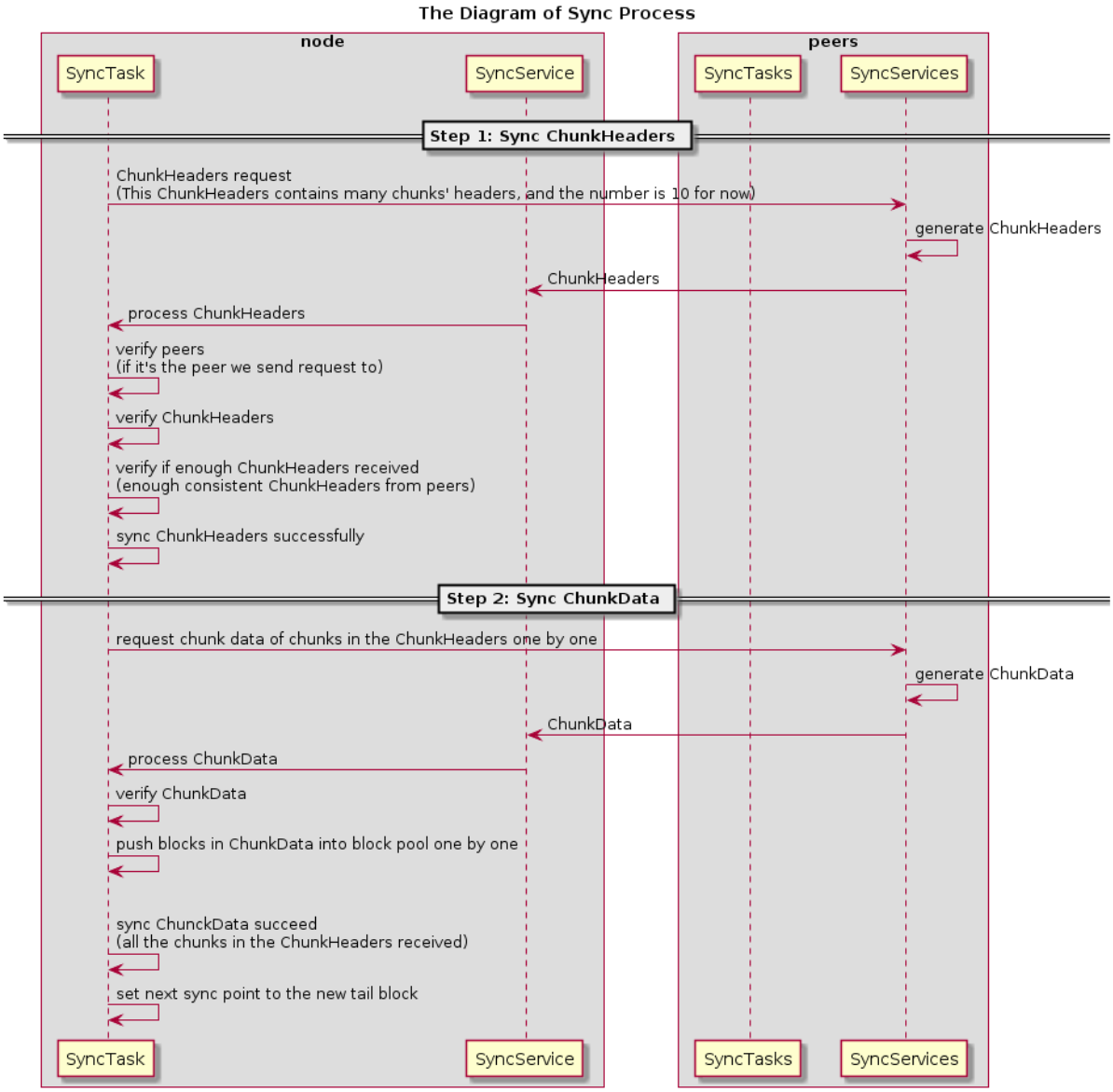
The procedure is as following,

```
1. A sends its tail block to N remote peers.
2. The remote peers locate the chunk C that contains A's tail block.
   Then they will send back the headers of 10 chunks, including the␣
↪chunk C and 9 C's subsequent chunks, and the hash H of the 10␣
↪headers.
3. If A receives >N/2 same hash H, A will try to sync the chunks␣
↪represented by H.
4. If A has fetched all chunks represented by H and linked them on␣
↪chain successfully, Jump to 1.
```

In steps 1~3, we use majority decision to confirm the chunks on canonical chain. Then we download the blocks in the chunks in step 4.

Note: `ChunkHeader` contains an array of 32 block hash and the hash of the array. `ChunkHeaders` contains an array of 10 `ChunkHeaders` and the hash of the array.

Here is a diagram of this sync procedure:



Block Downloader

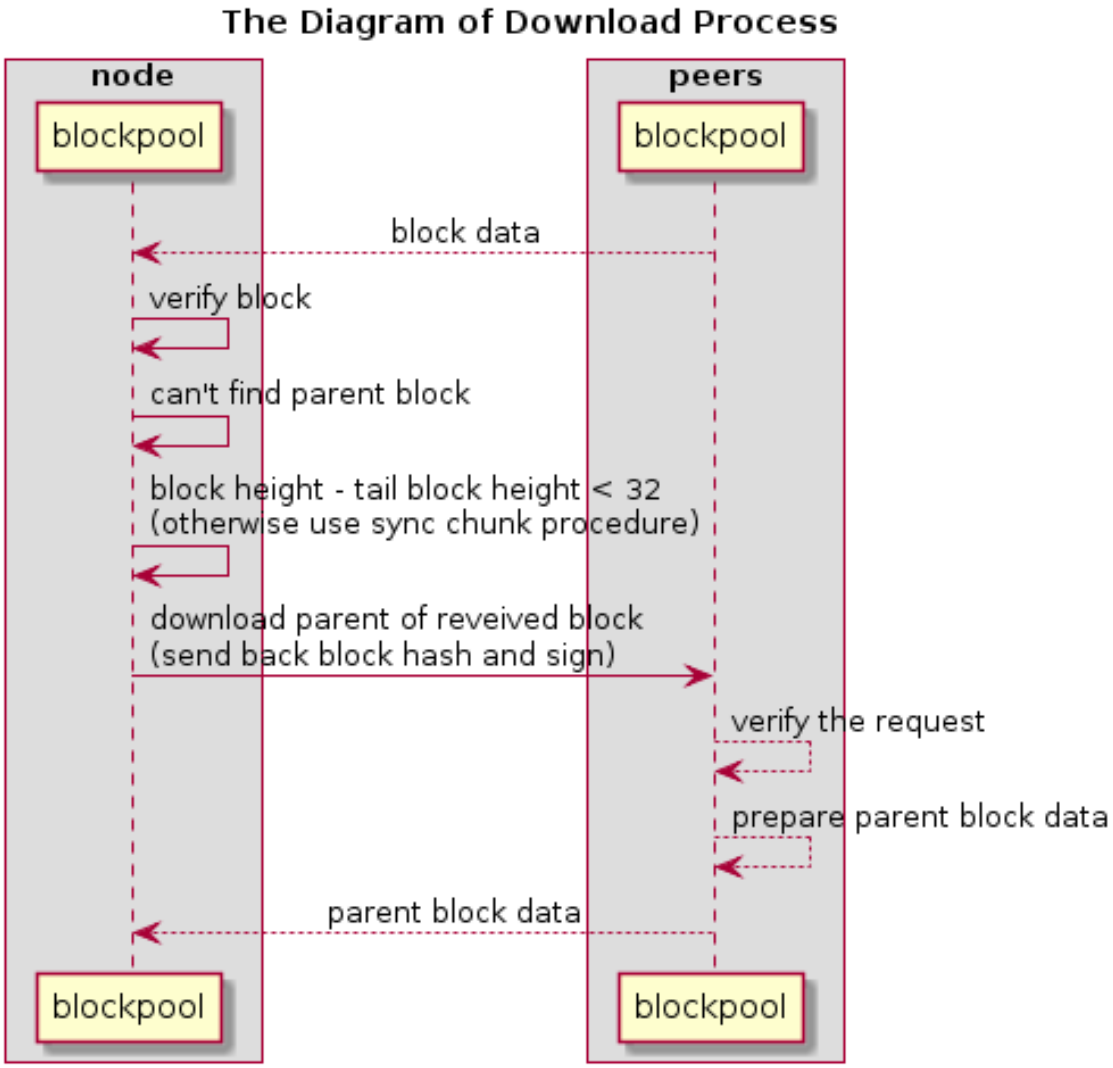
When the length gap between our local chain with the canonical chain is smaller than 32, we'll use Block downloader to download the missing blocks one by one.

The procedure is as following,

```
1. C relays the newest block B to A and A finds B's height is␣
↪bigger than current tail block's.
2. A sends the hash of block B back to C to download B's parent␣
↪block.
3. If A received B's parent block B', A will try to link B' with A
↪'s current tail block.
   If failed again, A will come back to step 2 and continue to␣
↪download the parent block of B'. Otherwise, finished.
```

This procedure will repeat until A catch up with the canonical chain.

Here is a diagram of this download procedure:



Merkle Patricia Tree

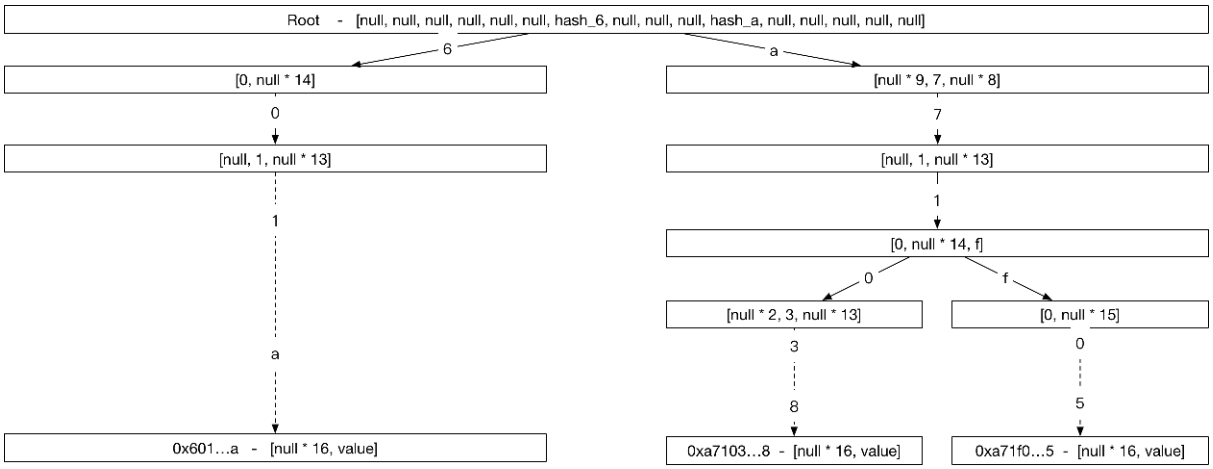
Basic: Radix Tree

Reference: https://en.wikipedia.org/wiki/Radix_tree

A Radix Tree using address as the key looks like below:

- Addresses are represented as Hex Characters
- Each node in the Tree is a 16-elements array, 16 branch-slots(0123...def)
- leaf node: value can be any binary data carried by the address
- non-leaf node: value is the hash value calculated based on the childrenâĂŹs data

As for a 160-bits address, the max height of the tree is 40



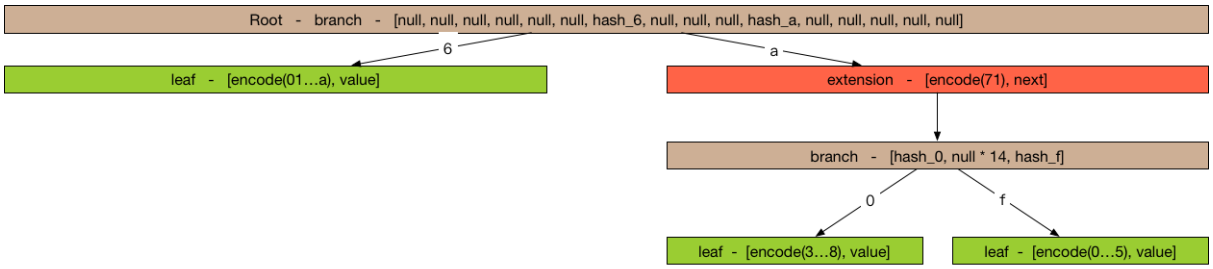
Problems: much space for a single entry 40 steps for each lookup

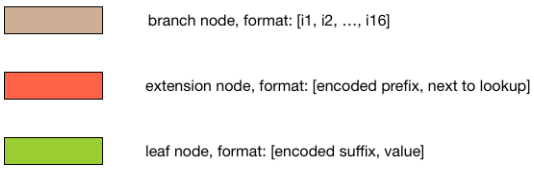
Advanced: Merkle Patricia Tree

Reference: https://github.com/ethereum/wiki/wiki/Patricia-Tree, http://gavwood.com/Paper.pdf

In order to reduce the storage of Radix Tree. The nodes in Merkle Patricia Tree are divided into three kinds,

- extension node: compress nodes using common prefix
- leaf node: compress nodes using unique suffix
- branch node: same as node in Radix Tree





How to store Merkle Patricia Tree

Key/Value Storage

hash(value) = sha3(serialize(value))

key = hash(value)

How to update Merkle Patricia Tree

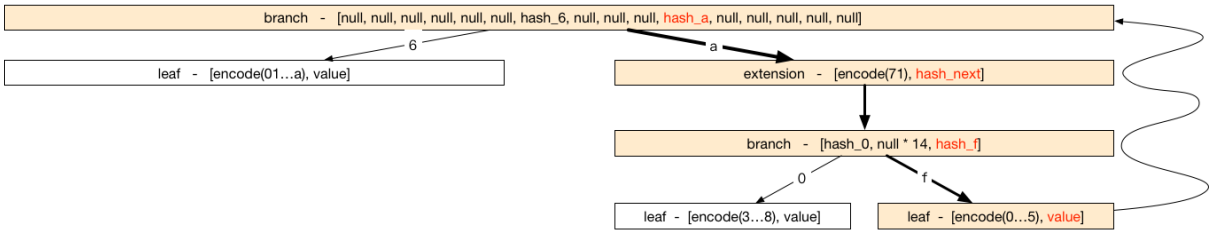
Query

DFS from top to bottom

Update, Delete or Insert

1.Query the node from top to bottom

2.update the hash along the path from bottom to top



Performance Each operation costs O(log(n))

How to verify using Merkle Patricia Tree

Theorems

1.Same merkle trees must have same root hash.

2.Different merkle trees must have different root hash.

Using the theorems, we can verify the result of the execution of transactions.

Quick Verification

A light client, without sync huge transactions, can immediately determine the exact balance and status of any account by simply asking the network for a path from the root to the account node.

Consensus

We think each consensus algorithm can be described as the combination of State Machine and Fork Choice Rules.

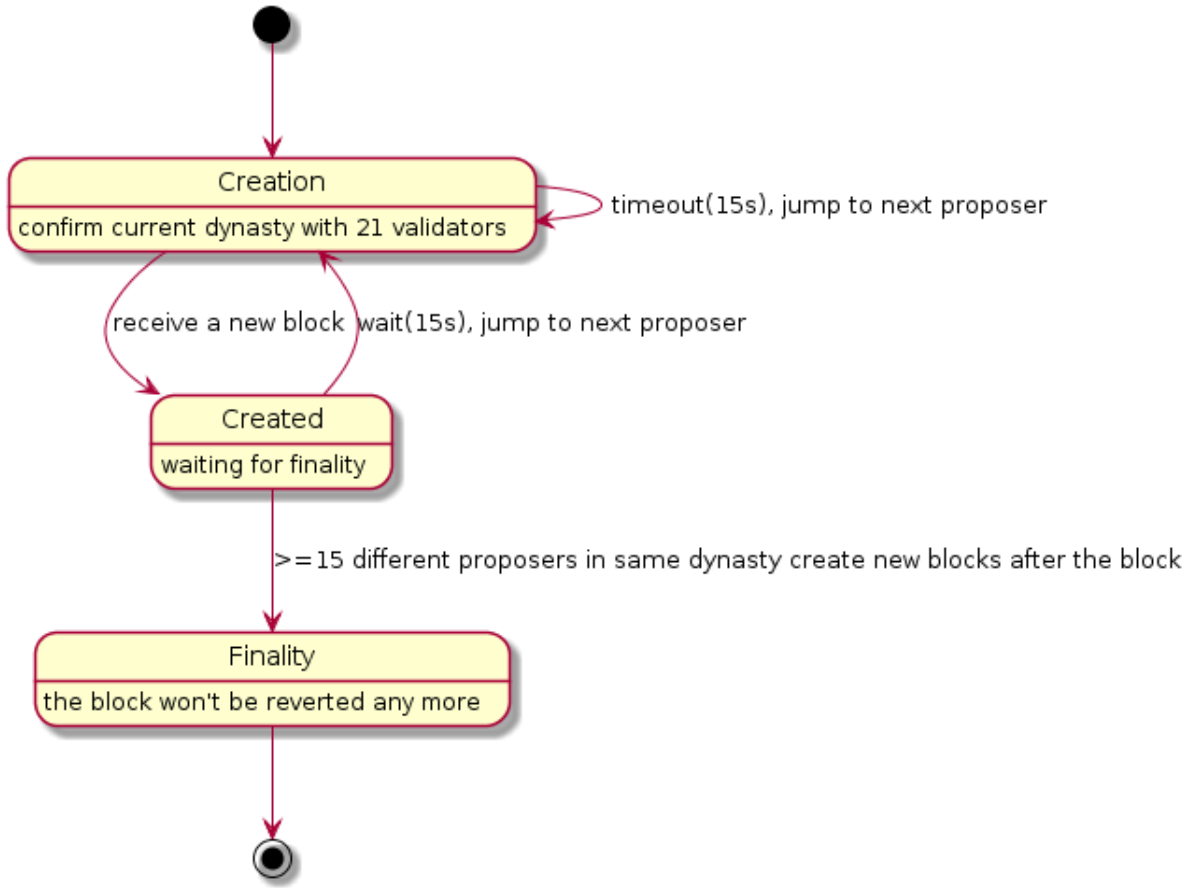
DPoS(Delegate Proof-of-Stake)

Notice For Nebulas, the primary consensus algorithm should be PoD, the DPoS algorithm is just a temporary solution. After the formal verification of PoD algorithm, we will transition mainnet to PoD. All witness (bookkeeper/miner) of DPoS are now accounts officially maintained by Nebulas. We will make sure a smooth

transition from DPoS to PoD. We will create new funds to manage all the rewards of bookkeeping. And we will NOT sell those NAS on exchanges. All NAS will be used for building the Nebulas ecosystem, for example, rewarding DApp developers on Nebulas. And we will provide open access to all the spending of these rewards periodically.

As for the DPoS in Nebulas, it can also be decribed as a state machine.

State Machine



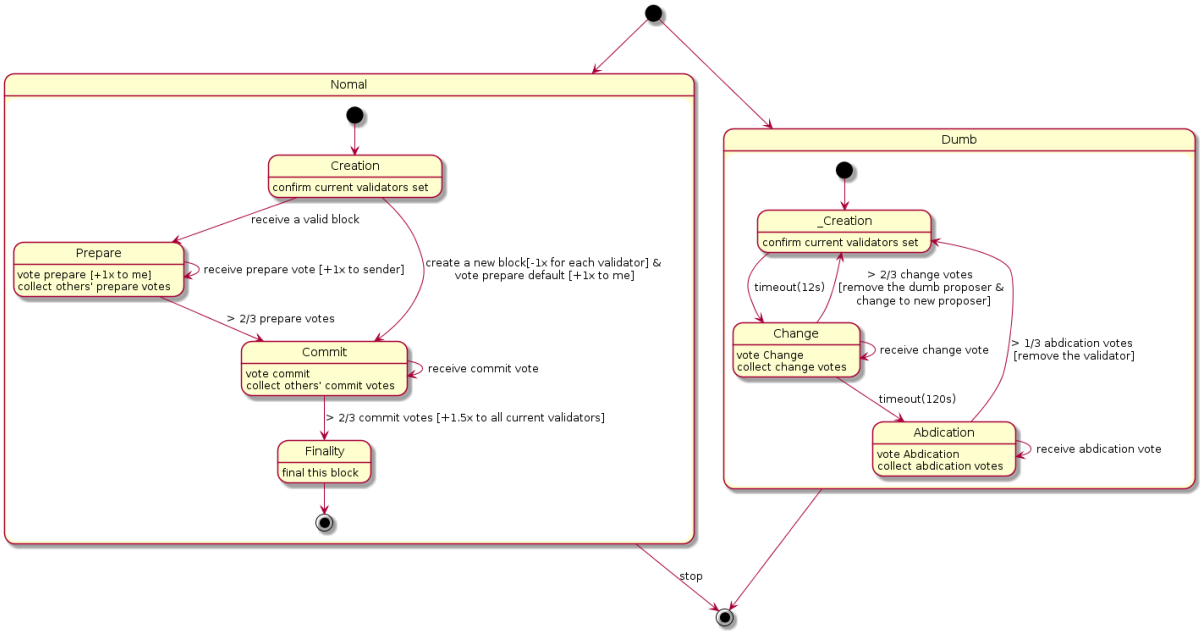
Fork Choice Rules

1. Always choose the longest chain as the canonical chain.
2. If A and B has the same length, we choose the one with smaller hash.

PoD (Proof-of-Devotion)

Here is a draft of PoD. The research on PoD is ongoing here.

State Machine



Fork Choice Rules

1. Always to choose the chain with highest sum of commit votes.
2. If A and B has the same length, we choose the one with smaller hash.

Transaction Process Diagram

When a transaction is submitted, it is necessary to check the chain in the transaction. Transactions that are submitted externally or have been packaged into the block are somewhat different when doing validation.

New Transaction Process (from network, rpc)

Transactions submitted through an RPC or other node broadcast.

- Api SendRawTransaction Verification below steps when exist fail, then return err
- check whether fromAddr and toAddr is valid (tx proto verification)
- check len of Payload <= MaxDataPayLoadLength (tx proto verification)
- 0 < gasPrice <= TransactionMaxGasPrice and 0 < gasLimit <= TransactionMaxGas (tx proto verification)
- check Alg is SECP256K1 (tx proto verification)
- chainID Equals, Hash Equals, Sign verify??; fail and drop;

- check nonceOfTx > nonceOfFrom
- check Contract status is ExecutionSuccess if type of tx is TxPayloadCallType, check toAddr is equal to fromAddr if type of tx is TxPayloadDeployType
- Transaction pool Verification
- gasPrice >= minGasPriceOfTxPool & 0 < gasLimit <= maxGasLimitOfTxPool??; fail and drop;
- chainID Equals, Hash Equals, Sign verify??; fail and drop;

Transaction in Block Process

The transaction has been packaged into the block, and the transaction is verified after receiving the block.

- Packed
- Nonce Verification: nonceOfFrom +1 == nonceOfTx ??; nonceOfTx < nonceOfFrom +1 fail and drop, nonceOfTx > nonceOfFrom +1 fail and giveback to tx pool;
- check balance >= gasLimit * gasPrice ??; fail and drop;
- check gasLimit >= txBaseGas(MinGasCountPerTransaction + dataLen*GasCountPerByte) ??; fail and drop;
- check payload is valid ??; fail and submit; gasConsumed is txBaseGas (all txs passed the step tx will be on chain)
- check gasLimit >= txBaseGas + payloasBaseGas(TxPayloadBaseGasCount[payloadType]) ??;fail and submit; gasConsumed is txGasLimit
- check balance >= gasLimit * gasPrice + value ??;fail and submit; gasConsumed is txBaseGas + payloadsBaseGas
- transfer value from SubBalance and to AddBalance ??;fail and submit; gasConsumed is txBaseGas + payloadsBaseGas
- check gasLimit >= txBaseGas + payloadsBaseGas + gasExecution ??;fail and submit; gasConsumed is txGasLimit
- success submit gasConsumed is txBaseGas + payloadsBaseGas + gasExecution
- Verify
- check whether fromAddr and toAddr is valid (tx proto verification) ??; fail and submit;
- check len of Payload <= MaxDataPayLoadLength (tx proto verification) ??; fail and submit;
- 0 < gasPrice <= TransactionMaxGasPrice and 0 < gasLimit <= TransactionMaxGas (tx proto verification)
- check Alg is SECP256K1 (tx proto verification) ??; fail and submit;
- chainID Equals, Hash Equals, Sign verify??; fail and drop;

- Next steps like Transaction Packed in Block Process.

Event functionality

The `Event` functionality is used to make users or developers subscribe interested events. These events are generated during the execution of the blockchain, and they record the key execution steps and execution results of the chain. To query and verify the execution results of transactions and smart contracts, we record these two types of events into a trie and save them to the chain.

Event structure:

```
type Event struct {
    Topic string // event topic, subscribe keyword
    Data  string // event content, a json string
}
```

After a event is generated, it will be collected for processing in eventEmitter. Users can use the emitter subscription event. If the event is not subscribed, it will be discarded, and for the event that has been subscribed, the new event will be discarded because of the non-blocking mechanism, if the channel is not blocked in time.

Events list:

- TopicNewTailBlock
- TopicRevertBlock
- TopicLibBlock
- TopicPendingTransaction
- TopicTransactionExecutionResult
- EventNameSpaceContract

Event Reference

TopicNewTailBlock

This event occurs when the tail block of the chain is updated.

- Topic:`chain.newTailBlock`
- Data:
  - `height`: block height
  - `hash`: block hash
  - `parent_hash`: block parent hash

  - `acc_root`: account state root hash
  - `timestamp`: block timestamp
  - `tx`: transaction state root hash
  - `miner`: block miner

TopicRevertBlock

This event occurs when a block is revert on the chain.

- Topic:`chain.revertBlock`
- Data: The content of this topic is like TopicNewTailBlock data.

TopicLibBlock

This event occurs when the latest irreversible block change.

- Topic:`chain.latestIrreversibleBlock`
- Data: The content of this topic is like TopicNewTailBlock data.

TopicPendingTransaction

This event occurs when a transaction is pushed into the transaction pool.

- Topic:`chain.pendingTransaction`
- Data:
  - `chainID`: transaction chain id
  - `hash`: transaction hash
  - `from`: transaction from address string
  - `to`: transaction to address string
  - `nonce`: transaction nonce
  - `value`: transaction value
  - `timestamp`: transaction timestamp
  - `gasprice`: transaction gas price
  - `gaslimit`: transaction gas limit
  - `type`: trsnaction type

TopicTransactionExecutionResult

This event occurs when the end of a transaction is executed. This event will be recorded on the chain, and users can query with RPC interface GetEventsByHash.

This event records the execution results of the transaction and is very important.

- Topic:`chain.transactionResult`
- Data:
  - `hash`: transaction hash
  - `status`: transaction status, 0 failed, 1success, 2 pending
  - `gasUsed`: transaction gas used
  - `error`: transaction execution error. If the transaction is executed successfully, the field is empty.

EventNameSpaceContract

This event occurs when the contract is executed. When the contract is executed, the contract can record several events in the execution process. If the contract is successful, these events will be recorded on the chain and can be subscribed, and the event of the contract will not be recorded at the time of the failure. This event will also be recorded on the chain, and users can query with RPC interface GetEventsByHash.

- Topic:`chain.contract.[topic]` The topic of the contract event has a prefix `chain.contract.`, the content is defined by the contract writer.
- Data: The content of contract event is defined by contract writer.

Subscribe

All events can be subscribed and the cloud chain provides a subscription RPC interface Subscribe. It should be noted that the event subscription is a non-blocking mechanism. New events will be discarded when the RPC interface is not handled in time.

Query

Only events recorded on the chain can be queried using the RPC interface GetEventsByHash. Current events that can be queried include:

- TopicTransactionExecutionResult
- EventNameSpaceContract

Transaction Gas

In Nebulas, either a normal transaction which transfer balance or a smart contract deploy & call burns gas, and charged from the balance of `from` address. A transaction contains two gas parameters `gasPrice` and `gasLimit` :

- `gasPrice`: the price of per gas.
- `gasLimit`: the limit of gas use.

The actual gas consumption of a transaction is the value: `gasPrice` * `gasUsed`, which will be the reward to the miner coinbase. The `gasUsed` value must less than or equal to the `gasLimit`. Transaction's `gasUsed` can be estimate by RPC interface estimategas and store in transaction's execution result event.

Design reason

Users want to avoid gas costs when the transaction is packaged. Like Bitcoin and Ethereum, Nebulas GAS is used for transaction fee, it have two major purposes:

- As a rewards for minter, to incentive them to pack transactions. The packaging of the transaction costs the computing resources, especially the execution of the contract, so the user needs to pay for the transaction.
- As a cost for attackers. The DDOS attach is quite cheap in Internet, black hackers hijack user's computer to send large network volume to target server. In Bitcoin and Ethereum network, each transaction must be paid, that significant raise the cost of attack.

Gas constitution

When users submit a transaction, gas will be burned at these aspects:

- `transaction submition`
- `transaction data storage`
- `transaction payload addition`
- `transaction payload execution`(smart contract execution)

In all these aspects, the power and resources of the net will be consumed and the miners will need to be paid.

Transaction submition

A transaction's submition will add a transaction to the tail block. Miners use resources to record the deal and need to be paid. It will burn a fixed number of gas, that would be defined in code as the following:

```
// TransactionGas default gas for normal transaction
TransactionGas = 20000
```

If the transaction verifies failed, the gas and value transfer will rollback.

Transaction data storage

When deploying a contract or call contract's method, the raw data of contract execution save in the transaction's data filed, which cost the storage of resources on the chain. A formula to calculate gas:

```
TransactionDataGas = 1

len(data) * TransactionDataGas
```

The `TransactionDataGas` is a fixed number of gas defined in code.

Different types of transactions' payload have different gas consumption when executed. The types of transactions currently supported by nebulas are as follows:

- `binary`: The `binary` type of transaction allows users to attach binary data to transaction execution. These binary data do not do any processing when the transaction is executed.
  - The fixed number of gas defined **0**.
- `deploy & call`: The `deploy` and `call` type of transaction allows users to deploy smart contract on nebulas. Nebulas must start `nvm` to execute the contract, so these types of transction must paid for the nvm start.
  - The fixed number of gas defined **60**.

Transaction payload execution(Smart contract deploy & call)

The `binary` type of transaction do not do any processing when the transaction is executed, so the execution need not be paid.

When a smart contract deploys or call in transaction submition, the contract execution will consume miner's computer resources and may store data on the chain.

- **execution instructions**: Every contract execution cost the miner's computer resources, the v8 instruction counter calculates the execution instructions. The limit of execution instructions will prevent the excessive consumption of computer computing power and the generation of the death cycle.
- **contract storage**: The smart contract's `LocalContractStorage` which storage contract objects also burn gas. Only one gas per 32 bytes is consumed when stored(`set`/`put`), `get` or `delete` not burns gas.

The limit of **contract execution** is:

```
    gasLimit - TransactionGas - len(data) * TransactionDataGas -␣
↪TransactionPayloadGasCount[type]
```

Gas Count Matrix

The gas count matrix of smart contract execution

| Operator | Gas Count/Opt. | Description | | — | —: | :— | | Binary | 1 | Binary & logical operator | | Load | 2 | Load from memory | | Store | 2 | Save to memory | | Return | 2 | Return value, save to memory | | Call (inner) | 4 | Call functions in the same Smart Contract | | Call (external) | 100 | Call functions from other Smart Contract |

| Expression | Sample Code | Binary Opt. | Load Opt. | Store Opt. | Return Opt. | Call (inner) Opt. | Gas Count | | | | — | :— | —: | —: | —: | —: | —: | | CallExpression | a(x, y) | 0 | 0 | 1 | 1 | 1 | 8 | | | | AssignmentExpression | x&=y | 1 | 0 | 1 | 0 | 0 | 3 | | | | BinaryExpression | x==y | 1 | 0 | 0 | 1 | 0 | 3 | | | | UpdateExpression | x++ | 1 | 0 | 1 | 0 | 0 | 3 | | | | UnaryExpression | x+y | 1 | 0 | 0 | 1 | 0 | 3 | | | | LogicalExpression | x | | y | 1 | 0 | 0 | 1 | 0 | 3 | | MemberExpression | x.y | 0 | 1 | 0 | 1 | 0 | 4 | | | | NewExpression | new X() | 0 | 0 | 1 | 1 | 1 | 8 | | | | ThrowStatement | throw x | 0 | 0 | 0 | 1 | 1 | 6 | | | | MetaProperty | new.target | 0 | 1 | 0 | 1 | 0 | 4 | | | | ConditionalExpression | x?y:z | 1 | 0 | 0 | 1 | 0 | 3 | | | | YieldExpression | yield x | 0 | 0 | 0 | 1 | 1 | 6 | | | | Event | | 0 | 0 | 0 | 0 | 0 | 20 | | | | Storage | | 0 | 0 | 0 | 0 | 0 | 1 gas/bit | | |

Tips

In nebulas, the transaction pool of each node has a minimum and maximum `gasPrice` and maximum `gasLimit` value. If transaction's `gasPrice` is not in the range of the pool's `gasPrice` or the `gasLimit` greater than the pool's gasLimit the transaction will be refused.

Transaction pool gasPrice and gasLimit configuration:

- `gasPrice`
  - minimum: The minimum gasPrice can be set in the configuration file. If the minimum value is not configured, the default value is `1000000`(10^6).
  - maximum: The maximum gasPrice is `1000000000000`(10^12), transaction pool's maximum configuration and transaction's `gasPrice` can't be overflow.
- `gasLimit`
  - minimum: The transaction's minimum gasLimit must greater than zero.
  - maximum: The maximum gasPrice is `50000000000`(50*10^9), transaction pool's maximum configuration and transaction's `gasLimit` can't be overflow.

Logs

Introduction

Nebulas provides two kinds of logs: console log & verbose log.

Console Log

Console Log(CLog) is used to help you understand which job **Neb** is working on now, including start/stop components, receive new blocks on chain, do synchronization and so on.

- CLog will print all logs to stdout & log files both. You can check them in your standard output directly.

Nebulas console log statements

```
// log level can be `Info`,`Warning`,`Error`
logging.CLog().Info("")
```

Startup specifications

Nebulas start service should give a console log, the logs should before the service start. The log format just like this:

```
logging.CLog().Info("Starting xxx...")
```

Stopping specifications

Nebulas stop service should give a console log, the logs should before the service stoped. The log format just like this:

```
logging.CLog().Info("Stopping xxx...")
```

Verbose Log

Verbose Log(VLog) is used to help you understant how **Neb** works on current job, including how to verifiy new blocks, how to discover new nodes, how to mint and so on.

- VLog will print logs to log files only. You can check them in your log folders if needed.

What'r more, you can set your concerned level to VLog to filter informations. The level filter follows the priority as **Debug < Info < Warn < Error < Fatal.**

Hookers

By default, Function hookers & FileRotate hookers are added to CLog & VLog both.

FunctionNameHooker

FunctionHooker will append current caller's function name & code line to the loggers. The result looks like this,

> time="2018-01-03T20:20:52+08:00" level=info msg="node init success" file=net_service.go **func=p2p.NewNetManager line=137** node.listen="[0.0.0.0:10001]"

FileRotateHooker

FileRotateHooker will split logs into many smaller segments by time. By default, all logs will be rotated every 1 hour. The log folder looks like this,

> neb-2018010415.log neb-2018010416.log neb.log - > /path/to/neb-2018010415.log

If you have any suggestions about logs, please feel free to submit issues on our wiki repo. Thanks!

Nebulas Address Design

Nebulas address system is carefully designed. As you will see below, both account and smart contract address are strings starting with a "n", which could be thought of as our faith Nebulas/NAS.

Account Address

Similar to Bitcoin and Ethereum, Nebulas also adopts elliptic curve algorithm as its basic encryption algorithm for Nebulas accounts. The address is derived from **public key**, which is in turn derived from the **private key** that encrypted with user's **passphrase**.Also we have the checksum design aiming to prevent a user from sending *Nas* to a wrong user account accidentally due to entry of several incorrect characters.

The specific calculation formula is as follows:

```
1.  content = ripemd160(sha3_256(public key))
    length: 20 bytes
                          +--------+--------+------------------+
2.  checksum = sha3_256( |  0x19  +  0x57  |      content     |␣
↪)[:4]
                          +--------+--------+------------------+
    length: 4 bytes
```

```
                          +--------+---------+-----------------+------
↪------+
3.  address = base58( |    0x19   |  0x57   |      content      | ␣
↪checksum  | ïijL'
                          +--------+---------+-----------------+------
↪------+
    length: 35 chars
```

0x57 is a one-byte "type code" for account address, **0x19** is a one-byte fixed "padding"

At this stage, Nebulas just adopts the normal bitcoin base58 encoding schema. A valid address is like: *n1TV3sU6jyzR4rJ1D7jCAmtVGSntJagXZHC*

Smart Contract Address

Calculating contract address differs slightly from account, passphrase of contract sender is not required but address & nonce. For more information, please check smart contract and rpc.sendTransaction. Calculation formula is as follows:

```
1.  content = ripemd160(sha3_256(tx.from, tx.nonce))
    length: 20 bytes
                           +--------+--------+------------------+
2.  checksum = sha3_256( |  0x19   |  0x58  +      content      |␣
↪)[:4]
                           +--------+--------+------------------+
    length: 4 bytes

                        +--------+---------+-----------------+--------
↪----+
3.  address = base58( |  0x19   |  0x58   |      content      | ␣
↪checksum  | ïijL'
                        +--------+---------+-----------------+--------
↪----+
    length: 35 chars
```

0x58 is a one-byte "type code" for smart contract address, **0x19** is a one-byte fixed "padding"

A valid address is like: *n1sLnoc7j57YfzAVP8tJ3yK5a2i56QrTDdK*

DIP (TBD)

3.2 How to Develop

3.2.1 Contribution Guideline

The go-nebulas project welcomes all contributors. The process of contributing to the Go project may be different than many projects you are used to. This document is intended as a guide to help you through the contribution process. This guide assumes you have a basic understanding of Git and Go.

Becoming a contributor

Before you can contribute to the go-nebulas project you need to setup a few prerequisites.

Contributor License Agreement

TBD.

Preparing a Development Environment for Contributing

Setting up dependent tools

1. Go dependency management tool

dep is an (not-yet) official dependency management tool for Go. go-nebulas project use it to management all dependencies.

For more information, please visit https://github.com/golang/dep

2. Linter for Go source code

Golint is official linter for Go source code. Every Go source file in go-nebulas must be satisfied the style guideline. The mechanically checkable items in style guideline are listed in Effective Go and the CodeReviewComments wiki page.

For more information about Golint, please visit https://github.com/golang/lint.

3. XUnit output for Go Test

Go2xunit could convert go test output to XUnit compatible XML output used in Jenkins/Hudson.

Making a Contribution

Discuss your design

The project welcomes submissions but please let everyone know what you're working on if you want to change or add to the go-nebulas project.

Before undertaking to write something new for the go-nebulas, please file an issue (or claim an existing issue). Significant changes must go through the change proposal process before they can be accepted.

This process gives everyone a chance to validate the design, helps prevent duplication of effort, and ensures that the idea fits inside the goals for the language and tools. It also checks that the design is sound before code is written; the code review tool is not the place for high-level discussions.

Besides that, you can have an instant discussion with core developers in **developers** channel of Nebulas.IO on Slack.

Making a change

Getting Go Source

First you need to fork and have a local copy of the source checked out from the forked repository.

You should checkout the go-nebulas source repo inside your $GOPATH. Go to $GOPATH run the following command in a terminal.

```
$ mkdir -p src/github.com/nebulasio
$ cd src/github.com/nebulasio
$ git clone git@github.com:{your_github_id}/go-nebulas.git
$ cd go-nebulas
```

Contributing to the main repo

Most Go installations project use a release branch, but new changes should only be made based on the **develop** branch. (They may be applied later to a release branch as part of the release process, but most contributors won't do this themselves.) Before making a change, make sure you start on the **develop** branch:

```
$ git checkout develop
$ git pull
```

Make your changes

The entire checked-out tree is editable. Make your changes as you see fit ensuring that you create appropriate tests along with your changes. Test your changes as you go.

Copyright

Files in the go-nebulas repository don't list author names, both to avoid clutter and to avoid having to keep the lists up to date. Instead, your name will appear in the change log and in the CONTRIBUTORS file and perhaps the AUTHORS file. These files are automatically generated from the commit logs perodically. The AUTHORS file defines who âĂIJThe go-nebulas AuthorsâĂİâĂŤthe copyright holdersâĂŤare.

New files that you contribute should use the standard copyright header:

```
// Copyright (C) 2017 go-nebulas authors
//
// This file is part of the go-nebulas library.
//
// the go-nebulas library is free software: you can redistribute it␣
↪and/or modify
// it under the terms of the GNU General Public License as␣
↪published by
// the Free Software Foundation, either version 3 of the License, or
// (at your option) any later version.
//
// the go-nebulas library is distributed in the hope that it will␣
↪be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License
// along with the go-nebulas library.  If not, see <http://www.gnu.
↪org/licenses/>.
//
```

Files in the repository are copyright the year they are added. Do not update the copyright year on files that you change.

Goimports, Golint and Govet

Every Go source file in go-nebulas must pass Goimports, Golint and Govet check. Golint check the style mistakes, we should fix all style mistakes, including comments/docs. Govet reports suspicious constructs, we should fix all issues as well.

Run following command to check your code:

```
$ make fmt lint vet
```

lint.report text file is the Golint report, **vet.report** text file is the Govet report.

Testing

You've written test code, tested your code before sending code out for review, run all the tests for the whole tree to make sure the changes don't break other packages or programs:

```
$ make test
```

test.report text file or **test.report.xml** XML file is the testing report.

Commit your changes

The most importance of committing changes is the commit message. Git will open an editor for a commit message. The file will look like:

```
# Please enter the commit message for your changes. Lines starting
# with '#' will be ignored, and an empty message aborts the commit.
# On branch foo
# Changes not staged for commit:
#    modified:   editedfile.go
#
```

At the beginning of this file is a blank line; replace it with a thorough description of your change. The first line of the change description is conventionally a one-line summary of the change, prefixed by the primary affected package, and is used as the subject for code review email. It should complete the sentence "This change modifies Go to _." The rest of the description elaborates and should provide context for the change and explain what it does. Write in complete sentences with correct punctuation, just like for your comments in Go. If there is a helpful reference, mention it here. If you've fixed an issue, reference it by number with a # before it.

After editing, the template might now read:

```
math: improve Sin, Cos and Tan precision for very large arguments

The existing implementation has poor numerical properties for
large arguments, so use the McGillicutty algorithm to improve
accuracy above 1e10.

The algorithm is described at http://wikipedia.org/wiki/
↪McGillicutty_Algorithm

Fixes #159

# Please enter the commit message for your changes. Lines starting
```

```
# with '#' will be ignored, and an empty message aborts the commit.
# On branch foo
# Changes not staged for commit:
#    modified:   editedfile.go
#
```

The commented section of the file lists all the modified files in your client. It is best to keep unrelated changes in different commits, so if you see a file listed that should not be included, abort the command and move that file to a different branch.

The special notation "Fixes #159" associates the change with issue 159 in the go-nebulas issue tracker. When this change is eventually applied, the issue tracker will automatically mark the issue as fixed. (There are several such conventions, described in detail in the GitHub Issue Tracker documentation.)

Creating a Pull Request

For more information about creating a pull request, please refer to the Create a Pull Request in Github page.

3.2.2 How to debug Go-Nebulas project

ä¡IJèĂĚïijŽWenbo Liu aries.lwb@gmail.com, July 17, 2017

Go-NebulaséąźçŽőåIJřåİĂïijŽhttps://github.com/nebulasio/go-nebulas.git

çőĂäżŃ

è£ŹçŕĞç§■æŰĞå§žäžŐMac OSX åŠŇ Ubuntuçşżçż§ïijŇçőĂå■ŢäżŃçż■åęĆä¡ŢèřČèŕŢGo-NebulaséąźçŽőïijŇäÿżèęĄäżŃçż■äÿL'çğ■æŰźæşŢèřČèŕŢïijŽdlvåŚ¡äžd'èąŇèřČèŕŢïijŇGogland IDEèřČèŕŢïijŇäžěåŔŁVisual Studio CodeèřČèŕŢãĂĆ

èřČèŕŢåŹÍDelveåőL'èčĚ

åIJÍ Mac OSX äÿŁåőL'èčĚDelve

GoogleåőŸæŰźäÿžgolangçŽĎèřČèŕŢä¿Ňå■ŘçŤÍgdbïijŇä¡ĘæŸŕdelveæŸŕæŻť'åŘĹéĂĆçŽĎèřČèŕŢåŹĺïij NebulasãĂĆæŹőéĂŽçŽĎgoéąźçŽőæŸŕåŔŕäżěçŽĎïijŇåĚůä¡Şä¡ŞçŐřåřśæŸŕèřČèŕŢGo-NebulaséąźçŽőæŮűïijŇæŰ■çĆźæŮăæşŢåĄIJä¡ŔïijŇäijŽæřÿè£IJhangä¡ŔãĂĆæĹŚäžňå£ĚéążäžőgithubäÿŁäÿ binaryïijŇæ■ěéłď'åęĆäÿŃïijŽ

åĚĹçŤÍHomebrewåőL'èčĚæIJL'bugçŽĎDelveïijŽ

```
brew install go-delve/delve/delve
rm /usr/local/bin/dlv
```

åőL'èčĚæ■ď'æIJL'éŮőéćŸçŽĎDelveïijŇåĚűåőđåřśæŸŕäÿžäžĘèől'åőČåÿőæĹŚäžňåIJĺMacæIJžåŹĺäÿŁç■¿
certèŕĄäźęãĂĆåęĆæđIJä¡äèĞłåůśæĎ£æĎŘçźĄçŘŘçŽĎæL'ŃåŁĺåĹŻåžžèŕĄäźęïijŇäź§åŘŕäžěäÿ■çŤĺåőL'èčĚ
//github.com/derekparker/delve/blob/v0.12.2/Documentation/installation/
osx/install.mdçŽĎãĂŘCreate a self-signed certificateãĂŚãĂĆ
çňňäžŇæİąrmåŚ¡äžď'æŸŕäÿžäžĘåĹäéŹď'è£ŹäÿłæIJL'éŮőéćŸçŽĎdlv bina-
ryïijŇæĹŚäžňéIJĂèęĄäžŐæžŘçăĄçijŰèŕŚåĞžäÿĂäÿłæ■čçąőçŽĎçL'ĹæIJňïijŇåźűäÿŤåĹl'çŤĺHomebewäÿžæĺ
äÿŃè¡¡æžŘäžčçăĄ

```
mkdir -p /Users/xxx/go-delve/src/github.com/derekparker
cd /Users/xxx/go-delve/src/github.com/derekparker
git clone https://github.com/derekparker/delve.git
```

åĹŻåžžäÿĂäÿłäÿť'æŮűæŰĞäžűåď'źïijŇäžŐgithubäÿŃè¡¡äžčçăĄąãĂĆæşĺæĎŘæŰĞäžűåď'źäÿ■æăĞæşĺçžc
not foundãĂĆåĚűåőČéČĺåĹĘèŕůæäźæ■őèĞłåůśæIJžåŹĺçŐŕåćČèő¿ç¡őãĂĆ

çijŰèŕŚ

```
export GOPATH=/Users/xxx/go-delve
cd /Users/xxx/go-delve/src/github.com/derekparker/delve
make install
```

åžŤèŕěäijŽåĞžçŐřåęĆäÿŃæŔŘçď'žïijŇèąĺæŸŐçijŰèŕŚæĹŘåŁ§ïijŽ

```
scripts/gencert.sh || (echo "An error occurred when generating and␣
↪installing a new certicate"; exit 1)
go install -ldflags="-s" github.com/derekparker/delve/cmd/dlv
codesign -s "dlv-cert"  /Users/xxx/go-delve/bin/dlv
```

çĎűåŘŐcp /Users/liuwb/go-delve/bin/dlv/usr/local/bin/ïijŇæŁŁçijŰèŕŚåě¡çŽĎdlvæŃůèť'Iè£Ż/usr/local/b
debuggerãĂĆè¿ŞåĚěåŚ¡äžď'dlv versionïijŇåęĆæđIJèČ¡æ■čåÿÿè£ŘèąŇïijŇæŸ¿çď'žçL'ĹæIJňåŘůïijŇèŕť'æŸŐ

åIJĺ Ubuntu äÿŁåőL'èčĚDelve

åŕźäžŐUbuntuçşžçž§ïijŇåŘŕäžěçŻť'æŐěä¡£çŤĺäÿŃéIćçŽĎæŇĞäžď'åőL'èčĚDelveïijŽ

```
go get -u github.com/derekparker/delve/cmd/dlv
```

äÿŃè¡¡Go-NebulasåůěçĺŃäžčçăĄ

```
mkdir /Users/xxx/workspace/blockchain/src/github.com/nebulasio/
cd /Users/xxx/workspace/blockchain/src/github.com/nebulasio/
git clone https://github.com/nebulasio/go-nebulas.git
```

åĹŻåžžäÿĂäÿłäÿť'æŮűæŰĞäžűåď'źïijŇäžŐgithubäÿŃè¡¡äžčçăĄąãĂĆæşĺæĎŘæŰĞäžűåď'źäÿ■æăĞæşĺçžc

DelveåŚ¡äžď'èąŇèřČèŕŢ åęĆæđIJä¡ăäžěåL'■çŤĺgdbèřČèŕŢè£ĞCçĺŃåžŘïijŇåŕźdlvåŚ¡äžď'èąŇèřČèŕŢçŽ
//github.com/derekparker/delve/blob/master/Documentation/usage/dlv.md
è£ŹéĞŇåŘłäžŃçż■debugéČĺåĹĘãĂĆ

è¿ŞåĚěåęĆäÿŃåŚ¡äžď'è£ŻåĚèřČèŕŢ

```
export GOPATH=/Users/xxx/workspace/blockchain/
cd /Users/xxx/workspace/blockchain/
dlv debug github.com/nebulasio/go-nebulas/cmd/neb -- --config /
 ↪Users/xxx/workspace/blockchain/src/github.com/nebulasio/go-
 ↪nebulas/conf/default/config.conf
```

è£ŘèąŇæŮăèŕŕçŽĎèŕİïijŇäijŽè£ŻåĚědebug sessionïijŽ

```
Type 'help' for list of commands.
(dlv)
```

æĹŚäžňæL'ŞçőŮåIJĺnebçŽĎåĞ¡æŢřåĚěåŔčèő¿ç¡őæŰ■çĆźïijŇè¿ŞåĚěåŚ¡äžd'

```
(dlv) break main.neb
Breakpoint 1 set at 0x4ba6798 for main.neb() ./src/github.com/
 ↪nebulasio/go-nebulas/cmd/neb/main.go:80
(dlv)
```

dlvèřČèŕŢåŹĺæŔŘçd'žäžčçăĄåřĘåIJĺcmd/neb/main.goçŽĎèąŇåŔů80èąŇåĄIJä¡ŔïijŇæşĺæĎŔè£ŹæŮűne

```
(dlv) continue
> main.neb() ./src/github.com/nebulasio/go-nebulas/cmd/neb/main.
 ↪go:80 (hits goroutine(1):1 total:1) (PC: 0x4ba6798)
    75:         sort.Sort(cli.CommandsByName(app.Commands))
    76:
    77:         app.Run(os.Args)
    78:     }
    79:
=>  80:     func neb(ctx *cli.Context) error {
    81:         n, err := makeNeb(ctx)
    82:         if err != nil {
    83:             return err
    84:         }
    85:
```

æ§ěçIJŇåŔŸéĞŔïijŇåŔŕçŤĺprintåŚ¡äžd'ïijŽ

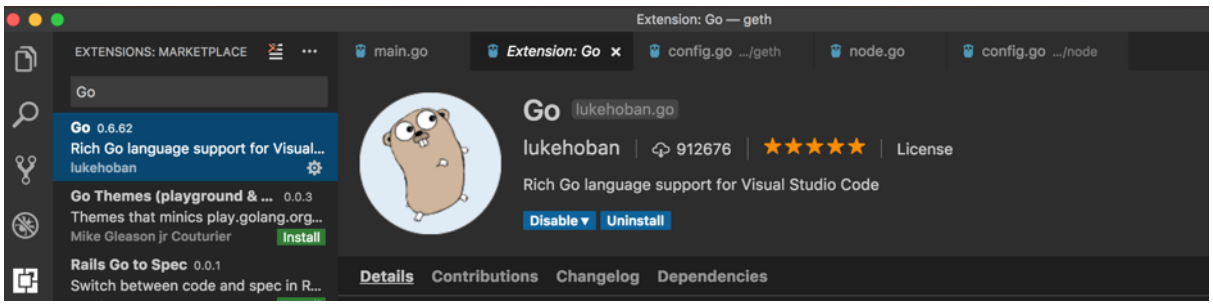
```
(dlv) print ctx
*github.com/nebulasio/go-nebulas/vendor/github.com/urfave/cli.
 ↪Context {
    App: *github.com/nebulasio/go-nebulas/vendor/github.com/urfave/
 ↪cli.App {
        Name: "neb",
        HelpName: "debug",
        Usage: "the go-nebulas command line interface",
        UsageText: "",
        ArgsUsage: "",
        Version: ", branch , commit ",
        Description: "",
        Commands: []github.com/nebulasio/go-nebulas/vendor/github.
 ↪com/urfave/cli.Command len: 11, cap: 18, [
```

```
            (*github.com/nebulasio/go-nebulas/vendor/github.com/
↪urfave/cli.Command)(0xc4201f4000),
            (*github.com/nebulasio/go-nebulas/vendor/github.com/
↪urfave/cli.Command)(0xc4201f4128),
            (*github.com/nebulasio/go-nebulas/vendor/github.com/
↪urfave/cli.Command)(0xc4201f4250),
            (*github.com/nebulasio/go-nebulas/vendor/github.com/
↪urfave/cli.Command)(0xc4201f4378),
            (*github.com/nebulasio/go-nebulas/vendor/github.com/
↪urfave/cli.Command)(0xc4201f44a0),
```

æŻť'åd'ŽæŁĂæIJŕèţĎæŰŹïijŇèŕůåŔĆèĂČ https://github.com/derekparker/delve/tree/master/Documentation/cli https://blog.gopheracademy.com/advent-2015/debugging-with-delve/ http://hustcat.github.io/getting-started-with-delve/

Visual Studio CodeèřČèŕţ

Visual Studio CodeæŸŕå¿ő è¡ŕåĚňåŔÿåŔŚåÿČçŽĎèůĺáźşåŔřäžčçăAçijŰè¿ŚåůěåĚůïijŇäÿŃè¡¡åIJřåİĂïijŽ //code.visualstudio.com/Download VS CodeéIJĂèęĄåőL'èčĚGoæŔŠäžű



æL'ŞåijĂæŰĞäžűåď'ź/Users/xxx/workspace/blockchain/src/github.com/nebulasio/go-nebulas/ïijŇåIJĺ.vscodeæŰĞäžűåď'źäÿŃåĹŽåžžäÿď'äÿłæŰĞäžűsettings.jsonåŠŇlaunch.jsonãĂĆ settings.jsonæŰĞäžűåĘĚåőźïijŽ

```
// Place your settings in this file to overwrite default and user␣
↪settings.
{
    "go.gopath": "/Users/xxx/workspace/blockchain/",
    "go.formatOnSave": true,
    "go.gocodeAutoBuild": false,
    "go.toolsGopath": "/Users/xxx/workspace/gotools",
    "explorer.openEditors.visible": 0,
}
```

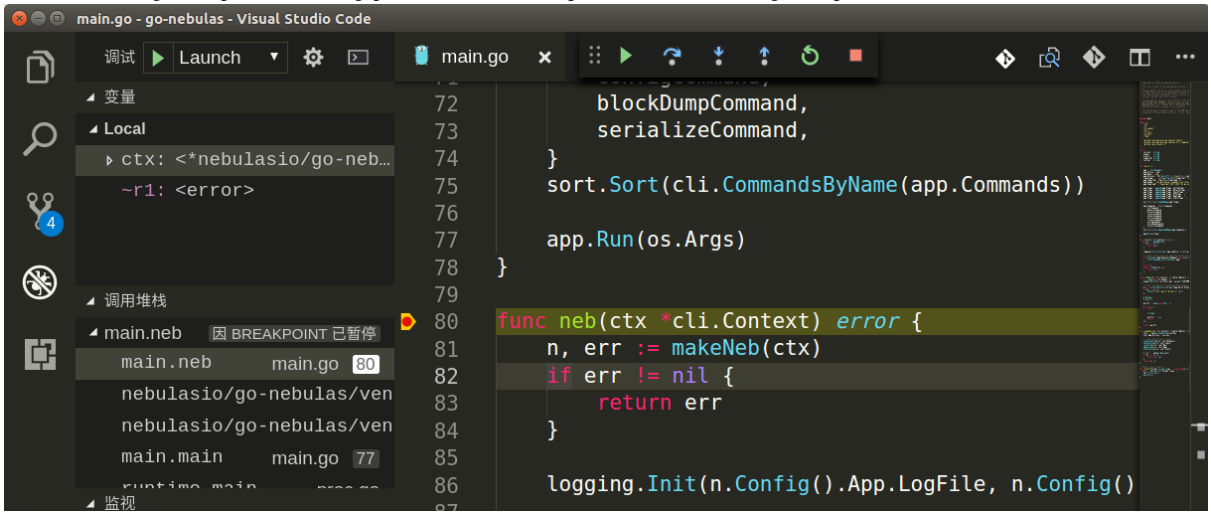
go.toolsGopathæŸŕanalysis toolsåőL'èčĚçŽĎåIJřåİĂïijŇåŔŕäžěæŇĞåőŽäÿžäžžä¡ŢçŽőå¡ŢïijŇè£ŹäžŽan toolsåŔŕäžěä¿ŽåĚűåőČworkspaceåĚšäžńãĂĆ

launch.jsonæŰĞäžűåĘĚåőźïijŽ

```
{
    "version": "0.2.0",
```

```
    "configurations": [
        {
            "name": "Launch",
            "type": "go",
            "request": "launch",
            "mode": "debug",
            "program": "${workspaceRoot}/cmd/neb",
            "env": {
                "GOPATH": "/Users/xxx/workspace/blockchain/"
            },
            "args": [
                "--config",
                "/Users/xxx/workspace/blockchain/src/github.com/
↪nebulasio/go-nebulas/conf/default/config.conf"
            ],
            "showLog": true
        }
    ]
}
```

åIJÍcmd/neb/main.goïijŇnebåĞ¡æŢřäÿ■èő¿ç¡őæÚ■çĆźïijŇF5è£ŘèąŇïijŇGo-NebulaséąźçŽőäijŽè£ŻèąŇçijÚèŕŚè£ŘèąŇïijŇåĄIJåIJÍæÚ■çĆźïijŽ



çĎűåŘŐïijŇåřšåŔŕäżěåijĂå£ČçŽĎåŘŕåŁÍNebulasäžčçăĄèřČèŕŢäźŃæŮĚïijĄ

3.2.3 debuging-with-gdb

OverView

Last week we found a lot of âĂIJFailed to update latest irreversible block.âĂİ in neb log with Leon. The reference code (nebulasio/go-nebulas/core/blockchain.go updateLatestIrreversibleBlock) ïijŇ in the code we found the cur variable is not equal to the tail variable , why? to find the cause, we try to use tool to dynamically display variable information and facilitate single-step debugging.

Goroutines

In c++ program we often use gbd to debug, so we think why not to use gdb to debug golang program . First we try to look up the BlockChain loop goroutine state and print the variables .

In c++ we all use `info threads` and thread x to show thread info but in the golang program ïijŇwe should use `info goroutines` and `goroutine xx bt` to displays the current list of running goroutines.

(gdb) `info goroutines` Undefined info command: "goroutines". Try "help info". (gdb) `source` /usr/local/go/src/runtime/runtime-gdb.py Loading Go Runtime support. (gdb) `info goroutines`

```
1 waiting  runtime.gopark
2 waiting  runtime.gopark
3 waiting  runtime.gopark
4 waiting  runtime.gopark
5 syscall  runtime.notetsleepg
6 syscall  runtime.notetsleepg
7 waiting  runtime.gopark
... ...
```

(gdb) goroutine 84 bt

```
#0 runtime.gopark (unlockf={void (struct runtime.g , void , bool␣
↪*)} 0xc420c57c80, lock=0x0, reason="select", traceEv=24 '\030',␣
↪traceskip=1) at /data/packages/go/src/runtime/proc.go:288
#1 0x0000000000440fd9 in runtime.selectgo (sel=0xc420c57f48, ~
↪r1=842353656960) at /data/packages/go/src/runtime/select.go:395
#2 0x0000000000ad2d73 in github.com/nebulasio/go-nebulas/core.
↪(*BlockChain).loop (bc=0xc4202c6320)at /neb/golang/src/github.com/
↪nebulasio/go-nebulas/core/blockchain.go:184
#3 0x0000000000460421 in runtime.goexit () at /data/packages/go/
↪src/runtime/asm_amd64.s:2337
#4 .....
```

But neb has too many goroutines, we donâĂŹt kown which one , we give up

BreakPoints

Second we try to set break point to debug

(gdb) `b blockchain.go:381`

Breakpoint 2 at 0xad4373: file /neb/golang/src/github.com/nebulasio/go-nebulas/core/blockchain.go, line 381.

(gdb) `b core/blockchain.go:390`

Breakpoint 3 at 0xad44c6: file /neb/golang/src/github.com/nebulasio/go-nebulas/core/blockchain.go, line 390.

(gdb) `info breakpoints` // show all breakpoints

(gdb) `d 2` //delete No 2 breakpoint

Now let the neb continue its execution until the next breakpoint, enter the c command: (gdb) `c` Continuing

```
Thread 6 "neb" hit Breakpoint 2, github.com/nebulasio/go-nebulas/
↪core.(*BlockChain).updateLatestIrreversibleBlock (bc=0xc4202c6320,
↪ tail=0xc4244198c0)
at /neb/golang/src/github.com/nebulasio/go-nebulas/core/blockchain.
↪go:382
382         miners := make(map[string
```

now we can use p(print) to print variables value

```
(gdb) `p cur`
$2 = (struct github.com/nebulasio/go-nebulas/core.Block *)␣
↪0xc420716f90
(gdb) `p cur.height`
$3 = 0
(gdb) `p bc`
$4 = (struct github.com/nebulasio/go-nebulas/core.BlockChain *)␣
↪0xc4202c6320
(gdb) `p bc.latestIrreversibleBlock`
$5 = (struct github.com/nebulasio/go-nebulas/core.Block *)␣
↪0xc4240bbb00
(gdb) `p bc.latestIrreversibleBlock.height`
$6 = 51743
(gdb) `p tail`
$7 = (struct github.com/nebulasio/go-nebulas/core.Block *)␣
↪0xc4244198c0
(gdb) `p tail.height`
$8 = 51749
```

now we can use `info goroutines` again, to find current goroutine. info goroutines with the * indicating the current execution, so we find the current goroutine nunmber quickly.

the next breakpoint we can use `c` command , so we found the cur and lib is not equal, because of length of the miners is less than ConsensusSizeïijŇ In the loop the cur change to the parent block .

Other

When compiling Go programs, the following points require particular attention:

- Using -ldflags "-s" will prevent the standard debugging information from being printed
- Using -gcflags "-N-l" will prevent Go from performing some of its automated optimizations -optimizations of aggregate variables, functions, etc. These optimizations can make it very difficult for GDB to do its job, so it's best to disable them at compile time using these flags.

References

- Debugging with GDB
- GDBèřČèŕŢGOçÍŃåžŔ

3.2.4 neb-dont-generate-coredump-file

OverView

During Testing, neb may be crash, and we want to get the coredump file which could help us to find the reason. However, neb don't generate coredump file by default. We can find the crash log in /var/log/apport.log when a crash occurred:

```
"called for pid 10110, signal 11, core limit 0, dump mode 1 "
```

The coredump file is very very important, it can serve as useful debugging aids in several situations, and help us to debug quickly. Therefore we should make neb to generate coredump file.

Set the core file size

We can use `ulimit -a` command to show core file size. If it's size is zero, which means coredump file is disabled, then we should set a value for core file size. for temporarily change we can use `ulimit -c unlimited` , and for permanently change we can edit `/etc/security/limits.conf` file, it will take effect after reboot or command `sysctl -p`.

```
<domain>     <type>     <item>         <value>
 * soft     core             unlimited
```

But these ways are't work, neb still can't generate coredump file and `cat /proc/$pid/limits` always "Max core file size 0"

Why? Why? Why? It doesn't Work

1. If the setting is wrong? Just try a c++ programe build, run it and we can find that it can generate coredump.
2. Neb is started by supervisord, is it caused by supervisordïij§
3. Try to start neb without supervisord, then the neb coredump is generated!
4. Yes, the reason is supervisord, then we can google "supervisord+coredump" to solve it.

Solution

Supervisord only set RLIMIT_NOFILE, RLIMIT_NOPROC by set_rlimits , others are seted default 0 1. modify supervisord code options.py in 1293 line

```
vim /usr/lib/python2.6/site-packages/supervisor/options.py

soft, hard = resource.getrlimit(resource.RLIMIT_CORE)
resource.setrlimit(resource.RLIMIT_CORE, (-1, hard))
```

1. restart supervisord and it works .

Other seetings

You can also change the name and path of coredump file by changing file `/proc/sys/kernel/core_pattern`:

```
echo "/neb/app/core-%e-%p-%t" > /proc/sys/kernel/core_pattern

%p: pid
%: '%' is dropped
%%: output one '%'
%u: uid
%g: gid
%s: signal number
%t: UNIX time of dump
%h: hostname
%e: executable filename
%: both are dropped
```

References

- supervisord coredump
- core_pattern

3.3 Tutorials

English 101

- Installation (thanks Victor)
- Sending a Transaction (thanks Victor)
- Writing Smart Contract in JavaScript (thanks otto)
- Introducing Smart Contract Storage (thanks Victor)
- Interacting with Nebulas by RPC API (thanks Victor)

äÿ■æŰĞ - åĚěéŮÍæŢŹçÍŃ

- çijŰèŕŚåőL'èčĚåŔŁè£ŘèąŇneb
- åIJÍæŸ§äžŚéŞ¿äÿŁåŔŚéĂĄäžd'æŸŞ
- ä¡£çŤÍJavaScriptçijŰåĘŹæŹžèČ¡åŘĹçžę
- æŹžèČ¡åŘĹçžęå■ŸåĆÍåŇžäżŃçż■
- éĂŽè£ĞRPCæŐěåŔčäÿŐæŸ§äžŚéŞ¿äžd'äžŠ

3.3.1 Nebulas 101 - 01 Compile and Install Nebulas

YouTube Tutorial

The project code for Nebulas has been released in several versions and tested to run locally. You can download the Nebulas source code to compile the private chain locally.

To learn about Nebulas, please read the Nebulas Non-Technical White Paper.

To learn about the technology, please read the Nebulas Technical White Paper and the Nebulas github code.

> Nebulas can only runs on Mac and Linux at this stage. The Windows version will be coming soon.

Golang Environment

Nebulas is implemented in Golang now.

| Components | Version | Description | | — | — | — | | Golang | > = 1.9.2 | The Go Programming Language |

Mac OSX

Homebrew is recommended for installing golang on Mac.

```
# install
brew install go

# environment variables
export GOPATH=/path/to/workspace
```

> Notice:GOPATH is a local golang working directory which could be decided by youself. After GOPATH is configured, your go projects need to be placed in GOPATH directory.

Linux

```
# download
wget https://dl.google.com/go/go1.9.3.linux-amd64.tar.gz

# extract
tar -C /usr/local -xzf go1.9.3.linux-amd64.tar.gz

# environment variables
export PATH=$PATH:/usr/local/go/bin
export GOPATH=/path/to/workspace
```

Compile Nebulas

Download

Clone source code with the following commands.

```
# enter workspace
mkdir -p $GOPATH/src/github.com/nebulasio
cd $GOPATH/src/github.com/nebulasio

# download
git clone https://github.com/nebulasio/go-nebulas.git

# enter repository
cd go-nebulas

# master branch is most stable
git checkout master
```

Install RocksDB

- **OS X**:
- Install rocksdb via Homebrew

```
brew install rocksdb
```

- **Linux - Ubuntu**
- Install Dependencies

```
apt-get update
apt-get -y install build-essential libgflags-dev libsnappy-dev␣
↪zlib1g-dev libbz2-dev liblz4-dev libzstd-dev
```

- Install rocksdb by source code:

```
git clone https://github.com/facebook/rocksdb.git
cd rocksdb && make shared_lib && make install-shared
```

- **Linux - Centos**
- Install Dependencies

```
yum -y install epel-release && yum -y update
yum -y install gflags-devel snappy-devel zlib-devel bzip2-devel␣
↪gcc-c++  libstdc++-devel
```

- Install rocksdb by source code:

```
git clone https://github.com/facebook/rocksdb.git
cd rocksdb & make shared_lib && make install-shared
```

Install Go Dependencies

Go dependencies in Go-Nebulas is managed by Dep.

| Components | Version | Description | | — | — | — |

Dep | > = 0.3.1 | Dep is a dependency management tool for Go. |

Install Dep

- **Mac OSX**
- Install Dep via Homebrew

```
brew install dep
brew upgrade dep
```

- **Linux**
- Install dep

```
cd /usr/local/bin/
wget https://github.com/golang/dep/releases/download/v0.3.2/dep-
↪linux-amd64
ln -s dep-linux-amd64 dep
```

Download Dependencies

Switch to the root directory of the project to download dependencies for Go-Nebulas:

```
cd $GOPATH/src/github.com/nebulasio/go-nebulas
make dep
```

`make dep` downloads lots of dependencies. It might take a long time to download for the first time. Some dependencies may fail to download. If you can not download, you can directly download the zipped dependency files generated by dep vendor.tar.gz and extract it to the nebulas root directory.

```
vendor.tar.gz
MD5: c2c1ff9311332f90e11fb81b48ca0984
```

Nebulas's NVM (Nebulas Virtual Machine) depends on the V8 JavaScript engine. We've built the v8 dependencies for Mac/Linux. Run the following commands to install them.

```
cd $GOPATH/src/github.com/nebulasio/go-nebulas
make deploy-v8
```

Build Neb

You can now build the executable for Nebulas after golang dependencies and V8 dependency packages is installed.

Build under the project root directory:

```
cd $GOPATH/src/github.com/nebulasio/go-nebulas
make build
```

Once the building is completeïijŇthere will be a executable file `neb` generated under the root directory.

```
shangshu at shangshudeMacBook-Pro in ~/workspace/blockchain/src/github.com/nebulasio/go-nebulas on master
› make build                                                                                    16:44
cd cmd/neb; go build -ldflags "-X main.version=1.0.1 -X main.commit=fbcdd8927b3ed5db9ccf889388bf8efb500d3357
 -X main.branch=master -X main.compileAt=`date +%s`" -o ../../neb-fbcdd8927b3ed5db9ccf889388bf8efb500d3357
cd cmd/crashreporter; go build -ldflags "-X main.version=1.0.1 -X main.commit=fbcdd8927b3ed5db9ccf889388bf8e
fb500d3357 -X main.branch=master -X main.compileAt=`date +%s`" -o ../../neb-crashreporter
rm -f neb
ln -s neb-fbcdd8927b3ed5db9ccf889388bf8efb500d3357 neb
```

Start NEB

Genesis Block

Before launching a new Nebulas chain, we have to define the configuration of genesis block.

Genesis Block Configuration

```
# Neb genesis text file. Scheme is defined in core/pb/genesis.proto.

meta {
# Chain identity
```

```
chain_id: 100
}

consensus {
dpos {
# Initial dynasty, including all initial miners
dynasty: [
[ miner address ],
...
]
}
}

# Pre-allocation of initial tokens
token_distribution [
{
address: [ allocation address ]
value: [ amount of allocation tokens ]
},
...
]
```

An example genesis.conf is located in `conf/default/genesis.conf`.

Configuration

Before getting a neb node started, we have to define the configuration of this node.

Neb Node Configuration

```
# Neb configuration text file. Scheme is defined in neblet/pb/
↪config.proto:Config.

# Network Configuration
network {
# For the first node in a new Nebulas chain, `seed` is not need.
# Otherwise, every node need some seed nodes to introduce it into␣
↪the Nebulas chain.
# seed: ["/ip4/127.0.0.1/tcp/8680/ipfs/
↪QmP7HDFcYmJL12Ez4ZNVCKjKedfE7f48f1LAkUc3Whz4jP"]

# P2p network service host. support mutiple ip and ports.
listen: ["0.0.0.0:8680"]

# The private key is used to generate a node ID. If you don't use␣
↪the private key, the node will generate a new node ID.
# private_key: "conf/network/id_ed25519"
}
```

```
# Chain Configuration
chain {
# Network chain ID
chain_id: 100

# Database storage location
datadir: "data.db"

# Accounts' keystore files location
keydir: "keydir"

# The genesis block configuration
genesis: "conf/default/genesis.conf"

# Signature algorithm
signature_ciphers: ["ECC_SECP256K1"]

# Miner address
miner: "n1SAQy3ix1pZj8MPzNeVqpAmu1nCVqb5w8c"

# Coinbase address, all mining reward received by the above miner␣
 ↪will be send to this address
coinbase: "n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE"

# The passphrase to miner's keystore file
passphrase: "passphrase"
}

# API Configuration
rpc {
# GRPC API port
rpc_listen: ["127.0.0.1:8684"]

# HTTP API port
http_listen: ["127.0.0.1:8685"]

# The module opened
http_module: ["api", "admin"]
}

# Log Configuration
app {
# Log level: [debug, info, warn, error, fatal]
log_level: "info"

# Log location
log_file: "logs"

# Open crash log
```

```
enable_crash_report: false
}

# Metrics Configuration
stats {
# Open node metrics
enable_metrics: false

# Influxdb configuration
influxdb: {
host: "http://localhost:8086"
db: "nebulas"
user: "admin"
password: "admin"
}
}
```

A lot of examples can be found in `$GOPATH/src/github.com/nebulasio/go-nebulas/conf/`

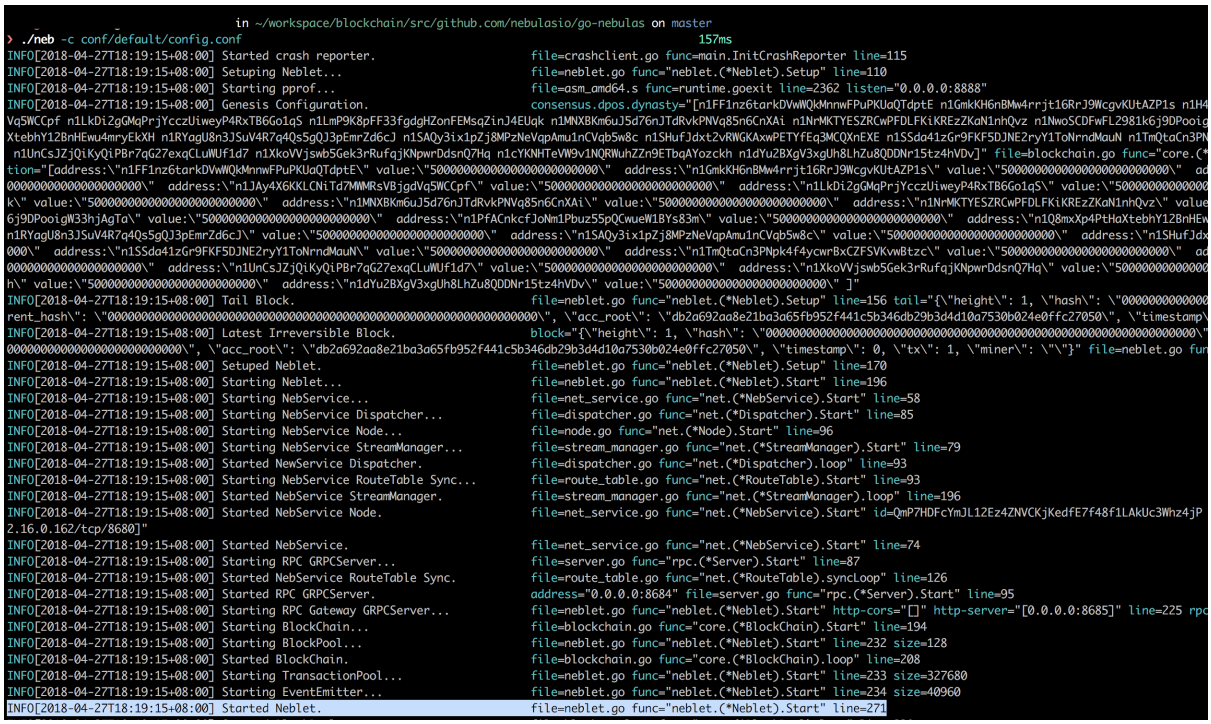
Run Nodes

> The Nebulas chain you are running at this point is private and is different with official Testnet and Mainnet.

Start your first Nebulas node with the following commands.

```
cd $GOPATH/src/github.com/nebulasio/go-nebulas
./neb -c conf/default/config.conf
```

After starting, the following should be visible in the terminal:



By default, the node using `conf/default/config.conf` won't mine new blocks. Start your first Nebulas mining node with another commands.

```
cd $GOPATH/src/github.com/nebulasio/go-nebulas
./neb -c conf/example/miner.conf
```

After the node starts, if the connection with the seed node is successful, you can see the following log which is in log file `logs/miner/neb.log`:

```
time="2018-03-29T20:50:38+08:00" level=info msg="Started Sync Service." file=sync_service.go func="sync.(*
Service).startLoop" line=150
time="2018-03-29T20:50:38+08:00" level=info msg="Started Dpos Mining." file=dpos.go func="dpos.(*Dpos).blo
ckLoop" line=619
time="2018-03-29T20:50:38+08:00" level=debug msg="Finished handshake." file=stream.go func="net.(*Stream).
onOk" line=610 stream="Peer Stream: QmP7HDFcYmJL12Ez4ZNVCKjKedfE7f48f1LAkUc3Whz4jP,/ip4/127.0.0.1/tcp/8680
"
time="2018-03-29T20:50:38+08:00" level=info msg="Enabled Dpos Mining..." file=dpos.go func="dpos.(*Dpos).E
nableMining" line=155
time="2018-03-29T20:50:38+08:00" level=info msg="Started Active Sync Task." file=blockchain.go func="core.
(*BlockChain).StartActiveSync" line=524 syncpoint="{\"height\": 1, \"hash\": \"0000000000000000000000000000
0000000000000000000000000000000000000\", \"parent_hash\": \"0000000000000000000000000000000000000000000000000
00000000000000000\", \"acc_root\": \"b58afe47c736957f7ab96dde946f539c2597555c7f8c2cd62eac4998d53fd08c\",
\"timestamp\": 0, \"tx\": 0, \"miner\": \"\"}"
```

Note: You can start many nodes locally. Please make sure the ports in your node configurations won't conflict with each other.

Next step: Tutorial 2

Sending Transactions on Nebulas

3.3.2 Nebulas 101 - 02 Sending Transactions on Nebulas

Youtube Tutorial

For this portion of the tutorial we will pick up where we left off in the Installation tutorial.

Nebulas provides three methods to send transactionsïijŽ

1. Sign & Send
2. Send with Passphrase
3. Unlock & Send

Here is an introduction to sending a transaction in Nebulas through the three methods above and verifying whether the transaction is successful.

Prepare Accounts

In Nebulas, each address represents an unique account.

Prepare two accounts: an address to send tokens (the sending address, called "from") and an address to receive the tokens (the receiving address, called "to").

The Sender

Here we will use the coinbase account in the `conf/example/miner.conf`, which is `n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE` as the sender. As the miner's coinbase account, it will receive some tokens as the mining reward. Then we could send these tokens to another account later.

The Receiver

Create a new wallet to receive the tokens.

```
$ ./neb account new
Your new account is locked with a passphrase. Please give a␣
↪passphrase. Do not forget this passphrase.
Passphrase:
Repeat passphrase:
Address: n1SQe5d1NKHYFMKtJ5sNHPsSPVavGzW71Wy
```

When you run this command you will have a different wallet address with `n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE`. Please use your generated address as the receiver.

The keystore file of the new wallet will be located in `$GOPATH/src/github.com/nebulasio/go-nebulas/keydir/`

Start the Nodes

Start Seed Node

Firstly, start a seed node as the first node in local private chain.

```
./neb -c conf/default/config.conf
```

Start Miner Node

Secondly, start a miner node connecting to the seed node. This node will generate new blocks in local private chain.

```
./neb -c conf/example/miner.conf
```

> **How long a new block will be minted?**
>
> In Nebulas, DPoS is chosen as the temporary consensus algorithm before Proof-of-Devotion(PoD, described in Technical White Paper) is ready. In this consensus algorithm, each miner will mint new block one by one every 15 seconds.
>
> In current context, we have to wait for 315(=15*21) seconds to get a new block because there is only one miner among 21 miners defined in `conf/default/genesis.conf` working now.

Once a new block minted by the miner, the mining reward will be added to the coinbase wallet address used in `conf/example/miner.conf` which is `n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE`.

Interact with Nodes

Nebulas provides developers with HTTP API, gRPC API and CLI to interact with the running nodes. Here, we will share how to send a transaction in three methods with HTTP API (API Module | Admin Module).

> The Nebulas HTTP Lisenter is defined in the node configuration. The default port of our seed node is `8685`.

At first, check the sender's balance before sending a transaction.

Check Account State

Fetch the state of sender's account `n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE` with `/v1/user/accountstate` in API Module using `curl`.

```
> curl -i -H Accept:application/json -X POST http://localhost:8685/
↪v1/user/accountstate -d '{"address":
↪"n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE"}'

{
    "result": {
        "balance": "670661800000000000000",
        "nonce": "0",
        "type": 87
    }
}
```

Note Type is used to check if this account is a smart contract account. `88` represents smart contract account and `87` means a non-contract account.

As we see, the receiver has been rewarded some tokens for mining new blocks.

Then let's check the receiver's account state.

```
> curl -i -H Accept:application/json -X POST http://localhost:8685/
↪v1/user/accountstate -d '{"address":"your_address"}'


{
    "result": {
        "balance": "0",
        "nonce": "0",
        "type": 87
    }
}
```

The new account doesn't have tokens as expected.

Send a Transaction

Now letâĂŹs send a transaction in three methods to transfer some tokens from the sender to the receiver!

Sign & Send

In this way, we can sign a transaction in an offline environment and then submit it to another online node. This is the safest method for everyone to submit a transaction without exposing your own private key to the Internet.

First, sign the transaction to get raw data.

```
> curl -i -H 'Content-Type: application/json' -X POST http://
 ↪localhost:8685/v1/admin/sign -d '{"transaction":{"from":
 ↪"n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE","to":
 ↪"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5", "value":
 ↪"1000000000000000000","nonce":1,"gasPrice":"1000000","gasLimit":
 ↪"2000000"}, "passphrase":"passphrase"}'

{"result":{"data":"CiAbjMP5dyVsTWILfXL1MbwZ8Q6xOgX/
 ↪JKinks1dpToSdxIaGVcH+WT/
 ↪SVMkY18ix7SG4F1+Z8evXJoA35caGhlXbip8PupTNxwV4SRM87r798jXWADXpWngIhAAAAAAAAAAAA
 ↪"}}
```

Note Nonce is an very important attribute in a transaction. It's designed to prevent replay attacks. For a given account, only after its transaction with nonce N is accepted, will its transaction with nonce N+1 be processed. Thus, we have to check the latest nonce of the account on chain before preparing a new transaction.

Then, send the raw data to an online Nebulas node.

```
> curl -i -H 'Content-Type: application/json' -X POST http://
 ↪localhost:8685/v1/user/rawtransaction -d '{"data":
 ↪"CiAbjMP5dyVsTWILfXL1MbwZ8Q6xOgX/JKinks1dpToSdxIaGVcH+WT/
 ↪SVMkY18ix7SG4F1+Z8evXJoA35caGhlXbip8PupTNxwV4SRM87r798jXWADXpWngIhAAAAAAAAAAAA
 ↪"}'

{"result":{"txhash":
 ↪"1b8cc3f977256c4d620b7d72f531bc19f10eb13a05ff24a8a792cd5da53a1277
 ↪","contract_address":""}}âŔŐ
```

Send with Passphrase

If you trust a Nebulas node so much that you can delegate your keystore files to it, the second method is a good fit for you.

First, upload your keystore files to the keydir folders in the trusted Nebulas node.

Then, send the transaction with your passphrase.

```
> curl -i -H 'Content-Type: application/json' -X POST http://
 ↪localhost:8685/v1/admin/transactionWithPassphrase -d '{
 ↪"transaction":{"from":"n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE","to":
 ↪"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5", "value":
 ↪"1000000000000000000","nonce":2,"gasPrice":"1000000","gasLimit":
 ↪"2000000"},"passphrase":"passphrase"}'

{"result":{"txhash":
 ↪"3cdd38a66c8f399e2f28134e0eb556b292e19d48439f6afde384ca9b60c27010
 ↪","contract_address":""}}
```

Note Because we have sent a transaction with nonce 1 from the account

`n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE`, new transaction with same `from` should be increased by 1, namely 2.

Unlock & Send

This is the most dangerous method. You probably shouldnâĂŹt use it unless you have complete trust in the receiving Nebulas node.

First, upload your keystore files to the keydir folders in the trusted Nebulas node.

Then unlock your accounts with your passphrase for a given duration in the node. The unit of the duration is nano seconds (300000000000=300s).

```
> curl -i -H 'Content-Type: application/json' -X POST http://
 ↪localhost:8685/v1/admin/account/unlock -d '{"address":
 ↪"n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE","passphrase":"passphrase",
 ↪"duration":"300000000000"}'

{"result":{"result":true}}
```

After unlocking the account, everyone is able to send any transaction directly within the duration in that node without your authorization.

```
> curl -i -H 'Content-Type: application/json' -X POST http://
 ↪localhost:8685/v1/admin/transaction -d '{"from":
 ↪"n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE","to":
 ↪"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5", "value":
 ↪"1000000000000000000","nonce":3,"gasPrice":"1000000","gasLimit":
 ↪"2000000"}'

{"result":{"txhash":
 ↪"8d69dea784f0edfb2ee678c464d99e155bca04b3d7e6cdba6c5c189f731110cf
 ↪","contract_address":""}}âŔŐ
```

Transaction Receipt

We'll get a `txhash` in three methods after sending a transaction successfully. The `txhash` value can be used to query the transaction status.

```
> curl -i -H Accept:application/json -X POST http://localhost:8685/
 ↪v1/user/getTransactionReceipt -d '{"hash":
 ↪"8d69dea784f0edfb2ee678c464d99e155bca04b3d7e6cdba6c5c189f731110cf
 ↪"}'

{"result":{"hash":
 ↪"8d69dea784f0edfb2ee678c464d99e155bca04b3d7e6cdba6c5c189f731110cf
 ↪","chainId":100,"from":"n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE","to":
 ↪"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5","value":"1000000000000000000
 ↪","nonce":"3","timestamp":"1524667888","type":"binary","data
 ↪":null,"gas_price":"1000000","gas_limit":"2000000","contract_
 ↪address":"","status":1,"gas_used":"20000"}}âŔŐ
```

The `status` fields may be 0, 1 or 2.

- **0: Failed.** It means the transaction has been submitted on chain but its execution failed.
- **1: Successful.** It means the transaction has been submitted on chain and its execution successeed.
- **2: Pending.** It means the transaction hasn't been packed into a block.

Double Check

Let's double check the receiver's balance.

```
> curl -i -H Accept:application/json -X POST http://localhost:8685/
↪v1/user/accountstate -d '{"address":
↪"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5"}'

{"result":{"balance":"30000000000000000000","nonce":"0","type":87}}
```

Here you should see a balance that is the total of all the successful transfers that you executed.

Next step: Tutorial 3

Write and run a smart contract with JavaScript

3.3.3 Nebulas 101 - 03 Write and run a smart contract

YouTube Tutorial

Through this tutorial we will learn how to write, deploy, and execute smart contracts in Nebulas.

Preparation

Before entering the smart contract, first review the previously learned content:

1. Install, compile and start neb application
2. Create a wallet address, setup coinbase, and start mining
3. Query neb node information, wallet address and balance
4. Send a transaction and verify the transaction was successful

If who have doubts about the above content you should go back to the previous chapters. So lets do this. We will learn and use smart contracts through the following steps:

1. Write a smart contract

2. Deploy the smart contract
3. Call the smart contract, and verify the contract execution results

Write a smart contract

Like Ethereum, Nebulas implements NVM virtual machines to run smart contracts, and the NVM implementation uses the JavaScript V8 engine, so for the current development we can write smart contracts using JavaScript and TypeScript.

Write a brief specification of a smart contract:

1. The Smart contract code must be a Prototype object;
2. The Smart contract code must have a init() method, this method will only be executed once during deployment;
3. The private methods in Smart contract must be prefixed with _ , and the private method cannot be a be directly called outside of the contract;

Below we use JavaScript to write the first smart contract: bank safe. This smart contract needs to fulfill the following functions:

1. The user can save money from this bank safe.
2. Users can withdraw money from this bank safe.
3. Users can check the balance in the bank safe.

Smart contract example:

```
'use strict';

var DepositeContent = function (text) {
  if (text) {
    var o = JSON.parse(text);
    this.balance = new BigNumber(o.balance);
    this.expiryHeight = new BigNumber(o.expiryHeight);
  } else {
    this.balance = new BigNumber(0);
    this.expiryHeight = new BigNumber(0);
  }
};

DepositeContent.prototype = {
  toString: function () {
    return JSON.stringify(this);
  }
};

var BankVaultContract = function () {
  LocalContractStorage.defineMapProperty(this, "bankVault", {
    parse: function (text) {
      return new DepositeContent(text);
```

```
    },
    stringify: function (o) {
      return o.toString();
    }
  });
};

// save value to contract, only after height of block, users can␣
↪takeout
BankVaultContract.prototype = {
  init: function () {
    //TODO:
  },

  save: function (height) {
    var from = Blockchain.transaction.from;
    var value = Blockchain.transaction.value;
    var bk_height = new BigNumber(Blockchain.block.height);

    var orig_deposit = this.bankVault.get(from);
    if (orig_deposit) {
      value = value.plus(orig_deposit.balance);
    }

    var deposit = new DepositeContent();
    deposit.balance = value;
    deposit.expiryHeight = bk_height.plus(height);

    this.bankVault.put(from, deposit);
  },

  takeout: function (value) {
    var from = Blockchain.transaction.from;
    var bk_height = new BigNumber(Blockchain.block.height);
    var amount = new BigNumber(value);

    var deposit = this.bankVault.get(from);
    if (!deposit) {
      throw new Error("No deposit before.");
    }

    if (bk_height.lt(deposit.expiryHeight)) {
      throw new Error("Can not takeout before expiryHeight.");
    }

    if (amount.gt(deposit.balance)) {
      throw new Error("Insufficient balance.");
    }

    var result = Blockchain.transfer(from, amount);
```

```
    if (!result) {
      throw new Error("transfer failed.");
    }
    Event.Trigger("BankVault", {
      Transfer: {
        from: Blockchain.transaction.to,
        to: from,
        value: amount.toString()
      }
    });

    deposit.balance = deposit.balance.sub(amount);
    this.bankVault.put(from, deposit);
  },
  balanceOf: function () {
    var from = Blockchain.transaction.from;
    return this.bankVault.get(from);
  },
  verifyAddress: function (address) {
    // 1-valid, 0-invalid
    var result = Blockchain.verifyAddress(address);
    return {
      valid: result == 0 ? false : true
    };
  }
};
module.exports = BankVaultContract;
```

As you can see from the smart contract example above, `BankVaultContract` is a prototype object that has an init() method. It satisfies the most basic specification for writing smart contracts that we have described before. BankVaultContract implements two other methods:

- save(): The user can save money to the bank safe by calling the save() method;
- takeout(): Users can withdraw money from bank safe by calling takeout() method;
- balanceOf(): The user can check the balance with the bank vault by calling the balanceOf() method;

The contract code above uses the built-in `Blockchain` object and the built-in `BigNumber()` method. Let's break down the parsing contract code line by line:

save():

```
// Deposit the amount into the safe

save: function (height) {
  var from = Blockchain.transaction.from;
  var value = Blockchain.transaction.value;
  var bk_height = new BigNumber(Blockchain.block.height);

  var orig_deposit = this.bankVault.get(from);
```

```
  if (orig_deposit) {
    value = value.plus(orig_deposit.balance);
  }
  var deposit = new DepositeContent();
  deposit.balance = value;
  deposit.expiryHeight = bk_height.plus(height);

  this.bankVault.put(from, deposit);
},
```

takeout ():

```
takeout: function (value) {
  var from = Blockchain.transaction.from;
  var bk_height = new BigNumber(Blockchain.block.height);
  var amount = new BigNumber(value);

  var deposit = this.bankVault.get(from);
  if (!deposit) {
    throw new Error("No deposit before.");
  }

  if (bk_height.lt(deposit.expiryHeight)) {
    throw new Error("Can not takeout before expiryHeight.");
  }

  if (amount.gt(deposit.balance)) {
    throw new Error("Insufficient balance.");
  }

  var result = Blockchain.transfer(from, amount);
  if (!result) {
    throw new Error("transfer failed.");
  }
  Event.Trigger("BankVault", {
    Transfer: {
      from: Blockchain.transaction.to,
      to: from,
      value: amount.toString()
    }
  });

  deposit.balance = deposit.balance.sub(amount);
  this.bankVault.put(from, deposit);
},
```

Deploy smart contracts

The above describes how to write a smart contract in Nebulas, and now we need to deploy the smart contract to the chain. Earlier, we have introduced how to make a transaction in Nebulas, and we used the sendTransaction() interface to initiate a transfer. Deploying a smart contract in Nebulas is actually achieved by sending a transaction by calling the sendTransaction() interface, just with different parameters.

```
// transaction - from, to, value, nonce, gasPrice, gasLimit,␣
↪contract
sendTransactionWithPassphrase(transaction, passphrase)
```

We have a convention that if `from` and `to` are the same address, `contract` is not null and `binary` is null, we assume that we are deploying a smart contract.

- `from`: the creator's address
- `to`: the creator's address
- `value`: it should be `"0"` when deploying the contract;
- `nonce`: it should be 1 more than the current nonce in the creator's account state, which can ben obtained via `GetAccountState`.
- `gasPrice`: The gasPrice used to deploy the smart contract, which can be obtained via `GetGasPrice`, or using default values: `"1000000"`;
- `gasLimit`: The gasLimit for deploying the contract. You can get the estimated gas consumption for the deployment via `EstimateGas`, and cannot use the default value. And you could also set a larger value. The actual gas consumption is decided by the deployment execution.
- `contract`: the contract information, the parameters passed in when the contract is deployed
  - `source`: contract code
  - `sourceType`: Contract code type, `js` and `ts` (corresponding to javaScript and typeScript code)
  - `args`: parameters for the contract initialization method. Use empty string if there is no parameter, and use JSON array if there is a parameter.

Detailed Interface Documentation API.

Example of deploying a smart contract using curl:

```
> curl -i -H 'Accept: application/json' -X POST http://
↪localhost:8685/v1/admin/transactionWithPassphrase -H 'Content-
↪Type: application/json' -d '{"transaction": {"from":
↪"n1H4MYms9F55ehcvygwWE71J8tJC4CRr2so","to":
↪"n1H4MYms9F55ehcvygwWE71J8tJC4CRr2so", "value":"0","nonce":1,
↪"gasPrice":"1000000","gasLimit":"2000000","contract":{"source":"\
↪"use strict\";var DepositeContent=function(text){if(text){var␣
↪o=JSON.parse(text);this.balance=new BigNumber(o.balance);this.
↪expiryHeight=new BigNumber(o.expiryHeight);}else{this.balance=new␣
↪BigNumber(0);this.expiryHeight=new BigNumber(0);}};
↪DepositeContent.prototype={toString:function(){return JSON.
↪stringify(this);}};var BankVaultContract=function()
↪{LocalContractStorage.defineMapProperty(this,\"bankVault\",
↪{parse:function(text){return new DepositeContent(text);}
```

```
{"result":{"txhash":
↪"aaebb86d15ca30b86834efb600f82cbcaf2d7aaffbe4f2c8e70de53cbed17889
↪","contract_address":"n1rVLTRxQEXscTgThmbTnn2NqdWFEKwpYUM"}}
```

The return value for deploying a smart contract is the transaction's hash address `txhash` and the contract's deployment address `contract_address`. Get the return value does not guarantee the successful deployment of the contract, because the sendTransaction () is an asynchronous process, which need to be packaged by the miner. Just as the previous transfer transaction, the transfer does not arrive in real time, it depends on the speed of the miner packing. Therefore we need to wait for a while (about 1 minute), then you can verify whether the contract is deployed successfully by querying the contract address or calling this smart contract.

Verify the deployment of the contract is successful

Check the receipt of the deploy transaction via `GetTransactionReceipt` to verify whether the contract has been deployed successfully.

```
> curl -i -H 'Content-Type: application/json' -X POST http:/
↪/localhost:8685/v1/user/getTransactionReceipt -d '{"hash":
↪"aaebb86d15ca30b86834efb600f82cbcaf2d7aaffbe4f2c8e70de53cbed17889
↪"}'

{"result":{"hash":
↪"aaebb86d15ca30b86834efb600f82cbcaf2d7aaffbe4f2c8e70de53cbed17889
↪","chainId":100,"from":
↪"n1H4MYms9F55ehcvygwWE71J8tJC4CRr2so","to":
↪"n1H4MYms9F55ehcvygwWE71J8tJC4CRr2so","value":"0","nonce":
↪"1","timestamp":"1524711841","type":"deploy","data":
↪"eyJTb3VyY2VUeXBlIjoianMiLCJTb3VyY2UiOiJcInVzZSBzdHJpY3RcIjt2YXIgRGVwb3Npc
↪ZmFsc2U6dHJ1ZX07fX07bW9kdWxlLmV4cG9ydHM9QmFua1ZhdWx0Q29udHJhY3Q7IiwiQXJncy
↪","gas_price":"1000000","gas_limit":"2000000","contract_
↪address":"n1rVLTRxQEXscTgThmbTnn2NqdWFEKwpYUM","status":1,
↪"gas_used":"22016"}}
```

As shown above, the status of the deploy transaction becomes 1. It means the contract has been deployed successfully.

Execute Smart Contract Method

The way to execute a smart contract method in Nebulas is also straightforward, using the sendTransactionWithPassphrase() method to invoke the smart contract method directly.

```
// transaction - from, to, value, nonce, gasPrice, gasLimit,␣
↪contract
sendTransactionWithPassphrase(transaction, passphrase)
```

- `from`: the user's account address
- `to`: the smart contract address

- `value`: The amount of money used to transfer by smart contract.
- `nonce`: it should be 1 more than the current nonce in the creator's account state, which can ben obtained via `GetAccountState`.
- `gasPrice`: The gasPrice used to deploy the smart contract, which can be obtained via `GetGasPrice`, or using default values `"1000000"`;
- `gasLimit`: The gasLimit for deploying the contract. You can get the estimated gas consumption for the deployment via `EstimateGas`, and cannot use the default value. And you could also set a larger value. The actual gas consumption is decided by the deployment execution.
- `contract`: the contract information, the parameters passed in when the contract is deployed
  - `function`:the contract method to be called
  - `args`: parameters for the contract initialization method. Use empty string if there is no parameter, and use JSON array if there is a parameter.

For example, execute save() method of the smart contract:

```
> curl -i -H 'Accept: application/json' -X POST http://
 ↪localhost:8685/v1/admin/transactionWithPassphrase -H 'Content-
 ↪Type: application/json' -d '{"transaction":{"from":
 ↪"n1LkDi2gGMqPrjYcczUiweyP4RxTB6Go1qS","to":
 ↪"n1rVLTRxQEXscTgThmbTnn2NqdWFEKwpYUM", "value":"100","nonce":1,
 ↪"gasPrice":"1000000","gasLimit":"2000000","contract":{"function":
 ↪"save","args":"[0]"}}, "passphrase": "passphrase"}'

{"result":{"txhash":
 ↪"5337f1051198b8ac57033fec98c7a55e8a001dbd293021ae92564d7528de3f84
 ↪","contract_address":""}}
```

Verify the execution of the contract method `save` is successful Executing a contract method is actually submitting a transaction on chain as well. We can verify the result through checking the receipt of the transaction via `GetTransactionReceipt`.

```
> curl -i -H 'Content-Type: application/json' -X POST http:/
 ↪/localhost:8685/v1/user/getTransactionReceipt -d '{"hash":
 ↪"5337f1051198b8ac57033fec98c7a55e8a001dbd293021ae92564d7528de3f84
 ↪"}'

{"result":{"hash":
 ↪"5337f1051198b8ac57033fec98c7a55e8a001dbd293021ae92564d7528de3f84
 ↪","chainId":100,"from":
 ↪"n1LkDi2gGMqPrjYcczUiweyP4RxTB6Go1qS","to":
 ↪"n1rVLTRxQEXscTgThmbTnn2NqdWFEKwpYUM","value":"100","nonce
 ↪":"1","timestamp":"1524712532","type":"call","data":
 ↪"eyJGdW5jdGlvbiI6InNhdmUiLCJBcmdzIjoiWzBdIn0=","gas_price
 ↪":"1000000","gas_limit":"2000000","contract_address":"",
 ↪"status":1,"gas_used":"20361"}}
```

As shown above, the status of the transaction becomes 1. It means the contract method has been executed successfully.

Execute the smart contract takeout() method:

```
> curl -i -H 'Accept: application/json' -X POST http://
 ↪localhost:8685/v1/admin/transactionWithPassphrase -H 'Content-
 ↪Type: application/json' -d '{"transaction":{"from":
 ↪"n1LkDi2gGMqPrjYcczUiweyP4RxTB6Go1qS","to":
 ↪"n1rVLTRxQEXscTgThmbTnn2NqdWFEKwpYUM", "value":"0","nonce":2,
 ↪"gasPrice":"1000000","gasLimit":"2000000","contract":{"function":
 ↪"takeout","args":"[50]"}}, "passphrase": "passphrase"}'

{"result":{"txhash":
 ↪"46a307e9beb21f52992a7512f3705fe58ee6c1887122a1b52f5ce5fd5f536a91
 ↪","contract_address":""}}
```

Verify the execution of the contract method `takeout` is successful In the execution of the above contract method `save`, we save 100 NAS into the smart contract `n1rVLTRxQEXscTgThmbTnn2NqdWFEKwpYUM`. Using the contract method `takeout`, we'll withdrawn 50 NAS from the 100 NAS. The balance of the smart contract should be 50 NAS now.

```
> curl -i -H 'Content-Type: application/json' -X POST http:/
 ↪/localhost:8685/v1/user/accountstate -d '{"address":
 ↪"n1rVLTRxQEXscTgThmbTnn2NqdWFEKwpYUM"}'

{"result":{"balance":"50","nonce":"0","type":88}}
```

The result is as expected.

Query Smart Contract Data

In a smart contract, the execution of some methods won't change anything on chain. These methods are designed to help us query data in readonly mode from blockchains. In Nebulas, we provide an API `call` for users to execute these readonly methods.

```
// transaction - from, to, value, nonce, gasPrice, gasLimit,␣
 ↪contract
call(from, to, value, nonce, gasPrice, gasLimit, contract)
```

The parameters of `call` is the same as the parameters of executing a contract method .

Call the smart contract method `balanceOf`:

```
> curl -i -H 'Accept: application/json' -X POST http://
 ↪localhost:8685/v1/user/call -H 'Content-Type: application/json' -
 ↪d '{"from":"n1LkDi2gGMqPrjYcczUiweyP4RxTB6Go1qS","to":
 ↪"n1rVLTRxQEXscTgThmbTnn2NqdWFEKwpYUM","value":"0","nonce":3,
 ↪"gasPrice":"1000000","gasLimit":"2000000","contract":{"function":
 ↪"balanceOf","args":""}}'
```

```
{"result":{"result":"{\"balance\":\"50\",\"expiryHeight\":\"84\"}",
↪"execute_err":"","estimate_gas":"20209"}}
```

Next step: Tutorial 4

Smart Contract Storage

3.3.4 Nebulas 101 - 04 Smart Contract Storage

YouTube Tutorial

Earlier we covered how to write smart contracts and how to deploy and invoke smart contracts in the Nebulas.

Now we introduce in detail the storage of the smart contract. Nebulas smart contracts provide on-chain data storage capabilities. Similar to the traditional key-value storage system (eg: redis), smart contracts can be stored on the Nebulas by paying with (gas).

LocalContractStorage

Nebulas' Smart Contract environment has built-in storage object `LocalContractStorage`, which can store numbers, strings, and JavaScript objects. The stored data can only be used in smart contracts. Other contracts can not read the stored data.

Basics

The `LocalContractStorage` API includes `set`, `get` and `del`, which allow you to store, read, and delete data. Storage can be numbers, strings, objects

Storing `LocalContractStorage` DataïijŽ

```
// store data. The data will be stored as JSON strings
LocalContractStorage.put(key, value);
// Or
LocalContractStorage.set(key, value);
```

Reading `LocalContractStorage` DataïijŽ

```
// get the value from key
LocalContractStorage.get(key);
```

Deleting `LocalContractStorage` DataïijŽ

```
// delete data, data can not be read after deletion
LocalContractStorage.del(key);
// Or
LocalContractStorage.delete(key);
```

Examples:

```
'use strict';

var SampleContract = function () {
};

SampleContract.prototype = {
    init: function () {
    },
    set: function (name, value) {
        // Storing a string
        LocalContractStorage.set("name",name);
        // Storing a number (value)
        LocalContractStorage.set("value", value);
        // Storing an objects
        LocalContractStorage.set("obj", {name:name, value:value});
    },
    get: function () {
        var name = LocalContractStorage.get("name");
        console.log("name:" + name)
        var value = LocalContractStorage.get("value");
        console.log("value:" + value)
        var obj = LocalContractStorage.get("obj");
        console.log("obj:" + JSON.stringify(obj))
    },
    del: function () {
        var result = LocalContractStorage.del("name");
        console.log("del result:" + result)
    }
};

module.exports = SampleContract;
```

Advanced

In addition to the basic `set`, `get`, and `del` methods, `LocalContractStorage` also provides methods to bind properties of smart contracts. We could read and write binded properties directly without invoking `LocalContractStorage` interfaces to `get` and `set`.

Binding Properties

Object instance, field name and descriptor should be provided to bind properties.

Binding Interface

```
// define a object property named `fieldname` to `obj` with␣
↪descriptor.
// default descriptor is JSON.parse/JSON.stringify descriptor.
// return this.
defineProperty(obj, fieldName, descriptor);

// define object properties to `obj` from `props`.
// default descriptor is JSON.parse/JSON.stringify descriptor.
// return this.
defineProperties(obj, descriptorMap);
```

Here is an example to bind properties in a smart contract.

```
'use strict';

var SampleContract = function () {
    // The SampleContract `size` property is a storage property.␣
↪Reads and writes to` size` will be stored on the chain.
    // The `descriptor` is set to null here, the default JSON.
↪stringify () and JSON.parse () will be used.
    LocalContractStorage.defineMapProperty(this, "size");

    // The SampleContract `value` property is a storage property.␣
↪Reads and writes to` value` will be stored on the chain.
    // Here is a custom `descriptor` implementation, storing as a␣
↪string, and returning Bignumber object during parsing.
    LocalContractStorage.defineMapProperty(this, "value", {
        stringify: function (obj) {
            return obj.toString();
        },
        parse: function (str) {
            return new BigNumber(str);
        }
    });
    // Multiple properties of SampleContract are set as storage␣
↪properties in batches, and the corresponding descriptors use JSON␣
↪serialization by default
    LocalContractStorage.defineProperties(this, {
        name: null,
        count: null
    });
};

module.exports = SampleContract;
```

Then, we can read and write these properties directly as the following example.

```
SampleContract.prototype = {
    // Used when the contract first deploys, can not be used a␣
↪second after the first deploy.
    init: function (name, count, size, value) {
        // Store the data on the chain when deploying the contract
        this.name = name;
        this.count = count;
        this.size = size;
        this.value = value;
    },
    testStorage: function (balance) {
        // value will be read from the storage data on the chain,␣
↪and automatically converted to Bignumber set according to the␣
↪descriptor
        var amount = this.value.plus(new BigNumber(2));
        if (amount.lessThan(new BigNumber(balance))) {
            return 0
        }
    }
};
```

Binding Map Properties

What's more, `LocalContractStorage` also provides methods to bind map properties. Here is an example to bind map properties and use them in a smart contract.

```
'use strict';

var SampleContract = function () {
    // Set `SampleContract`'s property to `userMap`. Map data then␣
↪can be stored onto the chain using `userMap`
    LocalContractStorage.defineMapProperty(this, "userMap");

    // Set `SampleContract`'s property to `userBalanceMap`, and␣
↪custom define the storing and serializtion reading functions.
    LocalContractStorage.defineMapProperty(this, "userBalanceMap", {
        stringify: function (obj) {
            return obj.toString();
        },
        parse: function (str) {
            return new BigNumber(str);
        }
    });

    // Set `SampleContract`'s properties to mulitple map batches
    LocalContractStorage.defineMapProperties(this,{
        key1Map: null,
        key2Map: null
```

```
    });
};

SampleContract.prototype = {
    init: function () {
    },
    testStorage: function () {
        // Store the data in userMap and serialize the data onto␣
↪the chain
        this.userMap.set("robin","1");
        // Store the data into userBalanceMap and save the data␣
↪onto the chain using a custom serialization function
        this.userBalanceMap.set("robin",new BigNumber(1));
    },
    testRead: function () {
        //Read and store data
        var balance = this.userBalanceMap.get("robin");
        this.key1Map.set("robin", balance.toString());
        this.key2Map.set("robin", balance.toString());
    }
};

module.exports = SampleContract;
```

Iterate Map

In contract, map does't support iterator. if you need to iterate the map, you can use the following way: define two map, arrayMap, dataMap, arrayMap with a strictly increasing counter as key, dataMap with data key as key.

```
"use strict";

var SampleContract = function () {
   LocalContractStorage.defineMapProperty(this, "arrayMap");
   LocalContractStorage.defineMapProperty(this, "dataMap");
   LocalContractStorage.defineProperty(this, "size");
};

SampleContract.prototype = {
    init: function () {
        this.size = 0;
    },

    set: function (key, value) {
        var index = this.size;
        this.arrayMap.set(index, key);
        this.dataMap.set(key, value);
        this.size +=1;
    },

    get: function (key) {
```

```
        return this.dataMap.get(key);
    },

    len:function(){
      return this.size;
    },

    iterate: function(limit, offset){
        limit = parseInt(limit);
        offset = parseInt(offset);
        if(offset>this.size){
           throw new Error("offset is not valid");
        }
        var number = offset+limit;
        if(number > this.size){
          number = this.size;
        }
        var result  = "";
        for(var i=offset;i<number;i++){
            var key = this.arrayMap.get(i);
            var object = this.dataMap.get(key);
            result += "index:"+i+" key:"+ key + " value:" +object+"_
↪";
        }
        return result;
    }

};

module.exports = SampleContract;
```

Next step: Tutorial 5

Interacting with Nebulas by RPC API

3.3.5 Nebulas 101 - 05 Interacting with Nebulas by RPC API

YouTube Tutorial

Nebulas chain node can be accessed and controlled remotely through RPC. Nebulas chain provides a series of APIs to get node information, account balances, send transactions and deploy calls to smart contracts.

The remote access to the Nebulas chain is implemented by gRPC, and also could be accessed by HTTP via the proxy (grpc-gateway). HTTP access is a interface implemented by RESTful, with the same parameters as the gRPC interface.

API

We've implemented RPC server and HTTP sercer to provide API service in Go-Nebulas.

Modules

All interfaces are divided into two modules: API and Admin.

- API: Provides interfaces that are not related to the user's private key.
- Admin: Provides interfaces that are related to the user's private key.

It's recommended for all Nebulas nodes to open API module for public users and Admin module for authorized users.

Configuration

RPC server and HTTP server can be configured in the configuration file of each Nebulas node.

```
rpc {
    # gRPC API service port
    rpc_listen: ["127.0.0.1:8684"]
    # HTTP API service port
    http_listen: ["127.0.0.1:8685"]
    # Open module that can provide http service to outside
    http_module: ["api", "admin"]
}
```

Example

HTTP

Here is some examples to invoke HTTP interfaces using `curl`.

GetNebState

We can invoke `GetNebState` in API module to fetch the current state of local Nebulas node, including chain identity, tail block, protocl version and so on.

```
> curl -i -H Accept:application/json -X GET http://localhost:8685/
 ↪v1/user/nebstate

{"result":{"chain_id":100,"tail":
 ↪"0aa1cceb7801b110fdd5217ba0a4356780c940133924d1c1a4eb60336934dab1
 ↪","lib":
 ↪"0000000000000000000000000000000000000000000000000000000000000000
 ↪","height":"479","protocol_version":"/neb/1.0.0","synchronized
 ↪":false,"version":"0.7.0"}}
```

UnlockAccount

We can invoke `UnlockAccount` in Admin module to unlock an account in memory. All unlocked accounts can be used to send transactions directly without passphrases.

```
> curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/admin/account/unlock -d '{"address":
↪"n1NrMKTYESZRCwPFDLFKiKREzZKaN1nhQvz", "passphrase": "passphrase"}
↪'

{"result":{"result":true}}
```

RPC

RPC server is implemented with GRPC. The serialization of GPRC is based on Protocol Buffers. You can find all rpc protobuf files in Nebulas RPC Protobuf Folder.

Here is some examples to invoke rpc interfaces using `golang`.

GetNebState

We can invoke `GetNebState` in API module to fetch the current state of local Nebulas node.

```
import(
    "github.com/nebulasio/go-nebulas/rpc"
    "github.com/nebulasio/go-nebulas/rpc/pb"
)

// GRPC server connection address configuration
addr := fmt.Sprintf("127.0.0.1:%d",uint32(8684))
conn, err := grpc.Dial(addr, grpc.WithInsecure())
if err != nil {
    log.Warn("rpc.Dial() failed:", err)
}
defer conn.Close()

// API interface to access node status information
api := rpcpb.NewAPIServiceClient(conn)
resp, err := ac.GetNebState(context.Background(), & rpcpb.
↪GetNebStateRequest {})
if err != nil {
    log.Println("GetNebState", "failed", err)
} else {
    log.Println("GetNebState tail", resp)
}
```

LockAccount

Account `n1NrMKTYESZRCwPFDLFKiKREzZKaN1nhQvz` has been unlocked after invoking `v1/admin/account/unlock` via HTTP request above. We can invoke `LockAccount` in Admin module to lock it again.

```
import(
    "github.com/nebulasio/go-nebulas/rpc"
    "github.com/nebulasio/go-nebulas/rpc/pb"
)

// GRPC server connection address configuration
addr := fmt.Sprintf("127.0.0.1:%d",uint32(8684))
conn, err := grpc.Dial(addr, grpc.WithInsecure())
if err != nil {
    log.Warn("rpc.Dial() failed:", err)
}
defer conn.Close()

// Admin interface to access, lock account address
admin := rpcpb.NewAdminServiceClient(conn)
from := "n1NrMKTYESZRCwPFDLFKiKREzZKaN1nhQvz"
resp, err = management.LockAccount(context.Background(), & rpcpb.
↪LockAccountRequest {Address: from})
if err != nil {
    log.Println("LockAccount", from, "failed", err)
} else {
    log.Println("LockAccount", from, "result", resp)
}
```

API List

For more interfaces, please refer to the official documentation:

- API Module
- Admin Module.

Next

Nice job! Let's join official Testnet or Mainnet to enjoy Nebulas now!

Join to Testnet Join to Mainnet

3.3.6 Nebulas 101 - 01 çijŰèŕŚåőL'èčĚæŸ§äžŚéŞ¿

æŸ§äžŚéŞ¿çŽĎéąźçŽőäžčçăĄåůšçżŕåŔŚåÿČäžĘåĞääÿłçL'ĹæIJñïijŇçżŔè£ĞætŃèŕŢåŔŕäžěåIJĺæIJňåIJï

æČşäžĘèğčæŸ§äžŚéŞ¿çŽĎåŘŇå■ęåŔŕäžěéŸĚèŕżæŸ§äžŚéŞ¿éİđæŁĂæIJŕçŹ¡çŽőäźęãĂĆ

åŕźæŁĂæIJŕæĎ§åĚt'èűčçŽĎåŘŇå■ęåŔŕäžěçIJŃæŸ§äžŚéŞ¿æŁĂæIJŕçŹ¡çŽőäźęåŠŇæŸ§äžŚéŞ¿Githubä

æŸ§äžŚéŞ¿çŐřéŸűæőţåŔłèČ¡åIJÍMacåŠŇLinuxäÿŁè£ŘèąŇïijŇåŘŐçż■äijŽæŐĺåĞžwindowsçĽĹæIJň

GolangçŐŕåćČæŘ■åžž

| Components | Version | Description | | — | — | — | | Golang | > = 1.9.2 | The Go Programming Language |

æĹŚäžňäijŽåĹĘåĹńäžŃçż■Mac OSXåŠŇLinuxäÿď˙çğ■çşżçż§äÿŃgolangçŐŕåćČçŽĎæŘ■åžžãĂĆ

Mac OSX

åIJÍMac OSXéĞŇïijŇæĹŚäžňæŐĺè■Řä¡£çŤĺHomebrewæİěåőĽ'èčĚGolang.

```
# åőL'èčĚ
brew install go

# éĚ■ç¡őçŐŕåćČåŔŸéĞŔ
export GOPATH=/path/to/workspace
```

æŔŘçď˙ž: åIJÍgolangçŽĎåijĂåŔŚäÿ■ïijŇGOPATHæŸŕå£ĚéążçŽĎïijŇåőČæŇĞåőŽäžĘæĹŚäžňä¡£çŤÍg

Linux

```
# download
wget https://dl.google.com/go/go1.9.3.linux-amd64.tar.gz

# extract
tar -C /usr/local -xzf go1.9.3.linux-amd64.tar.gz

# environment variables
export PATH=$PATH:/usr/local/go/bin
export GOPATH=/path/to/workspace
```

çijŰèŕŚæŸ§äžŚéŞ¿

äÿŃè¡¡æžŘçăĄ

åŔŕäžěä¡£çŤĺåęĆäÿŃæŇĞäžď˙çŻť˙æŐěäÿŃè¡¡æIJĂæŰřçĽĹæIJňçŽĎæŸ§äžŚéŞ¿æžŘçăĄãĂĆ

```
# è£ŻåĚěåůěä¡IJçŻőå¡Ţ
mkdir -p $GOPATH/src/github.com/nebulasio
cd $GOPATH/src/github.com/nebulasio

# äÿŃè¡¡æžŘçăĄ
git clone https://github.com/nebulasio/go-nebulas.git
```

```
# è£ŽåĚěéąźçŽőçŻőå¡Ţ
cd go-nebulas

# åĹĞæ■ćåĹřæIJĂçĺşåőŽçŽĎmasteråĹĘæŤŕ
git checkout master
```

åőL'èčĚrocksdbä¿ÌèţŰåžŞ

åŘŇæăůæĹŚäžňäijŽäžŃçż■åęĆä¡ŢåIJÍMAC OSXåŠŇLinuxæ■čçąőåőL'èčĚRocksDBãĂĆ

Mac OSX

åŔŕäżěçŻť'æŐěéĂŽè£ĞHomebrewåőL'èčĚïijŇè£ŘèąŇbrew install rocksdb

Linux

åIJÍlinuxçŐŕåćČäÿŃïijŇçŤśäžŐubuntuåŠŇcentosçşżçż§çŽĎçŤÍæĹůåĄŔåd'ŽïijŇæĹŚäžňářĘåĹĘåĹńäžŇ

Ubuntu

- éęŰåĚĹåőL'èčĚRocksDBæL'ĂéIJĂä¿ÌèţŰåžŞ

```
  apt-get update
  apt-get -y install build-essential libgflags-dev libsnappy-
↪dev zlib1g-dev libbz2-dev liblz4-dev libzstd-dev
```

- äÿŃè¡¡æžŘçăĄåźűçijŰèŕŚåőL'èčĚ

```
  git clone https://github.com/facebook/rocksdb.git
  cd rocksdb & make shared_lib && make install-shared
```

Centos

- éęŰåĚĹåőL'èčĚRocksDBæL'ĂéIJĂä¿ÌèţŰåžŞ

```
  yum -y install epel-release && yum -y update
  yum -y install gflags-devel snappy-devel zlib-devel bzip2-
↪devel gcc-c++  libstdc++-devel
```

- äÿŃè¡¡æžŘçăĄåźűçijŰèŕŚåőL'èčĚ

```
  git clone https://github.com/facebook/rocksdb.git
  cd rocksdb & make shared_lib && make install-shared
```

åőĽèčĚGoä¿ìèţŰåžŞ

åIJĺGo-Nebulasäÿ■ïijŇGoçŽĎäÿĽæŰźåžŞéČ¡éĂŽè£ĞDepæİěåĄŽçőąçŘĘãĂĆ

| Components | Version | Description | | — | — | — |

Dep | > = 0.3.1 | Dep is a dependency management tool for Go. |

åőĽèčĚDepåůěåĚů

æĹŚäžňåŘŇæăůåĹĘåĹńäżŃçż■Mac OSXåŠŇLinuxäÿŃDepçŽĎåőĽèčĚæŰźæşŢãĂĆ

Mac OSX

- éĂŽè£ĞHomebrewçŻťæŐěåőĽèčĚåźűå■ĞçžğDep

```
brew install dep
brew upgrade dep
```

Linux

- éĂŽè£ĞæžŘçăĄæİěåőĽèčĚDep

```
cd /usr/local/bin/
wget https://github.com/golang/dep/releases/download/v0.3.2/
↪dep-linux-amd64
ln -s dep-linux-amd64 dep
```

äÿŃè¡¡GoäÿĽæŰźåžŞ

æĹŚäžňåĹĞæ■ćåĹřGo-NebulaséąźçŻőæăźçŻőå¡ŢïijŇçĎűåŘŐä¡£çŤĺDepæİěäÿŃè¡¡äÿĽæŰźåžŞãĂĆ

```
cd $GOPATH/src/github.com/nebulasio/go-nebulas
make dep
```

æŔŘçď ž: `make dep`åřĘäijŽäÿŃè¡¡å¿Ĺåď Žä¿ìèţŰåžŞãĂĆåIJĺéČĺåĹĘåIJřåŇžïijŇè£Źäÿłè£ĞçĺŃåŔŕèČ

```
wget http://ory7cn4fx.bkt.clouddn.com/vendor.tar.gz
cd $GOPATH/src/github.com/nebulasio/go-nebulas
tar zxf vendor.tar.gz
```

åőĽèčĚChrome V8ä¿ìèţŰåžŞ

æŸ§äžŚèŹŽæŃ§æIJžçŻőåĽ■ä¿ìèţŰäžŐChromeçŽĎV8åijŢæŞŐïijŇäÿžäžĘåď ğåőűä¡£çŤĺæŰźä¿£ïijŇæĺ
OSXåŠŇLinuxçijŰèŕŚåě¡äžĘV8çŽĎåŁĺæĂĄåžŞãĂĆè£ŘèąŇåęĆäÿŃæŇĞäžď åŕśåŔŕäžěåőŇæĹŘåőĽèčĚãĂĆ

```
cd $GOPATH/src/github.com/nebulasio/go-nebulas
make deploy-v8
```

çijŰèŕŚåŔŕæĽğèąŇæŰĞäžű

åőŇæĹŘæĽĂæIJĽäÿŁè£řä¿ÌètŰåžŞçŽĎåőĽèčĚåŘŐïijŇçŐřåIJÍæĹŚäżňåŔŕäżěè£ŻåĚěGo-Nebulasæäźç Żőå¡ŢçijŰèŕŚæŸ§äžŚéŞ¿çŽĎåŔŕæĽğèąŇæŰĞäžűäžĘãĂĆ

```
cd $GOPATH/src/github.com/nebulasio/go-nebulas
make build
```

çijŰèŕŚæĹŘåŁ§åŘŐïijŇårĘäijŽçIJŃåĹřåęĆäÿŃä£ąæĄŕãĂĆ

```
shangshu at shangshudeMacBook-Pro in ~/workspace/blockchain/src/github.com/nebulasio/go-nebulas on master
› make build                                                                                          16:44
cd cmd/neb; go build -ldflags "-X main.version=1.0.1 -X main.commit=fbcdd8927b3ed5db9ccf889388bf8efb500d3357
 -X main.branch=master -X main.compileAt=`date +%s`" -o ../../neb-fbcdd8927b3ed5db9ccf889388bf8efb500d3357
cd cmd/crashreporter; go build -ldflags "-X main.version=1.0.1 -X main.commit=fbcdd8927b3ed5db9ccf889388bf8e
fb500d3357 -X main.branch=master -X main.compileAt=`date +%s`" -o ../../neb-crashreporter
rm -f neb
ln -s neb-fbcdd8927b3ed5db9ccf889388bf8efb500d3357 neb
```

è£ŘèąŇæŸ§äžŚéŞ¿

åĹŻäÿŰåŇžåİŮ

åIJÍåŘŕåŁÍäÿĂäÿłæŰřçŽĎæŸ§äžŚéŞ¿åĽ■ïijŇæĹŚäżňå£ĚéążåőŽäźĽåĹŻäÿŰåŇžåİŮçŽĎéĚ■ç¡őæŰĞäž

åĹŻäÿŰåŇžåİŮéĚ■ç¡ő

```
meta {
  # æŕŔæİąéŞ¿çŽĎåŤŕäÿĂæăĞèŕĘ
  #␣
 ↪æŕŔäÿłåŇžåİŮåŠŇäžd'æŸŞåŔłäijŽåśđäžŐäÿĂæİąåŤŕäÿĂçŽĎéŞ¿ïijŇä£ÌèŕĄåőL'åĚÍæĂğ
  chain_id: 100
}

consensus {
  #␣
 ↪åIJÍèt'açŇőåžęèŕĄæŸŐ(PoD)èćńåĚĚåĹĘéłŇèŕĄåL'■ïijŇæŸ§äžŚéŞ¿éĞĞçŤÍDPoSåĚśèŕĘçőŮæş
  # DPoSåĚśèŕĘäÿ■ïijŇ21äÿłäžžçżĎæĹŘäÿĂäÿłæIJİäżč
  #␣
 ↪æŕŔéŽŤäÿĂæőţæŮűéŮt'éČ¡äijŽåĹĞæ■ćæIJİäżčïijŇæŕŔäÿłæIJİäżčåĘĚïijŇ21äÿłçŞ£åůěè¡őæ
  #␣
 ↪çŤśäžŐDPoSåŘłæŸŕè£ĞæÿąæŰźæąĹïijŇæL'ĂäżěæŽĆæŮűäÿ■åijĂæŤ¿çżŹåĚñäijÛæŇŰçŞ£ïijŇå■ş
  dpos {
    # åĹİåğŃæIJİäżčïijŇåŇĚåŘń21äÿłåĹİåğŃçŞ£åůěåIJřåİĂ
    dynasty: [
      [ miner address ],
      ...
    ]
  }
```

```
}

# écĎåĹĘéĚ■çŽĎäżčåÿĄ
token_distribution [
  {
    address: [ allocation address ]
    value: [ amount of allocation tokens ]
  },
  ...
]
```

åŔŕäžěåIJĺæäźçŻőå¡Ţconf/default/genesis.confäÿŃïijŇæL'¿åĹřäÿĂäÿłåőŇæŢt'çŽĎåĹŻäÿŰ

éĚ■ç¡őæŰĞäżű

åIJĺæĹŚäžňåŔŕåŁĺäÿĂäÿłæŸ§äžŚèŁĆçĆźåL'■ïijŇæĹŚäžňéIJĂèęĄåőŽäźL'åě¡èŕěèŁĆçĆźçŽĎéĚ■ç¡őæŰ

æŸ§äžŚèŁĆçĆźéĚ■ç¡őæŰĞäżű

```
# ç¡ŚçżIJéĚ■ç¡ő
network {
  # åŕźäžŐåĚĺç¡ŚçňňäÿĂäÿłèŁĆçĆźïijŇäÿ■éIJĂèęĄéĚ■ç¡őseed
  #␣
↪åŘęåĹŹïijŇåĚűäżŰèŁĆçĆźåŔŕåŁĺæŮűéIJĂèęĄéĚ■ç¡őseedïijŇseedèŁĆçĆźåřĘäijŽæŁŁç¡ŚçżI
  # åŔŕäżěéĚ■ç¡őåd'Žäÿłseed, ["...", "..."]
  seed: ["/ip4/127.0.0.1/tcp/8680/ipfs/
↪QmP7HDFcYmJL12Ez4ZNVCKjKedfE7f48f1LAkUc3Whz4jP"]

  # èŁĆçĆźçŻŚåŘñç¡ŚçżIJæűĹæĄŕçńŕåŔčïijŇåŔŕäżěéĚ■ç¡őåd'Žäÿł
  listen: ["0.0.0.0:8680"]

  # ç¡ŚçżIJçğĄéŠěïijŇçŢĺäžŐçąőèőd'èžńäż¡èŁĆçĆź
  # private_key: "conf/network/id_ed25519"
}

# éŞ¿éĚ■ç¡ő
chain {
  # éŞ¿çŽĎåŤŕäÿĂæăĞèŕĘ
  chain_id: 100

  # æŢřæ■őå■ŸåĆĺåIJřåİĂ
  datadir: "data.db"

  # èt'ęæĹůkeystoreæŰĞäżűå■ŸåĆĺåIJřåİĂ
  keydir: "keydir"

  # åĹżäÿŰåŇžåİŮéĚ■ç¡ő
```

```
  genesis: "conf/default/genesis.conf"

  # ç■¿åŘ■çőŮæşŢïijÑèŕůåŃ£ä£őæŤź
  signature_ciphers: ["ECC_SECP256K1"]

  #␣
↪ç§£åůěåIJřåİĂïijÑç§£åůěçŽĎkeystoreæŰĞäżűéIJĂèęĄæŤ¿ç¡őåIJĺéĚ■ç¡őçŽĎkeydiräÿŃ
  miner: "n1XkoVVjswb5Gek3rRufqjKNpwrDdsnQ7Hq"

  #␣
↪CoinbaseåIJřåİĂïijÑèŕěåIJřåİĂçŢĺäžŐæŐěæŤűç§£åůěçŽĎæŇŰç§£åěŰåŁśïijÑåŕŕäżěåŠÑç§£
  #␣
↪èŕěåIJřåİĂçŽĎkeystoreæŮäéIJĂæŽt’éIJšïijÑäÿ■çŢĺæŤ¿ç¡őåIJĺéĚ■ç¡őçŽĎkeydiräÿŃ
  coinbase: "n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE"

  # ç§£åůěåIJřåİĂçŽĎåŕĘçăĄ
  passphrase: "passphrase"
}

# APIéĚ■ç¡ő
rpc {
    # GRPCæIJ■åŁąçńŕåŔč
    rpc_listen: ["127.0.0.1:8684"]

    # HTTPæIJ■åŁąçńŕåŔč
    http_listen: ["127.0.0.1:8685"]

    # åijĂæŤ¿çŽĎAPIæĺąåİŮ
    # APIæĺąåİŮåŃĚåŘńæL’ĂæIJL’åŠŃçŢĺæĹůçğĄéŠěæŮăåĚşçŽĎæŐěåŔč
    #␣
↪AdminæĺąåİŮåŃĚåŘńæL’ĂæIJL’åŠŃçŢĺæĹůçğĄéŠěçŻÿåĚşçŽĎæŐěåŔčïijÑéIJĂèęĄæĚŐéĞ■èĂČèŹ
    http_module: ["api", "admin"]
}

# æŮěå£ŮéĚ■ç¡ő
app {
    # æŮěå£Ůçžğåĺń: æŤŕæŃĄ[debug, info, warn, error, fatal]
    log_level: "info"

    # æŮěå£Ůå■ŸæŤ¿ä¡■ç¡ő
    log_file: "logs"

    # æŸŕåŘęæL’ŞåijĂcrash reportæIJ■åŁą
    enable_crash_report: false
}

# çŻŚæŐğæIJ■åŁąéĚ■ç¡ő
stats {
    # æŸŕåŘęæL’ŞåijĂçŻŚæŐğæIJ■åŁą
    enable_metrics: false
```

```
    # çŻŚæŐğæIJ■åŁąåřEæŢřæ■őäÿŁäijăåĹřInfluxdb
    # éĚ■ç¡őInfluxdbçŽĎèő£éŮőä£ąæĄŕ
    influxdb: {
        host: "http://localhost:8086"
        db: "nebulas"
        user: "admin"
        password: "admin"
    }
}
```

A lot of examples can be found in `$GOPATH/src/github.com/nebulasio/go-nebulas/conf/`

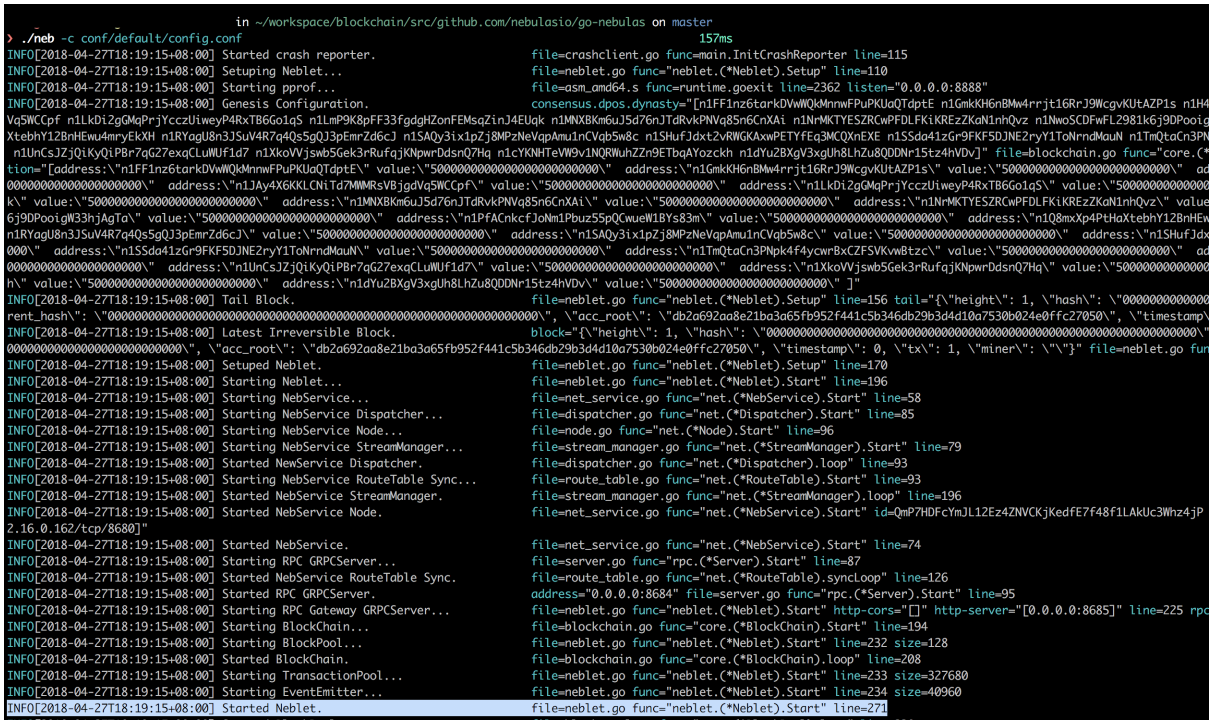
åŘŕåŁÍæŸ§äžŚéŞ¿

æ■đ'æŮűåŘŕåŁĺçŽĎæŸ§äžŚéŞ¿æŸŕæIJňåIJřçŽĎçğĄæIJL'éŞ¿ïijŇåŠŇåőŸæŰźçŽĎætŃèřŢç¡ŚåŠŇäÿż

åŘŕåŁĺä¡äçŽĎçňňäÿĂäÿłæŸ§äžŚèŁĆçĆźãĂĆ

```
cd $GOPATH/src/github.com/nebulasio/go-nebulas
./neb -c conf/default/config.conf
```

åŘŕåŁÍæĹŘåŁ§çŽĎèŕĺïijŇåřĘäijŽçIJŃåĹŕåęĆäÿŃä£ąæĄŕïijŇæIJL'`Started Neblet`çŽĎæŮěå£Ůè¿ŞåĞžãĂĆ



éżŸèőd'æČĚåĘţäÿŃïijŇä¡£çŤĺéĚ■ç¡őæŰĞäžűconf/default/config.confåŘŕåŁĺçŽĎèŁĆçĆźäÿ■æŸŕç§£åůěèŁĆçĆźãĂĆ

æŐěäÿŃæÌěïijŇåŘŕåŁĺä¡äçŽĎçňňäÿĂäÿłç§£åůěèŁĆçĆźïijŇåőČçŽĎseedèŁĆçĆźå■şæĹŚäžňåĹŽåĹŽåŘ

```
cd $GOPATH/src/github.com/nebulasio/go-nebulas
./neb -c conf/example/miner.conf
```

åIJÍè£ŹäÿłèŁĆçĆźåŘŕåŁĺåŘŐïijÑä¡ääijŽåĚĹçIJŃåĹřåęĆäÿŃä£ąæĄŕïijÑèąÍçd'žå¡ŞåL'■èŁĆçĆźæ■čåIJÍa

```
INFO[2018-04-27T19:05:31+08:00] Enabled Dpos Mining...                        file=dpos.go func="dpos.(*Dpos).EnableMi
ning" line=155
INFO[2018-04-27T19:05:31+08:00] Started Active Sync Task.                     file=blockchain.go func="core.(*BlockCha
in).StartActiveSync" line=528 syncpoint="{\"height\": 1, \"hash\": \"0000000000000000000000000000000000000000000000000
0000000000000\", \"parent_hash\": \"0000000000000000000000000000000000000000000000000000000000000000\", \"acc_root\"
: \"db2a692aa8e21ba3a65fb952f441c5b346db29b3d4d10a7530b024e0ffc27050\", \"timestamp\": 0, \"tx\": 1, \"miner\": \"\"}"
INFO[2018-04-27T19:05:31+08:00] Suspended Dpos Mining.                        file=dpos.go func="dpos.(*Dpos).SuspendM
ining" line=290
INFO[2018-04-27T19:05:31+08:00] Started Neblet.                               file=neblet.go func="neblet.(*Neblet).St
art" line=271
```

ç■L'å¿ĚäÿĂäijŽåĎ£ïijÑářĘäijŽçIJŃåĹřåęĆäÿŃä£ąæĄŕïijÑèąÍçd'žå¡ŞåL'■èŁĆçĆźåůšçźŔè£đäÿŁäžĘseed

```
INFO[2018-04-27T19:08:32+08:00] Active Sync Task Finished.                    file=blockchain.go func="core.(*BlockCha
in).StartActiveSync.func1" line=531 tail="{\"height\": 1, \"hash\": \"0000000000000000000000000000000000000000000000000
0000000000000\", \"parent_hash\": \"0000000000000000000000000000000000000000000000000000000000000000\", \"acc_root\
": \"db2a692aa8e21ba3a65fb952f441c5b346db29b3d4d10a7530b024e0ffc27050\", \"timestamp\": 0, \"tx\": 1, \"miner\": \"\"}
"
INFO[2018-04-27T19:08:32+08:00] Resumed Dpos Mining.                          file=dpos.go func="dpos.(*Dpos).ResumeMi
ning" line=296
```

åĘ■ç■L'å¿ĚåĞäåĹĘéŠ§ïijÑä¡ääijŽçIJŃåĹřåęĆäÿŃä£ąæĄŕïijÑèąÍçd'žå¡ŞåL'■ç§£åůëèŁĆçĆźæŇŰåĞžäžĹ

```
INFO[2018-04-27T19:10:28+08:00] My turn to mint block                         actual=n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdp
tE deadline=1524827430000 expected=195707f964ff495324635f22c7b486e05d7e67c7af5c9a00df97 file=dpos.go func="dpos.(*Dpos
).blockLoop" line=623 start=1524827428000 tail="{\"height\": 1, \"hash\": \"0000000000000000000000000000000000000000000
0000000000000000000\", \"parent_hash\": \"0000000000000000000000000000000000000000000000000000000000000000\", \"acc
_root\": \"db2a692aa8e21ba3a65fb952f441c5b346db29b3d4d10a7530b024e0ffc27050\", \"timestamp\": 0, \"tx\": 1, \"miner\":
 \"\"}"
INFO[2018-04-27T19:10:30+08:00] Minted new block                              block="{\"height\": 2, \"hash\": \"18377
702273d102b19ec4160f587b3c60fc0f3ec5bde695829ebb132778890e2\", \"parent_hash\": \"0000000000000000000000000000000000
0000000000000000000000000000\", \"acc_root\": \"afcd700aa49c6de6569c698b7324a4f30d2e7d1d995f0852881ce581e25ec578\", \"
timestamp\": 1524827430, \"tx\": 0, \"miner\": \"n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE\"}" deadline=1524827430000 end=15
24827430 file=dpos.go func="dpos.(*Dpos).blockLoop" line=623 packed=1524827430000 slot=1524827430000 start=15248274280
00 tail="{\"height\": 1, \"hash\": \"0000000000000000000000000000000000000000000000000000000000000000\", \"parent_hash
\": \"0000000000000000000000000000000000000000000000000000000000000000\", \"acc_root\": \"db2a692aa8e21ba3a65fb952f441
c5b346db29b3d4d10a7530b024e0ffc27050\", \"timestamp\": 0, \"tx\": 1, \"miner\": \"\"}"
INFO[2018-04-27T19:10:30+08:00] Succeed to update new tail.                   file=dpos.go func="dpos.(*Dpos).ForkChoi
ce" line=203 tail="{\"height\": 2, \"hash\": \"18377702273d102b19ec4160f587b3c60fc0f3ec5bde695829ebb132778890e2\", \"p
arent_hash\": \"0000000000000000000000000000000000000000000000000000000000000000\", \"acc_root\": \"afcd700aa49c6de656
9c698b7324a4f30d2e7d1d995f0852881ce581e25ec578\", \"timestamp\": 1524827430, \"tx\": 0, \"miner\": \"n1FF1nz6tarkDVwWQ
kMnnwFPuPKUaQTdptE\"}"
INFO[2018-04-27T19:10:30+08:00] Broadcasted new block                         block="{\"height\": 2, \"hash\": \"18377
702273d102b19ec4160f587b3c60fc0f3ec5bde695829ebb132778890e2\", \"parent_hash\": \"0000000000000000000000000000000000
0000000000000000000000000000\", \"acc_root\": \"afcd700aa49c6de6569c698b7324a4f30d2e7d1d995f0852881ce581e25ec578\", \"
timestamp\": 1524827430, \"tx\": 0, \"miner\": \"n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE\"}" file=dpos.go func="dpos.(*Dpo
s).mintBlock" line=610 tail="{\"height\": 1, \"hash\": \"0000000000000000000000000000000000000000000000000000000000
000\", \"parent_hash\": \"0000000000000000000000000000000000000000000000000000000000000000\", \"acc_root\": \"db2a692a
a8e21ba3a65fb952f441c5b346db29b3d4d10a7530b024e0ffc27050\", \"timestamp\": 0, \"tx\": 1, \"miner\": \"\"}"
```

æŔŘçd'ž: çŻőåL'■çŽDDPoSåĚśèŕĘçőŮæşŢïijÑäijŽæIJL'21äÿłèŁĆçĆźè¡őætĄåĞžåİŮãĂĆçŤśäžŐæĹŚ

äÿŃäÿĂçńă

åIJÍæŸ§äžŚéŞ¿äÿŁåŔŚéĂĄäžd'æŸŞ

3.3.7 Nebulas 101 - 02 åIJÍæŸ§äžŚéŞ¿äÿŁåŔŚéĂĄäžd'æŸŞ

NebulasæŔŘä¿ŻäžĘäÿL'çğ■æŰźåijŔåŐżåŔŚéĂĄæĹŚäžňçŽĎäžd'æŸŞïijŽ

1. ç■¿åŘ■ & åŔŚéĂĄ
2. årĘçăĄ & åŔŚéĂĄ
3. èğčéŤĄ & åŔŚéĂĄ

äÿŃéİćæĹŚäžňåĹĘåĹńäžŃçż■åęĆä¡ŢéĂŽè£ĞäžěäÿŁäÿL'çğ■æŰźåijŔåIJÍnebulasäÿ■åŔŚéĂĄäÿĂçňŤäž

åĞĘåd'Ğèť ęæĹů

åIJÍæŸ§äžŚéŞ¿äÿŁïijŇæŕŔäÿłåIJřåİĂèąÍçd'žäÿĂäÿłåŤŕäÿĂçŽĎèť ęæĹůïijŇäÿĂäÿĂåŕźåžŤãĂĆ

åIJÍåŔŚéĂĄäžd'æŸŞåL'■ïijŇæĹŚäžňéIJĂèęĄåĞĘåd'Ğäÿd'äÿłèť ęæĹůïijŽäÿĂäÿłèť ęæĹůÇŤÍæİěåŔŚéĂĄ (çğřäÿž"from") åŠŇåŔęäÿĂäÿłèť ęæĹůæİěæŐěåŔŮäžčåÿĄ (çğřäÿž"to").

åŔŚéĂĄèĂĚèť ęæĹů

åIJÍè£ŹéĞŇïijŇæĹŚäžňářĘäijŽä¡£çŤÍéĚ■ç¡őæŰĞäžűconf/default/genesis.conf äÿ■écĎåĹĘéĚ■è£Ğäžčåÿ ĄçŽĎèť ęæĹůäÿ■éĂL'æŃl'äÿĂäÿłä¡IJäÿžåŔŚéĂĄèĂĚèť ęæĹůïijŇézŸèőd'éĂ

æŐěåŔŮèĂĚèť ęæĹů

æĹŚäžňä¡£çŤÍåęĆäÿŃæŇĞäžd'åĹŻåžžäÿĂäÿłåĚÍæŰřçŽĎèť ęæĹůæİěåĄŽæŐěåŔŮèĂĚïijŇèŕůèőřä¡Ŕè¿

```
$ ./neb account new
Your new account is locked with a passphrase. Please give a␣
↪passphrase. Do not forget this passphrase.
Passphrase:
Repeat passphrase:
Address: n1SQe5d1NKHYFMKtJ5sNHPsSPVavGzW71Wy
```

æŔŘçd'žïijŽä¡ăåĹŻåžžçŽĎæŰřèť ęæĹůåŠŇäÿŁéİćåŔŕèČ¡äÿ■äÿĂæăůïijŇèŕůäžěä¡ăåĹŻåžžçŽĎèť ęæĹů

æŰřèť ęæĹůçŽĎkeystoreæŰĞäžűårĘäijŽècńæŤ¿ç¡őåIJÍ$GOPATH/src/github.com/nebulasio/go-nebulas/keydir/åĘĚãĂĆ

åŘŕåŁÍçğĄæIJL'éŞ¿

æĹŚäžňårĘåIJÍæIJňåIJřæŘ■åžžäÿĂäÿłçğĄæIJL'éŞ¿æİěä¡IJäÿžæIJňæŢŹçÍŃçŽĎætŃèŕŢçŐŕåćČãĂĆ

åŘŕåŁÍçğ■å■ŘèŁĆçĆź

éęŰåĚĹïijŇæĹŚäžňåŘŕåŁÍæIJňåIJřçğĄæIJL'éŞ¿çŽĎçňňäÿĂäÿłèŁĆçĆźïijŇåőČåŔŕäžěä¡IJäÿžåĚűäžŰèŁ

```
./neb -c conf/default/config.conf
```

åŘŕåŁÍç§£åůěèŁĆçĆź

æŐěçİĂïijŇæĹŚäžňåŘŕåŁÍäÿĂäÿłç§£åůěèŁĆçĆźæŐěåĚěæIJňåIJřçğĄæIJL'éŞ¿ïijŇè£ŹäÿłèŁĆçĆźäźŇåŘ

```
./neb -c conf/example/miner.conf
```

åd'ŽäźĚäijŽçŤ§æĹŘäÿĂäÿłæŰřçŽĎåŇžåİŮ?

åIJÍæŸ§äžŚéŞ¿äÿŁ, åIJÍèt'ąçŇőåžęèŕĄæŸŐïijĹProof-of-Devotionïij Ň æŁĂæIJŕçŹ¡çŽőäźęäÿ■æIJL'èŕęçżĘæŔŔè£ŕïijL'èćńåĚĚåĹĘéłŇèŕĄåL'■ïijŇDPoSèćńéĂL'æŃl'ä¡IJäÿžäÿ

åIJÍæĹŚäžňçŻőåL'■çŽĎætŃèŕŢçŐŕáćČäÿ■ïijŇçŤśäžŐæĹŚäžňåŔłåŘŕåŁÍäžĘ21äÿłç§£åůěäÿ■çŽĎäÿĂäÿ

äÿĂæŮęäÿĂäÿłæŰřåŇžåİŮèćńæŇŰåĞžïijŇæŇŰåİŮåěŰåŁśårĘäijŽèćńèĞłåŁÍåŔŚéĂĄåĹřå¡ŞåL'■ç§£åů
`example/miner.conf`éĞŇïijŇèŕěèt'ęæĹůåřśæŸŕ`n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE`.

æŸ§äžŚéŞ¿äžd'äžŠ

æŸ§äžŚéŞ¿æŔŘä¿ŻçżŹåijĂåŔŚèĂĚHTTP API, RPC APIåŠŇ-CLIæİěåŠŇè£ŘèąŇäÿ■çŽĎæŸ§äžŚèŁĆçĆźäžd'äžŠãĆĆåIJÍæŢŹçÍŃäÿ■ïijŇæĹŚäžňåřĘäijŽå§žäžŐHTTP APIïijĹAPI Module | Admin Moduleïij L'æİěäžŃçż■äÿL'çğ■åŔŚéĂĄäžd'æŸŞçŽĎæŰźæşŢãĆ

æŔŘçd'žïijŽæŸ§äžŚéŞ¿çŽĎHTTPæIJ■åŁąéżŸèőd'çńŕåŘčåŘůäÿž8685ãĆĆ

éęŰåĚĹïijŇåIJÍåŔŚéĂĄæŰřäžd'æŸŞåL'■ïijŇæĹŚäžňæčĂæ§ěäÿŇåŔŚéĂĄèĂĚèt'ęæĹůçŽĎçŁűæĂĄãĂ

æčĂæ§ěèt'ęæĹůçŁűæĂĄ

æŕŔäÿłäžd'æŸŞåęĆædIJéIJĂèęĄäÿŁéŞ¿ïijŇéČ¡éIJĂèęĄçżŹç§£åůěçijt'çžşäÿĂéČĺåĹĘæL'Ńçż■èt'źïijŇæ

æĹŚäžňåŘŕäžěéĂŽè£ĞAPI Moduleäÿ■çŽĎ`/v1/user/accountstate`æŐěåŘčæİěèŐůåŘŰåŘŚéĂĄèĂĚèt'ęæĹůn1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdp

```
> curl -i -H Accept:application/json -X POST http://localhost:8685/
↪v1/user/accountstate -d '{"address":
↪"n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE"}'

{"result":{"balance":"500000000000000000000000","nonce":"0","type
↪":87}}
```

æŔŘçd'žïijŽ`Type`çŤĺäžŐæăĞèőŕèt'ęæĹůçśžåđŇãĂĆ88èąĺçd'žèŕěèt'ęæĹůäÿžæŹžèČ¡åŘĹçžęèt'ęæĹůïij
`/neb account new`åĹŻåžžçŽĎèt'ęæĹůåřśæŸŕéIđåŘĹçžęèt'ęæĹůïijŇçŤĺæĹůå■ŸåĆĺéŞ¿äÿŁęŢĎäžğ

æŔŘçď žïijŽNonceçŤĺäžŐæäĞèőřèť ęæĹůåŔŚèţůçŽĎæĽ ĂæIJL'äžď æŸŞçŽĎéąžåžŔãĂĆåŘŇäÿĂäÿłè

åęĆæĹŚäžňæĽ ĂèğĄïijŇåŔŚéĂĄèĂĚèť ęæĹůåIJĺéćĎåĹEéĚ■åŘŐæŃěæIJL'5000000000000000000000
* 10^24)äÿłäžčåÿĄïijŇ1äÿłNASæŸŕ1000000000000000000ïijĹ10^18ïijL'äÿłäžčåÿĄïijŇçŤĺäžŐæŤŕäżŸäžď æ

çĎűåŘŐæĹŚäžňæčĂæ§ěæŐěåŔŮèĂĚèť ęæĹůçŽĎçŁűæĂĄãĂĆ

```
> curl -i -H Accept:application/json -X POST http://localhost:8685/
 ↪v1/user/accountstate -d '{"address":
 ↪"n1SQe5d1NKHYFMKtJ5sNHPsSPVavGzW71Wy"}'

{"result":{"balance":"0","nonce":"0","type":87}}
```

åęĆæĹŚäžňæIJ§æIJŻçŽĎéĆčæăůïijŇæŰřèť ęæĹůæšąæIJL'äżżä¡Ţäžčåÿ ĄãĂĆ

åŔŚéĂĄäžď æŸŞ

æŐěäÿŃæİěïijŇæĹŚäžňåřĘäżŃçż■æŸ§äžŚéŞ¿äÿŁäÿL'çğ■åŔŚéĂĄäžď æŸŞçŽĎæŰźåijŔãĂĆ

ç■¿åŘ■ & åŔŚéĂĄ

ä¡£çŤĺè£Źçğ■æŰźåijŔïijŇæĹŚäžňåŔŕäžěåIJÍçężçž£çŐŕåćČäÿŃåĚĹä¡£çŤĺçğĄéŠěç■¿åŘ■åě¡äžď æŸŞïijŃ
Walletæ■čæŸŕå§žäžŐNeb.jséĞĞçŤĺè£Źçğ■æŰźæşŢåŔŚéĂĄçŽĎäžď æŸŞãĂĆ

éęŰåĚĹïijŇæĹŚäžňä¡£çŤĺAdmin Moduleäÿ■çŽĎv1/admin/
signæŐěåŘčçżŹåĞĘåď ĞåŔŚçŽĎäžď æŸŞç■¿åŘ■ïijŇå¿ŮåĹřäžď æŸŞçŽĎäžŇè£ŻåĹűæŢřæ■õãĂĆ

```
> curl -i -H 'Content-Type: application/json' -X POST http://
 ↪localhost:8685/v1/admin/sign -d '{"transaction":{"from":
 ↪"n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE","to":
 ↪"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5", "value":
 ↪"1000000000000000000","nonce":1,"gasPrice":"1000000","gasLimit":
 ↪"2000000"}, "passphrase":"passphrase"}'

{"result":{"data":"CiAbjMP5dyVsTWILfXL1MbwZ8Q6xOgX/
 ↪JKinks1dpToSdxIaGVcH+WT/
 ↪SVMkY18ix7SG4F1+Z8evXJoA35caGhlXbip8PupTNxwV4SRM87r798jXWADXpWngIhAAAAAAAAAAAA
 ↪"}}
```

æŔŘçď žïijŽåIJĺåŔŚéĂĄäžď æŸŞæŮűïijŇåŕźäžŐåŘŇäÿĂäÿłèť ęæĹůïijŇåŔłæIJL'å¡ŞäžŰNonceäÿžNç

çĎűåŘŐïijŇæĹŚäžňåřĘç■¿åě¡åŘ■çŽĎäžď æŸŞåŐ§ågŃæŢřæ■õæŔŘäžď åĹřæIJňåIJřçğĄæIJL'éŞ¿éĞŃç

```
> curl -i -H 'Content-Type: application/json' -X POST http://
 ↪localhost:8685/v1/user/rawtransaction -d '{"data":
 ↪"CiAbjMP5dyVsTWILfXL1MbwZ8Q6xOgX/JKinks1dpToSdxIaGVcH+WT/
 ↪SVMkY18ix7SG4F1+Z8evXJoA35caGhlXbip8PupTNxwV4SRM87r798jXWADXpWngIhAAAAAAAAAAAA
 ↪"}'

{"result":{"txhash":
 ↪"1b8ec3f977256c4d620b7d72f531bc19f10eb13a05ff24a8a792cd5da53a1277
 ↪","contract_address":""}}âŔŐ
```

åŕĘçăĄ & åŔŚéĂĄ

åęĆæđIJä¡ăä£ąäżżäÿĂäÿłæŸ§äžŚèŁĆçĆźåÿőä¡ăä£İå■ŸkeystoreæŰĞäżűïijŇä¡ååŕŕäżěä¡£çŤĺçňňäžŇçğ■

éęŰåĚĹïijŇäÿŁäijää¡ăçŽĎkeystoreæŰĞäżűåĹřä¡ăä£ąäżżçŽĎæŸ§äžŚèŁĆçĆźçŽĎkeydiræŰĞäżűåď´źäÿ

```
cp /path/to/keystore.json /path/to/keydir/
```

çĎűåŘŐïijŇæĹŚäžňåŔŚéĂĄäžď´æŸŞçŽĎåŘŇæŮűïijŇåÿęäÿŁæĹŚäžňkeystoreçŽĎåŕĘçăĄïijŇåIJĺèćńä£

```
> curl -i -H 'Content-Type: application/json' -X POST http://
 ↪localhost:8685/v1/admin/transactionWithPassphrase -d '{
 ↪"transaction":{"from":"n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE","to":
 ↪"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5", "value":
 ↪"1000000000000000000","nonce":2,"gasPrice":"1000000","gasLimit":
 ↪"2000000"},"passphrase":"passphrase"}'

{"result":{"txhash":
 ↪"3cdd38a66c8f399e2f28134e0eb556b292e19d48439f6afde384ca9b60c27010
 ↪","contract_address":""}}
```

æŔŘçď´žïijŽåŽääÿžæĹŚäžňåIJĺäźŃåL’■ä¡£çŤĺn1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptEåŔŚ

èğčéŤĄ & åŔŚéĂĄ

è£ŹæŸŕæIJĂå■śéŹl’çŽĎåŔŚéĂĄäžď´æŸŞçŽĎæŰźæşŢãĂĆéŹď´éIđä¡ääőŇåĚĺä£ąäżżäÿĂäÿłæŸ§äžŚèŁĆ

éęŰåĚĹïijŇäÿŁäijää¡ăçŽĎkeystoreæŰĞäżűåĹřä¡ăä£ąäżżçŽĎæŸ§äžŚèŁĆçĆźçŽĎkeydiræŰĞäżűåď´źäÿ

```
cp /path/to/keystore.json /path/to/keydir/
```

çĎűåŘŐïijŇä¡£çŤĺä¡ăçŽĎkeystoreæŰĞäżűçŽĎåŕĘçăĄïijŇåIJĺæŇĞäőŽçŽĎæŮűéŮť’èŇČåŽť´æIěåIJĺèćń

```
> curl -i -H 'Content-Type: application/json' -X POST http://
 ↪localhost:8685/v1/admin/account/unlock -d '{"address":
 ↪"n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE","passphrase":"passphrase",
 ↪"duration":"300000000000"}'

{"result":{"result":true}}
```

äÿĂæŮęäÿĂäÿłèť´ęæĹůåIJĺèŁĆçĆźäÿŁèćńèğčéŤĄïijŇäżżä¡Ţåŕŕäžěèő£éŮőèŕěæIJžåŹĺSendTransactiona

```
> curl -i -H 'Content-Type: application/json' -X POST http://
 ↪localhost:8685/v1/admin/transaction -d '{"from":
 ↪"n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE","to":
 ↪"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5", "value":
 ↪"1000000000000000000","nonce":3,"gasPrice":"1000000","gasLimit":
 ↪"2000000"}'
```

```
{"result":{"txhash":
↪"8d69dea784f0edfb2ee678c464d99e155bca04b3d7e6cdba6c5c189f731110cf
↪","contract_address":""}}âŔŐ
```

äžď'æŸŞæŤűæ■ő

äÿ■èőžä¡£çŤĺçŽĎåŞłäÿĂçğ■æŰźæşŢåŔŚéĂĄäžď'æŸŞïijŇæĹŚäżňéČ¡äijŽå¿ŮåĹřäÿď'äÿłè£ŤåŻđåĂijïijĺ

ä¡£çŤĺtxhashæĹŚäżňåŔŕäžĕæ§ěçIJŃäžď'æŸŞæŤűæ■őïijŇç§ěéĄŞå¡ŞåL'■äžď'æŸŞçŽĎçŁűæĂĄãĂĆ

```
> curl -i -H Accept:application/json -X POST http://localhost:8685/
↪v1/user/getTransactionReceipt -d '{"hash":
↪"8d69dea784f0edfb2ee678c464d99e155bca04b3d7e6cdba6c5c189f731110cf
↪"}'

{"result":{"hash":
↪"8d69dea784f0edfb2ee678c464d99e155bca04b3d7e6cdba6c5c189f731110cf
↪","chainId":100,"from":"n1FF1nz6tarkDVwWQkMnnwFPuPKUaQTdptE","to":
↪"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5","value":"1000000000000000000
↪","nonce":"3","timestamp":"1524667888","type":"binary","data
↪":null,"gas_price":"1000000","gas_limit":"2000000","contract_
↪address":"","status":1,"gas_used":"20000"}}âŔŐ
```

è£ŹéĞŇçŽĎstatusåŔŕèČ¡æIJL'äÿL'çğ■çŁűæĂĄåĂijïijŇ0ïijŇ1åŠŇ2ãĂĆ

- **0: äžď'æŸŞåď'śèt'ě.** èąĺçď'žå¡ŞåL'■äžď'æŸŞåůšçżŔäÿŁéŞ¿ïijŇä¡ĘæŸŕæL'ğèąŇåď'śèt'ěäžĘãĂĆåŔŕèČ¡
- **1: äžď'æŸŞæĹŘåŁ§.** èąĺçď'žå¡ŞåL'■äžď'æŸŞåůšçżŔäÿŁéŞ¿ïijŇèĂŇäÿŤæL'ğèąŇæĹŘåŁ§äžĘãĂĆ
- **2: äžď'æŸŞå¿ĚåőŽ.** èąĺçď'žå¡ŞåL'■äžď'æŸŞè£Ÿæšąæ IJL'äÿŁéŞ¿ãĂĆåŔŕèČ¡æŸŕåŻääÿžå¡ŞåL'■äžď'æŸ

åď■æ§ěæŐěåŔŮèĂĚèt'ęæĹůä¡Źéći

æĹŚäżňåď'■æ§ěäÿĂäÿŇæŐěåŔŮèĂĚèt'ęæĹůäÿŁçŽĎéŠśæŸŕåŘęåůšçżŔåĹřèt'ęäžĘãĂĆ

```
> curl -i -H Accept:application/json -X POST http://localhost:8685/
↪v1/user/accountstate -d '{"address":
↪"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5"}'

{"result":{"balance":"3000000000000000000","nonce":"0","type":87}}
```

æĹŚäżňçŤĺäÿL'çğ■æŰźåijŔåĹĘåĹńåŔŚéĂĄäžĘäÿĂçňŤè¡ňèt'ęïijŇærŔçňŤè¡ňäÿĂäÿłNASïijŇæL'Ăäžěè

äÿŃäÿĂçńă

çijŰåĘŹåźűè£ŘèąŇæŹžèČ¡åŘĹçžę

3.3.8 Nebulas 101 - 03 çijŰåĘŹåźűè£ŘèąŇæŹžèČ¡åŘĹçžę

åIJÍè£ŹçŕĞæŢŹçÍŃäÿ■æĹŚäžňäijŽå■ęäźăæĂŐæăůåIJÍNebulasäÿ■çijŰåĘŹãĂĄéČÍç¡šåźűæĽğèąŇæŹžèČ

åĞĘåďĞåůëä¡IJ

åIJÍè£ŽåĚěæŹžèČ¡åŘĹçžęäźŃåĽ■ïijŇåĚĹæÿľ'äźăäÿŃåĚĹåĽ■å■ęè£ĞçŽĎåĘĚåőźïijŽ

1. åőĽ'èčĚãĂĄçijŰèŕŚåźűåŘŕåŁĺnebåžŤçŤÍ
2. åĹŻåžžéŠśåŇĚåIJŕåİĂïijŇèő¿ç¡őcoinbaseïijŇåźűåijĂåğŃæŇŰç§£
3. æ§ěèŕćnebèŁĆçĆźä£ąæĄŕãĂĄéŠśåŇĚåIJŕåİĂä¡ŹéćİçL'
4. åŔŚéĂĄè¡ňèť'ęäžď'æŸŞïijŇåźűéłŇèŕĄäžď'æŸŞæŸŕåŘęæĹŘåŁ§

åęĆæđIJåŕźäÿŁè£řçŽĎåĘĚåőźæIJL'çŰŚæČŚçŽĎåŘŇå■ęåŔŕäžěéĞ■æŰřåŐżå■ęäźăåL'■éİćçŽĎçńäèŁĆïi

1. çijŰåĘŹæŹžèČ¡åŘĹçžę
2. éČÍç¡šæŹžèČ¡åŘĹçžę
3. èřČçŤÍæŹžèČ¡åŘĹçžęïijŇéłŇèŕĄåŘĹçžęæL'ğèąŇçżŞæđIJ

çijŰåĘŹæŹžèČ¡åŘĹçžę

èů§äžěåď'łåİŁçśžäijijïijŇNebulasåőđçŐřäžĘNVMèŹŽæŃ§æIJžæİěè£ŘèąŇæŹžèČ¡åŘĹçžęïijŇNVMçŽĎ
V8åijŢæŞŐïijŇæL'Ăäžěå¡ŞåL'■çŽĎåijĂåŔŚçL'ĹïijŇæĹŚäžňåŔŕäžěä¡£çŤÍJavaScriptãĂĄTypeScriptæİěçijŰå

çijŰåĘŹæŹžèČ¡åŘĹçžęçŽĎçőĂèęĄègĎèŇČïijŽ

1. æŹžèČ¡åŘĹçžęäžčçăĄå£ĚéążæŸŕäÿĂäÿłPrototypeçŽĎåŕźèśąïijŻ
2. æŹžèČ¡åŘĹçžęäžčçăĄå£ĚéążæIJL'äÿĂäÿłinit()çŽĎæŰźæşŢïijŇè£ŹäÿłæŰźæşŢåŔłäijŽåIJÍéČÍç¡šçŽĎa
3. æŹžèČ¡åŘĹçžęéĞŇéİćçŽĎçğĄæIJL'æŰźæşŢæŸŕäžě_åijĂåď't'çŽĎæŰźæşŢïijŇçğĄæIJL'æŰźæşŢäÿ■è

äÿŃéİćæĹŚäžňä¡£çŤÍJavaScriptæİěçijŰåĘŹçňäÿĂäÿłæŹžèČ¡åŘĹçžęïijŽéŞűèąŇä£İéŹľæ§IJãĂĆ
è£ŹäÿłæŹžèČ¡åŘĹçžęéIJĂèęĄåőđçŐřäžěäÿŃåŁ§èČ¡ïijŽ

1. çŤÍæĹůåŔŕäžěåŘŚè£ŹäÿłéŞűèąŇä£İéŹľæ§IJå■ŸéŠśãĂĆ
2. çŤÍæĹůåŔŕäžěäżŐè£ŹäÿłéŞűèąŇä£İéŹľæ§IJåŔŰéŠśãĂĆ
3. çŤÍæĹůåŔŕäžěæ§ěèŕćéŞűèąŇä£İéŹľæ§IJäÿ■çŽĎä¡ŹéćİãĂĆ

æŹžèČ¡åŘĹçžęçď'žä¿ŃïijŽ

```
'use strict';

var DepositeContent = function (text) {
  if (text) {
    var o = JSON.parse(text);
    this.balance = new BigNumber(o.balance);
    this.expiryHeight = new BigNumber(o.expiryHeight);
```

```
  } else {
    this.balance = new BigNumber(0);
    this.expiryHeight = new BigNumber(0);
  }
};

DepositeContent.prototype = {
  toString: function () {
    return JSON.stringify(this);
  }
};

var BankVaultContract = function () {
  LocalContractStorage.defineMapProperty(this, "bankVault", {
    parse: function (text) {
      return new DepositeContent(text);
    },
    stringify: function (o) {
      return o.toString();
    }
  });
};

// save value to contract, only after height of block, users can␣
↪takeout
BankVaultContract.prototype = {
  init: function () {
    //TODO:
  },

  save: function (height) {
    var from = Blockchain.transaction.from;
    var value = Blockchain.transaction.value;
    var bk_height = new BigNumber(Blockchain.block.height);

    var orig_deposit = this.bankVault.get(from);
    if (orig_deposit) {
      value = value.plus(orig_deposit.balance);
    }

    var deposit = new DepositeContent();
    deposit.balance = value;
    deposit.expiryHeight = bk_height.plus(height);

    this.bankVault.put(from, deposit);
  },

  takeout: function (value) {
    var from = Blockchain.transaction.from;
    var bk_height = new BigNumber(Blockchain.block.height);
```

```
    var amount = new BigNumber(value);

    var deposit = this.bankVault.get(from);
    if (!deposit) {
      throw new Error("No deposit before.");
    }

    if (bk_height.lt(deposit.expiryHeight)) {
      throw new Error("Can not takeout before expiryHeight.");
    }

    if (amount.gt(deposit.balance)) {
      throw new Error("Insufficient balance.");
    }

    var result = Blockchain.transfer(from, amount);
    if (!result) {
      throw new Error("transfer failed.");
    }
    Event.Trigger("BankVault", {
      Transfer: {
        from: Blockchain.transaction.to,
        to: from,
        value: amount.toString()
      }
    });

    deposit.balance = deposit.balance.sub(amount);
    this.bankVault.put(from, deposit);
  },
  balanceOf: function () {
    var from = Blockchain.transaction.from;
    return this.bankVault.get(from);
  },
  verifyAddress: function (address) {
    // 1-valid, 0-invalid
    var result = Blockchain.verifyAddress(address);
    return {
      valid: result == 0 ? false : true
    };
  }
};
module.exports = BankVaultContract;
```

äÿŁéİćæŹžèČ¡åŘĹçžęçŽĎçď'žä¿ŃåŔŕäżěçIJŃåĹřïijŇBankVaultContractæŸŕäÿĂäÿłprototypeåŕźè

BankVaultContractåőđçŐřäžĘåŔęåď'ŰäÿđäÿłæŰźæşŢïijŽ

- save(): çŤĺæĹůåŔŕäżěéĂŽè£ĞèřČçŤĺsave()æŰźæşŢåŘŚéŞűèąŇä£ĺéŹľæ§IJå■ŸéŠśïijŻ
- takeout(): çŤĺæĹůåŔŕäżěéĂŽè£ĞèřČçŤĺtakeout()æŰźæşŢåŘŚéŞűèąŇä£ĺéŹľæ§IJåŘŰéŠśïijŻ

- balanceOf(): çŤÍæĹůåŔŕäžěéĂŽè£ĞèřČçŤÍbalanceOf()æŰźæşŢåŘŚéŞűèąŇä£ÍéŹľæ§IJæ§ěèřćä¡ŹéćÍïij äÿŁéÍćçŽĎåŘĹçžęäžčçăĄçŤÍåĹřäžĘåĘĚç¡őçŽĎBlockchainåŕźèśąåŠŇåĘĚç¡őçŽĎBigNumber()æ

  save():

```
// Deposit the amount into the safe

save: function (height) {
  var from = Blockchain.transaction.from;
  var value = Blockchain.transaction.value;
  var bk_height = new BigNumber(Blockchain.block.height);

  var orig_deposit = this.bankVault.get(from);
  if (orig_deposit) {
    value = value.plus(orig_deposit.balance);
  }
  var deposit = new DepositeContent();
  deposit.balance = value;
  deposit.expiryHeight = bk_height.plus(height);

  this.bankVault.put(from, deposit);
},
```

takeout():

```
takeout: function (value) {
  var from = Blockchain.transaction.from;
  var bk_height = new BigNumber(Blockchain.block.height);
  var amount = new BigNumber(value);

  var deposit = this.bankVault.get(from);
  if (!deposit) {
    throw new Error("No deposit before.");
  }

  if (bk_height.lt(deposit.expiryHeight)) {
    throw new Error("Can not takeout before expiryHeight.");
  }

  if (amount.gt(deposit.balance)) {
    throw new Error("Insufficient balance.");
  }

  var result = Blockchain.transfer(from, amount);
  if (!result) {
    throw new Error("transfer failed.");
  }
  Event.Trigger("BankVault", {
    Transfer: {
      from: Blockchain.transaction.to,
      to: from,
```

```
      value: amount.toString()
    }
  });

  deposit.balance = deposit.balance.sub(amount);
  this.bankVault.put(from, deposit);
},
```

éČÍç¡šæŹžèČ¡åŘĹçžę

äÿŁéÌćäżŃçż■äžĘåIJĺNebulasäÿ■æĂŐäźĹåŐżçijŰåĘŹäÿĂäÿłæŹžèČ¡åŘĹçžęïijŇçŐřåIJĺæĹŚäżňéIJÀèęA
& åŔŚéĂAçŽĎæŰźåijŔæÌěåŘŚéĂĄäžďæŸŞãĂĆ

éęŰåĚĹïijŇæĹŚäżňåIJĺconf/default/genesis.confäÿ■éćĎåĹĘéĚ■è£ĞäžčåÿĄçŽĎèt'ęæĹůéĞN

```
> curl -i -H Accept:application/json -X POST http://localhost:8685/
 ↪v1/user/accountstate -d '{"address":
 ↪"n1H4MYms9F55ehcvygwWE71J8tJC4CRr2so"}'

{"result":{"balance":"50000000000000000000000000","nonce":"0","type
 ↪":87}}
```

èŕěèt'ęæĹůæIJL'èűşåď§çŽĎéŠśæÌěæŤŕäžŸæL'Ńçż■èt'źïijŇæŐěäÿŃæÌěïijŇæĹŚäżňèğčéŤĄåŘŚéĂĄèĂĚ

```
> curl -i -H 'Content-Type: application/json' -X POST http://
 ↪localhost:8685/v1/admin/account/unlock -d '{"address":
 ↪"n1H4MYms9F55ehcvygwWE71J8tJC4CRr2so","passphrase":"passphrase",
 ↪"duration":"43200000000000"}'

{"result":{"result":true}}
```

çĎűåŘŐïijŇæĹŚäżňåŘŚéĂĄéČÍç¡šBankVaultåŘĹçžęçŽĎäžď'æŸŞãĂĆ

```
> curl -i -H 'Accept: application/json' -X POST http://
 ↪localhost:8685/v1/admin/transactionWithPassphrase -H 'Content-
 ↪Type: application/json' -d '{"transaction": {"from":
 ↪"n1H4MYms9F55ehcvygwWE71J8tJC4CRr2so","to":
 ↪"n1H4MYms9F55ehcvygwWE71J8tJC4CRr2so", "value":"0","nonce":1,
 ↪"gasPrice":"1000000","gasLimit":"2000000","contract":{"source":"\
 ↪"use strict\";var DepositeContent=function(text){if(text){var␣
 ↪o=JSON.parse(text);this.balance=new BigNumber(o.balance);this.
 ↪expiryHeight=new BigNumber(o.expiryHeight);}else{this.balance=new␣
 ↪BigNumber(0);this.expiryHeight=new BigNumber(0);}};
 ↪DepositeContent.prototype={toString:function(){return JSON.
 ↪stringify(this);}};var BankVaultContract=function()
 ↪{LocalContractStorage.defineMapProperty(this,\"bankVault\",
 ↪{parse:function(text){return new DepositeContent(text);},
 ↪stringify:function(o){return o.toString();}});};BankVaultContract.
 ↪prototype={init:function(){},save:function(height){var␣
 ↪from=Blockchain.transaction.from;var value=Blockchain.transaction.
 ↪value;var bk_height=new BigNumber(Blockchain.block.height);var␣
 ↪orig_deposit=this.bankVault.get(from);if(orig_deposit)
 ↪{value=value.plus(orig_deposit.balance);} var deposit=new␣
 ↪DepositeContent();deposit.balance=value;deposit.expiryHeight=bk_
 ↪height.plus(height);this.bankVault.put(from,deposit);},
```

```
{"result":{"txhash":
↪"aaebb86d15ca30b86834efb600f82cbcaf2d7aaffbe4f2c8e70de53cbed17889
↪","contract_address":"n1rVLTRxQEXscTgThmbTnn2NqdWFEKwpYUM"}}
```

- from: åŘĹçžęåĹŻåžžèĂĚèť¸æĹůåIJřåİĂ
- to: åŠŇfromäÿĂèĞt'ïijŇåŘŇäÿžåŘĹçžęåĹŻåžžèĂĚåIJřåİĂ
- valueïijŽéČĺç¡šåŘĹçžęæŮűäÿž"0"
- nonce: æŕŤåĹŻåžžèĂĚå¡ŞåL'■çŽĎnonceåď'Ž1ïijŇåŕŕäžěéĂŽè£ĞGetAccountStateèŐůåŔŰåĹŻ
- gasPriceïijŽéČĺç¡šæŹžèČ¡åŘĹçžęçŤĺåĹřçŽĎgasPriceïijŇåŕŕäžěéĂŽè£ĞGetGasPriceèŐůåŔŰïijŇæ
- gasLimit: éČĺç¡šåŘĹçžęçŽĎgasLimitïijŇéĂŽè£ĞEstimateGasåŕŕäžěèŐůåŔŰéČĺç¡šåŘĹçžęçŽĎgas
- contract: åŘĹçžęä£ąæĄŕïijŇéČĺç¡šåŘĹçžęæŮűäijäåĚěçŽĎåŔĆæŢř
  - source: åŘĹçžęäžčçăĄ
  - sourceType: åŘĹçžęäžčçăĄçśžåđŃïijŇæŤŕæŇĄjsåŠŇts(åŕźåžŤjavaScriptåŠŇtypeScriptäžč
  - args: åŘĹçžęåĹİåğŃåŇŰæŰźæşŢåŔĆæŢřïijŇæŮäåŔĆæŢřäÿžçľžå■ŮçňęäÿšïijŇæIJL'åŔĆæŢřa

éČĺç¡šæŹžèČ¡åŘĹçžęçŽĎè£ŤåŻđåĂijæŸŕtransactionçŽĎhashåIJřåİĂtxhashåŠŇåŘĹçžęçŽĎéČĺç¡šåIJ
å¿ŮåĹřè£ŤåŻđåĂijåźűäÿ■èČ¡ä£ÌèŕĄåŘĹçžęåůšçżŔéČĺç¡šæĹŘåŁ§ïijŇåŽääÿžåŔŠéĂĄäžď'æŸŞæŸŕäÿĂäÿłåi

élŇèŕĄåŘĹçžęæŸŕåŘęéČĺç¡šæĹŘåŁ§

åIJĺéČĺç¡šæŹžèČ¡åŘĹçžęçŽĎæŮűåĂŹå¿ŮåĹřäžĘtransactionçŽĎhashåIJřåİĂtxhashïijŇæĹŚäžňåŔŕä

```
> curl -i -H 'Content-Type: application/json' -X POST http:/
↪/localhost:8685/v1/user/getTransactionReceipt -d '{"hash":
↪"aaebb86d15ca30b86834efb600f82cbcaf2d7aaffbe4f2c8e70de53cbed17889
↪"}'

{"result":{"hash":
↪"aaebb86d15ca30b86834efb600f82cbcaf2d7aaffbe4f2c8e70de53cbed17889
↪","chainId":100,"from":
↪"n1H4MYms9F55ehcvygwWE71J8tJC4CRr2so","to":
↪"n1H4MYms9F55ehcvygwWE71J8tJC4CRr2so","value":"0","nonce":
↪"1","timestamp":"1524711841","type":"deploy","data":
↪"eyJTb3VyY2VUeXBlIjoianMiLCJTb3VyY2UiOiJcInVzZSBzdHJpY3RcIjt2YXIgRGVwb3Npc
↪ZmFsc2U6dHJ1ZX07fX07bW9kdWxlLmV4cG9ydHM9QmFua1ZhdWx0Q29udHJhY3Q7IiwiQXJncy
↪","gas_price":"1000000","gas_limit":"2000000","contract_
↪address":"n1rVLTRxQEXscTgThmbTnn2NqdWFEKwpYUM","status":1,
↪"gas_used":"22016"}}
```

åęĆäÿŁæL'Äçď'žïijŇéČĺç¡šåŘĹçžęçŽĎäžď'æŸŞçŽĎçŁűæĂĄåŔŸæĹŘäžĘ1ïijŇèąĺçď'žåŘĹçžęéČĺç¡šæ

æĽ'ğèąŇæŹžèČ¡åŘĹçžęæŰźæşŢ

åIJÍNebulasäÿ■èřĈçŤĺæŹžèČ¡åŘĹçžęçŽĎæŰźåijŔäź§å¿ĹçőĂå■ŢïijŇåŘŇæăůæŸŕéĂŽè£ĞåŔŠéĂĄäžď'

èřČçŤÍæŹžèČ¡åŘĹçžęçŽĎsaveæŰźæşŢ

```
> curl -i -H 'Accept: application/json' -X POST http://
 ↪localhost:8685/v1/admin/transactionWithPassphrase -H 'Content-
 ↪Type: application/json' -d '{"transaction":{"from":
 ↪"n1LkDi2gGMqPrjYcczUiweyP4RxTB6Go1qS","to":
 ↪"n1rVLTRxQEXscTgThmbTnn2NqdWFEKwpYUM", "value":"100","nonce":1,
 ↪"gasPrice":"1000000","gasLimit":"2000000","contract":{"function":
 ↪"save","args":"[0]"}}, "passphrase": "passphrase"}'

{"result":{"txhash":
 ↪"5337f1051198b8ac57033fec98c7a55e8a001dbd293021ae92564d7528de3f84
 ↪","contract_address":""}}
```

- from: çŤÍæĹůçŽĎèt'ęæĹůåIJřåİĂ
- to: æŹžèČ¡åŘĹçžęåIJřåİĂ
- value: èřČçŤÍsave()æŰźæşŢæŮűæČşèęĄå■ŸåĚěæŹžèČ¡åŘĹçžęäžčåÿĄæŢřéĞŔ
- nonce: æŕŤåĹŻåžžèĂĚå¡ŞåL'■çŽĎnonceåd'Ž1ïijŇåŔŕäżěéĂŽè£ĞGetAccountStateèŐůåŔŰůåĹŻ
- gasPriceïijŽéČĺç¡šæŹžèČ¡åŘĹçžęçŤĺåĹřçŽĎgasPriceïijŇåŔŕäżěéĂŽè£ĞGetGasPriceèŐůåŔŰïijŇæ
- gasLimit: éČĺç¡šåŘĹçžęçŽĎgasLimitïijŇéĂŽè£ĞEstimateGasåŔŕäżěèŐůåŔŰéČĺç¡šåŘĹçžęçŽĎgas
- contract: åŘĹçžęä£ąæĄŕïijŇéČĺç¡šåŘĹçžęæŮűäijååĚěçŽĎåŔĆæŢř
  - function: èřČçŤĺåŘĹçžęæŰźæşŢ
  - args: åŘĹçžęæŰźæşŢåŔĆæŢřïijŇæŮååŔĆæŢřäÿžçl'žå■ŮçňęäÿšïijŇæIJL'åŔĆæŢřæŮűäÿžJSON

élŇèŕĄæŹžèČ¡åŘĹçžęçŽĎæŰźæşŢsaveæŸŕåŘęæL'ğèąŇæĹŘåŁ§

çŤśäžŐæL'ğèąŇåŘĹçžęæŰźæşŢæIJňèt'ÍæŸŕæŔŘäžd'äÿĂäÿłäžd'æŸŞïijŇæL'ĂäžěæĺŝäžňåŔŕäżěéĂŽè

```
> curl -i -H 'Content-Type: application/json' -X POST http:/
 ↪/localhost:8685/v1/user/getTransactionReceipt -d '{"hash":
 ↪"5337f1051198b8ac57033fec98c7a55e8a001dbd293021ae92564d7528de3f84
 ↪"}'

{"result":{"hash":
 ↪"5337f1051198b8ac57033fec98c7a55e8a001dbd293021ae92564d7528de3f84
 ↪","chainId":100,"from":
 ↪"n1LkDi2gGMqPrjYcczUiweyP4RxTB6Go1qS","to":
 ↪"n1rVLTRxQEXscTgThmbTnn2NqdWFEKwpYUM","value":"100","nonce
 ↪":"1","timestamp":"1524712532","type":"call","data":
 ↪"eyJGdW5jdGlvbiI6InNhdmUiLCJBcmdzIjoiWzBdIn0=","gas_price
 ↪":"1000000","gas_limit":"2000000","contract_address":"",
 ↪"status":1,"gas_used":"20361"}}
```

åęĆäÿŁæL'Ăçd'žïijŇäžd'æŸŞçŁűæĂĄåŔŸäÿžäžĘ1ïijŇèąĺçd'žæL'ğèąŇsaveæŰźæşŢæĹŘåŁ§äžĘãĂĆ

èřČçŤÍæŹžèČ¡åŘĹçžęçŽĎtakeoutæŰźæşŢ

```
> curl -i -H 'Accept: application/json' -X POST http://
 ↪localhost:8685/v1/admin/transactionWithPassphrase -H 'Content-
 ↪Type: application/json' -d '{"transaction":{"from":
 ↪"n1LkDi2gGMqPrjYcczUiweyP4RxTB6Go1qS","to":
 ↪"n1rVLTRxQEXscTgThmbTnn2NqdWFEKwpYUM", "value":"0","nonce":2,
 ↪"gasPrice":"1000000","gasLimit":"2000000","contract":{"function":
 ↪"takeout","args":"[50]"}}, "passphrase": "passphrase"}'

{"result":{"txhash":
 ↪"46a307e9beb21f52992a7512f3705fe58ee6c1887122a1b52f5ce5fd5f536a91
 ↪","contract_address":""}}
```

élŇèŕĄæŹžèČ¡åŘĹçžęçŽĎæŰźæşŢtakeoutæŸŕåŘęæL'ğèąŇæĹŘåŁ§

åIJÍäÿŁéİćsaveæŰźæşŢçŽĎæL'ğèąŇäÿ■ïijŇæĹŚäžňåIJÍåŘĹçžęn1rVLTRxQEXscTgThmbTnn2NqdW

```
> curl -i -H 'Content-Type: application/json' -X POST http:/
 ↪/localhost:8685/v1/user/accountstate -d '{"address":
 ↪"n1rVLTRxQEXscTgThmbTnn2NqdWFEKwpYUM"}'

{"result":{"balance":"50","nonce":"0","type":88}}
```

çżŞædIJåŠŇécĎæIJ§çŻÿçňęãĂĆ

æ§èèŕćæŹžèČ¡åŘĹçžęæŢřæ■ő

åIJÍæŹžèČ¡åŘĹçžęäÿ■ïijŇæĹŚäžňæIJL'äÿĂäžŻæŰźæşŢåźűäÿ■æŻť'æŤźåŘĹçžęçŽĎçŁűæĂĄïijŇè£ŹäžZ
Moduleäÿ■äÿžçŤÍæĹůæŔŘä¿ŻäžĘCallæŐěåŔčæİěåÿőåŁl'çŤÍæĹůæİěæL'ğèąŇè£ŹäžŻåŔłèŕżçŽĎæŰźæşŢï

æĹŚäžňèřČçŤÍåŘĹçžęn1rVLTRxQEXscTgThmbTnn2NqdWFEKwpYUMäÿ■çŽĎbalanceOfæŰźæş

```
> curl -i -H 'Accept: application/json' -X POST http://
 ↪localhost:8685/v1/user/call -H 'Content-Type: application/json' -
 ↪d '{"from":"n1LkDi2gGMqPrjYcczUiweyP4RxTB6Go1qS","to":
 ↪"n1rVLTRxQEXscTgThmbTnn2NqdWFEKwpYUM","value":"0","nonce":3,
 ↪"gasPrice":"1000000","gasLimit":"2000000","contract":{"function":
 ↪"balanceOf","args":""}}'

{"result":{"result":"{\"balance\":\"50\",\"expiryHeight\":\"84\"}",
 ↪"execute_err":"","estimate_gas":"20209"}}
```

äÿŃäÿĂçńă

æŹžèČ¡åŘĹçžęå■ŸåĆĺåŇž

3.3.9 Nebulas 101 - 04 æŹžèČ¡åŘĹçžęå■ŸåĆĺåŇž

åL'■éİćæĹŚäžňäžŃçż■äžĘæĂŐäźĹçijŰåĘŹæŹžèČ¡åŘĹçžęäžěåŔŁæĂŐæăůåIJĺæŸ§äžŚéŞ¿éČĺç¡šåŠŇèř

äžŁåd'l'æĹŚäžňæİèèŕęçżĘçŽĎäżŃçż■æIJL'åĚşæŸ§äžŚéŞ¿æŹžèČ¡åŘĹçžęçŽĎå■ŸåĆĺãĆæŸ§äžŚéŞ¿æ
contract)æŔŘä¿ŻäžĘéŞ¿äÿŁæŢřæ■őå■ŸåĆĺåŁ§èČ¡ãĂĆçśżäijijäžŐäijăçż§çŽĎkey-
valueå■ŸåĆĺçşżçż§ïijĹeg:redisïijL'ïijŇåŔŕäžěäžŸèť źïijĹæűĹèĂŮgasïijL'åřĘæŢřæ■őå■ŸåĆĺåĹræŸ§äžŚéŞ¿äj

LocalContractStorage

æŸ§äžŚéŞ¿çŽĎæŹžèČ¡åŘĹçžęè£ŘèąŇçŐŕåćČåĘĚç¡őäžĘå■ŸåĆĺårźèśąLocalContractStorageïij

å§žçąĂçŤĺæşŢ

LocalContractStorageçŽĎçőĂå■ŢæŐěåŔčåŇĚæŃňset,get,delæŐěåŔčïijŇåðđçŐřäžĘå■ŸåĆ

LocalContractStorageå■ŸåĆĺæŢřæ■ő

```
// å■ŸåĆĺæŢřæ■őïijŇæŢřæ■őäijžèćńjsonåžŘåĹŮåŇŰæĹŘå■Ůçňęäÿšä£Ìå■Ÿ
LocalContractStorage.put(key, value);
// æĹŰèĂĚ
LocalContractStorage.set(key, value);
```

LocalContractStorageèŕżåŘŰæŢřæ■ő

```
// èŐůåŘŰæŢřæ■ő
LocalContractStorage.get(key);
```

LocalContractStorageåĹăéŹd'æŢřæ■ő

```
// åĹăéŹd'æŢřæ■ő, æŢřæ■őåĹăéŹd'åŘŐæŮăæşŢèŕżåŘŰ
LocalContractStorage.del(key);
// æĹŰèĂĚ
LocalContractStorage.delete(key);
```

äÿŃéİćæŸŕäÿĂäÿłåĚůä¡ŞåIJĺåŘĹçžęäÿ■ä¡£çŤĺLocalContractStorageçŽĎåðđä¿ŃïijŽ

```
'use strict';

var SampleContract = function () {
};

SampleContract.prototype = {
    init: function () {
    },
    set: function (name, value) {
        // å■ŸåĆĺå■Ůçňęäÿš
        LocalContractStorage.set("name",name);
        // å■ŸåĆĺæŢřå■Ů
```

```
        LocalContractStorage.set("value", value);
        // å■ŸåĆÍåŕźèšą
        LocalContractStorage.set("obj", {name:name,value:value});
    },
    get: function () {
        var name = LocalContractStorage.get("name");
        console.log("name:"+name)
        var value = LocalContractStorage.get("value");
        console.log("value:"+value)
        var obj = LocalContractStorage.get("obj");
        console.log("obj:"+JSON.stringify(obj))
    },
    del: function () {
        var result = LocalContractStorage.del("name");
        console.log("del result:"+result)
    }
};

module.exports = SampleContract;
```

énŸçžğçŤÍæşŢ

LocalContractStorageéŹď'äžĘå§žæIJňçŽĎset,get,delæŰźæşŢïijŇè£ŸæŔŘä¿ŻæŰźæşŢæİěç

çżŚåőŽåšđæĂğ

åIJÍçżŚåőŽäÿĂäÿłåŘĹçžęåšđæĂğæŮűïijŇéIJĂèęĄæŔŘä¿Żåŕźèšąåőđä¿ŃïijŇåšđæĂğåŘ■åŠŇåžŔåĹŮåŇ

çżŚåőŽæŐěåŔč

```
// define a object property named `fieldname` to `obj` with␣
↪descriptor.
// default descriptor is JSON.parse/JSON.stringify descriptor.
// return this.
defineProperty(obj, fieldName, descriptor);

// define object properties to `obj` from `props`.
// default descriptor is JSON.parse/JSON.stringify descriptor.
// return this.
defineProperties(obj, descriptorMap);
```

äÿŃéÍćæŸŕäÿĂäÿłåIJÍåŘĹçžęäÿ■ä¡£çŤÍLocalContractStorageçżŚåőŽåšđæĂğçŽĎä¿Ńå■Ř:

```
'use strict';

var SampleContract = function () {
    //␣
↪SampleContractçŽĎ`size`åšđæĂğäÿžå■ŸåĆÍåšđæĂğïijŇåŕź`size`çŽĎèŕżåĘŹäijžå■ŸåĆÍåĹ
```

```
    //␣
↪æ■d'åd'ĎçŽĎ`descriptor`èő¿ç¡őäÿžnullïijŇåřĘä¡£çŤĺéżŸèőd'çŽĎJSON.
↪stringify()åŠŇJSON.parse()
    LocalContractStorage.defineMapProperty(this, "size", null);

    //␣
↪SampleContractçŽĎ`value`åśđæĂğäÿžå■ŸåĆĺåśđæĂğïijŇårź`value`çŽĎèŕżåĘŽäijŽå■ŸåĆĺ
    //␣
↪æ■d'åd'ĎçŽĎ`descriptor`èĞłåőŽäźL'åőđçŐřïijŇå■ŸåĆĺæŮűçŻt'æŐěè¡ñäÿžå■ŮçňęäÿšïijŇ
    LocalContractStorage.defineMapProperty(this, "value", {
        stringify: function (obj) {
            return obj.toString();
        },
        parse: function (str) {
            return new BigNumber(str);
        }
    });
    //␣
↪SampleContractçŽĎåd'ŽäÿłåśđæĂğæL'źéĞŔèő¿ç¡őäÿžå■ŸåĆĺåśđæĂğïijŇårźåžŤçŽĎdescrip
    LocalContractStorage.defineProperties(this, {
        name: null,
        count: null
    });
};
module.exports = SampleContract;
```

çĎűåŘŐïijŇæĹŚäžňåŕŕäžěåęĆäÿŃåIJĺåŘĹçžęéĞŇçŻť æŐěèŕżåĘŹè£ŹäžŻåśđæĂğãĂĆ

```
SampleContract.prototype = {
    // åŘĹçžęéČĺç¡šæŮűèřČçŤĺïijŇéČĺç¡šåŘŐæŮăæşŢäžŇæňąèřČçŤĺ
    init: function (name, count, size, value) {
        // åIJĺéČĺç¡šåŘĹçžęæŮűårĘæŢřæ■őå■ŸåĆĺåĹřéŞ¿äÿŁ
        this.name = name;
        this.count = count;
        this.size = size;
        this.value = value;
    },
    testStorage: function (balance) {
        //␣
↪ä¡£çŤĺvalueæŮűäijŽäżŐå■ŸåĆĺäÿ■èŕżåŔŮéŞ¿äÿŁæŢřæ■őïijŇåźűæăźæ■ődescriptorèő¿ç¡őèČ
        var amount = this.value.plus(new BigNumber(2));
        if (amount.lessThan(new BigNumber(balance))) {
            return 0
        }
    }
};
```

çżŚåőŽMapåšđæĂğ

LocalContractStorageè£ŸæŔŘä¿ŻäžĘåŕźåŘĹçžęäÿ■mapåšđæĂğçŽĎçżŚåőŽæŰźæşŢãĂĆäÿŃéÍćæŸŕäÿĂäÿłçżŚåőŽmapåšđæĂğçŽĎä¿Ńå■ŘïijŽ

```
'use strict';

var SampleContract = function () {
    //␣
↪äÿž`SampleContract`åőŽäźL'`userMap`çŽĎåšđæĂğéŻĘåŘĹïijŇæŢŕæ■őåŔŕäżěéĂŽè£Ğ`userM
    LocalContractStorage.defineMapProperty(this, "userMap");

    //␣
↪äÿž`SampleContract`åőŽäźL'`userBalanceMap`çŽĎåšđæĂğéŻĘåŘĹïijŇåźűäÿŤå■ŸåĆĺåŠŇèŕ
    LocalContractStorage.defineMapProperty(this, "userBalanceMap", {
        stringify: function (obj) {
            return obj.toString();
        },
        parse: function (str) {
            return new BigNumber(str);
        }
    });

    // äÿž`SampleContract`åőŽäźL'åd'ŽäÿłéŻĘåŘĹ
    LocalContractStorage.defineMapProperties(this,{
        key1Map: null,
        key2Map: null
    });
};

SampleContract.prototype = {
    init: function () {
    },
    testStorage: function () {
        // åŕĘæŢŕæ■őå■ŸåĆĺåĹřuserMapäÿ■ïijŇåźűåžŔåĹŮåŇŰåĹřéŞ¿äÿŁ
        this.userMap.set("robin","1");
        //␣
↪åŕĘæŢŕæ■őå■ŸåĆĺåĹřuserBalanceMapäÿ■ïijŇä¡£çŤĺèĞłåőŽäźL'åžŔåĹŮåŇŰåĞ¡æŢŕïijŇä£İå■
        this.userBalanceMap.set("robin",new BigNumber(1));
    },
    testRead: function () {
        //èŕżåŔŰå■ŸåĆĺæŢŕæ■ő
        var balance = this.userBalanceMap.get("robin");
        this.key1Map.set("robin", balance.toString());
        this.key2Map.set("robin", balance.toString());
    }
};

module.exports = SampleContract;
```

éĄ■åŐĘmapæŢřæ■ő

MapæŢřæ■őéĄ■åŐĘ

åIJÍæŹžèČ¡åŘĹçžęäÿ■åęĆæđIJéIJĂèęĄéĄ■åŐĘmapéŻĘåŘĹïijŇåŕŕäžééĞĞçŤĺåęĆäÿŃæŰźåijŕïijŽåőŽ

```
"use strict";

var SampleContract = function () {
   LocalContractStorage.defineMapProperty(this, "arrayMap");
   LocalContractStorage.defineMapProperty(this, "dataMap");
   LocalContractStorage.defineProperty(this, "size");
};

SampleContract.prototype = {
    init: function () {
        this.size = 0;
    },

    set: function (key, value) {
        var index = this.size;
        this.arrayMap.set(index, key);
        this.dataMap.set(key, value);
        this.size +=1;
    },

    get: function (key) {
        return this.dataMap.get(key);
    },

    len:function(){
      return this.size;
    },

    forEach: function(limit, offset){
        limit = parseInt(limit);
        offset = parseInt(offset);
        if(offset>this.size){
           throw new Error("offset is not valid");
        }
        var number = offset+limit;
        if(number > this.size){
          number = this.size;
        }
        var result  = "";
        for(var i=offset;i<number;i++){
            var key = this.arrayMap.get(i);
            var object = this.dataMap.get(key);
            result += "index:"+i+" key:"+ key + " value:" +object+"_
↪";
        }
```

```
        return result;
    }
};

module.exports = SampleContract;
```

éĂŽè£ĞRPC APIåŠŇæŸ§äžŚéŞ¿äžd'äžŠ

3.3.10 Nebulas 101 - 05 éĂŽè£ĞRPCæŐěåŕčäÿŐæŸ§äžŚéŞ¿äžd'äžŠ

æŸ§äžŚéŞ¿èŁĆçĆźåŕŕåŁĺåŘŐåŕŕäžěéĂŽè£ĞRPCè£IJçĺŃæŐğåĹűèő£éŮőãĂĆæŸ§äžŚéŞ¿æŔŘä¿ŻäžĘ

æŸ§äžŚéŞ¿çŽĎè£IJçĺŃèő£éŮőæŸŕGRPCåőđçŐřçŽĎïijŇéĂŽè£ĞäžčçŘĘ(GRPC Gateway)äźšåŕŕäžěéĂŽè£ĞHTTPèő£éŮőãĂĆHTTPèő£éŮőæŸŕRESTfulåőđçŐřçŽĎæŐěåŕčïijŇåŕĆæŢřäÿŐGR

API

æĹŚäžňåůšçżŕåIJĺæŕŕäÿłæŸ§äžŚèŁĆçĆźäÿ■åőđçŐřäžĘRPCæIJ■åŁąåŹĺåŠŇHTTPæIJ■åŁąåŹĺïijŇæŔŘ

æŐěåŕčæĺąåİŮ

çŐřåIJĺïijŇæŸ§äžŚèŁĆçĆźçŽĎæL'ĂæIJL'çŽĎæŐěåŕčèćńåĹĘäÿžäÿd'äÿłæĺąåİŮïijŽAPIåŠŇAdminãĂĆ

- APIïijŽæŔŘä¿ŻæL'ĂæIJL'åŠŇçŤĺæĹůçğĄéŠěæŮååĚşçŽĎæŐěåŕč
- AdminïijŽæŔŘä¿ŻæL'ĂæIJL'åŠŇçŤĺæĹůçğĄéŠěçŻÿåĚşçŽĎæŐěåŕč

åžžèőőæŸ§äžŚèŁĆçĆźåŕźåd'ŰæŔŘä¿ŻæIJ■åŁąæŮűïijŇåŕŕäžěæŁŁAPIæŐěåŕčåijĂæŤ¿çżŹåĚñäijŮïijŇ

éĚ■ç¡őæŰĞäžű

æŸ§äžŚèŁĆçĆźäÿ■çŽĎRPCæIJ■åŁąåŹĺåŠŇHTTPæIJ■åŁąåŹĺéČ¡åŕŕäžěåIJĺèŁĆçĆźçŽĎéĚ■ç¡őäÿ■éĚ■

```
#␣
 ↪çŤĺæĹůäÿŐèŁĆçĆźäžd'äžŠçŽĎæIJ■åŁąéĚ■ç¡őïijŇåŘŇäÿĂåŕŕæIJžåŹĺåŕŕåŁĺåd'Žäÿ
rpc {
    # gRPC APIæIJ■åŁąçńŕåŕč
    rpc_listen: ["127.0.0.1:8684"]
    # HTTP APIæIJ■åŁąçńŕåŕč
    http_listen: ["127.0.0.1:8685"]
    # åijĂæŤ¿åŕŕåŕźåd'ŰæŔŘä¿ŻhttpæIJ■åŁąçŽĎæĺąåİŮ
    http_module: ["api","admin"]
}
```

ä¡£çŤĺåőđä¿Ń

HTTP

éĂŽè£ĞHTTPæŐěåŔčåŠŇæŸ§äžŚèŁĆçĆźäžd'äžŠãĂĆ

GetNebState

æĹŚäžňåŕŕäżěèřČçŤĺAPIæĺąåİŮäÿ■çŽĎGetNebStateæŐěåŔčæİěèŐůåŔŰèŁĆçĆźå¡ŞåL'■çŁűæĂĄï

```
> curl -i -H Accept:application/json -X GET http://localhost:8685/
↪v1/user/nebstate

{"result":{"chain_id":100,"tail":
↪"0aa1cceb7801b110fdd5217ba0a4356780c940133924d1c1a4eb60336934dab1
↪","lib":
↪"0000000000000000000000000000000000000000000000000000000000000000
↪","height":"479","protocol_version":"/neb/1.0.0","synchronized
↪":false,"version":"0.7.0"}}
```

UnlockAccount

æĹŚäžňåŕŕäżěèřČçŤĺAdminæĺąåİŮäÿ■çŽĎUnlockAccountæŐěåŔčæİěåIJĺèŁĆçĆźåĘĚå■Ÿäÿ■èğčéŤ

```
> curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/admin/account/unlock -d '{"address":
↪"n1NrMKTYESZRCwPFDLFKiKREzZKaN1nhQvz", "passphrase": "passphrase"}
↪'

{"result":{"result":true}}
```

RPC

RPCæIJ■åŁąåŹĺå§žäžŐGRPCåőđçŐř. GRPCçŽĎå§žäžŐProtocol BuffersæİěåĄŽåžŔåĹŮåŇŰïijŇä¡ăåŕŕäżěåIJĺæŸ§äžŚRPC ProtobufæŰĞäžűåd'źäÿŇæL'¿åĹřæL'ĂæIJL'çŽĎRPCçŻÿåĚşçŽĎProtoæŰĞäžűåőŽäźL'ãĂĆ

è£ŹéĞŇæIJL'äÿĂäžŻä¡£çŤĺgolangèřČçŤĺRPCæŐěåŔčçŽĎåőđä¿ŃãĂĆ

GetNebState

æĹŚäžňåŕŕäżěä¡£çŤĺAPIæĺąåİŮäÿ■çŽĎGetNebStateæŐěåŔčæİěèŐůåŔŰèŁĆçĆźå¡ŞåL'■çŁűæĂĄã

```
import(
    "github.com/nebulasio/go-nebulas/rpc"
    "github.com/nebulasio/go-nebulas/rpc/pb"
)

// GRPC server connection address configuration
addr := fmt.Sprintf("127.0.0.1:%d",uint32(8684))
conn, err := grpc.Dial(addr, grpc.WithInsecure())
```

```
if err != nil {
    log.Warn("rpc.Dial() failed:", err)
}
defer conn.Close()

// API interface to access node status information
api := rpcpb.NewAPIServiceClient(conn)
resp, err := ac.GetNebState(context.Background(), & rpcpb.
↪GetNebStateRequest {})
if err != nil {
    log.Println("GetNebState", "failed", err)
} else {
    log.Println("GetNebState tail", resp)
}
```

LockAccount

æĹŚäžňåůšçżŕåIJĺäźŃåL'■ä¡£çŤĺHTTPæŐěåŕčæŁŁèťęæĹůn1NrMKTYESZRCwPFDLFKiKREzZKaN
æĹŚäžňåŕŕäžěěřČçŤĺAdminæĺąåİŮäÿ■çŽĎLockAccountåĘ■æňąéŤĄåőŽåőČãĂĆ

```
import(
    "github.com/nebulasio/go-nebulas/rpc"
    "github.com/nebulasio/go-nebulas/rpc/pb"
)

// GRPC server connection address configuration
addr := fmt.Sprintf("127.0.0.1:%d",uint32(8684))
conn, err := grpc.Dial(addr, grpc.WithInsecure())
if err != nil {
    log.Warn("rpc.Dial() failed:", err)
}
defer conn.Close()

// Admin interface to access, lock account address
admin := rpcpb.NewAdminServiceClient(conn)
from := "n1NrMKTYESZRCwPFDLFKiKREzZKaN1nhQvz"
resp, err = management.LockAccount(context.Background(), & rpcpb.
↪LockAccountRequest {Address: from})
if err != nil {
    log.Println("LockAccount", from, "failed", err)
} else {
    log.Println("LockAccount", from, "result", resp)
}
```

æŐěåŔčåĹŮèąĺ

æŻťåď'ŽçŽĎæŐěåŔčåĹŮèąĺèŕůåŔĆèĂČåőŸæŰźæŰĞæąčãĂĆ

- API Module

- Admin Module.

åőŇæĹŘ

æĄ■åŰIJä¡ăæĹŘåŁ§èţřåőŇäžĘæŢťäÿłæŢŹçÍŃ! æňćè£ŐéŸĚèŕżäÿŃåĹŮæŇĞå■ŮæİěåŁäåĚěåőŸæŰźçŽ

Join to Testnet Join to Mainnet

3.4 Todo List

3.4.1 Go-Nebulas

- åÿőåŁl'æţŃèŕŢNebulasïijŇèől'NebulasæŻť'åŁäåĄěåčőïijŇæŻť'åď'ŽèŕęæČĚ
- åÿőåŁl'NebulasåijĂåŔŚåď'Žèŕ■èÍĂçŽĎsdkåžŞïijŇåęĆNode, Ruby, Python, Php, Javaç■L'ç■L'ïijŇæŐěåŔčæŰĞæąč
- åÿőåŁl'NebulasåijĂåŔŚåŔŕäžď'äžŠæŰĞæąčïijŇæŐěåŔčæŰĞæąč

3.4.2 Research

- åÿőåŁl'äijŸåŇŰNebulas RankçőŮæşŢïijŇæŻť'åď'ŽèŕęæČĚ
- åÿőåŁl'NebulasåĹl'çŤĺå¡ćåijŔåŇŰèŕĄæŸŐçŽĎæŰźåijŔèŕĄæŸŐåĚśèŕĘçőŮæşŢPoDçŽĎåőL'åĚÍæĂğï

3.4.3 Wiki

- åÿőåŁl'NebulasæŁŁwikiç£żèŕŚæĹŘä¡ăçŽĎæŕ■èŕ■ïijŇèől'æŻť'åď'ŽäžžäžĘèğčåŇžåİŮéŞ¿ïijŇäžĘèğčNe
- åÿőåŁl'NebulasåĹűä¡IJçğŚæŹőæŢŹçÍŃïijŇåÿőåŁl'æŻť'åď'ŽæšąæIJL'çijŰçÍŃèČŇæŹŕçŽĎäžžçŘĘèğčåź

3.4.4 Explorer

- åÿőåŁl'NebulasåőŇåŰĎåŇžåİŮæţŔèğĹåŹÍïijŇæŻť'åď'ŽèŕęæČĚ

3.4.5 Wallet

- åÿőåŁl'NebulasåőŇåŰĎç¡ŚéąţçL'ĹéŠśåŇĚïijŇæŻť'åď'ŽèŕęæČĚ
- åÿőåŁl'NebulasåőŇåŰĎæąŇéİćçL'ĹéŠśåŇĚïijŇæŻť'åď'ŽèŕęæČĚ

Crash Reporter in Nebulas

In this doc, we introduce the crash reporter in Nebulas, which is used to collect crash reports in Nebulas and send it back to Nebulas Team, so the whole community can help improving the quality of Nebulas.

Overview

We, the Nebulas Team and the Nebulas community, always try our best to ensure the stability of Nebulas, since people put their faith and properties on it. That means critical bugs are unacceptable, and we are aware of that. However, we can't blindly think Nebulas is stable enough or there won't be any bugs. Thus, we have plan B, the crash reporter, to collect crash report and send it back to Nebulas community. We hope the whole community can leverage the crash reports and keep improving Nebulas.

Using crash reporter is a very common practice. For example, Microsoft Windows includes a crash reporting service called Windows Error Reporting that prompts users to send crash reports to Microsoft for online analysis. The information goes to a central database run by Microsoft. Apple also involves a standard crash reporter in macOS, named Crash Reporter. The Crash Reporter can send the crash logs to Apple Inc, for their engineers to review. Opensource community also have their own crash reporter, like Bug Buddy for Gnome, Crashpad for Chrome, Talkback for Mozilla, and etc.

In Nebulas, the crash reporter just works like the other crash reporters. It's aware of the crash, collects necessary information about the crash, and sends it back the Nebulas server. The server is hosted by Nebulas, and accessible for the whole community.

As a opensource, decentralized platform, we are aware of that the crash reporter may violate some users' privacy concern. Thus, we remove all private information in the crash report, like the user name, user id, user's home path and IP address. Furthermore, the crash reporter is optional and users may choose close it if users still have some concerns.

How to use it

To enable or disable the crash reporter, you need to look into the configuration file, `config.conf`, and change `enable_crash_reporter` to `true` to enable it, while `false` to disable it.

How it works

In this section, we would like to share some tech details. If you are not interested in the details, you can ignore this section.

The crash reporter is actually a daemon process, which is started by `neb`. When starting the crash reporter, `neb` will tell it the process id (pid) of `neb` process, and the crash file path. For the crash reporter, it will periodically check if the `neb` process and the crash file exists.

At the time it finds the crash file, it will eliminate the private information and send it back to Nebulas.

Currently, the crash report is generated by the `stderr` output from `neb`. We'd like the work with the whole community to collect detailed information in the future.

3.5 Roadmap of Nebulas

3.5.1 Milestones

- In 2017 December, Nebulas test-net will be online.
- In 2018 Q1, Nebulas v1.0 will be released and main-net will be online (ahead of the original schedules).

v1.0 (2018 Q1)

- Fully functional blockchain, with JavaScript and TypeScript as the languages of Smart Contract.
- A user-friendly Nebulas Wallet for both desktop and mobile device to manage their own assets on Nebulas.
- A web-based Nebulas Block Explorer to let developers and users search and view all the data on Nebulas.

v2.0 (2018 Q4)

- Add Nebulas Rank (NR) to each addresses on Nebulas, help users and developers finding more values inside.
- Implement Developer Incentive Protocol (DIP) to encourage developers build more valuable decentralized applications on Nebulas.

v3.0 (2019 Q4)

- Fully functional Nebulas Force and PoD implementation.

3.5.2 Long term goals

- Scalability for large transaction volume.
- Subchain support.
- Zero-knowledge Proof integration.

3.5.3 Versions

v0.1.0 [done]

Goals

- Implement a nebulas kernel.
- In-memory blockchain with PoW consensus.
- Fully P2P network support.

Download here.

v0.2.0 [done]

Goals

- Provide (RPC) API to submit/query transaction externally.
- Implement Sync Protocol to bootstrap any nodes that join into nebulas network at any time, from any tail.

Core

- Implement transaction pool.
- Prevent record-replay attack of transaction.
- Integrate Protocol Buffer for serialization.

Net

- Refactor the design of network.
- Implement Sync Protocol.
- Implement Broadcast and Relay function.

API

- Add Balance API.
- Add Transaction API.
- Add some debugging API, eg âĂIJDump ChainâĂİ, âĂIJDump BlockâĂİ.

Crypto

- Support Ethereum-keystore file.
- Support multi key files management in KeyStore.

Download here.

v0.3.0 [done]

Goals

- Support disk storage for all blockchain data.
- Add smart contract execution engine, based on Chrome V8.

Core

- Add disk storage with a middleware of storage.
- Implement smart contract transaction.

NVM

- Integrate Chrome V8 as Smart Contract execution engine.

Download here.

v0.4.0 [done]

Goals

- Implement Gas calculating in Smart Contract Execution Engine.
- Support more API.
- Add repl in neb application.
- Add metrics and reporting capability.

Core

- Add Gas related fields in Transaction.
- Implemented Gas calculation mechanism.

NVM

- Add execution limits to V8 Engine.
- Add Gas calculation mechanism.

CMD

- Add repl in neb application

Misc

- Add more API.
- Add metrics and reporting capability.

Download here.

v0.5.0 [done]

Goals

- Prepare for test-net releasing, improve stability.

Core

- Improve stability and missing functions if we miss anything.

Consensus

- Implement DPoS consensus algorithm and keep developing PoD algorithm.

NVM

- Finalize the Gas Cost Matrix.
- Support Event liked pubsub functionality.

Misc

- Add more metrics to monitor the stability of neb applications.

Download here.

v0.6.0 [done]

Goals

- Stability improvement, performance optimization.
- Reconstruct P2P network.
- Redesign block sync logic.

Testnet

- Fix bugs & improv the performance.

Network

- Add *Stream* for single connection management.
- Add *StreamManager* for connections management.
- Implement priority message *chan*.
- Add route table persistence strategy.
- Improve strategy to process TCP packet splicing.

Log

- Add console log(CLog), printing log to both console & log files, to inform developers whatâĂŹs happening in Neb.
- Add verbose log(VLog), printing log to log files, to inform devs how Neb works in details.

- Log adjustment.

Sync

- Use chunk header hash to boost the sync performance.
- Adjust the synchronous retry logic and timeout configuration.
- Fix bugs in synchronization and add more metrics statistics.

Download here.

v0.6.1 [done]

Goals

- Improve test net compatibility.

Core

- Upgrade the storage structure of the block

Download here.

v0.8.0 [done]

Goals

- New Nebulas Block Explorer.
- New Nebulas Wallet.
- New web-based Playground tools to interactive with Nebulas.

v1.0.0 [done]

Goals

- Ready for main-net.
- Support JavaScript and TypeScript as Smart Contract Language.
- Stable and high performance blockchain system.
- Release new Nebulas Block Explorer.
- Release new Nebulas Wallet for both desktop and mobile device.
- A web-based playground tools for developer.

Download explorer.

Download wallet.

Download neb.js.

3.6 Frequently Asked Questions

This document will focus on the technology behind the Nebulas platform. For broader questions, please view the Reddit FAQ.

For a better understanding of the Nebulas platform it's highly recommended to read the Nebulas Technical Whitepaper.

Table of Contents

3.6.1 Nebulas Rank (NR)

Measures value by considering liquidity and propagation of the address. Nebulas Ranking tries to establish a trustful, computable and deterministic measurement approach. With the value ranking system, we will see more and more outstanding applications surfacing on the Nebulas platform.

When will Nebulas Rank (NR) be ready?

answer here

Will dApps with more transactions naturally be ranked higher?

answer here

How does the Nebulas Rank (NR) separate quality dApps from highly transacted dApps?

answer here

Is the Nebulas Ranking algorithm open-source?

Yes

Who can contribute to the algorithm?

At this time the Nebulas core team is responsible for the development of the algorithm. Over time we will open it up to the community to contribute and vote to determine the future of the algorithm.

Can the Nebulas Rank (NR) algorithm be cheated?

We will implement strict manipulation controls, and of course the Nebulas Rank (NR) will continually be evolving to meet the needs of the community.

3.6.2 Nebulas Force (NF)

Supports upgrading core protocols and smart contracts on the chains. It provides self-evolving capabilities to Nebulas system and its applications. With Nebulas Force, developers can build rich applications in fast iterations, and the applications can dynamically adapt to community or market changes.

When will Nebulas Force (NF) be ready?

answer here

Can smart contracts be upgraded?

Yes, [short summary explaining how it works]

How is Nebulas Force (NF) smart contract upgrading better than other solutions that are currently or soon-to-be available?

answer here

Can the Nebulas blockchain protocol code be upgraded without forking?

Yes, [short summary explaining how it works]

Can the Nebulas Virtual Machine (NVM) be upgraded?

Yes, [short summary explaining how it works]

3.6.3 Developer Incentive Protocol (DIP)

Designed to build the blockchain ecosystem in a better way. The Nebulas token incentives will help top developers to create more values in Nebulas.

When will the Developer Incentive Protocol (DIP) be ready?

answer here

Will there be a limit as to how many rewards one dApp can receive?

answer here

Will developers still be able to do their own ICOs?

answer here

Will only the top Nebulas Rank (NR) dApps receive rewards?

answer here

How often will rewards be given?

answer here

How will you stop cheaters?

The way the DIP is is designed makes it very hard for cheaters to be successful. Since smart contracts can only be called passively, it would be highly cost ineffective for a user to try to cheat the system. More about this topic can be read in the Technical Whitepaper.

3.6.4 Proof of Devotion (PoD) Consensus Algorithm

To build a healthy ecosystem, Nebulas proposes three key points for consensus algorithm: speediness, irreversibility and fairness. By adopting the advantages of PoS and PoI, and leveraging NR, PoD will take the lead in consensus algorithms.

When will the Proof of Devotion (PoD) Consensus Algorithm be ready?

answer here

What consensus algorithm will be used until PoD is ready?

answer here

How are bookkeepers chosen?

The PoD consensus algorithm uses the Nebulas Rank (NR) to qualify nodes to be eligible. One node from the set is randomly chosen to propose the new block and the rest will become the validators.

Do bookkeepers still have to stake?

Yes, once chosen to be a validator for a new block, the validator will need to place a deposit to continue.

How many validators will there be in each set?

answer here

What anti-cheating mechanisms are there?

answer here

3.6.5 Nebulas Search Engine

Nebulas constructs a search engine for decentralized applications based on Nebulas value ranking. Using this engine, users can easily find desired decentralized applications from the massive market.

When will the Nebulas Search Engine be ready?

answer here

Will you be able to search dApps not on the Nebulas platform?

answer here

Will the Nebulas Search Engine also be decentralized?

answer here

Will the Nebulas Rank (NR) control the search results ranking?

answer here

What data will you be able to search?

We plan many different ways to be able to search the blockchain:

- crawl relevant webpages and establish mapping between them and the smart contracts
- analyze the code of open-source smart contracts
- establish contract standards that enable easier searching

3.6.6 Fundamentals

Nebulas Name Service (NNS)

By using smart contracts, the Nebulas development team will implement a DNS-like domain system named Nebulas Name Service (NNS) on the chain while ensuring that it is unrestricted, free and open. Any third-party developers can implement their own domain name resolution services independently or based on NNS.

When will the Nebulas Name Service be ready?

answer here

When a name is bid on, how long do others have to place their bid?

answer here

How do others get notified that a name is being bid on?

answer here

When a name is reserved who gets the bid amount?

answer here

If I want to renew my name after one year will I need to deposit more NAS?

answer here

Will we be able to reserve names prior to the launch of NNS?

answer here

Lightning Network

Nebulas implements the lightning network as the infrastructure of blockchains and offers flexible design. Any third-party developers can use the basic service of lightning network to develop applications for frequent transaction scenarios on Nebulas. In addition, Nebulas will launch the worldâĂŹs first wallet app that supports the lightning network.

When will lightning network be supported?

answer here

The Nebulas Token (NAS)

The Nebulas network has its own built-in token, NAS. NAS plays two roles in the network. First, as the original money in the network, NAS provides asset liquidity among users, and functions as the incentive token for PoD bookkeepers and DIP. Second, NAS will be charged as the calculation fee for running smart contracts. The minimum unit of NAS is 10âĹŠ18 NAS.

What will happen to the Nebulas ERC20 tokens when NAS is launched?

answer here

Will dApps on the Nebulas platform be able to issue their owns ICOs and tokens?

answer here

Smart Contracts

What languages will be supported when Main-net launches?

answer here

Will Ethereum Smart Contracts (Solidity) be fully supported?

answer here

What other language support will follow (and when)?

answer here

binary storage

What is recommended way to store binary data in Nebulas blockchain? Is it possible at all? Do you encourage such use of blockchain? Also, i couldn't find information regarding GlobalContractStorage mentioned in docs, what is it?

> Currently binary data can be stored on chain by binary transaction. The limit size of binary is 128k. But we donâĂŹt encourage storing data on the chain because the user might store some illegal data.
>
> `GlobalContractStorage`not currently implemented. It provides support for multiple contract sharing data for the same developer.

ChainID & connect

Can you tell us what the chainID of Mainnet and Testnet is? I have compiled the source code of our nebulas, but not even our test network?

chainID of Nebulas:

- Mainnet: 1
- Testnet: 1001
- private: default 100, users can customize the values.

The network connection:

- Mainnet:
  - source code:master
  - wiki:Mainnet
- Testnet:

- source code:testnet
- wiki:Testnet

smart contract deploy

Our smart contract deployment, I think is to submit all contract code directly, is the deployment method like this?

> Yeah, We can deploy the contract code directly, just as it is to release code to the NPM repository, which is very simple and convenient.

smart contract IDE

We don't have any other smart contract ides, like solidity's "Remix"? Or is there documentation detailing which contract parameters can be obtained? (because I need to implement the random number and realize the logic, I calculate the final random number according to the parameters of the network, so I may need some additional network parameters that will not be manipulated.)

> You can use web-wallet to deploy the contract, it has test function to check the parameters and contract execution result.

CHAPTER 4

DApp Development

4.1 How to Join Nebulas Mainnet

4.1.1 Introduction

We are glad to release Nebulas Mainnet here. Please join and enjoy Nebulas Mainnet.

```
https://github.com/nebulasio/go-nebulas/tree/master
```

Configuration

The Mainnet configuration files are in folder `mainnet/conf`, including

genesis.conf

All configurable information about genesis block is defined in genesis.conf, including

- **meta.chain_id:** chain identity
- **consensus.dpos.dynasty:** the initial dynasty of validators
- **token_distribution:** the initial allocation of tokens

  Attention: DO NOT change the genesis.conf.

config.conf

All configurable information about runtime is defined in config.conf.

Please check the `template.conf` to find more details about the runtime configuration.

Tips: the official seed node info is as below,

```
seed:["/ip4/52.2.205.12/tcp/8680/ipfs/
↪QmQK7W8wrByJ6So7rf84sZzKBxMYmc1i4a7JZsne93ysz5","/ip4/52.56.55.
↪238/tcp/8680/ipfs/QmVy9AHxBpd1iTvECDR7fvdZnqXeDhnxkZJrKsyuHNYKAh",
↪"/ip4/13.251.33.39/tcp/8680/ipfs/
↪QmVm5CECJdPAHmzJWN2X7tP335L5LguGb9QLQ78riA9gw3"]
```

API List

Main Endpoint:

| API | URL | Protocol | | — | :—: | :—: | | RESTful | https://mainnet.nebulas.io/ | HTTP |

- GetNebState : returns nebulas client info.
- GetAccountState: returns the account balance and nonce.
- Call: execute smart contract local, don't submit on chain.
- SendRawTransaction: submit the signed transaction.
- GetTransactionReceipt: get transaction receipt info by tansaction hash.

More Nebulas APIs at RPC.

4.1.2 Tutorials

English

1. Installation (thanks Victor)
2. Sending a Transaction (thanks Victor)
3. Writing Smart Contract in JavaScript (thanks otto)
4. Introducing Smart Contract Storage (thanks Victor)
5. Interacting with Nebulas by RPC API (thanks Victor)

äÿ■æŰĞ

1. çijŰèŕŚåőL'èčĚåŔŁè£Řèą Ňneb
2. åIJÍæŸ§äžŚéŞ¿äÿŁåŔŚéĂĄäžd'æŸŞ
3. ä¡£çŤĺJavaScriptçijŰåĘŹæŹžèČ¡åŘĹçžę
4. æŹžèČ¡åŘĹçžęå■ŸåĆĺåŇžäżŃçż■
5. éĂŽè£ĞRPCæŐěåŔčäÿŐæŸ§äžŚéŞ¿äžd'äžŠ

4.1.3 Contribution

Feel free to join Nebulas Mainnet. If you did find something wrong, please submit a issue or submit a pull request to let us know, we will add your name and url to this page soon.

4.2 How to Join Nebulas Testnet

4.2.1 Introduction

We are glad to release Nebulas Testnet here. It simulate the Nebulas network and NVM, and allow developers to interact with Nebulas without paying the cost of gas.

```
https://github.com/nebulasio/go-nebulas/tree/testnet
```

Configuration

The testnet configuration files are in folder `testnet/conf` under `testnet` branch, including

genesis.conf

All configurable information about genesis block is defined in genesis.conf, including

- **meta.chain_id:** chain identity
- **consensus.dpos.dynasty:** the initial dynasty of validators
- **token_distribution:** the initial allocation of tokens

Attention: DO NOT change the genesis.conf.

config.conf

All configurable information about runtime is defined in config.conf.

Please check the `template.conf` to find more details about the runtime configuration.

Tips: the official seed node info is as below,

```
seed:["/ip4/52.60.150.236/tcp/8680/ipfs/
↪QmVJikqWQst13QsgdCLBjgcSWwpAAdZjoExGdvK3r2CNhv"]
```

API List

Test Endpoint:

| API | URL | Protocol | | — | :—: | :—: | | RESTful | https://testnet.nebulas.io/ | HTTP |

- GetNebState : returns nebulas client info.
- GetAccountState: returns the account balance and nonce.
- LatestIrreversibleBlock: returns the lastest irreversible block.
- Call: execute smart contract locally. the tx won't be submitted on chain.
- SendRawTransaction: submit signed transaction. The transaction must be signed before send.
- GetTransactionReceipt: get transaction receipt info by tansaction hash.

More Nebulas APIs at RPC.

Token Claim

Every email can claim some tokens every day at here.

4.2.2 Tutorials

English

1. Installation (thanks Victor)
2. Sending a Transaction (thanks Victor)
3. Writing Smart Contract in JavaScript (thanks otto)
4. Introducing Smart Contract Storage (thanks Victor)
5. Interacting with Nebulas by RPC API (thanks Victor)

äÿ■æŰĞ

1. çijŰèŕŚåőL'èčĚåŔŁè£ŘèąŇneb
2. åIJÍæŸ§äžŚéŞ¿äÿŁåŔŚéĂĄäžd'æŸŞ
3. ä¡£çŤÍJavaScriptçijŰåĘŹæŹžèČ¡åŘĹçžę
4. æŹžèČ¡åŘĹçžęå■ŸåĆÍåŇžäżŃçż■
5. éĂŽè£ĞRPCæŐěåŔčäÿŐæŸ§äžŚéŞ¿äžd'äžŠ

4.2.3 Contribution

Feel free to join Nebulas Testnet. If you did find something wrong, please submit a issue or submit a pull request to let us know, we will add your name and url to this page soon.

4.3 Smart Contract

4.3.1 Languages

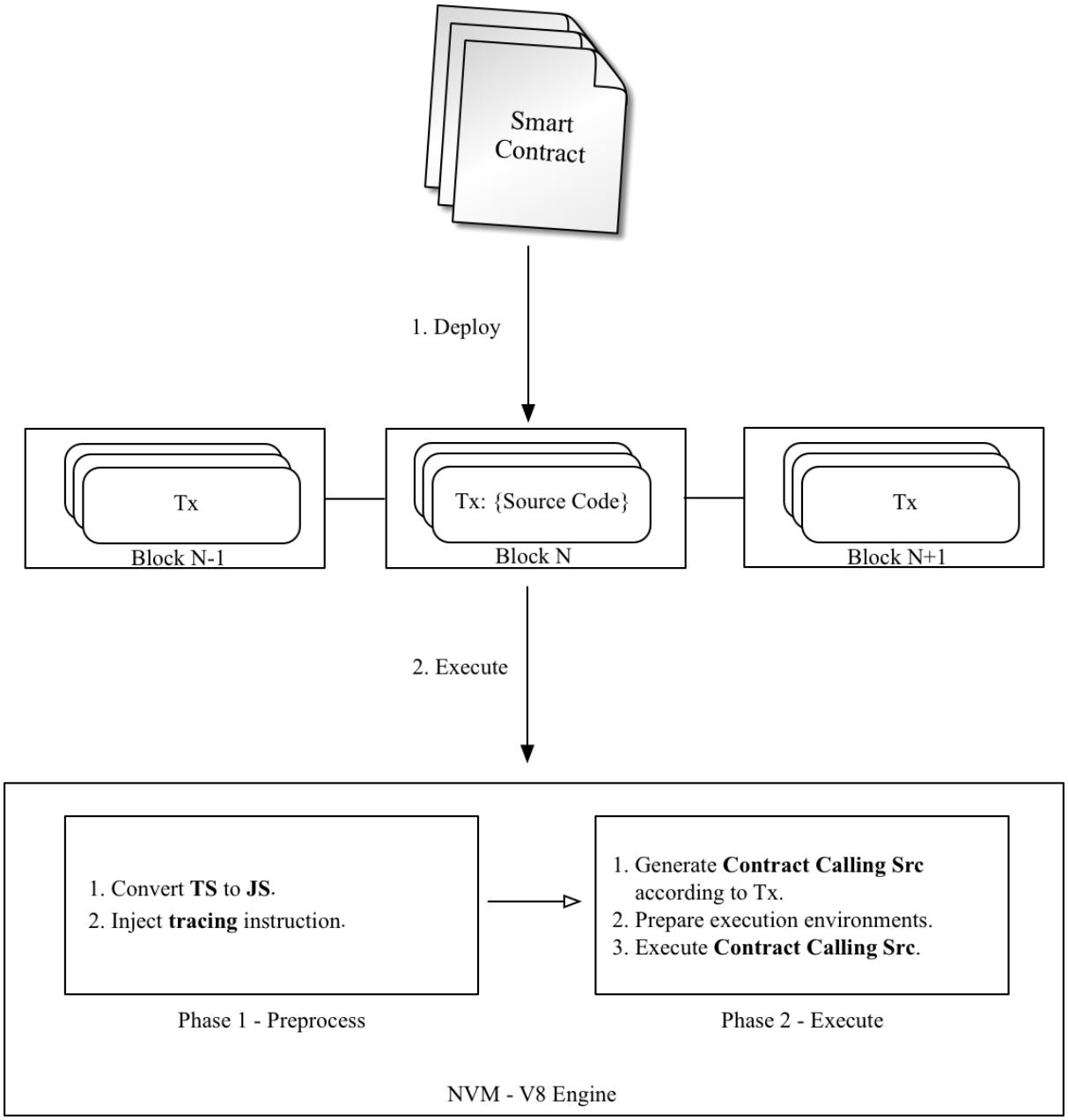
In Nebulas, there are two supported smart contract languages:

- JavaScript
- TypeScript

They are supported by the integration of Chrome V8, a widely used JavaScript engine developed by The Chromium Project for Google Chrome and Chromium web browsers.

4.3.2 Execution Model

The diagram below is the Execution Model of Smart Contract:



1. All src of Smart Contract and arguments are packaged in Transaction and deployed on Nebulas.
2. The execution of Smart Contract are divided into two phases:
   (a) Preprocess: inject tracing instruction, etc.
   (b) Execute: generate executable src and execute it.

4.3.3 Contracts

Contracts in Nebulas are similar to classes in object-oriented languages. They contain persistent data in state variables and functions that can modify these variables.

Writing Contract

A contract must be a Prototype Object or Class in JavaScript or TypeScript.

A Contract must include an `init` function, it will be executed only once when deploying. Functions, named starting with _ are `private`, can't be executed in Transaction. The others are all `public` and can be executed in Transaction.

Since Contract is executed in Chrome V8, all instance variables are in memory, it's not wise to save all of them to state trie in Nebulas. In Nebulas, we provide `LocalContractStorage` and `GlobalContractStorage` objects to help developers define fields needing to be saved to state trie. And those fields should be defined in `constructor` of Contract, before other functions.

The following is a sample contract:

```
class Rectangle {
    constructor() {
        // define fields stored to state trie.
        LocalContractStorage.defineProperties(this, {
            height: null,
            width: null,
        });
    }

    // init function.
    init(height, width) {
        this.height = height;
        this.width = width;
    }

    // calc area function.
    calcArea() {
        return this.height * this.width;
    }

    // verify function.
    verify(expected) {
        let area = this.calcArea();
        if (expected != area) {
            throw new Error("Error: expected " + expected + ",␣
↪actual is " + area + ".");
        }
    }
}
```

Visibility

In JavaScript, there is no function visibility, all functions defined in prototype object are public.

In Nebulas, we define two kinds of visibility `public` and `private`:

- `public` All functions whose name matches regexp `^[a-zA-Z$][A-Za-z0-9_$]*$` are public, except `init`. Public functions can be called via Transaction.
- `private` All functions whose name starts with _ are private. A private function can only be called by public functions.

4.3.4 Global Objects

console

The `console` module provides a simple debugging console that is similar to the JavaScript console mechanism provided by web browsers.

The global console can be used without calling `require('console')`.

console.info([...args])

- `...args <any>`

  The console.info() function is an alias for `console.log()`.

console.log([...args])

- `...args <any>`

  Print `args` to Nebulas Logger at level `info`.

console.debug([...args])

- `...args <any>`

  Print `args` to Nebulas Logger at level `debug`.

console.warn([...args])

- `...args <any>`

  Print `args` to Nebulas Logger at level `warn`.

console.error([...args])

- `...args <any>`

  Print `args` to Nebulas Logger at level `error`.

LocalContractStorage

The `LocalContractStorage` module provides a state trie based storage capability. It accepts string only key value pairs. And all data are stored to a private state trie associated with current contract address, only the contract can access them.

```
interface Descriptor {
    // serialize value to string;
    stringify?(value: any): string;

    // deserialize value from string;
    parse?(value: string): any;
}

interface DescriptorMap {
    [fieldName: string]: Descriptor;
}

interface ContractStorage {
    // get and return value by key from Native Storage.
    rawGet(key: string): string;
    // set key and value pair to Native Storage,
    // return 0 for success, otherwise failure.
    rawSet(key: string, value: string): number;

    // define a object property named `fieldname` to `obj` with␣
↪descriptor.
    // default descriptor is JSON.parse/JSON.stringify descriptor.
    // return this.
    defineProperty(obj: any, fieldName: string, descriptor?:␣
↪Descriptor): any;

    // define object properties to `obj` from `props`.
    // default descriptor is JSON.parse/JSON.stringify descriptor.
    // return this.
    defineProperties(obj: any, props: DescriptorMap): any;

    // define a StorageMap property named `fieldname` to `obj` with␣
↪descriptor.
    // default descriptor is JSON.parse/JSON.stringify descriptor.
    // return this.
    defineMapProperty(obj: any, fieldName: string, descriptor?:␣
↪Descriptor): any;
```

```
    // define StorageMap properties to `obj` from `props`.
    // default descriptor is JSON.parse/JSON.stringify descriptor.
    // return this.
    defineMapProperties(obj: any, props: DescriptorMap): any;

    // delete key from Native Storage.
    // return 0 for success, otherwise failure.
    del(key: string): number;

    // get value by key from Native Storage,
    // deserialize value by calling `descriptor.parse` and return.
    get(key: string): any;

    // set key and value pair to Native Storage,
    // the value will be serialized to string by calling␣
↪`descriptor.stringify`.
    // return 0 for success, otherwise failure.
    set(key: string, value: any): number;
}

interface StorageMap {
    // delete key from Native Storage, return 0 for success,␣
↪otherwise failure.
    del(key: string): number;

    // get value by key from Native Storage,
    // deserialize value by calling `descriptor.parse` and return.
    get(key: string): any;

    // set key and value pair to Native Storage,
    // the value will be serialized to string by calling␣
↪`descriptor.stringify`.
    // return 0 for success, otherwise failure.
    set(key: string, value: any): number;
}
```

BigNumber

The `BigNumber` module use the bignumber.js, a JavaScript library for arbitrary-precision decimal and non-decimal arithmetic. The contract can use `BigNumber` directly to handle the value of the transaction and other values transfer.

```
var value = new BigNumber(0);
value.plus(1);
...
```

Blockchain

The `Blockchain` module provides a object for contracts to obtain transactions and blocks executed by the current contract. Also, the NAS can be transferred from the contract and the address check is provided.

Blockchain API:

```
// current block
Blockchain.block;

// current transaction, transaction's value/gasPrice/gasLimit auto␣
↪change to BigNumber object
Blockchain.transaction;

// transfer NAS from contract to address
Blockchain.transfer(address, value);

// verify address
Blockchain.verifyAddress(address);
```

properties:

- `block`: current block for contract execution
  - `timestamp`: block timestamp
  - `seed`: random seed
  - `height`: block height
- `transaction`: current transaction for contract execution
  - `hash`: transaction hash
  - `from`: transaction from address
  - `to`: transaction to address
  - `value`: transaction value, a BigNumber object for contract use
  - `nonce`: transaction nonce
  - `timestamp`: transaction timestamp
  - `gasPrice`: transaction gasPrice, a BigNumber object for contract use
  - `gasLimit`: transaction gasLimit, a BigNumber object for contract use
- `transfer(address, value)`: transfer NAS from contract to address
  - params:
    - `address`: nebulas address to receive NAS
    - `value`: transfer value, a BigNumber object
  - return:

        * `0`: transfer success
        * `1`: transfer failed
- `verifyAddress(address)`: verify address
    - params:
        * `address`: address need to check
    - return:
        * `1`: address is valid
        * `0`: address is invalid

Example to use:

```
'use strict';

var SampleContract = function () {
    LocalContractStorage.defineProperties(this, {
        name: null,
        count: null
    });
    LocalContractStorage.defineMapProperty(this, "allocation");
};

SampleContract.prototype = {
    init: function (name, count, allocation) {
        this.name = name;
        this.count = count;
        allocation.forEach(function (item) {
            this.allocation.put(item.name, item.count);
        }, this);
        console.log('init: Blockchain.block.coinbase = ' +␣
↪Blockchain.block.coinbase);
        console.log('init: Blockchain.block.hash = ' + Blockchain.
↪block.hash);
        console.log('init: Blockchain.block.height = ' + Blockchain.
↪block.height);
        console.log('init: Blockchain.transaction.from = ' +␣
↪Blockchain.transaction.from);
        console.log('init: Blockchain.transaction.to = ' +␣
↪Blockchain.transaction.to);
        console.log('init: Blockchain.transaction.value = ' +␣
↪Blockchain.transaction.value);
        console.log('init: Blockchain.transaction.nonce = ' +␣
↪Blockchain.transaction.nonce);
        console.log('init: Blockchain.transaction.hash = ' +␣
↪Blockchain.transaction.hash);
    },
    transfer: function (address, value) {
        var result = Blockchain.transfer(address, value);
```

```
        console.log("transfer result:", result);
        Event.Trigger("transfer", {
            Transfer: {
                from: Blockchain.transaction.to,
                to: address,
                value: value
            }
        });
    },
    verifyAddress: function (address) {
         var result = Blockchain.verifyAddress(address);
        console.log("verifyAddress result:", result);
    }
};

module.exports = SampleContract;
```

Event

The `Event` module records execution events in contract. The recorded events are stored in the event trie on the chain, which can be fetched by `FetchEvents` method in block with the execution transaction hash. All contract event topics have a `chain.contract.` prefix before the topic they set in contract.

```
Event.Trigger(topic, obj);
```

- `topic`: user-defined topic
- `obj`: JSON object

You can see the example in `SampleContract` before.

Math.random

- `Math.random()` returns a floating-point, pseudo-random number in the range from 0 inclusive up to but not including 1. The typical usage is:

```
"use strict";

var BankVaultContract = function () {};

BankVaultContract.prototype = {

    init: function () {},

    game: function(subscript){

        var arr =[1,2,3,4,5,6,7,8,9,10,11,12,13];
```

```
        for(var i = 0;i < arr.length; i++){
            var rand = parseInt(Math.random()*arr.length);
            var t = arr[rand];
            arr[rand] =arr[i];
            arr[i] = t;
        }

        return arr[parseInt(subscript)];
    },
};
module.exports = BankVaultContract;
```

- `Math.random.seed(myseed)` if needed, you can use this method to reset random seed. The argument `myseed` must be a **string**.

  ‘‘‘js

  “use strict”;

  var BankVaultContract = function () {};

  BankVaultContract.prototype = {

```
init: function () {},

game:function(subscript, myseed){

    var arr =[1,2,3,4,5,6,7,8,9,10,11,12,13];

    console.log(Math.random());

    for(var i = 0;i < arr.length; i++){

        if (i == 8) {
            // reset random seed with `myseed`
            Math.random.seed(myseed);
        }

        var rand = parseInt(Math.random()*arr.length);
        var t = arr[rand];
        arr[rand] =arr[i];
        arr[i] = t;
    }
    return arr[parseInt(subscript)];
},
```

  };

  module.exports = BankVaultContract;

```
### Date
```js
"use strict";
```
```

```
var BankVaultContract = function () {};

BankVaultContract.prototype = {
    init: function () {},

    test: function(){
        var d = new Date();
        return d.toString();
    }
};

module.exports = BankVaultContract;
```

Tips:

- Unsupported methodsïijŽ`toDateString()`, `toTimeString()`, `getTimezoneOffset()`,`toLocaleXXX()`.
- `new Date()`/`Date.now()` returns the timestamp of current block in milliseconds.
- `getXXX` returns the result of `getUTCXXX`.

accept

this method is aimed to make it possible to send a binary transfer to a contract account. As the `to` is a smart contact address, which has declared a function `accept()` and it excutes correctly, the transfer will succeed. If the Tx is a non-binary Tx,it will be treated as a normal function.

```
"use strict";
var DepositeContent = function (text) {
    if(text){
            var o = JSON.parse(text);
            this.balance = new BigNumber(o.balance);//ä¡ŹéćÌä£ąæĄŕ
            this.address = o.address;
    }else{
            this.balance = new BigNumber(0);
            this.address = "";
        }
};

DepositeContent.prototype = {
    toString: function () {
          return JSON.stringify(this);
    }
};

var BankVaultContract = function () {
    LocalContractStorage.defineMapProperty(this, "bankVault", {
```

```
        parse: function (text) {
            return new DepositeContent(text);
        },
        stringify: function (o) {
            return o.toString();
        }
    });
};

BankVaultContract.prototype = {
    init: function () {},

    save: function () {
        var from = Blockchain.transaction.from;
        var value = Blockchain.transaction.value;
        value = new BigNumber(value);
        var orig_deposit = this.bankVault.get(from);
        if (orig_deposit) {
            value = value.plus(orig_deposit.balance);
        }

        var deposit = new DepositeContent();
        deposit.balance = new BigNumber(value);
        deposit.address = from;
        this.bankVault.put(from, deposit);
    },

    accept:function(){
        this.save();
        Event.Trigger("transfer", {
            Transfer: {
                from: Blockchain.transaction.from,
                to: Blockchain.transaction.to,
                value: Blockchain.transaction.value,
            }
        });
    }

};
module.exports = BankVaultContract;
```

4.4 NRC20

4.4.1 Abstract

The following standard allows for the implementation of a standard API for tokens within smart contracts. This standard provides basic functionality to transfer tokens, as well as allows

tokens to be approved so they can be spent by another on-chain third party.

4.4.2 Motivation

A standard interface allows that a new token can be created by any application easily : from wallets to decentralized exchanges.

4.4.3 Methods

name

Returns the name of the token - e.g. `"MyToken"`.

```
// returns string, the name of the token.
function name()
```

symbol

Returns the symbol of the token. E.g. “TK”.

```
// returns string, the symbol of the token
function symbol()
```

decimals

Returns the number of decimals the token uses - e.g. `8`, means to divide the token amount by `100000000` to get its user representation.

```
// returns number, the number of decimals the token uses
function decimals()
```

totalSupply

Returns the total token supply.

```
// returns string, the total token supply, the decimal value is␣
↪decimals* total.
function totalSupply()
```

balanceOf

Returns the account balance of a address.

```
// returns string, the account balance of another account with␣
↪address
function balanceOf(address)
```

transfer

Transfers `value` amount of tokens to `address`, and MUST fire the `Transfer` event. The function SHOULD `throw` if the `from` account balance does not have enough tokens to spend.

Note Transfers of 0 values MUST be treated as normal transfers and fire the `Transfer` event.

```
// returns `true`, if transfer success, else throw error
function transfer(address, value)
```

transferFrom

Transfers `value` amount of tokens from address `from` to address `to`, and MUST fire the `Transfer` event.

The `transferFrom` method is used for a withdraw workflow, allowing contracts to transfer tokens on your behalf. This can be used for example to allow a contract to transfer tokens on your behalf and/or to charge fees in sub-currencies. The function SHOULD `throw` unless the `from` account has deliberately authorized the sender of the message via some mechanism.

Note Transfers of 0 values MUST be treated as normal transfers and fire the `Transfer` event.

```
// returns `true`, if transfer success, else throw error
function transferFrom(from, to, value)
```

approve

Allows `spender` to withdraw from your account multiple times, up the `currentValue` to the `value` amount. If this function is called again it overwrites the current allowance with `value`.

NOTE: To prevent attack vectors, the user needs to give a previous approve value, and the default value that is not approve is 0.

```
// returns `true`, if approve success, else throw error
function approve(spender, currentValue, value)
```

allowance

Returns the amount which `spender` is still allowed to withdraw from `owner`.

```
// returns string, the value allowed to withdraw from `owner`.
function allowance(owner, spender)
```

Events

transferEvent

MUST trigger when tokens are transferred, including zero value transfers.

A token contract which creates new tokens SHOULD trigger a Transfer event with the `from` address set to `totalSupply` when tokens are created.

```
function transferEvent: function(status, from, to, value)
```

approveEvent

MUST trigger on any call to `approve(spender, currentValue, value)`.

```
function approveEvent: function(status, from, spender, value)
```

4.4.4 Implementation

Example implementations are available at

- NRC20.js

```
'use strict';

var Allowed = function (obj) {
    this.allowed = {};
    this.parse(obj);
}

Allowed.prototype = {
    toString: function () {
        return JSON.stringify(this.allowed);
    },

    parse: function (obj) {
        if (typeof obj != "undefined") {
            var data = JSON.parse(obj);
            for (var key in data) {
```

```
                this.allowed[key] = new BigNumber(data[key]);
            }
        }
    },

    get: function (key) {
        return this.allowed[key];
    },

    set: function (key, value) {
        this.allowed[key] = new BigNumber(value);
    }
}

var StandardToken = function () {
    LocalContractStorage.defineProperties(this, {
        _name: null,
        _symbol: null,
        _decimals: null,
        _totalSupply: {
            parse: function (value) {
                return new BigNumber(value);
            },
            stringify: function (o) {
                return o.toString(10);
            }
        }
    });

    LocalContractStorage.defineMapProperties(this, {
        "balances": {
            parse: function (value) {
                return new BigNumber(value);
            },
            stringify: function (o) {
                return o.toString(10);
            }
        },
        "allowed": {
            parse: function (value) {
                return new Allowed(value);
            },
            stringify: function (o) {
                return o.toString();
            }
        }
    });
};

StandardToken.prototype = {
```

```
    init: function (name, symbol, decimals, totalSupply) {
        this._name = name;
        this._symbol = symbol;
        this._decimals = decimals || 0;
        this._totalSupply = new BigNumber(totalSupply).mul(new␣
↪BigNumber(10).pow(decimals));

        var from = Blockchain.transaction.from;
        this.balances.set(from, this._totalSupply);
        this.transferEvent(true, from, from, this._totalSupply);
    },

    // Returns the name of the token
    name: function () {
        return this._name;
    },

    // Returns the symbol of the token
    symbol: function () {
        return this._symbol;
    },

    // Returns the number of decimals the token uses
    decimals: function () {
        return this._decimals;
    },

    totalSupply: function () {
        return this._totalSupply.toString(10);
    },

    balanceOf: function (owner) {
        var balance = this.balances.get(owner);

        if (balance instanceof BigNumber) {
            return balance.toString(10);
        } else {
            return "0";
        }
    },

    transfer: function (to, value) {
        value = new BigNumber(value);
        if (value.lt(0)) {
            throw new Error("invalid value.");
        }

        var from = Blockchain.transaction.from;
        var balance = this.balances.get(from) || new BigNumber(0);
```

```
        if (balance.lt(value)) {
            throw new Error("transfer failed.");
        }

        this.balances.set(from, balance.sub(value));
        var toBalance = this.balances.get(to) || new BigNumber(0);
        this.balances.set(to, toBalance.add(value));

        this.transferEvent(true, from, to, value);
    },

    transferFrom: function (from, to, value) {
        var spender = Blockchain.transaction.from;
        var balance = this.balances.get(from) || new BigNumber(0);

        var allowed = this.allowed.get(from) || new Allowed();
        var allowedValue = allowed.get(spender) || new BigNumber(0);
        value = new BigNumber(value);

        if (value.gte(0) && balance.gte(value) && allowedValue.
↪gte(value)) {

            this.balances.set(from, balance.sub(value));

            // update allowed value
            allowed.set(spender, allowedValue.sub(value));
            this.allowed.set(from, allowed);

            var toBalance = this.balances.get(to) || new␣
↪BigNumber(0);
            this.balances.set(to, toBalance.add(value));

            this.transferEvent(true, from, to, value);
        } else {
            throw new Error("transfer failed.");
        }
    },

    transferEvent: function (status, from, to, value) {
        Event.Trigger(this.name(), {
            Status: status,
            Transfer: {
                from: from,
                to: to,
                value: value
            }
        });
    },

    approve: function (spender, currentValue, value) {
```

```
        var from = Blockchain.transaction.from;

        var oldValue = this.allowance(from, spender);
        if (oldValue != currentValue.toString()) {
            throw new Error("current approve value mistake.");
        }

        var balance = new BigNumber(this.balanceOf(from));
        var value = new BigNumber(value);

        if (value.lt(0) || balance.lt(value)) {
            throw new Error("invalid value.");
        }

        var owned = this.allowed.get(from) || new Allowed();
        owned.set(spender, value);

        this.allowed.set(from, owned);

        this.approveEvent(true, from, spender, value);
    },

    approveEvent: function (status, from, spender, value) {
        Event.Trigger(this.name(), {
            Status: status,
            Approve: {
                owner: from,
                spender: spender,
                value: value
            }
        });
    },

    allowance: function (owner, spender) {
        var owned = this.allowed.get(owner);

        if (owned instanceof Allowed) {
            var spender = owned.get(spender);
            if (typeof spender != "undefined") {
                return spender.toString(10);
            }
        }
        return "0";
    }
};

module.exports = StandardToken;
```

4.5 RPC Overview

Remote Procedure Calls (RPCs) provide a useful abstraction for building distributed applications and services.

Nebulas provides both gRPC and RESTful API for users to interact with Nebulas.

grpc provides a concrete implementation of the gRPC protocol, layered over HTTP/2. These libraries enable communication between clients and servers using any combination of the supported languages.

grpc-gateway is a plugin of protoc. It reads gRPC service definition, and generates a reverse-proxy server which translates a RESTful JSON API into gRPC. we use it to map gRPC to HTTP.

4.5.1 Endpoint

Default endpoints:

API	URL	Protocol
gRPC	http://localhost:8684	Protobuf
RESTful	http://localhost:8685	HTTP

gRPC API

We can run the gRPC example testing client code:

```
go run main.go
```

The testing client gets account state from sender address, makes a transaction from sender to receiver, and also checks the account state of receiver address.

We can see client log output like:

```
GetAccountState n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5 nonce 4 value␣
↪314283103999999999992
SendTransaction n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5 ->␣
↪n1Zn6iyyQRhqthmCfqGBzWfip1Wx8wEvtrJ value 2 txhash:
↪"2c2f5404a2e2edb651dff44a2d114a198c00614b20801e58d5b00899c8f512ae"
GetAccountState n1Zn6iyyQRhqthmCfqGBzWfip1Wx8wEvtrJ nonce 0 value 10
```

HTTP

Now we also provided HTTP to access the RPC API. The file that ends with **gw.go** is the mapping file. Now we can access the rpc API directly from our browser, you can update the **rpc_listen** and **http_listen** in **conf/default/config.conf** to change RPC/HTTP port.

Example:

```
curl -i -H 'Content-Type: application/json' -X GET http://
↪localhost:8685/v1/user/nebstate
```

if success, response will be returned like this

```
{
    "result":{
        "chain_id":100,
        "tail":
↪"b10c1203d5ae6d4d069d5f520eb060f2f5fb74e942f391e7cadbc2b5148dfbcb
↪",
        "lib":
↪"da30b4ed14affb62b3719fb5e6952d3733e84e53fe6e955f8e46da503300c985
↪",
        "height":"365",
        "protocol_version":"/neb/1.0.0",
        "synchronized":false,
        "version":"0.7.0"
    }
}
```

Or, there is error form grpc, repose will carry the error message

```
{
    "error":"message..."
}
```

4.5.2 RPC methods

- GetNebState
- GetAccountState
- LatestIrreversibleBlock
- Call
- SendRawTransaction
- GetBlockByHash
- GetBlockByHeight
- GetTransactionReceipt
- GetTransactionByContract
- GetGasPrice
- EstimateGas
- GetEventsByHash
- Subscribe

- GetDynasty

4.5.3 RPC API Reference

GetNebState

Return the state of the neb.

Protocol	Method	API
gRpc		GetNebState
HTTP	GET	/v1/user/nebstate

Parameters

none

Returns

`chain_id` Block chain id

`tail` Current neb tail hash

`lib` Current neb lib hash

`height` Current neb tail block height

`protocol_version` The current neb protocol version.

`synchronized` The peer sync status.

`version` neb version.

HTTP Example

```
// Request
curl -i -H 'Content-Type: application/json' -X GET http://
↪localhost:8685/v1/user/nebstate

// Result
{
    "result":{
        "chain_id":100,
        "tail":
↪"b10c1203d5ae6d4d069d5f520eb060f2f5fb74e942f391e7cadbc2b5148dfbcb
↪",
        "lib":
↪"da30b4ed14affb62b3719fb5e6952d3733e84e53fe6e955f8e46da503300c985
↪",
        "height":"365",
        "protocol_version":"/neb/1.0.0",
        "synchronized":false,
        "version":"0.7.0"
    }
}
```

GetAccountState

Return the state of the account. Balance and nonce of the given address will be returned.

Protocol	Method	API
gRpc		GetAccountState
HTTP	POST	/v1/user/accountstate

Parameters

`address` Hex string of the account addresss.

`height` block account state with height. If not specified, use 0 as tail height.

Returns

`balance` Current balance in unit of 1/(10^18) nas.

`nonce` Current transaction count.

`type` The type of address, 87 stands for normal address and 88 stands for contract address

HTTP Example

```
// Request
curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/user/accountstate -d '{"address":
↪"n1Z6SbjLuAEXfhX1UJvXT6BB5osWYxVg3F3"}'

// Result
{
    result {
        "balance":"948999999898000000000"
        "nonce":51
        "type":87
    }
}
```

LatestIrreversibleBlock

Return the latest irreversible block.

Protocol	Method	API
gRpc		LatestIrreversibleBlock
HTTP	GET	/v1/user/lib

Parameters

none

Returns

`hash` Hex string of block hash.

`parent_hash` Hex string of block parent hash.

`height` block height.

`nonce` block nonce.

`coinbase` Hex string of coinbase address.

`timestamp` block timestamp.

`chain_id` block chain id.

`state_root` Hex string of state root.

`txs_root` Hex string of txs root.

`events_root` Hex string of event root.

`consensus_root`

- `Timestamp` time of consensus state
- `Proposer` proposer of current consensus state
- `DynastyRoot` Hex string of dynasty root

`miner` the miner of this block

`is_finality` block is finality

`transactions` block transactions slice.

- `transaction` GetTransactionReceipt response info.

HTTP Example

```
// Request
curl -i -H 'Content-Type: application/json' -X GET http://
↪localhost:8685/v1/user/lib

// Result
{
    "result":{
        "hash":
↪"c4a51d6241db372c1b8720e62c04426bd587e1f31054b7d04a3509f48ee58e9f
↪",
        "parent_hash":
↪"8f9f29028356d2fb2cf1291dcee85785e1c20a2145318f36c136978edb6097ce
↪",
        "height":"407",
        "nonce":"0",
        "coinbase":"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5",
        "timestamp":"1521963660",
        "chain_id":100,
        "state_root":
↪"a77bbcd911e7ee9488b623ce4ccb8a38d9a83fc29eb5ad43009f3517f1d3e19a
↪",
```

```
        "txs_root":
↪"664671e2fda200bd93b00aaec4ab12db718212acd51b4624e8d4937003a2ab22
↪",
        "events_root":
↪"2607e32c166a3513f9effbd1dc7caa7869df5989398d0124987fa0e4d183bcaf
↪",
        "consensus_root":{
            "timestamp":"1521963660",
            "proposer":"GVeOQnYf20Ppxa2cqTrPHdpr6QH4SKs4ZKs=",
            "dynasty_root":
↪"IfTgx0o271Gg4N3cVKHe7dw3NREnlYCN8aIl8VvRXDY="
        },
        "miner": "n1WwqBXVMuYC3mFCEEuFFtAXad6yxqj4as4"
        "is_finality":false,
        "transactions":[]
    }
}
```

Call

Call a smart contract function. The smart contract must have been submited. Method calls are run only on the current node, not broadcast.

Protocol	Method	API
gRpc		Call
HTTP	POST	/v1/user/call

Parameters

The parameters of the `call` method is the same as the SendTransaction parameters. Special attention:

`to` Hex string of the receiver account addresss. **The value of**`to`** is a contract address.**

`contract` transaction contract object for call smart contract.

- Sub properties(`source`** and **‘‘sourceType‘‘** are not need**):
  - `function` the contract call function for call contarct function.
  - `args` the params of contract. The args content is JSON string of parameters array.

Returns

`result` result of smart contract method call

`execute_err` execute error

`estimate_gas` estimate gas used

HTTP Example

```
// Request
curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/user/call -d '{"from":
↪"n1Z6SbjLuAEXfhX1UJvXT6BB5osWYxVg3F3","to":
↪"n1mLzWCzyR1foELEugfCZoNAW3dt8QpHtJw","value":"0","nonce":3,
↪"gasPrice":"1000000","gasLimit":"2000000","contract":{"function":
↪"transferValue","args":"[500]"}}'
```

```
// Result
{
   "result": "0",
   "execute_err": "insufficient balance",
   estimate_gas: "22208"
}
```

SendRawTransaction

Submit the signed transaction. The transaction signed value should be return by SignTransactionWithPassphrase.

Protocol	Method	API
gRpc		SendRawTransaction
HTTP	POST	/v1/user/rawtransaction

Parameters

`data` Signed data of transaction

Returns

`txhash` Hex string of transaction hash.

`contract_address` returns only for deploy contract transaction.

HTTP Example

```
// Request
curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/user/rawtransaction -d '{"data":"CiCrHtxyyIJks2/
↪RErvBBA862D6iwAaGQ9OK1NisSGAuTBIYGiY1R9Fnx0z0uPkWbPokTeBIHFFKRaosGhgzPLPtjEF5c
↪i9wAiEAAAAAAAAAAADeC2s6dkAAAoAjDd/
↪5jSBToICgZiaW5hcnlAZEoQAAAAAAAAAAAAAAAAA9CQFIQAAAAAAAAAAAAAAAAABOIFgBYkGLnnv
↪"}'

// Result
{
    "result":{
        "txhash":
↪"f37acdf93004f7a3d72f1b7f6e56e70a066182d85c186777a2ad3746b01c3b52"
    }
}
```

Deploy Contract Example

```
// Request
curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/user/rawtransaction -d '{"data":"CiDam3G9Sy5fV6/
↪ZcjasYPwSF39ZJDIHNB0Us94vn6p6ohIaGVfLzJ83pom1DO1gD307f1JdTVdDLzbMXO4aGhlXy8yfN
↪CEbThvI0iKcjHhgBZUB"}'
```

```
// Result
{
    "result":{
        "txhash":
↪"f37acdf93004f7a3d72f1b7f6e56e70a066182d85c186777a2ad3746b01c3b52
↪",
        "contract_address":
↪"4702b597eebb7a368ac4adbb388e5084b508af582dadde47"
    }
}
```

GetBlockByHash

Get block header info by the block hash.

Protocol	Method	API
gRpc		GetBlockByHash
HTTP	POST	/v1/user/getBlockByHash

Parameters

`hash` Hex string of transaction hash.

`full_fill_transaction` If true it returns the full transaction objects, if false only the hashes of the transactions.

Returns

See LatestIrreversibleBlock response.

HTTP Example

```
// Request
curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/user/getBlockByHash -d '{"hash":
↪"00000658397a90df6459b8e7e63ad3f4ce8f0a40b8803ff2f29c611b2e0190b8
↪", "full_fill_transaction":"true"}'

// Result
{
    "result":{
        "hash":
↪"c4a51d6241db372c1b8720e62c04426bd587e1f31054b7d04a3509f48ee58e9f
↪",
        "parent_hash":
↪"8f9f29028356d2fb2cf1291dcee85785e1c20a2145318f36c136978edb6097ce
↪",
        "height":"407",
        "nonce":"0",
        "coinbase":"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5",
```

```
        "timestamp":"1521963660",
        "chain_id":100,
        "state_root":
↪"a77bbcd911e7ee9488b623ce4ccb8a38d9a83fc29eb5ad43009f3517f1d3e19a
↪",
        "txs_root":
↪"664671e2fda200bd93b00aaec4ab12db718212acd51b4624e8d4937003a2ab22
↪",
        "events_root":
↪"2607e32c166a3513f9effbd1dc7caa7869df5989398d0124987fa0e4d183bcaf
↪",
        "consensus_root":{
            "timestamp":"1521963660",
            "proposer":"GVeOQnYf20Ppxa2cqTrPHdpr6QH4SKs4ZKs=",
            "dynasty_root":
↪"IfTgx0o271Gg4N3cVKHe7dw3NREnlYCN8aIl8VvRXDY="
        },
        "miner": "n1WwqBXVMuYC3mFCEEuFFtAXad6yxqj4as4"
        "is_finality":false,
        "transactions":[{
            "hash":
↪"1e96493de6b5ebe686e461822ec22e73fcbfb41a6358aa58c375b935802e4145
↪",
            "chainId":100,
            "from":"n1Z6SbjLuAEXfhX1UJvXT6BB5osWYxVg3F3",
            "to":"n1orSeSMj7nn8KHHN4JcQEw3r52TVExu63r",
            "value":"10000000000000000000","nonce":"34",
            "timestamp":"1522220087",
            "type":"binary",
            "data":null,
            "gas_price":"1000000",
            "gas_limit":"2000000",
            "contract_address":"",
            "status":1,
            "gas_used":"20000"
        }]
    }
}
```


GetBlockByHeight

Get block header info by the block height.

Protocol	Method	API
gRpc		GetBlockByHeight
HTTP	POST	/v1/user/getBlockByHeight

Parameters

`height` Height of transaction hash.

`full_fill_transaction` If true it returns the full transaction objects, if false only the hashes of the transactions.

Returns

See LatestIrreversibleBlock response.

HTTP Example

```
// Request
curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/user/getBlockByHeight -d '{"height": 256, "full_
↪fill_transaction": true}'

// Result
{
    "result":{
        "hash":
↪"c4a51d6241db372c1b8720e62c04426bd587e1f31054b7d04a3509f48ee58e9f
↪",
        "parent_hash":
↪"8f9f29028356d2fb2cf1291dcee85785e1c20a2145318f36c136978edb6097ce
↪",
        "height":"407",
        "nonce":"0",
        "coinbase":"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5",
        "timestamp":"1521963660",
        "chain_id":100,
        "state_root":
↪"a77bbcd911e7ee9488b623ce4ccb8a38d9a83fc29eb5ad43009f3517f1d3e19a
↪",
        "txs_root":
↪"664671e2fda200bd93b00aaec4ab12db718212acd51b4624e8d4937003a2ab22
↪",
        "events_root":
↪"2607e32c166a3513f9effbd1dc7caa7869df5989398d0124987fa0e4d183bcaf
↪",
        "consensus_root":{
            "timestamp":"1521963660",
            "proposer":"GVeOQnYf20Ppxa2cqTrPHdpr6QH4SKs4ZKs=",
            "dynasty_root":
↪"IfTgx0o271Gg4N3cVKHe7dw3NREnlYCN8aIl8VvRXDY="
        },
        "miner": "n1WwqBXVMuYC3mFCEEuFFtAXad6yxqj4as4"
        "is_finality":false,
        "transactions":[{
            "hash":
↪"1e96493de6b5ebe686e461822ec22e73fcbfb41a6358aa58c375b935802e4145
↪",
            "chainId":100,
            "from":"n1Z6SbjLuAEXfhX1UJvXT6BB5osWYxVg3F3",
            "to":"n1orSeSMj7nn8KHHN4JcQEw3r52TVExu63r",
```

```
            "value":"10000000000000000000","nonce":"34",
            "timestamp":"1522220087",
            "type":"binary",
            "data":null,
            "gas_price":"1000000",
            "gas_limit":"2000000",
            "contract_address":"",
            "status":1,
            "gas_used":"20000"
        }]
    }
}
```

GetTransactionReceipt

Get transactionReceipt info by tansaction hash. If the transaction not submit or only submit and not packaged on chain, it will reurn not found error.

Protocol	Method	API
gRpc		GetTransactionReceipt
HTTP	POST	/v1/user/getTransactionReceipt

Parameters

`hash` Hex string of transaction hash.

Returns

`hash` Hex string of tx hash.

`chainId` Transaction chain id.

`from` Hex string of the sender account addresss.

`to` Hex string of the receiver account addresss.

`value` Value of transaction.

`nonce` Transaction nonce.

`timestamp` Transaction timestamp.

`type` Transaction type.

`data` Transaction data, return the payload data.

`gas_price` Transaction gas price.

`gas_limit` Transaction gas limit.

`contract_address` Transaction contract address.

`status` Transaction status, 0 failed, 1 success, 2 pending.

`gas_used` transaction gas used

HTTP Example

```
// Request
curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/user/getTransactionReceipt -d '{"hash":
↪"cda54445ffccf4ea17f043e86e54be11b002053f9edbe30ae1fbc0437c2b6a73
↪"}'

// Result
{
    "result":{
        "hash":
↪"cda54445ffccf4ea17f043e86e54be11b002053f9edbe30ae1fbc0437c2b6a73
↪",
        "chainId":100,
        "from":"n1Z6SbjLuAEXfhX1UJvXT6BB5osWYxVg3F3",
        "to":"n1PxKRaJ5jZHXwTfgM9WqkZJJVXBxRcggEE",
        "value":"10000000000000000000",
        "nonce":"53",
        "timestamp":"1521964742",
        "type":"binary",
        "data":null,
        "gas_price":"1000000",
        "gas_limit":"20000",
        "contract_address":"",
        "status":1,
        "gas_used":"20000"
    }
}
```

GetTransactionByContract

Get transactionReceipt info by contract address. If contract not exists or packaged on chain, a not found error will be returned.

Protocol	Method	API
gRpc		GetTransactionByContract
HTTP	POST	/v1/user/getTransactionByContract

Parameters

`address` Hex string of contract account address.

Returns

The result is the same as that of GetTransactionReceipt

HTTP Example

```
// Request
curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/user/getTransactionByContract -d '{"address":
↪"n1sqDHGjYtX6rMqFoq5Tow3s3LqF4ZxBvE3"}'

// Result
{
    "result":{
        "hash":
↪"c5a45a789278f5cce9e95e8f31c1962567f58844456fed7a6eb9afcb764ca6a3
↪",
        "chainId":100,
        "from":"n1Z6SbjLuAEXfhX1UJvXT6BB5osWYxVg3F3",
        "to":"n1Z6SbjLuAEXfhX1UJvXT6BB5osWYxVg3F3",
        "value":"0",
        "nonce":"1",
        "timestamp":"1521964742",
        "type":"deploy",
        "data":
↪"eyJTb3VyY2VUeXBlIjoianMiLCJTb3VyY2UiOiJcInVzZSBzdHJpY3RcIjtcblxudmFyIENvbnRyY
↪.....
↪UmFuZG9tMlwiOiByMTIsXG4gImRlZmF1bHRTZWVkUmFuZG9tM1wiOiByMTMsXG4gICAgICAgICAgIC
↪",
        "gas_price":"1000000",
        "gas_limit":"20000",
        "contract_address":"n1sqDHGjYtX6rMqFoq5Tow3s3LqF4ZxBvE3",
        "status":1,
        "gas_used":"20000",
        "execute_error":"",
        "execute_result":"\"\""
    }
}
```

Subscribe

Return the subscribed events of transaction & block. The request is a keep-alive connection.

Protocol	Method	API
gRpc		Subscribe
HTTP	POST	/v1/user/subscribe

Parameters

`topics` repeated event topic name, string array.

The topic name list:

- `chain.pendingTransaction` The topic of pending a transaction in transaction_pool.
- `chain.latestIrreversibleBlock` The topic of updating latest irreversible block.
- `chain.transactionResult` The topic of executing & submitting tx.
- `chain.newTailBlock` The topic of setting new tail block.
- `chain.revertBlock` The topic of reverting block.

Returns

`topic` subscribed event topic name.

`data` subscribed event data.

HTTP Example

```
// Request
curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/user/subscribe -d '{"topics":["chain.linkBlock",
↪ "chain.pendingTransaction"]}'

// Result
{
    "result":{
        "topic":"chain.pendingTransaction",
        "data":"{
                \"chainID\":100,
                 \"hash\":\
↪"b466c7a9b667db8d15f74863a4bc60bc989566b6c3766948b2cacb45a4fbda42\
↪",
                 \"from\":\"n1Z6SbjLuAEXfhX1UJvXT6BB5osWYxVg3F3\",
                 \"to\":\"n1Z6SbjLuAEXfhX1UJvXT6BB5osWYxVg3F3\",
                 \"nonce\":6,
                 \"value\":\"0\",
                 \"timestamp\":1522215320,
                 \"gasprice\": \"1000000\",
                 \"gaslimit\":\"20000000\",
                 \"type\":\"deploy\"}"
    }
    "result":{
        "topic":"chain.pendingTransaction",
        "data": "..."
    }
    ...
}
```

GetGasPrice

Return current gasPrice.

Protocol	Method	API
gRpc		GetGasPrice
HTTP	GET	/v1/user/getGasPrice

Parameters

none

Returns

`gas_price` gas price. The unit is 10^-18 NAS.

HTTP Example

```
// Request
curl -i -H 'Content-Type: application/json' -X GET http://
↪localhost:8685/v1/user/getGasPrice

// Result
{
    "result":{
        "gas_price":"1000000"
    }
}
```

EstimateGas

Return the estimate gas of transaction.

Protocol	Method	API
gRpc		EstimateGas
HTTP	POST	/v1/user/estimateGas

Parameters

The parameters of the `EstimateGas` method is the same as the SendTransactionparameters.

Returns

`gas` the estimate gas.

`err` error message of the transaction executing

HTTP Example

```
// Request
curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/user/estimateGas -d '{"from":
↪"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5","to":
↪"n1SAeQRVn33bamxN4ehWUT7JGdxipwn8b17", "value":
↪"1000000000000000000","nonce":1,"gasPrice":"1000000","gasLimit":
↪"2000000"}'

// Result
{
    "gas":"20000",
    "err":""
}
```

GetEventsByHash

Return the events list of transaction.

Protocol	Method	API
gRpc		GetEventsByHash
HTTP	POST	/v1/user/getEventsByHash

Parameters

`hash` Hex string of transaction hash.

Returns

`events` the events list.

- `topic` event topic;
- `data` event data.

HTTP Example

```
// Request
curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/user/getEventsByHash -d '{"hash":
↪"ec239d532249f84f158ef8ec9262e1d3d439709ebf4dd5f7c1036b26c6fe8073
↪"}'

// Result
{
    "result":{
        "events":[{
            "topic":"chain.transactionResult",
            "data":"{
                \"hash\":\
↪"d7977f96294cd232781d9c17f0f3212b48312d5ef0f556551c5cf48622759785\
↪",
                \"status\":1,
                \"gas_used\":\"22208\",
                \"error\":\"\"
            }"
        }]
    }
}
```

GetDynasty

GetDynasty get dpos dynasty.

Protocol	Method	API
gRpc		GetDynasty
HTTP	POST	/v1/user/dynasty

Parameters

`height` block height

Returns

`miners` repeated string of miner address.

HTTP Example

```
// Request
curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/user/dynasty -d '{"height": 1}'

// Result
{
    {
        "result":{
            "miners":[
                "n1FkntVUMPAsESuCAAPK711omQk19JotBjM",
```

```
                "n1JNHZJEUvfBYfjDRD14Q73FX62nJAzXkMR",
                "n1Kjom3J4KPsHKKzZ2xtt8Lc9W5pRDjeLcW",
                "n1TV3sU6jyzR4rJ1D7jCAmtVGSntJagXZHC",
                "n1WwqBXVMuYC3mFCEEuFFtAXad6yxqj4as4",
                "n1Zn6iyyQRhqthmCfqGBzWfip1Wx8wEvtrJ"
            ]
        }
    }
}
```

Management RPC

Beside the NEB API RPC interface nebulas provides additional management APIs. Neb console supports both API and management interfaces. Management RPC uses the same gRPC and HTTP port, which also binds NEB API RPC interfaces.

Nebulas provide both gRPC and RESTful management APIs for users to interact with Nebulas. Our admin proto file defines all admin APIs. **We recommend using the console access admin interfaces, or restricting the admin RPC to local access.**

Default management RPC Endpoint:

| API | URL | Protocol | | — | :—: | :—: | | gRPC | http://localhost:8684 | Protobuf | | RESTful | http://localhost:8685 | HTTP |

Management RPC methods

- NodeInfo
- Accounts
- NewAccount
- UnLockAccount
- LockAccount
- SignTransactionWithPassphrase
- SendTransactionWithPassphrase
- SendTransaction
- SignHash
- StartPprof
- GetConfig

Management RPC API Reference

NodeInfo

Return the p2p node info.

| Protocol | Method | API | | — | — | — | | gRpc | | NodeInfo | | HTTP | GET | /v1/user/nodeinfo |

Parameters

none

Returns

`id` the node ID.

`chain_id` the block chainID.

`coninbase` coinbase

`peer_count` Number of peers currenly connected.

`synchronized` the node synchronized status.

`bucket_size` the node route table bucket size.

`protocol_version` the network protocol version.

`RouteTable*[] route_table` the network routeTable

```
message RouteTable {
    string id = 1;
    repeated string address = 2;
}
```

HTTP Example

```
# Request
curl -i -H 'Content-Type: application/json' -X GET http://
↪localhost:8685/v1/admin/nodeinfo

# Result
{
    "result":{
        "id":"QmP7HDFcYmJL12Ez4ZNVCKjKedfE7f48f1LAkUc3Whz4jP",
        "chain_id":100,
        "coinbase":"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5",
        "peer_count":4,
        "synchronized":false,
        "bucket_size":64,
        "protocol_version":"/neb/1.0.0",
        "route_table":[
            {
                "id":"QmP7HDFcYmJL12Ez4ZNVCKjKedfE7f48f1LAkUc3Whz4jP
↪",
```

```
                "address":[
                    "/ip4/127.0.0.1/tcp/8680",
                    "/ip4/192.168.1.206/tcp/8680"
                ]
            },
            {
                "id":"QmUxw4PZ8kMEnHD8WaSVE92dtvdnwgufM6m5DrWemdk2M7
↪",
                "address":[
                    "/ip4/192.168.1.206/tcp/10003","/ip4/127.0.0.1/
↪tcp/10003"
                ]
            }
        ]
    }
}
```

Accounts

Return account list.

| Protocol | Method | API | | — | — | — | | gRpc | | Accounts | | HTTP | GET | /v1/admin/accounts |

Parameters

none

Returns

`addresses` account list

HTTP Example

```
# Request
curl -i -H 'Content-Type: application/json' -X GET http://
↪localhost:8685/v1/admin/accounts

# Result
{
    "result":{
        "addresses":[
            "n1FkntVUMPAsESuCAAPK711omQk19JotBjM",
            "n1JNHZJEUvfBYfjDRD14Q73FX62nJAzXkMR",
            "n1Kjom3J4KPsHKKzZ2xtt8Lc9W5pRDjeLcW",
```

```
            "n1NHcbEus81PJxybnyg4aJgHAaSLDx9Vtf8",
            "n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5",
            "n1TV3sU6jyzR4rJ1D7jCAmtVGSntJagXZHC",
            "n1WwqBXVMuYC3mFCEEuFFtAXad6yxqj4as4",
            "n1Z6SbjLuAEXfhX1UJvXT6BB5osWYxVg3F3",
            "n1Zn6iyyQRhqthmCfqGBzWfip1Wx8wEvtrJ"
        ]
    }
}
```

NewAccount

NewAccount create a new account with passphrase.

| Protocol | Method | API | | — | — | — | | gRpc | | NewAccount | | HTTP | POST | /v1/admin/account/new |

Parameters

`passphrase` New account passphrase.

Returns

`address` New Account address.

HTTP Example

```
# Request
curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/admin/account/new -d '{"passphrase":"passphrase
↪"}'

# Result

{
    "result":{
        "address":"n1czGUvbQQton6KUWga4wKDLLKYDEn39mEk"
    }
}
```

UnLockAccount

UnlockAccount unlock account with passphrase. After the default unlock time, the account will be locked.

| Protocol | Method | API | | — | — | — | | gRpc | | UnLockAccount | | HTTP | POST | /v1/admin/account/unlock |

Parameters

`address` UnLock account address.

`passphrase` UnLock account passphrase.

`duration` Unlock accoutn duration.

Returns

`result` UnLock account result, unit is ns.

HTTP Example

```
# Request
curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/admin/account/unlock -d '{"address":
↪"n1czGUvbQQton6KUWga4wKDLLKYDEn39mEk","passphrase":"passphrase",
↪"duration":"1000000000"}'

# Result
{
    "result":{
        "result":true
    }
}
```

LockAccount

LockAccount lock account.

| Protocol | Method | API | | — | — | — | | gRpc | | LockAccount | | HTTP | POST | /v1/admin/account/lock |

Parameters

`address` Lock account address.

Returns

`result` Lock account result.

HTTP Example

```
# Request
curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/admin/account/lock -d '{"address":
↪"n1czGUvbQQton6KUWga4wKDLLKYDEn39mEk"}'

# Result
{
    "result":{
        "result":true
    }
}
```

SignTransactionWithPassphrase

SignTransactionWithPassphrase sign transaction. The transaction's from addrees must be unlocked before sign call.

| Protocol | Method | API | | — | — | — | | gRpc | | SignTransactionWithPassphrase | | HTTP | POST | /v1/admin/sign |

Parameters

`transaction` this is the same as the SendTransaction parameters.

`passphrase` from account passphrase

Returns

`data` Signed transaction data.

sign normal transaction Example

```
# Request
curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/admin/sign -d '{"transaction":{"from":
↪"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5","to":
↪"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5", "value":
↪"1000000000000000000","nonce":1,"gasPrice":"1000000","gasLimit":
↪"2000000"}, "passphrase":"passphrase"}'

# Result
{
    "result":{
        "data":
↪"CiBOW15yoZ+XqQbMNr4bQdJCXrBTehJKukwjcfW5eASgtBIaGVduKnw+6lM3HBXhJEzzuvv3yNdYA
↪BwhwhqUkp/
↪gEJtE4kndoc7NdSgqD26IQqa0Hjbtg1JaszAvHZiW+XH7C+Ky9XTKRJKuTOc446646d/
↪Sbz/nxQE="
    }
}
```

SendTransactionWithPassphrase

SendTransactionWithPassphrase send transaction with passphrase.

| Protocol | Method | API | | — | — | — | | gRpc | | SendTransactionWithPassphrase | | HTTP | POST | /v1/admin/transactionWithPassphrase |

Parameters

`transaction` transaction parameters, which is the same as the SendTransaction parameters.

`passphrase` From address passphrase.

Returns

`txhash` transaction hash.

`contract_address` returns only for deploy contract transaction.

Example

```
# Request
curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/admin/transactionWithPassphrase -d '{
↪"transaction":{"from":"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5","to":
↪"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5", "value":
↪"1000000000000000000","nonce":1,"gasPrice":"1000000","gasLimit":
↪"2000000"},"passphrase":"passphrase"}'

# Result
{
    "result":{
        "hash":
↪"143eac221da8079f017bd6fd6b6a08ea0623114c93c638b94334d16aae109666
↪",
        "contract_address":""
    }
}
```

SendTransaction

Send the transaction. Parameters `from`, `to`, `value`, `nonce`, `gasPrice` and `gasLimit` are required. If the transaction is to send contract, you must specify the `contract`.

| Protocol | Method | API | | — | — | — | | gRpc | | SendTransaction | | HTTP | POST | /v1/user/transaction |

Parameters

`from` Hex string of the sender account addresss.

`to` Hex string of the receiver account addresss.

`value` Amount of value sending with this transaction.

`nonce` Transaction nonce.

`gas_price` gasPrice sending with this transaction.

`gas_limit` gasLimit sending with this transaction.

`type` transaction payload type. If the type is specified, the transaction type is determined and the corresponding parameter needs to be passed in, otherwise the transaction type is determined according to the contract and binary data. [optional]

- type enum:
  - `binary`: normal transaction with binary

  - `deploy`: deploy smart contract
  - `call`: call smart contract function

`contract` transaction contract object for deploy/call smart contract. [optional]

- Sub properties:
  - `source` contract source code for deploy contract.
  - `sourceType` contract source type for deploy contract. Currently support `js` and `ts`
    * `js` the contract source write with javascript.
    * `ts` the contract source write with typescript.
  - `function` the contract call function for call contarct function.
  - `args` the params of contract. The args content is JSON string of parameters array.

`binary` any binary data with a length limit = 64bytes. [optional]

Notice:

- `from = to` when deploy a contract, the `to` address must be equal to `from` address.
- `nonce` the value is **plus one**(+1) on the nonce value of the current from address. Current nonce can get from GetAccountState.
- `gasPrice` and `gasLimit` need for every transaction. We recommend taking them use GetGasPrice and EstimateGas.
- `contract` parameter only need for smart contract deploy and call. When a smart contract is deployed, the `source` and `sourceType` must be specified, the `args` is optional and passed in when the initialization function takes a parameter. The `function` field is used to call the contract method.

Returns

`txhash` transaction hash.

`contract_address` returns only for deploying contract transaction.

Normal Transaction Example

```
# Request
curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/admin/transaction -d '{"from":
↪"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5","to":
↪"n1SAeQRVn33bamxN4ehWUT7JGdxipwn8b17", "value":
↪"1000000000000000000","nonce":1000,"gasPrice":"1000000","gasLimit
↪":"2000000"}'

# Result
{
    "result":{
      "txhash":
↪"fb5204e106168549465ea38c040df0eacaa7cbd461454621867eb5abba92b4a5
↪",
```

```
      "contract_address":""
    }
}
```

Deploy Smart Contract Example

```
# Request
curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/admin/transaction -d '{"from":
↪"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5","to":
↪"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5", "value":"0","nonce":2,
↪"gasPrice":"1000000","gasLimit":"2000000","contract":{
"source":"\"use strict\";var BankVaultContract=function()
↪{LocalContractStorage.defineMapProperty(this,\"bankVault\")};
↪BankVaultContract.prototype={init:function(){},
↪save:function(height){var deposit=this.bankVault.get(Blockchain.
↪transaction.from);var value=new BigNumber(Blockchain.transaction.
↪value);if(deposit!=null&&deposit.balance.length>0){var␣
↪balance=new BigNumber(deposit.balance);value=value.plus(balance)}
↪var content={balance:value.toString(),height:Blockchain.block.
↪height+height};this.bankVault.put(Blockchain.transaction.from,
↪content)},takeout:function(amount){var deposit=this.bankVault.
↪get(Blockchain.transaction.from);if(deposit==null){return 0}
↪if(Blockchain.block.height<deposit.height){return 0}var␣
↪balance=new BigNumber(deposit.balance);var value=new␣
↪BigNumber(amount);if(balance.lessThan(value)){return 0}var␣
↪result=Blockchain.transfer(Blockchain.transaction.from,value);
↪if(result>0){deposit.balance=balance.dividedBy(value).toString();
↪this.bankVault.put(Blockchain.transaction.from,deposit)}return␣
↪result}};module.exports=BankVaultContract;","sourceType":"js",
↪"args":""}}'

# Result
{
    "result":{
        "txhash":
↪"3a69e23903a74a3a56dfc2bfbae1ed51f69debd487e2a8dea58ae9506f572f73
↪",
        "contract_address":"n21Y7arNbUfLGL59xgnA4ouinNxyvz773NW"
    }
}
```

SignHash

SignHash sign the hash of a message.

| Protocol | Method | API | | — | — | — | | gRpc | | SignHash | | HTTP | POST | /v1/admin/sign/hash |

Parameters

`address` Sign address

`hash` A sha3256 hash of the message

`alg` Sign algorithm

Returns

`data` Signed transaction data.

sign normal transaction Example

```
# Request
curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/admin/sign/hash -d '{"address":
↪"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5","hash":"W+rOKNqs/
↪tlvz02ez77yIYMCOr2EubpuNh5LvmwceI0=","alg":1}'

# Result
{
    "result":{
        "data":
↪"a7HHsLRvKTNazD1QEogY+Fre8KmBIyK+lNa4zv0Z72puFVkY9uZD6nGixGx/
↪6s1x6Baq7etGwlDNxVvHsoGWbAA="
    }
}
```

StartPprof

StartPprof starts pprof

| Protocol | Method | API | | — | — | — | | gRpc | | Pprof | | HTTP | POST | /v1/admin/pprof |

Parameters

`listen` the address to listen

Returns

`result` start pprof result

Example

```
# Request
curl -i -H 'Content-Type: application/json' -X POST http://
↪localhost:8685/v1/admin/pprof -d '{"listen":"0.0.0.0:1234"}'

# Result
{
    "result":{
        "result":true
    }
}
```

GetConfig

GetConfig return the config current neb is using

| Protocol | Method | API | | — | — | — | | gRpc | | GetConfig | | HTTP | GET | /v1/admin/getConfig |

Parameters

none

Returns

`config` neb config

Example

```
# Request
curl -i -H 'Content-Type: application/json' -X GET http://
↪localhost:8685/v1/admin/getConfig

# Result
{
    "result":{
        "config":{
            "network":{
                "seed":[],
                "listen":["0.0.0.0:8680"],
                "private_key":"conf/network/ed25519key",
                "network_id":1
            },
            "chain":{
                "chain_id":100,
                "genesis":"conf/default/genesis.conf",
                "datadir":"data.db",
                "keydir":"keydir",
                "start_mine":true,
                "coinbase":"n1QZMXSZtW7BUerroSms4axNfyBGyFGkrh5",
                "miner":"n1Zn6iyyQRhqthmCfqGBzWfip1Wx8wEvtrJ",
                "passphrase":"",
                "enable_remote_sign_server":false,
                "remote_sign_server":"",
                "gas_price":"",
                "gas_limit":"",
                "signature_ciphers":["ECC_SECP256K1"]
            },
            "rpc":{
                "rpc_listen":["127.0.0.1:8684"],
                "http_listen":["127.0.0.1:8685"],
                "http_module":["api","admin"],
                "connection_limits":0,
                "http_limits":0,
                "http_cors":[]
```

```
            },
            "stats":{
                "enable_metrics":false,
                "reporting_module":[],
                "influxdb":{
                    "host":"http://localhost:8086",
                    "port":0,
                    "db":"nebulas",
                    "user":"admin",
                    "password":"admin"
                },
                "metrics_tags":[]
            },
            "misc":null,
            "app":{
                "log_level":"debug",
                "log_file":"logs",
                "log_age":0,
                "enable_crash_report":true,
                "crash_report_url":"https://crashreport.nebulas.io",
                "pprof":{
                    "http_listen":"0.0.0.0:8888",
                    "cpuprofile":"",
                    "memprofile":""
                },
                "version":"0.7.0"
            }
        }
    }
}
```

4.6 REPL console

Nebulas provide an interactive javascript console, which can invoke all API and management RPC methods. The console is connected to the local node by default without specifying host.

4.6.1 start console

Start console using the command:

```
./neb console
```

In the case of not specifying the configuration file, the terminal's startup defaults to the configuration of `conf/default/config.conf`. If the local configuration file is not available or you want to specify the configuration file, the terminal starts like this:

```
./neb -c <config file> console
```

console interaction

The console can use the `admin.setHost` interface to specify the nodes that are connected. When the console is started or the host is not specified, the terminal is interacting with the local node. **Therefore, you need to start a local node before starting the console.**

```
> admin.setHost("https://testnet.nebulas.io")
```

Tips: The Testnet only starts the RPC interface of the API, so only the api scheme is available.

4.6.2 console usage

We have API and admin two schemes to access the console cmds. Users can quickly enter instructions using the `TAB` key.

```
> api.
api.call                    api.getBlockByHash          api.
↪getNebState              api.subscribe
api.estimateGas             api.getBlockByHeight        api.
↪getTransactionReceipt
api.gasPrice                api.getDynasty              api.
↪latestIrreversibleBlock
api.getAccountState         api.getEventsByHash         api.
↪sendRawTransaction
```

```
> admin.
admin.accounts                      admin.nodeInfo
↪    admin.signHash
admin.getConfig                     admin.sendTransaction
↪    admin.signTransactionWithPassphrase
admin.lockAccount                   admin.
↪sendTransactionWithPassphrase admin.startPprof
admin.newAccount                    admin.setHost
↪    admin.unlockAccount
```

Some management methods may require passphrase. The user can pass in the password when the interface is called, or the console prompts the user for input when the password is not entered. **We recommend using a console prompt to enter your password because it is not visible.**

Enter the password directly:

```
> admin.unlockAccount("n1UWZa8yuvRgePRPgp8a2jX4J9UwGXfHp6i",
↪"passphrase")
{
```

```
    "result": {
        "result": true
    }
}
```

Use terminal prompt:

```
> admin.unlockAccount("n1UWZa8yuvRgePRPgp8a2jX4J9UwGXfHp6i")
Unlock account n1UWZa8yuvRgePRPgp8a2jX4J9UwGXfHp6i
Passphrase:
{
    "result": {
        "result": true
    }
}
```

The interfaces with passphrase prompt:

```
admin.newAccount
admin.unlockAccount
admin.signHash
admin.signTransactionWithPassphrase
admin.sendTransactionWithPassphrase
```

The command parameters of the command line are consistent with the parameters of the RPC interface. NEB RPC and NEB RPC_Admin.

4.6.3 console exit

The console can exit with the `ctrl-C` or `exit` command.

CHAPTER 5

Infrastructure

5.1 Network Protocol

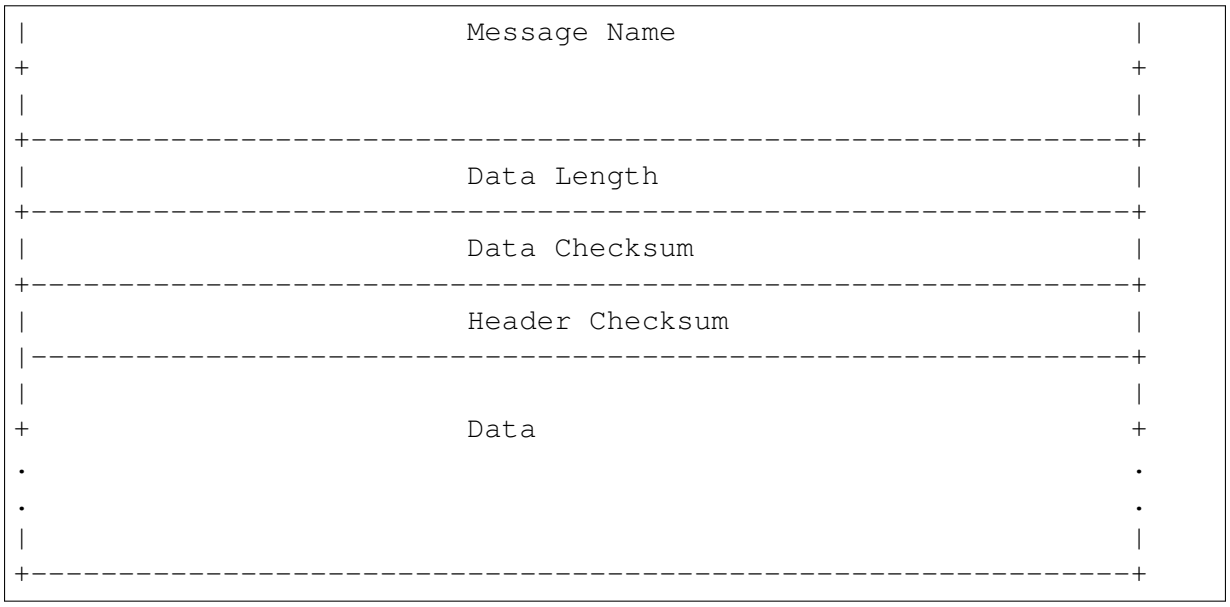
For the network protocol, there are lots of existing solution. However, the Nebulas Team finally decides to define our own wire protocol, ensures the following principles to design the protocol:

- the protocol should be simple and straight.
- the message can be verified before receiving all package, fail early.
- the protocol should be debugging friendly, developer can easily understand the raw message.

5.1.1 Protocol

In Nebulas, we define our own wire protocol, as the following:

```
 0               1               2               3               ␣
↪(bytes)
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Magic Number                         |
+---------------------------------------------------------------+
|                          Chain ID                             |
+-----------------------------------------------+---------------+
|                          Reserved             |   Version     |
+-----------------------------------------------+---------------+
|                                                               |
+                                                               +
```



- Magic Number: 32 bits (4 chars)
  - The protocol magic number, A constant numerical or text value used to identify protocol.
  - Default: 0x4e, 0x45, 0x42, 0x31
- Chain ID: 32 bits
  - The Chain ID is used to distinguish the test network and the main network.
- Reserved: 24 bits
  - reserved field.
  - The first bit indicates whether the network message is compressed.
  - compressed: {0x80, 0x0, 0x0}; uncompressed: {0x0, 0x0, 0x0}
- Version: 8 bits
  - The version of the Message Name.
- Message Name: 96 bits (12 chars)
  - The identification or the name of the Message.
- Data Length: 32 bits
  - The total length of the Data.
- Data Checksum: 32 bits
  - The CRC32 checksum of the Data.
- Header Checksum: 32 bits
  - The CRC32 checksum of the fields from Magic Number to Data Checksum, totally 256 bits.
- Data: variable length, max 512M.

- The message data.

We always use Big-Endian in message protocol.

5.1.2 Handshaking Messages

- Hello

the handshaking message when peer connect to others.

```
version: 0x1

data: struct {
    string node_id  // the node id, generated by underlying libp2p.
    string client_version // the client version, x.y.z schema, eg.␣
↪0.1.0.
}
```

- OK

the response message for handshaking.

```
version: 0x1

data: struct {
    string node_id // the node id, generated by underlying libp2p.
    string node_version // the client version, x.y.z schema, eg. 0.
↪1.0.
}
```

- Bye

the message to close connection.

```
version: 0x1
data: struct {
    string reason
}
```

5.1.3 Networking Messages

- NetSyncRoutes

request peers to sync route tables.

```
version: 0x1
```

- NetRoutes

contains the local route tables.

```
version: 0x1
data: struct {
    PeerID[] peer_ids // router tables.
}

struct PeerID {
    string node_id  // the node id.
}
```

5.1.4 Nebulas Messages

TBD.

5.2 Crypto Design Doc

Similar to Bitcoin and Ethereum, Nebulas also adopts elliptic curve algorithm as its basic encryption algorithm for Nebulas transactions. UsersâĂŹ private key will be encrypted with userâĂŹs passphrases and stored in keystore.

5.2.1 Hash

Support generic hash functions, like sha256, sha3256 and ripemd160 etc.

5.2.2 Keystore

Nebulas Keystore are designed to manage userâĂŹs keys.

Key

The Key interface is designed to support various keys, including symmetric keys and asymmetric keys.

Provider

Keystore provide different methods to save keys, such as `memory_provider` and `persistence_provider`. Before saved, key has been encrypted in keystore.

- `memory provider`: This type of provider keep keys in memory. After the key has been encrypted with the passphrase when user setkey or load, it is cached in memory provider.

- `persistence provider`: This type of provider serialize the encrypted key to the file. The file is compatible with the ethereumâĂŹs keystore fileïijŇusers can back up the address with its privatekey in it.

Signature

The Signature interface is used to provide applications the functionality of a digital signature algorithm. A Signature object can be used to generate and verify digital signatures.

There are two phases to use a Signature object for either signing data :

- Initialization: with a private key, which initializes the signature for signing (see initSign() in the source code of go-nebulas).
- Signing on all input bytes.

A Signature object can recover the public key with a signatrue and the plain text was singed on(see function RecoverSignerFromSignature in go-nebulas). So just comparing the from address and the address derived from the public key can verfiy a transaction

> Similar as Android Keystore, TPM, TEE and hardware low level security protection will be supported as a provider later.

NVM - Nebulas Virtual Machine

NVM is one of the most important components in Nebulas. As the name described, it provides a managed virtual machine execution environments for Smart Contract and Protocol Code.

go-nebulas now support two kinds of Virtual Machine:

- V8: Chrome V8
- LLVM: Low-Level Virtual Machine

Nebulas V8 Engine

In go-nebulas, we design and implement Nebulas V8 Engine based on Chrome V8.

Nebulas V8 Engine provides a high performance sandbox for Smart Contract execution. It guarantees user deployed code is running in a managed environment, and prevents massive resource consumption on hosts. Owing to use of Chrome V8, JavaScript and TypeScript are first-class languages for Nebulas Smart Contract. Anyone familiar with JavaScript or TypeScript can write their own Smart Contract and run it in Nebulas V8.

The following content is an example of Smart Contract written in JavaScript:

```
"use strict";

var BankVaultContract = function() {
    LocalContractStorage.defineMapProperty(this, "bankVault");
```

```
};

// save value to contract, only after height of block, users can
↪takeout
BankVaultContract.prototype = {
    init:function() {},
    save:function(height) {
        var deposit = this.bankVault.get(Blockchain.transaction.
↪from);
        var value = new BigNumber(Blockchain.transaction.value);
        if (deposit != null && deposit.balance.length > 0) {
            var balance = new BigNumber(deposit.balance);
            value = value.plus(balance);
        }
        var content = {
            balance:value.toString(),
            height:Blockchain.block.height + height
        };
        this.bankVault.put(Blockchain.transaction.from, content);
    },
    takeout:function(amount) {
        var deposit = this.bankVault.get(Blockchain.transaction.
↪from);
        if (deposit == null) {
            return 0;
        }
        if (Blockchain.block.height < deposit.height) {
            return 0;
        }
        var balance = new BigNumber(deposit.balance);
        var value = new BigNumber(amount);
        if (balance.lessThan(value)) {
            return 0;
        }
        var result = Blockchain.transfer(Blockchain.transaction.
↪from, value);
        if (result > 0) {
            deposit.balance = balance.dividedBy(value).toString();
            this.bankVault.put(Blockchain.transaction.from,
↪deposit);
        }
        return result;
    }
};

module.exports = BankVaultContract;
```

For more information about the smart contract in Nebulas, please go to Smart Contract.

For more information about the design of Nebulas V8 Engine, please go to Nebulas V8 Engine.

LLVM

TBD.

5.3 Nebulas V8 Engine

Nebulas V8 Engine is

5.4 LLVM Engine

TBD.

5.5 permission_control_in_smart_contract

5.5.1 What Is Permission Control Of Smart Contract

The permission control of a smart contract refers to whether the contract caller has permission to invoke the function in the contract. There are two types of permission control: owner permission control and other permission control.

Owner permissions control: Only the creator of the contract can call this method, other callers can not call the method.

Other permission control: The contract method can be invoked if the contract developer defines a conditional caller according to the contract logic. Otherwise, it cannot be invoked.

5.5.2 Owner Permission Control

If you want to specify a owner to a small contract and wish if some functions could be called only by the owner and no one else. You can use following lines of code in your smart contract.

```
"use strict";
var onlyOwnerContract = function () {
    LocalContractStorage.defineProperty(this, "owner");
};
onlyOwnerContract.prototype = {
  init: function() {
          this.owner=Blockchain.transaction.from;
  },
  onlyOwnerFunction: function(){
          if(this.owner==Blockchain.transaction.from){
              //your smart contract code
```

```
            return true;
        }else{
            return false;
        }
  }
};
module.exports = BankVaultContract;
```

Explanation:

The function init is only called once when the contract is deployed, there you specify the owner of the contract.The onlyOwnerFunctiuon ensures that the function is called by the owner of contact.

5.5.3 Other Permission Control

In your smart contract, if you need to specify other permission control to a smart contract. For example, in your smart contract, you need to verify the transaction value in your smart contract. you can write your smart contract in the following way.

```
'use strict';
var Mixin = function () {};
Mixin.UNPAYABLE = function () {
    if (Blockchain.transaction.value.gt(0)) {
        return false;
    }
    return true;
};
Mixin.PAYABLE = function () {
    if (Blockchain.transaction.value.gt(0)) {
        return true;
    }
    return false;
};
Mixin.POSITIVE = function () {
    console.log("POSITIVE");
    return true;
};
Mixin.UNPOSITIVE = function () {
    console.log("UNPOSITIVE");
    return false;
};
Mixin.decorator = function () {
    var funcs = arguments;
    if (funcs.length < 1) {
        throw new Error("mixin decorator need parameters");
    }
    return function () {
        for (var i = 0; i < funcs.length - 1; i ++) {
```

```
            var func = funcs[i];
            if (typeof func !== "function" || !func()) {
                throw new Error("mixin decorator failure");
            }
        }
        var exeFunc = funcs[funcs.length - 1];
        if (typeof exeFunc === "function") {
            exeFunc.apply(this, arguments);
        } else {
            throw new Error("mixin decorator need an executable␣
↪method");
        }
    };
};
var SampleContract = function () {
};
SampleContract.prototype = {
    init: function () {
    },
    unpayable: function () {
        console.log("contract function unpayable:", arguments);
    },
    payable: Mixin.decorator(Mixin.PAYABLE, function () {
        console.log("contract function payable:",arguments);
    }),
    contract1: Mixin.decorator(Mixin.POSITIVE, function (arg) {
        console.log("contract1 function:", arg);
    }),
    contract2: Mixin.decorator(Mixin.UNPOSITIVE, function (arg) {
        console.log("contract2 function:", arg);
    }),
    contract3: Mixin.decorator(Mixin.PAYABLE, Mixin.POSITIVE,␣
↪function (arg) {
        console.log("contract3 function:", arg);
    }),
    contract4: Mixin.decorator(Mixin.PAYABLE, Mixin.UNPOSITIVE,␣
↪function (arg) {
        console.log("contract4 function:", arg);
    })
};
module.exports = SampleContract;
```

Explanation:

Mixin.UNPAYABLE,Mixin.PAYABLE,Mixin.POSITIVE ,Mixin.UNPOSITIVE are permission control functionãĂĆThe permission control function as follows:

- Mixin.UNPAYABLE: check the transaction sent value, if value is less than 0 return true, otherwise returns false
- Mixin.UNPAYABLE : check the transaction sent value, if value is greater than 0 return

true, otherwise returns false

- Mixin.UNPOSITIVE ïijŽoutput log UNPOSITIVE
- Mixin.POSITIVE ïijŽoutput log POSITIVE

Implement permission control in Mixin.decoratorïijŽ

- check arguments: if (funcs.length < 1)
- invoke permission control function: if (typeof func !== “function” || !func())
- if permission control function success ,invoke other function: var exeFunc = funcs[funcs.length - 1]

Permission control tests in smart contracts are as follows:

- The permission control function of the contract1 is Mixin.POSITIVE. If the permission check passes, the output is printed, otherwise the error is thrown by the permission check function.

```
    contract1: Mixin.decorator(Mixin.POSITIVE, function (arg)
↪{
        console.log("contract1 function:", arg);
    })
```

- The permission control function of the contract2 is Mixin.UNPOSITIVE. If the permission check passes, the output is printed, otherwise the error is thrown by the permission check function.

```
    contract2: Mixin.decorator(Mixin.UNPOSITIVE, function␣
↪(arg) {
            console.log("contract2 function:", arg);
    })
```

- The permission control function of the contract3 is Mixin.PAYABLE, Mixin.POSITIVE. If the permission check passes, the output is printed, otherwise the error is thrown by the permission check function.

```
   contract3: Mixin.decorator(Mixin.PAYABLE, Mixin.POSITIVE,␣
↪function (arg) {
            console.log("contract3 function:", arg);
    })
```

- The permission control function of the contract4 is Mixin.PAYABLE, Mixin.UNPOSITIVE. If the permission check passes, the output is printed, otherwise the error is thrown by the permission check function.

```
    contract4: Mixin.decorator(Mixin.PAYABLE, Mixin.
↪UNPOSITIVE, function (arg) {
             console.log("contract4 function:", arg);
    })
```

Tips:

With reference to the above example, the developer needs only three steps to implement other permission controls:

- Implement permission control functions.
- Implement the decorator function, and the permission check is completed by the conditional statement if (typeof func !== “function” || !func()).
- Refer to the contract1 function to implement other permission control.

CHAPTER 6

Licensing

6.1 Nebulas Open Source Project License

The preferred license for the Nebulas Open Source Project is the GNU Lesser General Public License Version 3.0 (âĂIJLGPL v3âĂİ), which is commercial friendly, and encourage developers or companies modify and publish their changes.

However, we also aware that big corporations is favoured by other licenses, for example, Apache Software License 2.0 (âĂIJApache v2.0âĂİ), which is more commercial friendly. For the Nebulas Team, we are very glad to see the source code and protocol of Nebulas is widely used both in open source applications and non-open source applications.

In this way, we are still considering the license choice, which kind of license is the best for nebulas ecosystem. We expect to select one of the LGPL v3, the Apache v2.0 or the MIT license. If the latter is chosen, it will come with an amendment allowing it to be used more widely.

6.2 Contributor License Agreement

TBD.

6.2.1 Config

There are four types of configuration files in Nebulas.

- Normal node.
- Miner node.(Miner - related configuration is increased relative to normal nodes)

- Super node.(Some connection limits are higher than normal nodes)
- Sign node. (Do not synchronize information with any node, only do signature and unlock)

Normal node

```
network {
  seed: ["/ip4/13.251.33.39/tcp/8680/ipfs/
↪QmVm5CECJdPAHmzJWN2X7tP335L5LguGb9QLQ78riA9gw3"]
  listen: ["0.0.0.0:8680"]
  private_key: "conf/networkkey"
}

chain {
  chain_id:1
  datadir: "data.db"
  keydir: "keydir"
  genesis: "conf/genesis.conf"
  signature_ciphers: ["ECC_SECP256K1"]
}

rpc {
    rpc_listen: ["0.0.0.0:8784"]
    http_listen: ["0.0.0.0:8785"]
    http_module: ["api","admin"]
    connection_limits:200
    http_limits:200
}

app {
    log_level: "debug"
    log_file: "logs"
    enable_crash_report: true
}

stats {
    enable_metrics: false
}
```

Miner node

```
network {
  seed: ["/ip4/13.251.33.39/tcp/8680/ipfs/
↪QmVm5CECJdPAHmzJWN2X7tP335L5LguGb9QLQ78riA9gw3"]
  listen: ["0.0.0.0:8680"]
  private_key: "conf/networkkey"
}
```

```
chain {
  chain_id: 1
  datadir: "data.db"
  keydir: "keydir"
  genesis: "conf/genesis.conf"
  coinbase: "n1EzGmFsVepKduN1U5QFyhLqpzFvM9sRSmG"
  signature_ciphers: ["ECC_SECP256K1"]
  start_mine:true
  miner: "n1PxjEu9sa2nvk9SjSGtJA91nthogZ1FhgY"
  remote_sign_server: "127.0.0.1:8694"
  enable_remote_sign_server: true
}

rpc {
    rpc_listen: ["127.0.0.1:8684"]
    http_listen: ["0.0.0.0:8685"]
    http_module: ["api","admin"]
    connection_limits:200
    http_limits:200
}

app {
    log_level: "debug"
    log_file: "logs"
    enable_crash_report: true
}

stats {
    enable_metrics: false
}
```

Super node

```
network {
  seed: ["/ip4/13.251.33.39/tcp/8680/ipfs/
↪QmVm5CECJdPAHmzJWN2X7tP335L5LguGb9QLQ78riA9gw3"]
  listen: ["0.0.0.0:8680"]
  private_key: "conf/networkkey"
  stream_limits: 500
  reserved_stream_limits: 50
}

chain {
  chain_id:1
  datadir: "data.db"
  keydir: "keydir"
  genesis: "conf/genesis.conf"
  signature_ciphers: ["ECC_SECP256K1"]
```

```
}

rpc {
    rpc_listen: ["0.0.0.0:8684"]
    http_listen: ["0.0.0.0:8685"]
    http_module: ["api"]
    connection_limits:500
    http_limits:500
    http_cors: ["*"]
}

app {
    log_level: "debug"
    log_file: "logs"
    enable_crash_report: true
    pprof:{
        http_listen: "0.0.0.0:8888"
    }
}

stats {
    enable_metrics: false
}
```

Sign node

```
network {
  listen: ["0.0.0.0:8680"]
  private_key: "conf/networkkey"
}

chain {
  chain_id:0
  datadir: "data.db"
  keydir: "keydir"
  genesis: "conf/genesis.conf"
  signature_ciphers: ["ECC_SECP256K1"]
}

rpc {
    rpc_listen: ["0.0.0.0:8684"]
    http_listen: ["127.0.0.1:8685"]
    http_module: ["admin"]
    connection_limits:200
    http_limits:200
}

app {
    log_level: "debug"
```

```
    log_file: "logs"
    enable_crash_report: true
    pprof:{
        http_listen: "127.0.0.1:8888"
    }
}

stats {
    enable_metrics: false
}
```

6.2.2 Contributors

Coming Soon.

CHAPTER 7

Indices and tables

- genindex
- modindex
- search