

# ביטקוין ושרשראות בלוקים

# Bitcoin and Blockchains

אראל סגל-הלוי

מקורות:

\* המאמר של Satoshi Nakamoto משנת 2008

\* הקורס של Tim Roughgarden, הרצאות 9-10

\* הספר של Parkes & Seuken, פרק 21

\* מצגת של אביב זוהר

כלכלה

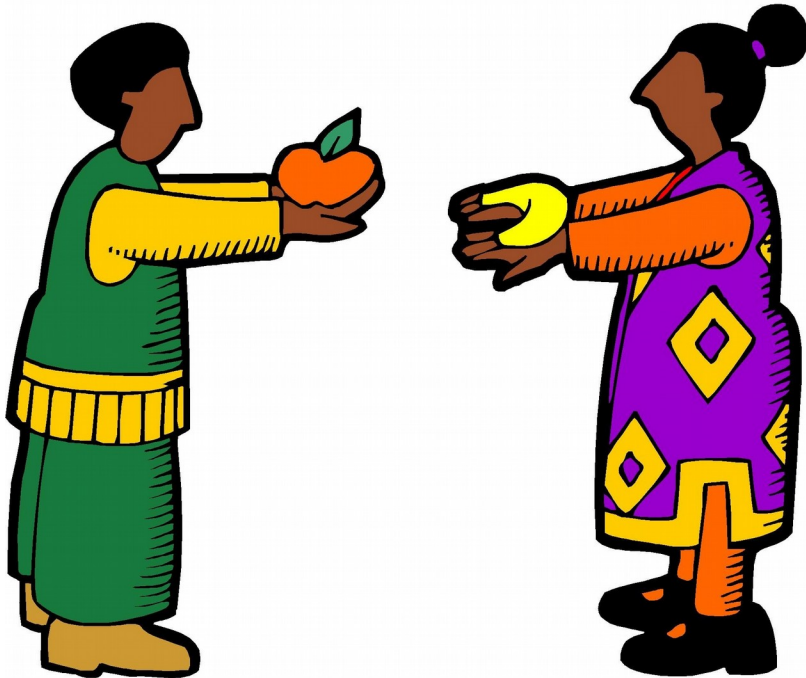
מדעי המחשב



מתמטיקה

# מה זה בכלל כסף ולמה צריך אותו?

- מסחר בין שני אנשים יכול לשפר את התועלת של שניהם.
- סחר-חליפין הוא יעיל אבל דורש התאמה הדדית ברצונות: א רוצה את הסחורה של ב ולהיפך.
- ראינו דוגמאות לכך בתחילת הקורס הזה – אלגוריתם מעגלי-המסחר להחלפת בתיים.



# מה זה בכלל כסף ולמה צריך אותו?

- כסף משמש לתיווך במסחר.
- אדם נותן חפץ בתמורה לכסף, כי הוא מאמין שבעתיד, יוכל לתת את הכסף בתמורה לחפץ אחר.

# תנאים הכרחיים למטבע

- (1) קשה לייצר מטבע (אחרת אף אחד לא ייתן תמורתו חפצים – כולם ייצרו בעצמם).
- (2) קל להוכיח שיש לי מטבע.
- (3) אי-אפשר לשכפל – לשלם וגם להשאיר את המטבע אצלי (double-spend).

התנאים לא מספיקים – גם אם כל התנאים מתקיימים, עדיין צריך אמו · במטבע.

זהב (או מתכות יקרות אחרות) כמטבע

(1) קשה לייצר – אפשר לכרות מהאדמה אבל זה לוקח הרבה זמן.

(2) קל להוכיח – כולם רואים שאני מחזיק זהב.

(3) אי-אפשר לשכפל – כששילמתי, הזהב כבר לא אצלי.



# שטרות מנייר

- (1) קשה לייצר – יש אמצעים נגד זיוף.  
מצד שני – הממשלה עצמה יכולה להחליט  
להדפיס כסף מסיבות פוליטיות.
- (2) קל להוכיח – כולם רואים מי מחזיק שטר.
- (3) אי-אפשר לשכפל – כששילמתי, השטר  
כבר לא אצלי.

# חשבון אלקטרוני בבנק מסורתי

(1) קשה לייצר - אא"כ פורצים למחשבי הבנק.  
מצד שני - הבנק יכול לייצר כסף ע"י הלוואות.

(2) קל להוכיח - הבנקים שומרים רישומים  
מפורטים של כמה כסף שייר למי.  
מצד שני - לא כל אחד זכאי לפתוח חשבון.

(3) אי אפשר לשכפל - הבנקים מפקחים על  
היתרות, כל קניה מורידה את היתרה שלך.  
מצד שני - תיתכן מעילה או פריצה.



# סלעי-גלגל - יאפ (Yap)

(1) קשה לייצר - אפשר להביא מאיים סמוכים אבל זה לוקח הרבה זמן.

(2) קשה להוכיח - אם קיבלתי מטבע, יהיה לי מאד קשה לסחוב אותו הביתה.



Eric Guinther - English Wikipedia

הפתרון שלהם: במקום  
לסחוב - הם פשוט **זוכרים**  
למי שייך כל מטבע!  
- קהילה קטנה - קל לזכור.

# מטבעות קריפטוגרפיים

"מטבע" מוגדר כאוסף של עסקאות, ביתר פירוט:

"We define an electronic coin as **a chain of digital signatures**. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership." (Satoshi Nakamoto, 2008, <https://bitcoin.org/bitcoin.pdf>)

# מטבעות קריפטוגרפיים

(1) קשה לייצר - דורש **אמו** .

(2) קל להוכיח - דורש חתימות דיגיטליות <--

(3) אי-אפשר לשכפל - דורש אלגוריתם <--

# מושגים בסיסיים בקריפטוגרפיה

מערכת חתימה דיגיטלית כוללת כמה רכיבים:

- אלגוריתם ייצור זוגות (מפתח סודי - < מפתח ציבורי)

- *ssh-keygen*

- *gpg --gen-key / --list-keys*

- *gpg --armor --export/ --export-secret-keys*

- אלגוריתם חתימה בעזרת מפתח סודי:

- *gpg --default-key=BF8C1203 --clearsign message.txt*

- אלגוריתם אימות בעזרת מפתח ציבורי:

- *gpg --verify message.txt.asc*

- מפתח ציבורי הוא כמו "שם משתמש" גלובלי.

# איפה נמצא המטבע?

**הגדרה:** "מטבע קריפטוגרפי" הוא רשימה מקושרת-אחורה של הודעות מהצורה:

(1) "מטבע נוצר ונמסר למפתח-ציבורי א".

(2) "א שילם את המטבע שקיבל בהודעה 1, למפתח-ציבורי ב" [חתימה ע"י א].

(3) "ב שילם את המטבע שקיבל בהודעה 2, למפתח-ציבורי ג" [חתימה ע"י ב]

(4) ...

מי שקורא את השרשרת, יכול לוודא שהיא תקינה ע"י אימות כל ההודעות בעזרת המפתחות הציבוריים. כך אפשר לדעת למי שיך המטבע.

# מניעת שיכפול

הבעיה העיקרית ברשימה המקושרת היא -

איך מונעים תשלום כפול (*double-spending*)?

מה יקרה למשל אם ב ישלח במקביל שתי הודעות:

(1) "ב שילם את המטבע שקיבל בהודעה 2,

למפתח-ציבורי ג" [חתימה ע"י ב]

(2) "ב שילם את המטבע שקיבל בהודעה 2,

למפתח-ציבורי ד" [חתימה ע"י ב]

לכאורה כל אחד יכול לשכפל את המטבעות שלו –  
לקנות כמה דברים באותו מטבע!

זה האתגר העיקרי שפותרת מערכת ביטקוין.

# איך מונעים שיכפול מטבעות? (א)

**דרך א - גוף מרכזי (כמו ויזה / פייפאל):**

- הקונה שולח בקשת תשלום למרכז;
- המרכז בודק שהבקשה חוקית;
- המרכז שולח אישור למוכר;
- המוכר נותן את החפץ לקונה.

**הבעיה – ריכוזיות – כל המערכת תלויה בגוף אחד.**

• אנשים רבים, במיוחד במדינות עולם שלישי, לא

זכאים לפתוח חשבון בבנק או בפייפאל.

• **דוגמה מונצואלה:**

<https://cryptohustle.com/using-bitcoin-to-survive-in-venezuela>

# איך מונעים שיכפול מטבעות? (ב)

**דרך ב – הצבעה בין כל המשתמשים:**

- הקונה מפרסם בקשת תשלום ברשת-המשתמשים.
- כל משתמש בודק שהבקשה חוקית.
- המוכר נותן את החפץ לקונה רק אם הרוב אישרו.

**הבעיה – התחזות (Sybil Attack)**

**ע** .. יכול ליצור הרבה משתמשים ולהשיג רוב.

אפשר לדרוש הרשמה, אבל אז חוזרת הריכוזיות..

מערכות עם הרשמה נקראות **permissioned**.

מערכות ללא הרשמה נקראות **permissionless**.

ביטקוין היא מערכת **permissionless**.



# איך מונעים שיכפול מטבעות? (ג)

הדרך של ביטקוין - הוכחת-עבודה (proof-of-work):

- הקונה שולח בקשת תשלום לרשת.
- כל משתמש בודק שהבקשה חוקית ומנסה לאשר.
- כדי לאשר בקשה  $m$ , צריך לפתור חידה קשה -  
להפוך פונקציה חד-כיוונית - למצוא  $x$  כך ש:

$$\text{SHA256}(m+x) < 2^{224} / D$$

כאשר  $D$  הוא מספר המייצג את רמת הקושי.

- הראשון שמצליח לפתור את החידה - שולח את הבלוק עם הפתרון לכולם וכך מצרפו לשרשרת.

הדגמה חיה: <http://blockchain.mit.edu/how-blockchain-works>

התחזות לא תעזור - המערכת חסינה ל-Sybil!

# שרשרת הבלוקים - מושגים

האישור מתבצע לא על כל עיסקה בנפרד, אלא על **בלוקים** של עסקאות (מכאן המושג **blockchain**).

- בלוק מכיל מגה-בייט אחד של עסקאות.
- כל עיסקה תופסת בערך 0.5 קילו-בייט.
- לכן בכל בלוק יש מקום לכ-2000 עסקאות.

- פתרון החידה (x) נקרא **nonce**.
- תהליך מציאת ה-**nonce** נקרא **כריה (mining)**.
- רמת הקושי (L) נקבעת באופן דינמי כך שהזמן הדרוש למציאת **nonce** יהיה כ-10 דקות (כדי שהבלוק יספיק לפעפע ברשת).

- **ציוד כריה:** <https://www.bitcoinmining.com/bitcoin-mining-hardware/>

# מה מרויחים הכורים?

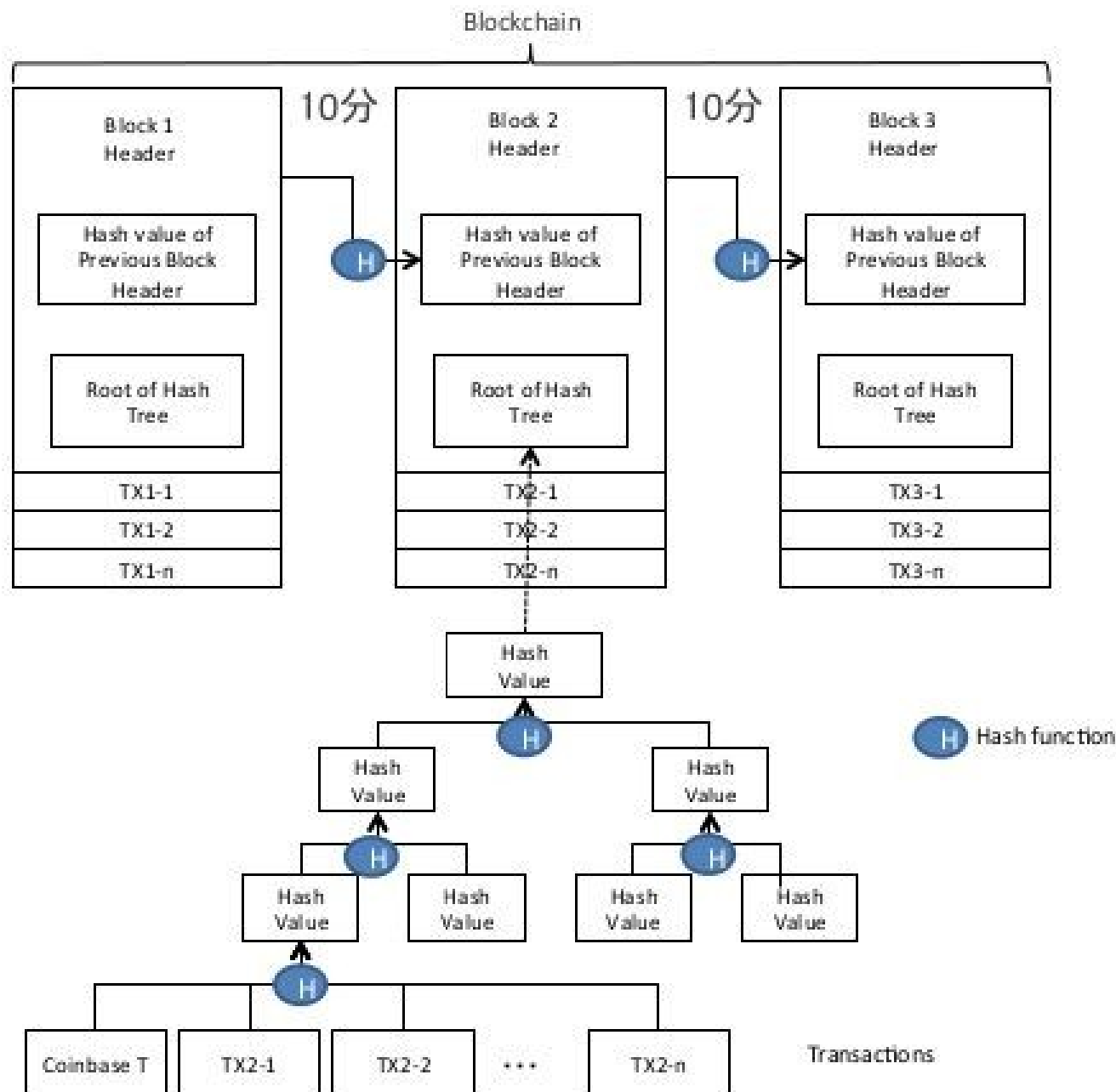
הכריה דורשת זמן וחשמל – מה יוצא להם מזה?

- "דמי כריה" קבועים (coinbase) – נוצרים "יש מאין"
  - התחילו מ-50 ביטקוין.
  - כל 210000 בלוקים – קטנים פי 2.
  - (הקוד: <https://github.com/bitcoin/bitcoin/blob/master/src/validation.cpp#L1186>)
  - לכן מספר הביטקוין המקסימלי יהיה כ-21 מיליון.
- "עמלת עסקה" משתנה – נקבעת ע"י המשלם בכל עסקה. ככל שהעמלה גבוהה יותר – יש סיכוי גדול יותר שאחד הכורים יסכים להכניס את העסקה לבלוק (<https://bitcoinfees.info/>).

# מבנה של שרשרת בלוקים

## Structure of Blockchain

Connection  
of Blocks



# מבנה של בלוק בשרשרת

מזהה (hash) של הבלוק הקודם;

- כ-2000 עיסקאות. כל עיסקה כוללת:
- מפתח ציבורי של שולח אחד או יותר;
- מפתח ציבורי של מקבל אחד או יותר;
- כמה כסף עובר מכל שולח לכל מקבל;
- קישור לעסקאות קודמות שבהן התקבל הכסף;
- "עמלת אישור".

- פתרון החידה המתאימה לתוכן הבלוק (nonce);
- מפתח ציבורי של המאשר הזוכה בדמי הכרייה.

סייר הבלוקים: <https://blockchain.info/>

עסקאות שעדיין לא אושרו: <https://blockchain.info/unconfirmed-transactions>

<https://testnet.blockchain.info/tx/cde964a61778103938fbc0d17ec932761f054301ac4caad1b9ea85409666f2a4>

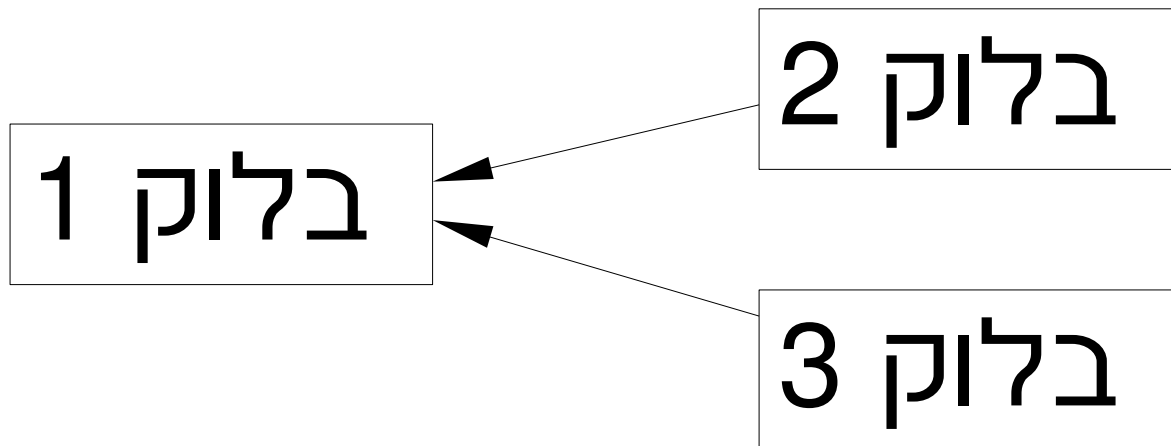
• ברז ביטקוין לניסויים: <https://testnet.manu.backend.hamburg/faucet>

# מועדוני כריה – mining pools

- לכורה בודד יש סיכוי מאד קטן למצוא בלוק.
- שיתוף פעולה בין כמה כורים מגדיל את הסיכוי.
- **במועדון כריה** העבודה על כל בלוק מתחלקת בין הרבה כורים; כשמישהו מוצא בלוק, המועדון לוקח את הכסף ומחלק אותו בין הכורים.
- <https://blockchain.info/pools>

# מזלגות ובלוקים יתומים

- ברגע שבלוק מאושר נשלח לרשת - כל שאר הכורים צריכים לזרוק את הבלוק שניסו לאשר, ולהתחיל לעבוד על בלוק חדש שבו ה"קישור לבלוק הקודם" הוא מזהה הבלוק החדש שאושר.
- אם שני כורים מאשרים בלוקים שונים בערך באותו זמן, נוצר **מזלג (fork)** בשרשרת הבלוקים.



# מזלגות ובלוקים יתומים

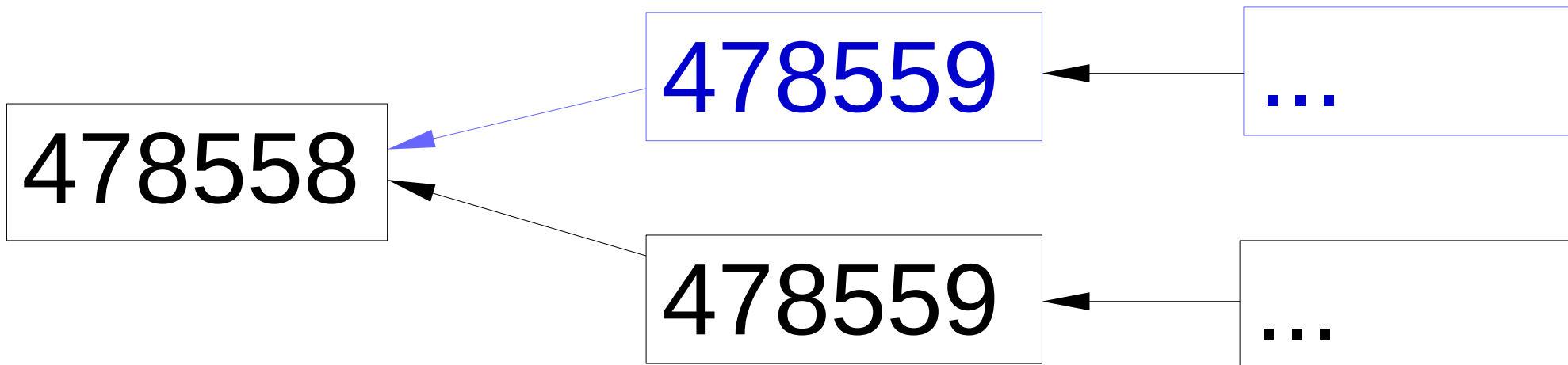
- איך מחליט כל כורה, לאיזה בלוק-קודם לקשר?
- כלל א: בחר את השרשרת הארוכה ביותר.
- כלל ב: אם יש כמה שרשראות ארוכות ביותר – קשר לבלוק ששמעת עליו מוקדם ביותר.
- בלוק שנמצא מחוץ לשרשרת הארוכה ביותר נקרא "יתום" (orphaned); העסקאות בו לא מאושרות.





# פיצולים מכוונים

- הקוד של ביטקוין פתוח, ויש ויכוחים בין המפתחים.
- כשלא מצליחים להכריע בויכוח, המטבע מתפצל.
- למשל: ב 1/8/2017 היה פיצול בשרשרת ביטקוין בגלל ויכוח על גודל הבלוק – להשאיר 1 מ"ב או להגדיל ל-8 מ"ב.
- הרוב תמכו ב-1 מ"ב; תומכי ה-8 מ"ב התפצלו וקראו לעצמם "Bitcoin Cash" - מטבע חדש:



# שרשראות בלוקים (blockchain)

- ביטקוין היה היישום הראשון של שרשרת בלוקים.
- אבל שרשרת בלוקים היא מושג כללי יותר –
- **מבנה-נתונים מבוזר להסכמה על סדר אירועים.**

• סוגי שרשראות בלוקים:

- **ציבורית** – כל אחד יכול לקרוא, לכתוב ולאשר.
- דרושה הוכחת-עבודה (PoW) או שיטה דומה.
- **קבוצתית** – כל אחד יכול לקרוא ולכתוב, אבל רק קבוצה נבחרת של מנהלים יכולה לאשר (ברוב).
- **פרטית** – רק המנהל יכול לכתוב ולאשר.

תוכנה לבניית שרשראות בלוקים: <https://www.hyperledger.org>

# מתקפות על שרשראות-בלוקים

# האם פרוטוקול ביטקוין אמיתי?

- פרוטוקול נקרא "אמיתי" אם התנהגות בהתאם לפרוטוקול ממקסמת את הרווחים.
- התשלומים לכורים נועדו לעודד אותם לפעול לפי הפרוטוקול.
- אבל יש כמה מקרים שבהם כדאי לכורה לפעול בניגוד לפרוטוקול. <--

# מתקפת תשלום-כפול (double-spend, 51%)

כורה המחזיק מעל 50% מכוח-הכרייה יכול לשלם פעמיים באותו מטבע, באופן הבא:

- נניח שהבלוק הנוכחי הוא בלוק א. התוקף קונה חפץ, והתשלום מאושר בבלוק ב המקושר ל-א.
- התוקף כורה בלוקים המקושרים לבלוק א, עד שהשרשרת שלו ארוכה יותר מהשרשרת העוברת דרך בלוק ב.

• בלוק ב נעשה "יתום", והאישור מתבטל! לכן, תנאי הכרחי לאמיתיות של ביטקוין הוא שכוח-הכרייה של כל כורה יחיד קטן מ-50%.

מתקפת 51% במציאות:

<https://www.investopedia.com/news/bitcoin-gold-hack-shows-51-attack-real/>

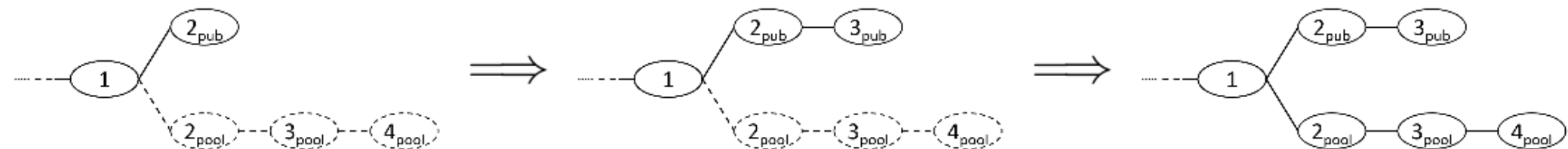
# מתקפת קרטל הכורים (mining cartel)

מועדון-כורים המחזיק מעל **שליש** מכוח-הכרייה יכול להרויח מהסתרת בלוקים שמצא.

נניח שהבלוק הנוכחי הוא א, והקרטל מצא בלוק ב המקושר אליו. במקום לפרסם את הבלוק, התוקף ממשיך לחפש בלוק ג המקושר לבלוק ב.

• **מקרה א:** מישהו אחר מצא בלוק ד המקושר לבלוק א – התוקף הפסיד את תשלום בלוק ב.

• **מקרה ב:** התוקף מצא בלוק ג – הוא ממשיך כך עוד כמה בלוקים ואז מפרסם את כל השרשרת.



# מתקפת קרטל הכורים (mining cartel)

- המתקפה גורמת לשאר הכורים לבזבז אנרגיה על בלוקים שבסוף יהפכו להיות יתומים.
- אפשר להוכיח, שאם הקרטל מחזיק לפחות  $1/3$ , הרווח לכורה בקרטל גדול יותר מהרווח לכורה מחוץ לקרטל (ראו סימולציה בקובץ `mining-cartel.ods`).
- לכן לכורים בודדים יש תמריץ להצטרף לקרטל!
- הקרטל גדל עד שהוא מגיע מחזיק מעל 50%.
- המתקפה מעולם לא נצפתה במציאות.
- מאמיני-ביטקוין מאמינים שהיא לא תקרה לעולם:

<http://hackingdistributed.com/2013/11/04/bitcoin-is-broken/>

# צליפת-עמלות (fee-sniping)

- בעתיד הקרוב, דמי-הכריה הקבועים (coinbase) יקטנו, ועמלת-העיסקה תהיה חלק משמעותי יותר מהשכר של הכורים.

- זה ייתן תמריצים חדשים להתנהגות לא-אמיתית.

- נניח, שבבלוק האחרון שנוסף לשרשרת, יש עיסקה עם עמלה מאד גבוהה.

- לכורה יש תמריץ להמשיך את הבלוק הלפני-אחרון, כדי שיוכל לשים בבלוק שלו את העיסקה הזאת ולקחת את העמלה לעצמו.

- זה נקרא **fee-sniping**.

- אם כולם יעשו כך – השרשרת תיתקע.



# שבירת-שיוויון אנוכית (selfish tie-breaking)

- לפי הפרוטוקול, במקרה של פיצול בשרשרת, כל כורה צריך להמשיך את הבלוק ששמע עליו ראשון.
- כשיש רק דמי-כריה קבועים, זה לא משנה.
- אבל כשיש גם עמלות-עיסקה משתנות – כדאי להמשיך דווקא את הבלוק שיש בו **פחות** עמלות, כי הוא משאיר **יותר** עמלות לכורים הבאים ומגדיל את הסיכוי ש"צלפי עמלות" ימשיכו אותו.

# חיתוך (undercutting)

- בניח שכמה כורים מבצעים שבירת-שיווין אנוכית.
- אז כדאי לכורים אחרים "לחתוך" את הבלוק הנוכחי - להמשיך את הבלוק הקודם בבלוק שמכיל פחות עמלות, בתקוה שה"אנוכיים" ימשיכו אותך.
- כשכולם "חותכים" אחד את השני, נוצרת פרימת-שוק (unraveling), וכולם יוצרים בלוקים עם מעט מאד עמלות.
- כל המתקפות האלו עדיין לא נצפו בשטח כי העמלות עדיין נמוכות, אבל מה יהיה בעתיד?

?