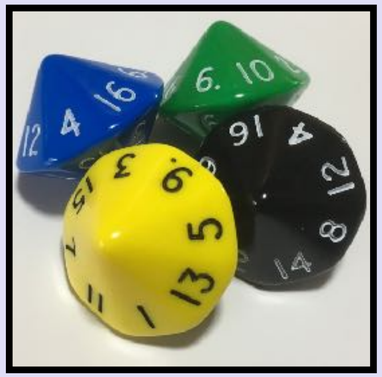
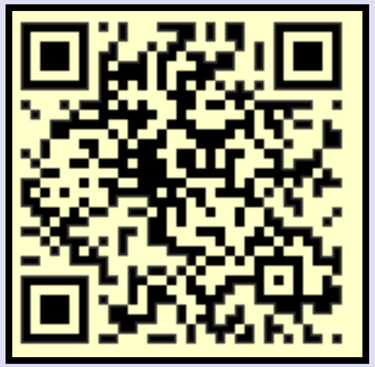
BLOCKCHAIN TUTORIAL 18

Create Bitcoin address with 16-sided dices





CREATE BITCOIN ADDRESS WITH 16-SIDED DICES

- A 16-sided dice has values 1 till 16.
  You always need to subtract 1 to get the hexadecimal representation.

- 4 bits has in total 16 combinations.

Binary	Decimal	Hex	Binary	Decimal	Hex
0000	0	0	1000	8	8
0001	1	1	1001	9	9
0010	2	2	1010	10	a
0011	3	3	1011	11	b
0100	4	4	1100	12	c
0101	5	5	1101	13	d
0110	6	6	1110	14	e
0111	7	7	1111	15	f

CREATE BITCOIN ADDRESS WITH 16-SIDED DICES

- Which means, the value of one 16-sided dice represents 4 bits.
- If you throw a 16-sided dice twice, the two dice values represents 1 byte.

1 - 1 = 0

0

14 - 1 = 13

D

← hexadecimal representation

← binary representation

CREATE BITCOIN ADDRESS WITH 16-SIDED DICES

- To create a 32 bytes random number you need to throw one 16-sided dice 32 * 2 = 64 times.
- If you have four 16-sided dices you only need to throw these 4 dices, 64 / 4 =16 times to get a 32 bytes random number.
- If you use more than one 16-sided dice, use different colour dices.
- Use each colour in a particular order when creating the random number.

CREATE BITCOIN ADDRESS WITH 16-SIDED DICES

- A 32 bytes random number has in total $2^{(32*8)} = 2^{256}$ combinations
- 2^{256} = 115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,936007,913,129,639,936
- This value has 78 digits and is approximately 10^{77}
- The number of atoms in the entire observable universe is estimated to be within the range of 10^{78} to 10^{82}
- Because of the above mentioned, when a Bitcoin client creates a Bitcoin address it never checks if this address already exists because it is improbable that it will happen (but it is not impossible!)