**<Cryptocurrency>**

מסמך אפיון

<איילון נוה>

<גרסה 1>

<20.12.18>

**היסטוריית גרסאות המסמך**

|  |  |  |
| --- | --- | --- |
| **תאריך** | גרסה | **תקציר השינויים** |
| 20.12.18 | 1 | מסמך התחלתי בסיסי |
| 27.5.19 | 2 | מסמך שני כאשר מרבית הקוד כתוב ואני יודע מה הולך להיות בפרוייקט |
|  |  |  |
|  |  |  |



**1. הקדמה**

1.1 מטרה

*המטרה של המסמך היא להסביר את דרישות הפרויקט- Cryptocurrency*

1.2 המוצר

* *שם המוצר הוא Leprecoin מטבע דיגיטלי מאובזר מסוג cryptocurrency*
* *המוצר הוא המטבע הדיגיטלי והטכנולוגיה מאחוריו.*
* *מטרת המוצר היא בעצם יצירת ארנקים המאפשרים העברת המטבע באופן מאובטח ותקין. ההבטחה תתבצע בעזרת הבלוקצ'יין ומפתחות פרטיים וציבוריים.*

1.3 הגדרות

*מטבע דיגיטלי ( (Cryptocurrency- המטבע הדיגיטלי מונפק על ידי גוף פרטי כלשהו שמפתח טכנולוגיה שאינה מאפשרת לשכפל אותו. המטבע בדרך כלל אינו שייך לגוף שהנפיק אותו אלא פתוח לכולם. למעשה מדובר בפרוטוקול (תוכנה), שרץ במקביל על אלפי מחשבים ונרשם על ידיהם. מטבע דיגיטלי קריפטוגרפי הוא מטבע שאבטחתו נעשת באמצעות מפתחות פרטיים וציבוריים.*

*בלוק צ'יין - היא תפיסה טכנולוגית במחשוב המאפשרת פעילות עסקית מאובטחת באינטרנט ואימות של טרנזקציות עסקיות בין צדדים שונים ללא צורך בישות ניהול מרכזית.*

*ביטקוין - הביטקוין הוא מטבע שאינו תלוי בגוף מרכזי. במקום זאת, ביטקוין הוא רשומה בקובץ ציבורי המכונה "שרשרת בלוקים" (בלוקצ'יין), ניתן לנהל אותו או להשתמש בו בעזרת תוכנה המכונה "ארנק". מערכת הביטקוין היא מערכת המבטיחה שהתשלומים יתבצעו באופן תקין כך שסכום שהועבר בתשלום אכן נגרע מארנק המקור והתווסף לארנק היעד.*

*כרייה – הוספת בלוק לשרשרת הבלוקים על ידי תהליך מסובך הכולל חישובים מתמטיים ודורש יכולות מחשוב גדולות*

*מפתח פרטי- מפתח פרטי השייך למי שיצר אותו ורק הוא יכול להשתמש בוא על מנת לחתום מידע.*

*מפתח ציבורי- לכל מפתח פרטי יש מפתח ציבורי שמטרתו שיהיה ידוע לכולם, בעזרת המפתח הציבורי אפשר לאמת את החותם על חתימות דיגיטלות. אי אפשר לחשב את המפתח הפרטי מהציבורי*

*חתימה דיגיטלית- מידע אשר עבר עלי שימוש במפתח פרטי (נחתם על ידו) נקרא חתימה. בעזרת מפתח הציבורי אפשר לאמת אם החותם הוא בעל המפתח הפרטי שמתאים לציבורי.*

**1.4** תקציר

*בהמשך המסמך ישנו תיאור כללי על הפרוייקט, קהל היעד ועל הפונקציות שבו. בנוסף לכך, ישנם דרישות מפורטות של החלקים המרכזיים במערכת הכוללים את ממשק המשתמש הארנק.*

1. תיאור כללי

2.1 פונקציונליות

*המערכת מחולקת לכמה חלקים שיצרו את הבלוק צ'יין, את הארנק הכולל ממשק גרפי ואת הסחר במטבע.*

2.2 קהל היעד

*קהל היעד של המערכת הוא בעצם כל אדם שרוצה לרכוש, לסחור ולהעביר את המטבע הווירטואלי שאני יוצר.*

*המשתמשים במערכת צריכים הבנה בסיסית במטבעות, כלומר, הם צריכים לדעת שערכם משתנה ומה היתרונות והחסרונות של להחזיק מטבע ווירטואלי. המערכת אינה מתאימה לילדים.*

2.3 אילוצים עיקריים

**- המערכת דורשת חיבור לאינטרנט**

**- המערכת צריכה לתמוך במספר רב של משתמשים**

**- השרת שיוצר את הבלוקים ואת הכרייה יצטרך יכולות מחשוב גבוהות**

**- המערכת צריכה אבטחה גבוהה מאוד**

2.4 הנחות ותלויות

**- המערכת תרוץ על ווינדוס**

**- המטבע לא יסחר גם כמטבע אמתי וגם במערכת עצמה**

**2.5** סיקור מצב השוק כיום (אופציונלי)

ישנם כמה מטבעות העובדים בטכנולוגיה כמו שאני ממש. הגדולים בהם הם: ביטקוין ואת'ריום שלשניהם שווי שוק של עשרות מיליוני דולרים.

בנוסף טכנולוגית בלוק צ'יין משמשת כיום ליצירת חוזים ולמימושם באופן אלקטרוני, העברות רשומות רפואיות באופן מאובטח, ועוד.

1. דרישות מפורטות

3.1 דרישות פונקציונליות

*פונקציות בארנק*

*פונקציות הנמצאות בארנק של המשתמש. הארנק מוצג בממשק גרפי*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *שם* | *הסבר כללי* | *קלט* | *תהליך* | *פלט* | *טיפול בשגיאות* |
| *העברת מטבעות* | העברת מטבעות למשתמש אחר | כמות המטבעות שהמשתמש רוצה להעביר ואת פרטי המשתמש שהוא רוצה להעביר אליו | שליחת הבקשה ואת פרטיה לשרת |  | בדיקה שלא מעבירים כסף שאין בארנק. |
| *הצגת העסקאות*  *של הארנק* | הצגת כל העסקאות שהמשתמש עשה ושהעבירו כסף אליו | העסקאות שכללו את הארנק | הצגת הקלט במסך |  |  |
| *הצגת הכסף הכולל של בעל הארנק* | הצגה על המסף של סך כל המאזן של בעל הארנק | הכסף שיש לבעל הארנק | הכסף הקלט במסך |  |  |

*איך נכנ*

3.2 דרישות של ממשקים חיצוניים

**3.2.1 ממשקי משתמש**:

ממשק הארנק – ממשק הארנק הוא gui הכולל:

- כמות הכסף הנוכחית בארנק

- כפתורים המבצעים את הפעולות שמתוארות בדרישות הפונקציונליות.

- כפתור שמאפשר כניסה להיסטוריית העברות שביצע.

- ממשק משתמש נוסף המאפשר כניסה לארנק על פי שם משתמש וסיסמא

\* הפעולות שידרשו קלט מהמשתמש של כמות כסף למכור או לקנות יקלטו בעזרת תיבת טקסט שבה המשתמש מכניס את הקלט

**3.2.2 ממשקי חומרה**

**3.2.3 ממשקי תוכנה** (אם התכנה מחולקת לכמה תוכנות שונות שצריכות לתקשר בניהן)

**3.2.4 ממשקי תקשורת (למשל תקשורת בין שר**ת ללקוחות)

3.3 דרישות לא פונקציונליות

**3.3.1 דרישות ביצועים (performance)**

**3.3.2 מהימנות.**

**3.3.3 השרת זמין 24.7 ומאפשר כל זמן כרייה**

**3.3.4 אבטחה מקסימלית**

**3.3.5 דרישות תחזוקה (maintainability)**

**3.3.6 דרישות ניידות (portability)**

3.4 דרישות בסיס נתונים

* *ישמרו הנתונים של העסקאות במטבע (על ידי הבלוק צ'יין) וגם הסיסמאות על מנת להכנס לארנק. בנוסף יהיה מאגר של פרטי האשראי וחשבונות בנק מדומים.*
* *המידע ישמר גם בdb וגם הבלוק צ'יין הוא מאגר מידע השומר את מיקומן של כל המטבעות המונפקים והעסקאות שהתרחשו.*
* *מה יכולות האחסון הנדרשות (נפח אחסון לדוגמא)*
* *נדרשת רמת הבטחה גבוהה שבה יצפינו את הסיסמאות ופרטי האשראי המעוברים.*

3.5 דרישות נוספות

5. נספחים