International Journal of Serious Games

ISSN: 2384-8766
https://journal.seriousgamessociety.org/

Article

MnemonicMaker: A Serious Game for Reconstructing Bitcoin Wallet Mnemonic Phrases

George Vlahavas[1], Christos Karakasis[1] and Athena Vakali[1]

[1]*School of Informatics, Faculty of Sciences, Aristotle University of Thessaloniki, Thessaloniki, Greece*
gvlahavas@csd.auth.gr, karakasisx@gmail.com, avakali@csd.auth.gr

Corresponding author: George Vlahavas (gvlahavas@csd.auth.gr)

Keywords:

Bitcoin
Mnemonic Phrase
Method of Loci
Memory palace
BIP 39
User study

Received: November 2024
Accepted: April 2025
Published: May 2025
DOI: 10.17083/ijsg.v12i2.911

Abstract

Mnemonic recovery phrases are crucial for securing cryptocurrency assets, yet their memorization presents significant challenges for users. Traditional approaches to storing these phrases often compromise between security and ease of use. This paper presents MnemonicMaker, a serious game that leverages the Method of Loci (memory palace technique) through interactive gameplay to enhance the memorization and retention of BIP 39 recovery phrases. We conducted a two-month user study with 38 participants to evaluate the effectiveness of MnemonicMaker compared to traditional memorization methods. Results show that participants using MnemonicMaker maintained high recovery success rates after 60 days, significantly outperforming the control group. Most users required only a few practice attempts to memorize their routes, indicating a manageable learning curve. The study demonstrates that gamified spatial mnemonic techniques can effectively address the challenge of recovery phrase retention while maintaining high user engagement. These findings suggest promising applications for game-based approaches in cryptocurrency security and broader contexts requiring secure information retention.

1. Introduction

Bitcoin, introduced in 2008 [1], revolutionized digital finance by enabling peer-to-peer transactions without intermediaries. In Bitcoin, private keys play a crucial role in securing and managing transactions. The private key, a 256-bit number, is used to create digital signatures, which verify the ownership of bitcoins and authorize transactions [2].

Each Bitcoin address has a corresponding private key, which is used to spend or transfer bitcoins from that address. Private keys are used to unlock and access the bitcoins associated with a particular address, allowing users to make transactions [3]. The security of private keys is essential, as anyone with access to a private key can spend the associated bitcoins [4]. Losing a private key can result in the loss of access to the associated bitcoins, making them effectively unusable. Private keys should be kept secret and secure, as sharing or exposing them can compromise the security of

the associated bitcoins [5][6]. Overall, private keys are a critical component of the Bitcoin network, and their security and management are essential for maintaining the integrity and security of Bitcoin transactions [7].

Several methods exist for storing private keys. Users can keep them in software wallets (hot storage), hardware wallets (cold storage), or paper wallets. Each method presents trade-offs between security and convenience [8]. Software wallets are convenient but vulnerable to malware. Hardware wallets offer better security but can be lost or damaged. Paper wallets risk physical deterioration, theft, or loss [9].

To address some of these challenges, BIP 39 introduced a standardized method for generating deterministic wallets using mnemonic phrases [10]. BIP 39 converts the random entropy used to generate private keys into a sequence of 12 or 24 words chosen from a predefined list of 2048 words. This human-readable format makes backup and recovery more practical compared to managing raw private keys. An example of such a mnemonic phrase is “must marble prize dumb ask mixed hurry pudding ozone wood useful cash”. This is easier to store and remember than the private key, a 256-bit number, and the private key can be derived from the mnemonic phrase.

However, securely storing mnemonic phrases presents its own challenges. Writing them down creates physical security risks, while digital storage is vulnerable to cyber threats. In certain scenarios, memorizing the mnemonic phrase becomes advantageous: when crossing borders where physical backups might be confiscated [11], in regions where cryptocurrency ownership might be scrutinized, or in situations requiring plausible deniability [12].

There have been only a limited number of attempts to make committing of BIP 39 mnemonic phrases to memory easier. Border Wallets [13] is a promising technique that substitutes memorizing of the mnemonic phrase with remembering a specific pattern on a grid of words. This is based on the picture superiority effect [14], which is a phenomenon in which pictures and images are more likely to be remembered than words. Another attempt at making BIP 39 mnemonic phrases easier to remember is Formosa [15], which attempts to replace remembering the seemingly disconnected words in BIP 39 phrases with meaningful phrases with a certain theme. Unfortunately, no user studies have been performed for the effective evaluation of either of these solutions.

The Method of Loci, also known as the memory palace technique, is a mnemonic device dating back to ancient Greece [16]. At its foundation, the Method of Loci combines three fundamental cognitive processes: spatial organization, visual encoding, and sequential navigation. The technique capitalizes on the human brain's capacity for spatial memory by anchoring information to specific locations within a familiar environment [17]. These items are transformed into vivid, memorable images and recalled by mentally traversing the space in a predetermined sequence [18].

The technique's effectiveness has been well-documented across various domains. Research shows improved retention rates compared to conventional memorization methods, with studies demonstrating robust recall even weeks or months after initial learning. The method is proven to be effective because it engages multiple memory systems simultaneously, creating redundant pathways for information retrieval [19].

The implementation of the Method of Loci begins with selecting a familiar location, such as one's home, daily commute route, or workplace. This environment serves as the foundation of the memory palace, providing a stable framework for information storage. The chosen location should offer distinct, ordered spaces that can be reliably navigated in sequence [23]. Virtual environments have been used multiple times in literature to implement memory palaces with very good results (for example [23]-[25]).

In this paper, we present MnemonicMaker, a serious game that combines the Method of Loci with interactive gameplay to facilitate memorization of BIP39 recovery phrases. The game transforms abstract word sequences into a journey through a virtual world, where players collect objects corresponding to BIP39 words in specific locations. By engaging multiple memory systems - spatial, visual, and sequential elements - MnemonicMaker aims to enhance both initial learning and long-term retention of recovery phrases.

The main contributions of this work include:

- A novel application of the Method of Loci in cryptocurrency security through a serious game implementation
- An empirical evaluation of the system's effectiveness compared to traditional memorization methods

The rest of the paper is organized as follows. Section 2 introduces the MnemonicMaker game, its gameplay modes, and design rationale. Section 3 outlines the methodology and participant details of a longitudinal user study evaluating the game's effectiveness. Section 4 presents the study's results, which are then discussed in Section 5. The paper concludes with a summary of the main findings in the final section.

2. MnemonicMaker

In this section, the MnemonicMaker game is presented, and its various gameplay modes are described. Additionally, the reasoning behind certain design elements of the game is provided.

MnemonicMaker is a serious game that serves as an alternative memorization system for Bitcoin BIP39 passphrases, featuring an open-world, explore-and-collect gameplay style with a top-down RPG (Role Playing Game) aesthetic, based on the Method of Loci memorization technique. The primary objective of MnemonicMaker is to provide an innovative approach to password management, offering users a unique and interactive way to reconstruct their wallet recovery phrase. By harnessing the power of muscle memory and gaming instincts, individuals can effortlessly recall their recovery phrases. This alternative solution complements the traditional use of BIP 39 passphrases, giving users more options for managing their cryptocurrency wallets.

MnemonicMaker is designed to enhance long-term retention of recovery phrases by embedding cognitive science principles directly into an interactive gamified experience. Rather than treating gamification as an external layer of engagement, using reward systms such as points, levels, badges and leaderboards, the game itself is structured around established memory enhancement techniques, particularly the Method of Loci. This technique leverages the brain's natural ability to associate information with spatial environments, facilitating stronger encoding and retrieval processes [16]-[19].

The core game mechanics mirror key cognitive processes involved in memory formation. Instead of passively memorizing words, users actively navigate a virtual space, placing mnemonic phrases within distinct locations. This interactive engagement reinforces spatial-contextual memory, which has been shown to significantly improve recall accuracy [18]. Additionally, the process of mentally reconstructing the path through the memory palace strengthens retrieval practice, a well-documented method for improving long-term retention [20].

Unlike traditional gamification approaches that rely on extrinsic motivators such as points or leaderboards, MnemonicMaker sustains user engagement through meaningful cognitive interactions. The immersive spatial experience provides a self-paced learning structure, allowing users to revisit their memory palaces as needed, reinforcing learning through repetition and active recall. By embedding well-established cognitive science principles—such as the Method of Loci for spatial memory encoding [18], retrieval practice to reinforce active recall [20], spaced repetition to prevent forgetting [21], and encoding specificity to strengthen contextual retrieval [22], MnemonicMaker ensures that engagement is not just about short-term motivation. Instead, it fosters durable, retrievable memory traces, helping users retain and accurately recall their cryptocurrency recovery phrases even after extended periods.

The player, through the game, collects a series of objects that are scattered on the vast game map. The game is designed with the aim to maximize immersion. To accomplish this, all in-game terminology, including location names and item names fit with the fantasy setting of the game. Therefore, objects have names such as “Golden Horn”, “Gem of Justice” and “Mandle of Gluttony” with each one corresponding to one of the 2048 words of the BIP 39 specification. The player

moves through the map, collecting these objects and adds them to their inventory. The position of each object in the inventory also corresponds to the position of the respective word in the BIP 39 recovery phrase. Once the player has collected all twelve items and their inventory is full, the corresponding BIP 39 recovery phrase is revealed to them.

At the start of the game, the player is presented with a game mode selection screen (Figure 1) and is requested to select a "blessing". These include:

- **"The Virtue of Freedom" (VoF – Normal Mode):** This mode is intended for users who want to play the game solely to retrieve their previously known personal recovery phrase. The player should only select this game mode if they have played the game previously and are aware of exactly which in-game items to collect.
- **"The Virtue of Knowledge" (VoK – Practice Mode):** In this mode, the user can spend as much time as needed to become accustomed to the world and learn about their personal route for collecting items specifically picked to reconstruct their recovery phrase. In this game mode, the user should already have a recovery phrase, produced by other means (e.g., online generator, Bitcoin wallet, etc.), that they would like to memorize. The user will then be assisted by the Pathfinder tool, which will pinpoint the locations of all the necessary items and suggest a path for the user to memorize.
- **"The Virtue of Adventure" (VoA – Demo Mode):** In this mode, the user will interact with the game in a similar way to the practice mode, with the key difference being that here, users do not input a recovery phrase they already have. Instead, the game will generate a new, random phrase for them, using the BIP 39 generation algorithm and assist them in memorizing the locations of the respective items as well as the path to reach them.

An overview of the game play process for all game modes is shown in Figure 2. The player is expected to select either the VoK or the VoA mode the first time they play the game. In the case of the VoK mode, the player is presented with a screen to input their recovery phrase (Figure 3). A word filtering mechanism is provided to the player so that word input is easier. In the case of the VoA mode, a recovery phrase for a new Bitcoin private key is randomly created and presented to the player.

Having a recovery phrase, the player's objective is to collect the respective objects and place them in their inventory in the correct order. The player is free to collect the objects in any order they wish, and it is possible to rearrange objects in the inventory. The pathfinding tool (Figure 4) is used in both VoK and VoA modes to guide the player in locating the next object until their inventory is filled. Anytime the player clicks on an object in the pathfinding tool, stylized arrows are shown at the screen edges to indicate where the user should move to, in order to reach that object. The player can also choose to view a zoomed-out view of the world map, where the position of the object on the map is shown relative to the player's position (Figure 5). The player can choose their own strategy for obtaining all objects. For example, some players might choose to first collect objects located in closer proximity on the map, while others might choose to collect objects as they are listed from top to bottom in the pathfinding tool. The goal of both VoK and VoA modes is for the player to select a path that will lead them through all object positions, and through repetition, memorize that path.

Objects in the inventory are shown as coins with the Bitcoin logo. These come in two colors, dark blue and golden. The two colors serve no purpose other than providing a way to differentiate between different objects that may appear in the same location (Figure 6). Objects are located individually on the map, or inside pouches and chests, where more than one object may be found.

The game also features a mechanism for switching between day and night. Different objects are scattered in the daytime and nighttime maps, with the two maps being otherwise identical. This mechanism serves to essentially double the available world map, without the player having to memorize a map that is double the size. When the game starts, the player is shown to a house, which they can use to "rest". By using the bed that is inside the house and "sleep", the player may

switch the time between day and night. The pathfinding tool indicates whether an object is located in the daytime or nighttime map by showing a sun or a crescent moon, respectively (Figure 4).

Once the player has filled their inventory with objects and taking the order of the objects into account, the game reveals the corresponding BIP 39 passphrase (Figure 7).

In the VoF mode, the pathfinding tool is not available. The player has complete freedom to collect any objects in any order they prefer. In all other respects, including the map and object placement, this mode is identical to the VoK and VoA modes.

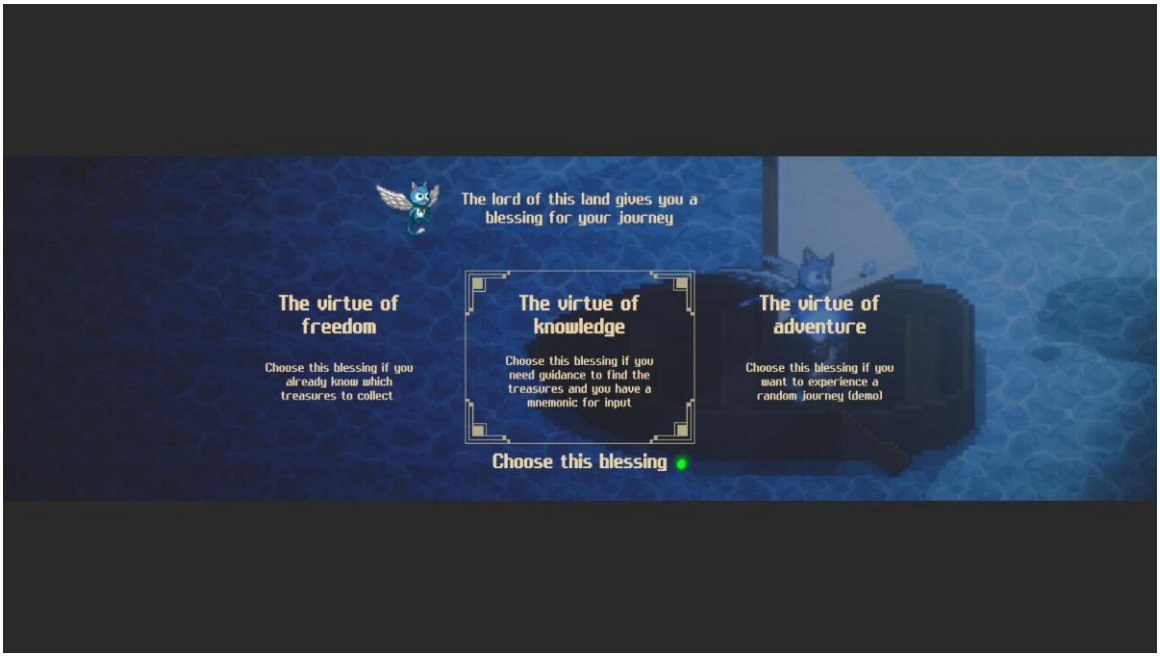


Figure 1. Choosing a game mode (“blessing”) at the start of the game.

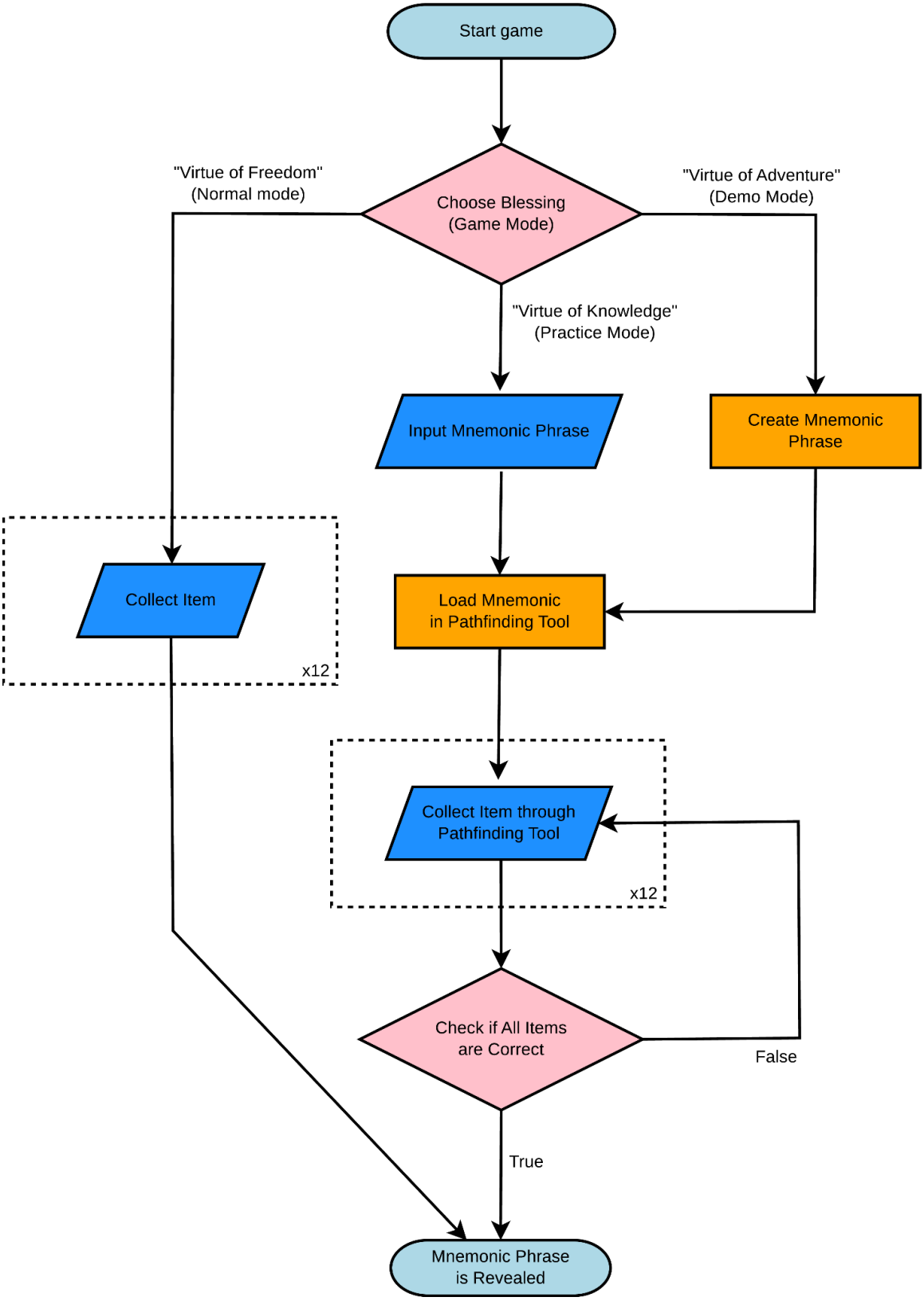


Figure 2. MnemonicMaker game flow diagram.

Figure 3. Inputting a recovery phrase when starting the game in the “Virtue of Knowledge” mode.

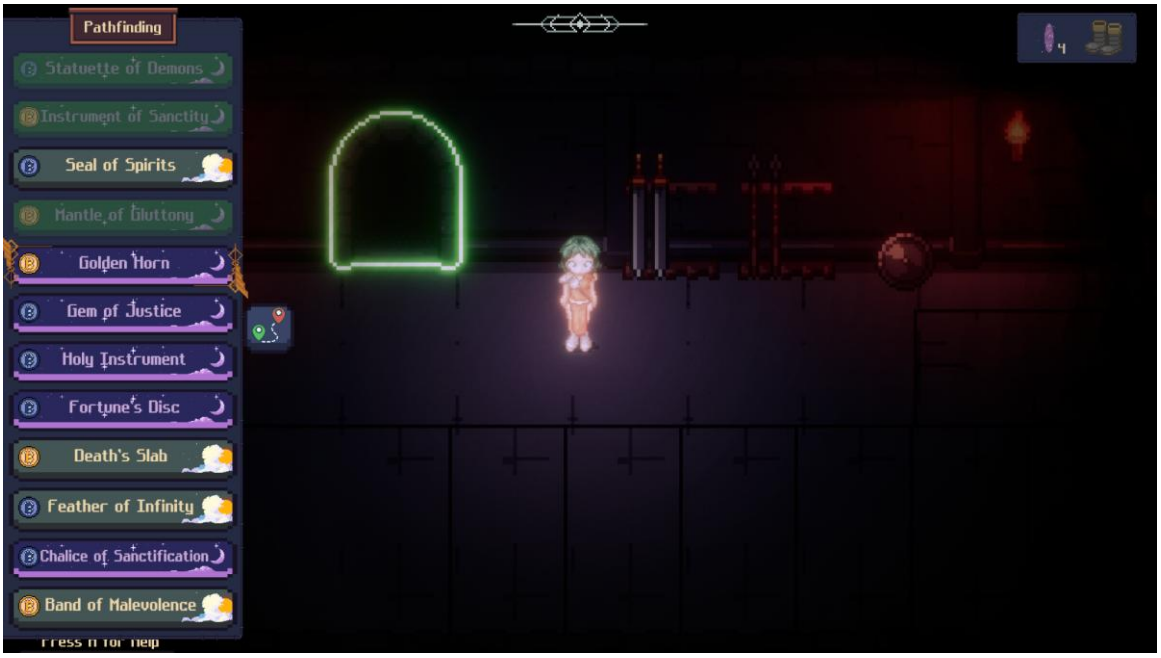


Figure 4. The pathfinding tool at the left side of the screen, featuring already obtained objects (greyed out), objects to be obtained (highlighted) and the next object that is selected to be obtained (decorated). A highlighted exit, where the user should move to, is also shown.

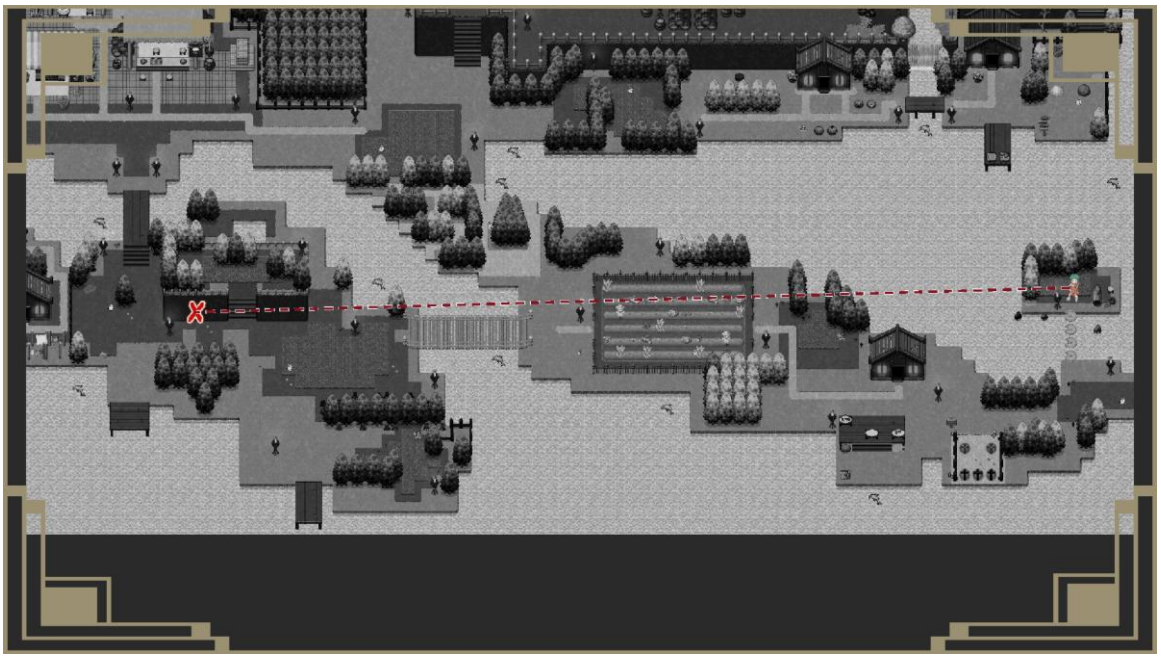


Figure 5. Partial view of the world map showing where the next object is located relative to the player's position.

Figure 6. The game inventory, showing an object that is placed in the correct position at the first slot and an object that is placed in an incorrect position at the sixth slot.

Figure 7. The revealed mnemonic phrase after the player has gathered all items and has placed them in their correct positions inside the inventory.

The world map consists of four different map layers. When the player arrives at the landing dock, where the game starts, they are positioned on the top-level layer, called the "Overworld". This is the largest area that the player has to discover. The Overworld includes entrances that lead to all other map layers (Figure 8). The first of these is the "Housing" layer, which contains a total of ten houses within the Overworld. Another layer is the "Tomb" layer, with eight tomb entrances that lead to an equal number of tomb rooms. Finally, there is the "Dungeon" layer, with four

dungeon entrances scattered around the Overworld. Each of the dungeons includes several dungeon rooms for the player to explore. Objects are located in all layers of the game.

When the player is located on the Overworld and the pathfinding tool leads them to an object that is in one of the other map layers, the entrance to that layer is highlighted (Figure 4). When the player goes through the entrance, the pathfinding tool continues to lead the player to the object within that layer's map. Similarly, when the player is inside one of the other layers, the pathfinding tool will first lead them to that layer's exit and then through the Overworld to the target object.

Additionally, the Overworld layer, although flat, incorporates areas that follow different themes, such as desert-themed areas, islands, fields, and forests. This design choice is intended to make it easier for the player to learn and remember how to navigate through them. An effort has been made to strategically place distinct landmarks and items unrelated to gameplay in several locations throughout the world map, allowing the player to use them as points of reference while exploring and discovering the map.

The Overworld map is very large. Therefore, the player could potentially require a lot of time to move between locations. In order to help the player with that, two tools are provided: a “Portal” tool and a “Boost” tool. Both are located at the top right of the user’s screen (Figure 4). The Portal button allows the player to warp from their current location to in front of the main house, close to the map's center. In VoF mode, the portal button has unlimited charges, meaning the player can use it whenever they wish. However, in VoK or VoA modes, it has a limited number of five charges. This was designed to encourage the user to explore the open world during VoK or VoA modes, thereby familiarizing themselves with the map. The Boost tool is represented by a button showing a pair of boots. This is a toggle button that sets the player's speed to normal or fast. It is recommended that the player should ignore this feature on their initial playthroughs, allowing them to become acquainted with the environment. However, it is available for repeated runs in VoF mode, when the player is likely already familiar with the map.

MnemonicMaker has been created using Unity Engine in C#. The game’s source code is publicly available under the MIT license.[1]

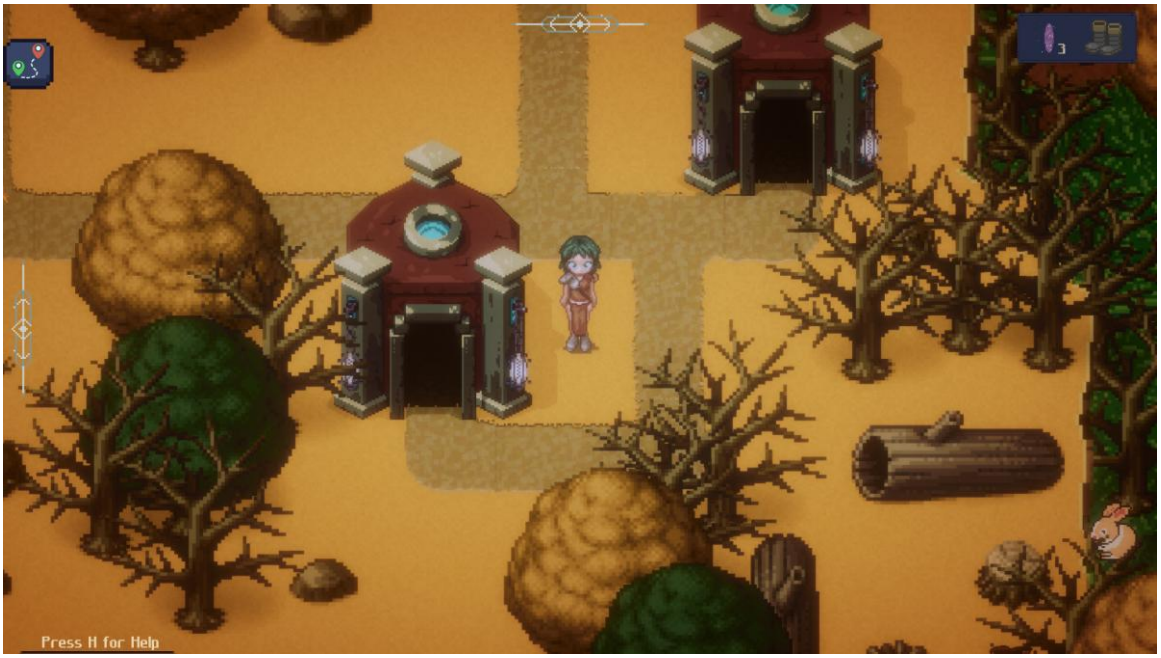


Figure 8. Game screenshot showing the entrance to two different tombs during daytime.

[1] https://github.com/Datalab-AUTH/MnemonicMaker

3. User Study

In this section, we present a longitudinal user study that was conducted to evaluate the effectiveness of MnemonicMaker. The methodology used in the study is described, and details about the participants and their involvement are provided.

The aim of this study is to evaluate the utility of MnemonicMaker in helping users remember the mnemonic phrases that control their Bitcoin wallet keys. The user study was conducted with the informed consent of all participants, who were fully briefed on the study's purpose and procedures before providing their agreement to participate.

All participants were MSc students who had enrolled in a class on "Decentralized Technologies". As such, they were already familiar with Bitcoin keys, passphrases, the BIP 39 specification, and their importance, while they also attended a brief presentation about the game's purpose and features.

In total, 38 individuals participated in the user study, 30 males and 8 females. Each participant was provided with a different random BIP 39 mnemonic phrase consisting of twelve words. Participants were randomly split into two groups: a control group and a test group, each consisting of 19 individuals. The control group consisted of 16 males and 3 females, while the test group included 14 males and 5 females. All participants from both groups completed all experimental sessions without any dropout.

Participants in the control group were instructed to memorize their assigned mnemonic phrases and attempt to retain them in memory. They were asked to destroy any copies of the mnemonic phrase after five days, including hard copies or digital notes on computers, phones, or cloud storage. The objective was for these individuals to practice learning the mnemonic phrase over this period and recall it without external aids thereafter. While participants could use any techniques they deemed appropriate during those initial five days to commit the phrases to memory (such as spaced repetition or flashcards), assistance from other people was explicitly discouraged.

Participants in the test group were asked to destroy any copies of the mnemonic phrase after five days as well. During this period, they used MnemonicMaker, first in VoK mode and then in VoF mode, with no restrictions, at their own time. The goal was to memorize a route that would lead them to all objects necessary to recreate their respective mnemonic phrase. To succeed, participants needed to play the game as many times as they believed were sufficient. They were also discouraged from seeking assistance from others.

All participants were asked to accurately reproduce the mnemonic phrase they were assigned at four intervals: after one week, two weeks, one month, and two months. The control group simply had to write it down, while the test group was asked to play the game and go through the route they had memorized in order to recreate it. For the test group, the completion time in minutes until the participants had gathered all objects and produced the mnemonic phrase was recorded as well. A repeated measures ANOVA was performed to test if completion time changed significantly over time.

The recalled mnemonic phrases were compared against the original ones the participants had been provided with. Whether participants had recalled them successfully was noted. To be considered successful, the recalled phrases had to perfectly match the original ones, with no single-word differences or mistakes in word order, as these would render the phrase useless for accessing hypothetical funds locked to the respective private keys. Each participant's recall success was recorded as either a "success" (1) or "fail" (0) for each time point.

We employed Generalized Estimating Equations (GEE) [26] to analyze the binary outcome data, accounting for the repeated measures within subjects. GEE is suitable for longitudinal data analysis and handles correlated data effectively. The GEE model was specified as follows:

$$logit(P(Y_{it} = 1)) = \beta_0 + \beta_1 Group_i + \beta_2 Time_t + \beta_3 (Group_i \times Time_t)$$

where Y_{it} represents the binary outcome (recall success) for participant i at time point t, $Group_i$ indicates the participant's group (control or test), and $Time_t$ indicates the specific time point (7, 14,

30 and 60 days). The baseline group for the GEE model was defined as the control group at the time point of 7 days, against which the effects of the other groups and time points were compared.

The GEE model was fitted using the geepack package [28] in GNU R [27]. The estimated marginal means and their confidence intervals for each group at each time point were obtained using the emmeans package [29]. The results were then visualized using the ggplot2 package [30].

Post-hoc pairwise comparisons using Tukey's test were conducted for all group combinations to determine the specific differences between the control and test groups as well as all time points.

The estimated marginal means from the GEE model provided the predicted probabilities of recall success for both the control and test groups at each time point. These probabilities were plotted with their corresponding 95% confidence intervals and are derived from the fitted GEE model. They represent the expected proportion of participants who would successfully recall the mnemonic phrase, given the effects of the group (control vs. test), time, and their interaction. The plot enabled a clear visual comparison of the two groups over the four time points.

Upon completion of the experiment, participants of the test group were asked to complete a short questionnaire (see Appendix) in order to evaluate the effectiveness of the game in achieving its intended objectives and overall user satisfaction with the game's design and functionality. The questionnaire was filled anonymously. The questions can be categorized in broader dimensions as follows:

- User Background and context:
  - Q1: How often do you play computer or mobile phone games?
  - Q2: Do you play any games that involve moving through a map? For example Role Playing Games?
- Engagement:
  - Q3: How would you rate your overall experience with MnemonicMaker?
- Ease of use:
  - Q4: Did you find the world layout complicated?
  - Q5: How would you rate the Pathfinding tool?
  - Q6: Do you agree that the day/night switching mechanism helps with the game’s purpose?
- Effectiveness:
  - Q7: How confident are you that you will be able to remember your mnemonic phrase using MnemonicMaker?

4. Results

The success and failure results of the participants of both groups at the four different time points is shown in Table 1. Participants that failed at a certain time point were unable to recover later, with the exception of one participant of the test group that failed at 30 days, but succeeded at 60 days. Another participant of the test group succeeded during the first 30 days, but failed to recover their respective phrases at 60 days. In both failures, it was a matter of confusing the order of two items, rather than the items themselves. One participant of the test group consistently failed at all time points. The majority of participants in the control group failed at all times.

Table 1. Success/failure of participants of the control and test groups by time

Group	Outcome	Time point (days)			
		7	14	30	60
Control	Success	4	3	2	2
	Fail	15	16	17	17
Test	Success	18	18	17	17
	Fail	1	1	2	2

The results of the Generalized Estimating Equations (GEE) analysis are presented in Table 2. Overall, there were significant differences between groups ($\beta = 3.66$, $p = 0.001$), with participants in the test group (serious game) showing higher success rates compared to the control group at baseline. Success at 30 and 60 days was less likely than 7 days for both groups. Success at 14 days was not significantly different compared to the 7 days time point.

Table 2. Results of Generalized Estimating Equations Analysis for success rate

Contrast	β	Std. Error	Wald	P-value
Intercept	-0.7732	0.4935	2.454	0.11721
Group (Test)	3.6636	1.1398	10.331	0.0013 **
Time (14 days)	-0.5486	0.3715	2.18	0.1398
Time: (30 days)	-1.3669	0.6556	4.346	0.0371 *
Time: (60 days)	-1.3669	0.6556	4.346	0.0371 *
Group (Test)/Time (14 days)	0.5486	0.3715	2.18	0.1398
Group (Test)/Time (30 days)	0.6166	0.9943	0.385	0.5352
Group (Test)/Time (60 days)	0.6166	0.9943	0.385	0.5352

*Note: Reference categories are Control group and 7 days. *p < 0.05, **p < 0.01*

Within-group comparisons across time points revealed no statistically significant differences after adjusting for multiple comparisons using the Tukey method (Table 3). In the control group, despite an apparent trend toward declining performance (odds ratio between day 7 and day 30/60 = 3.92, SE = 2.57, $p = 0.138$), none of the pairwise comparisons reached statistical significance. Similarly, the test group showed stability across time points, with all comparisons yielding non-significant differences (all $p > 0.74$). The most stable period was observed between days 7 and 14 in the test group (odds ratio = 1.00), while later time points showed a slight but non-significant trend toward lower performance (odds ratio between day 7 and day 30/60 = 2.12, SE = 1.58, $p = 0.747$).

Table 3. Odds Ratios for Group Comparisons (Control/Test) at each time point

Time Point	Odds Ratio	Standard Error	z-ratio	P-value
7 days	0.0256	0.0292	-3.214	0.0013**
14 days	0.0148	0.0174	-3.596	0.0003***
30 days	0.0138	0.0146	-4.049	0.0001***
60 days	0.0138	0.0146	-4.049	0.0001***

*Note: Odds ratios < 1 indicate better performance in the test group. *p < 0.05, **p < 0.01, ***p < 0.001*

Figure 9 displays the predicted probabilities of success for both groups across all time points. The test group demonstrated consistently high success probabilities, starting at 0.947 (SE = 0.051) for both day 7 and day 14, with a slight decrease to 0.895 (SE = 0.070) at days 30 and 60. In contrast, the control group showed notably lower probabilities that declined over time, starting at 0.316 (SE = 0.107) at day 7, decreasing to 0.211 (SE = 0.094) at day 14, and further declining to 0.105 (SE = 0.070) at days 30 and 60. The substantial gap in predicted probabilities between groups remained evident throughout the study period, with the test group maintaining success probabilities that were significantly higher than the control group at all time points.

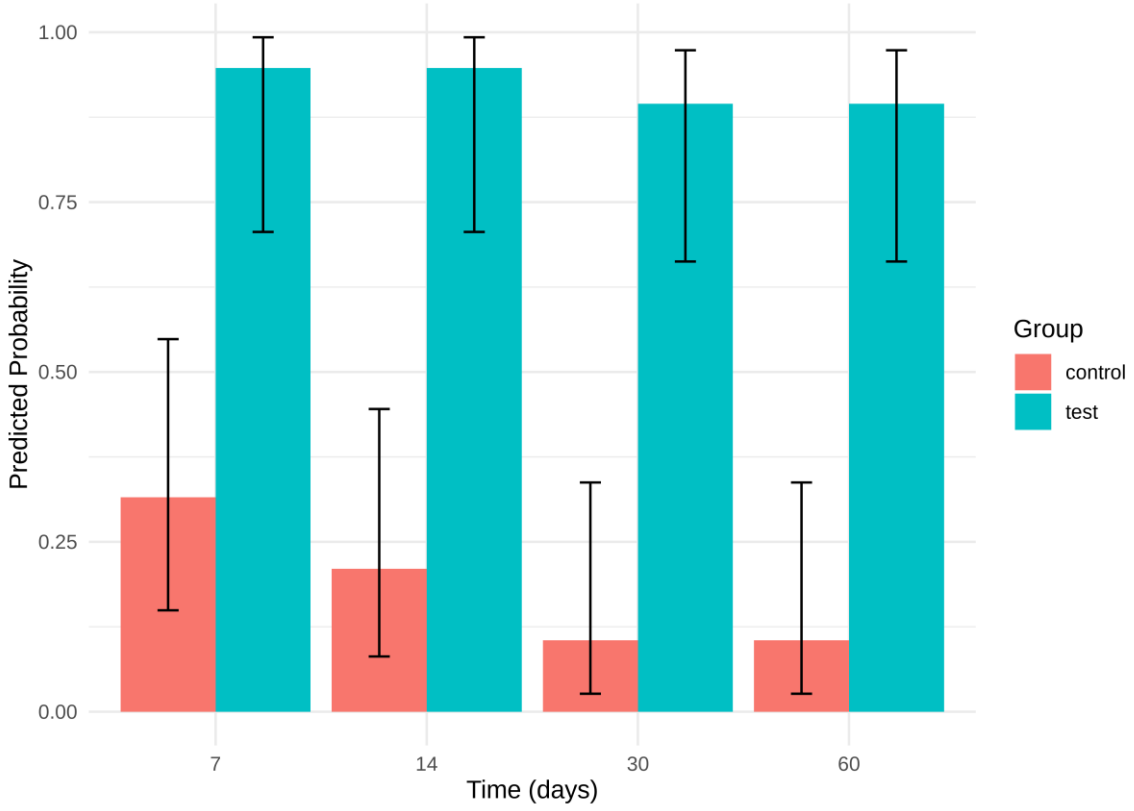


Figure 9. Predicted probabilities of success with 95% Confidence Intervals for the control and test groups by time.

Figure 10 displays the time that was required for the participants of the test group to complete gathering all items in their inventories and recovering their phrases. The median value for task completion was 10 minutes at all times, with the results not having statistical significance (repeated

measures ANOVA, df = 3, F = 0.123, p = 0.946). The minimum completion time was 6 minutes, while the maximum completion time was 14 minutes in all cases.

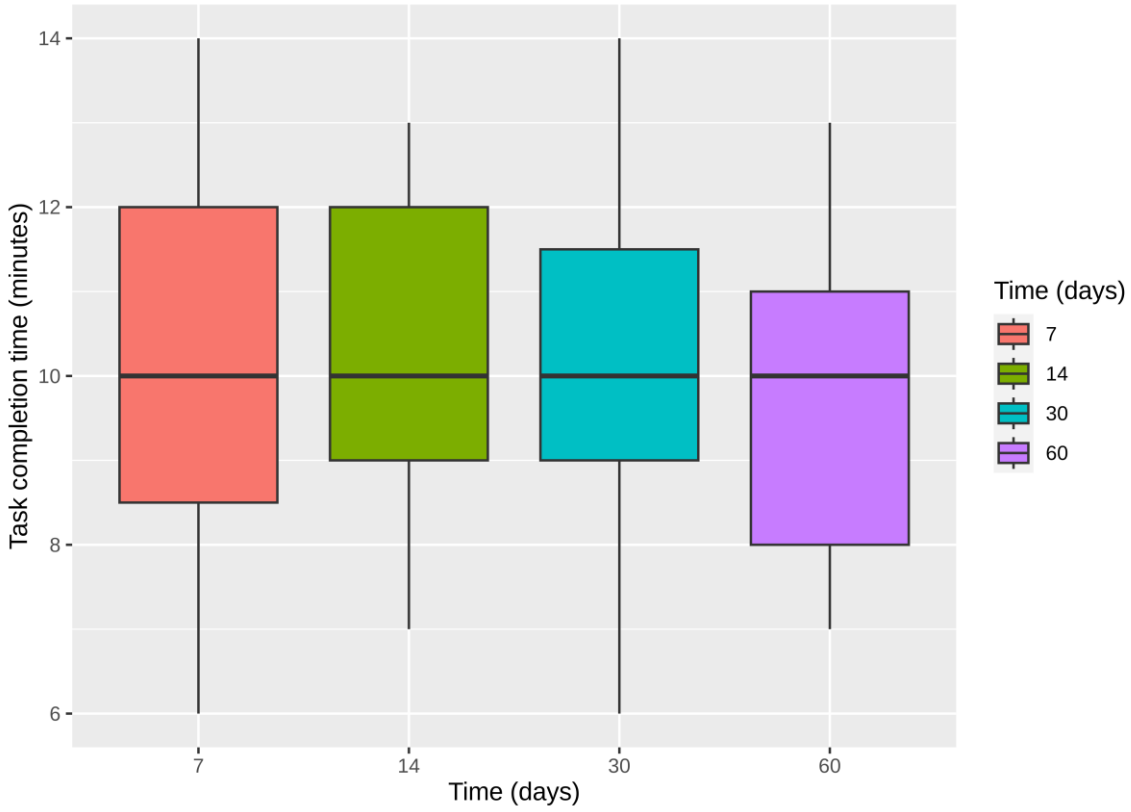


Figure 10. Recovery phrase retrieval time for the test group by time.

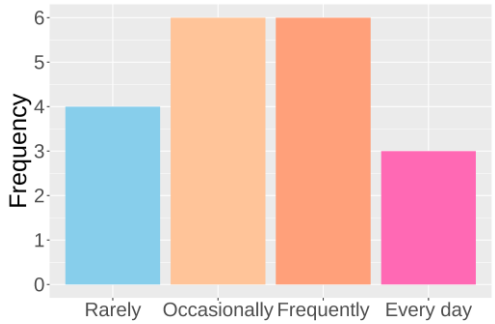
Questionnaire results are shown in Figure 11. Bars represent the frequency of responses for each category. Panel labels (a-h) correspond to different aspects of user experience and interaction with the system.

All 19 participants from the test group completed the questionnaire. Most participants reported being regular gamers, with 15 participants (79%) playing computer or mobile games occasionally or more frequently. The majority of participants (68%) replied that they have experience with map based games.

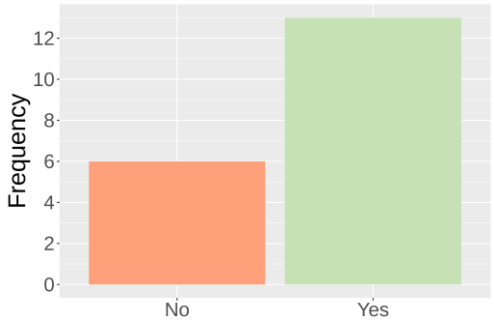
The majority of participants (79%) rated their overall experience with MnemonicMaker as positive (good or very good), with only one participant rating it as poor.

Regarding ease of use, the vast majority (84%) found the world layout uncomplicated. The pathfinding tool was well-received, with 17 participants (89%) finding it easy or very easy to follow. The day/night switching mechanism received mixed feedback, with most participants (58%) remaining neutral about its utility, while 7 participants (37%) agreed or strongly agreed that it helped with the game's purpose.

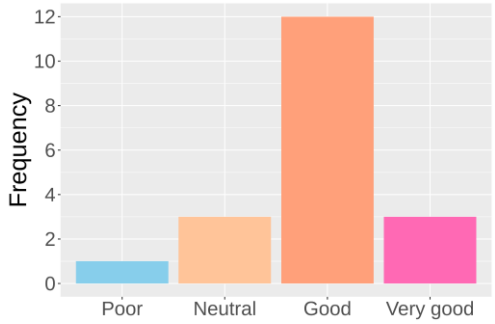
Notably, participants reported high confidence levels in their ability to remember their mnemonic phrases, with 15 participants (79%) feeling extremely confident and the remaining 4 participants being moderately or very confident. This confidence appears justified by the relatively low number of practice attempts needed: 13 participants (68%) required only 1-5 practice attempts to memorize their route, 4 participants (21%) needed 6-10 attempts, and only 2 participants (11%) required 11-15 attempts. No participants reported being unable to memorize their route.



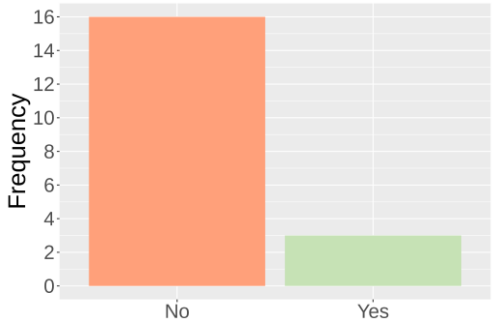
(a) Q1: How often do you play computer or mobile phone games?



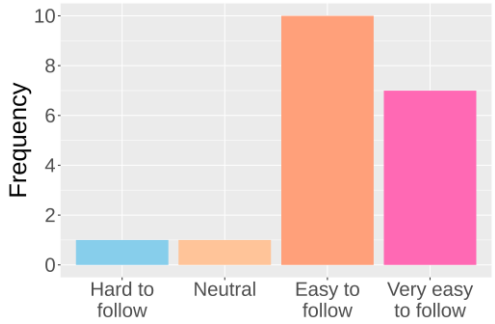
(b) Q2: Do you play any games that involve moving through a map? For example Role Playing Games?



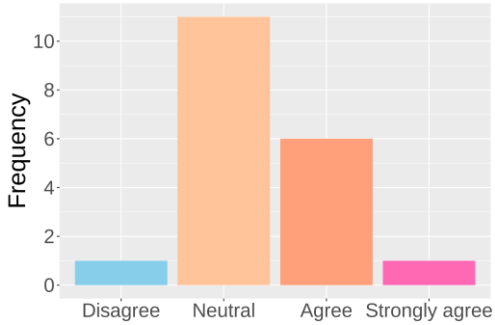
(c) Q3: How would you rate your overall experience with MnemonicMaker?



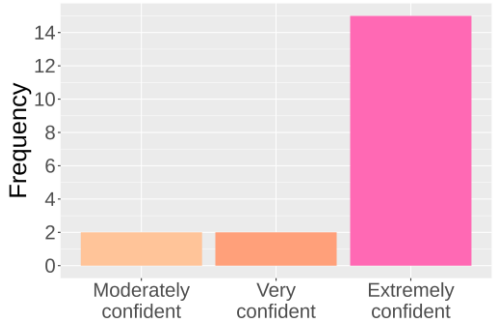
(d) Q4: Did you find the world layout complicated?



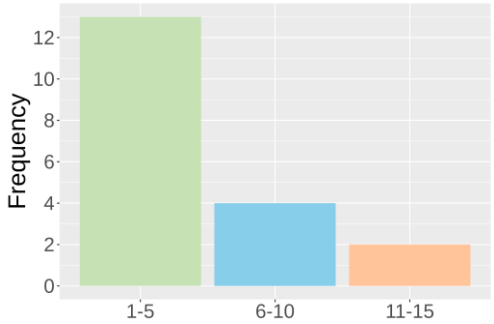
(e) Q5: How would you rate the Pathfinding tool?



(f) Q6: Do you agree that the day/night switching mechanism helps with the game's purpose?



(g) Q7: How confident are you that you will be able to remember your mnemonic phrase using MnemonicMaker?



(h) Q8: How many times did you play in practice mode until you believed you had the route memorized?

Figure 11. Results from the user questionnaire (n=19).

5. Discussion

Results from the user study demonstrate the effectiveness of MnemonicMaker as an alternative memorization system for Bitcoin BIP39 passphrases. The significantly higher success rates in the test group across all time points (from 94.7% at day 7 to 89.5% at day 60) compared to traditional methods (31.6% declining to 10.5%) suggest that the game-based approach substantially improves both initial learning and long-term retention of recovery phrases. The stability of performance in the test group, particularly during the first two weeks, indicates that the Method of Loci, when implemented through an interactive gaming environment, creates robust memory traces that resist decay over time.

Regarding the questionnaire results, our analysis of **User Background and Context** revealed that our participant pool included users with a wide range of gaming experience, from rare to daily players. Additionally, most participants were familiar with games involving map-based navigation. The similar distribution of general gaming experience and map-based gaming experience in our sample suggests a potential self-selection bias, as participants who felt comfortable with gaming interfaces might have been more inclined to volunteer.

In terms of **Engagement**, participants generally rated their experience positively, indicating strong engagement with the game. The high success rates in mnemonic recall suggest that the immersive and interactive elements of the game effectively captured users' attention and reinforced memory strategies. The strong correlation between positive engagement ratings and retention rates suggests that user engagement played a key role in the effectiveness of MnemonicMaker. A well-received user interface and intuitive interactions likely reduced cognitive load, allowing users to focus on mnemonic encoding rather than on navigating the system itself.

With respect to **Ease of Use**, most users found the game to be straightforward, with the pathfinding tool receiving particularly favorable ratings. However, the neutral responses regarding the day/night switching mechanism suggest that not all game features contributed equally to the memorization process. This feedback indicates that features perceived as more intuitive and helpful (such as the pathfinding tool) may have directly supported participants' ability to apply the Method of Loci effectively, further reinforcing long-term recall.

When considering **Effectiveness**, the consistently high retention rates, along with participants' confidence in their mnemonic recall, demonstrate that MnemonicMaker effectively supports both initial memorization and long-term retention of passphrases. These findings reinforce the utility of the Method of Loci within a game-based framework, highlighting how a well-designed serious game can transform a complex memorization task into a manageable and engaging experience.

The high confidence levels reported by participants, coupled with their actual performance, suggests that MnemonicMaker effectively builds the memory capability to recall mnemonic phrases. The fact that most users required only 1-5 practice attempts to memorize their route indicates that the learning curve is manageable. It is interesting that one user in the test group consistently failed to recover their phrase correctly, yet all users responded in the questionnaire that they believed they were able to memorize their route after at most 15 practice sessions. It is possible that this participant had memorized the wrong route from the beginning.

The positive ratings for ease of use, particularly regarding the pathfinding tool and world layout, suggest that the game successfully balances complexity with functionality. This is especially noteworthy given the varying levels of gaming experience of the participants.

Several limitations should be considered when interpreting our results. First, the sample size was relatively small (N=38), which may limit the statistical power and generalizability of our findings. Additionally, our participants were MSc students with prior familiarity with decentralized technologies, leading to a relatively homogeneous demographic. This introduces potential bias, as their existing knowledge and technical background may not reflect the experiences of broader populations, including those with less familiarity with mnemonic phrases and cryptographic concepts. However, it is likely that individuals who engage with Bitcoin wallets and need to

remember mnemonic phrases already possess some level of technical familiarity with the subject as well, meaning our participant profile may still be relevant to a significant subset of real-world users. Future studies should validate these findings with a more diverse participant pool, including individuals from different educational backgrounds and varying levels of cryptocurrency experience. While our two-month follow-up period exceeds many memory studies, longer-term retention remains unknown. Additionally, the study was conducted under controlled conditions; real-world usage patterns and stress scenarios (such as urgent need to recover funds) might yield different results. Expanding the study to include real-world testing environments would provide further insights into the practical effectiveness of MnemonicMaker.

As we wanted to assess some specific aspects of gameplay with our questionnaire, we opted to use a custom questionnaire instead of a standardized one. While the questionnaire collected valuable user feedback, it did not incorporate validated usability scales such as the System Usability Scale (SUS) [31]. The use of such standardized tools would enable greater comparability with similar studies, enhance reliability, and provide a more structured assessment of user experience. Future work should integrate these established usability metrics to strengthen the robustness of the evaluation and ensure that MnemonicMaker's effectiveness can be benchmarked against other security training tools.

A limitation of MnemonicMaker in its current version is that it only supports mnemonic phrases with a length of 12 words, whereas the BIP-39 standard supports mnemonic phrases of any length between 12 and 24 words. To the best of our knowledge, no data is available on the most commonly used lengths of BIP-39 mnemonic phrases. However, even though most software and hardware wallets support lengths of up to 24 words, they typically default to 12 words [32][33].

To support phrases longer than 12 words in MnemonicMaker, several changes need to be implemented, primarily in its user interface. Specifically, the inventory should be upgraded to accommodate a variable number of items, ranging from 12 to 24. However, MnemonicMaker in its current form can be used to recover 24 word phrases. As a 24 word phrase can be considered to be a concatenation of two 12 word phrases, this would involve the user memorizing two differenet routes and then constructing the 24 word phrase from the two halves.

Regarding memory phrase retention, expanding the inventory length and requiring users to search the map for additional items would make the game longer and likely more challenging. Recovery phrase retrieval times would increase considerably; we expect this increase to be linear, doubling from 12 words to 24. Success probabilities over time would also likely be affected, but a new user study would be necessary to determine whether this effect is significant.

While our study focused on comparing MnemonicMaker to traditional memorization techniques, as previously mentioned, other mnemonic-support tools exist. However, in designing our user study, we intentionally limited our comparison to traditional memorization methods rather than incorporating other mnemonic-support tools. Including multiple tools with varying mechanisms and user experiences would have introduced additional complexity, making it more challenging to isolate the specific effects of our serious game on memorization performance. Furthermore, given the limited number of participants, introducing additional comparison groups would have reduced the statistical power of our analysis and made it more difficult to draw meaningful conclusions.

Even though we did not include other mnemonic-support tools in our study, we can discuss some of their different aspects with respect to MnemonicMaker. Formosa [15] replaces the seemingly disconnected words in a BIP 39 mnemonic phrase with themed sentences. There are several themes, like medieval fantasy, sci-fi, farm animals and tourism. An example of a Formosa themed sentence is "A speculator accepts a marginal compound interest from the banker at Liberland". While this seems easier to remember than a 12 word mnemonic phrase of unrelated words, at least two such sentences are required to recreate a BIP 39 mnemonic phrase, while it is preferable to use four, as suggested by the Formosa authors. At the absence of a respective user study, it is not certain if that can facilitate an improvement in mnemonic phrase recall ability. The

user has to remember an even longer list of words, although these form properly structured sentences. In comparison, MnemonicMaker replaces the need to remember a list of words with spatial navigation through an interactive map. Our approach has been proven to be effective in similar cases in literature, where system assigned passwords have been effectively replaced by similar methods [34][35].

Border Wallets [13] is a method of recalling BIP 39 mnemonic phrases that uses the picture superiority effect [14], which refers to the phenomenon where information presented in the form of pictures or images is better remembered and recognized compared to information presented in the form of words or text. With Border Wallets, the user is assigned a grid of 2048 words that is 16 columns wide and 128 rows long. The user is asked to fill in parts of the grid, selecting 12 to 24 cells that represent the words in their mnemonic phrase. Ideally, the user will draw a shape that is easy to remember and recall in the future. No user study exists for the evaluation of Border Wallets, however, similar techniques have been evaluated in literature. Stobert and Biddle [36] found that selecting items on a grid can be an effective alternative to remembering a text password. However, their study extended only to 7 days and the variant that was less efficient was the blank grid, which is more similar to the grid used by Border Wallets. Other variants included a grid made up of individual object drawings and a grid with parts of a larger picture. The grids were also considerably smaller, having a size of 8x6, for a total of 48 cells and the users would have to select and remember the position of 5 cells only. Jermyn et al. [37] proposed a similar grid based scheme to replace text passwords, but the grid is even smaller in this case, having a size of 5x5. With the much larger grid of Border Wallets, it is more likely for a user to make small mistakes, confusing a cell with an adjacent one and therefore recalling a mnemonic phrase that is wrong. Another issue with Border Wallets is that the assignment of words on the grid is not static. The main reason for designing it that way, is that users are more likely to draw easy to remember patterns, like a cross, or a circle. If all users had the same grid of words, it would be more likely for them to end up with the same mnemonic phrase. In Border Wallets, each user generates their own grid, with a random assignment of the 2048 words in the cells. Therefore, in order for them to recall their mnemonic phrase, they need to both recall the specific pattern they designed, but also have access to their own personalized grid of words. So, there is still a physical item that they need to store and carry with them if they want to recall their mnemonic phrase. MnemonicMaker also supports a use case which Border Wallets does not support well. This is the case where the user already possesses a mnemonic phrase and wants to memorize it. With Border Wallets, this would probably create a grid with cells filled in random positions, which would not be easy to recall. But with MnemonicMaker, a path through the game can always be drawn.

Future research could explore how our approach compares to other mnemonic-support tools, providing a broader understanding of its relative advantages in different contexts.

A significant consideration is the potential impact of participant motivation on the results. The low success rates in the control group might partially reflect a lack of motivation to engage with traditional memorization methods, rather than purely cognitive limitations. No actual funds were ever at stake. However, we believe this interpretation actually strengthens our findings: participants in the test group faced the same motivational context yet achieved significantly higher success rates. This suggests that MnemonicMaker's game-based approach successfully overcomes motivational barriers that might hinder traditional memorization methods. The high completion rates and positive user experience reported in the questionnaire further support this interpretation.

Completion times observed for participants in the test group were relatively short and practical. This could suggest that the game mechanics and spatial cues are well-suited for rapid, confident recall. This aligns with the intended purpose of MnemonicMaker as a practical tool for securely memorizing and retrieving mnemonic phrases. Additionally, the short completion time could indicate that even brief, repeated gameplay sessions might effectively reinforce memory, opening possibilities for adaptable, time-efficient learning experiences for users across varying skill levels.

Several directions for future research emerge from our findings. First, investigating the efficacy of MnemonicMaker across different demographic groups, particularly those with limited gaming experience, would enhance understanding of its broader applicability. Second, examining how different game features (world design, object placement, navigation mechanics) contribute to memorization success could inform optimization of the system.

Another area to examine is the potential for adapting the game mechanics for other types of secure information storage. While MnemonicMaker was designed for BIP-39 mnemonic phrase recovery in Bitcoin, it is equally applicable to other cryptocurrencies that follow the same standard, such as Ethereum, Solana, and Polkadot. Since these networks use identical BIP-39-based wallet recovery mechanisms, MnemonicMaker could be used without modification to train users in securing and recovering wallets across multiple blockchain ecosystems.

Beyond traditional cryptocurrency wallets, MnemonicMaker could also be adapted to support Shamir's Secret Sharing (SSS) [38]. In this scheme, a secret, such as a private key, is divided into multiple parts, requiring a subset of those parts to reconstruct the original secret. This approach is used in multi-signature wallets, institutional key management, and secure backup solutions. Since SSS often involves shorter phrases or numerical shares rather than standard 12 or 24-word mnemonics, modifying MnemonicMaker to handle shorter and variable-length sequences would allow users to practice and understand threshold-based secret recovery in a more interactive way.

Another potential expansion involves password managers and encrypted vaults, which store sensitive credentials in an encrypted format, typically secured by a master password or a cryptographic key. Many modern password managers offer backup or emergency access mechanisms that rely on mnemonic-like recovery phrases. By adapting MnemonicMaker to simulate these scenarios, users could improve their ability to recover lost access credentials securely.

Expanding MnemonicMaker to support these additional cryptographic applications and refining its evaluation framework with standardized usability scales would increase its relevance, reliability, and impact as a versatile educational and security training tool.

6. Conclusions

This paper presented MnemonicMaker, a serious game that combines the Method of Loci with interactive gameplay to facilitate the memorization of BIP39 recovery phrases. Our experimental results demonstrated that this gamified approach significantly outperforms traditional memorization methods, with participants maintaining a high success rate after 60 days, compared to the low success rates of the control group, which used more traditional means of keeping the mnemonic phrases in memory. The rapid learning curve, evidenced by most users mastering their routes within 1-5 practice attempts, suggests that the system successfully transforms a complex security task into an intuitive experience.

While our study focused specifically on BIP39 recovery phrases, the underlying principles of combining spatial memory techniques with game mechanics have broader implications for cybersecurity education and practice. The demonstrated effectiveness of this approach suggests potential applications in other areas requiring secure information retention, from encryption keys to authentication credentials. Furthermore, the positive user engagement observed in our study indicates that the implementation of the Method of Loci through a serious game could serve as a valuable tool for overcoming the traditional barriers to adoption of security best practices.

Despite the limitations of our study, our results provide a promising foundation for future research in this domain. MnemonicMaker demonstrates the potential for innovative, user-centered approaches to addressing cryptocurrency security challenges.

As digital assets become increasingly mainstream, the need for intuitive and reliable methods of recovery phrase management will only grow. Our findings suggest that gamified mnemonic

techniques could play a crucial role in meeting this need, simplifying cryptocurrency security for a broader population while maintaining the high reliability required for financial applications.

Acknowledgments

The authors would like to extend their gratitude to the numerous individuals, online communities and platforms who have contributed to the creation and sharing of the game artwork and assets used in the MnemonicMaker serious game and which are available freely online. A detailed document with credits and licensing for every third-party asset used when making the game can be found alongside the game's source code. Finally, we are grateful to all the participants who have committed time and effort in completing the user study.

Conflicts of interest

The authors hereby declare that they have no competing interests, financial or otherwise, that could be perceived as influencing the objectivity, validity, or integrity of this research.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Decentralized Bus. Rev., 2008. [Online]. Available: https://bitcoin.org/en/bitcoin-paper. [Accessed: Jun. 15, 2024]

[2] A. M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*. 2017. ISBN: 978-1491954386.

[3] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," in *2015 IEEE Symposium on Security and Privacy*, San Jose, CA, USA, 2015, pp. 104-121, doi: 10.1109/SP.2015.14.

[4] I. Giechaskiel, C. Cremers, and K. B. Rasmussen, "When the Crypto in Cryptocurrencies Breaks: Bitcoin Security under Broken Primitives," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 46-56, Jul./Aug. 2018, doi: 10.1109/MSP.2018.3111253.

[5] T. Bamert, C. Decker, L. Elsen, R. Wattenhofer, and S. Welten, "Have a Snack, Pay with Bitcoins," in *IEEE P2P 2013 Proceedings*, Trento, Italy, 2013, pp. 1-5, doi: 10.1109/P2P.2013.6688717.

[6] P. Wuille, "BIP32: Hierarchical Deterministic Wallets," *Bitcoin Improvement Proposals*, 2012. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki. [Accessed: Oct. 10, 2024].

[7] C. I. Fan, Y. F. Tseng, and H. P. Su, "Secure Hierarchical Bitcoin Wallet Scheme Against Privilege Escalation Attacks," *Int. J. Inf. Secur.*, vol. 19, pp. 245–255, 2020, doi: 10.1007/s10207-019-00476-5.

[8] S. Eskandari, J. Clark, D. Barrera, and E. Stobert, "A First Look at the Usability of Bitcoin Key Management," *arXiv*, 2018, doi: 10.48550/arXiv.1802.04351.

[9] S. He, Q. Wu, X. Luo, Z. Liang, D. Li, H. Feng, H. Zheng, and Y. Li, "A Social-Network-Based Cryptocurrency Wallet-Management Scheme," *IEEE Access*, vol. 6, pp. 7654-7663, 2018, doi: 10.1109/ACCESS.2018.2799385.

[10] M. Palatinus, P. Rusnak, A. Voisine, and S. Bowe, "BIP39: Mnemonic Code for Generating Deterministic Keys," *Bitcoin Improvement Proposals*, 2013. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki. [Accessed: Oct. 10, 2024].

[11] J. Tommerdahl, "Introduction to the Blockchain, Bitcoin, and Other Cryptocurrencies for Educators," *Neural Comput. & Applic.*, vol. 36, pp. 20527–20536, 2024, doi: 10.1007/s00521-024-10209-y.

[12] A. Saxena, J. Misra, and A. Dhar, "Increasing Anonymity in Bitcoin," in *Financial Cryptography and Data Security, FC 2014*, R. Böhme, M. Brenner, T. Moore, and M. Smith, Eds. Springer, Berlin, Heidelberg, 2014, vol. 8438, doi: 10.1007/978-3-662-44774-1_9.

[13] "BORDER WALLETS: Introducing a new way to quickly and reliably memorise Bitcoin seed phrases." Border Wallets, 2022 [Online]. Available: https://www.borderwallets.com/. [Accessed: Feb. 10,

2025].
[14] T. Curran and J. Doyle, "Picture Superiority Doubly Dissociates the ERP Correlates of Recollection and Familiarity," J. Cogn. Neurosci., vol. 23, no. 5, pp. 1247–1262, 2011, doi: 10.1162/jocn.2010.21464.
[15] Y. S. Villas Boas, “Formosa: Improvement upon BIP39 - changed from disconnected words to themed sentences.” Github, 2023 [Online]. Available: https://github.com/Yuri-SVB/formosa/. [Accessed: Feb 10, 2025].
[16] F. A. Yates, *The Art of Memory*. London, UK: Routledge and Kegan Paul, 1966.
[17] E. A. Maguire, H. J. Spiers, C. D. Good, T. Hartley, R. S. Frackowiak, and N. Burgess, "Navigation Expertise and the Human Hippocampus: A Structural Brain Imaging Analysis," *Hippocampus*, vol. 13, no. 2, pp. 250-259, 2003, doi: 10.1002/hipo.10087.
[18] E. Maguire, E. Valentine, J. Wilding, et al., "Routes to Remembering: The Brains Behind Superior Memory," *Nat. Neurosci.*, vol. 6, pp. 90–95, 2003, doi: 10.1038/nn988.
[19] A. Y. Wang and M. H. Thomas, "Looking for Long-Term Mnemonic Effects on Serial Recall: The Legacy of Simonides," *Am. J. Psychol.*, vol. 113, no. 3, pp. 331-340, Fall 2000, doi: 10.2307/1423362.
[20] H. L. Roediger and A. C. Butler, "The critical role of retrieval practice in long-term retention," Trends Cogn. Sci., vol. 15, no. 1, pp. 20–27, 2011, doi: 10.1016/j.tics.2010.09.003.
[21] N. J. Cepeda, H. Pashler, E. Vul, J. T. Wixted, and D. Rohrer, "Distributed practice in verbal recall tasks: A review and quantitative synthesis," Psychol. Bull., vol. 132, no. 3, p. 354, 2006, doi: 10.1037/0033-2909.132.3.
[22] E. Tulving and D. M. Thomson, "Encoding specificity and retrieval processes in episodic memory," Psychol. Rev., vol. 80, no. 5, pp. 352–373, 1973, doi: 10.1037/h0020071.
[23] S. Das, D. Lu, T. Lee, J. Lo, and J. I. Hong, "The Memory Palace: Exploring Visual-Spatial Paths for Strong, Memorable, Infrequent Authentication," in *Proceedings of the 32nd Annual ACM Symposium on User Interface Software and Technology (UIST '19)*, New York, NY, USA: ACM, 2019, pp. 1109–1121, doi: 10.1145/3332165.3347917.
[24] E. Fassbender and W. Heiden, "The Virtual Memory Palace," *J. Comput. Inf. Syst.*, vol. 2, no. 1, pp. 457-464, 2006.
[25] E. L. G. Legge, C. R. Madan, E. T. Ng, and J. B. Caplan, "Building a Memory Palace in Minutes: Equivalent Memory Performance Using Virtual Versus Conventional Environments with the Method of Loci," *Acta Psychologica*, vol. 141, no. 3, pp. 380-390, 2012, doi: 10.1016/j.actpsy.2012.09.002.
[26] J. Hardin and J. Hilbe, *Generalized Estimating Equations*. London, UK: Chapman and Hall/CRC, 2003, doi: 10.1201/9781420035285.
[27] R Core Team, "R: A Language and Environment for Statistical Computing," R Foundation for Statistical Computing, Vienna, Austria, 2023. [Online]. Available: https://www.R-project.org/. [Accessed: Jul. 24, 2024].
[28] S. Højsgaard, U. Halekoh, and J. Yan, "The R Package geepack for Generalized Estimating Equations," *J. Stat. Softw.*, vol. 15, no. 2, pp. 1-11, 2006, doi: 10.18637/jss.v015.i02.
[29] R. Lenth, "emmeans: Estimated Marginal Means, aka Least-Squares Means. R Package Version 1.8.9," 2023. [Online]. Available: https://CRAN.R-project.org/package=emmeans. doi: 10.1080/00031305.1980.10483031.
[30] H. Wickham, *ggplot2: Elegant Graphics for Data Analysis*. New York, NY, USA: Springer-Verlag, 2016, doi: 10.1007/978-3-319-24277-4.
[31] J. R. Lewis, "The System Usability Scale: Past, Present, and Future," International Journal of Human–Computer Interaction, vol. 34, no. 7, pp. 577–590, 2018. doi: 10.1080/10447318.2018.1455307.
[32] “User Guide: Secret Recovery Phrase, password, and private keys.” Metamask, 2025. [Online]. Available: https://support.metamask.io/start/user-guide-secret-recovery-phrase-password-and-private-keys/ [Accessed: Feb. 21 2025].
[33] “What is BIP39?” Trezor, 2025. [Online]. Available: https://trezor.io/learn/a/what-is-bip39 [Accessed: Feb. 21 2025].
[34] M. Clark, S. Ruoti, M. Mendoza, and K. Seamons, "A comparison of three approaches to assist users in memorizing system-assigned passwords," in Proc. Symposium on Usable Security and Privacy (USEC), Feb. 2024, doi: 10.14722/usec.2024.23030.
[35] J. Doolani, M. Wright, R. Setty, and S. M. Taiabul Haque, “LociMotion: Towards learning a

strong authentication secret in a single session," in Proc. 2021 CHI Conf. Human Factors Comput. Syst. (CHI '21), New York, NY, USA, 2021, Article 689, pp. 1–13, doi: 10.1145/3411764.3445105.
[36] E. Stobert and R. Biddle, "Memory retrieval and graphical passwords," in Proc. 9th Symp. Usable Privacy Secur., Jul. 2013, pp. 1–14, doi: 10.1145/2501604.2501619.
[37] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proc. 8th USENIX Security Symp. (USENIX Security '99), 1999.
[38] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979. doi: 10.1145/359168.359176

Appendix

Questionnaire

Q1. How often do you play computer or mobile phone games?

- ☐ Never
- ☐ Rarely
- ☐ Occasionally
- ☐ Frequently
- ☐ Every day/Almost every day

Q2. Do you play any games that involve moving through a map? For example Role Playing Games?

☐ Yes ☐ No

Q3. How would you rate your overall experience with MnemonicMaker?

- ☐ Very Poor
- ☐ Poor
- ☐ Neutral
- ☐ Good
- ☐ Very Good

Q4. Did you find the world layout complicated?

☐ Yes ☐ No

Q5. How would you rate the Pathfinding tool?

- ☐ Very hard to follow
- ☐ Hard to follow
- ☐ Neutral
- ☐ Easy to follow
- ☐ Very easy to follow

Q6. Do you agree that the day/night switching mechanism helps with the game's purpose?

- ☐ Strongly disagree
- ☐ Disagree
- ☐ Neutral
- ☐ Agree
- ☐ Strongly agree

Q7. How confident are you that you will be able to remember your mnemonic phrase using MnemonicMaker?

- ☐ Not at all confident
- ☐ Slightly confident
- ☐ Moderately confident
- ☐ Very confident
- ☐ Extremely confident

Q8. How many times did you play in practice mode until you believed you had the route memorized?

- ☐ 1-5
- ☐ 6-10
- ☐ 11-15
- ☐ >15
- ☐ I could not memorize it