

An abstract composition on a dark gray background. It features several diagonal lines: a white line in the upper left, a light gray line in the lower left, and a bright pink line in the lower right. The word 'Substrate' is written in a bold, orange, sans-serif font, positioned between the white and light gray lines. The word 'River' is written in the same font and color, positioned between the light gray and pink lines.

Substrate

River



Kitties-001

Generating Random Data

<https://substrate.dev/substrate-collectables-workshop/#/2/generating-random-data>



为什么需要随机数

我们需要创建很多Kitty，需要对生成的Kitty做区分，每一个Kitty都需要唯一的id



生成随机数的方法

1- Generating a Random Seed

`<system::Module<T>>::random_seed()` : 对于同一块中的多个事务，随机种子不会改变

Substrate使用一种安全的混合算法，它使用前面块的熵为后面块生成新的随机数据。

2- Using a Nonce

```
let nonce = <Nonce<T>>::get();
```



生成随机数的方法

3 - Hashing Data

```
let sender = ensure_signed(origin)?;  
let nonce = <Nonce<T>>::get();  
let random_seed = <system::Module<T>>::random_seed();  
  
let random_hash = (random_seed, sender, nonce).using_encoded(<T as  
system::Trait>::Hashing::hash);  
  
<Nonce<T>>::mutate(|n| *n += 1);
```



Checking for Collision

```
ensure!(!<Kitties<T>>::exists(new_id), "This new id already exists");
```



```
support::ensure
```



You turn

1-create unique id

2- create a new kitties storage : map id=>kitty

3- create a KittyOwner storage: map id=>AccountId

4- function: create_kitty()



```
error[E0382]
--> /Users/*/blockchain/substrate/record-substrate/substrate-package/substratekitties/
runtime/src/substratekitties.rs:62:50
|
39 |         let sender = ensure_signed(origin)?;
    |           ----- move occurs because `sender` has type `::AccountId`, which does not implement the `Copy` trait
...
47 |         let random_hash = (random_seed, sender, nonce).using_encoded(<T as system::Trait>::Hashing::hash);
    |                                     ----- value moved here
...
62 |         <KittyOwner<T>>::insert(random_hash, &sender); //&sender是sender的引用
    |                                           ^^^^^^^^ value borrowed here after move
```




视频内容备注

Kitties get(kitty): map T::Hash => Kitty<T::Hash, T::Balance>;

1- kitty_id和Kitty对象的对应关系

KittyOwner get(owner_of): map T::Hash => Option<T::AccountId>;

2- kitty_id和创建者账户的对应关系

OwnedKitty get(kitty_of_owner): map T::AccountId => T::Hash;

3- 创建者账户和kitty_id的对应关系



Substrate

River

Thanks