IOTA Deep Dive

Jan-Erik Sandberg
GM Q-FREE MALTA

www.blockchainrebels.com

IOTA Denominations

i - iota	ki – kiloiota	Mi - Megaiota
Gi - Gigaiota	Ti - Terraiota	Pi - Petaiota

Hashing

Length of output always the same

Digital fingerprint

One-way

Hashing

```
{Output          Ten(input    )}
```

```
input=5 gives output=10
input=4 gives output=10
input=3 gives output=10
input=9 gives output=20
```

Hashing in IOTA

KECCAK-384

Sponge construction

CURL

Trinary

-1,0,1

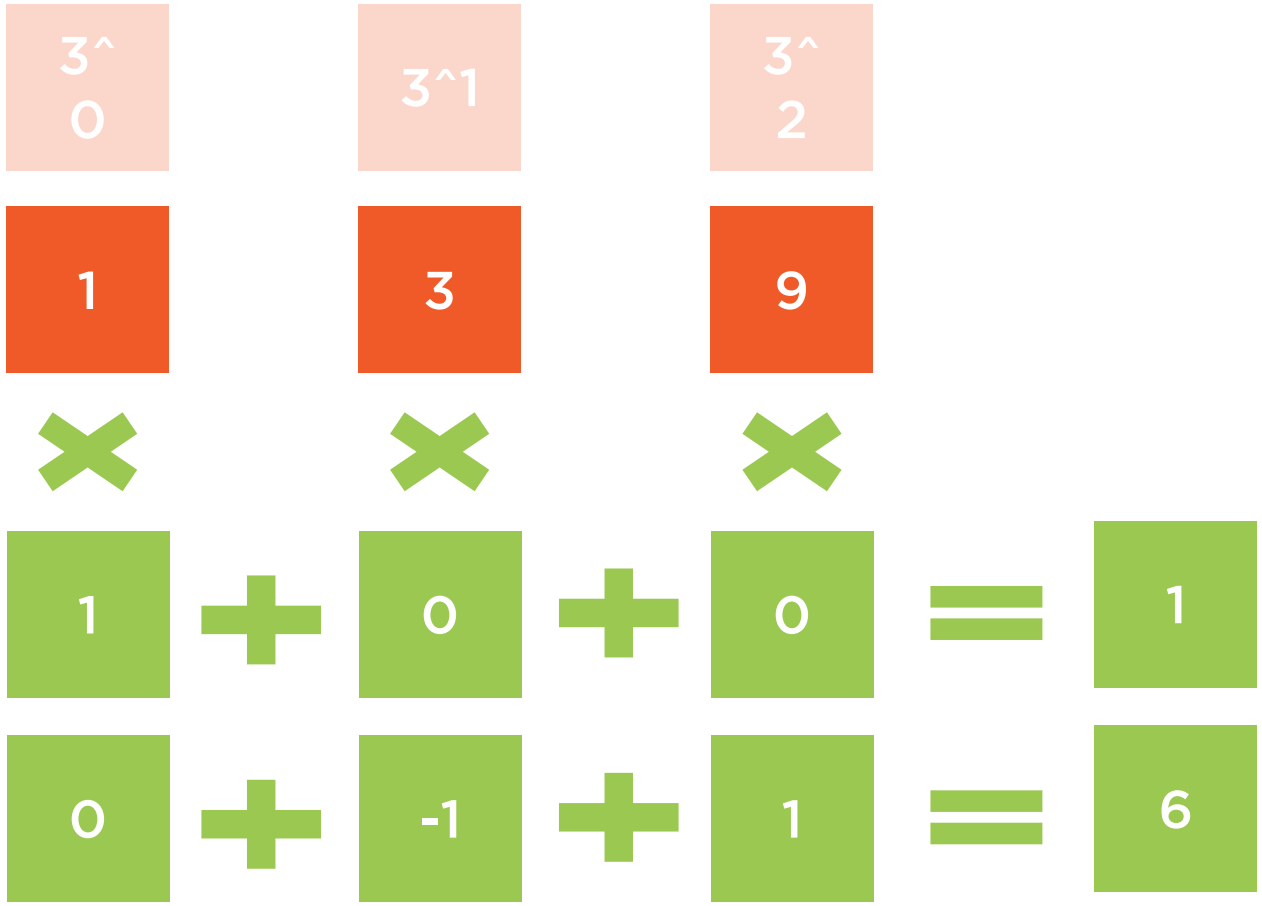
Trits and Trytes

Efficient for new processors

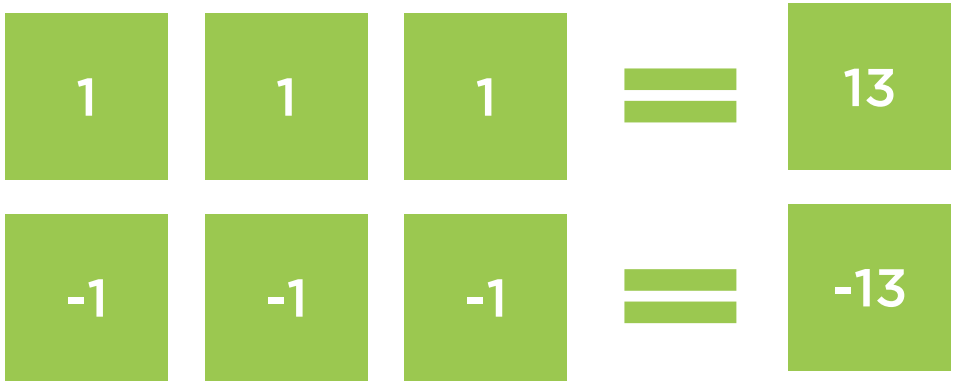
Balanced vs. unbalanced

A-Z and 9

Tryte Example



Tryte Example



Two Trytes

The IOTA Tryte Alphabet

Human readable

26 letters and the number 9

27 different combinations= 1 tryte

0,0,0 = 9
1,0,0 = A
-1,1,0 = B

Seed

Combined username and password

81 Trytes

8.7x10^115 Combinations

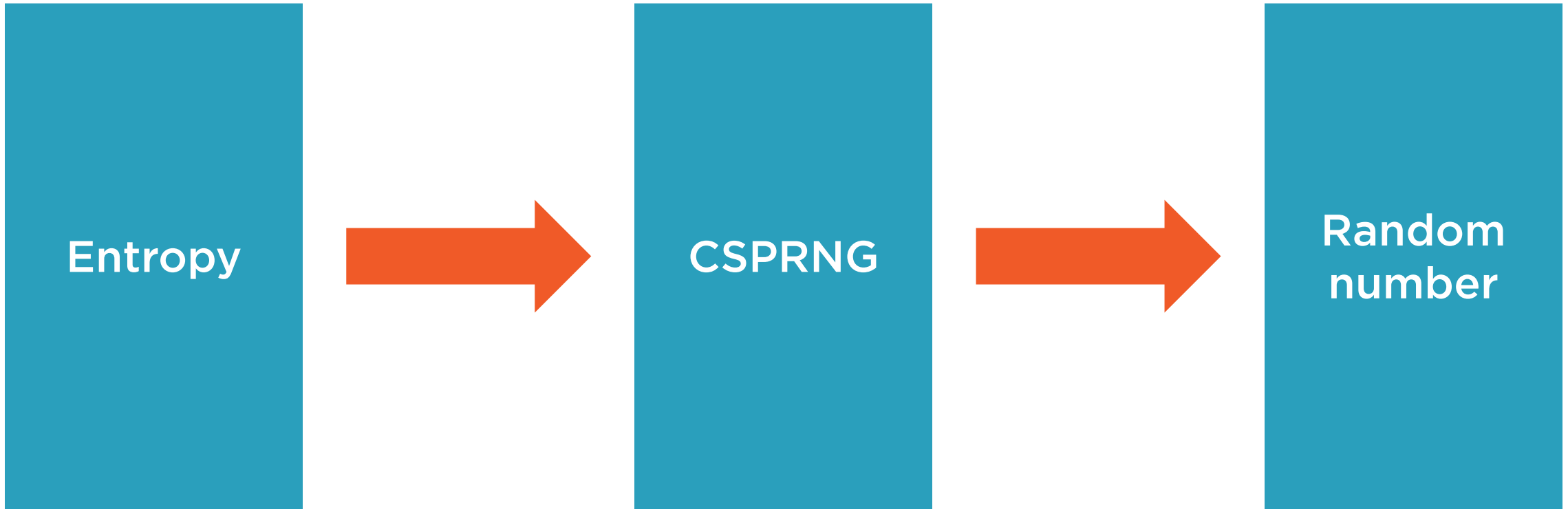
Generating addresses

Generating Seeds

Script-based generation

Online generators

Randomizers



Seed Generation “Do Not”

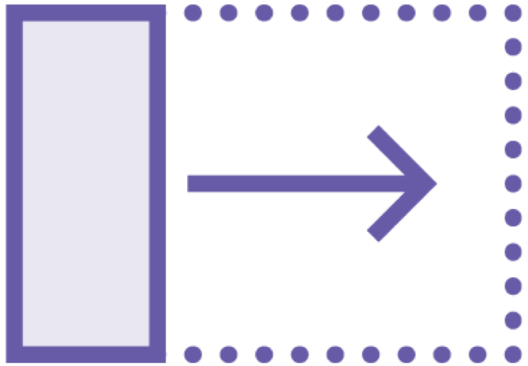
Keyboard

Unknown

Demo

Making a seed

IOTA Addresses



Receive many, send once

Public key

Quantum resistant

Generating Addresses

Address Examples

Seed:

WPLXWGFOJHFKTFTEQGQAYQBFHTDJADNNTISLXONXTOULCLTPFM
NMGJCZNYCUAJPOEDTCNU99WDNWGNJHV

Address, index 0, security level 1:

EYLVEDYDEUTAAZVKWVMXUXRNOTOBIPEUTHYJH9X9PPKTYBWUCB
NMFBJJJQW9OJRNSAHCCATVM9BPDR9ADZBYTTIQZZ

Address, index 0, security level 2:

LQ9XXXPLSKHCSH9W9PFTTJOLJOILMKSVOIUAJGBGOEZBL9CQFLQ
XENMYVDLQYATYUJLLKDPDWUPWBYGGDS9XPTYUXD

Same Seed, Different Index

0 - LQ9XXXPLSKHCSH9W9PFTTJOLJOILMKSVOIUAJGBGOEZBL9CQFLQXENMYVDLQYATYUJLLKDPDWUPWBYGGDS9XPTYUXD
1 - XCWFACTCNOJQCPHCHXWLBVT9ZSUVBNYXERXDDJJODHEACTRLWPKOHEAXPDLWZGWLEAMOR9KPOBUUMEVUDYAQNIPCJW
2 - TYUAPJTFMMFHPLZHMTSGQKNOHH9OAYGDXIMMTGJSHYVBULFT9XEGR9RGZENMBCMTJJNUUAWXMRJSRYBEYAMFGZFPXC
3 - KX9HOQ9JSHTZDPIOUFEWXFYQF9IECHGAWHPVOHYJFMIKJWCCBMMQEGNVKWQCSTQSRQOQBVIXUGIVSTUBCHXCMSA9FY
4 - EULMXXNMJYWEKANFRDSFGUMXKQETIXIBDVQIOIEDPPGWIIPSLCUZDXMJJCMHQUEORDHVOUACCBLKRCGFXIWABREADW
5 - MQPZUBLWTTYURCNUUHHPOBYP9OZMSMCWJEEXASEYRZUWJEMECOHRPA9LULN9VSORUXHITEXUFFIMRTXKWNYFA99CPC
6 - ZAIZYDETIZ9VQGAWOBJHEEEVQSYNCTOQTIFOQEYUFWWNRRCYPZ9JAFOOJUHVSAUSGBXPAVJQDUMPSVRIWKCRCQISFA
7 - WRI9PHFXNOSKKBZXSVXQHRDPHOSOYRJFMVPOOXQCUZGEZKZRPNQMVMHIFQOBZZJWENUXHXXUPMDVQXUFAWEXDV9DFA
8 - UAQQLNZDHECTWGOEACPCHVBPLJFSNKFCDEAQCWWANIHBLMATVQ9CVGAJFIJEQGBM9IDKIOIWGB9RZ9IIYOAFDPRCA9
9 - 9PWKXIGD9LDICYXJMTYEQMJLJMCJGHHWPYPQHRAFRDVBFAP9BZKDCSHZZDGDWVOFRAHYMUQ9WMAWVTWFDFNHCFTKXB

Reuse of Addresses

Share 50% of private key

1/2^256 to 1/2^128

1/2^128 to 1/2^64

1/2^64 to 1/2^32

Transaction Bundle

Transaction info

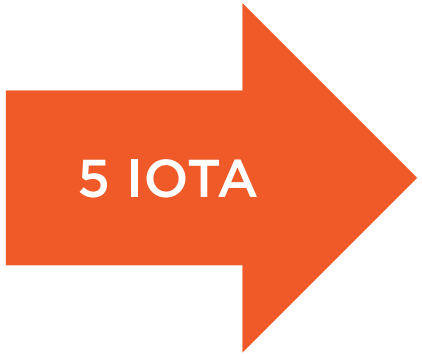
Bundle reference

Index

Sending the Full Value

Victoria's Wallet

Address 0: 5 IOTA



Oliver's Wallet

Address 0: 0 IOTA

Sending the Full Value

Victoria's Wallet

Address 0: 0 IOTA

Victoria's
Address 0: -5

Oliver's
Address 0: 5

Oliver's Wallet

Address 0: 5 IOTA

Sending the Full Amount

Victoria's Wallet

Address 0: 10 IOTA

Oliver's Wallet

Address 0: 5 IOTA

Change Addresses

Victoria's Wallet

Address 0: 10 IOTA

Victoria's Address 0: -10
Address 1: 5

Oliver's Address 0: 5

Oliver's Wallet

Address 0: 0 IOTA

Change Addresses

Victoria's Wallet

Address 0: 0 IOTA
Address 1: 5 IOTA

Oliver's Wallet

Address 0: 5 IOTA

Spending from Multiple Addresses

Victoria's Wallet

Address 0: 3 IOTA
Address 1: 3 IOTA

Victoria's
Address 0: -3
Address 1: -3
Address 2: 1

Oliver's
Address 0: 5

Oliver's Wallet

Address 0: 0 IOTA

Spending from Multiple Addresses

Victoria's Wallet

Address 0: 0 IOTA
Address 1: 0 IOTA
Address 2: 1 IOTA

Oliver's Wallet

Address 0: 5 IOTA

Attaching an Address to Tangle

Verify

Security

Snapshots

Announced

Clean up

Evolve

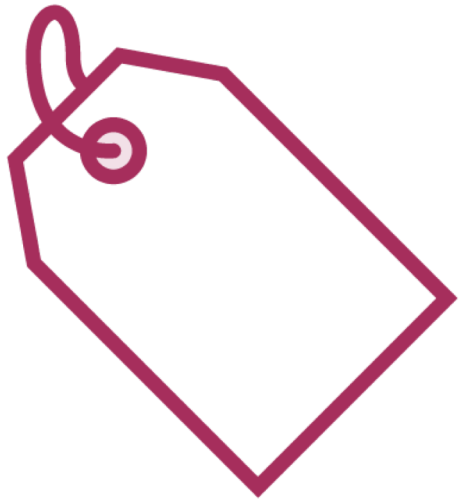
Transition

Permanodes

Validating Transactions

Random Walk Monte Carlo (RWMC)	Select random new transactions	Reference
Less than 50%	More than 50%	99% considered validated

Tag and Message



Tag

Message

Summary

- Denominations and hashing
- Trinary
- Seeds and addresses
- Bundles
- Verifications
- Message and tag