Accounts

`Account` is a very important object entity in the Conflux network. It is used to store CFX (every account has its CFX balance) and send Conflux transactions. Accounts and account balances are stored in a huge table in the Conflux VM, and they are part of the full state of the Conflux ledger.

Types of Accounts

Conflux has two types of accounts.

- External accounts (private key accounts) - are controlled by the holder of the private key
- Smart Contracts - are the ones deployed in the network and controlled by the contract codes

Note: There is a special type of smart contract in the Conflux network - the internal contracts. They are created automatically when the network is started or upgraded, but not by deploying contract codes. There are currently 6 internal contracts.

Similarities of Accounts

- Both of them can accept, hold, and send CFX and tokens
- Both of them can interact with smart contracts in the network

Differences of Accounts

External Accounts

- Creating external accounts does not have costs, such as CFX or other resources
- They can send transactions to others
- Transactions between external accounts can only be CFX or token transactions

Smart Contracts

- Creating smart contracts does have costs, as it uses the network's storage and computational resources
- Transactions can only be sent to other contracts as a response to a received transaction
- Transactions sent from external accounts to contract accounts can trigger the smart contract's codes to perform many different operations, such as token transfers, creating new contracts, etc.

External Accounts and Public-private Key Pairs

An external account is generated by a public-private key pair that can be used to prove that a transaction was indeed signed by the account, in order to prevent transaction falsification. The private key is used by the user to sign a transaction. It gives you the right to operate the assets on the account corresponding to the private key. Essentially, the user does not hold the CFX or the tokens but the private key. CFX is always present in Conflux's ledger.

This mechanism prevents malicious users from broadcasting fake transactions, as we can verify the address that sends the transaction at any time.

For example, if Alice wants to send CFX from her account to Bob's account, she needs to create a transaction and send it to the network for verification. Conflux uses the public key encryption mechanism to ensure that Alice can prove that the transaction is sent by herself. Suppose now, Eve, a malicious user, directly broadcasts a transaction, say, "send 5 CFX from Alice's account to Eve's account". Without the above-mentioned mechanism, no one would be able to verify that the transaction was sent by Alice.

External Account Creation

When you want to create an external account, you can use a wallet, like FluentWallet, or any language library, where essentially both of them generate a random private key.

A private key contains 64 hexadecimal characters and can be encrypted using a password.

```
ffffffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd036415f
```

The public key is calculated from the private key by the Elliptic Curve Cryptography Algorithm. Then, Keccak-256 hashing is performed on the public key, and the Conflux address is yielded by encoding the last 20 bytes (the first 4 bit will be set to 0001) of the result with base 32 formats.

```
// Mainnet address
cfx: aatktb2te25ub7dmyag3p8bbdgr31vrbeackztm2rj
// Testnet address
cfxtest: aatktb2te25ub7dmyag3p8bbdgr31vrbeajcg9pwkc
```

The public key can be calculated from the private key, but the private key cannot be calculated from the public key. The private key has to be kept safe by the user.

Smart Contract Account

Smart contracts also have base32 encoded addresses

```
cfx: acf2rcsh8payyxpg6xj7b0ztswwh81ute60tsw35j7
```

This address is determined when the contract is deployed and is calculated by the deployed transaction's `sender address`, `nonce`, and the smart contract's `code`.

Note: The addresses of internal contracts are special - they are assigned by the network itself.

Details of Accounts

The global state of Conflux is composed of individual account states, each of which is an address-state pair (key pair).

A Conflux account state includes five parts:

- `Basic state` is the basic state of the account.
- `Storage state` is a key/value database or storage space that can be used to store custom states or data of smart contracts.
- `Code information` is the code information of the smart contract account. It includes the `contract codes` and the `address` of the account that paid the fee for the storage space occupied by the codes.
- `Staking deposit list` is the list of Staking operations of the accounts (it will be removed in the next Hardfork).
- `Staking vote lock list` is the list of lock operations performed by the account to participate in DAO voting.

The basic status of the account consists of eight fields as follows:

- `nonce` is a counter to keep track of the number of transactions sent by an account. It is also used to ensure that each transaction can only be executed once. For contract accounts, this value indicates the number of `contracts created by this contract`.
- `balance` is the number of CFX of the address in Drip. Drip is the smallest unit of CFX, where 1CFX=10^{18} Drip.
- `codeHash` is the hash of the code of the contract account. The user can reference the contract code, the code cannot be modified after the contract is created. The code will be executed when the contract receives a message call. For external accounts, codeHash is a hash of an empty string.
- `stakingBalance` is the balance of the staked amount. Similarly, the unit is Drip.
- `admin` is the administrator address of the `contract account` recorded in the AdminControl internal contract. In default, the contract administrator is set to the account which deployed this contract when it is created. The administrator can destroy the contract it

manages through the internal contract AdminControl, or give the administrator role to another account. The administrator address of an external account is itself.
- `sponsorInfo` is the information of the contract sponsor. It contains `sponsor for gas`, `sponsor for collateral`, `sponsor gas limit`, `sponsor balance for gas`, and `sponsor balance for collateral`.
- `storageCollateral` is the amount of Drip staked to use the storage spaces.
- `accumulatedInterestReturn` is the amount of cumulative reward of the account from Staking. The unit of it is Drip. Starting with Conflux 2.0, users must also participate in PoS in order to receive the reward.

For more details about accounts, please refer to the `Accounts` section in Conflux Protocol Specification.

Revision #6
Created 2 August 2022 07:51:04 by Pana
Updated 2 August 2022 08:04:16 by Pana