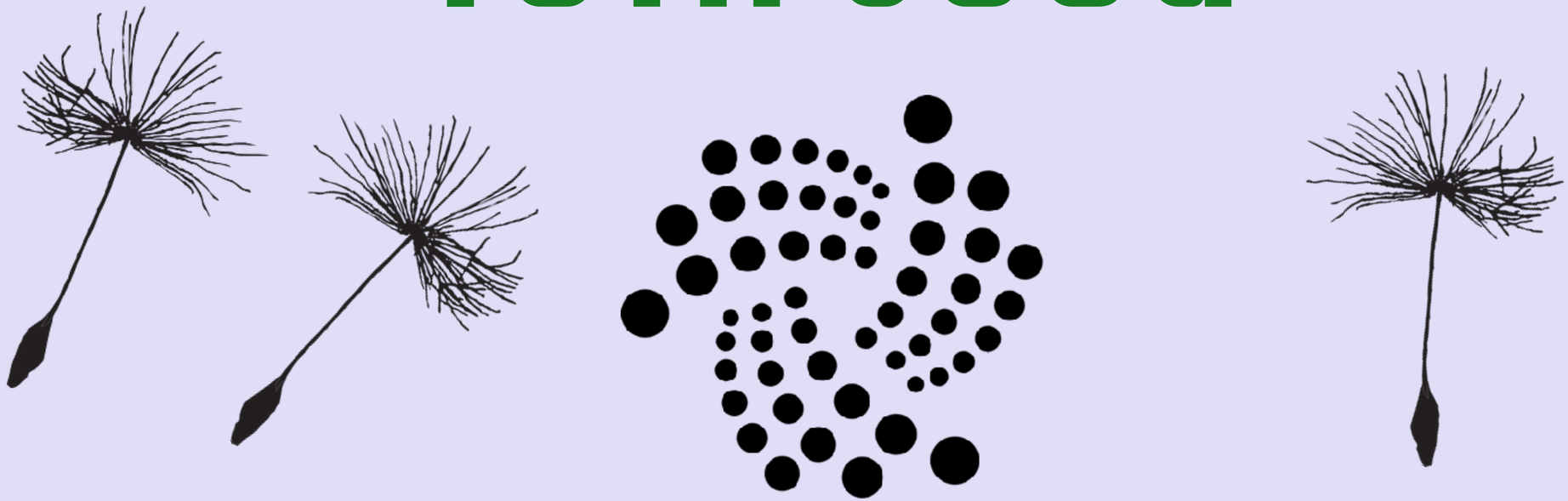
IOTA TUTORIAL 3

IOTA Seed



C9RQFODNSAEOZVZKEYNVZDHYUJSA9QQRCUJVBJD9
KHAKPTAKZSNNKLJHEFFVK9AWVDAUJRYYKHGWQIAWT

WHAT IS AN IOTA SEED

- An IOTA seed is 81 characters long and only consists of the latin alphabet characters and the number 9: ABCDEFGHIJKLMNOPQRSTUVWXYZ9
- The characters A-Z are all upper case.
- With the seed the IOTA wallet can generate corresponding addresses.
- Each specific seed generate addresses belonging to the seed.
- An IOTA seed looks like:
  C9RQFODNSAEOZVZKEYNVZDHYUJSA9QQRCUJVBJD9KHAKPTAKZSNNKLJHE
  FFVK9AWVDAUJRYYKHGWQIAWT

GENERATE IOTA SEED USING TERMINAL

- According to the official IOTA knowledge base:
  https://kb.helloiota.com/KnowledgebaseArticle50005.aspx
  you can use the following methods to generate IOTA seeds:

- Linux Operating System:
  Open a terminal and enter the following command:
  ```
  cat /dev/urandom |tr -dc A-Z9|head -c${1:-81}
  ```

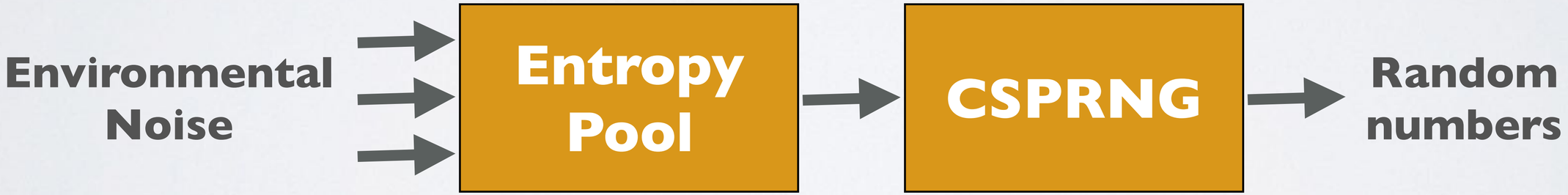
- Mac Operating System:
  Open a terminal and enter the following command:
  ```
  cat /dev/urandom |LC_ALL=C tr -dc 'A-Z9' | fold -w 81 |
  head -n 1
  ```

WHAT IS /DEV/URANDOM

- The function /dev/urandom creates cryptographically random numbers by gathering random data for example environmental noise (entropy) from device drivers, network packet timings and other sources into an entropy pool.

- The data from the entropy pool is used as input for the **C**ryptographically **S**ecure **P**seudo**R**andom **N**umber **G**enerator (CSPRNG)

- This generator will generate the random numbers.



WHAT IS /DEV/URANDOM

- urandom means unlimited random

- On the Mac there is no difference between /dev/**random** and /dev/**urandom**, both behave identically.

- On Linux systems there are differences between /dev/random and /dev/urandom. In this presentation these differences will not be discussed.

GENERATE IOTA SEED USING BROWSER

- Another solution the IOTA knowledge base recommends to generate an IOTA seed is using this web application:
  https://ipfs.io/ipfs/QmdqTgEdyKVQAVnfT5iV4ULzTbkV4hhkDkMqGBuot8egfA

- The source code for this seed generator can be found at:
  https://github.com/knarz/seedgen

- The knarz/seedgen uses the Stanford Javascript Crypto Library. This library can be found at: https://github.com/bitwiseshiftleft/sjcl

- More information about this library can be found at:
  http://bitwiseshiftleft.github.io/sjcl/
  http://bitwiseshiftleft.github.io/sjcl/doc

STANFORD JAVASCRIPT CRYPTO LIBRARY

- The **S**tanford **J**avascript **C**rypto **L**ibrary (SJCL) is a project by the Stanford Computer Security Lab to build a secure, powerful, fast, small, easy-to-use, cross-browser library for cryptography in Javascript.

- The SJCL library is used in many web applications.

GENERATE IOTA SEED USING BROWSER

- If you want to use the web application to generate an IOTA seed do the following:
- Goto https://ipfs.io/ipfs/QmdqTgEdyKVQAVnfT5iV4ULzTbkV4hhkDkMqGBuot8egfA and save the webpage locally on your computer.
- Disconnect your computer from the Internet (disable WiFi, or remove your Ethernet cable)
- Open the webpage and move your mouse until its reaches 100%
- Store your IOTA seed in a secure location.

YOU SHOULD…

- **NEVER** create an IOTA seed by entering 81 characters (A-Z9) yourself on a keyboard.

- **NEVER** create an IOTA seed using an web application while you are online.

- **NEVER** use unknown IOTA seed generators. Use the seed generators recommended by the official IOTA knowledge base:
  https://kb.helloiota.com/KnowledgebaseArticle50005.aspx
  There are several online IOTA seed generators which do not generate Cryptographically Secure Random Numbers which means there is big chance someone else can generate the same seed as you have.