מה בנוגע למחשבים וזיכרון –

* זיכרון וCPU (CPU -יחידת עיבוד מרכזי) אם במחשב אין את אלו הוא לא נחשב מחשב , כל היתר יכול להיות ויכול גם לא. לתוכנה ונתונים משתמשים באותו זיכרון (למשל טקסט וקודים של הטקסט נשמרים באותו זיכרון). מה יותר יקר – תוכנה או חומרה ? תוכנה!

מה נכון בנוגע למערכות הפעלה –

* בלי תוכנה אין מחשב.
* מחשב זה מכונה אוניברסלית לעיבוד נתונים.
* צריך לדעת מהי תפקידה של מערכת הפעלה, למה צריך מערכת הפעלה?
* מחשב יכול להתקיים בלי מערכת הפעלה אבל זה מקרה מאוד נדיר (אבל כן אפשרי), רוב המחשבים כיום הם עם מערכת הפעלה – מחשב ללא מערכת הפעלה לדוג' טיל\מכוניות.
* תפקידה של מערכת ההפעלה – תפקידה לתת לתוכנה להשתמש בחומרה, תוכנה שהיא אפליקציה (אפליקציה = תוכנה שמביאה תועלת למשתמש הקצה) לא פונה ישירות לחומרה אלא פונה למערכת הפעלה שהיא פונה לחומרה (תוכנה -> מערכת הפעלה -> חומרה) .
* האם טוב שתוכנה תפנה ישירות למסך? לא כי אז היא מוגבלת לסוג המסך ואם יחליפו מסך המסך לא יעבוד, האם מערכת הפעלה חייבת להכיר מקלדת חדשה? כן. במערכת הפעלה יש מכשיר שנקרא דרייבר שמתאים ספציפי לחומרה. אם מפתחים תוכנה אי אפשר לפתח עבור כל המחשבים אלא עבור פלטפורמה ספציפית. מערכת הפעלה נותנת אפשרות להתקדם בחומרה מבלי לשנות את התוכנה.
* מערכות הפעלה – 4 מערכות הפעלה גדולים – ווינדוס, לינוקס (מבוסס על יוניקס) , אנדרואיד, IOS.

מה נכון לגבי תוכנות –

* יש סוגים שונים של תוכנה – 4 סוגים :

1. מערכת הפעלה שתפקידו לנהל את החומרה (כולל זכרון וכולל CPU) . כדי להפעיל תוכנה כלשהי צריך דרך מערכת הפעלה, אין דרך אחרת.
2. תוכנות עזר – תוכנות שעוזרת לתחזק את המחשב יותר טוב ( למשל אנטי וירוס , העתק קבצים, סדר) מי שמתמש בדר"כ עם התוכנות האלה – טכנאי מחשבים.
3. התוכנה הכי חשובה – אפליקציות, כל תוכנה שמביאה תועלת למשתמש הקצה. כל העבודה במחשב זה בעצם שימוש באפליקציות (אינטרנט וכו' )
4. כלים לפיתוח תוכנות .

* מעבד תמלילים זה אפליקציה.
* תוכנה שיודעת לבדוק האם הארד דיסק עובד טוב? תוכנת עזר.
* תוכנה שבאה ביחד עם דרייבר ? מערכת הפעלה.

מה נכון בנוגע לשפות תכנות –

* כדי לפתח אפליקציה (=תוכנה) צריך שפה שהCPU מבין אותה
* שפה עילית – שפה שמצד אחד פורמלית שממנו אפשר לתרגם לשפת מכונה ומצד שני שפה שיותר מתאימה לבן אדם, כל שפת עילית חייבת להיות מתורגמת לשפת מכונה.
* מה תפקידו של קומפיילר – לתרגם משפה עילית לשפת מכונה.

מה נגון בנוגע לטיפול בשגיאות תוכנה

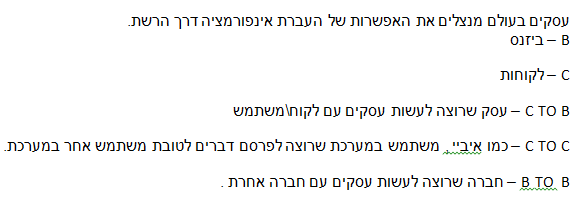
* מתברר כאשר בן אדם כותב משהו בשפות תכנות הוא יכול לטעות.
* BAG – תוכנה לבדיקת שגיאות בכתיבת תוכנה. האם קיימת תוכנה גדולה שאין בה באגים ? לא, תמיד יש באגים כי אי אפשר לעשות בדיקה אידיאלית של כל המקרים של הפעלה גדולה. אפילו בוורד שזה כבר גירסה 12,13 יש באגים. האם קל לטפל בבאגים? לא , כי בין מה שקרה ומה שאני רואה יש הבדל, בין הרגע שהיה הכשל ובין הרגע שרואים את הכשל יש הבדל זמן ולכן קשה למצוא את הבאג שכנראה קרה בזמן מוקדם יותר.

מה נכון בנוגע לניהול גרסאות תוכנה

* כל תוכנה בגרסא הראשונה היא לא מספיק טובה, למה? כי מי שמפתח לא יודע את כל היכולות של השימוש של התוכנה והוא עושה שגיאות (לא רק באגים) . תוכנה איכותית היא תוכנה שמשתמש יודע בדיוק איך להשתמש בה. ולכן הגרסאות הראשונות מלאות באגים וכל תוכנה משתפרת מגרסא לגרסא.
* פאצ' – תוספת לתוכנה שמתקנת אותה מבפנים , אבל לא מוסיף יכולות נוספות.
* גרסאת אפס – תוכנה שאינה בשלה ולכן אי אפשר לקנות\למכור אבל נותנים למשתמש הקצה כדי שיעשה בדיקה עד כמה היא טובה ויתנו חוות דעת .

מה נכון בנוגע לאינטרנט

* אינטרנט זו תשתית שנותנת אפשרות מכל מחשב בעולם לשלוח ולקבל נתונים .
* אינטרנט זה יקר מאוד – קווי תקשורת חיבורים.. חינמי בגלל שלא מוסיפים סכום כסף אם רוצים לשלוח מהארץ משהו לאפריקה.
* באינטרנט יש גרעין שמורכב מנתבים (ראוטר) וקצוות (מחשב שמנצל את האינטרנט , מחשב שמנצל את האינטרנט נקרא הוסט)
* הוסט – מישהו שמארח, מה מארח ? תוכנה שמנצלת אינטרנט, קצה של אינטרנט.
* בין ההוסטים יש תוכנות שנותנים שירות לאינטרנט שנקראים שרתים.
* שרתים – מחשב שנותן שירות דרך האיטנרנט. איזה שירות הוא יכול לתת? יכול לשלוח אינפורמציה.

מה נכון בנוגע לעסקים באינטרנט

* האם מסוכן לעשות עסקים באינטרנט ? לא! HTPS
* מסוכן לא להגן על המחשב עצמו (את ההוסט) .

מה נכון בנוגע לתוצאות חיפוש במנוע חיפוש מודרני בwab

* וואב – אוסף מסמכים מקושרים זה לזה.
* איך אני מקבל אינפורמציה שנדרשת לי ? מנוע חיפוש
* מנוע חיפוש – אי אפשר שזה ילך לחפש באינטרנט משהו ספציצי, יקח שעות אז מה הוא עושה? קיים ספיידר שעושה סדר בין כל הדפים.
* ספיידר מטייל בWAB , ספיידר מביא את כל המסמכים (האתרים) לתוך השרתים של המנוע החיפוש ואח"כ הוא בונה ממנו אינדקס, אינדקס זאת טבלה שבטבלה רשומים כל המילים ובאיזה מקומות באינטרנט אפשר למצוא כל מילה.
* אם ספיידר לא נמצא באתר כלשהו, האתר לא נמצא בגוגל. לא כל האתרים נמצאים באינטרנט.
* שאני מחפש משהו , למה החיפוש כל כך חשוב? גוגל מצא את האלגוריתם שלדף שיש הכי הרבה חיפושים הוא יהיה בראש הרשימה בגוגל. שחברת גוגל הוקמה היו כבר 20 מנועי חיפוש טובים אבל היו גרועים בסינון התוצאות (נתנו תוצאה עם המילה שחיפשו הכי הרבה) וגוגל לעומתם המציאו את הדירוג של הדפים – דף חשוב זה דף שיש בו יותר הצבעות \ לינקים, שבונים אינדקס לכל דף יש את הדירוג. דף חשוב זה דף שדפים אחרים שמו עליו לינק.

מה נכון בנוגע ל SEO – search engine optimization

* יכולת לעשות אופטימיזציה לאתר שלי, כך שגוגל תחליט שהוא צריך להיות ראשון.

יש שני סוגים –

1. סוג אחד שחוקי ואפ/ילו גוגל ממליצה ומראה איך לעשות – משפרים את האתר עצמו שיהיה יותר יפה , שהתוכן שלו והמילים שיש בו יהיו בדיוק המילים שמחפשים בדר"כ, מנתחים לפי לקוחות ,איזה מילים, ולפי מילים אלו מנסחים סיפור כדי שימשוך יותר ויותר לקוחות להכנס לדף.
2. סוג אחד שלא חוקי – יש חברות שמשלמים להן על מנת שהדירוג של האתר יהיה גבוה יותר , הם משתמשים בלינקים מלאכותיים , פורצים לאתרים ושותלים שם לינק מלאכותי. (שבעל האתר לא יכול לראות את הלינק , אבל רובוט שסורק את הדף הוא רואה את הלינק המלאכותי)

**חומרה – HARDWARE**

היא אוסף כל הרכיבים הפיזיים ב[מחשב](https://he.wikipedia.org/wiki/%D7%9E%D7%97%D7%A9%D7%91) או בהתקן [אלקטרוני](https://he.wikipedia.org/wiki/%D7%90%D7%9C%D7%A7%D7%98%D7%A8%D7%95%D7%A0%D7%99%D7%A7%D7%94) אחר, כמו [טלפון סלולרי](https://he.wikipedia.org/wiki/%D7%98%D7%9C%D7%A4%D7%95%D7%9F_%D7%A1%D7%9C%D7%95%D7%9C%D7%A8%D7%99) או [ציוד תקשורת](https://he.wikipedia.org/w/index.php?title=%D7%A6%D7%99%D7%95%D7%93_%D7%AA%D7%A7%D7%A9%D7%95%D7%A8%D7%AA&action=edit&redlink=1), כלומר כל אובייקט הנתפס ב[חוש המישוש](https://he.wikipedia.org/wiki/%D7%97%D7%95%D7%A9_%D7%94%D7%9E%D7%99%D7%A9%D7%95%D7%A9) .

התקני חומרה

* CPU- היחידה הזו מורכבת משני מרכיבים: אריתמטית לוגית שמבוססת על מתמטיקה, ויחידת הבקרה שמפקחת על כל הדברים שעליהם אחראי המעבד. היא שולטת ביחידה האריתמטית וגם ביחידת הפלט. דאטה- אפיק של זרימת נותנים, אדרס- שייך למבנה נתונים והקונטרול- שמווסת את כל הפעילות הזאת של המעבד המרכזי.
* איך עובד המעבד? המעבד למעשה עובד עם שפת מכונה "אסמבלי" בעל 4 פעולות יסוד שבו משתמש המעבד (פירוט במצגת).
* זיכרון- חלק מהזיכרון (בתוך המחשב) RAM- זיכרון בגישה אקראית אפשרי לגשת לכתובת בצורה רנדומלית ולא סידרתית( שמאטה את קצב הפעילות) הRAM מורכב משני חלקים DRAM דינאמי SRAM סטטאטי. ככל שהRAM יותר גדול ביצועי המחשב יותר טובים. הוא זיכרון מחיק והוא תלוי בזרם החשמל לעומת הארדידסק שנשמר גם לאחר ריסטרט.
* ROM- זה זיכרון שהוא רק לקריאה ואפשרי לשאוב משם אינפו וזה אנו מקבלים עם המחשב.זה זיכרון שלא ניתן לשימוש המשתמש. BIOS- זו המערכת שמאתחלת את המחשב כדי שאני אוכל להתחיל לעבוד עם המחשב. הוא חלק מהROM. זיכרון וירטואלי- המערכת מקצה חלק מהדיסק שלנו לשימוש להעלאת מהירות המערכת וזה נלקח מהדיסק הקשיח כשמעבד צריך לעשות אותם שאין מספיק זיכרון בRAM.שם אנו שומרים אינפו שלא קשורה להארדדיסק.
* Cache- הוא שומר את ההיסטוריה של הפעולות שביצעתי במחשב ואם אני חוזר על פעולה מספר רב של פעמים אני לא צריך לחזור על הפעולה אלא לגשת לכתובת המסוימת וזה חוזר על אותה פעולה.
* לוח אם- הלוח הירוק שעליו מולבשים כל הרכיבים של החומרה. המעבד, זיכרון ומותקנים ישירות ללוח שמותקן דרך הBUS שזה הכבלים המאוגדים יחדיו בצבע אפור והם מחבים בין לוח האם לכל ההתקנים הנוספים שנמצאים במחשב.
* ספק כוח- שנאי חשמלי
* זיכרון משני- ככל שהדיסק מסתובב מהר יותר המחשב עובד מהר יותר. מה שחשוב כאן זה מהירות הסיבוב של הדיסק (5400,7200).
* מסך מגע- מסכי נגיעה משנים את צורת העבודה שלנו.

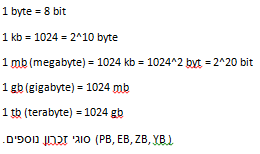
**חוק מור –**

**חוק מור** הוא תחזית או ניבוי משנת [1965](https://he.wikipedia.org/wiki/1965" \o "1965) של [גורדון מור](https://he.wikipedia.org/wiki/%D7%92%D7%95%D7%A8%D7%93%D7%95%D7%9F_%D7%9E%D7%95%D7%A8" \o "גורדון מור) לפיה צפיפות [הטרנזיסטורים](https://he.wikipedia.org/wiki/%D7%98%D7%A8%D7%A0%D7%96%D7%99%D7%A1%D7%98%D7%95%D7%A8" \o "טרנזיסטור) [במעגלים משולבים](https://he.wikipedia.org/wiki/%D7%9E%D7%A2%D7%92%D7%9C_%D7%9E%D7%A9%D7%95%D7%9C%D7%91) במחיר מינימלי, תוכפל כל שמונה עשר עד עשרים וארבעה חודשים.

הגדרת קצב הגידול של צפיפות הטרנזיסטורים גרמה ליצרנים להשתדל להגשים את התחזית. מאוחר יותר, יצרני המעגלים המשולבים והשבבים האלקטרוניים החלו להנמיך את הציפיות ואת קצב הגידול בפועל לעומת הצפוי לפי חוק מור, על אף שככל הנראה יכלו להגדיל את צפיפות הטרנזיסטורים מהר יותר. יש הגורסים כי טענה זו אינה נכונה ואינה מתאימה לשוק תחרותי. התחזית של מור שונתה כך שעוצמת המחשוב באופן כללי תוכפל כל שנתיים בערך.

לסיכום , חוק מור מציג תחזית התפתחות של תעשיית המעבדים וה[מחשבים](https://he.wikipedia.org/wiki/%D7%9E%D7%97%D7%A9%D7%91%D7%99%D7%9D" \o "מחשבים) ומצד שני הוא משמש גם מעין מפת דרכים לתעשייה עצמה. הפחד של החברות בתחום המעבדים והמחשבים הוא להישאר מאחור וה[מוטיבציה](https://he.wikipedia.org/wiki/%D7%94%D7%A0%D7%A2%D7%94" \o "הנעה) שלהן להמשיך לפתח [טכנולוגיה](https://he.wikipedia.org/wiki/%D7%98%D7%9B%D7%A0%D7%95%D7%9C%D7%95%D7%92%D7%99%D7%94" \o "טכנולוגיה) בקצב מהיר היא רבה. חוק מור איננו חוק פיזיקלי, הוא איננו חוק [טבע](https://he.wikipedia.org/wiki/%D7%98%D7%91%D7%A2" \o "טבע) ובהחלט מפתיעה העובדה שהוא מתקיים בדיוק טוב למדי מעל ארבעים שנה. חברת אינטל עדיין מציגה את חוק מור כחוק פלאי המוסיף להתקיים כבר שנים רבות למרות שישנם מבקרים המציגים את ירידת קצב ההכפלה מאחת לשנה וחצי לאחת לשנתיים כפגם משמעותי.

**הזיכרון –**

זיכרון המחשב משמש לאחסון התוכנית שהמחשב מבצע ולאחסון הנתונים שתוכנית זו קוראת או כותבת בעת ביצועה על ידי המעבד. בהתאם לכך, תוכנו של הזיכרון משתנה תוך כדי פעולת התוכנית. בעיקר משתנה החלק שבו נמצאים הנתונים המעובדים, אך לעתים משתנה גם החלק שבו נמצאת התוכנית (הוא בוודאי משתנה כאשר התוכנית המתבצעת מוחלפת באחרת). בנוסף לזיכרון, רוב המחשבים מכילים גם אמצעי אחסון חיצוניים, שתוכנם נשמר לטווח ארוך, ובהם [דיסק קשיח](https://he.wikipedia.org/wiki/%D7%93%D7%99%D7%A1%D7%A7_%D7%A7%D7%A9%D7%99%D7%97), [תקליטור](https://he.wikipedia.org/wiki/%D7%AA%D7%A7%D7%9C%D7%99%D7%98%D7%95%D7%A8), [דיסק און קי](https://he.wikipedia.org/wiki/%D7%93%D7%99%D7%A1%D7%A7_%D7%90%D7%95%D7%9F_%D7%A7%D7%99) ועוד. בעבר כונו שני הסוגים הללו "זיכרון ראשי" ו"זיכרון משני", בהתאמה. גודל הזיכרון שהמחשב זקוק לו תלוי ב[יישומי המחשב](https://he.wikipedia.org/wiki/%D7%99%D7%99%D7%A9%D7%95%D7%9E%D7%99_%D7%9E%D7%97%D7%A9%D7%91" \o "יישומי מחשב) אותם מפעיל המשתמש וביעילות [מערכת ההפעלה](https://he.wikipedia.org/wiki/%D7%9E%D7%A2%D7%A8%D7%9B%D7%AA_%D7%94%D7%A4%D7%A2%D7%9C%D7%94" \o "מערכת הפעלה) של המחשב. מערכות ההפעלה ותוכנות מחשב בכלל דורשות כמות מינימלית של זיכרון RAM כדי לפעול כהלכה.

סיבית \ יחידת זיכרון קטנה = bit

**טבלת קידוד -**

ארכיטקטורת החומרה - רעיון הראשוני, תכנון ובמבנה הביצועי של מערכת [מחשב](https://he.wikipedia.org/wiki/%D7%9E%D7%97%D7%A9%D7%91). התחום הוא אבן בניין בתיאור הדרישות והמפרט, התכנון והמימוש של חלקים רבים ממערכת מחשב תוך כדי התמקדות בדרך בה המעבד המרכזי [CPU](https://he.wikipedia.org/wiki/CPU) מבצע גישה לזיכרון. התחום גם מהווה את התורה בה מתכננים ובוחרים את מרכיבי המחשב ואת החיבוריות ביניהם בצורה הטובה ביותר לעמידה בציפיות הביצועים והעלות.

**DATABASE**

 הוא אמצעי המשמש לאחסון מסודר של [נתונים](https://he.wikipedia.org/wiki/%D7%A0%D7%AA%D7%95%D7%A0%D7%99%D7%9D) ב[מחשב](https://he.wikipedia.org/wiki/%D7%9E%D7%97%D7%A9%D7%91), לשם אחזורם ועיבודם. בסיס נתונים מאוחסן ב[אמצעי אחסון נתונים](https://he.wikipedia.org/wiki/%D7%90%D7%9E%D7%A6%D7%A2%D7%99_%D7%90%D7%97%D7%A1%D7%95%D7%9F_%D7%A0%D7%AA%D7%95%D7%A0%D7%99%D7%9D), בדרך כלל על גבי [דיסק קשיח](https://he.wikipedia.org/wiki/%D7%93%D7%99%D7%A1%D7%A7_%D7%A7%D7%A9%D7%99%D7%97), המאפשר גישה ישירה לנתונים. הגישה לבסיס הנתונים נעשית באמצעות [תוכנה](https://he.wikipedia.org/wiki/%D7%AA%D7%95%D7%9B%D7%A0%D7%94) ייעודית - [מערכת לניהול בסיס נתונים](https://he.wikipedia.org/w/index.php?title=%D7%9E%D7%A2%D7%A8%D7%9B%D7%AA_%D7%9C%D7%A0%D7%99%D7%94%D7%95%D7%9C_%D7%91%D7%A1%D7%99%D7%A1_%D7%A0%D7%AA%D7%95%D7%A0%D7%99%D7%9D&action=edit&redlink=1) . בסיס הנתונים בנוי לפי מודל לאחסון הנתונים, כמו מנגנונים פנימיים ל[מיון](https://he.wikipedia.org/wiki/%D7%9E%D7%99%D7%95%D7%9F_(%D7%9E%D7%93%D7%A2%D7%99_%D7%94%D7%9E%D7%97%D7%A9%D7%91)) ול[חיפוש](https://he.wikipedia.org/wiki/%D7%90%D7%9C%D7%92%D7%95%D7%A8%D7%99%D7%AA%D7%9D_%D7%97%D7%99%D7%A4%D7%95%D7%A9).

המודל הנפוץ ביותר היום, הוא המודל הטבלאי שמכונה גם יחסי. במודל זה בסיס הנתונים בנוי מטבלאות, כאשר כל טבלה מכילה מידע על ישות מסוימת (לדוגמה, לקוחות במערכת בנקאית). בכל טבלה יש רשומות (שורות), כאשר כל רשומה מתייחסת למקרה ספציפי (למשל לקוח מסוים). לכל רשומה בטבלה יש [מפתח ראשי](https://he.wikipedia.org/wiki/%D7%9E%D7%A4%D7%AA%D7%97_%D7%A8%D7%90%D7%A9%D7%99) שמזהה באופן ייחודי את הרשומה. הקשר בין הרשומות בטבלאות שונות נעשה באמצעות שדה [מפתח זר](https://he.wikipedia.org/wiki/%D7%9E%D7%A4%D7%AA%D7%97_%D7%96%D7%A8" \o "מפתח זר)כאשר מספר הפעמים בו יכול להיות משויך המפתח לרשומה ספציפית בטבלה האחרת מגדיר את ריבוי הקשר (יחיד לרבים - רבים לרבים וכו'). שליפת מידע ופעולות עדכון בבסיס נתונים טבלאי נעשות באמצעות שפת  [SQL](https://he.wikipedia.org/wiki/SQL), המהווה ממשק המאפשר גישה לנתונים מבלי להתייחס לאופן שמירתם בבסיס הנתונים.

קיימת תוכנה ספציפית שיודעת לארגן נתונים בהארד דיסק ולתת גישה מהירה לנתונים האלה לפי השאילתות – database management system .

לכל relational DBMS יש שפה משותפת שמאפשרת גישה לנתונים – SQL שמארגנת את הנתונים בטבלה.

(שאלת מבחן) תוכנה חינמית בopen source– קוד פתוח משמש בעולם ה[תוכנה](https://he.wikipedia.org/wiki/%D7%AA%D7%95%D7%9B%D7%A0%D7%94) לציון תוכנה ש[קוד המקור](https://he.wikipedia.org/wiki/%D7%A7%D7%95%D7%93_%D7%9E%D7%A7%D7%95%D7%A8) שלה פתוח ונגיש לכל מי שחפץ בו והוא חופשי לשימוש, לצפייה, לעריכת שינויים ולהפצה מחודשת לכל אחד ואחת. שיטת פיתוח כזו מאפשרת בעצם לכל מי שחפץ בכך לקחת חלק ב[פיתוח התוכנה](https://he.wikipedia.org/wiki/%D7%A4%D7%99%D7%AA%D7%95%D7%97_%D7%AA%D7%95%D7%9B%D7%A0%D7%94) ולתרום לשיפורה.

Nosql DBMS - SQL ללא טבלאות, שאילתות אחרות למשל גרף .

המדע המודרני מובסס על נתונים ויש לנו יכולות כאנושות לתפקד בעזרת הbigdata .

Bigdata – יכולת של האנושות לעשות עיבוד וניתוח (לא רק לשמור) של הנתונים.

יש היום מקצוע שנקרא – data analyst\ data scientists – לוקח המון מקורות של נתונים ומנתח את הנתונים ללקוח שלו.

מה ההבדל בין ניתוח נתונים לבין סטיסטיקה –

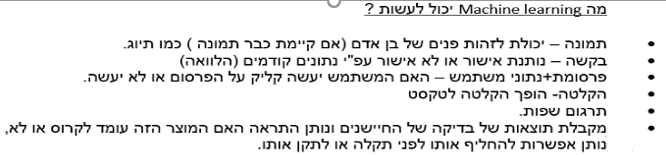
הכלים הסטטיסטים נותנים (statistics)– לאשר או לדחות השערות לפי הנתונים ולא מנסה להגיד מה יהיה בעתיד.

הכלי ניתוח נתונים (analysis) – לא יודעים מה ההשפעה, חיזוי ע"י למידה מתוך הנתונים- לוקחת את כל התונים ובונה מודל מתמטי. מה שמאפיין את הכלי הזה זה שהיא לומדת מהנתונים הקודמים. על סמך נתונים רוצה להגיד מה יהיה בעתיד.

Bigdata - כמות גדולה של נתונים שיש גישה אליהם דרך המחשב.

Datamining – יכולת לניתוח את האלגוריתמים והכלים לניתוח נתונים שמביא תועלת. (חייב להיות כמות גדולה של נתונים )

Artificial intelligence -אוסף אלגוריתמים המחקים את הפעילות של הבן אדם ויכולים לפתוח משימות שדורשות מחשבות , למשל – מחשב שמשחק בשח.

Machine learning - תוכנות שלומדות מנתונים רבים, לדוגמה אישור\לא אישור הלוואה – נותנים נתונים רבים שהיו בעבר ועפ"י זה בנק יכול לאשר או לא לאשר הלוואה.

Deep learning – שיטה חדשה ללימוד מהנתונים שקיימים.

**תוכנה**

**תוכנה** – תוכנה היא אוסף פקודות אשר נועדות לפקח על פעולת המחשב.  
**תוכנית מחשב** – היא רצף של פקודות המתאר ומגדיר כיצד לבצע פעילות מסוימת.  
**תוכנת הפעלה** – מנהלת את משאבי המחשב  
**השבחה upgrade –** גרסא חדשה לתוכנה קיימת הכוללת תיקון שגיאות או תוספות.  
**תאימות –** התאמה לחומרה או מערכת הפעלה ,לא ניתן להריץ תוכנה על פלטפורמה לא מותאמת.  
**כתב ויתור –** התקנה של תוכנה מסחרית כרכה בויתור על אחריות כלשהי מצד מפתח התוכנה על כל שגיאה שהתוכנה עלולה ליצור בעת השימוש בה.  
**רישיון** – קניית תוכנה פירושה רכישת רישיון להשתמש בתוכנה,הסכמים יכולים להשתנות מתוכנה לתוכנה.  
ישנם סוגים שונים של שיטות רישוי (לפי מס' משתמשים,רישיונות "צפים" וכו'...) כמו כן ניתן גם לשכור תוכנה ולהחליפה בגרסה חדשה בעת הצורך.  
**זכויות יוצרים –** לא כל התוכנות מוגבלות בשימוש ישנן תוכנות המוגדרות כציבוריות וניתן להשתמש בהם חינם.ישנם תוכנת דמו אשר מאפשרות חלק מהפונקציות רק כדי להתרשמות ולקניה במידת הצורך.  
**הפצה –** תוכנה נמכרת בחנויות,באינטרנט,דרך מפצי משנה,לאחר הרכישה ניתן לפנות לשירות הלקוחות כדי לקבל סיוע.  
**גרסת בטא** – לאחר גמר פיתוח ומבדקים מפיץ היצרן את התוכנה לשותפים עסקיים ע"מ שישתמשו בה ויבדוק אותה בשטח לפניי ההפצה של הגרסה הרשמית.

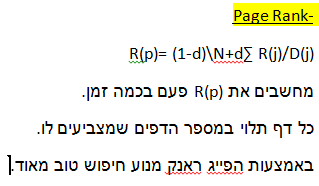
**מערכת הפעלה :** היא [תוכנה](https://he.wikipedia.org/wiki/%D7%AA%D7%95%D7%9B%D7%A0%D7%94) המגשרת בין המשתמש, ה[חומרה](https://he.wikipedia.org/wiki/%D7%97%D7%95%D7%9E%D7%A8%D7%94) ויישומי התוכנה. זו התוכנה הראשונה שעולה עם הדלקת המחשב והיא זו המאפשרת לו לפעול. מערכת ההפעלה מספקת שלושה ממשקים: [ממשק משתמש](https://he.wikipedia.org/wiki/%D7%9E%D7%9E%D7%A9%D7%A7_%D7%9E%D7%A9%D7%AA%D7%9E%D7%A9) (User Interface), ממשק עבור ה[חומרה](https://he.wikipedia.org/wiki/%D7%97%D7%95%D7%9E%D7%A8%D7%94) על ידי [מנהלי התקנים](https://he.wikipedia.org/wiki/%D7%9E%D7%A0%D7%94%D7%9C_%D7%94%D7%AA%D7%A7%D7%9F) ו[ממשק תכנות היישומים](https://he.wikipedia.org/wiki/%D7%9E%D7%9E%D7%A9%D7%A7_%D7%AA%D7%9B%D7%A0%D7%95%D7%AA_%D7%99%D7%99%D7%A9%D7%95%D7%9E%D7%99%D7%9D) (API). מערכת ההפעלה היא רכיב חיוני בכל [מחשב](https://he.wikipedia.org/wiki/%D7%9E%D7%97%D7%A9%D7%91). תהליך טעינתה של מערכת ההפעלה, המתבצע עם הדלקת המחשב, קרוי [אתחול](https://he.wikipedia.org/wiki/%D7%90%D7%AA%D7%97%D7%95%D7%9C).  
מערכות ההפעלה הנפוצות הם windows,unix,linux ,max os x.  
**multitasking** - אחת היכולות של מערכת ההפעלה היא ריבוי משימות בו זמנית מערכת ההפעלה מקצה זמן cpu לכל תוכנית.  
**multitasking** - יכולת מערכת ההפעלה לבצע חלקים שונים של אותה תוכנית במקביל.  
חלוקת זמן ( time sharing ) – מאפשרת למספר משתמשים לעבוד מול cpu אחד,ומחלק את זמן המעבד ביניהם.  
**multiprocessing**  - טיפול במספר מעבדים במקביל.  
**זיכרון וירטואלי** – יכולתה של מערכת ההפעלה לחלק תוכנית לחלקים ולאחסן רק את החלק הנמצא בעיבוד בזיכרון הפנימי,בעוד שאת שאר החלקים בזיכרון המשני.  
**ניטור משאבים** – הגדרת משתמשים והרשאות,בקרת הגישה למשתמשים ע"פ זיהוי סיסמה,הגנה מפני וירוסים וסוסים טרויאנים.  
**תוכניות שירות –** תוכניות עזר הנלוות למערת ההפעלה ומאפשרות שליטה טובה יותר במשאבי המחשוב (משותפות לכל המשתמשים).

**שפות תכנות:**  
תוכנית נכתבת בשפת המקור לאחר מכן "מהדר" (קומפיילר) מתרגם אותה לשפת מכונה ואז התוכנית מוכנה לריצה.

**תכנות מוכוון עצמים-** מאחד פעולות ונתונים לתוך עצם (אובייקט) יחיד,השייך למחלקה (class),התוכנית מעבירה מסר לעצם לבצע את הפעולה השייכת לו,הפעולות מהוות הניתן ע"י העצם.  
נתוני האובייקט כמוסים ואינם נגישים מבחוץ ללא הרשאות.  
יתרונות – אפשרות לשימוש חוזר ולפיתוח תוכנה מבוסס רכיבים,מפחית זמן עלות ופיתוח תוכנה,אפשרות לתכנות ויזואלי ע"י בחירה ועריכה של אובייקטים במקום כתיבת קוד לדוגמא :c++,java.

**תוכנות יישומיות:**  
תוכנה לשימוש כללי כגון:עיבוד תמלילים,גיליון אלקטרוני,דואר אלקטרוני....  
**תוכנה מותאמת –**תוכנה המפותחת עבור דישות של לקוח מסוים לשימוש הארגון.  
תוכנת מדף – תוכנה המיועדת למכירה של הרבה לקוחות,הפצה בכמה גרסאות,לקונה אין גישה לקוד ואינו יכול להשפיע על לוח הזמנים של ההפצה.  
**קוד פתוח-** שיתוף פעולה בין מפתחים עצמאיים כל אחד יכול להשתתף ולתרום הגרסא זמינה לכולם השימוש במוצר חופשי תחת הגבלות מסוימות למשל לינוקס,מוזילה,ביטורנט.מכיוון שהזכויות בה ציבוריות אסור לגבות תשלום על שימוש בתוכנה אבל מותר לגבות תשלום על שירותים נלווים כגון הפצה שיווק תמיכה יעוץ.  
תוכנה יישומית בתחום העסקי הינה חבילות תוכנה המשרתות אלפי ארגונים בניהול קשרי לקוחות,ניהול משאבי הארגון,ניהול שרשת האספקה,מסחר אלקטרוני וכדומה...  
יתרונות:זול יותר מאשר לקנות כל מוצר בנפרד,ממשק דומה,אינטגרציה.  
חסרונות:לא משתמשים בכל היכולות תופס מקום.  
**storage service provider -** אחסון נתוני החברה בשטח אחסון מרוחק דרך web.השטח מנוהל ע"י ספק שמשקיע בטכנולוגיות החדשות ביותר ומבטיח לספק זמינות,אמינות,מהירות ובטחון.החברה מחויבת עבור השימוש,וחוסכת עלויות של תשתיות אחסון אחזקה שדרוג ותמיכה.

BAG – תוכנה לבדיקת שגיאות בכתיבת תוכנה. האם קיימת תוכנה גדולה שאין בה באגים ? לא, תמיד יש באגים כי אי אפשר לעשות בדיקה אידיאלית של כל המקרים של הפעלה גדולה. אפילו בוורד שזה כבר גירסה 12,13 יש באגים. האם קל לטפל בבאגים? לא , כי בין מה שקרה ומה שאני רואה יש הבדל, בין הרגע שהיה הכשל ובין הרגע שרואים את הכשל יש הבדל זמן ולכן קשה למצוא את הבאג שכנראה קרה בזמן מוקדם יותר.

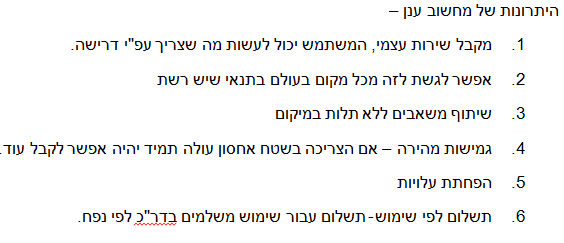
* **גוגל ניצל את חוכמת ההמונים –**

מנוע חיפוש גוגל עובד עפ"י רוב האנשים שאהבו אתר מסוים , אם יש אתר שהרבה אתרים הפיצו את הלינק שלו והאתר מכיל את המילת חיפוש שהמשתמש חיפש אז האתר הזה יהיה האתר הראשון ברשימת תוצאת החיפוש.

* איך גוגל הפכה לחברה ריווחית? גוגל בשנים הראשונה אינה הייתה רווחית. גוגל נהייתה רווחית באמצעות פרסומות, כל לחיצה על פרסומת כלשהי בעל הפרסומת העביר כסף לגוגל. גוגל יכול לעשות התאמה אישית בפרסומות עפ"י החיפוש של הבן אדם.

כל האתרים (שנמצאים דרך מנוע חיפוש גוגל) שבעלי מוניטין גבוה – הרבה מבקרים באתר, יכול לנצל את המוניטין לטובת מכירת השטח באתר לפרסומות – גוגל לוקחת עמלות על כל הפרסומות שנמצאות בכל האתרים. השיטה הזאת היא בין ההכנסות הגדולות של גוגל.

* מנוע החיפוש - מנועי החיפוש סורקים את רשת האינטרנט בחיפוש אחר [דפים](https://he.wikipedia.org/wiki/%D7%93%D7%A3_%D7%90%D7%99%D7%A0%D7%98%D7%A8%D7%A0%D7%98) באמצעות שימוש ב[ספיידר](https://he.wikipedia.org/wiki/%D7%96%D7%97%D7%9C%D7%9F_%D7%A8%D7%A9%D7%AA) אינטרנט. הספיידר מעביר עותקים של הדפים שנסרקו למנוע ה[אינדקס](https://he.wikipedia.org/wiki/%D7%90%D7%99%D7%A0%D7%93%D7%A7%D7%A1_(%D7%9E%D7%97%D7%A9%D7%91)" \o "אינדקס (מחשב)) לצורך פירוק הדף למרכיביו ובניית מאגר מידע של תוכן הדפים. בעת ביצוע חיפוש נשלחת [שאילתה](https://he.wikipedia.org/wiki/%D7%A9%D7%90%D7%99%D7%9C%D7%AA%D7%94_(%D7%AA%D7%95%D7%9B%D7%A0%D7%94)) למאגר המידע, והמידע המתקבל כפלט מוצג למשתמש על פי מידת הרלוונטיות שלו כתוצאת החיפוש.
* תוצאות חיפוש – ישנו אלגוריתם בגוגל שהאלגוריתם מחשב עבור כל דף אינטרנט את מידת החשיבות שלו ומציג אותו בדירוג תוצאות החיפוש בהתאם. דירוג של דף נקבע על פי כמות הדפים שמקשרים אליו וחשיבותם של הדפים המקשרים. כלומר, אם דפים רבים מקשרים אל דף מסוים האלגוריתם קובע את מידת החשיבות של דפים אלה ומדרג את הדף על פי מידת חשיבותם.

**מסחר אלקטרוני**

**מחשוב ענן -** קבלת כל משאבי מכשור מחברה אחרת ( icloud )

* הענן טוב יותר מאוסף שרתים.
* יכולות להעביר קבצים ממקום למקום.
* בעיית אבטחה – הענן הוא ציבורי לכן ישנה בעית אבטחה
* ניתן לקנות ענן פרטי - מחשוב ענן יכול להיות פרטי או ציבורי. מחשוב ענן פרטי הוא רשת מחשוב ייעודית או מרכז נתונים ארגוני שמספק שירותים מתארחים עבור מספר מצומצם של אנשים או מחלקות בארגון.קיימים ארגונים שהרגולציה אינה מאפשרת להם שימוש מחשוב ענן, למשל - בנקים או שירותי בריאות ורפואה, בשל חשש מבעיות אבטחה. ארגונים אלה וכן ארגונים גדולים אחרים, יעברו ל"ענן פרטי" , הפעלת כל המערכות ממקום מרכזי בארגון עצמו. למעבר כזה נדרשים האחדת יישומים, אחסון מרכזי, אמצעי בקרה וגיבוי וכן שימוש בוירטואליזציה.ענן פרטי יכיל את המאפיינים הבאים (כולם או חלקם): שיתוף משאבים בין יישומים, שיתוף משאבי מחשוב, שטחי אחסנה, רשת תקשורת, סביבות תוכנה, רישיונות, וירטואליזציה, סטנדרטים ואחידות, ריבוי דיירים ועוד.
* **ענן משולב (Hybrid Cloud):**חברות גדולות יכולות ליישם ענן פרטי ולהעביר יישומים לא קריטיים ולא מרכזיים לענן הציבורי ובמילים אחרות לשלב יישומים בענן הפרטי והציבורי.
* **תשתית כשירות (IaaS - Infrastructure as a Service):**שירותים מסוג זה הם שירותים בהם המשתמש מקבל משאבי מחשוב לשימושו: שרתים, אחסון, שולחן עבודה או רשת. כך למשל לצורך גיבוי של קבצים אפשר לקבל שטח אחסון באחד מהאמצעים לאחסון נתונים בענן מחשוב של ספק.לדוגמא, ארגון המעונין בשטחי אחסון עבור קבצי נתונים או עבור גיבוי, ספק השירות יקצה לארגון את השטחים המבוקשים ברמת זמינות המבוקשת לפרק זמן מבוקש.בכל המקרים האלה חיוב הלקוח יעשה לפי שימוש במשאבים בפועל. במודל IaaS, הניהול וההפעלה של התשתיות הם באחריות הלקוח בזמן שהוא משתמש בשירותים.
* **פלטפורמה כשירות (PaaS - Platform as a Service):**השירות הניתן במקרה זה הוא פלטפורמה הנדרשת להרצה, הפעלה או פיתוח יישומים ע"י הלקוח. מדובר הן ביישומי מדף והן בפיתוח אפליקציות של המשתמש. במקרה זה, מקבל המשתמש גם משאבי מחשוב וגם תוכנות תשתית הנדרשות לצורך הרצת המערכת או פיתוחה. זאת, מבלי לדאוג לתחזוקה של מערכת ההפעלה, חומרת השרתים, איזון עומסים או קיבולת מחשוב.
* **תוכנה כשירות (Saas - Software as a Service):**במקרה זה המשתמש משתמש גם בתשתית חומרה, גם בפלטפורמה וגם בשירותים אפליקטיביים שפותחו על ידי הספק. במקרים רבים השירותים המסופקים בשיטת SaaS הם שירותים בתפיסת SOA (Service Oriented Architecture).

**מנגנון - transaction**

בזמן שעושים עסקים מעבירים עסקאות וכספים בין מחשבים. - המטרה לשמור שהתנועה תתבצע בשלמותה או לא תתבצע כלל, כדי לשמור על עקביות הנתונים העסקיים. לדוגמה, בפעולה של העברת כספים בין חשבונות [בנק](https://he.wikipedia.org/wiki/%D7%91%D7%A0%D7%A7), חשוב שאם סכום כלשהו הוחסר מהחשבון המשלם הוא יופקד בחשבון הנמען. אם, בשל כשל כלשהו, תהליך העברת הכספים נקטע לפני שהושלם, המערכת עלולה להיוותר במצב לא עקבי. לדוגמה, הסכום הוחסר אך לא הועבר. מטרת התנועה היא להבטיח את שלמות הנתונים, גם לנוכח מקרי כשל.

**מנגנון - הצפנה**

כל משתמש מכין לעצמו זוג מפתחות: **מפתח ציבורי**  שהוא מפתח הצפנה הנגיש לכל ו**מפתח פרטי** מתאים, הנשמר בסוד ומשמש לפענוח. ההתאמה היא [חד-חד-ערכית](https://he.wikipedia.org/wiki/%D7%97%D7%93_%D7%97%D7%93_%D7%A2%D7%A8%D7%9B%D7%99%D7%AA)(לכל מפתח ציבורי קיים אך ורק מפתח פרטי יחיד המתאים לו, ולהפך.

כדי להצפין מסר בשיטה זו על המצפין להשיג לידיו עותק אותנטי של המפתח הציבורי של המקבל, שבעזרתו הוא מצפין ושולח לו את המסר. רק המקבל מסוגל לשחזר את הטקסט המוצפן בעזרת המפתח הפרטי המתאים שברשותו. ביטחון שיטת המפתח הציבורי נשען על הקושי שב[חישוב](https://he.wikipedia.org/wiki/%D7%97%D7%99%D7%A9%D7%95%D7%91) המפתח הפרטי מתוך המפתח הציבורי. מסיבה זו מכונה שיטה זו "א-סימטרית", בניגוד לשיטת הצפנה [סימטרית](https://he.wikipedia.org/wiki/%D7%A6%D7%95%D7%A4%D7%9F_%D7%A1%D7%99%D7%9E%D7%98%D7%A8%D7%99), שבה מפתח הפענוח זהה למפתח ההצפנה

**המנגנון – חתימה דיגיטלית**

המטרה – מטרתה לאשר מסמך כלשהו, ולהיות בטוח מי האדם הספציפי שחתם.- חתימה דיגיטלית מבחינת היכולות שלה הרבה יותר חזקה מחתימה רגילה, אם לא הייתה חתימה דיגיטלית היה מאוד קשה לעשות עסקים.

חתימה דיגיטלית היא תת-קבוצה של מושג כללי הנקרא חתימה אלקטרונית מקובל לראות בחתימה אלקטרונית שם כללי לאמצעי [אלקטרוני](https://he.wikipedia.org/wiki/%D7%90%D7%9C%D7%A7%D7%98%D7%A8%D7%95%D7%A0%D7%99%D7%A7%D7%94) מסוים המפיק מידע כגון: סמלים (תווים או מספרים), [צלילים](https://he.wikipedia.org/wiki/%D7%A6%D7%9C%D7%99%D7%9C) או תמונות, משויך למדיה אלקטרונית כלשהי ומאפשר [אימות](https://he.wikipedia.org/wiki/%D7%90%D7%99%D7%9E%D7%95%D7%AA_%D7%96%D7%94%D7%95%D7%AA) המידע או זיהוי בעל האמצעי. חתימה אלקטרונית מקבילה במובנים מסוימים ל[חתימה](https://he.wikipedia.org/wiki/%D7%97%D7%AA%D7%99%D7%9E%D7%94) פיזית כגון חתימה [ידנית](https://he.wikipedia.org/wiki/%D7%9B%D7%AA%D7%91_%D7%99%D7%93_(%D7%9B%D7%AA%D7%91)) בכלי כתיבה או באמצעים פיזיים אחרים.

מי שרוצה ליצור מסמך עם חתימה דיגיטלית צריך ליצור 2 מפתחות, אחד הצפנה אחד פענוח (שמפורסם ופומבי) עם מספר אקראי גדול ויחודיים, בעזרת המפתחות חותמים דיגיטלית מצרפים למסמך hash code\צאק סאם ועושים לו הצפנה.

חתימת דיגיטלית יותר בטוחה מחתימה פיזית בגלל האלגוריתם ותקף בביהמ"ש בכל העולם.

איך יודעים שהטקסט מקורי -

1. צריך להשיג מפתח פומבי שהיה מפורסם בעת היצירה, והמפתח מתאים רק למפתח שהצפינו ע"י את hash code ואז לפענח את הטקסט.

2. עושים בדיקה שהאש קוד לא השתנה.

(Hash code) צ'ק סאם – cheek sum -

מספר שהוא מחושב מאינפורמציה שיש לו, נניח יש טקסט ובטקסט יש תמונה יש אלגוריתם שהוא מהטקסט הזה מחשב מספר שאורכו מוגדר מראש והמספר הזה ישתנה אם נשנה משהו בתוך הטקסט, המספר הזה נקרא צק סאם .

ב[מדעי המחשב](https://he.wikipedia.org/wiki/%D7%9E%D7%93%D7%A2%D7%99_%D7%94%D7%9E%D7%97%D7%A9%D7%91) **סיכום ביקורת**: **Checksum** הוא [קוד לזיהוי שגיאות](https://he.wikipedia.org/wiki/%D7%A7%D7%95%D7%93_%D7%AA%D7%99%D7%A7%D7%95%D7%9F_%D7%A9%D7%92%D7%99%D7%90%D7%95%D7%AA), המאפשר זיהוי של שגיאות .

ספרת ביקורת זאת דוגמה לצאק סאם – ספרה שנגזרת מהספרות הקודמות , תפקידה לוודא שהספרות שנמצאות לפניה נכונות. זה נותן אפשרות לא לטעות בהקלדת המספר (למשל ת"ז – שמונה ספרות והתשיעית הינה ספרת ביקורת שמוודא ששמונת הספרות לפניה נכונות)

לפני ששולחים מסמך מוסיפים צאק סאם – אומר שאי אפשר לשנות את המסמך, ואם רוצים לשנות את המסמך צריך לשנות גם את הצאק סאם. שבודקים צאק סאם בודקים שאין שינויים בדרך במסמך.

חתימה דיגטלית – המשתמש כותב מסמך כלשהו וכדי לוודא שאין שגיאות במסמך הוא מוסיף צא קסאם, המשתמש צריך ליצור 2 מפתחות מפתח הצפנה ומפתח פענוח, המפתח להצפנה הפעם יהיה מפתח פרטי והמפתח לפענוח יהיה פומבי. המפתח הפומבי נמצא אצל כולם ולכן ברגע שהמשתמש מפיץ את המסמך כולם יכולים לראות וזה יכול לשמש כהוכחה שבאמת אותו משתמש הוא זה שכתב את המסמך.

**בלוק צ'יין (blockchain)**

המטרה – לעשות רשימת טרנזקציות \ נתונים שלא ניתן לשנות, לבנות מנגנון שלא יהיה ניתן לשנות בעתיד את המסמך.

בלוקצ'יין היא תפיסה טכנולוגית במחשוב המאפשרת פעילות עסקית מאובטחת באינטרנט ואימות של טרנזקציות עסקיות בין צדדים שונים ללא צורך בישות ניהול מרכזית . את הגורם המנהל מחליפים "בלוקים" מוצפנים של מידע הנוצרים באמצעות שיתוף מבוסס רשת תקשורת מסוג עמית לעמית , בלוקצ'יין מיועד להגיע להסכמה בין גורמים שונים ובלתי תלויים על בלוקים של מידע שמחוברים בשרשרת. כל בלוק כולל מזהה וגיבוב של תוכן הבלוק הקודם וכן מתחבר אליו. כך נוצר מבנה נתונים מבוזר שעל תוכנו יכולים להסכים כל הגורמים המעורבים. אין אפשרות לשנות את תוכן הבלוקים מרגע שהם נקבעו.

למה אי אפשר לשנות בבלוקציין? כי יש כבר חתימה, והוא כבר נמצא אצל גורמים רבים. הבלוקציין נמצא לא רק במחשב אחד אלא באוסף מחשבים.

**ביטקויין – bitcoin**

הוא [מטבע](https://he.wikipedia.org/wiki/%D7%90%D7%9E%D7%A6%D7%A2%D7%99_%D7%AA%D7%A9%D7%9C%D7%95%D7%9D) [ממוחשב](https://he.wikipedia.org/wiki/%D7%9E%D7%97%D7%A9%D7%95%D7%91) [ומבוזר](https://he.wikipedia.org/wiki/%D7%9E%D7%98%D7%91%D7%A2_%D7%9E%D7%91%D7%95%D7%96%D7%A8). הגרסה הראשונה של [הפרוטוקול](https://he.wikipedia.org/wiki/%D7%A4%D7%A8%D7%95%D7%98%D7%95%D7%A7%D7%95%D7%9C_%D7%AA%D7%A7%D7%A9%D7%95%D7%A8%D7%AA) וה[תוכנה](https://he.wikipedia.org/wiki/%D7%AA%D7%95%D7%9B%D7%A0%D7%94) פותחה בנובמבר 2008 על ידי אדם או קבוצת אנשים המכנים עצמם [סאטוֹשי נַקאמוֹטוֹ](https://he.wikipedia.org/wiki/%D7%A1%D7%90%D7%98%D7%95%D7%A9%D7%99_%D7%A0%D7%90%D7%A7%D7%90%D7%9E%D7%95%D7%98%D7%95)

להבדיל מכסף מסורתי, הביטקוין הוא מטבע עצמאי לחלוטין שאינו תלוי בגוף מרכזי. במקום זאת, ביטקוין הוא רשומה בקובץ ציבורי המכונה "שרשרת בלוקים" \ "[בלוקצ'יין](https://he.wikipedia.org/wiki/%D7%91%D7%9C%D7%95%D7%A7%D7%A6%27%D7%99%D7%99%D7%9F)" ניתן לנהל/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.

הביטקוין אינו מופק או מנוהל על ידי [ממשלה](https://he.wikipedia.org/wiki/%D7%9E%D7%9E%D7%A9%D7%9C%D7%94) או [בנק מרכזי](https://he.wikipedia.org/wiki/%D7%91%D7%A0%D7%A7_%D7%9E%D7%A8%D7%9B%D7%96%D7%99) של מדינה כלשהי. במקום זאת, הביטקוין מבוסס על מנגנוני [קריפטוגרפיה](https://he.wikipedia.org/wiki/%D7%A7%D7%A8%D7%99%D7%A4%D7%98%D7%95%D7%92%D7%A8%D7%A4%D7%99%D7%94) ורשת תקשורת [עמית לעמית](https://he.wikipedia.org/wiki/%D7%A2%D7%9E%D7%99%D7%AA_%D7%9C%D7%A2%D7%9E%D7%99%D7%AA). תהליך הנפקת מטבעות חדשים למחזור מכונה "כרייה" באנלוגיה ל[כריית](https://he.wikipedia.org/wiki/%D7%9B%D7%A8%D7%99%D7%99%D7%94) [זהב](https://he.wikipedia.org/wiki/%D7%96%D7%94%D7%91). בתהליך זה יש להקדיש כוח חישוב רב בו מונפקים מטבעות חדשים הניתנים לשימוש.

יתרון חשוב של הביטקוין כאמצעי תשלום הוא הנגישות לשימוש בו ברחבי העולם: ניתן להעביר כספים ממדינה למדינה תוך דקות ספורות. עם זאת, ישנם גם חסרונות לביטקוין. הראשון בהם הוא הקושי הטכני להשתמש בביטקוין באינטראקציות פשוטות, מאחר שהמטבע, בניגוד לזה "המסורתי", ניתן לשימוש באמצעות [מחשב](https://he.wikipedia.org/wiki/%D7%9E%D7%97%D7%A9%D7%91) או [סמארטפון](https://he.wikipedia.org/wiki/%D7%A1%D7%9E%D7%90%D7%A8%D7%98%D7%A4%D7%95%D7%9F), ולכן זקוק למקור אנרגיה [חשמלי](https://he.wikipedia.org/wiki/%D7%97%D7%A9%D7%9E%D7%9C) ולחיבור ל[אינטרנט](https://he.wikipedia.org/wiki/%D7%90%D7%99%D7%A0%D7%98%D7%A8%D7%A0%D7%98) כדי לבצע כל פעולה של העברת כספים.

[איך עובד הביטקויין – A רוצה לשלוח לB ביטקוויין, כדי לעשות את זה הוא צריך ארנק אלקטרוני בנוסף הוא צריך את מס' ארנק של B לאחר מכן הוא צריך להכניס כמה כסף הוא רוצה לשלוח מהביטקויין וכמה העמלה שהוא מוכן לשלם עבור טרנזקציה ( אפשר להכניס גם 0 אבל אז יהיו השלכות במהירות העברה) , הארנק האלקטורני שולח את הנתונים האלה לאוסף תוכנות שנקרא מיינרים (כורה) ]

מה עושה הכרייה? מקבלת כמות גדולה של טרנזקציה ומנסים לבנות בלוק חדש בתוך בלוקציין של ביטקויין, לכל מיינר (למעשה מחשב) יש בתוכו בלוקציין של כל הטרנזקציות הקודמות.

מי שרוצה לשלוח את הכסף מהר יותר צריך לשלם עמלה גדולה יותר.

איפה אפשר לקנות ולמכור – בת"א יש כספומט וכדי לקבל את הכסף צריך להכניס מס' ארנק ומס' מפתח אישי.

לביטקויין למעשה אין מטבע פיזי, מודפס על שטר.

בבלוקציין כתוב שכסף מועבר מבין אדם אחד לשני וכמה סכום יש לכל בן אדם.

כל אחד יכול לפתוח ארנק חדש ובארנק דיגיטלי כתוב רק מס' ארנק.

מה עושה מחשב למיינר ? מקבל אינפורמציה שמישהו מעביר כסף למישהו אחר ומנסה לבנות בלוק חדש לבלוקצ'יין.

ניתן לשלוח ביטקויין גם בפתק – כותבים בפתק מס' ארנק ופרייבט קי.

ארנק זה איזשהי אפליקצייה לשליחה ולקבלת נתונים.

מחיר הביטקויין עולה בגלל הביקוש, פיראמידה .

**ארנק-** מטבעות ביטקוין הם רשומה ייחודית בקובץ ציבורי המכונה "שרשרת בלוקים" [בלוקצ'יין](https://he.wikipedia.org/wiki/%D7%91%D7%9C%D7%95%D7%A7%D7%A6%27%D7%99%D7%99%D7%9F). ניתן לנהל/להשתמש במטבעות בעזרת "**ארנק**", שהוא תוכנה המחוברת לרשת המטבע (לכל מטבע רשת משתמשים משלו) ויכולה לנהל שליחה וקבלת תשלומים. ארנק ביטקוין יכול להיות מאוחסן במחשב מקומי או על שרת מרוחק. הארנק מציג את המידע על כמות הכסף שיש למשתמש מסוים, כולל היסטוריית השימוש בו והיתרה שלו בסך כל הכתובות המנוהלות דרך אותו ארנק. מערכת ביטקוין היא מערכת מבוזרת, כלומר, כל אחד יכול להחזיק ארנק משלו, כך שלכל אחד יש יכולת עצמאית לניהול מלא של כספו, ללא מעורבות של גורם מנהל מרכזי. המערכת צריכה עדיין להבטיח שבעת תשלום לא 'יומצאו' מטבעות שאינם קיימים, ושסכום שהועבר בתשלום אכן גרע מטבעות בסך המתאים מכתובת השולח כך שלא יוכל להשתמש בהם בתשלומים נוספים.

**העברת כספים -**העברה היא הוראה מוצפנת, חתומה דיגיטלית, שנשלחת לרשת המטבע על ידי בעלי הארנק, להעביר סכום מארנקו לארנק אחד אחר. ההעברה משודרת לכל משתמשי ביטקוין דרך רשת התקשורת העולמית - האינטרנט. קיים [ספר חשבונות](https://he.wikipedia.org/wiki/%D7%A1%D7%A4%D7%A8_%D7%97%D7%A9%D7%91%D7%95%D7%A0%D7%95%D7%AA) דיגיטלי ומבוזר שנגיש לכל אחד ברשת שבו רשומות כל העברות הכספים ההיסטוריות מיום הקמת הביטקוין. ספר חשבונות זה מחולק ל'בלוקים', בכל בלוק ישנה כמות מסוימת של רישומי העברות כספים החל מסיום חישוב הבלוק הקודם. כך שלמעשה אם מחברים את כל הבלוקים, מקבלים יומן העברות כספים של כל פעילי הביטקוין מאז הקמתו ועד לרגע הנוכחי.

**יצירת הכסף -** יצרני הבלוקים, הנקראים גם "כורים", בונים כל הזמן תיעוד של העברות הכספים האחרונות ברשת המטבע. בלוק הוא הבסיס התפעולי המאפשר שימוש תקין במטבע. יצרנים אלו בעצם מבצעים את העבודה שהבנקים עושים היום. במבנה התפעולי ארוך הטווח של הביטקוין, מקור המוטיבציה להמשיך ולבצע את תהליך הכרייה הוא השכר שמקבלים הכורים עבור פעולת העיבוד הדורשת זמן (חשמל ותחזוקה) וחומרה ייעודיים. הכורה מקבל תשלום מסוים בצורת אחוז מתוך העברת הכספים שנרשמו בבלוק, מעין 'עמלת העברה'. גובה העמלה נקבע על ידי מבצע העסקה, קרי, המשתמש. צורת תשלום שנייה לכורה היא סכום מוגדר מראש של מטבעות ביטקוין שנוצרים בתהליך העיבוד. תהליך זה מתרחש בממוצע כל 10 דקות ברשת ביטקוין. צורת חישוב זו של תגמול על יציר

**הצפנה -**

A רוצה לשלוח נתונים לB בצורה סודית.

לB צריך להיות 2 מפתחות , אחד שיודע לעשות הצפנה ואחד לפענוח, לכל משתמש באינטרנט יש זוג אחר.

ליצירת מפתחות צריך מספר רנדומלי ומאוד גדול ולכן זה מקשה על גילוי הקוד של המפתח.

המפתח לפענוח הוא מפתח פרטי , B שומר אותו ולא נותן לאף אחד.

המפתח למצפנה הוא מפתח ציבורי .

כדי שA ישלח את המידע לB היא צריכה את המפתח הסודי ועושה הצפנה ,

לאחר הצפנה הנתונים מוצפנים (למשל טקסט יהפוך לג'יבריש),

לB יש מפתח לפענוח ולכן רק הוא יוכל לקרוא את הנתונים שA שלחה.

רק מי שייצר את ההצפנה יכול לשנות ולערוך את המפתח.

מפתחות -

כל משתמש מכין לעצמו זוג מפתחות: מפתח ציבורי שהוא מפתח הצפנה הנגיש לכל ומפתח פרטי  מתאים, הנשמר בסוד ומשמש לפענוח. ההתאמה היא [חד-חד-ערכית](https://he.wikipedia.org/wiki/%D7%97%D7%93_%D7%97%D7%93_%D7%A2%D7%A8%D7%9B%D7%99%D7%AA)(לכל מפתח ציבורי קיים אך ורק מפתח פרטי יחיד המתאים לו, ולהפך). כדי להצפין מסר בשיטה זו על המצפין להשיג לידיו עותק אותנטי של המפתח הציבורי של המקבל, שבעזרתו הוא מצפין ושולח לו את המסר. רק המקבל מסוגל לשחזר את הטקסט המוצפן בעזרת המפתח הפרטי המתאים שברשותו. ביטחון שיטת המפתח הציבורי נשען על הקושי שב[חישוב](https://he.wikipedia.org/wiki/%D7%97%D7%99%D7%A9%D7%95%D7%91) המפתח הפרטי מתוך המפתח הציבורי. מסיבה זו מכונה שיטה זו "א-סימטרית", בניגוד לשיטת הצפנה [סימטרית](https://he.wikipedia.org/wiki/%D7%A6%D7%95%D7%A4%D7%9F_%D7%A1%D7%99%D7%9E%D7%98%D7%A8%D7%99), שבה מפתח הפענוח זהה למפתח ההצפנה (על כל פנים ניתן לחישוב בקלות מתוך מפתח ההצפנה).