**Leprecoin>>**

מסמך אפיון

<איילון נוה>

<גרסה 2>

<27.5.19>

**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. הבלוקצ'יין היא בעצם שרשרת של בלוקים כשכל בלוק מקושר לקודמו ולכל בלוק יש קוד hash יחודי.*

*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.*

*P2P- בניגוד לתקשורת הנפוצה כיום- בין שרת ללקוח. p2p זאת שיטת תקשורת שלא תלויה בשרת שמנהל אותה אלא כל המשתמשים במערכת מקימים אותה. מטבע המשתמש ברשת כזאת נקרא מטבע מאובזר*

**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, את הכרייה ואת התקשורת*

2.2 קהל היעד

*קהל היעד של המערכת הוא בעצם כל אדם שרוצה לסחור במטבע הווירטואלי שאני יוצר.*

*המשתמשים במערכת צריכים אינם צריכים להבין במטבעות משום שהמטבע לא נסחר, אך הבנה בבסיסית על איך הטכנולוגיה עובדת- שהיא לאת תלויה בשרת אחד, שעל מנת להחיל עסקאות לוקח זמן (בגלל הכרייה) ושם חייבים לשמור את הקובץ עם המטבע הפרטי שלהם.*

2.3 אילוצים עיקריים

**- המערכת דורשת חיבור לאינטרנט**

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

**- המערכת צריכה אבטחה גבוהה מאוד (על ידי הבלוק צ'יין והמפתחות)**

**- יהיה מחשב שידוע שרץ קבוע כמארח והוא יאפשר** peer discovery

2.4 הנחות ותלויות

**- המערכת תרוץ על ווינדוס**

**- המערכת תשתמש בפייתון** 2.7.16

**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 |  |  |

*הכניסה לארנק מבוצעת על ידי קובץ שמכיל את המפתח הפרטי של המשתמש. בדומה לביטקוין אם המשתמש מאבד גישה למפתח, הוא מאבד את היכולת להשתמש במטבעות שלו. כאשר אין קובץ של המפתח, נוצר מפתח חדש וכתובת חדשה.*

*איך נכנס כסף לארנק?*

*בביטקוין על מנת לקבל כסף המשתמש צריך לפנות לבנק המאפשר חלופת כספים בבטיקוין. אבל גם הבנק צריך לקבל את הכסף, אז איך נוצר כסף במערכת?*

*רשימת כל הכספים של כל המשתמשים מאוכסנת בבלוקצ'יין ועל מנת להוסיף עוד עסקאות צריך להוסיף לבלוקצ'ין עוד בלוק שמכיל את העסקאות. הוספת הבלוק ככרוכה בתהליך שנקרא כרייה והוא כרוך בכוחות מחשוב רבים. לכן, הכורה מתוגמל על ידי הקוד בכמות מסוימת של מטבעות על כל כרייה, בכך, נוספים מטבעות לכמות הכוללת יש מאין.*

*במערכת שלי אין בנק סוחר והכסף יכול לעבור עלי ידי העברות בידי הארנקים.*

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.

- 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. על מנת להריץ כרייה באופן הכי טוב צריך חומרה חזקה**

**3.2.3 ממשקי תוכנה** הכולל את הקוד הליבה המכיל את מבנה הנתונים השונים

**3.2.4 ממשקי תקשורת. תקשורת** p2p  **על ידי סוקטים.**

3.3 דרישות לא פונקציונליות

**3.3.1 דרישות ביצועים (performance) – תהליך הכרייה לא יקח יותר מחמש דקות**

**3.3.2 משימוש ברשת** p2p **המהימנות שלה תלויה ברוב המשתמשים ברשת. אם רוב המשתמשים ברשת יריצו את הקוד שלי הם יקראו "מהימנים" והם יקימו רשת תקינה. ברגע שרוב הרשת נשלטת מורכבת ממשתמשים לא מהימנים, שלדוגמא מוסיפים לעצמם מטבעות, הם יתגברו יפגעו במהימנות המטבע. דבר זה נקרא התקפת 51 אחוז בביטקוין.**

**3.3.3 דרישות זמינות- המערכת על מנת ל"הכיר" משתמשים נוספים תצטרך לפנות לכתובת מוכרת שתעזור לה למצוא משתמשים נוספים. הקוד של כתובות אלו חייב לרוץ תמיד.**

**3.3.4 אבטחה גבוהה שתתבסס על הבלוקצ'יין ומפתחות קריפטוגרפיים.**

**3.3.6 דרישות ניידות (portability)- אם המשתמש רוצה להריץ את הארנק שלו ממחשב אחר הוא חייב להעביר אתו את הקובץ של המפתח הפרטי שלו.**

3.4 דרישות בסיס נתונים

* *ישמרו הנתונים של הבלוק צ'יין בבסיס הנתונים. לאחר כמה זמן על מנת להתחבר למערכת שוב, הארנק לא יצטרך להוריד את כל הבלוק צ'יין מהמשתמשים האחרים אלא רק את הבלוקים שחסרים לו.*
* *יישמרו הכתובות ip של מחשבים שתקשרת איתם בעבר, על מנת לנסות להתחבר אליהם שוב לאחר התנתקות מהמערכת, ולא להצטרך לקבל נתונים מכתובת שידוע שהיא אמינה ותמיד מחוברת*
* *ישמר המפתח הפרטי של כל ארנק בקובץ*