Freeman Family

4 ביולי 2019

EPIC CASH

EPIC PRIVATE INTERNET CASH

מערכת כספים אלקטרונית מסוג עמית-לעמית

אמצעי לשמירת ערך+ כלי חליפין+ יחידה חשבונאית

1.7 מיליארד מבוגרים חסרי גישה למערכת הפיננסית העולמית כיום, בעוד 1.3 מיליארד נוספים בעלי גישה חלקית. EpicCash חושף את הפוטנציאל של אנשים פרטיים על ידי חיבור של האנשים הללו לשוק העולמי. מהיר, כמעט בחינם ונגיש לכולם.

Version 7.1b

תוכן

I. תמצות

Epic Cash , היא הנקודה הסופית במסע האמיתי של מזומנים P2P באינטרנט, אבן הפינה של מערכת פיננסית פרטית. מטבע Epic שואפת להפוך את הצורה הטובה ביותר בעולם להגנה על הפרטיות של כסף דיגיטלי. על מנת להגשים את המטרה, Epic מספקת את שלושת התפקידים העיקריים של הכסף:

1. **אמצעי לשמירה על ערך** - ניתן לאחסן, להסיר ולהחליף אחר כך; יחד עם זאת, יש ערך צפוי עם קבלתו;
2. **אמצעי חליפין** - כל מה שמקובל כסטנדרט של ערך, וניתן להחליף אותו בסחורות או בשירותים;
3. **יחידת חשבון** - היחידה שבאמצעותה מדווחים ומשווים ערך של דבר מה.

	BTC	$ USD	EPIC
כלי לשמירת ערך	✓	✓	✗
אמצעי חליפין	✓	✗	✓
יחידת חשבון	✓	✗	✓

בשנת 2009, הביטקוין הפך למטבע הדיגיטלי הראשון מבוסס על הבלוקצ'יין ואז נקבעו שלושה מאפיינים שעל פיהם הוערכו קריפטו-מטבעות אחרים:

✓ **חוסר צורך באמון-** "בכדי שהרשת תפעל, אין צורך באמון בין הצדדים בשביל תפקוד מלא של הרשת".

✓ **חוסר יכולת לביטול-** אין אפשרות לבטל עסקאות:
א. שכתוב של עסקאות בלתי אפשרי או דורש להשקיע הרבה מאד כסף.
ב. אף אחד, למעט הבעלים של המפתח(הסגור) הפרטי אינו יכול להעביר כספים בלי רשות.
ג. כל העסקאות נכתבות לבלוקצ'יין.

✓ **ביזור-** "בלוקציינים מכל סוג מבוזרים פוליטית (אף אחד לא שולט בהם), ומבוזרים ארכיטקטונית (אין נקודת כישלון תשתיתית)".[1]

ביטקוין בנה יסודות חדשים מבחינה טכנולוגית, תוך הקפדה על יסודות וההגדרות שנבדקו בזמן הפיתוח במבנה המדיניות המוניטרית שלו בתחילת הדרך.
ההצלחה של הביטקוין קשורה מאד להיצע המצומצם שלו בשילוב עם בלוקציין, חוסר הצורך באמון, בלתי אפשרי לשינוי של הבלוקציין, וביזור מלא שלו.
Epic Cash מחקים את המדיניות המוניטרית של הביטקוין בהפחתת האינפלציה, והיצע מוגבל מבטיח שהמטבע יכל לשמר כמאגר ערך יעיל עם שמירת ערך.

למרות ההצלחה של ביטקוין, חסרונות מסוימים נחשפו מאז הקמתו לפני עשר שנים. פרויקטים אחרים ניסו להתגבר עליהם ובחנו את הטובים שבהם כדי לבנות עליהם את הפיתוח שלנו. החלטנו להשתמש בבסיס הקוד של Grin וההישגים הטובים ביותר של כמה פרויקטים אחרים כדי לעזור לנו להיות מושלמים ולהתגבר על הטעויות והתקלות שהתגלו אצל קודמי Epic Cash.

Epic Cash הוא בעל התכונות העיקריות להיות מטבע אידיאלי מושלם:

✓ **קישור -** הערך של יחידה נתונה של Epic, חייב להיות תמיד שווה ליחידה אחרת של Epic, בדיוק כמו שיואן ויין אחד שווה ואפשר להחלפה ביין ויואן אחר .השגת הקישור הזה במידה משמעותית תלויה בסודיות.

✓ **סודיות -** Epic Cash בלוקציין מבטיח את האנונימיות של מחזיקי Epic המשתמשים ב- Epic, ומגן על פרטי העסקאות מפני גישה לצד שלישי; זה נועד להיות בלתי ניתן לצפייה ומעקב עבור העוקבים .

✓ **מדרגיות -** Epic Cash תומך בבלוקציין קומפקטי שיכול להתקין פתחי יציאה חדשים בקלות ללא שימוש בציוד עתיר משאבים. Epic Cash בלוקציין מסוגל להכפיל את רוחב הפס של הביטקוין.

✓ **מהירות -** עסקאות Epic Cash מתרחשות בצורה חלקה, ברציפות ומבוצעות הרבה יותר מהר מאשר בטכנולוגיית הבלוקציין בדורות הקודמים. בזמן שלביטקואין, יש שישה חסימות של 10 דקות כדי לקבל אישור עסקה מלא, על מנת לאשר את העסקה, לEpic נדרש אישור אחד, המשמעות של זה שהכל מסתיים במהירות לאחר הבלוק הראשון שבשבילו נדרשת דקה 1 בלבד .

[1] Buterin, Vitalik, *The Meaning of Decentralization*, 6 February, 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

II. סודיות

אפשר להבין את השימוש הנוכחי בכסף כהעברה קולקטיבית של יחידות ספירה חשבונאית בין אנשים למוסדות, ניתן להציג את עמדת הכסף בכל זמן נתון לאחר קבלת תשובות לשאלות הבאות:

1. מי מחזיק אותם, וכמה הוא מחזיק?

2. מי ועם מי מבצעת העסקה תמורת כמה?

לגבי מטבעות פיאט מסורתיים, וכמובן שגם ביטקוין, אנו יכולים לענות על שאלות אלו. בכך ניתן לחשוף הרבה על חייהם של אנשים, כמו למשל דפוסי צריכה, בעלות ועסקאות בין צדדים נגדיים. ניתן להסיק מסקנות די מדויקות לגבי האינטרסים והכוונות של האדם על ידי מעקב אחר העברות בעלות ערך שהוא עושה. ללא פרטיות, נתוני עסקאות יכולים להיות מידע מסוכן בידי צדדים שלישיים שלא מעורבים בעסקה.

השימוש בעשור האחרון במטבעות קריפטו מראה בעיות של "פרטיות" בסוגי בלוקציין שונים. אם אנחנו לוקחים בחשבון את סולם הפרטיות, הוא נע בין פתוח לשמצה בקצה אחד לאנונימי מצד שני. ברגע שיש שחיקה של פרטיות, קורס אחד הדברים החשובים במטבעות קריפטו- חוסר הצורך באמון. בזמן האחרון אנחנו רואים הצלחה של שירותים לניתוח העברות בבלוקציין של הביטקוין, ואפשר לומר שהאנונימיות שלו פוחתת מיום ליום. על המשתמשים לנקוט יותר ויותר צעדים כדי להבטיח שהם לא מבצעים שום העברות בביטקוין נגוע שחשוד בפלילים.

הפיתרון של Epic Cash מביא את כל הכוח לעבר אנונימיות. והכי חשוב משחזר נכס חיוני זה על ידי הבטחת כי הן פרטיות הפרט, והן פרטיות העסקאות הינם מהונדסים למערכת ברמה בסיסית.

פרטיות של הזהות

פרטיות של העסקה

פרטיות של הזהות

רוב מטבעות הקריפטו כמו הביטקוין מאוחסנים בארנקים שכתובותיהם מתייחס למפתחות ציבוריים הנגזרים ממפתחותם הפרטיים של הארנקים שבהם הם מאוחסנים. ניתן לחשוב על כתובות אלה כמאתרים של הכספת הפרטית של האדם בעולם הדיגיטלי .
הבלוקציין של Epic Cash מבטל כתובות לחלוטין ובמקום זאת מחיל ריבוי עצמים רב-תכליתי אחד ממנו נוצרים כל המפתחות הציבוריים והפרטיים על בסיס חד-פעמי.

מכיוון שכתובות ארנק ביטקוין הינן אפשרות איתור כספת בעולם הדיגיטלי, ניתן לאתר את הארנק לכתובת IP של פרוטוקול הבעלים (IP), המאגן את הבעלים למחשב ייחודי במיקום ייחודי בנקודת זמן נתונה.

בפשטות, הנה ההסבר: כאשר מתבצעת עסקת ביטקוין, העסקה משודרת ממרכז תקשורת הנקרא "צומת" ואז מועברת לצמתים אחרים שנקראים "עמיתים".

מידע זה מתפשט במהירות לכל אחד מהעמיתים שנותרו באותו הזמן והצמתים בגל הרשת כולה. תהליך זה נקרא "פרוטוקול הרכילות". בפשטות, לכל ביטקוין יש מיקום מקוון גלוי ומיקום פיזי בו ניתם למצוא אותו, או לייתר דיוק, את בעל הביטקוין.

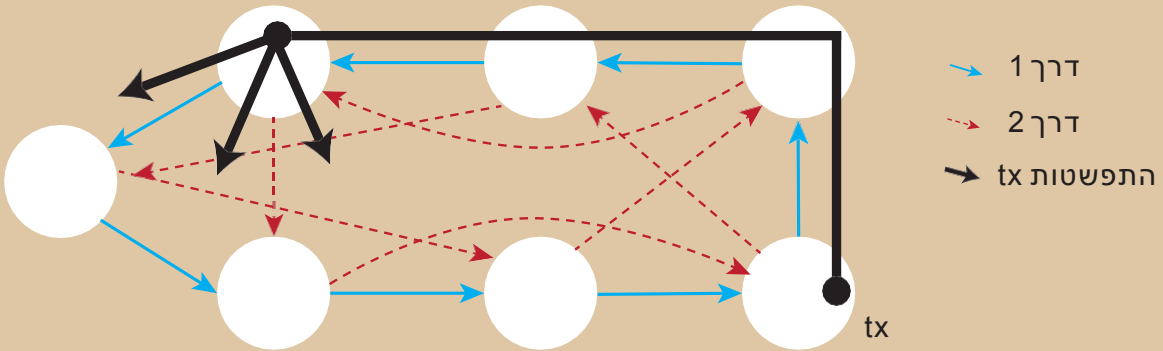
כפי שציין העיתונאי גרייס קיין, הביטקוין הוא "לא סוד יותר מחיפוש קצר בגוגל מחיבור אינטרנט ביתי". [2]

בנוסף לביטול השימוש בכתובות ארנק, ה- Blockchain של Epic Cash מבטיח סודיות של נתונים אישיים ולא מאפשר לעקוב אחר כתובות IP.

זה נובע משילוב של פרוטוקול **Dandelion ++**. ולמעשה זה **פרוטוקול Dandelion** המקורי, ששופר ביחס לקודמו. פרוטוקול **Dandelion ++** הוא תוצאה של עבודתם המתמשכת של 7 חוקרים למאבק העיקש בהתקפות שמטרתן דינונימיזציה על הבלוקצ'יין. בזכות **Dandelion ++**, עסקאות מועברות בשבילים כבולים זה בזה באופן אקראי, או "כבלים", ואז מפוזרים במפתיע בין רשת גדולה של צמתים, כמו כמוסות פרחי שן הארי המפוצצות מגבעול (איור 1). זה כמעט בלתי אפשרי לעקוב אחר עסקאות למקור שלהם, וכמובן שבלתי אפשרי לעקוב אחרי IP שמהם הם נשלחו.

איור 1: אימות אנונימי של עסקאות בפרוטוקול Dandelion ++.

Dandelion ++ מעביר הודעות לאורך אחד משני נתיבים שזורים בגרף עם 4 רגיל ואז מתרגם אותם בעמצעות דיפוזיה.
באיור, העסקה מתפשטת בדרך הכחולה המודגשת [3]. תהליך זה מקשה מאוד על מעקב אחר עסקאות בדרך למקור שממנו הם נשלחו, ובכך שומר על סודיות.



[2] F2Caffyn, Grace, ***Chainalysis CEO Denies 'Sybil Attack' on Bitcoin's Network,*** 14 March, 2015, https://www.coindesk.com/chainalysis-ceo-denies-launching-sybil-attack-on-bitcoin-network

[3] Fanti, G, Venkatakrishnan, S B, Bakshi, S, Denby, B, Bhargava, S, Miller, A & Viswanath, P 2018, 'Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees', ***Proc. ACM Meas. Anal. Comput. Sys.***, Vol. 2, Article 29, pg. 8, https://www.readkong.com/page/dandelion-lightweight-cryptocurrency-networking-with4805755-?p=1

פרטיות של העסקה

הבלוקצ'יין של Epic Cash מבטיח פרטיות של העסקאות על ידי טשטוש סכומים ויחסי שולח-מקבל של עסקה .זה מושג באמצעות יישום רעיונות המוכרים מעסקאות סודיות *CT*[4] ו *CoinJoin*[5], שיטות בחלקן הגדול שפותחו על ידי גרגורי מקסוול Gregory Maxwell (מפתח Bitcoin Core, מייסד משותף ו- CTO של בלוקסטרים).

CT (עסקאות סודיות), שנוצרו במקור על ידי אדם ואחרי זה ושכללו אחר כך על ידי מקסוול, פועל על ידי חילוק העסקאות לחלקים קטנים יותר באמצעות הצפנה הומומורפית, שיטה לביצוע חישובים על מידע מוצפן מבלי לפענח אותו לראשונה לשמירה על הפרטיות. לאחר חלוקתם, הצופים לא יכולים לראות את הכמויות שיש בפועל בעסקאות בגלל גורמים שסנוורים אותם, על ידי מערכת שזורקת מספרים אקראיים לתערובת של שברי העסקה כדי להסתיר את הערכים של אותם שברים.

לאחר חלוקתם, הצופים לא יכולים לראות את הכמויות שיש בפועל בעסקאות בגלל גורמים שסנוורים אותם, על ידי מערכת שזורקת מספרים אקראיים לתערובת של שברי העסקה כדי להסתיר את הערכים של אותם שברים. בסופו של דבר, רק גורמים שפעילים בעסקה יודעים את הערך שלה, בעוד שהעסקה מאומתת על ידי הרשת באמצעות ההצהרה כי סכום ערכי הפלט שווה לסכום ערכי הקלט, וסכום הגורמים המסנוורים בפלט שווה לסכום מהגורמים המסנוורים בקלט.

כדי לסבך עוד יותר את המשימה של גורמי צד שלישי סקרניים, כל העסקאות Epic Cash מכוסות בעסקאות סודיות, ומשולבים זה בזה כדי להסתיר את הקשרים בין גורמים בעסקים. זה נעשה באמצעות הקונספט השני של מקסוול, CoinJoin.

כדי להמחיש את CoinJoin בפשטות, דמיין ש- A, B ו- C שולחים את הEpic Cash ל- X, Y ו- Z, בהתאמה. נשלח באמצעות CoinJoin, וכל מה שידוע הוא ש- A, B ו- C שולחים ו- X, Y ו- Z מקבלים, בעוד סכומי העסקה נשארים בלתי נראים.

מערכת CoinJoin היא בסיסית ל- Epic Cash באמצעות חתימות מצטברות לכיוון אחד (OWAS), המשלבות את כל העסקאות בתוך גוש אחיד לעסקה יחידה.

פרטיות: סיכום

ה- Blockchain של Epic Cash מגן על פרטיותם של אנשים ועל עסקאותיהם:

- **ביטול כתובות ארנק - בתוך הבלוקצין אין זיהוי מיקום של כספות דיגיטליים. והכי חשוב העסקאות מבוססות על "אדם לאדם" ועל בסיס "מארנק לארנק".**
- **פרוטוקול *Dandelion ++* - מסתיר את הנתיבים הדיגיטליים של העסקה מכתובת IP של שולח העסקה.**
- **עסקאות סודיות - מחלקים עסקאות למספר חלקים ומכניסים גורמים מסנוורים לאוסף אותם חלקים, כך שלא ניתן יהיה לדעת על ערכי החלקים ופרמטרים עסקיים אחרים.**
- ***CoinJoin* - משלב עסקאות לחבילות כדי להסוות את מערכות היחסים בין גורמים פעילים ובין העסקאות עצמם.**

[4] Maxwell, Gregory, ***Confidential Transactions,*** Technical Report (2015), https://people.xiph.org/~greg/confidential_values.txt

[5] Maxwell, Gregory, ***CoinJoin: Bitcoin Privacy for the Real World***, 22 August, 2013, post on Bitcoin Forum, https://bitcointalk.org/index.php?topic=279249.0

III. קישור

צ׳רלי לי, היוצר של לייטקואין, הצהיר, כי הקישור - היא המאפיין היחיד של כסף אמין, מה שחסר מאד גם בביטקואין וגם בלייטקואין, והכיר בכך, כי הסודיות וחליפיות הפכו לשדה קרב של המטבעות הללו [6]. אנדראס אנטונופולוס, אחד במומחים הגדולים בעולם בתחום הבלוקציין, אמר כי ״...מטבעות פגועים הם הרסניים. ואם אתה מפר את החליפיות והסודיות, אתה מפר והורס את המטבע.״[7]

קישור - הוא נכס של קבוצת טובין או נכסים שמבטיחה כי ליחידות הבודדות של קבוצה זו יש ערך שווה וניתן להחלפה ביניהן. זה מה שמבדיל בין צורות המטבע המוקדמות ביותר ממערכות סחר קודמות. כסף מאבד במהירות את התועלת שלו אם יש חוסר ביטחון בהחלפה שלו בדברים אחרים.

כפי שיפורט בהמשך, הפטריות של מרבית הקריפטו מטבעות אינה ודאית, בעוד שארכיטקטורת הפרטיות של Epic Cash מבטיחה שהיא אטומה לאותם איומים.

ניתן לעקוב אחר מרבית הקריפטו-מטבעות הדומים לביטקוין, לפי טבעם של מחסומי החסימה השקופים עליהם הם קיימים, דרך כל ארנק בו הם הוחזקו. צדדים שלישיים פרטיים וממשלות כאחד עוקבים אחר הבלוקציין של הביטקוין באמצעים מתוחכמים יותר ויותר לזהות במהירות מטבעות המשמשים בפעילויות אסורות קודמות. זה מוביל באופן טבעי לחששות שמא עלול יום אחד להיות אסור על עסקאות, ומותיר את מחזיקי הביטקואין בתום לב לאחר מכן בהפסדים גדולים.

ב- 19 במרץ 2018, הודיעה המשרד לבקרת נכסי חוץ של ארצות הברית (**OFAC**) כי היא שוקלת לרשום מטבעות דיגיטליים ברשימת הגופים הלאומיים המיועדים להם במיוחד (**SDN**), שהם אנשים איתם אסור על יחידים אמריקאיים וישויות משפטיות לסחור ולבצע עסקאות.

מדאיג עוד יותר, שOFAC אינו שולל הכללה של כתובות המאחסנות אותם.

כרגע הכנסת אחזקה של מטבעות נגועות ברשימת SDN, תביא באופן מקרי לבעלי מטבעות קריפו תמימים של ברשימה נגועה שחורה ופלילית בגלל שיוך של המטבעות הנגועים בבעלותם. זה הביא את הפרופסור למשפטים באוניברסיטת ניו יורק, אנדרו הינקס, להגיד, "להתראות קישוריות וחליפיות", וכי הציבור צריך לצפות ל"פרמיה על מטבעות שהוטבעו לאחרונה, או לייחס עדיף למטבעות נקיים שלא מעורבים בפלילים״[8].

בהתחשב בכל אלה, לא קשה לדמיין הפיכה בשוק הקריפטו ומורת רוח, או אפילו היעלמותם של הרבה מטבעות קריפטו שהוקמו. עם זאת, Epic Cash הוא אחד ממטבעות קריפטו מועטים אשר ימנעו מבעיה זו בזכות תכונות הפרטיות החזקות המתוארות במאמר זה. בשל הדרת היחסים בין היחיד לנכס, כמו גם אי האפשרות לקיים קישור יחסים ומעקב בין הצדדים לעסקה, מטבעות Epic לעולם אינם יכולים להיות קשורים לאדם או פעילות מסוימים. לפיכך, הערך של Epic הוא עצמאי למשתמש; עם זאת, Epic מספקת דרגה גבוהה של סודיות וביטחון, מה שיסבך משמעותית את יכולתם של התוקפים לתפעל מטרות פליליות, פיננסיות ופוליטיות.

> **״...מטבעות פגועים הם הרסניים. ואם אתה מפר את החליפיות והסודיות, אתה מפר והורס את המטבע.״**
>
> **אנדראס אנטונופולוס**

[6] Njui, John P, ***Charlie Lee: Litecoin (LTC) To Soon Have Confidential Transactions for Fungibility***, 29 January, 2019, https://ethereumworldnews.com/charlie-lee-litecoin-ltc-to-soon-have-confidential-transactions-for-fungibility/

[7] Carl T, ***Andreas Antonopoulos Says If Fungibility Is Not Fixed Bitcoin Could Be Attacked,*** 9 April, 2019, https://bitcoinexchangeguide.com/andreas-antonopoulos-says-if-fungibility-is-not-fixed-bitcoin-could-be-attacked/

[8] Hinkes, Andrew, Ciccolo, Joe, ***OFAC's Crypto Blacklist Could Change Crypto***, 24 March, 2018, https://www.coindesk.com/goodbye-fungibility-ofacs-bitcoin-blacklist-remake-crypto

IV. מדרגיות

Epic Cash -הוא יישום של MimbleWimble בלוקציין, אשר מספק מדרגיות בזכות תכנון מרחבי יעיל שמבטל נתוני עסקאות מיותרים.

הפונקציונליות של שיטת Cut-Through אחראית לכך מבטיחה כי הבלוקציין יחסוך מקום רב יותר לאורך זמן בהשוואה להרבה מטבעות קריפטו, כולל הביטקוין, וכי ניתן ליצור צמתים חדשים עם מינימום זיכרון וכוח עיבוד. שימוש יעיל בשטח יאפשר התארגנות של רשת מפוזרת מאוד וביזור. יתר על כן, למרות שעל כל צומת ביטקוין יש צורך לאחסן את כל הרשת, צמתים של Epic Cash מסוגלים לתרום לאבטחת רשת המבוססת על תת-קבוצה קטנה של בלוקים.

מרבית מטבעות דורשים מקום כמעט בלתי מוגבל כדי לאחסן את כל נתוני העסקאות בבלוקציין שלהם. רשת ביטקוין צומחת כיום במהירות של 0.1353 גיגה-בייט בכל יום, בעוד שרשת Ethereum צומחת בקצב מהיר עוד יותר של 0.2719 גיגה-בייט ליום.

אם שרשרת הביטקוין תמשיך לצמוח בקצב שכזה, אז עד 2140 - כאשר ייכרה הבלוק אחרון, גודלה יגיע לכ- 6 ט"ב.

גודל שרשרת Ethereum עד תאריך זה תעלה על 10TB.[9]

ברוב מחסומי החסימה שאינם משתמשים בפרוטוקול של MimbleWimble יש לאמת עסקאות על ידי צמתים(נודים) ברחבי העולם.

ככל שכמות הנתונים גדלה, העומס והנטל על כל צומת גדל.

אפילו ב -200 ג'יגה-בייט בלבד (הגודל המשוער של שרשרת הביטקוין הנוכחית), סינכרון הנתונים דורש רשת יציבה ויכולת קריאה וכתיבה של דיסק במהירות גבוהה מה שלא אפשרי תמיד.

כתוצאה מכך, הכרייה הופכת לריכוזית יותר, ומרכז הכרייה נעים לעבר בריכות גדולות שיכולות להרשות לעצמן להשתמש במשאבים מרכזיים יקרים. **אם כל ההיסטוריה של בלוקצ'יין הביטקוין הייתה נשמרת על ידי הבלוקציין של Epic Cash, אז הוא היה תופס 90 אחוז פחות מקום.** כעיקרון ככל שהבלוקציין קטן יותק הוא מהיר יותר, וכל עסקה תדרוש פחות זמן להעברה ולהגנה.

MimbleWimble בלוקציין פותר את המצב הקשה של ארגון אחסון נתונים בשיטה חדשנית לחיתוך בלוקים המכונה - "Cut-Through". כדי להבין טוב יותר כיצד עובדת שיטת הגזירה, כדאי לראות כיצד עסקאות וחסימות מורכבות בתוך MimbleWimble בלוקציין.

עודף:

ההבדל בין יציאות לבין הכניסות, בתוספת **חתימה** (בשביל אימות והוכחה של מחסור באינפלציה).

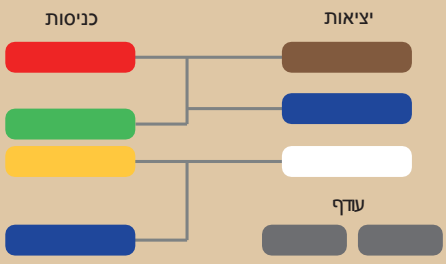
יציאות:

*יציאות של עסקאות חסויות ו- **rangerproofs***

כניסות:

קישורים לכניסות ישנות:

איור 2:
חלקי טרנזקציה של MimbleWimble.



כל הבלוקים של EpicCash מכילים בתוכם:

עצי מרקל של תפוקות העסקאות שנכנסות:

עצי מרקל של תפוקות עסקאות יוצאות ו-rangerproofs-

רשימת ערכים של עודפים וחתימות שלהם.

באיורים 2 ו -3, שהותאמו ממצגות של אנדרו פולוסטרה[10], אנו יכולים לראות מטבעות Epic שנכרו לאחרונה, המוצגים כתאי קלט לבנים. תאים צבעוניים זהים מייצגים תפוקות עם תשומות שהוצאו בהתאמה. הודות לתהליך הקיצוץ, נמחקות התשומות והתפוקות המשומשות התואמות שלהם כדי לפנות שטח בבלוק, מה שמקטין את כמות הנתונים שצריך לאחסן בבלוקציין בתהליך של אי-הכללת עסקאות מהרישום, והגרעינים שנותרו מיותרים)100 סך הכל(, מתעדים כל הזמן כי העסקאות הושלמו.

זה שונה מאוד מהבלוקצ'יין של הביטקוין, בו כל צומת חייב לאחסן את הבלוקציין המלא. עם הזמן, כאשר היעילות המרחבית של בלוקצ'יין Epic Cash עולה לעומת הבלוקציין של הביטקוין, עלות האפקטיביות של השתתפות הצמתים ברשת Epic Cash תגדל גם היא. הפחתת חסמי ההשתתפות תעזור להבטיח חוסן קריטי ברמת הצומת ובעיצוב רשת.

כאשר ממשיכים להיווצר בלוקים, MimbleWimble משתמש בשיטת Cut-Through עבור בלוקים; בסופו של דבר, כל שנותר לטווח הארוך הוא רק כותרת חסימות(כ-250 בתים), יסקאות שלא הוצרו וגרעיני עסקאות(כמאה בתים) .

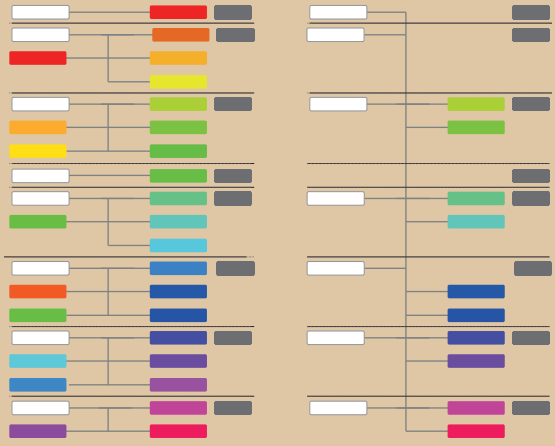
בעזרת הדוגמה של Grin, היישום השני של MimbleWimble שהושק, ניתן לראות כי הגודל הכולל של רשת MimbleWimble עם אותו מספר עסקאות כמו רשת הביטקואין הוא רק 10% מהגודל הכולל של רשת הביטקואין[11]. יתר על כן, גודל הצומת יהיה "בסדר גודל של מספר גיגה-בייט עבור רשת הביטקוין וניתן יהיה לייעל אותה עד כמה מאות מגה-בייט"[12].

הודות ליישום MimbleWimble והקטנת הרשת באמצעות תהליך Cut-Through, ובלוקציין Epic Cash מציע מדרגיות, שלעתים קרובות מתעלמים מקהילת הקריפטו. Epic Cash משרתים את המטרה שבשבילה נבנה הביטקוין ופרויקטים דומים בעבר: ביזור. לא משנה כמה עסקאות בשנייה מטבע יכול לעבד, מה מועיל אם הוא אינו נתמך על ידי רשת רחבה והטרוגנית?

אם דרישות הזיכרון הן כאלה שתוקף בסופו של דבר יילך לכיוון תאגידי כרייה חזקים, אז כל המאמצים של קהילת הקריפטו ליצור מערכת מבוזרת יהיו חסרי תוחלת. כדי לספק רוחב פס נוסף, תוכנית הפיתוח של Epic Cash כוללת יישום Tier2 בסגנון Lightning כמטרה לטווח קצר.

איור 3:
MimbleWimble לפני ואחרי Cut-Through. עסקאות

בנטרול עסקאות קיזוז



[9] Li, Crypto, ***Blockchain's Big Data Problem,*** 27 January, 2019, https://www.longhash.com/news/blockchains-big-data-problem

V. מדיניות מוניטרית

המדיניות המוניטרית של Epic Cash וביטקוין דומה מאוד. מלאי התפוצה של Epic Cash יגדל תחילה די מהר, ובשנת 2028 הוא ייסונכרן עם מלאי התפוצה של הביטקוין. לאחר מכן, שיעור ייצירת Epic Cash יגיע לכמות המירבית של 21 מיליון Epic בשנת 2140. Epic Cash הוא מאגר כספי בעל ערך לטווח הארוך, מכיוון שמלאי התפוצה ידוע בכל זמן מסויים במהלך מחזור החיים של ההנפקה, ובעל ייתרה של מטבעות מקסימאלית קבועה. המדיניות המוניטרית של Epic Cash מאופיינת ב-4 תכונות הבאות:

- במהלך 9 השנים הראשונות של מחזור החיים, תתרחש הנפקה מהירה; במהלך מחזור זה ייכרו 20,343,750 Epic (96.875% מכלל הכמות). נתוני ההנפקה המדוייקים מצויינים בחלק של תרשים ההנפקה בהמשך.
- המלאי הכללי ושיעור ההנפקה של Epic ייסונכרנו עם הביטקוין בנקודת סינגולריתי של Epic סביב 24 במאי 2028. לאחר שתושג סינגולריות, שיעור ההנפקה יתחיל לרדת במהירות גוברת, ואילו מלאי התפוצה יגדל במהירות פוחתת.
- ההנפקה המירבית הכוללת - 21 מיליון מטבעות Epic - תושג עד 2140, זה יקרה בערך באותו הזמן, שהביטקוין יגיע לכמות המירבית שלו של 21 מיליון יחידות.
- ל-Epic מבנה חלוקה של עד 8 מקומות עשרוניים אחרי הנקודה - בדומה לביטקוין. 1 Epic שווה ל-100,000,000 פרימן(באופן דומה, ביטקוין שווה ל 100,000,000 סטושי).

המדיניות המוניטרית של Epic Cash מעוצבת בדומה לביטקוין מהסיבות הבאות:

- הציבור כבר מכיר את מודל הביטקוין ואת המוניטין המוכח של הביטקוין בעשר השנים האחרונות מאז הקמת הביטקוין.
  לאחר סינכרון בערך עם מלאי התפוצה של ביטקוין ושיקוף המלאי המרבי של ביטקוין ומבנה ההתחלקות, Epic הולכת בדרך של הכי פחות התנגדות לאימוץ המוני.
- הסכימו ליסודות הכלכליים של ביטקוין - כלומר, שמירת הערך מבוססת על הגירעון של המטבע והחיזוי של הון חוזר.

VI. לוח-זמנים של שינוי ההיצע

ל-Epic Cash סך הכל 33 תקופות כרייה, כאשר בכל אחת מהם מתבצעת ירידה בתקבולים לבלוק ביחס לעידן הקודם. בלוק ההתחלתי של Epic- התאריך בו כריית בלוק # 1 התרחשה - לאוגוסט 2019. בדקה אחת ייכרה בלוק אחד בלבד. ב-5 העידנים הראשונים, ייכרו בערך 97% מהכמות הכללית של Epic .
ייצירת Epic במשך 9 השנים הראשונות יהיו שווים בערך לכמות הכללית של הביטקוין שנכרה במשך 20 שנה .
אפשר לראות בכך "הזדמנות להחזיר את הגלגל לאחור" עבור מי שפספס את הצמיחה המרשימה של הביטקוין.

לוח שינוי ההיצע בטבלה 1 מציג את תאריכי ההתחלה והסיום של 7 תקופות הכרייה הראשונות, תקופת תגמול הבלוק המתאימות לכל תקופה, ואת עתודת המחזור העוקבת לכל תקופה נתונה. בשביל הקיצור, עידני מ 8 עד 33 אינם כלולים בטבלה.

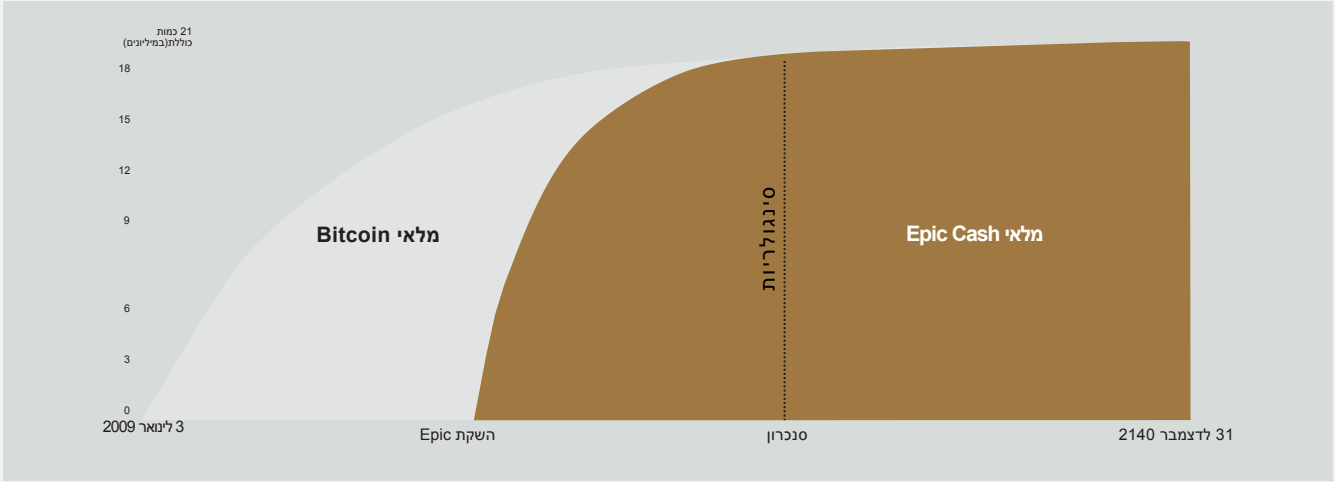
די להבין שעבור תקופות אלה, תגמול לכל בלוק יהיה שווה למחצית בדיוק מכמות התגמול שהתרחשה בעידן הקודם (כמו גם בביטקוין). מספר מטבעות Epic שהונפקו במהלך כל עידן יהיה שווה לסכום התקבולים לכל בלוק בעידן של 4 שנים(כ-1,460 יום).

כשתגיע הסינגולריות (2028), מלאי המחזור של Epic יהיה כמעט זהה למלאי התפוצה של הביטקוין, לאחר מכן Epic Cash יקבל את תגמול לבלוק וחילוק תגמול בדומה לביטקוין, בו יש **חילוק תגמול** לבלוק כל 4 שנים. היוצא היחיד מן הכלל הוא שבלוקי Epic ימשיכו להיות מיוצרים כל ידי כרייה במהירות של בלוק אחד לדקה(בלוק הביטקוין נכרע במהירות של 1 בלוק כל 10 דקות). כתוצאה מכך מלאי התפוצה של Epic יתאים בערך לצלאי התפוצה של הביטקוין.

טבלה 1: תרשים יצירת המטבעות ב7 עידני כרייה ראשונים. התאריכים משוערים.

עידן	1	2	3	4	5	סינגולריות	6	7
תגמול לכל בלוק	16	8	4	2	1		0.15625	0.078125
תאריך התחלה	1, באוגוסט 2019	29 ביוני, 2020	11 באוקטובר, 2021	3 ביוני, 2023	10 באוגוסט, 2025		24 במאי, 2028	22 במאי, 2032
תאריך סיום	29 ביוני, 2020	11 באוקטובר, 2021	3 ביוני, 2023	10 באוגוסט, 2025	24 במאי, 2028		22 במאי, 2032	20 במאי, 2036
אורך (בימים)	334	470	601	800	1019		1460	1460
כמות התחלתית	0	7,695,360	13,109,760	16,571,520	18,875,520		20,342,880	20,671,380
כמות מירבית	7,695,360	13,109,760	16,571,520	18,875,520	20,342,880		20,671,380	20,835,630
% מהכמות הכוללת	36.6%	62.4%	78.9%	89.9%	96.9%		98.4%	99.2%

איור 4: תרשימי ייצירה של Epic ושל Bitcoin



VII. כרייה

בלוקציין Epic Cash מספק ביזור בגלל העובדה שניתן לבצע כרייה על מגוון רחב של ציוד מחשוב. כריית Epic זמינה בתחילה במעבד CPU , GPU ו-ASIC, תוך שימוש בשלושה אלגוריתמים של גיבוב, בהתאמה: RandomX, ProgPOW ו- CuckAToo+. ניתן להחליף את האלגוריתמים בצורה טריוויאלית "במצב חם" מבלי לפגוע בשלמות המעגל.

1 CPUs ו RandomX

- RandomXאלגוריתם הוכחת עבודה (POW), המותאם למעבדים כלליים. הוא משיק באופן אקראי תוכנית לטעינת זיכרון כבדה (שיטת memory-hard) מה שמאפשר להשיג כמה יעדים:

• מניעת פיתוח שבבי ASIC חד-שבביים.
• מזעור יתרונות הביצועים של ציוד מיוחד על פני מעבדי CPU שנבנו למטרה כללית.

בשביל כריית Epic במעבד נדרשת הקצאה קבועה של 2 ג'גה-בייט של זיכרון RAM פיזי, 16 ק"ב של זיכרון קש ברמה הראשונה L1, 256 ק"ב של מטמון ברמה L2, ו -2 מגה-בייט של מטמון ברמת L3 עבור זרם הכרייה [13]. התקני Windows10 דורשים זיכרון של 8 גיגה-בייט RAM או יותר. יתכן שמתישהו בעתיד הקרוב, טלפונים ניידים יהפכו לצמתי כרייה ברי-קיימא. שילובו המוקדם של המעבד CPU לרשת הכרייה של Epic Cash הוא הזדמנות מצוינת עבור רבים שיש להם רק משאבי מחשוב צנועים לקבל תגמול הולם בהגנה על אבטחת הרשת של Epic Cash.

2 GPUs ו ProgPow

תוכנת הוכחת העבודה של Proof-of-Work (ProgPow), אלגוריתם התלוי ברוחב הפס הזיכרון ובחישובים בסיסיים של רצפים מתמטיים אקראיים; הוא מנצל את פונקציות המחשוב הרבות של ה-GPU ובכך למעשה חוסך את צריכת החשמל הכוללת של החומרה. מכיוון ש-ProgPow תוכנן במיוחד על מנת לנצל את מלוא השימוש ב-GPUs המקובלים, קשה ויקר להשיג יעילות גבוהה משמעותית באמצעות ציוד מיוחד. לפיכך, אלגוריתם ה-ProgPow מחליש את התמריץ לבריכות ASIC גדולות להעמיס GPU, אשר לרוב ניתן לראות באלגוריתמי POW רבים אחרים, כמו 256-SHA עבור ביטקוין. אם כי GPUs אינם נפוצים כמו מעבדים, הם עדיין פופולריים למדי. בזכות ההתפתחות הטכנולוגית שאנו עדים לה ביחס ל-Nvidia ו-AMD, GPUs יכולים במקביל לעבד פתרונות כרייה רבים, מה שמשווה אותם עם ה- לCPU. זה בגלל השילוב שיש בין נגישות וכוח מחשוב גבוהה ש-GPUs יהפכו לבסיס לקוב פעולות הכרייה בתקוות הראשונות, כפי שמוצג בטבלה מספר 2.

3 CuckAToo+31 ו ASICs

+ CuckATo31הוא שינוי אלגוריתם ידידותי ל- ASIC של האלגוריתם Cuckoo Cycle, שפותח על ידי המתכנת ההולנדי גון טרומפ. קרוב משפחה של האלגוריתם העמיד לASIC, CuckARoo29-, אלגוריתם CuckAtoo31+ מייצר גרפים דו-חלקיים אקראיים ומספק לכורים את המשימה למצוא לולאה באורך נתון "N" העוברת בקודקודי הגרף הזה.

[13] Tevador, ***RandomX***, 28 March, 2019, https://github.com/tevador/RandomX

זו - משימה הקשורה לשימוש בזיכרון; זמן ההחלטה תלוי ברוחב הפס של הזיכרון, ולא במהירות המעבד או ה- GPU. כתוצאה מכך, אלגוריתמי Cuckoo Cycle גורמים לפחות חום וצורכים פחות אנרגיה משמעותית מאלגוריתמי ה- POW המסורתיים. תואם ל- ASIC +Cuckatoo31, מאפשר לשפר את הביצועים על פני GPUs באמצעות מאות מגה-בייט SRAM, שהם צוואר הבקבוק ל I/0 זכרון [14].

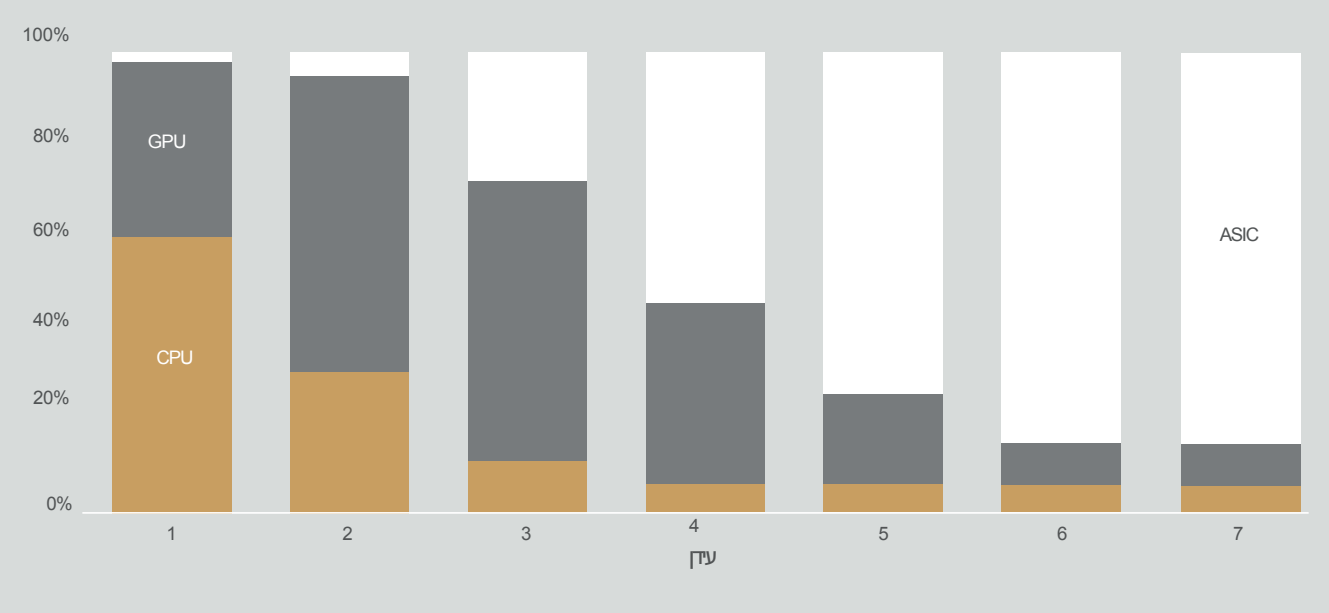
בסופו של דבר, ASIC מציעה את החיסכון הפוטנציאלי הגדול ביותר באמצעות שלוש אפשרויות כרייה.

לצורך אינטגרציה, בשלבים המוקדמים ASIC יקבלו חלק קטן מהתגמול עבור הכרייה לעומת ה-CPU וה-GPU; בעתיד, ASICs יקבלו חלק ניכר מתגמול הבלוק בתנאי שיש מערכת אקולוגית תחרותית של יצרני מכשירים עבור CuckATOo31+.

טבלה 2: חלוקת תגמולי הכרייה. להיבדק. אפשרויות ההפצה יכוונו להשיג ביזור מירבי בהתאם לאינטרסים לטווח הארוך של הרשת.

עידן	1	2	3	4	5	6	7
ימים	334	470	601	800	1019	1460	1460
CPUs	60%	30%	10%	5%	5%	5%	5%
GPUs	38%	65%	62%	40%	20%	10%	10%
ASICs	2%	5%	28%	55%	75%	85%	85%

איור 5: חלוקת תגמול הכרייה לכל עידן לפי טבלה 2. בכפוף לשינויים.



[14] Le Sceller, Quentin, *An Introduction to Grin Proof-of-Work,* 16 November, 2018, https://blog.blockcypher.com/an-introduction-to-grin-proof-of-work-103aaa9f66ce

4 תרומות מהכרייה

החל מהסימן של הבלוק הראשון של 2019(Epic(ועד לסיום הסינגולריות הייחודיות של 2028(Epic), במהלך יישום תהליך הכרייה, יוקצה אחוז מסוים מהכרייה (תרומת מכרייה) לקרן ה- Blockchain EPIC.

קרן הבלוקציין של EPIC הוקמה על מנת להבטיח פיתוח טכני וקידום פרויקט Epic Cash בשנים הראשונות לקיומו בזכות יישום פעילויות שיווק ופיתוח שותפויות בענף הטכנולוגיה הפיננסית.

לאחר הסינגולריות, תאגיד האוטונומי המבוזר EDAC ייקח על עצמו את תפקיד של קרן ה-EPIC, את התאגיד יפתח הקרן לצורך העברת פונקציות.

קרן הבלוקציין של EPIC תמומן מאחוז מסוים מהפרס לכריית הבלוקים שנוכה מתגמול הבלוק הכולל בהתאם לשיעורים השנתיים הבאים:

טבלה 3: שיעורים שנתיים של תרומות הכרייה לקרן - אחוז מהתגמול בגוש הכרייה.

שנה	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
מתגמול הכרייה לכל בלוק %	8.88 %	7.77 %	6.66 %	5.55 %	4.44 %	3.33 %	2.22 %	1.11 %	1.11 %	0 %

VIII. סיכום

Epic שואף להפוך ל"כסף דיגיטלי מבוזר" מוכר, אמצעי חילופין, אנלוגי למעמדו המוכר של ביטקוין כזהב דיגיטלי מבוזר. על ידי הכנסת החליפיות האבודה לתחום החומרה הוא הרבה יותר חסכוני באנרגיה וידידותי לסביבה, Epic Cash משנה את מאזן הכוחות לטובת משתמשים בודדים, המנוגדת בחדות למגמות הריכוזיות האחרונות. השילוב בין הכלכלה של ביטקוין, תורת המשחקים ונוסחה מוכחת להוכחת עבודה עם מיטב טכנולוגיות הבלוקצ'יין המודרניות, מוביל ליצירת מטבע אמין, בלתי משתנה ומבוזר, הניתן להרחבה, להחלפה ושומר על פרטיות המשתמשים. בלוקציין Epic Cash הוא פתוח, פומבי, חסר גבולות ובעל עמידות לצנזורה. הוא שומר על פרטיותם וערכיהם של המשתמשים שלו ומתגמל את המשתמשים המשתמשים בציוד שלהם כדי לתמוך ברשת באמצעות כרייה. כל מטבע Epic נכרה באמצעות POW. ייצירת מטבעות חדשים מתחילה מאפס)ללא כרייה מוקדמת(, כך שההשקה של הרשת מאורגנת בצורה הוגנת; עכשיו עובדת הרשת בבדיקות פונקציונליות.

עובדות עיקריות על Epic Cash :

- **הכרייה מתחילה ב -באוגוסט 2019 .**
- **הבלוקציין של Epic Cash מבוסס על MimbleWimble.**

התכונות המגדירות את הפרוטוקול הן:

1. **Cut-Through -** הסרת מידע מיותר מהבלוקצ'יין כדי להגביר את היעילות של השימוש במקום שלו, עידוד השתתפות רחבת היקף בתיקוף רשת ובניהול ביזור נכון.
2. **CoinJoin -** איחוד עסקאות בבלוק אחד כדי להבטיח חליפיות של מטבע הקריפטו Epic.
3. **פרוטוקול Dandelion++ -** חלוקת עסקאות באמצעות מעבר בין ערוצים שזורים זה בזה והפרדה דרך רשת רחבה של צמתים, מה שמוביל לניתוק הקשר בין עסקאות למקורם.
4. **אין כתובות ארנק -** באמצעות רב-חתימות גדולה נוצרים מפתחות סודיים (פרטיים) חד פעמיים לביצוע עסקיות, מה שמבטל לחלוטין את הצורך בשימוש בכתובות ארנק.

- **המדיניות המוניטרית של Epic Cash** נועדה לסנכרן את מלאי של Epic ומלאי התפוצה של ביטקוין בעוד כ-9 שנים, ולהשיג כמות ייצור מקסימלית יחד עם הביטקוין- ב 2140. מדיניות דפלציונית זו מבטיחה שקיפות, חיזוי ייצירת מטבעות חדשים וצחסור שלהם, מה שתורם לביטחון האחסון ושמירה בערך לטווח ארוך.

- **כרייה** המשלבת את ה-CPU, GPU, ו-ASIC באמצעות האלגוריתמים מתאימים, RandomX, ProgPOW, ו- CuckAtoo31++ כדי להקל פריסה המונית ויעולות מירבית של הרשת.

IX. מפרט טכני

שם הפרוייקט: EpicCash
שם המטבע: Epic
זמן בין הבלוקים: 60 שניות
גודל הבלוק: 1MB
כמות התחלתית: 0
כמות סופית: 21,000,000
בלוק ראשון: לאוגוסט, 2019
קונצנסוס: RandomX (CPUs), ProgPow (GPUs) ו CuckAToo31+ ASICs

קישורים:

www.epic.tech

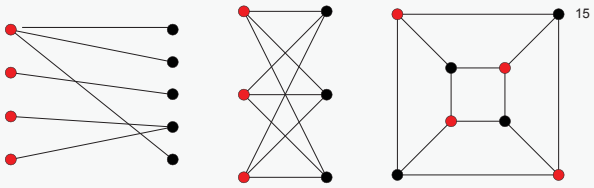
טלגרם – t.me/EpicCash

t.me/EpicCashHebrew

X. מילון מונחים

ASIC מעגלים משולבים למטרות מיוחדות; שבבים המיועדים למטרה אחת.

גרף דיקוטילוני קבוצה של קודקודי תרשים מפורקת לשתי קבוצות לא משותפות, כך שאף אחד מקודקודים של הגרף בתוך אותה קבוצה אינם סמוכים .



גורם מסנוור אלמנט אקראי שהוצג בהודעה דיגיטלית כדי להקל על ההצפנה; סוד נפוץ בין שני הצדדים, המשמש להצפנת נתוני קלט ופלט של עסקה מסוימת, כמו גם מפתחות ציבוריים ופרטיים (פרטיים) של צדדים עסקיים[16].

תגמול תמורת בלוק מטבעות Epic חדשים שהופצו על ידי הרשת כתגמול על חישובים שבוצעו לצורך אימות העסקאות בבלוק חדש.

זכרון מטמון רכיב חומרה או תוכנה המאחסן נתונים כך יכול לקבל שירות מהיר יותר בבקשות עתידיות לנתונים אלה.

מלאי מחזור המטבע מספר המטבעות Epic הקיימים בזמן הנתון הזה.

CPU יחידת עיבוד מרכזית: רכיב מחשב שאחראי על פרשנות וביצוע של מרבית הפקודות מחומרה ותוכנה למחשבים אחרים.

Cut-Through תהליך בלוקציין MimbleWimble בו נמחקות הכניסות והיציאות שמשומשות כדי לפנות שטח בבלוק, מה שמקטין את כמות הנתונים הדרושה לאחסון בבלוקציין.

ביזור מצב פיזור וחוסר מרכז אחד ביחס לפעולות וניהול ברשת.

יצירת מטבעות חדשים יצירת מטבעות Epic חדשים שהכורים קיבלו כפרס בלוק. מטבעות Epic נוצרים כל 60 שניות לאחר האישור של העסקה בבלוקציין.

הסינגולריות של Epic 2028 הנקודה בה יהיה סנכרון של מלאי מחזור Epic עם מלאי מחזור הביטקוין (מאי 2028).

עודף(MimbleWimble) ההבדל בין כניסות ליציאות, פלוס חתימות (לצורך אימות והוכחת חוסר אינפלציה).

חליפיות זהו מאפיין של מוצר או חומר גלם שבהם יחידות ניתנות להחלפה למעשה, וכל חלק ניתן להחלפה עם חלק אחר.

בלוק ראשון(אירוע) כריית הבלוק הראשון של Epic וההתחלה הרשמית של הבלוקצ'יין.

GPU מעבד גרפי: בלוק המכיל שבב (מעבד) שניתן לתכנות המיועד להציג פונקציות. מה שמתאים היטב לכריית מטבעות קריפטו.

חילוק(בשביל ביטקוין) קורה כל 4 שנים. רמת ההיצע מופחתת ב- 50% לאחר כל אירוע חצייה.

גיבוב ערך המחושב על בסיס מספר קלט בסיס באמצעות פונקציית.

אלגוריתם גיבוב (פונקציה) אלגוריתם מתמטי שממיר נתונים בגודל שרירותי לגודל קבוע, המשמש לייצור ואימות חתימות דיגיטליות, קודי וצורות אימות אחרות (MAC)ואימות הודעות.

הצפנה הומומורפית שיטה לביצוע חישובים של מידע מוצפן ללא פענוח מקדים (בתכנות).

Immutability מטבעות Epic חדשים שהופצו על ידי הרשת כתגמול על חישובים שבוצעו לצורך אימות העסקאות בבלוק חדש.

כניסה(MimbleWimble) רכיב הטרנזקציה של MimbleWimble המייצג את הצד השולח של העסקה; נוצר מכניסות של עסקאות קודמות.

I/O קלט / פלט; האינטראקציה בין מערכת לעיבוד מידע, כגון מחשב, לבין העולם החיצון, אדם או מערכת אחרת בשביל עיבוד מידע.

[15] http://mathworld.wolfram.com/BipartiteGraph.html

[16] Macdonald, Andrew, ***Grin Coin and MimbleWimble: An Introductory Guide***, 18 October, 2018, https://cryptobriefing.com/grin-coin-mimblewimble-introduction/

מלאי מקסימאלי	מספר המטבעות Epic שלאחריהם ההיצע במחזור כבר לא יגדל(Epic 21,000,000).
Memory-Hard	שימוש בכמות גדולה של זיכרון RAM כדי למנוע ניסיונות בו זמנית להתחיל חיבורים מקבילים. פונקציות קשיחות בזיכרון הן אלגוריתמים שזמן החישוב נקבע בעיקר על ידי הזיכרון הזמין בשביל לאחסן נתונים.
עץ מרקל	מבנה נתונים המשמש ביישומי מדעי המחשב. על רשתות בלוקציין, עצי מרקל מספקים אימות יעיל ובטוח של תוכן במבני נתונים גדולים.
MimbleWimble	פרוטוקול, שהגיש המחבר תחת הכינוי Tom Elvis Jedusor, בצ'אט מפתחי הביטקוין.
ריבוי חתימות	ערכת חתימה דיגיטלית המאפשרת לקבוצת משתמשים לחתום על מסמך אחד. ככלל, האלגוריתם יוצר חתימה אחידה שהיא קומפקטית יותר מקבוצה של חתימות נפרדות מכל המשתמשים[17].
נודה	מחשב שמתחבר לרשת בלוקציין ומתפזר לצמתים אחרים ברשת, להפצת נודים של מידע על עסקאות ועל בלוקים שיש בבלוקציין.
חתימה מצטברת לכיוון אחד(OWAS)	חתימת עסקה, המורכבת מחתימות רבות (סיגנטור) המוצפנות בצורה כזו שקשה מאוד לחשב את החתימות האישיות בנפרד שהן חלק מהכלל.
יציאה(MimbleWimble)	רכיב הטרנזקציה של MimbleWimble, שהוא קלט העסקה ומשמש כקלט לעסקאות עוקבות אחריו.
תרשים התחייבות של פדרסן	פרימיטיב קריפטוגרפי המאפשר לאמת לתקן את הערך שנבחר מבלי לחשוף מידע כלשהו אודותיו ומבלי שהמאמת יוכל לבטל את קיבוע הערך.
(מפתח (סגור) פרטי	פיסת קוד קטנה, שבשילוב עם מפתח ציבורי, משמשת להפעלת אלגוריתמים של הצפנת ופענוח טקסט. זה נוצר כחלק מקריפטוגרפיה של מפתח ציבורי במהלך הצפנה א-סימטרית, ומשמש לפענוח והמרת ההודעה לפורמט קריא.
Proof of Work (PoW)	פיסת נתונים שקשה ליצור (יקרה וגוזלת זמן) ליצירה, אך קלה לבדוק לאחרים ואשר עומדת בדרישות מסוימות. הוכחת עבודה(POW) משמשת לעיתים קרובות בעת ייצור בלוקים של קריפטו.
(מפתח (פתוח) ציבורי	המפתח הציבורי נוצר בקריפטוגרפיה של מפתח ציבורי באמצעות אלגוריתמים להצפנה עם מפתח אסימטרי. מפתחות ציבוריים משמשים להמרת הודעה לפורמט שלא ניתן לקרוא.
(זיכרון גישה אקראי) RAM	שבבי גישה מהירה לאחסון נתונים בהם מאוחסנת מערכת ההפעלה, תוכנות יישומים ונתונים המשמשים כעת; הודות לכך, המעבד יכול לקבל גישה מהירה לנתונים.
Rangeproof	אימות התחייבות המוודא כי סכום קלט העסקה גדול מסכום תפוקת העסקה וכי כל ערכי העסקה חיוביים. עמידות רמה מבטיחה כי לא נפגעו בפליטות הכספיות.
חתימה(דיגיטלית)	חתימה(דיגיטלית) היא חלק סטנדרטי בפרוטוקול, המשמש בעיקר להגנה על עסקאות וחסימות עסקאות, העברת מידע, ניהול חוזים ולכל מקרים אחרים בהם חשוב לאתר ולמנוע התערבות חיצונית כלשהי. הוא מספק שלושה יתרונות של אחסון והעברת מידע על הבלוקצ'יין: זה מציין אם טיפלו בנתונים שנשלחו ושינו אותם בודק את השתתפותו של גורם מסוים בעסקה עשוי להיות בעל כוח משפטי
(גישה אקראית סטטית) SRAM	זיכרון גישה אקראית(RAM), המאגר ושומר פיסות נתונים בזיכרון שלו כל עוד ישנה אספקת חשמל.
תפוקה אפשרית	מספר העסקאות בשנייה שניתן לבצע על ידי פרוטוקול הקריפטו הזה.
Trustlessness(ללא צורך באמון)	האיכות של רשת בלוקציין המאפשרת לך לעקוב אחר כללי הפרוטוקול ללא כפייה של הרשות המרכזית שלו.

[17] Bellare, Mihir, Neven, Gregory, 2007, ***Identity-based Multi-signatures from RSA***, Lecture Notes in Computer Science vol. 4377, https://link.springer.com/chapter/10.1007%2F11967668_10

EPIC CASH

EPIC PRIVATE INTERNET CASH