



SAKURA BLOOM (SKB) white paper << system >>

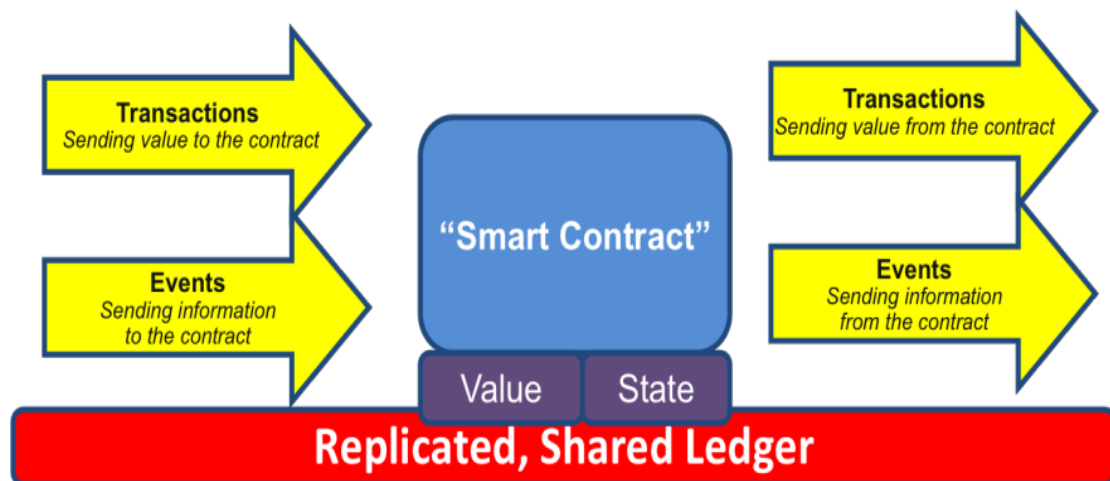
SKBはETHスマート契約技術に基づくものであり、これは現実世界の資産のデジタル化を行ない、最新のERC20トークン規格を通じて実現し、他の種類のトークンと比べ、より強い安全性と急速振替の優位性を持っています。

技術

ETHはビットコインのブロックチェーン技術を参考にして、その応用範囲を拡張しています。ビットコインはブロックチェーン技術を利用する専用計算器であるとするれば、ETHはブロックチェーン技術を利用した汎用コンピュータです。簡単に言えば、ETH＝ブロックチェーン+スマート契約です。

スマート契約

スマート契約プログラムは自動的に実行可能なコンピュータプログラムではありません。その自身はシステム参加者でもあります。これは受信した情報に対して応答し、価値の受信と保存ができ、また、外に情報と価値を送信することもできます。このプログラムは信頼できる人間のように、一時的に資産を保管することができ、いつも予め定められたルールに従って操作することができます。下記のイメージ図は一つのスマート契約モデルであり：1段コード（スマート契約）は共有可能でコピー可能な帳簿の上に配置されており、これは自分の状態を保持し、自分の資産をコントロールし、受信した外部情報または資産に対し応答できます。



スマート契約モデル: コピー可能で共有可能な帳簿の上で運転するコンピュータプログラムであり、情報を処理し、価値の受信・保存・送信できます。

ERC20 トークン

● ERC20 トークン規格

ERC20 トークン規格は約束されたワンセットのスマート契約関数とイベント名称です。トークンとは何ですか？トークン (Token) はブロックチェーンの中で価値を定義する方式であり、金融またはデジタル資産の評価に用いられるものです。

```
// https://github.com/ethereum/EIPs/issues/20
contract ERC20 {
    function totalSupply() constant returns (uint totalSupply);
    function balanceOf(address _owner) constant returns (uint balance);
    function transfer(address _to, uint _value) returns (bool success);
    function transferFrom(address _from, address _to, uint _value) returns (bool success);
    function approve(address _spender, uint _value) returns (bool success);
    function allowance(address _owner, address _spender) constant returns (uint remaining);
    event Transfer(address indexed _from, address indexed _to, uint _value);
    event Approval(address indexed _owner, address indexed _spender, uint _value);
}
```

これらの関数集を通じて、トークン発行総量、残高、トークン譲渡移転と承認コストなどの機能を得ることができます。これらの規格があると、ウォレットをデザイン・開発する拠所があり、あらゆるこれらの規格によって開発されたウォレットのサポートを得ることができます。

● ERC20 トークンの特徴

ERC20 規格に準拠したトークンは下記の特徴を持っています。

分散化

資産総量確定

資産移転可能

分散化

「分散化」は一種の現象または構造であり、多くのユーザーまたはノードを持ったシステムのみにも出現でき、各ユーザーは接続されることができ、また、他のノードに影響します。簡単に言えば、あらゆる人は中心であり、だれも他のノードと接続でき、また、他のノードに影響することができ、このフラット化、オープンソース化、平等化の現象または構造は「分散化」と言われています。

同時に、「分散化」はブロックチェーンの典型的な特徴の一つであり、それは分散型保存とアルゴリズムを使用しており、ネットワークノード全体の権利と義務が同じであり、システムにあるデータが基本的にネットワーク全体のノードによって共同で保持しており、これによって、ブロックチェーンが中央処理ノードに依存せず、データの分散型保存、記録とアップデートを実現しています。各ブロックチェーンは統一的な規則に遵守すべきであり、この規則は信用証明書ではなく、暗号アルゴリズムに基づくものであり、また、そのデータアップデート過程はユーザーの承認を必要とし、これによって、ブロックチェーンは仲介と信頼機関の裏書を必要としません。

資産総量確定

ERC20に基づくトークンは発行されると、その総量は変更できないこととなります。これによって、発行側は随意にトークンの総量を増加することを避けることができ、トークン価値の安定さを確保できます。

資産移転可能

各アドレスのトークンはアドレス保有人の資産を示しており、これらの資産は一定の価値を持っています。これらの資産を他人に移転する場合、ウォレットまたは取引所を通じて他人のアドレスに振替するだけで良いです。

English

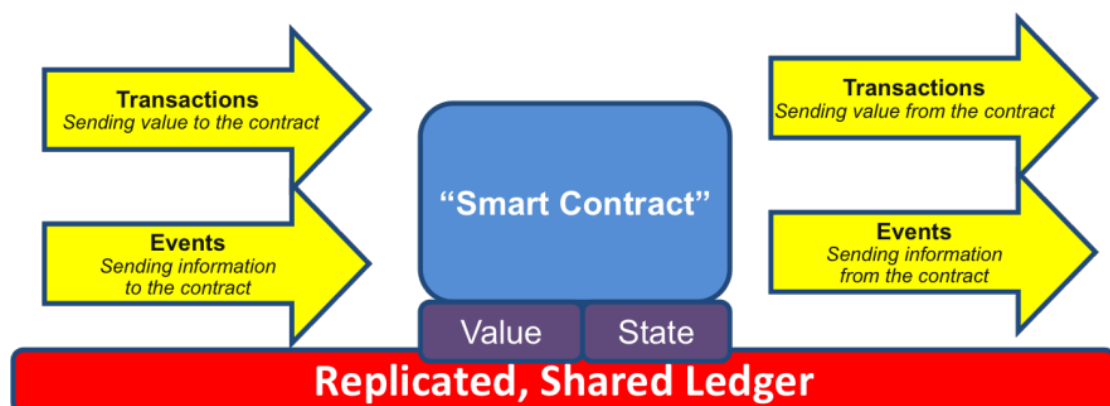
SKB is a product of intelligent contract technology based on Ethereum. It digitized the assets of the physical world and implemented it through the latest ERC20 tokens. It has greater security and the advantages of faster transfer money than other kinds of tokens.

Ethereum Technology

The Ethereum learns from the technology of bitcoin block chain and expands its application scope. If the bitcoin uses the dedicated calculator with block chain technology, the Ethereum will use the general-purpose computer with block chain technology. Briefly speaking, the Ethereum = block chain + intelligent contract.

Intelligent Contract

The intelligent contract program is not just a computer program that can be automatically executed. It's a system actors. It responds to the received information. It can receive and store value and also can send out information and value. This program is like a trusted person who can hold assets temporarily and always follow the rules in advance. The following diagram is an intelligent contract model. A piece of code (intelligent contract) is deployed in a shared and duplicated ledger. It can maintain its own state. It controls its own assets and responds to the received external information or assets.



Intelligent Contract Model: It's a computer program that runs on a duplicated and shared ledger. It can process information, receive, store, and send value.

ERC20

ERC20 Tokens

ERC20 Token Code

The ERC20 token code is a set of agreed intelligent contract function and event name. What is a token? A token (Token) is a way of defining value in a block chain that is used to demarcate financial or digital assets.

```
// https://github.com/ethereum/EIPs/issues/20
contract ERC20 {
    function totalSupply() constant returns (uint totalSupply);
    function balanceOf(address _owner) constant returns (uint balance);
    function transfer(address _to, uint _value) returns (bool success);
    function transferFrom(address _from, address _to, uint _value) returns (bool success);
    function approve(address _spender, uint _value) returns (bool success);
    function allowance(address _owner, address _spender) constant returns (uint remaining);
    event Transfer(address indexed _from, address indexed _to, uint _value);
    event Approval(address indexed _owner, address indexed _spender, uint _value);
}
```

Through these function sets, you can get the functions of total number of tokens issued, balance, transfer and distribution of the tokens, and approval of the currency. With these specifications, there is a basis for designing and developing wallets that can be supported by the wallets developed.

ERC20 Token Characteristics

The tokens defined by the ERC20 code have the following major features:

Decentralization

Determination of total assets

Assets transferable

Decentralization

"Decentralization" is a phenomenon or structure. It can only be present in a system with many users or nodes. Each user can connect and affect other nodes. Generally speaking, everyone is a center. Everyone can connect and affect other nodes. This flat, open-sourced, equality of the phenomenon or structure is called "decentralization".

At the same time, "decentralization" is one of the typical characteristics of block chain. It uses the distributed storage and computing power. The rights and obligations of the entire network node are the same. The data nature in the system is maintained by the whole network node, thus the block chain is no longer dependent on the central processing node to realize the distributed

storage, recording and updating of the data. Each block chain follows the uniform rules. This rule is based on a cipher algorithm rather than a credit certificate. The process of data update requires the approval of the user, thus laying the block chain does not require intermediary and trust agencies endorsement.

Determination of total assets

Based on the ERC20 tokens, once issued, its total can no longer be modified so as to avoid the issuers arbitrarily increase the total amount of tokens, which results in the instability of tokens value.

Assets transferable

The tokens of each address represent the assets of the address holders. These assets have some value. When you need to transfer these assets to others, you only need to transfer money to the addresses of others by the wallet or Exchange.