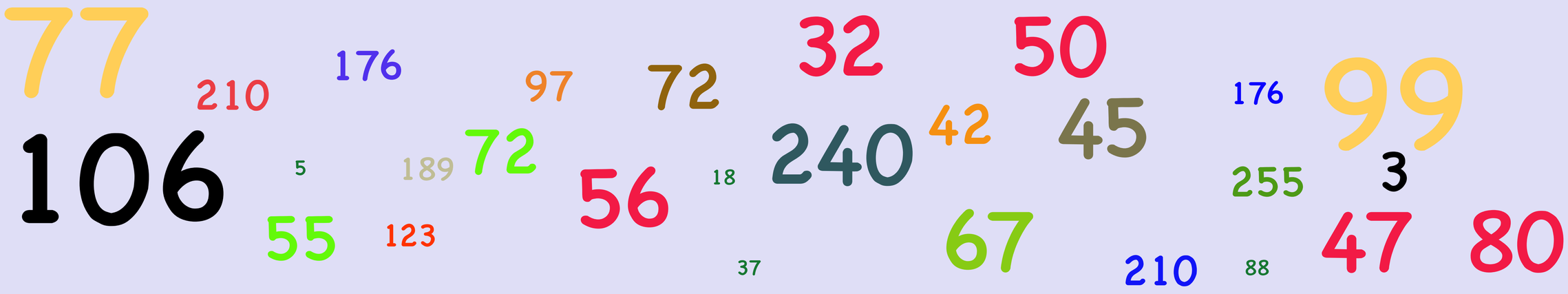
BLOCKCHAIN TUTORIAL 2

Random numbers



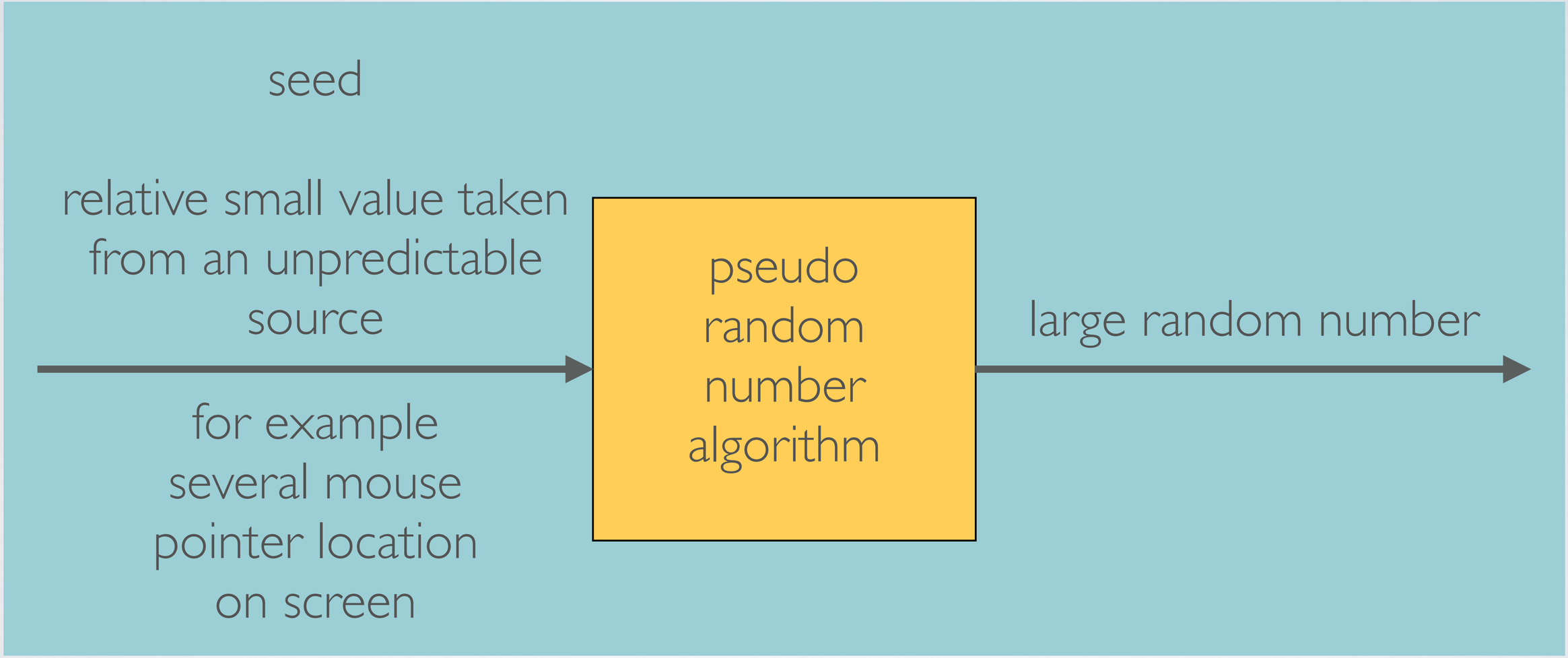
BLOCKCHAIN TUTORIAL 2

Random numbers

RANDOM NUMBERS

- Random numbers are numbers which are randomly generated, like throwing a dice or flipping a coin
- However a computer can not generate true random numbers it creates so called pseudo random numbers using a **P**seudo **R**andom **N**umber **G**enerator (PNRG)
- A PNRG uses a "seed" as input and a mathematical function which generates a random number
- The seed is a relative small number and the generated random number is usually a large number
- In the Blockchain world random numbers are for example used to generate public and private keys

PSEUDO RANDOM NUMBER GENERATOR



MIDDLE SQUARES ALGORITHM

- Start with seed = 135 and multiply the seed by itself
- Result: 135 x 135 = 1**822**5 => Random number: **822**
- Multiply the result by itself
- Result: 18225 x 18225 = 332**150**625 => Random number: **822 150**
- Multiply the result by itself
- Result: 332150625 x 332150625 = 110324**376**87890625 => Random number: **822 150 376**
- Repeat steps until generated random number has your desired number of digits