Dreamveil –

Blockchain

פתיחה

מטרת הפרוייקט היא יצרת בלוקצ'יין – מסד נתונים המאוחסן ללא צורך בשרת מרכזי (Decentralized). בפרויקט זה מסד הנתונים יתמוך בהעברה של כסף דיגיטלי (Cryptocurrency) ובהוכחת בעלות על מדיה והטמעת הוכחת הבעלות בפומבי במסד הנתונים.

על מנת לבצע זאת נדרש להגדיר מספר דברים:

* עותק של מסד הנתונים יהיה מאוחסן בכל אחד מהלקוחות המשתמשים במסד הנתונים.
* המערכת חייבת להתנהל ללא אמון באף אחד מהמשתתפים (הלקוחות) בפרט.
* על מסד הנתונים להיות חסין מפני שינוי ספונטני או זיוף וזהום של כל אחד מהלקוחות.

עקרונות אלו יכוננו את ארכיטקטורת הפרויקט.

מבנה הבלוקצ'יין

העברה – Transaction

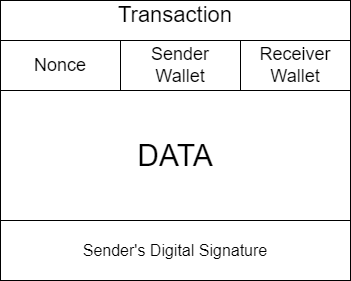
בבלוקצ'יין העברה היא המידע הבסיסי שמסד הנתונים מכיל, כל העברה היא הצהרה על מידע שיש לשמר בבלוקצ'יין. העברה יכולה להכיל הוכחות בעלות מדיה או הכרזה על העברת מטבעות דיגיטליים מארנק אחד לארנק אחר. ההעברות ישודרו בפומבי אל משתמשי הרשת על מנת שיועברו על להעברות מספר תנאים שיש לעמוד בהם על מנת לממש רכיב זה בבלוקצ'יין.

1. כל העברה חייבת להיות מיוצרת על ידי המקור המצוין בה בהכרח.
2. יש למנוע מכלל הלקוחות לשנות את התוכן של העברה לאחר שפורסמה ברשת
3. נדרשת היכולת להבדיל בין העברה אחת להעברה אחרת ללא תלות בתוכן ההעברה.

אתגרים במימוש ופתרונות

* כיצד ניתן למנוע מגוף זר לבצע העברה עבור לקוח אחר? על מנת לפתור בעיה זו נפנה למושג בקריפטוגרפיה הנקרא חתימה דיגטלית. כל לקוח ייצר צמד מפתחות אחד פרטי ואחד ציבורי, כאשר לקוח מעוניין לחבר העברה, הוא יצמיד אליה את המפתח הציבורי שלו (הוא גלוי לכולם). בסוף ההעברה ייצר המחבר חתימה דיגטלית המושפעת מגוף ההעברה ויצרף אותו אל סוף ההעברה. בסופו של דבר תתקבל מערכת שבה ניתן לוודא שהעברה מסוימת אכן חוברה על ידי השולח. כל לקוח כעת יוכל לאמת זאת באמצעות המפתח הציבורי המצורף בהודעה, והחתימה הדיגיטלית בסוף ההודעה.
* החתימה הדיגטלית גם פותרת בעיה נוספת, היא מונעת מכול זר לשנות את התוכן הקיים בה, זאת משום שכל שינוי של התוכן אמור לשנות את ערך החתימה הדיגטלית ולא ניתן לשנות את ערך החתימה משום שהמפתח הפרטי נדרש על מנת לייצר אותה, אך אין לאף זר מלבד השולח את אותו מפתח הפרטי. כל שינוי של התוכן יבטל את ההתאמה של המפתח הציבורי שצירף השולח לחתימה הדיגיטלית של ההעברה.
* כיצד ניתן לדעת אם יש לשלוח שרירותי יתרה מספקת על מנת לבצע העברה? הבלוקצ'יין מקליט העברות של כספים דיגטליים בין הארנקים השונים, אך הוא אינו מכיר במושג של יתרת חשבון. על מנת לחשב כמה יתרה יש לארנק, נדרש לסכום את העברות אליו ולחסר את העברות ממנו, כך נקבל את יתרת הארנק. למרות זאת, מעבר על שרשרת הבלוקים במלואה כולל שני חסרונות משמעותיים; יש לעבור על כל הבלוקצ'יין ולדוג אחר כל אחת מהעברות הקודמות עבור כל ארנק שולח עבור כל העברה. פעולה זו עלולה להיות מאוד לא יעילה משום שבמקרה הכי גרוע, נדרש לעבור על הבלוקצ'יין במלואה, כאשר גודלה יכול להגיע לסדר גודל ענק (במטבע הפופולרי Bitcoin שרשרת הבלוקים מגיעה ליותר מ700,000 בלוקים). חסרון נוסף הוא שנדרש על כל לקוח להוריד את כל שרשרת הבלוקים על מנת להשתמש בה, אין זה אידיאלי משום שהגודל שלה עלול גם הוא להיות גדול מאוד. על מנת למגר את החסרונות הללו, נשתמש במבנה נתונים יעיל: AVL. ונשמור עליו באופן ממוין לפי ארנק השולח של ההעברה את כל ההעברות שמתקבלות. בAVL, הכנסת ערך והוצאת ערך נעשית בסיבוכיות O(log n), בנוסף לכך על מנת לחשב את היתרה של ארנקים, רק עץ ההעברות נדרש, ובכך ניתן להימנע מהורדה של שרשרת הבלוקים השלמה.

הינה תרשים של מחלקת Transaction המתארת את מאפייני ההעברה.



* Sender/Receiver wallet – הארנק של שולח ויוצר העברה והארנק של הגוף המקבל בהעברה (שאליו מועבר) בהתאמה. הארנקים יהוו מפתחות ציבוריים במערכת הצפנה א-סימטרית
* Nonce – מספר אקראי שמטרתו להשפיע על החתימה הדיגטלית של הבלוק, על מנת למנוע שיכפולים.
* DATA – המידע שמכילה ההעברה, המידע יכול לסמל מדיה מסוימת או פקודת העברה של כסף דיגיטלי מכתובת השולח אל כתובת המקבל.
* Sender’s Digital Signature – החתימה הדיגיטלית של מחבר ההעברה, החתימה כוללת את כל העברה ומושפעת מערך הNonce. מטרתה להבטיח שימור של הערכים בהעברה ולהבטיח ששולח ההעברה הוא גם המחבר שלה.