תוכנה 1

שחר פרץ

4 בנובמבר 2024

RANDOM STUFF ..... (1)

1.1 על טל

- טל פרנג'י – קו"ח מרצועיים
- בומר
- אוהב bitcoin
- תחרות הסמסטר – מי קורה יותר מטבעות קריפטוגרפיים

מנהל פיתוח, מהנדס בכיר בגוגל, סמנכ"ד פיתוח של חברת מידע פיננסי קטנה, 7 שנים יועץ ב־big-data, לימד כאן במשך שלוש שנים. כרגע ראש צוות מהנדסים ב־ebay שמייעץ בנודע ל־AI.

מעבר על דרכים לעשות אלגוריתם פשוט של חלוקת string למילים.

1.2 דברים כלליים

מבחן אמצע סמסטר ־ 30.12. אמצע שנה – 2.5, 16.2.

1.3 מה אנחנו נעשה

(במסגרת הפרויקט). נבנה רשת של כריית מטבעות (מטבעות וירטואלים בשם דמי חנוכה).

1.4 דלית

הציונים יגיעו (לא היום). "מתי הכי מוקדם זה יפורסם?" "זה יפורסם אל תדאג". **לא למתוח את הגבולות של הגשת התרגילים**. אם דברים נהיהים לחוצים, אז אפשר לפנות לדלית. תרגילים יהיו כל שבוע. לעשות משימות של הפקולטה בקורס של תוכנה 1. לא להניח הנחות – לשאול את דלית או את פרנג'י. העתקות, בעיות בתרגילים ועוד – הן בעיות שיש לסטודנטים בתוכנה 1 ובמבני נתונים. (אני באופן אישי לא אעלה פתרונות).

המרה לבגרות – כרגע חסרים 30% – 10 על בדידה 2 ו־20 על ליניארית. כשהכל יגמר, אז נקבל אישור לזכאות להמרה. לציונים לוקח המון זמן להתעדכן (אבל נדע לחשב אותו לפני כן). רישמית, אסור לתת פטורים (למרות שבתי ספר מאפשרים). לא למתוח גבולות מבחינת בית הספר. רישמית, מותר לשחרר לאחר 70% המרה ולאחר י"א.

BITCOIN ..... (2)

כל הנאמר שנוי במחלוקת. אל תרוצו לקחת כסף מאמא לקנות ביטקוין. תפקיד הכסף:

- אכסון ערך
- יחידת חליפין (מסחר)
- יחידות חישוב מחיר אחידה
- ולאחרונה – לאפשר קניית מוצרים אלקטרוניים.

מראים שהציוויליזציות התחילו באמצעות בהן גידלו דגנים שאפשר לשמר.

מסחר התחיל בהחלפת סחורות. כסף מאפשר חלופה לזאת. יחידת המידה המקובלת בעולם כיום היא הדולר האמריקאי. הזהב שימש כמטבע האוניברסלי כבר 5000 שנה. באיזשהו שלב הבנקים החליטו שהם מחזיקים זהב אצלם, המגבה את הכסף, בצ'קים שהם נותנים. ב־1971 ניקסון הכריז כי ארה"ב מתנתקת מתקן הזהב (כלומר הבנק לא חייב להחזיק הזהב כנגד כל דולר). בכך, הסחורות התנתקו מסחורה ממשית. מדינות אחרות מיהרו לעשות דברים דומים. המצב הנוכחי הדפיס 9T דולר (כלומר, הוא מוכר אגח"ים למדינות אחרות ומקבל דולרים. זהו החוב של הבנק).

"כסף הוא דת" – הוא לא קיים אם לא מאמינים בו. אין ערך למה שבארנק אם לא תסכים לקבלו כסחורה.

בנק הוא למעשה רשיון להדפסת כסף. הבנק צריך להחזיק רק 10% מכל ההלוואות הוא נותן – הוא יצר פי 10 מזה "מהאוויר". ההנחה היא שלא כולם מוציאים כסף בבת אחת.

2.1 תכונות של כסף

- נדירות
- עמידות
- ניתן לחלוקה
- קשה לזיוף
- קל להעברה
- חוסר ייחוד (קילו אחד של זהב = קילו אחר. לא כמו יהלומים)

ביטקוין יותר טוב מזהב

- **נדירות** – כמות הביטקויינים החדשים קטנה בחצי כל 4 שנים. בשנת 2140 לא יהיה ניתן לכרות יותר (מטבע דיפלציוני - הערך תמיד עולה, לעומת מטבע אינפציוני שאפשר להדפיס ממנו עוד)
- **עמידות** – למטבע אלקטרוני אין שחיקה
- **ניתן לחלוקה** – ביטקוין ניתן לחלוקה 8 ספרות אחרי הנקודה. עד מאית מיליונית היטקוין. גם אם הוא יהיה שווה מיליון דולר, יהיה אפשר להעביר סנט.
- **קשה לזייף** – אי אפשר להדפיס ביטקוין מזוייף. הוא מוגן קריפטוגרפית בבסיס נתונים שמשוכפל על אלפי מחשבים.
- **קל להעברה** – לא צריך להעביר דבר פיזית.
- **חוסר ייחוד** – יש בעיה. הביטקוין שומר את היסטוריית הטקנסזקציות. יש מטבעות שמנסים להעלים את זה.

2.2 טכנולוגיה

מפתח ציבורי, גיבוב קרפיטוגרפי (הטכנולוגיה המאפשרת כרייה) וה־blockchain – הטכנולוגיה המאפשרת חוסר תלות בבנק. היום גודלו 40GB.

CRYPTOGRAPHY . . . . . (3)

ביטקוין משתמש בשתי שיטות קריפטוגרפיה שפותחו ב־20 השנה האחרונות. הראשונה – הצפנה עם מפתח פרטי/ציבורי, והשנייה – פונקציית גיבוב (hash function). ("או שזה גיבוב של שטויות").

חתימה אלקטרונית – כל העולם יכול להשתמש במפתח הציבורי ובכך יכול להבין מה המידע. בכך נוכל לאמת שבעל המפתח הפרטי הוא באמת היוצר של הקובץ.

פונקציית האש קריפטוגרפית (לא "סתם" כזאת של מבנה נתונים) בעלות התכונה שקשה לייצר שתי הודעות בעלות אותו ה־hash.

מחוץ להקשר של ביטקוין – בגלל שזהו שימוש "כבד" יחסית מבחינת עלות חישוב (אם כי לא אקספוננציאלי) להצפין מסמך שלב, מייצרים האש קריפטוגרפי, עליו חותמים. האש הוא קל חישובית בכיוון אחד.

בביטקוין השתמשו ב־hash כמו "חידה". לדוגמה, תייצר טקסט כך שה־hash יתחיל ב־3 אפסים.

BACK TO ECONOMY . . . . . (4)

4.1 מה זה בנק?

ערימה של חשבונות וכמה כסף יש בהם. פשוט ספר רישומים ענק. וההנחה היא שכולם סומכים עליו. ואם המחשב נהרס? נרצה לבזר את המידע. ואם כן, איך אפשר לבצע העברה ולעדכן את כל העותקים?

4.2 ה־blockchain

רשימת הטקנזקציות בעולם. רשת הסיטקוין מכילה כ־12K (לפני כמה שנים) ציברי מחשבים בחרבי העולם הנקראים "צמתים". כל פעם שיש שינוי, הצומת שולח את העדכון ל־8 צמתים אקראיים ברשימה. שינוי מתפשט לכמעט על המחשבים לאחר כ־40 שניות. כל מי ש"חותם" אוסף של טקנזאקציות (אוסף כזה נקרא בלוק), מקבל שבריר מטקבע ביטקוין. זהו האינטרס לקבל ארזנקציות, לתחזק את בסיס הנתונים ולשדר ולקבל עידכונים מצמתים אחרים. חתימה דורשת למצוא האש מתאים – ומי שמצליח לאיסוף אוסף טראנזקציות ושולח אותן ל־blockchain הכי מהר, מקבל את שבריר הביטקוין בתמורה לזה.

4.2.1 למה לא לחתום בלוקים בעצמי

כי אם אני אאריך את ה־blockchain שלי בהתאם למה שאני אוסיף לעצמי, אז כולם ייקחו את ה־block היותר ארוך שנשלח ע"י מישהו אחר. לכן ברגע שהחידה פוצחה ומצאנו האש מתאים, חותמים ושולחים מיד. לא רוצים שאחרים יישיגו אותך.

PROGRAMMING 1 STUFF . . . . . (5)

בבית תעברו עם שיעורי הבית, ותבינו את הצד הטעני. לפני 4 שנים היה קורס "מזעזע" (ברמת, בו נכנס לפינות הכי רחוקות של ג'אווה, בלי סיבה). המרצה החדשה, מנסה גם ללמד עקרונות של פיתוח תוכנה. "הרבה מהדברים האלו הם בולשיט". פרנג'י אומר שיש רעיונות טובים, אבל אנשים מקצינים איתם והופכים אותם לדת.

נצטרך להכיר מספר פרדיגמות תכנות. java, לדוגמה, היא שפה מתקמפלת, עם OOP. שפות שכדאי לדעת:

- bash (scripting)
- python / js / ruby (inteptated)
- Java / Rust / cpp / Go (compiled)
- List / Scheme (functional)

חשוב להגיע למצב שאפשר לכתוב hello world ולהריץ. הרצה באמצעות: `java -cp /target/... *arguments`

5.1 compiling etc.

הסברים קצרים על מה זה קימפול (אני לא אעתיק אותם, אני מניח שאתם יודעים את זה). פייתון שומר .pyc כשלב pre-compiling.

ג'אווה מריץ דברים בתוך ה־JVM – java virtual machine – שיש לה שפת מכונה בעצמה. קובץ ג'אווה עובר **קימפול** לקוד jvm, ואז מבצעת **אינטרפיטציה** לקוד מכונה אמיתי. זה נותן אפשרות להריץ ב־cross-platfrom. ה־JRE, הוא java runtime envirement, הוא סוג של אינטרפטר שמעביר קוד jvm לקוד מכונה. ל־JRE חדשים יש מקמפל just in time compiler – GIC, עליו דיברנו בקורס הקודם.

בהינתן ה־apple silicon המפונפן עם M4, והמפתח רוצה להריץ משהו על arch linux עם חומרת אינטל. יוצא קובץ executable מקומפל מקוד ה־C, שיכול לרוץ על מעבד כללי. אבל מה אם נרצה להריץ על האינטל? נוכל להשתמש ב־cross compiler שיקמפל להוראות מכונה של אינטל. אם נכתוב ב־Java, אם נצא עם קובץ יחיד שאפשר להריץ על שניהם. ה־JRE יהיה יחודי בעבור כל אחד מהמחשבים, אבל ה־executable הוא cross-platform. בשביל זה יש לנו גרסאות שונות של JRE שעושות לנו בלגן. קוד ה־JRE, הוא בעצם zip שמכיל את הבצים המקומפלים, נקרא JAR – java acrhive.

יש עוד שפות מתקמפלות ל־JVM. לדוגמה: Kotlin ,scala, ועוד. הן גם יכולות להשתמש בספרויות של java. אפשר גם לכתוב דברים כמו Jython, שהוא python שרץ על jvm.

יש מעט מאוד שפות שאין להם runtime. אולי חוץ מ־C שטכנית אפשר להריץ בלי. ה־runtime liberary.