SeedQuest

A 3-D Game Mnemonic for Key Recovery

SeedQuest

encode and decode your private key

CONSENSYS

IIW 2019 Fall
https://github.com/reputage/seedQuest
Samuel M. Smith Ph.D. sam.smith@consensys.net

Human-Friendly Mnemonic

Memorize random seed by memorizing a sequence of game actions

Maximize compatibility with human memory

Geo-Temporal-Spacial

Rich Sensory Experience

Episodic vs Semantic Memory

Hunter Gatherer Tasks

First High Tech Mnemonic

SeedQuest
encode and decode your private key

References

https://en.wikipedia.org/wiki/Elaborative_encoding

https://www.academia.edu/4503195/Adaptive_memory_Fitness-relevance_and_the_hunter-gatherer_mind

Spatial Mnemonic Encoding: Theta Power Decreases and Medial Temporal Lobe BOLD Increases Co-Occur during the Usage of the Method of Loci

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5223054/

Although less relevant storytelling is a well developed human mnemonic. But seems to benefit from elaborative encoding.

https://www.nature.com/articles/s41467-017-02036-8

GeoTemporalSpatial uses episodic memory in contrast to semantic memory which are strings or words or images

https://en.wikipedia.org/wiki/Episodic_memory

https://www.sciencedirect.com/science/article/pii/B9780080450469007609

http://wheelerlab.gatech.edu/wp-content/uploads/2018/04/Wheeler_EncyNeuro_2007.pdf

Cryptographic-Strength Mnemonic

128 bits = twelve word BIP-39 seed phrase

128 bit seed may be converted to/from twelve word BIP-39 seed phrase

Seed may be used to generate blockchain private key

ECDSA (*Ethereum, Bitcoin, Dash, Ripple, …*)

EDDSA (*Monero, NEM, R3, Stellar, …*)

Seed may be used to symmetrically encrypt a set of blockchain private keys

SeedQuest

Entropy

16 sites choices per scene = 4 bits per site choice

4 action choices per site choice = 2 bits per action choice

3 site-actions in sequence per scene = 3 * (4+2) = 18 bits per scene-site-action sequence

16 scene choices = 4 bits per scene choice = 4 + 18 = 22 bits per scene choice

6 scenes in sequence per play = 6 * 22 = 132 bits per play

Throw away 4 bits to get 128 bits per play

052A117257D1DA55C8E23E1B5EA5CB50A

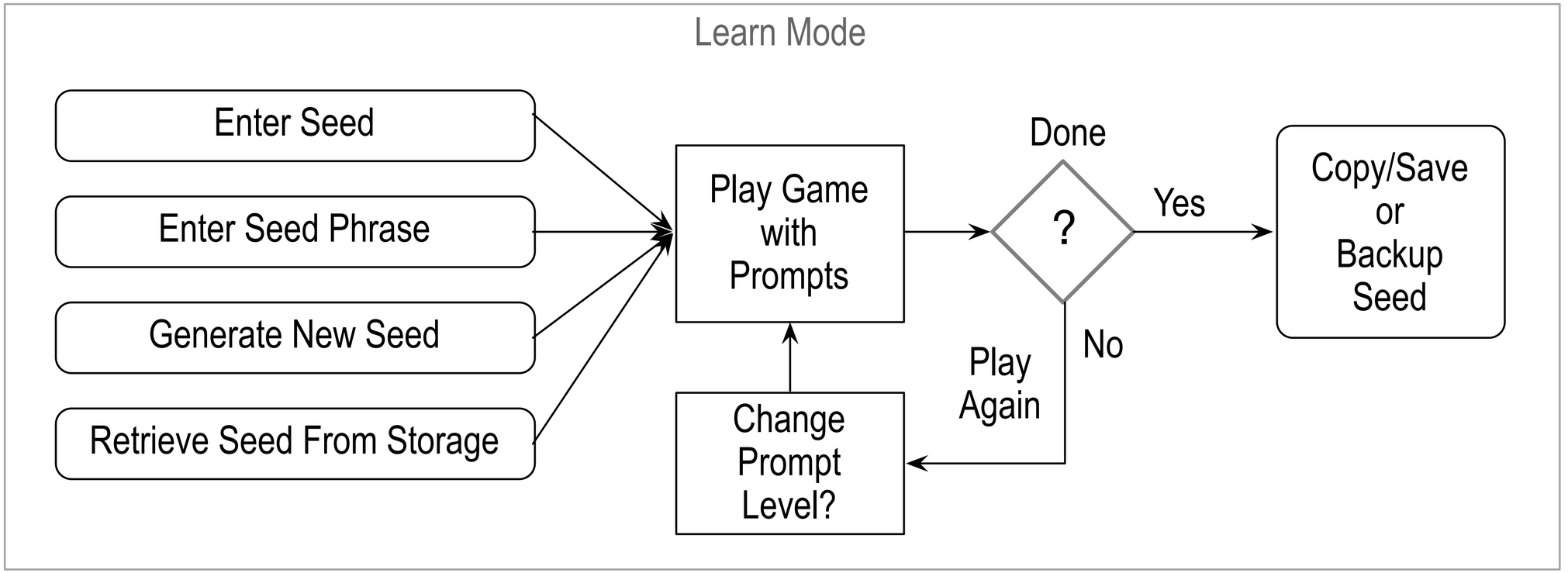
052A117257D1DA55C8E23E1B5EA5CB50A

Learn Mode

SeedQuest

Learn seed in only a few minutes by playing game with prompts

easy + fun = attractive mnemonic

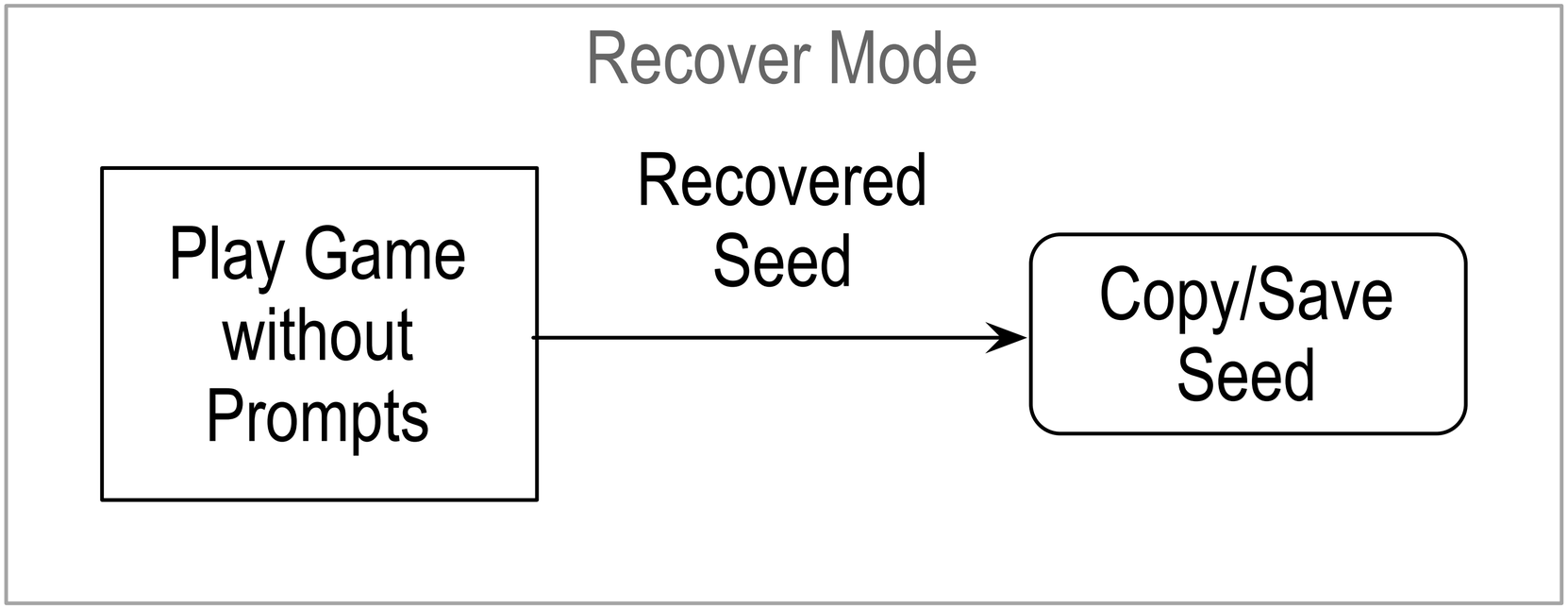


Game play action sequence determined by seed

Recover Mode

Recover seed by playing game without prompts

Memory refreshed every play (recover or practice)



Platforms

Unity3D Game Engine (C-#)

All Platforms supported (standalone or plugin)

iOS, Android, Web, macOS, Windows, Linux, VirtualReality

Enhances or extends existing seed generation, backup, and recovery methods

Integrations

SeedQuest

Mobile – Multiple use wallet app

- Seed stored on mobile device
- Learn mode to backup seed in human memory.
- Recover mode to restore seed when device replaced

Web – One-time use wallet

- Seed not stored
- Learn mode to backup seed in human memory
- Recover mode to restore seed for each wallet use

Web/Desktop – Multiple use wallet

- Seed stored in browser data-store or file system storage
- Learn mode to backup seed in human memory.
- Recover mode to restore seed when computer replaced

Repo

SeedQuest

https://github.com/reputage/seedQuest