Random EOSIO

rubenabix - EOS Costa Rica

Julio 2020

1 Problema

Calcular un número pseudo aleatorio entre 1 y 50, mediante operaciones a nivel de bits.

Componentes de entropía:

- Current blocktime
- tapos_block_prefix\tapos_block_num

2 Función en EOSIO

```
uint64_t getRandom(int max) {
  uint64_t A = eosio::tapos_block_num();
  uint64_t B = eosio::tapos_block_prefix();
  uint64_t C = A ^ B;
  uint64_t D = eosio::current_time_point().sec_since_epoch();
  uint64_t E = D << 32;
  uint64_t F = (C | E);
  uint64_t G = (F % max) + 1;
  eosio::print(":random:");
  eosio::print(G);
  return G;
}
```

3 Algoritmo

1. Combinar los números de bloque A y B mediante el operador XOR y obtener el valor C.

	Decimal	Binario
tbn: A	62163	00000000000000001111001011010011
tbp: B	1714367418	01100110001011110010101110111010
A XOR B: C	1714411881	01100110001011111101100101101001

2. Tomar el tiempo actual D y hacer un deplazamiento de 32 bits en una variable uint64_t y aplicar la operación OR junto con el valor anterior C.

	Decimal
(uint64_u) time: D	1595303468
(uint64_u) time <<32: E	6851776222255382528

	Binario
D:	00000000000000000000000000000000010111110001011001100011000101100
E:	01011111000101100110011000101100000000000000000000000000000000000

	Binario / Decimal
C:	00000000000000000000000000000000011001100010111111011001011010 01
E:	01011111000101100110011000101100000000000000000000000000000000000
C OR E: F	01011111000101100110011000101100011001100010111111011001011010 01
F	6851776223969794409

Se aplica el módulo de la división

G: 6851776223969794409 % 50 + 1 = 10
G: 9 + 1 = 10