**האוניברסיטה הפתוחה**

**המחלקה למתמטיקה ולמדעי המחשב**



## עבודה מסכמת במדעי המחשב:

# מערכת יומני ביקורת מאובטחת כשירות ענן מבוססת בלוקצ'יין

# Secured Audit Logs as a Service – Blockchain & Cloud (SALaaS)

עבודה זו מוגשת כחלק מהדרישות לקבלת תואר

"מוסמך למדעים" M.Sc. במדעי המחשב

באוניברסיטה הפתוחה

החטיבה למדעי המחשב


מגיש: ניר מקמל, ת.ז 034490698

מנחה: פרופ' אהוד גודס


אוקטובר 2023

## תקציר

בעבודה זו אסקור את חשיבות יומני ביקורת במערכות מידע, אסביר מהי רשת בלוקצ׳יין וסוגי רשתות בלוקצ׳יין כגון רשת פרטית, ציבורית ופדרלית.

אתן הסבר מפורט על אופן שמירה ואחזור מידע של יומני הביקורת ברשת בלוקצ׳יין, אעבור על הסבר של פתרונות העושים שימוש ברשת הבלוקצ׳יין, כפי שמובא במאמרים הבאים: מידע כללי על ביטקוין [9], אסקור במפורט את המאמרים בנושא יומני ביקורת על גבי רשת בלוקצ׳יין [1], [3] ו [4], אסקור בקצרה את המאמרים לגבי שימוש בטכנולוגיית ענן לרשתות בלוקצ׳יין [8] ו [2] ובנוסף אכלול מאמרים נוספים אשר יתנו מבט נוסף.

בעבודה זו אראה דרך חדשנית להתמודד עם אמינות יומני המידע שהם אחד מהכלים בתחום הזיהוי הפלילי הדיגיטלי (Computer forensics), תחום למציאת ראיות משפטיות בעולם הדיגיטלי.

בכדי להתחקות אחרי עקבות דיגיטליים יש צורך בקריאה של יומני מערכת ומקורות מידע נוספים בכדי לבצע זיהוי ברמה גבוהה היכול גם לשמש לראייה משפטית, אחת הבעיות המאתגרות היא: כיצד ארגונים יכולים לעמוד בתקנות פנימיות ו/או ממשלתיות, רגולציות, חוזים משפטים אם וכאשר הם נדרשים להוכיח ראיות אשר תקפות גם בבתי המשפט לצורך תביעה של תוקף או משתמש שחדר/חיבל במערכת בזדון או לצורך תחקיר תקלות שנעשו לא בזדון. אחת הדרכים החדשניות היא שימוש במערכת כשירות ענן מבוססת טכנולוגיית בלוקצ׳יין, המאפשרת מערכת המבצעת שמירה וניתוח יומני ביקורת בצורה מאובטחת ולא ניתנת לשינוי.

החלק היישומי של העבודה כולל פיתוח הפרויקט אשר מממש מערכת כשירות, המערכת מאפשרת שמירה וניתוח יומני ביקורת בצורה מאובטחת אשר לא ניתנת לשינוי. זאת על מנת להבטיח לארגונים יכולת לעמוד בתקנות, רגולציות, חוקי ממשל, חוזים משפטים כאשר הם נדרשים להוכיח ראיות אשר תקפות גם בבית המשפט לצורך תביעה של תוקף או משתמש שחדר/חיבל במערכת בזדון או לצורך תחקיר תקלות שהתרחשו במערכת.

**הפרויקט שפיתחתי התבסס על המאמרים העוסקים בנושא יומני ביקורת על גבי רשת בלוקצ׳יין [1], [3] ו [4], והמאמרים לגבי שימוש בטכנולוגיית ענן לרשתות בלוקצ׳יין [8] ו [2].**

המערכת כוללת מספר רכיבים, מרכיב המקבל את המידע למערכת, רכיב המעביר את נתוני הביקורת לתהליך אימות, חתימה ועד לרכיב אשר מבצע שמירה ברשת הבלוקצ׳יין פרטית וציבורית.

המערכת יכולה להיות מותקנת בתשתיות ענן ורשתות בלוקצ׳יין לצורך נגישות, אבטחה, יכולות גדילה דינמית בהתאם למידע הנדרש.

**המערכת מאפשרת למשתמשים המורשים יכולת שליפה ואחזור של יומני ביקורת הנדרשים לצורך ביקורת אבטחת מידע או עקב דרישה של מנהלי החברה או ארגוני ממשל לצורכי חקירה או תביעה.**

# תוכן עניינים

# 1. מבוא

בעבודה זו אסקור מספר מאמרים אשר הציעו דרך חדשנית ואמינה יותר לעומת מערכות שהיו מבוססות על תצורה ריכוזית אשר מנוהלת ע״י ארגון יחיד, נראה איך שימוש בטכנולוגיה מבוזרת, כגון רשת בלוקצ׳יין יכולה לשמש כמערכת לצורך שמירה וניתוח יומני ביקורת בצורה מאובטחת אשר לא ניתנת לשינוי, מערכת אשר תבטיח לארגונים יכולת לעמוד בתקנות, רגולציות, חוקי ממשק, חוזים משפטים כאשר נדרשים להוכיח ראיות שיהיו תקפות גם בבתי המשפט לצורך תביעה של תוקף או משתמש שחדר/חיבל במערכת בזדון או לצורך תחקיר תקלות שנעשו לא בזדון.

המערכות במאמרים השונים כוללות מספר רכיבים, רכיב המקבל את המידע למערכת ומעביר את נתוני הביקורת תהליך אימות, חתימה ושמירה ברשת הבלוקצ׳יין.

חלק מהמערכות של המאמרים משתמשות בתשתיות ענן ורשתות בלוקצ׳יין לצורך נגישות, אבטחה, יכולות גדילה דינמית בהתאם למידע הנדרש.

במאמרים הנסקרים המערכות מאפשרות למשתמשים המורשים יכולת שליפה ואחזור של יומני ביקורת הנדרשים לצורך ביקורת אבטחת מידע או דרישה של מנהלי החברה או ארגוני ממשל לצורכי חקירה או תביעה.

## 1.1. מבנה העבודה

- מבוא:
  - סקירה קצרה של טכנולוגיית בלוקצ׳יין.
  - סקירה על סוגי רשתות בלוקצ׳יין: פרטית, ציבורית, פדרלית והיברידית.
  - סקירה קצרה של חשיבות יומני ביקורת במערכות מידע.
  - סקירה קצרה על טכנולוגיית ענן ציבורי.
  - סקירה קצרה על זיהוי פלילי דיגיטלי
- הסבר על טכנולוגיית הצפנה ורשת בלוקצ׳יין.
- הסבר מפורט על שמירת ואחזור מידע של יומני הביקורת ברשת בלוקצ׳יין.
- הצגה והסבר של פתרונות העושים שימוש ברשת הבלוקצ׳יין, כפי שמובא במאמרים.
אסקור במפורט את המאמרים: [1], [3] ו [4], אסקור בקצרה את המאמרים [8] ו [2] ובנוסף אתייחס לכל שאר המאמרים.
- דיווח קצר על תוצאות הפרויקט המעשי בו מימשתי מערכת מבוססת ענן ורשת בלוקצ׳יין לאבטחת יומני ביקורת.

## 1.2. חשיבות העבודה

העבודה חשובה בכדי להעלות את המודעות של אבטחת המידע בארגונים ע״י העלאת רמת האבטחה לרמה גבוהה המאפשרת לארגונים להשתמש בנתוני המערכת לצורך ראיות, חקירה, זיהוי בעיות ושחזור אירוע פריצה, ע״י שימוש בטכנולוגיית בלוקצ׳יין ותשתיות ענן ציבורי, בכך העבודה מאפשרת מערכת מאובטחת אשר יכולה לגדול בצורה דינמית בהתאם לקצב שידור המידע לצורך שמירה מאובטחת.

## 1.3. רקע

כיום יש יותר ויותר מתקפות על שרתי מחשב, ולכן נדרשת הגנה ברמה גבוהה יותר יחסית לשנים קודמות.
לכן, ישנה חשיבות עליונה בהגנה על יומני הביקורת (Audit Logs) של מערכות הארגון, אחד היעדים המרכזיים של התוקפים היא מערכת יומני הביקורת בה נרשמים אירועי מערכת במידה והתוקף הצליח להשבית את מערכת יומני הביקורת, הוא יכול לשנות נתונים במערכת מבלי להשאיר עקבות ובכך משאיר את הארגון בלי יכולת לזהות שנתוני המערכת שונו. לדוגמא תוקף חדר למאגר הנתונים ועשה שינוי נתוני מאגר הנתונים, ובכך פוגע הן בנתוני החברה והן בלקוחות של החברה.
לכן, בכדי לתת מענה הולם לחולשות של אבטחת יומני ביקורת, נשתמש בטכנולוגיית בלוקצ׳יין אשר תוכל לספק לנו הגנה ויכולת אי-הכחשה ברמה גבוהה, היא תאפשר לארגונים לסמוך על המידע שנשמר ברשת הבלוקצ׳יין בזכות מהימנות רשת הבלוקצ׳יין, וגם בזכות התכונה של מערכת מבוזרת אשר מפחיתה ריכוזיות של גורם יחיד, אשר יש לו שליטה על המידע ויכול לשנות אותו במידה והוא השולט היחיד במערכת.
לכן מערכת כזו היא חשובה על מנת להעלות את רמת אבטחת המידע בארגונים ע״י אבטחה ברמה גבוהה המאפשרת לארגונים להשתמש בנתוני המערכת לצורך ראיות, חקירה, זיהוי בעיות ושחזור אירוע פריצה.

## 1.4. סקירה קצרה של טכנולוגיית בלוקצ׳יין

### 1.4.1. טכנולוגיית בלוקצ׳יין - רקע

ב31 לאוקטובר בשנת 2008 פורסם מאמר בשם ״ביטקוין : מערכת תשלומים אלקטרונית לקוח-לקוח״ [9].
המאמר מתאר טכנולוגיה מהפכנית שעד לשנת 2008 לא הייתה אפשרית בעולם, המאמר סוקר אפשרות מעשית לבצע עסקאות תשלומים ללא צורך בצד שלישי ( ממשלות, בנקים...).
הביטקוין היה המימוש הראשוני והמוצלח למערכת המבוססת על רשת בלוקצ׳יין, לאחר מכן מומשו עוד מטבעות דיגיטליים וטכנולוגיות מבוססות על רשת בלוקצ׳יין.

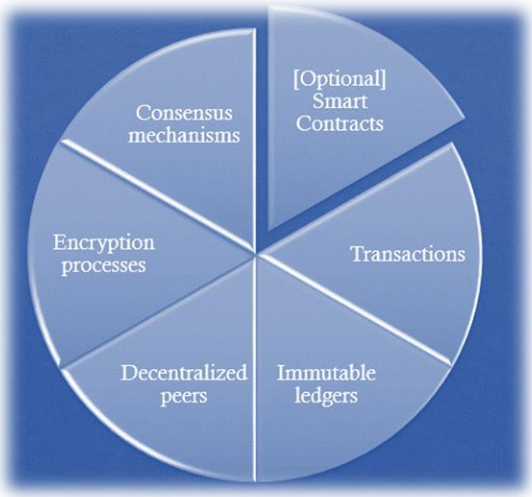
עם יציאתו של מטבע הביטקוין, ב2008 לראשונה, נחשפנו לטכנולוגית הבלוקצ׳יין שהיא הבסיס למערכות מבוזרות אשר מאפשרות לנהל יומן נתונים בלתי ניתן לשינוי שתומך גם בתצורה שאינה מצריכה תלות בגורם עניין יחיד ברשתות בלוקצ׳יין ציבוריות כגון ביטקוין.
ניתן לראות שטכנולוגיית הבלוקצ׳יין ישימה בתעשיות שונות ורבות כגון : משפטי, שרשרת אספקה, ממשלות, אנרגיה, מזון, מסחר, בריאות, ביטוח, נסיעות ותיירות השכלה ועוד ולא רק בתחום הפיננסי.
החידוש המרכזי שרשת בלוקצ׳יין הביאה לעולם הדיגיטלי הוא **האפשרות המעשית והבטוחה** להחליף מערכות ריכוזיות (כמו בנקים, מוסדות ועוד ) **למערכות מבוזרות,** ובכך לייתר את הצורך בתלות בבנקים או ארגונים המשמשים כצד שלישי מאושר בין שני צדדים הרוצים להחליף או לאמת מידע ביניהם.
לדוגמא אימות מסמך כמו דיפלומה של תואר ראשון יכול להתבצע ע״י הבלוקצ׳יין, במקום לגשת לנוטריון כדי לאשר את המקוריות של המסמך, ניתן להסתמך על רישום ברשת בלוקצ׳יין. **לכן במידה והישגי ההשכלה האקדמאית של האנשים תשמר על רשת בלוקצ׳יין ציבורית כל אחד בעולם יוכל לאמת את אמיתות התואר ללא צורך באישור נוטריוני.**

### 1.4.2. טכנולוגיית בלוקצ'יין - אבני היסוד ברשת

למעשה טכנולוגיית בלוקצ'יין מבוססת על שישה אבני יסוד אשר ביחד מהווים את היסודות המעשיים לשימוש ברשת בלוקצ'יין בתעשייה.

עד שנת 2008 הרעיון של מטבע דיגיטלי לא היה מעשי. רק שילוב של התכונות הבאות הוא מה שהפך את השימוש של רשת בלוקצ'יין למעשי, המהווה את הבסיס של המטבע הדיגיטלי הראשון בעולם, שהוא מטבע הביטקוין.

1. **תנועות** – (Transactions) — כל עסקה/תנועה נרשמת ביומן העסקאות ונחתמת ע"י השולח.
2. **יומן תנועות בלתי ניתן לשינוי** - (Immutable ledgers) –בכדי לשנות תנועה שנחתמה ביומן יש צורך במשאבים עצומים שעלותו הכספית אדירה, כך שבפועל ניתן לומר שתנועה אשר נחתמה היא בלתי ניתנת לשינוי.
3. **רשת מבוזרת** – (Decentralized peers) –בניגוד לפתרונות מרכזיים כמו בנקים, ממשלות וחברות מסחריות, זוהי מערכת רבת משתתפים מה שמאפשר להעלות את רמת האבטחה והצורך לתת אמון מערכת מרכזית המשתמשת בצד שלישי לצורך ביצוע עסקאות.
4. **מנגנוני הצפנה** (Encryption process) –ע"י שימוש בפרוטוקולי הצפנה מתקדמים, המידע נשמר בצורה מאובטחת ושלמה.
5. **מנגנון הסכמה כוללת** (Consensus mechanisms) –זהו החלק הכי חשוב במערכת הבלוקצ'יין, הצפנה וחתימה דיגיטלית הייתה קיימת גם לפני, וגם מנגנוני הסכמה כוללת בסיסיים, אך, גילוי מנגנון קונצנזוס הוכחת עבודה (PoW), הוא זה שפתר את בעיית "**התשלום הכפול**" (Double-spending) ברשת ציבורית, בעיה שבה ניתן לעשות שימוש נוסף במטבע דיגיטלי שכבר ניצלנו בתנועה אחרת.
6. **חוזים חכמים** (Smart contracts) – זוהי יכולת אופציונלית, המאפשרת לבצע פעולות חישוב וניהול נכסים, על גבי רשת הבלוקצ'יין לדוגמא השימוש בהם ברשת אתריום (Ethereum) [15] [18] [22]




*איור 1 אבני היסוד ברשת בלוקצ'יין*

### 1.5. סקירה על סוגי רשתות בלוקצ׳יין פרטית, ציבורית, פדרלית והיברידית

ישנן ארבע סוגי רשתות בלוקצ׳יין [15], לכל אחת מהן תכונות ומאפיינים ייחודיים משלה.

אחד הסוגים הידועים ביותר של רשתות בלוקצ׳יין, היא רשת **הבלוקצ׳יין הציבורי**. זוהי למעשה רשת מבוזרת הפתוחה לכל אחד. כל אחד יכול להצטרף לרשת ולהשתתף בתהליך הקונצנזוס, שהוא האופן שבו עסקאות מאומתות ומתווספות לבלוקצ׳יין. הדוגמה הידועה ביותר לבלוקצ׳יין ציבורי היא רשת הביטקוין.

סוג נוסף של רשת בלוקצ׳יין הוא **הבלוקצ׳יין הפרטי**. בניגוד לבלוקצ׳יין ציבורי, בלוקצ׳יין פרטי מורשה, כלומר רק אנשים או ארגונים מסוימים מורשים להצטרף לרשת ולהשתתף בתהליך ההסכמה. בלוקצ׳יין פרטי משמש לעתים קרובות ארגונים שרוצים לשמור על שליטה ברשת ובמשתתפים בה.

בנוסף לבלוקצ׳יין ציבורי ופרטי, ישנן גם רשתות **בלוקצ׳יין פדרליות**. רשתות אלה נמצאות בין בלוקצ׳יין ציבורי ופרטי, מכיוון שהן מבוזרות אך לא פתוחות לחלוטין. רשתות **קונסורציום** או **פדרליות** נשלטות בדרך כלל על ידי קבוצה של ארגונים, שלכל אחד מהם יש רמה מסוימת של שליטה על הרשת.

לכל אחת מהרשתות יש תכונות ומאפיינים ייחודיים משלה. בלוקצ׳יין ציבורי פתוח לכל אחד, בלוקצ׳יין פרטי, בלוקצ׳יין קונסורציום או מאוחד נשלטים על ידי קבוצת ארגונים המוגדרים מראש ויש ביניהם אמון.

### 1.5.1. רשת בלוקצ׳יין ציבורית

זוהי רשת מבוזרת פתוחה לציבור, משמעותה היא שכל אחד יכול להצטרף לרשת ולהשתתף בתהליך הקונצנזוס, שהוא האופן שבו עסקאות מאומתות ומתווספות לבלוקצ׳יין, אחד המאפיינים המרכזיים של מערכת בלוקצ׳יין ציבורי **שאין בה מנגנון הרשאה,** כלומר לא ניתן למנוע מאף אחד גישה לרשת. זאת בניגוד למערכות בלוקצ׳יין פרטיות, שיש בהן מנגנוני הרשאה אשר מאפשרים רק לאנשים או ארגונים מסוימים להצטרף לרשת.

רשתות בלוקצ׳יין ציבוריות מבוזרות ברחבי העולם, **הן <u>אינן</u> נשלטות על ידי ישות אחת.** הרשת מתוחזקת על ידי רשת של צמתים, לכל צומת יש יכולות מחשוב בכדי לבצע פעולות על גבי הרשת.

מכיוון שהצמתים מבוזרים ברחבי העולם, ובנוסף יש צורך להעלות את הקושי בכריית בלוק חדש, נדרשות מספר דקות בכדי להוסיף בלוק חדש לרשת.

לדוגמא ברשת הביטקוין שהיא רשת בלוקצ׳יין כל יצירה של בלוק חדש לוקח כ-10 דקות, אך זה לא מספיק, **<u>למעשה כדי להיות בטוחים שהעסקה נחתמה ותהיה בלתי ניתנת לשינוי צריך לחכות 60 דקות!</u>** (הזמן שלוקח לשישה אישורים).

אחד היתרונות של רשתות בלוקצ׳יין ציבוריות הוא שהן עמידות בפני חבלה וצנזורה. מכיוון שהרשת מבוזרת ופתוחה לציבור, והיא רשת ללא הרשאות, קשה לישות אחת לשלוט ברשת או לתפעל אותה. בנוסף, השימוש בטכנולוגיות הצפנה, כגון חתימות דיגיטליות, מסייע להבטיח את האבטחה והשלמות של הרשת.

**בעבודה זו אראה איך שימוש ברשת ציבורית ביחד עם רשת פרטית, מעלה את רמת הבטחון של יומני מערכת מפני שינוי או מחיקה ברשת בלוקצ׳יין ציבורית, כגון עיגון לרשת ביטקוין לצורך שמירה של הוכחות אשר יעידו על תקינות יומני ביקורת.**

### 1.5.2. רשת בלוקצ׳יין פרטית

רשת בלוקצ׳יין פרטית היא למעשה יומן תנועות דיגיטלי מבוזר, הרשת מנוהלת על ידי ארגון יחיד או קבוצה של משתתפים מורשים. בניגוד לרשת בלוקצ׳יין ציבורית, הפתוחה לכל אחד, ברשת בלוקצ׳יין פרטית יש מנגנוני הרשאה, רק גורמים מורשים, יוכלו להתחבר לרשת ולהשתתף בה.

כמו לרשתות בלוקצ׳יין ציבוריות, לרשתות בלוקצ׳יין פרטיות יש גם יתרון של ניהול פנקס בלתי ניתן לשינוי. בנוסף לרשתות פרטיות יש יתרון נוסף של אבטחה ופרטיות נתונים, אשר חשובים מאוד בתעשייה הפיננסית או בניהול נתונים רפואיים רגישים, מכיוון שהם מנוהלות על ידי ישות אחת, ובכך הן מציעות גם יותר שליטה וגמישות במונחים של מי רשאי לגשת לרשת ומה ניתן לעשות ברשת.

מאפיין מרכזי אחד של רשתות בלוקצ׳יין פרטיות הוא שלעתים קרובות הן משתמשות באלגוריתם קונצנזוס כדי להגיע להסכמה על מצב יומן תנועות. משמעות הדבר היא כי כל המשתתפים ברשת חייבים להסכים על תוקפן של עסקאות לפני שניתן להוסיף אותם ליומן תנועות. מה **שדורש אמון בין המשתתפים**, סוג רשת זאת מאפשרת **למשתתפים להגיע להסכמה מהירה** על תקינות בלוק חדש ללא צורך בתהליך כרייה איטי ויקר כמו ברשת ציבורית.

הרשאות קריאה וכתיבה ניתנת לפי רמת הרשאות שהגוף המנהל את הרשת הפרטית מחליט על מדיניות ההרשאות, דבר המאפשר להשיג רמת בטחון גבוהה של יומני מערכת מפני שינוי או מחיקה ברמה גבוהה, בנוסף לרשת פרטית יש יתרון של **קצב ביצוע פעולות ברשת, קצב העסקאות לשנייה גבוה יותר** בצורה משמעותית מרשת ציבורית, דבר המאפשר לעמוד בקצב הנדרש בכדי לטפל בהודעות של יומני המערכת שהמערכת מייצרת כל שניה.

**החיסרון של רשתות פרטיות הוא <u>שליטה של גוף יחיד</u>**, אשר יכול לחבל ברשת במידה ואין מספר גדול של צמתים ברשת הפרטית או שרמת אבטחת הרשת לא מספיק חזקה.

**חסרון נוסף הוא <u>העלויות והמשאבים</u>** הגדולים הנדרשים להקים ולתחזק רשת כזאת בארגון.

רשתות הבלוקצ׳יין הפרטיות הפופולריות הנמצאות בשימוש ע״י חברות וממשלות הן:
**היפרלד׳ר פבריק [21]** Hyperledger Fabric פלטפורמת בלוקצ׳יין פרטית בקוד פתוח המנוהלת על ידי קרן לינוקס, משמשת מגוון רחב של ארגונים, כולל בנקים, חברות שרשרת אספקה וחברות המספקות שירותי בריאות.

מכיוון שרשת הפבריק היא רשת הנמצאת בשימוש כבר בחברות מובילות במשק כגון: אורקל, מיקרוסופט, IBM, SAP וחברות נוספות רבות. **בחרתי להשתמש ברשת היפרלד'ר פבריק כרשת בלוקצ'יין פרטית בפרויקט הגמר.**

רשת נוספת הנמצאת בשימוש במוסדות פיננסיים היא רשת קורדה (Corda) [20], פותחה ע"י קונסורציום R3, קבוצה של מעל 200 מוסדות פיננסיים, שמה דגש על פרטיות ותאימות גבוהה בין ארגונים, משתמשת במנגנון קונצנזוס חדשני נוטרי (Notary) אשר מאפשר יצירת אמון בין המשתתפים, תומכת בחוזים חכמים (flows) בשפות Java ו – Kotlin.

### 1.5.3. רשת בלוקצ'יין פדרלית (מאוחדת/קונסורציום)

זוהי סוג של רשת פרטית מורחבת, המאפשרת לארגונים שונים לבצע עסקאות או להעביר נתונים בין הצדדים **שיש ביניהם אמון.**

רשתות בלוקצ'יין של קונסורציום משמשות לעתים קרובות בתעשיות שבהן יש מספר מוגבל של משתתפים ידועים ומהימנים, הנמצאת בשימוש בתעשיות הפיננסים, שרשרת האספקה והבריאות.

רשתות אלה מספקות דרך מאובטחת ושקופה עבור המשתתפים לשתף נתונים ולבצע עסקאות זה עם זה, תוך שמירה על שליטה על מי שיש לו גישה לרשת ומי יכול לראות את הנתונים והעסקאות ברשת.

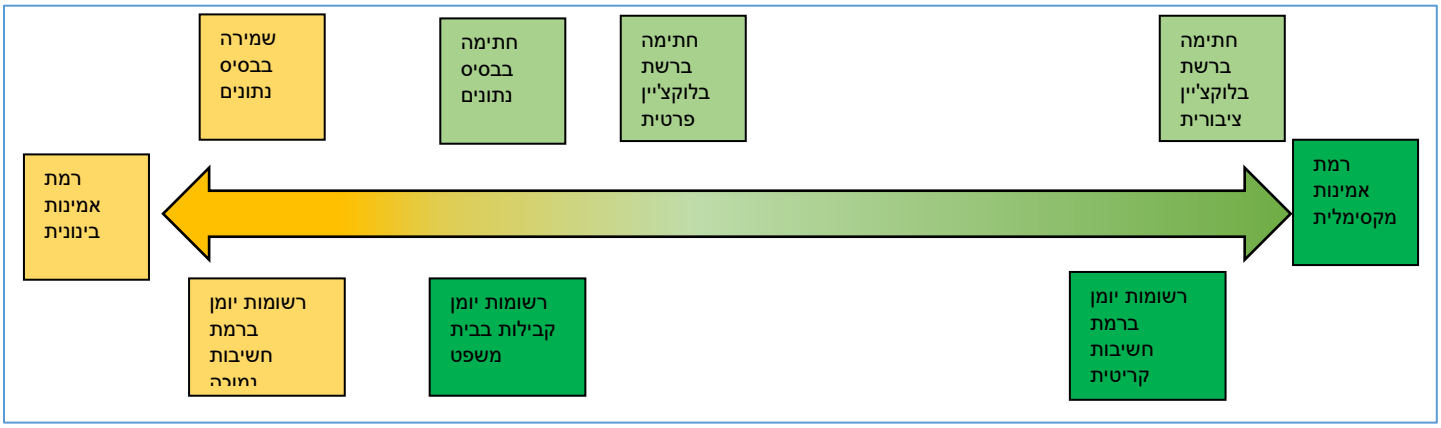
### 1.5.4. רשת בלוקצ'יין היברידית – שילוב של רשת פרטית ורשת ציבורית

שיטה זו למעשה משלבת את שני העולמות בצורה טובה יותר מבלי צורך שהארגון יצטרך להשתמש רק ברשת פרטית או ציבורית, **נוכל לנצל את היתרון של הרשת פרטית המאפשרת פרטיות גבוהה ויכולת עיבוד עסקאות בצורה מהירה מאוד יחסית לרשת ציבורית**. ובנוסף גם לנצל את היתרון של רשת ציבורית אשר נותנת אמינות של המידע מכיוון שהרשת מבוזרת מאוד ולכן חשופה הרבה פחות לשליטה של גורם יחיד היכול לשנות את המידע.

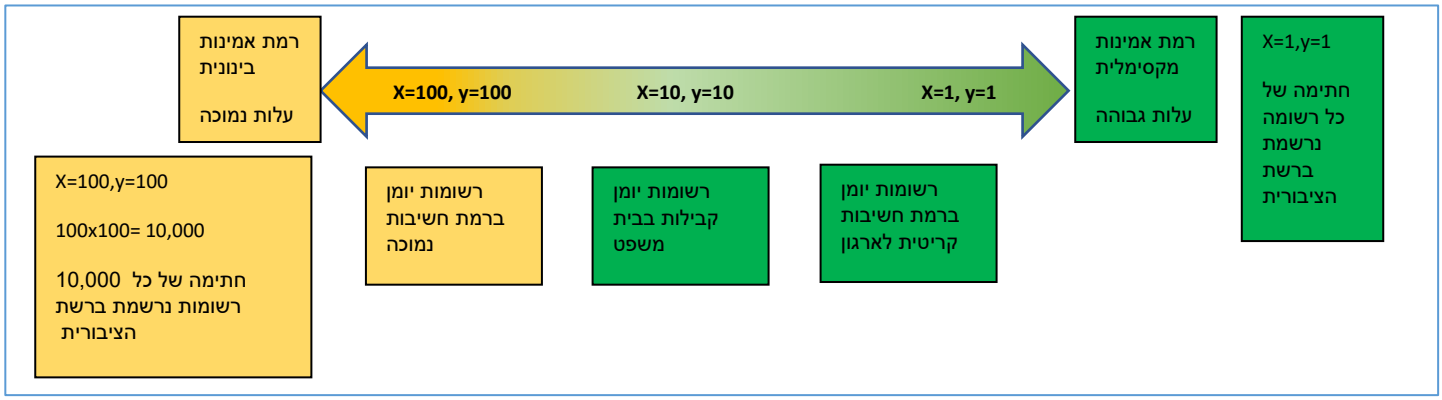
בזכות השילוב הנ"ל, סוג רשת זו מאפשרת לשמור על בטחון גבוהה של יומני ביקורת, זוהי שיטה המשלבת את היעילות והפרטיות של רשת פרטית עם רמת אמינות של הרשת הציבורית, **בעבודה זו נראה שהשיטה הטובה ביותר לניהול יומני מערכת בצורה מאובטחת היא שימוש ברשת היברידית**, מכיוון שהיא עונה על התנאי שראיות היומן יישארו קבילות, היכולת של ארגון להיות מסוגל לספק הוכחה לשלמותו, ולהבטיח כי לא התרחשו שינויים במהלך העיבוד. **ברשת היברידית נעשה שימוש ברשת פרטית כדי לאחסן את מידע-העל** (metadata) והוכחה של כל X רשומות ביקורת ב- Y בלוקים **(איור 2)**, וברשת הציבורית נשתמש כמערכת עוגן, בכדי לשמור את ההוכחה (proof) המבוססת על פונקציית גיבוב של קבוצת רשומות ביקורת הנמצאות בכל Y בלוקים ברשת הפרטית, ובכך אנו נתקף את

אמינות רשומות הביקורת בצורה גלויה ופומבית לכל אחד, וברשת הפרטית נוכל לתקף שרשומת הביקורת לא שונתה והיא קבילה כראיה ברמת אמינות גבוהה מאשר בסיס נתונים מוצפן.

**בנוסף בשיטה ההיברידית אנו יכולים לבחור בין עלות גבוהה עם ביצועים נמוכים אשר תיתן לנו רמת אמינות גבוהה ביותר עלות נמוכה עם ביצועים גבוהים, אשר תיתן לנו רמת אמינות נמוכה יותר.<u>ככל שערך של X ו - Y יהיו גדולים כך רמת האמינות תהיה נמוכה יותר</u>** והעלות הפתרון נמוכה יותר, הערך הכי נמוך הוא x=1 ו y=1 זה למעשה מייתר את מרבית היתרונות ברשת פרטית והיתרון היחיד הוא שנקבל שברשת הפרטית יהיה לנו את מידע העל (metadata) אשר יאפשר לנו להפיק תובנות על הרשומות יומן המקוריות במידה הם נמחקו או שונו בשרתי הלקוח. **(איור 2),תדירות העיגון צריכה להיות מאוזנת בקפידה כדי למזער עלויות, אך גם כדי למנוע מהארגון להחליף את נתוני הבלוקצ'יין בחלון הזמן שבין הבלוקים.**




איור א2 : תרשים שהכנתי המראה את רמות אמינות המערכת בשילוב בין רשת פרטית לציבורית




איור ב2 : תרשים שהכנתי המראה את רמות אמינות המערכת בשילוב בין רשת פרטית לציבורית – דוגמא לערכים

## 1.6. סקירה קצרה של חשיבות יומני ביקורת במערכות מידע

רישומי יומן ממלאים תפקיד משמעותי בפשעי סייבר, חקירה וניתוח פורנזי דיגיטלי. [4] יש חשיבות בעמידה בתקן אבטחת הנתונים של תעשיית כרטיסי התשלום (PCI DSS) או עמידה בתקן ניידות ואחריות של חוק ביטוח בריאות (HIPAA) תקנים אלו ואחרים מחייבים שהרשומה ביומן צריכה להישמר בצורה נכונה מבחינה משפטית. רק יומן שאינו ניתן לשינוי יכול להיחשב בבית משפט כראיה קבילה. **לכן חשיבות שמירת יומני המערכת היא לא רק עבור צורך פנימי של הארגון לחקירה וזיהוי תקיפות, אלא גם חובה חוקית של הארגון.**

כיום יש יותר ויותר מתקפות על שרתי מחשב, ונדרשת הגנה ברמה גבוהה יותר יחסית לשנים קודמות.

יש חשיבות עליונה בהגנה על יומני הביקורת (Audit Logs) של מערכות הארגון, אחד היעדים המרכזיים של התוקפים היא מערכת יומני הביקורת בה נרשמים אירועי מערכת במידה והתוקף הצליח להשבית את מערכת יומני הביקורת הוא יכול לשנות נתונים במערכת מבלי להשאיר עקבות ומבלי יכולת של הארגון לזהות שנתוני המערכת שונו, לדוגמא פריצה למאגר הנתונים ושינוי פרטים במאגר.

### 1.6.1. יומני ביקורת מאמר [1]

במאמר [1] דנו בחשיבות של הצורך בניתוח נתוני היומן המיוצרים על ידי מערכות המידע של הארגון באופן שוטף, על מנת למנוע פרצות אבטחה ולזהות התקפות פוטנציאליות על תשתית הארגון. במקרה של פריצה מוצלחת, חיוני לזהות את התוקף ע״י ביצוע חקירה פורנזית ולהעמידו לדין. עם זאת, תוקפים עשויים לנסות לשנות או למחוק ערכי יומן שיכולים לשמש כראיות, מה שמקשה על הוכחת מעשיהם בבית המשפט. לכן בכדי להבטיח שראיות יומן יישארו קבילות, על הארגון להיות מסוגל לספק הוכחה לשלמותו, ולהבטיח כי לא התרחשו שינויים במהלך העיבוד.

השימוש במערכות כמו SIEM (Security information and event management) יכול לסייע בניתוח זה ובשימור נתוני יומן.

כשמדובר בשימוש בראיות דיגיטליות בהליכים משפטיים, ישנן דרישות מסוימות שיש לעמוד בהן על מנת שהראיות ייחשבו קבילות מבחינה משפטית. דרישות אלה הן **רלוונטיות ואותנטיות**. על מנת שפיסת ראיה דיגיטלית תהיה **רלוונטית**, עליה להיות קשורה ישירות למקרה הנדון ולהיות מסוגלת לספק מידע שימושי לבית המשפט. בנוסף, הראיות חייבות להיות **אותנטיות**, כלומר הן חייבות להיות אמיתיות ולא שונו בצורה בלתי חוקית.

#### 1.6.1.1. שרשרת מתמשכת של משמורת [1]

אחת הדרכים להבטיח את האותנטיות של ראיות דיגיטליות היא לשמור על שרשרת מתמשכת של משמורת. משמעות הדבר היא שיש ליצור, להעביר ולאחסן את הראיות באופן שניתן לאמת ולהסתמך עליו. זה חשוב במיוחד במקרה של נתוני יומן, אשר יכול לספק מידע בעל ערך רב על אירועים שהתרחשו על מערכות המידע של הארגון. **על מנת שנתוני יומן אלו ייחשבו קבילים בבית המשפט, על הארגון להיות מסוגל לספק הוכחה לכך שהם נוצרו, הועברו ואוחסנו באופן אמין וניתן לאימות.**

נהלי יצירת ראיות הניתנים לאימות הם דרישה מרכזית עבור תשתיות רישום הניתנות לביקורת. הליכים אלה מסייעים להבטיח שנתוני יומן הרישום לא שונו בצורה לא חוקית וייאשרו מקוריים, זה דבר חיוני בכדי להשתמש בהם כראיה בהליכים משפטיים. הבטחת שלמות הראיות הדיגיטליות חיונית כדי להביא את התוקפים לדין ולחייב אותם לתת דין וחשבון על מעשיהם.

**לפני טכנולוגיית הבלוקצ׳יין הפתרונות הקיימים היו ועדיין יקרים וקשים להטמעה**, מכיוון שכדי לענות על משמורת ראיות דיגיטליות, יש צורך לוודא שהמידע הנשמר בבסיס הנתונים הוא מוצפן ומאובטח ברמה מאוד גבוהה, בנוסף יש צורך במספר שכבות הגנה, וגם בסופו של דבר נשלטת ע״י גורם עניין יחיד, כמו החברה, כמו כן, הרשאות מנהל מערכת צריכות להיות מוענקות למספר מצומצם של בעלי תפקידים, כל זה בעל מורכבות מאוד גבוהה הן טכנולוגית והן אנושית, אחד החסרונות העיקרים בשיטה זו הוא שיש גורם עניין יחיד, בעלי התפקידים בחברה הם למעשה אנשים מתוך החברה אשר מאחסנת את הנתונים, לכן יכולים להיות מצבים שהם ישנו נתונים או מצב שתוקף הצליח לקבל רמת גישה של מנהל מערכת וע״י לשנות את הנתונים מבלי יכולת לזהות, ולכן כדי להוכיח שהראיה קבילה יש צורך באמון בחברה התובעת או הנתבעת. [1]

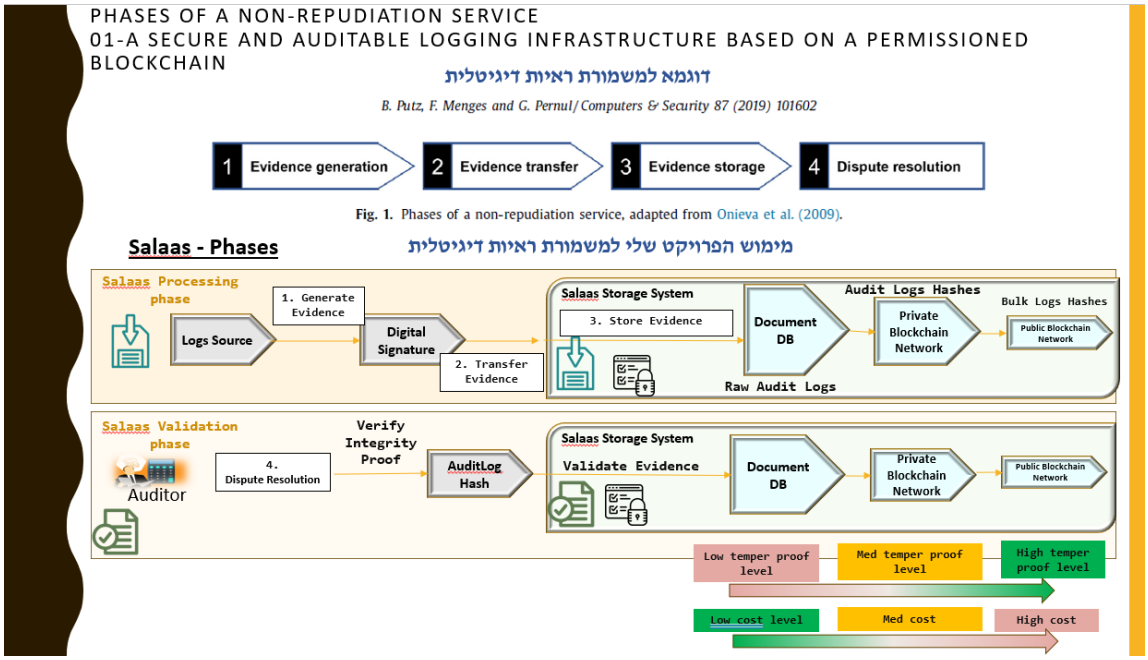
**בכדי להתגבר על אתגרים אלו ניתן לעשות שימוש בטכנולוגיית הבלוקצ׳יין אשר מציעה גישה חדשנית להבטחת שלמות ואי-התכחשות לאירועי יומן באופן מאובטח**. על ידי שימוש בטכנולוגיית בלוקצ׳יין, ניתן לפתח תשתית מאובטחת שאינה דורשת צד שלישי ותלות בגורם יחיד. תשתית זו משתמשת בשכבת ביקורת מבוזרת כדי לאחסן הוכחות של כל ערך יומן, אשר ניתנות לאימות על ידי גורמים מורשים לעריכת תחקור יומני הביקורת. רשת הבלוקצ׳יין המאחסנת את ההוכחות הללו מתוחזקת על ידי קונסורציום של מפעילים עצמאיים, מה שמבטיח שהנתונים יישארו עמידים בפני חבלה וגם זמינים. יצירה אוטומטית של חתימה, אחסון והוכחת תקינות עבור כל אירוע יומן רישום מספקת את האימות הדרוש ואת אי-ההתכחשות. גישה זו מציעה דרך אמינה וניתנת לאימות, אשר מאפשרת לשמור על שלמות נתוני היומן ולהשתמש בהם כראיה בהליכים משפטיים.

#### 1.6.1.1.1. מימוש הפרויקט לאחסון נתונים מאובטח

באיור 3, בחלק העליון ניתן לראות דוגמא ממאמר [1] לארבעת השלבים של משמורת ראיות דיגיטליות.

ובחלק התחתון ניתן לראות את הרכיבים העיקריים של המערכת שמימשתי.

1. תחילה הרשומה המקורית נחתמת ע"י חתימה דיגיטלית בכדי להעלות את רמת האבטחה של הנתונים.
2. שלב העברת הראיות נעשה בצורה מוצפנת ע"י TLS כדי למנוע שינוי נתונים בזמן העברת המידע ברשת.
3. שלב אחסון הראיות:
   a. אני שומר את הנתונים הגולמיים במסד נתונים מסוג NoSQL, וממדל אותם לסכמה של המערכת שלי.
   b. לאחר מכן אני שומר את הגיבובים (HASH) של הלוגים ברשת בלוקצ'יין פרטית.
   c. בנוסף, בכדי להעלות את רמת האמינות של המערכת אני שומר ברשת בלוקצ'יין ציבורית גיבוב של מספר לוגים בתנועה אחת.




*איור 3 משמורת ראיות דיגיטלית – והמערכת שפיתחתי לאחסון ושליפה של יומני ביקורת על רשת בלוקצ'יין*

## 1.7. סקירה על מחשוב ענן ציבורי. [4]

אנחנו חיים בעידן של טכנולוגיית המידע. [4] חיי היום יום שלנו תלויים בו מאוד ולכן יש משמעות חשובה ביותר לרמת אבטחת המידע. בכל דקה מתרחשות אלפי מתקפות סייבר ברחבי העולם. התוקפים מפתחים ללא הרף טכניקות מתוחכמות אשר מטשטשים את עקבותיהם. הם **נוקטים בכל אמצעי הזהירות כדי להסיר עקבות תקיפה, אחד האמצעים שהם נוקטים הוא שיבוש יומני מערכת ומידע קשור על מערכות המותקף, כך שלא ניתן יהיה לאתר את עקבותיהם**.

כדי להבין ולזהות התקפה מורכבת אשר מתרחשת לאורך זמן, יש צורך לשמור רשומות **יומן מאובטחות לאורך פרק זמן ממושך.** עם זאת, שמירה על רשומות יומן הרישום למשך זמן רב יותר היא בעיה לא פשוטה. המערכת צריכה גם להבטיח את שלמות קבצי יומן הרישום ותהליך הרישום. על מנת להתגבר על בעיות אלה, במאמר [4] החוקרים מציעים אחסון יומן מאובטח באמצעות פלטפורמת בלוקצ'יין בענן. טכנולוגיית בלוקצ'יין תסייע ליצור יומני ביקורת העמידים לשינויים, ובנוסף תספק הוכחה לשינויים ביומן ולעקרון אי-התכחשות.

### 1.7.1.פשע בסביבות ענן [5]

מחשוב ענן הפך לדרך פופולרית עבור ארגונים ויחידים לגשת למשאבי ושירותי מחשוב. זאת בשל הנוחות של מודל "**שלם לפי שימוש**" (pay as you go), המאפשר למשתמשים לגשת לשירותים בעלות מינימלית. עם זאת, גורמים זדוניים גם ניצלו תכונה זו של מחשוב ענן כדי לבצע פשעים בענן. **פשעים אלה יכולים לנוע בין התקפות על מערכות יומן**, שהן מסמכים ראייתיים חשובים, לחבלה בקבצי יומן כדי להסתיר ראיות למעשים לא חוקים. כדי לטפל בבעיות אלה, צוותים מיוחדים המכונים זיהוי פלילי בענן מופקדים על איתור וחקירה של מתקפות בסביבות ענן. כל הפעילויות המבוצעות על-ידי משתמש בענן נרשמות בדרך כלל וניתן לעקוב אחריהן באמצעות יומני פעילות. עם זאת, קבצי יומן חשופים להתקפות ולחבלה על ידי גורמים שונים המעורבים במערכת, כגון ספקי תשתית או פלטפורמה, או רשויות גישה ליומן. ישנם גם סוגים שונים של מודלים של ענן, כגון עננים פרטיים, קהילתיים וציבוריים, שלכל אחד מהם יש אתגרי אבטחה ייחודיים משלו. לדוגמה, **בענן פרטי, למחלקות IT יכולה להיות מוטיבציה לחבל בקבצי יומן רישום אם הן אינן מצליחות ליצור גיבויים עקב בעיות טכניות**. בענן שיתופי, שותפים עשויים להיות אחראים על משימות התפעול והתחזוקה שלהם, מה שעלול להוביל לחבלה ביומן אם נעשות טעויות. **בענן ציבורי, ייתכן שלמשתמשים לא תהיה שליטה על תשתית** הענן והם עשויים להסתמך על ספק השירות לצורך דוחות מפורטים על השירותים שלהם. במקרים כאלה, **לספק השירות עלולה להיות מוטיבציה לחבל ביומנים כדי להגן על האינטרסים שלהם.**

## 1.8 זיהוי פלילי דיגיטלי

זיהוי פלילי דיגיטלי ממלא תפקיד חיוני בחקירת פשעים המערבים מכשירים דיגיטליים. זהו תהליך הכולל מספר שלבים לזיהוי, איסוף, ארגון והצגת ראיות בבית משפט. [5]

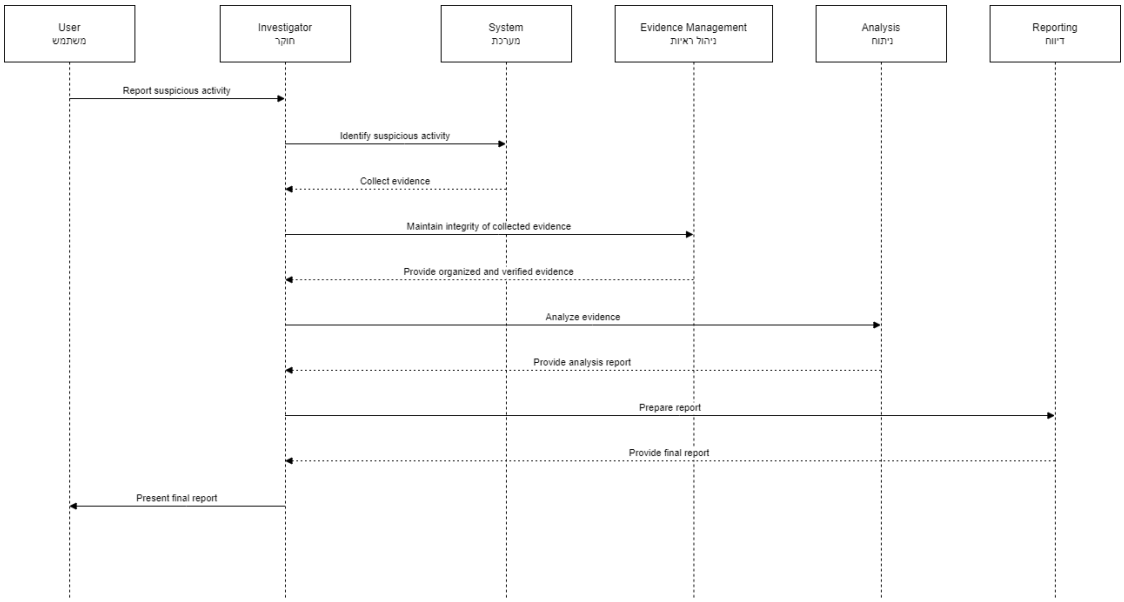
1. **זיהוי** : הצעד הראשון בזיהוי פלילי דיגיטלי הוא לזהות נוכחות של פעילויות זדוניות או פשעים. הדבר עשוי לכלול זיהוי דפוסים חריגים בקבצי יומן רישום או פעילות חשודה במכשיר.
2. **איסוף** : השלב הבא הוא לאסוף ראיות הקשורות לפעילות הזדונית. זה כולל איסוף קבצי יומן, גיבויי מערכת ונתונים רלוונטיים אחרים מהמכשיר או המערכות השונות. חשוב לשמור על שלמות הראיות שנאספו כדי להבטיח את מהימנותן כראיה בבית המשפט.
3. **ארגון** : לאחר איסוף הראיות, יש לארגן אותן ולבחון אותן על ידי החוקר. זה עשוי לכלול ניתוח קבצי יומן, בחינת גיבויי מערכת וחיפוש דפוסים או אנומליות שעשויים להצביע על נוכחות של פעילות זדונית.
4. **הצגה** : השלב האחרון בתהליך זיהוי פלילי דיגיטלי הוא הצגת הראיות בצורה של דו״ח לבית המשפט או לחבר המושבעים. דו״ח זה צריך להראות בבירור את ממצאי החקירה ולספק ראיות התומכות במסקנות שאליהן הגיע החוקר.

**באופן כללי, זיהוי פלילי דיגיטלי הוא כלי חשוב לחקירת פשעים המערבים מכשירים דיגיטליים ולהבטחת עשיית צדק. על ידי ביצוע צעדים אלה, חוקרים יכולים לאסוף ביעילות ולהציג ראיות כדי לתמוך בממצאים שלהם ולעזור להביא את העבריינים לדין.**

### 1.8.1. זיהוי פלילי דיגיטלי - תהליך איסוף וניתוח ראיות

ניתן לראות באיור 4 את שלבי התהליך.

1. **משתמש (User)**: התהליך מתחיל כאשר המשתמש מדווח על פעילות חשודה.
2. **חוקר (Investigator)**:
   - זיהוי הפעילות החשודה.
   - איסוף הראיה.
3. **מערכת (System)**: אחסון של שמירה על תקינות הראיה שהוכנסה.
4. **ניהול הראיה (Evidence Management)**:
   - הספקת הראיה השמורה והמאומתת.
5. **ניתוח (Analysis)**:
   - ניתוח הראיה.
   - הכנת דוח תחקיר זמני.
6. **דיווח (Reporting)**:
   - הכנת הדוח הסופי.
   - הספקת הדוח הסופי למשתמש.




*איור 4 תיאור לדוגמא של תהליך זיהוי פלילי דיגיטלי*

### 1.8.2. סוגים של זיהוי פלילי בענן

ישנם שני סוגים של זיהוי פלילי בענן מונחה ספקים [5]

- פתרון זיהוי פלילי **מבוסס סוכן**
- פתרון זיהוי פלילי **מבוסס יומן רישום**

זיהוי פלילי בענן הוא תהליך של בחינה וניתוח של נתונים וראיות בסביבת מחשוב ענן לצורך גילוי ושחזור אירועי עבר. המכון הלאומי לתקנים וטכנולוגיה (NIST) מגדיר זיהוי פלילי בענן כיישום של עקרונות מדעיים, פרקטיקות טכנולוגיות ושיטות מוכחות לשחזור אירועי מחשוב ענן בעבר.
ישנם שני סוגים של זיהוי פלילי מונחה ספקים בענן: פתרונות מבוססי סוכנים ופתרונות מבוססי יומן.

**פתרונות מבוססי סוכן** - סוכנים אלה מחלצים מידע ממכונות וירטואליות, אשר מומר לאחר מכן לפורמט מובנה לשימוש בתהליך הפורנזי.

**פתרונות מבוססי יומן רישום** מסתמכים על קבצי יומן רישום, שהם מסמכים המכילים אירועים ותהליכים המתרחשים במערכת מחשב. קבצי יומן אלה הם נכסים חשובים בתהליך החקירה הפורנזית ויכולים לספק מידע על המקור וציר הזמן של האירועים. **בסביבת מחשוב ענן, סוגים שונים של יומני רישום נוצרים ומאוחסנים, כולל יומני ביקורת, יומני שרת אינטרנט, יומני אבטחה ויומני יישומים.** חשוב לשמור על **הסודיות והשלמות** של יומנים אלה בתהליך הפורנזי, שכן הם חיוניים למציאת ראיות בחקירות פורנזיות בענן. **<u>אם היומנים נפגעים, תהליך החקירה עלול להיות להתקדם בכיוון הלא נכון</u>**

# 2. הסבר על טכנולוגיית הצפנה ורשת בלוקצ'יין.

## 2.1. טכנולוגיית הצפנה

קריפטוגרפיה היא למעשה תיאוריה ופרקטיקה העושה שימוש באלגוריתמים מתמטיים בכדי להצפין ולפענח נתונים על מנת לאבטח מידע רגיש. יסודות הקריפטוגרפיה, כוללים שימוש במפתחות ציבוריים ופרטיים, חתימות דיגיטליות ואלגוריתמים שונים המשמשים בקריפטוגרפיה המודרנית.

### 2.1.1. צמד מפתחות ציבוריים ופרטיים

אחד העקרונות הבסיסיים של קריפטוגרפיה הוא השימוש בצמד מפתחות ציבוריים ופרטיים. מפתחות אלה משמשים להצפנה ופענוח של נתונים, והם נוצרים בדרך כלל באמצעות אלגוריתם מתמטי. בהקשר של קריפטוגרפיה, המונחים "בוב" ו"אליס" משמשים לעתים קרובות להתייחסות לשני הצדדים המעורבים בתיאור תרחישים שונים.

### 2.1.2. שימוש בחתימה דיגיטלית בטכנולוגיית בלוקצ'יין

בנוסף להצפנת הודעות, ניתן להשתמש במפתחות ציבוריים ופרטיים גם ליצירת חתימות דיגיטליות. חתימה דיגיטלית היא דרך לאמת את האותנטיות של הודעה או קובץ. כדי ליצור חתימה דיגיטלית, השולח משתמש במפתח הפרטי שלו כדי להצפין את ההודעה או את הגיבוב של ההודעה. לאחר מכן, הנמען יכול להשתמש במפתח הציבורי של השולח כדי לאמת את האותנטיות של החתימה.

ישנם אלגוריתמים ופרוטוקולים רבים ושונים המשמשים בקריפטוגרפיה המודרנית, כולל אלגוריתם ריבסט-שמיר-אדלמן (RSA), אלגוריתם העקומה האליפטית (EC) ואלגוריתם החתימה הדיגיטלית (DSA). לכל האלגוריתמים הללו יש חוזקות וחולשות ייחודיות משלהם, והם מתאימים ליישומים שונים.

**טכנולוגיית בלוקצ'יין עושה שימוש בחתימה דיגיטלית** בכדי לודא את אותנטיות הפעולות והמטבעות הדיגיטליים בתוך הרשת. כאשר המשתמש מבצע עסקה, הוא "חותם" עליה באמצעות המפתח הפרטי שלו. משתמשים אחרים ברשת, המכונים "כורים" או "מאמתים", משתמשים במפתח הציבורי של השולח כדי לוודא את החתימה הדיגיטלית ולאשר את הפעולה. במסגרת רשת הבלוקצ'יין, השימוש בחתימות דיגיטליות מאפשר להבטיח שהפעולה אכן בוצעה ע"י השולח המצויין ושהיא לא נערכה לאחר השליחה.

בנוסף, חתימה דיגיטלית מאפשרת את הפרטיות, מכיוון שהשולח יכול לשמור על זהותו בסודיות תוך כדי אימות הפעולה. במערכות בלוקצ'יין רבות, הזהות האמיתית של השולח איננה ידועה לציבור, אך הפעולות עצמן אינן אנונימיות וניתן לאמת את האותנטיות שלהן באמצעות החתימה הדיגיטלית.

### 2.1.3.פונקציית גיבוב – HASH function

פונקציית גיבוב היא אלגוריתם מתמטי שלוקח קלט בכל גודל ומפיק פלט בגודל קבוע. לפלט של פונקציית גיבוב, הידועה גם בשם HASH, יש כמה תכונות חשובות שהופכות אותה לשימושית במגוון רחב של יישומים, כולל טכנולוגיית בלוקצ'יין.

אחד המאפיינים המרכזיים של גיבוב הוא שמדובר בפונקציה חד-כיוונית, קל לחשב את הגיבוב של הקלט, אך מעשית זה בלתי מעשי לקבוע את הקלט המקורי מהגיבוב.

תכונה זו של גיבוב מבטיחה שהפלט יהיה עקבי וניתן לשחזור על-ידי כל מי שיש לו את אותו הקלט, **הדבר חשוב מאוד לאפשרות של אימות מהיר בלוקים ברשת בלוקצ'ין וע"י שימוש במשאבים נמוכים.**

#### 2.1.3.1. שימושים של פונקציית גיבוב ברשת הביטקוין

רשת הביטקוין עושה שימוש בפונקציית גיבוב מסוג SHA-256 ,

פונקציית הגיבוב SHA-256 מייצרת גיבוב של 256 סיביות, המיוצג כמספר בן 64 ספרות הקסדצימליות.

ברשת הביטקוין, SHA-256 עושה שימוש במספר דרכים שונות כדי להבטיח את האבטחה והשלמות של הבלוקצ'יין. **שימוש ראשון**, SHA-256 משמש **לגיבוב נתוני עסקאות** וליצירת חתימה דיגיטלית עבור כל עסקה. פעולה זו מבטיחה שלא ניתן יהיה לשנות נתוני העסקה מבלי לשנות את החתימה, מה שיהפוך את העסקה ללא חוקית.

**שימוש שני**, SHA-256 משמש לגיבוב התוכן של כל בלוק בבלוקצ'יין, מה שמייצר מזהה ייחודי לבלוק. גיבוב זה, המכונה **"גיבוב בלוק" (ראה פירוט למטה),** נכלל בכותרת הבלוק, יחד עם הפניה לגיבוב של הבלוק הקודם. פעולה זו יוצרת שרשרת של בלוקים, שבהם הגיבוב של כל בלוק תלוי בתוכן של הבלוק הקודם.

**שימוש נוסף**, SHA-256 משתמש באלגוריתם **הוכחת העבודה** POW המשמש לאבטחת רשת הביטקוין. באלגוריתם זה, כורים מתחרים כדי לפתור חידה מתמטית על ידי חישוב הגיבוב SHA-256 של כותרת הבלוק. הכורה הראשון שיפתור את החידה מתוגמל במספר מסוים של ביטקוינים, והבלוק החדש מתווסף לבלוקצ'יין.

**<u>לכן ניתן לומר ש-SHA-256 הוא חלק חשוב מרשת הביטקוין. הוא מבטיח את השלמות, היעילות וחוסר ההשתנות של הבלוקצ'יין, והוא חיוני לתפעול מאובטח ואמין של הרשת.</u>**

### 2.1.3.1.1. פונקציית גיבוב- גיבוב בלוק - טכנולוגיית בלוקצ'יין

פונקציות גיבוב משמשות במגוון רחב של יישומים, כולל טכנולוגיית בלוקצ'יין. ברשת בלוקצ'יין, כל בלוק בשרשרת מכיל רשימה של עסקאות, כמו גם הפניה לבלוק הקודם בשרשרת. הפניה זו, המכונה "**גיבוב הבלוק הקודם**", היא הגיבוב של תוכן הבלוק הקודם. לדוגמה, נניח שיש לנו בלוקצ'יין עם שלושה בלוקים, A, B ו-C, כאשר כל בלוק מכיל רשימה של עסקאות והפניה לבלוק הקודם.

**הגיבוב של שלושת הבלוקים עשוי להיראות כך:**

בלוק A:

**עסקאות: T1, T2, T3**

**גיבוב בלוק קודם: Null**

**גיבוב בלוק A:** 80b88aae07b46e30e43753045135d4b9b338cc7ae832d0e0dd530b42adb1e9c6

בלוק B:

**עסקאות: T4, T5, T6**

**גיבוב בלוק קודם:** 80b88aae07b46e30e43753045135d4b9b338cc7ae832d0e0dd530b42adb1e9c6

**גיבוב בלוק B:** 6c060f1b9a81a53f051d6f7b3c019232ff54bae31bf5b18c181240ae1c7a2a5d

בלוק C:

**עסקאות: T7, T8, T9**

**גיבוב בלוק קודם:** 6c060f1b9a81a53f051d6f7b3c019232ff54bae31bf5b18c181240ae1c7a2a5d

**גיבוב בלוק C:** 2640bc2c7d8174cd2e95731bb2516041ef86ce317691a300bffbf2241a0be37d

בדוגמה זו, קוד הגיבוב הקודם של כל בלוק הוא הגיבוב של תוכן הבלוק הקודם. פעולה זו **יוצרת שרשרת של בלוקים**, שבהם הגיבוב של כל בלוק תלוי בתוכן של הבלוק הקודם.

לשימוש בגיבובים בטכנולוגיית הבלוקצ'יין יש כמה יתרונות חשובים:

**ראשית, זה מבטיח את שלמות הבלוקצ'יין** בכך שהוא מקשה על התוקף לשנות את התוכן של בלוק מבלי לשנות גם את הגיבוב של הבלוק. **מכיוון שהגיבוב של כל בלוק נכלל בבלוק הבא בשרשרת, כל שינוי בתוכן של בלוק ישנה גם את הגיבוב של אותו בלוק, מה שיפסול את הבלוקים הבאים בשרשרת.**

**<u>בנוסף</u>**, השימוש בגיבובים בטכנולוגיית הבלוקצ׳יין **<u>מאפשר אימות יעיל ומהיר של תוכן הבלוק</u>**. מכיוון שכל בלוק מכיל את הגיבוב של הבלוק הקודם, קל לצומת ברשת לאמת את שלמות הבלוק על-ידי חישוב הגיבוב של הבלוק הקודם והשוואתו לקוד הגיבוב הקודם של הבלוק הכלול בבלוק הנוכחי. **זה מאפשר לצמתים ברשת לאמת במהירות וביעילות את שלמות הבלוקצ׳יין מבלי להוריד ולעבד את השרשרת כולה.**

יתרה מכך, השימוש בגיבובים בטכנולוגיית הבלוקצ׳יין מבטיח את **יכולת האי-ההשתנות** (כמו שראינו זו תכונה חשובה במשמורת ראיות דיגיטליות) של הבלוקצ׳יין. מכיוון שהגיבוב של כל בלוק תלוי בתוכן של הבלוק הקודם, לא ניתן לשנות את התוכן של בלוק מבלי לשנות גם את תוצאות הגיבוב של כל הבלוקים הבאים בשרשרת. זה הופך **<u>את הבלוקצ׳יין ליומן תיעוד העונה על עקרון שבו זה לא מעשי לשנות את כל העסקאות שעובדו אי פעם ברשת.</u>** **<u>ולכן פונקציות גיבוב הן חלק חשוב בטכנולוגיית הבלוקצ׳יין. דבר זה מבטיח את השלמות, היעילות ותמיכה באי-השתנות של הבלוקצ׳יין, דבר חיוני לתהליך זיהוי פלילי דיגיטלי, בנוסף גם חיוני לתפעול המאובטח והאמין של הרשת</u>**

## 2.2. הסבר על טכנולוגית בלוקצ׳יין

### 2.2.1.פירוט אבני היסוד ברשת

#### 2.2.1.1. תנועות (Transaction)

כל עסקה/תנועה נרשמת ביומן העסקאות ונחתמת בצורה אמינה ביותר.

עסקה ברשת בלוקצ׳יין מתייחסת להעברת נתונים או ערך בין שני צדדים. ברשת בלוקצ׳יין, עסקאות נרשמות בבלוקים ומתווספות לבלוקצ׳יין הקיים בסדר ליניארי כרונולוגי.

כל עסקה ברשת בלוקצ׳יין מורכבת ממספר רכיבים, כולל כתובות השולח והמקבל, הסכום המועבר וחתימה דיגיטלית לאימות העסקה. החתימה הדיגיטלית נוצרת באמצעות מפתח פרטי, הידוע רק לשולח.

לאחר התחלת עסקה, היא משודרת לכל הצמתים ברשת. צמתים אלה, המכונים גם ״**כורים**״, מאמתים את העסקה כדי לוודא שהיא חוקית ולא עובדה בעבר. תהליך זה מכונה ״**קונצנזוס**״, והוא מבטיח את שלמות העסקה.

לאחר אימות העסקה, היא מתווספת ל״**בלוק** ״יחד עם עסקאות אחרות. לכל בלוק יש קוד מזהה ייחודי, המכונה **גיבוב** (HASH), המקשר אותו לבלוק הקודם בשרשרת. פעולה זו יוצרת תיעוד כרונולוגי ברור של כל העסקאות שעובדו ברשת.

לאחר הוספת בלוק לבלוקצ׳יין, העסקה נחשבת לשלמה. נתוני העסקה זמינים כעת עבור כל הצמתים ברשת להצגה ולאימות. שקיפות וביזור אלה הם מאפיינים מרכזיים

של טכנולוגיית הבלוקצ'יין, והם מספקים מספר יתרונות, כולל אבטחה מוגברת ועלויות עסקה מופחתות.

#### 2.2.1.2 יומן תנועות בלתי ניתן לשינוי (Immutable ledgers)

בכדי לשנות תנועה שנחתמה ביומן יש צורך במשאבים עצומים שעלותם הכספית אדירה, כך שמעשית אפשר לומר שתנועה שנחתמה היא בלתי ניתנת לשינוי.

היכולת של בלוקצ'יין לשמור על יומן תנועות בלתי ניתן לשינוי מושגת באמצעות שימוש בטכניקות קריפטוגרפיות אשר חלקן סקרתי למעלה. כל בלוק בבלוקצ'יין מקושר לבלוק הקודם באמצעות שימוש בקוד מזהה ייחודי, המכונה גיבוב (HASH). גיבוב זה נוצר באמצעות הנתונים הכלולים בבלוק, כמו גם הגיבוב של הבלוק הקודם. כאשר בלוק מתווסף לבלוקצ'יין, הגיבוב שלו מחושב ומתווסף לבלוק. אם נתונים כלשהם בבלוק ישתנו, גם הגיבוב של הבלוק ישתנה. **משמעות הדבר היא שכל ניסיון לחבל בנתונים בבלוק יהיה ניתן לזהות אותו באופן מיידי**, מכיוון שהשינוי שנוצר בגיבוב לא יתאים לערך של הגיבוב של הבלוק הקודם.

על מנת לחבל ולשנות נתונים בבלוק ברשת בלוקצ'יין, התוקף יצטרך לא רק לשנות את הנתונים בבלוק אחד, אלא גם לחשב מחדש את הגיבוב של הבלוק ואת הגיבוב של כל הבלוקים הבאים בשרשרת. **זהו תהליך הדורש יכולת עיבוד גבוהה ויקרה מאוד, והוא הופך לקשה יותר ויותר ככל שהבלוקצ'יין גדל**.

בנוסף, רוב רשתות הבלוקצ'יין הן **מבוזרות**, כלומר הן מתוחזקות על ידי רשת של צמתים, ולא על ידי ישות אחת. **לכן על מנת לחבל בבלוק, התוקף יצטרך להשיג שליטה על רוב הצמתים ברשת, דבר שכמעט בלתי אפשרי להשיג ברשת מבוזרת ציבורית גדולה.**

#### 2.2.1.3 רשת מבוזרת (Decentralized peers)

עמיתים מבוזרים, המכונים גם "**צמתים**", הם מרכיב חיוני ברשת בלוקצ'יין. ברשת מבוזרת, אין רשות מרכזית השולטת ברשת, וכל הצמתים הם משתתפים שווים ברשת. כל צומת ברשת בלוקצ'יין שומר עותק של יומן התנועות המבוזר, המכיל תיעוד של כל העסקאות שעובדו ברשת. כאשר מתבצעת עסקה חדשה, היא משודרת לכל הצמתים ברשת. צמתים אלה מאמתים את העסקה כדי לוודא שהיא חוקית ולא עובדה בעבר. תהליך אימות העסקאות מכונה "**קונצנזוס**". ברשת מבוזרת כגון ביטקוין, הסכמה מושגת באמצעות תהליך שנקרא "**כרייה**", שבו צמתים מתחרים כדי לפתור משוואות מתמטיות מורכבות כדי לאמת עסקאות ולהוסיף אותן לבלוקצ'יין.

הצמתים המאמתים בהצלחה עסקאות ומוסיפים אותן לבלוקצ׳יין מתוגמלים בסכום מסוים של המטבע הקריפטוגרפי המקורי של הרשת. זה מתמרץ צמתים להשתתף ברשת ומבטיח שהרשת תישאר מבוזרת ומאובטחת.

עמיתים מבוזרים מספקים מספר יתרונות מרכזיים לרשת בלוקצ׳יין. ראשית, הם מבטיחים שהרשת אינה נשלטת על ידי ישות אחת, מה שהופך אותה לעמידה יותר בפני צנזורה וחבלה. שנית, הם חולקים בעומס העבודה של אימות טרנזקציות ברחבי הרשת, מה שהופך את הרשת למדרגית ויעילה יותר.

לכן ניתן לראות שעמיתים מבוזרים הם מרכיב חיוני ברשת בלוקצ׳יין. הם מבטיחים שהרשת תהיה **מבוזרת**, **מאובטחת ויעילה, והם ממלאים תפקיד מכריע בתהליך ההגעה להסכמה ואימות העסקאות ברשת.**

### 2.2.1.4. שימוש במנגנוני הצפנה (Encryption process)

הצפנה היא מרכיב בסיסי בטכנולוגיית הבלוקצ׳יין, המאפשרת העברה מאובטחת ופרטית של נתונים בתוך רשת מבוזרת. ברשת בלוקצ׳יין, ההצפנה משמשת להגנה על סודיות נתוני עסקאות, כמו גם לאימות האותנטיות של עסקאות בודדות.

תהליך ההצפנה ברשת בלוקצ׳יין כולל בדרך כלל שימוש באלגוריתמים קריפטוגרפים, כגון אלגוריתם RSA. אלגוריתמים זה מאפשר יצירת מפתח הצפנה ייחודי, המכונה מפתח פרטי, אשר ניתן להשתמש בו כדי להצפין ולפענח נתונים.

כאשר משתמש יוזם עסקה ברשת בלוקצ׳יין, נתוני העסקה מוצפנים באמצעות **המפתח הפרטי של המשתמש. נתונים מוצפנים אלה משודרים לאחר מכן לרשת, שם הם מאומתים ומתווספים לבלוקצ׳יין.**

תהליך ההצפנה ברשת בלוקצ׳יין כולל גם שימוש במפתח ציבורי, שנוצר על בסיס המפתח הפרטי. **המפתח הציבורי משמש לאימות האותנטיות של עסקה, ומבטיח שרק הבעלים של המפתח הפרטי יוכל ליזום עסקה ברשת**.

**בנוסף להגנה על סודיות הנתונים של התנועות, הצפנה ברשת בלוקצ׳יין מבטיחה גם את שלמות הנתונים**. ברגע שעסקה נוספה לבלוקצ׳יין, היא הופכת לחלק מהיומן תנועות הבלתי משתנה, וכל ניסיון לשנות את הנתונים יזוהה מיד על ידי הרשת בשל האופי הקריפטוגרפי של תהליך ההצפנה.

באופן כללי, השימוש בהצפנה ברשת בלוקצ׳יין חיוני להבטחת האבטחה והפרטיות של נתוני טרנזקציות, כמו גם לתקינות הרשת כולה. על ידי שימוש באלגוריתמים קריפטוגרפיים ושימוש במפתחות פרטיים וציבוריים, רשתות בלוקצ׳יין מסוגלות לספק פלטפורמה מאובטחת ומבוזרת לשידור ואימות נתונים.

### 2.2.1.5. מנגנון הסכמה כוללת (Consensus mechanisms)

מנגנוני קונצנזוס הם מרכיב חיוני בטכנולוגיית הבלוקצ'יין, שכן הם מאפשרים למשתתפי הרשת להגיע להסכמה על המצב הנוכחי של יומן התנועות המבוזר. ללא קונצנזוס, לא ניתן יהיה לרשת מבוזרת לתפקד ביעילות, מכיוון שלא תהיה דרך לקבוע אילו עסקאות תקפות ויש להוסיף אותן לבלוקצ'יין.

ישנם מנגנוני קונצנזוס שונים שניתן להשתמש בהם ברשת בלוקצ'יין, שלכל אחד מהם מאפיינים ופשרות ייחודיים משלו. מנגנוני הקונצנזוס הנפוצים ביותר הם **הוכחת עבודה (PoW)** ו**הוכחת החזקה (*Proof of Stake* - PoS)**.

**<u>הוכחת עבודה</u>** (*Proof of Work* - PoW) הוא מנגנון קונצנזוס שבו משתתפי הרשת מתחרים כדי לפתור חידות חישוביות מורכבות על מנת לאמת עסקאות ולהוסיף אותן לבלוקצ'יין. תהליך זה, המכונה כרייה, **דורש כמות משמעותית של כוח חישובי**, והכורה הראשון שיפתור את החידה מתוגמל בסכום מוגדר מראש של המטבע הקריפטוגרפי המקורי של הרשת.

**<u>הוכחת החזקה (PoS)</u>** היא מנגנון קונצנזוס שבו משתתפי הרשת נבחרים לאמת עסקאות בהתבסס על כמות המטבעות הקריפטוגרפיים שהם מחזיקים. במערכת PoS, ההסתברות שמשתתף ייבחר לאמת עסקה היא פרופורציונלית לסכום ההימור שלו, או לכמות המטבע הקריפטוגרפי שהוא מחזיק.

גם ל- PoW וגם ל- PoS יש יתרונות וחסרונות משלהם. **PoW** הוא מנגנון קונצנזוס מבוזר ובטוח יותר, שכן הוא אינו מסתמך על השתתפות של קבוצה נבחרת של משתתפים. עם זאת, הוא גם דורש משאבים רבים ויכול להוביל לריכוזיות של כוח הכרייה. **PoS**, לעומת זאת, יעיל ומדרגי יותר, אך הוא גם רגיש יותר לריכוזיות ולהתקפות פוטנציאליות מצד משתתפים "עשירים" עם נתח גדול ברשת.

**ניתן לומר שמנגנוני קונצנזוס הם חלק חיוני בטכנולוגיית הבלוקצ'יין, ומאפשרים אימות מבוזר ומאובטח של עסקאות בתוך רשת**. למנגנון הקונצנזוס הספציפי שבו נעשה שימוש יכולה להיות השפעה משמעותית על האבטחה, המדרגיות והביזור של הרשת, לדוגמא בשנת 2022 רשת **את'ריום** התחילה תהליך למעבר מ*POW* ל*PoS* בכדי לחסוך באנרגיה וגם בכדי להעלות את רמת האמינות של העמיתים, במידה ומשתתף מנסה להכניס בלוק זדוני הרבה יותר קל לזהות את הזהות שלו לחסום אותו ולחייב אותו בקנס.

מנגנוני קונצנזוס הם מה שלמעשה אפשר ליישם ולהשתמש במטבע הדיגיטלי הראשון, ביטקוין, מנגנון זה פתר את בעיית "**התשלום הכפול**" (*Double-spending*), בעיה שבה ניתן לעשות שימוש באותו אסימון דיגיטלי המייצג תנועת תשלום.

#### 2.2.1.5.1. בעיית ההוצאה הכפולה

בעיית ההוצאה הכפולה היא פגם פוטנציאלי במערכת מזומנים דיגיטלית שבה **ניתן להוציא את אותו אסימון דיגיטלי יותר מפעם אחת**. זו בעיה מכיוון שהמשמעות היא שניתן להעתיק אסימון דיגיטלי, כמו ביטקוין, ולהשתמש בעותקים כדי לבצע רכישות, ובכך למעשה ליצור כסף יש מאין. זה יגרום לאינפלציה ויערער את שלמות המערכת כולה.

טכנולוגיית בלוקצ'יין הצליחה לפתור את בעיית ההוצאות הכפולות ללא צורך ברשות מרכזית שתאמת עסקאות. מכיוון שבבלוקצ'יין, עסקאות נרשמות על יומן תנועות מבוזר המתוחזק על ידי רשת מחשבים. לכל מחשב ברשת יש עותק של יומן תנועות, וכאשר מתבצעת עסקה חדשה, היא משודרת לכל המחשבים ברשת. מחשבים אלה מתחרים לאחר מכן כדי לאמת את העסקה על ידי פתרון בעיה מתמטית מורכבת. המחשב הראשון לפתור את הבעיה יזכה להוסיף את העסקה החדשה לפנקס ולהרוויח פרס קטן בצורה של מטבע קריפטוגרפי, כמו שעושה רשת ביטקוין.

לאחר שעסקה נוספה ליומן תנועות, לא ניתן לשנות או למחוק אותה, מה שאומר שהיא נרשמת לצמיתות וניתן לסמוך עליה. זה מבטל את האפשרות של הוצאה כפולה, שכן כל אסימון דיגיטלי ניתן להוציא רק פעם אחת, יש לציין שמכיוון שיכולים להיות מצבים שבלוק שנכנס יתחלף יש צורך לחכות ברשת ביטקוין לשישה אישורים (עוד חמישה בלוקים אחרי הבלוק שלנו) בכדי להיות בטוחים שהעסקה סופית ומאושרת, מכיוון **שהוספת בלוק חדש לוקח בערך כ-10 דקות, אזי רק לאחר כ-60 דקות אנו יכולים להיות בטוחים שהעסקה אושרה סופית ברשת ביטקוין.**

### 2.2.2. חשיבות שימוש בעץ מרקל ברשת בלוקצ׳ין

עץ מרקל (באנגלית: Merkle tree), הידוע גם כעץ גיבוב בינארי, הוא מבנה נתונים המשמש בקריפטוגרפיה ובמדעי המחשב לאחסון ואימות כמויות גדולות של נתונים. הוא נקרא על שם ראלף מרקל, שרשם פטנט על הרעיון בשנת 1979. [19]

עץ Merkle הוא מבנה נתונים דמוי עץ שבו כל צומת עלה מייצג בלוק נתונים, וכל צומת שאינו עלה מייצג את הגיבוב של צמתי הצאצא שלו. צומת השורש של העץ מייצג את הגיבוב של ערכת הנתונים כולה.

היתרון העיקרי של עץ Merkle הוא שהוא **מאפשר אימות יעיל של תוכן ערכת הנתונים מבלי להוריד ולעבד את כל מערך הנתונים**. הסיבה לכך היא שכל צומת בעץ מכיל את הגיבוב של צמתי הצאצא שלו, וצומת השורש מכיל את הגיבוב של ערכת הנתונים כולה.

כדי לאמת את שלמות ערכת הנתונים, המאמת צריך רק להוריד את צומת השורש של העץ ואת hashes של כמה צמתים עלים. לאחר מכן המאמת יכול לחשב את הגיבוב של צמתי העלים וצמתי הביניים בעץ, ולהשוות אותם לגיבובים שהורדו. אם קודי ה- Hash המחושבים תואמים לקודי ה- Hash שהורדו, המאמת יכול להיות בטוח שערכת הנתונים לא טופלה שלא כדין.

עצי Merkle משמשים במגוון רחב של יישומים, כולל טכנולוגיית בלוקצ׳יין. ברשת בלוקצ׳יין, כל בלוק בשרשרת מכיל רשימה של עסקאות והפניה ל-hash של הבלוק הקודם. כדי להבטיח את שלמות העסקאות, כל בלוק מכיל גם עץ Merkle של העסקאות בבלוק.

**לשימוש בעצי Merkle בטכנולוגיית הבלוקצ׳יין יש כמה יתרונות חשובים. ראשית, הוא מאפשר אימות יעיל של העסקאות בבלוק, כפי שתואר לעיל. שנית, הוא מקטין את כמות הנתונים שצריך לאחסן ולהעביר בבלוקצ׳יין, מכיוון שרק הגיבוב של העסקאות ושורש עץ Merkle צריכים להיות מאוחסנים בכל בלוק. זה הופך את הבלוקצ׳יין למדרגי ויעיל יותר.**

לכן, עץ Merkle הוא מבנה נתונים המשמש לאחסון ואימות כמויות גדולות של נתונים. הוא משמש במגוון רחב של יישומים, כולל טכנולוגיית בלוקצ׳יין, שם הוא מאפשר אימות יעיל של תוכן הבלוק מבלי להוריד ולעבד את הבלוק כולו.

### 2.2.3.שמירת נתונים ברשת ביטקוין

בכדי לאחסן נתונים בבלוקצ'יין של ביטקוין מבלי לבצע העברת מטבעות, נשתמש **בעסקת נתונים ריקים**, הידועה גם בשם פלט נתונים ריקים או עסקת **OP_RETURN**. עסקאות נתונים ריקים הן סוג מיוחד של עסקת ביטקוין המאפשרת למשתמשים להטמיע נתונים בבלוקצ'יין.

כדי ליצור עסקת נתונים ריקים, ניתן להשתמש בצד לקוח ביטקוין התומך בסוג זה של עסקה. כמה תוכנות צד לקוח פופולריות התומכות בעסקאות נתונים ריקים כוללים את צד לקוח ליבת הביטקוין המקורי, צד לקוח אלקטרום וארנק Blockchain.com.

כדי ליצור עסקת נתונים ריקים, תחילה צריך ליצור כתובת ביטקוין ולקבל את המפתח הפרטי עבור כתובת זו. לאחר מכן להשתמש במפתח הפרטי כדי לחתום על עסקת נתונים ריקים הכוללת את הנתונים שרוצים להטביע בבלוקצ'יין.

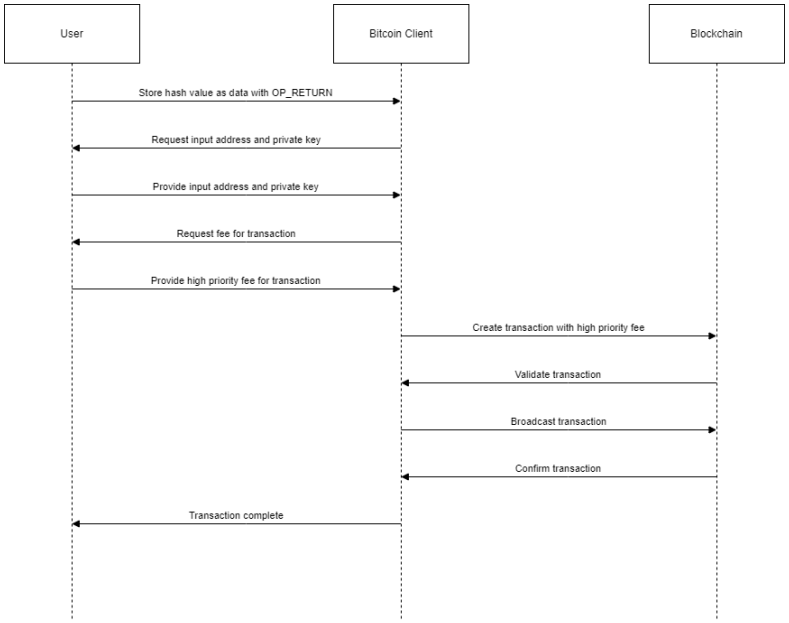
לאחר חתימת העסקה, יש לשדר אותה לרשת באמצעות תוכנת הביטקוין. העסקה תאומת על ידי הרשת ותיכלל בבלוקצ'יין, יחד עם הנתונים שכללת בעסקה.

**בפרויקט הגמר שלי אני שומר נתונים ברשת ביטקוין כדי להעלות את רמת האמינות של המערכת, לכן יש חשיבות בהבנת דרך שמירת נתונים ברשת ביטקוין.**

### 2.2.3.1. שמירת נתונים ברשת ביטקוין

איור 5, התרשים מתאר את תהליך הוספת נתונים לבלוקצ׳יין של ביטקוין באמצעות עסקת נתונים ריקים.

1. **המשתמש (User):**
   - מאחסן ערך הגיבוב כנתון באמצעות OP_RETURN
   - מספק כתובת ביטקוין ומפתח פרטי לאחר שהוא מתבקש לכך.
   - המשתמש מעדכן את עמלה שהוא מוכן לשלם כדי לקבל עדיפות גבוהה להכנסת התנועה לרשת.
2. **הלקוח ביטקוין (Bitcoin Client):**
   - יוצר טרנזקציה עם עמלה עדיפות גבוהה.
   - אימות הטרנזקציה.
   - שידור הטרנזקציה לרשת.
   - אישור הטרנזקציה ברשת.
3. **בלוקצ׳יין (Blockchain):**
   - הבלוקצ׳יין מאשר את הטרנזקציה לאחר שהיא מתפרסמת בו.




*איור 5 שמירת מידע ברשת ביטקוין ע"י עסקת נתונים ריקה*

### 2.2.4. השוואת נתונים וביצועי מערכת בין רשתות שונות

בכדי לתת מבט מהיר על הגישות השונות ומהן הנקודות החשובות שיש לפתור, הכנתי טבלאות השוואה..

| מספר | תכונה | יישום ללא רשת בלוקצ'יין | רשת בלוקצ'יין ציבורית | רשת בלוקצ'יין פרטית | רשת בלוקצ'יין פדרלית | רשת בלוקצ'יין היברידית |
|---|---|---|---|---|---|---|
| 1 | **מנגנון יתירות של המידע** | קיים | קיים | קיים | קיים | קיים |
| 2 | **עלות הוספת תנועות לרשת** | זולה | יקרה | בינונית | בינונית | בינונית |
| 3 | **עלות חומרה, תשתיות** | זולה | זולה | יקרה | יקרה | יקרה |
| 4 | **קצב עיבוד תנועות (transactions)** | מהיר מאוד | איטי (ביטקוין מספק קצב של 7 תנועות/לשנייה) | בינוני (גבוה בסדר גדול של מאות ואלפים מרשת ביטקוין Bano et al., 2017) | בינוני | בינוני |
| 5 | **זמן שיהוי ( latency time)** | נמוך | גבוה | בינוני | בינוני | בינוני |
| 6 | **יכולת גדילה של המערכת** | גבוהה | בינוני (בביטקוין יכולת הגדילה מוגבלת ע"י גודל בלוק וקצב תפוקה) | גבוהה | גבוהה | גבוהה |
| 7 | **גודל המידע הניתן לעיבוד בבלוק** | גדול | קטן *bitcoin max 1MB * Ethereum MAX GAS is 12.5 (~few MB size) | גדול | גדול | גדול |
| 8 | **רמת זמינות המערכת למקרה של גישה למידע** | בינונית | גבוהה | בינונית | בינונית | גבוהה |

*טבלה 1 - טבלת השוואה נתונים וביצועי מערכת*

**טבלה 2** משווה תכונות שונות של סוגים שונים של רשתות בלוקצ׳יין: עצמאית, ציבורית, פרטית, מאוחדת והיברידית:

1. **מנגנון יתירות של המידע**: ללא רשת בלוקצ׳יין אפשר להשתמש בפרוטוקולי RAFT או אחרים בכדי לוודא שהמידע משכופל בצורה תקינה על גבי מספר שרתים, בבלוקצ׳יין ציבורי כמו ביטקוין יש רמה חזקה של יתירות מידע, מכיוון שהמידע משוכפל לרוב הצמתים ברשת, אשר כוללת אלפי עמיתים, וברשת פרטית, פדרלית והיברידית יש פחות צמתים ולכן רמת היתירות בה בינונית ביחס לרשת ציבורית.
2. **עלות הוספת עסקאות לרשת**: לרשתות בלוקצ׳יין ציבוריות, כמו ביטקוין, יש עלויות בגין תשלומי עמלות גבוהות יחסית עבור הוספת עסקאות לרשת, מכיוון שהמשתמשים צריכים לשלם עבור עלות הדלק או דמי הכורה. עם זאת, רשתות בלוקצ׳יין פרטיות בעלות עלויות נמוכות יותר, מכיוון שהן שאין צורך בתשלום דמי עמלה עבור עסקאות.
3. **עלות חומרה ותשתית:** לרשתות בלוקצ׳יין ציבוריות, כמו ביטקוין, יש עלות חומרה ותשתית נמוכה יחסית מכיוון שהן מבוזרות ואינן דורשות חומרה או תוכנה מיוחדות כדי לפעול. לעומת זאת, רשתות בלוקצ׳יין פרטיות עשויות להיות בעלות עלויות חומרה ותשתית גבוהות יותר, מכיוון שהן עשויות לדרוש חומרה או תוכנה מיוחדות כדי לפעול.
4. **מהירות עיבוד עסקאות:** לרשתות בלוקצ׳יין ציבוריות, כמו ביטקוין, יש מהירויות עיבוד עסקאות נמוכות יחסית, ובדרך כלל הן מעבדות כ-7 טרנזקציות בשנייה. רשתות בלוקצ׳יין פרטיות, לעומת זאת, עשויות להיות בעלות מהירויות גבוהות בהרבה, מה שעשוי לעבד מאות או אלפי עסקאות בשנייה.
5. **זמן השהייה:** זמן השהייה מתייחס למשך הזמן שלוקח לעבד עסקה ולהוסיף אותה לבלוקצ׳יין. לרשתות בלוקצ׳יין עצמאיות, ציבוריות ופרטיות, זמני השהייה גבוהים יחסית, שכן בלוקים מתווספים לשרשרת כל 10 דקות. רשתות בלוקצ׳יין מאוחדות והיברידיות עשויות להיות בעלות זמני השהייה נמוכים יותר, מכיוון שהן בעלות מרווחי בלוקים שונים ומשתמשות במנגנוני קונצנזוס שונים.
6. **מדרגיות:** מדרגיות מתייחסת ליכולת של רשת בלוקצ׳יין להתמודד עם מספר גדל והולך של משתמשים ועסקאות. לרשתות בלוקצ׳יין ציבוריות, כמו ביטקוין, יש מדרגיות נמוכה יחסית, שכן גודל הבלוק ומרווח הבלוקים מגבילים את מספר העסקאות שניתן לעבד. רשתות בלוקצ׳יין פרטיות, לעומת זאת, עשויות להיות בעלות מדרגיות גבוהה בהרבה.
7. **קיבולת עיבוד נתונים:** קיבולת עיבוד נתונים מתייחסת לכמות הנתונים שניתן לאחסן בבלוקצ׳יין. לרשתות בלוקצ׳יין עצמאיות וציבוריות, כמו ביטקוין, יש יכולת עיבוד נתונים נמוכה יחסית, עם גודל בלוק מקסימלי של 1MB. רשתות בלוקצ׳יין פרטיות, לעומת זאת, עשויות להיות בעלות יכולת עיבוד נתונים גבוהה בהרבה.

8. **זמינות מערכת:** זמינות המערכת מתייחסת לזמינות של רשת הבלוקצ׳יין למשתמשים. לרשתות בלוקצ׳יין עצמאיות, ציבוריות ופרטיות, יש זמינות מערכת גבוהה יחסית, מכיוון שהן מבוזרות ויכולות להמשיך לפעול גם אם צמתים מסוימים נכשלים. רשתות בלוקצ׳יין מאוחדות והיברידיות, עשויות להיות בעלות זמינות מערכת נמוכה יותר, מכיוון שהן ריכוזיות ועשויות להיות רגישות יותר להפסקות או כשלים.

לסיכום, טבלה זו משווה בין סוגים שונים של רשתות בלוקצ׳יין ותכונותיהן. לכל סוג של רשת בלוקצ׳יין יש סט מאפיינים ייחודי משלו שהופך אותו למתאים למקרי שימוש שונים.

### 2.2.5. השוואת רמת אבטחת המידע בין רשתות שונות

| מספר | תכונה | יישום ללא רשת בלוקצ׳יין | רשת בלוקצ׳יין ציבורית | רשת בלוקצ׳יין פרטית | רשת בלוקצ׳יין פדרלית | רשת בלוקצ׳יין היברידית |
|---|---|---|---|---|---|---|
| 1 | **רמת הגנה מפני שינוי מידע לאחר שמירת המידע.** | מתונה *לא תומך בהגנה על מחיקה של המידע | גבוהה מאוד | גבוהה | גבוהה | גבוהה מאוד |
| 2 | **קבילות ראיה בבית משפט** | בינונית | גבוהה | בינונית | בינונית | גבוהה |
| 3 | **רמת עקרון אי-הכחשה של המידע** | בינונית | גבוהה | בינונית | בינונית | גבוהה |
| 4 | **דורש צד שלישי מהימן** | כן | לא | *לא | *לא | *לא |
| 5 | **יכולת של מבקר חיצוני ופנימי לוודא את שלמות המידע של ראיה שהוגשה לבית משפט auditability** | בינונית | גבוהה | בינונית | בינונית | גבוהה |
| 6 | **רמת סודיות המידע, הגנה מפני חשיפת מידע רגיש (PII)** | *לא (אפשרי ע״י פיתוח מגנון משלים) | *לא (אפשרי ע״י פיתוח מגנון משלים) | *לא (אפשרי ע״י פיתוח מגנון משלים) | *לא (אפשרי ע״י פיתוח מגנון משלים) | *לא (אפשרי ע״י פיתוח מגנון משלים) |
| 7 | **עמידות למתקפת מחיקה** | נמוכה Ma and Tsudik (2009) | גבוהה | גבוהה | גבוהה | גבוהה |

*טבלה 2 - טבלת השוואה רמת אבטחת המידע: השוואה בין תכונות שונות ויישומן בסוגים שונים של רשתות: ללא בלוקצ׳יין, בלוקצ׳יין ציבורי, בלוקצ׳יין פרטי, בלוקצ׳יין קונסורציום ובלוקצ׳יין היברידי*

.

1. **רמת הגנה על נתונים לאחר אחסון נתונים** : רמת ההגנה הגבוהה ביותר מוצעת על ידי בלוקצ׳יין קונסורציום, ואחריו בלוקצ׳יין ציבורי, פרטי והיברידי. ללא בלוקצ׳יין, רמת ההגנה מתונה, אך היא אינה תומכת בהגנה גבוהה על מחיקת נתונים.

2. **רמת הקבילות הראייתי בבית המשפט**: ללא בלוקצ'יין, בלוקצ'יין פרטי, בלוקצ'יין קונסורציום הרמה מתונה, בעוד שבבלוקצ'יין הציבורי ובלוקצ'יין היברידי הרמה חזקה.
3. **רמת אי ההתכחשות לנתונים**: ללא בלוקצ'יין, הרמה מתונה, בעוד שבבלוקצ'יין הציבורי ובלוקצ'יין היברידי היא גבוהה. בבלוקצ'יין פרטי ובלוקצ'יין קונסורציום הרמה מתונה.
4. **הצורך בצד שלישי מהימן:** ללא בלוקצ'יין, נדרש צורך בצד שלישי מהימן, בעוד שבבלוקצ'יין ציבורי, פרטי, קונסורציום והיברידי הוא ברוב המקרים לא נדרש צד שלישי מהימן, למעט מקרים שבהם נעשה שימש ברשת בלוקצ'יין לצורך ממסדי כגון ממשלה שרוצה לנהל בעצמה את המידע שלה ברשת קונסורציום שבה ארגונים יקבלו גישה לרשת הפרטית החשופה למורשים.
5. **היכולת של מבקרים חיצוניים ופנימיים לאמת** את שלמות הנתונים של הראיות שהוגשו לבית המשפט (Auditability): ללא בלוקצ'יין, הרמה מתונה, בעוד שבבלוקצ'יין הציבורי ובלוקצ'יין היברידי היא גבוהה. בבלוקצ'יין פרטי ובלוקצ'יין קונסורציום הרמה מתונה.
6. **רמת פרטיות הנתונים וההגנה על PII :** ללא רשתות בלוקצ'יין היא נמוכה, אך ניתן לשפר אותה באמצעות פיתוח אמצעי אבטחה משלים. היא נמוכה ברשתות בלוקצ'יין ציבוריות, פרטיות, קונסורציום והיברידיות, אך ניתן לשפר אותו באמצעות פיתוח אמצעי אבטחה משלימים.
7. **עמידות למתקפת מחיקה:** ללא בלוקצ'יין, הרמה נמוכה, (Ma and Tsudik, 2009) וחשופה למתקפת מחיקה של כל יומני הביקורת, בעוד שבבלוקצ'יין ציבורי הרמה גבוהה מאוד יהיה צורך בשימוש במשאבים עתירים כדי לבצע זאת, ובבלוקצ'יין פרטי, קונסורציום והיברידי הרמה גבוהה.

## 3. הסבר מפורט על שמירת ואחזור מידע של יומני הביקורת ברשת בלוקצ׳יין.

**בחלק זה, אסקור את שלבי ההתפתחות של פתרונות אבטחת יומני ביקורת, כותבי המאמרים [1] [3] , התייחסו לטכנולוגיות קודמות למאמר, נעמוד על ההבדלים השונים ונחדד את הצורך במציאת פתרון שייתן מענה לליקויים של הפתרונות הקודמים.**

יומני ביקורת חשובים למערכות עסקיות ארגוניות ולארגונים ארגוניים מכיוון שהם מאפשרים ניטור רציף וביקורת שקופה של אירועי מערכת. חוקים ותקנות פדרליים, כגון קוד התקנות הפדרליות של ה-FDA וחוק הניידות והאחריות של ביטוח בריאות, מחייבים ארגונים לנהל יומני ביקורת למטרות ביקורת נתונים, ציות וביטוח.

יומני ביקורת מאובטחים מאפשרים לבעלי העניין לבקר את מצב המערכות, לנטר את פעילויות המשתמשים ולהבטיח אחריות ביחס לתפקידיהם ולביצועיהם. בשל מאפיינים אלה, יומני ביקורת משמשים מערכות רגישות לנתונים כדי לרשום פעילויות במערכות מסדי נתונים של מסוף. זה עוזר להבטיח את השלמות והאבטחה של המערכות והנתונים שהן מכילות.

יומני ביקורת משמשים לעתים קרובות לשחזור נתונים למצב קודם לאחר שיתקלו בשינויים לא רצויים. שינויים אלה יכולים לנבוע מהתקפות של גורמים זדוניים, מתקלות תוכנה או מרשלנות של המשתמש. מסדי נתונים קונבנציונליים משמשים כמדיום לאחסון יומני ביקורת, המשתמשים במודל שרת-לקוח של תקשורת וחילופי נתונים. עם זאת, **מודל זה הופך את יומני הביקורת לפגיעים לנקודת כשל אחת, שבה תוקף יכול לגשת למסד הנתונים ו/או ליומני הביקורת ולחבל במידע קריטי**. **לכן**, **בכדי לטפל בפגיעויות אלה יש צורך ביומני ביקורת מאובטחים**, משוכפלים, עמידים בפני גישה לא מורשית בעלי יכולות הגנה יעילות. טכנולוגיית בלוקצ׳יין יכולה לספק פתרון בכך שהיא מאפשרת שמירת רשומות מאובטחת, שקופה ובלתי ניתנת לשינוי במערכות מבוזרות ללא צורך בצד שלישי נאמן. בלוקצ׳יין, המיושם על יישומי יומן ביקורת, יכול לשכפל יומני ביקורת ברשת של עמיתים, ולספק תצוגה עקבית ועמידה בפני חבלה של המערכת. יתר על כן, גורם זדוני שינסה לפרוץ למערכת יצטרך לשנות את יומני הרישום של כל העמיתים, מה שיגדיל את העלות והמורכבות של ההתקפה ובכך ישפר את האבטחה הכוללת של יישום יומן הביקורת.

זה הניע את החוקרים לפיתוח של BlockAudit, פתרון מקצה לקצה שמשלב יומני ביקורת עם מערכות בלוקצ׳יין. BlockAudit הופך את יומני הביקורת למבנה נתונים תואם בלוקצ׳יין ויוצר טרנזקציות עם חותמת זמן מהנתונים בתוך היומנים. **עסקאות אלה נצברות לאחר מכן לבלוקים ופרוטוקול הסובלנות תקלות ביזנטית (BFT) משמש ליצירת קונצנזוס בקרב העמיתים לגבי מצב הבלוקצ׳יין**. BlockAudit הוא אגנוסטי ליישומים ומספק שירותי הכנס-הפעל עבור יישומי יומן ביקורת. BlockAudit מציעה פתרון לניהול מאובטח ויעיל של יומני ביקורת באמצעות טכנולוגיית בלוקצ׳יין.

## 3.1. מחקרים קודמים

בחלק זה אסקור את המאמרים השונים אשר פורסים לפנינו את המחקרים השונים שנעשו בשנים האחרונות כדי לאבטח יומני ביקורת נתונים.

### 3.1.1. מחקרים קודמים מאמר 1

במאמר זה דובר על כך שמחקרים קודמים התמקדו בפיתוח גישות שונות ליצירה והגנה על יומנים מאובטחים מפני תוקפים. גישות אלה כוללות לעתים קרובות שימוש בהתקני כתיבה בלבד או באחסון מוגן גישה כדי לשמור על שלמות הראיות. לאחרונה, טכנולוגיית הבלוקצ'יין התגלתה כדרך חדשנית להשיג מטרות אלה. מערכות בלוקצ'יין הן מאגרי נתונים יתירים ביותר שנועדו לנהל יומן הוספה בלבד של עסקאות. מכיוון שהנתונים משותפים עם ארגונים עצמאיים אחרים על בסיס קונצנזוס מבוזר, הם עמידים בפני חבלה ושינוי. במידה ורוב המשתתפים כנים, הזמינות והשלמות של הנתונים המאוחסנים נשמרת. [1]

#### 3.1.1.1. סקירה של מחקרים קודמים בנושא מערכות רישום מאובטחות

כדי להשיג את מטרות האבטחה של מערכות רישום מאובטחות, חומרה או תוכנה מיוחדות נדרשות לעתים קרובות. [1] ניתן לחלק עבודות קודמת על מערכות רישום מאובטחות לשלושה קטגוריות:

1. מערכות אחסון להוספה בלבד.
2. חתימות מתפתחות מאובטחות קדימה.
3. שירותי נוטריון מהימנים של צד שלישי (TTP).

##### 3.1.1.1.1. טכנולוגיות מבוססי חומרה [1]

התקני כתיבה בלבד מבוססי חומרה הם התקני חומרה מיוחדים שתוכננו במיוחד לצורך אחסון נתוני יומן רישום. מכשירים אלה משמשים בדרך כלל לאחסון נתוני יומן באופן מאובטח ומוגן מפני חבלה, והם משמשים לעתים קרובות במצבים שבהם חשוב לשמור תיעוד של נתוני יומן למטרות משפטיות או למטרות תאימות.

אחד היתרונות העיקריים של מכשירי כתיבה בלבד מבוססי חומרה הוא שהם מציעים רמה גבוהה של אבטחה, מכיוון שהנתונים המאוחסנים במכשירים אלה בדרך כלל אינם נגישים או ניתנים לשינוי על-ידי משתמשים. זה הופך אותם לפתרון אידיאלי לאחסון נתוני יומן שיש לשמור בצורה ללא שינוי, כגון למטרות ביקורת או תאימות.

עם זאת, התקני כתיבה בלבד מבוססי חומרה יכולים להיות **פתרון בעלי עלויות גבוהות מאד**, במיוחד כאשר יש כמות גדולה של נתוני יומן שנוצרים ברציפות. הסיבה לכך היא שמכשירים אלה דורשים לעתים קרובות השקעה משמעותית בחומרה ובתחזוקה, ועשויים לדרוש כוח אדם ייעודי כדי לנהל ולתחזק אותם. בנוסף, ייתכן שהתקני כתיבה בלבד מבוססי חומרה לא יהיו גמישים או מדרגיים כמו פתרונות אחסון יומן רישום אחרים, כגון אחסון מבוסס ענן או פתרונות מבוססי תוכנה.

באופן כללי, התקני כתיבה בלבד מבוססי חומרה יכולים להיות פתרון שימושי לאחסון נתוני יומן במצבים מסוימים, **אך ייתכן שהם לא יהיו האפשרות החסכונית או הגמישה ביותר בכל המקרים**. לכן חשוב לשקול היטב את הצרכים והדרישות הספציפיים של ארגון בעת ההחלטה אם להשתמש בהתקן כתיבה בלבד מבוסס חומרה לאחסון יומן. **התקני כתיבה בלבד מבוססי חומרה** המשמשים בדרך כלל לאחסון נתוני יומן רישום יכולים להיות **כונני כתיבה לקריאה חוזרת** (Write Once, Read Many - WORM.) אלה הם כוננים קשיחים מיוחדים שנועדו לאפשר לכתוב אליהם נתונים פעם אחת, ולאחר מכן לא ניתן לשנות או למחוק את הנתונים. כונני WORM משמשים לעתים קרובות במצבים שבהם חשוב לשמור תיעוד של נתוני יומן רישום בצורה ללא שינוי, כגון למטרות משפטיות או למטרות תאימות.

**גם מערכות אחסון מבוססות דיסקים אופטיים,** נותנות מענה להתקן כתיבה בלבד, ע״י שימוש בדיסקים אופטיים מיוחדים, כגון תקליטורי CD-R או DVD-R, כדי לאחסן נתוני יומן רישום בתבנית כתיבה אחת. מערכות אלה עשויות לשמש במצבים שבהם חשוב לשמור על תיעוד ארוך טווח של נתוני יומן, שכן הדיסקים הם לעתים קרובות עמידים יותר ויש להם אורך חיים ארוך יותר מאשר סוגים אחרים של מדיית אחסון.

השימוש בטכנולוגיית WORM התחילה בשנות ה-80 של המאה ה-20. השימוש הראשון היה דרך לאחסן נתונים על דיסקים אופטיים, כגון תקליטורים ותקליטורי DVD.

עם הזמן, טכנולוגיית WORM התפתחה כדי לכלול סוגים אחרים של מדיית אחסון, כגון סרטים וכוננים קשיחים. בנוסף, טכנולוגיית WORM שימשה במגוון תעשיות, כולל ממשל, פיננסים, בריאות ועוד.

WORM שימש לאחסון ושימור נתונים בהתאם לתקנות שונות. דוגמאות לכך כוללות את תקני אבטחת מידע כגון: HIPAA, ISO-9001 ואחרים.

**בעבודה זו אראה את התהליך של השנים האחרונות, שבהן השימוש בטכנולוגיית WORM הוחלף בפתרונות אחסון מבוססי תוכנה ובלי רמת חסינות גבוהה מפני חבלה, כגון בלוקצ׳יין, המציעים פונקציונליות דומה עם יותר גמישות ומדרגיות.**

### 3.1.1.1.2. טכנולוגיות מבוססי תוכנה [1]

#### 3.1.1.1.2.1. גישות מבוססות תוכנה מערכות אחסון הניתנות להוספה בלבד

מערכות אחסון להוספה בלבד הן מערכות המאפשרות להוסיף נתונים, אך לא לשנות או למחוק. מערכות אלה משמשות לעתים קרובות לאחסון יומנים או סוגים אחרים של רשומות שיש לשמור לתקופה ארוכה של זמן.

ישנם יתרונות וחסרונות לשימוש במערכות אחסון עם הוספה בלבד.

**יתרונות**:

- מערכות אחסון להוספה בלבד מספקות תיעוד ברור של נתונים, מכיוון שלא ניתן לשנות או למחוק נתונים לאחר הוספתם.
- ניתן להשתמש במערכות אחסון להוספה בלבד כדי לאחסן כמויות גדולות של נתונים ביעילות, מכיוון שהן אינן דורשות תקורה של שמירה על מנגנון מחיקה או עדכון.

**חסרונות:**

- מערכות אחסון להוספה בלבד עלולות להיות יקרות ליישום, מכיוון שהן דורשות תשתית מיוחדת לתמיכה במנגנון המתווסף בלבד.
- ייתכן שמערכות אחסון להוספה בלבד לא יתאימו לכל סוגי הנתונים, מכיוון שחוסר היכולת לשנות או למחוק נתונים עשוי להיות מגביל במקרים מסוימים.

**כדי לצמצם את הסיכונים הכרוכים בשימוש במערכות אחסון בהוספה בלבד, ארגונים יכולים ליישם אמצעים כגון מערכות אחסון יתירות, מערכות גיבוי וניטור כדי להבטיח את ההמשכיות והאבטחה של הנתונים המאוחסנים.**

במאמר [1] דובר על מחקר על שימוש בטכנולוגיית בלוקצ׳יין כדי להבטיח שלמות יומן ויכולת ביקורת. לדוגמה, Jämthagen and Hell (2016) השתמשו בבלוקצ׳יין של ביטקוין כדי לפרסם קודי Hash שורש של ערכי יומן, ו-Cucurull and Puiggalí (2016) השתמשו ברשת הביטקוין כדי לתעד בלוקים של שרשראות יומנים מקומיות. Sutton and Samavi (2017) **השתמשו במסד נתונים מקומי של גרפים כדי לאחסן יומנים ולשלוח תקצירי הוכחת שלמות לבלוקצ׳יין של ביטקוין לצורך ביקורת.**

חוקרים אחרים השתמשו במסגרת הבלוקצ׳יין המורשית Hyperledger Fabric לרישום מאובטח. Ahmad et al. (2018) התמקדו במעקב אחר שינויים שבוצעו בערכי מסד נתונים על ידי אחסון קטעי שינוי ב- Hyperledger Fabric, ו- Shekhtman and Waisbard (2018) אחסנו את התוכן של קבצי יומן ישירות ב- Hyperledger Fabric. **בעוד שגישות אלה מדגימות את ההיתכנות של רישום הניתן לביקורת המבוסס על בלוקצ׳יין מורשה, לא ברור אם הן ניתנות להרחבה לניהול כמויות גדולות של נתוני רישום בפריסות מעשיות. מדרגיות היא שיקול חשוב עבור מערכות רישום מאובטחות, מכיוון שהן עשויות להזדקק לטיפול בכמויות גדולות של נתונים.**

### 3.1.1.1.2.2. חתימות מתפתחות מאובטחות קדימה forward-secure evolving signatures.

חתימות מתפתחות מאובטחות קדימה, סוג של מנגנון הצפנה שניתן להשתמש בו כדי לזהות שינויים בקבצי יומן. זה מספק אבטחה קדימה, **מה שאומר שערכי יומן קודמים נשארים מאובטחים גם אם אחד ממפתחות החתימה נחשף לסכנה בעתיד**. חתימות מתפתחות מאובטחות קדימה יכולות גם להיות ניתנות לאימות ציבורי, מה שמאפשר לכל אחד לאמת את שלמות היומן. [1]

ישנן מספר דוגמאות לסכמות חתימה מתפתחות מאובטחות קדימה:

- **אוגרים חד-כיווניים (OWA)** One-Way Accumulators: סכמה זו משתמשת בפונקציה חד-כיוונית, כגון פונקציית גיבוב, כדי ליצור חתימה עבור ערך יומן רישום. החתימה מבוססת על ערך היומן הקודם ומפתח סודי, וניתן לאמת אותה באמצעות המפתח הציבורי. OWA מספק אבטחה קדימה, שכן החתימה של ערך יומן עבר נשארת מאובטחת גם אם המפתח הסודי נחשף לסכנה בעתיד.
- **עצי גיבוב** (עצי מרקל):Hash Trees (Merkle Trees) : סכמה זו משתמשת במבנה דמוי עץ כדי ליצור חתימה לערך יומן. החתימה מבוססת על קודי הגיבוב של ערכי היומן וניתן לאמת אותה באמצעות גיבוב השורש של העץ. עצי גיבוב מספקים אבטחה קדימה, מכיוון שהחתימה של ערך יומן מהעבר נשארת מאובטחת גם אם גיבוב השורש ייחשף בעתיד.
- **שרשרת של גיבובים**: Chain of Hash: סכמה זו משתמשת בשרשרת של קודי גיבוב כדי ליצור חתימה עבור ערך יומן רישום. החתימה מבוססת על הגיבוב הקודם בשרשרת וניתן לאמת אותה באמצעות הגיבוב הראשוני בשרשרת. שרשרת הגיבוב מספקת אבטחה קדימה, שכן החתימה של ערך יומן עבר נשארת מאובטחת גם אם הגיבוב הראשוני ייחשף בעתיד.

אלה הן רק כמה דוגמאות **לסכמות חתימה מתפתחות מאובטחות קדימה**. ישנן תוכניות רבות אחרות שניתן להשתמש בהן כדי לספק רישום מאובטח וניתן לאימות.

#### 3.1.1.1.2.3. שירותי צד שלישי מהימן (TTP)

צד שלישי מהימן (TTP – Trusted Third Party) מתייחס לישות או לארגון מהימנים המספקים שירותים מסוימים, כגון חתימה דיגיטלית וחותמת זמן, כדי לאמת ולאמת את האותנטיות של מידע דיגיטלי. [1]

הצד השלישי פועל כישות ניטרלית ועצמאית, האחראית לשמירה על שלמותו ואבטחת המידע שהוא מנהל, כגון שימוש לצורך מתן רישום מאובטח לחקירות פורנזיות.

היתרונות של TTP הוא שהם יכולים לספק שירות מאובטח ומהימן, אך, הם יכולים לעתים קרובות לספק שירותים שקשה או יקר לארגון ליישם בעצמם.

לצד היתרונות שימוש ב-TTP יש לו מספר חסרונות, חסרון ראשון, הם דורשים לעתים קרובות **עלות נוספת עבור השירותים שלהם**.

חסרון נוסף, ל TTPs -עשויות להיות **פגיעויות** שיכולות להיות מנוצלות על-ידי תוקפים, מה **שעלול לסכן את אבטחת** השירותים שהם מספקים.

בנוסף, ייתכן ש TTPs -**לא תמיד יהיו זמינים או נגישים**, מה שעלול לשבש את זמינות השירותים שהם מספקים.

כדי לצמצם את הסיכונים הכרוכים בשימוש ב- TTPs, ארגונים יכולים ליישם אמצעים כגון TTPs יתירים, מערכות גיבוי וניטור כדי להבטיח את ההמשכיות והאבטחה של השירותים הניתנים.

במאמר [1] נתנו דוגמה לפתרון חותמת זמן מבוסס TTP, שהיא תשתית החתימה ללא מפתח Keyless Signature Infrastructure (KSI) המופעלת על ידי חברת האבטחה האסטונית Guardtime (2018). מערכת KSI מבוססת על יצירת הוכחות תקינות ללא צורך במפתחות הצפנה. **זה מושג על ידי צבירת גיבוב ממקורות שונים (Buldas et al., 2013). המערכת פועלת במרווחי זמן קבועים, ומייצרת עץ צבירה אחד לכל סיבוב. קודי הגיבוב של שורשי העץ מאוחסנים במבנה נתונים מותאם אישית המכונה לוח שנה של גיבובים. גיבוב השורש של לוח השנה מתפרסם באופן קבוע בעיתונים אסטוניים לצורך אימות ציבורי (Buldas et al., 2014).**

אחד היתרונות של שיטת KSI הוא שהיא פחות מועדת להתקפות של אלגוריתמים מבוססי מחשוב קוונטי מכיוון שהיא מסתמכת רק על גיבוב ואינה משתמשת בקריפטוגרפיה של מפתח ציבורי (Buldas et al., 2014). בנוסף, המערכת ניתנת להרחבה רבה הודות לשימוש במספר שכבות צבירה. **עם זאת, אחד החסרונות של הפלטפורמה הוא שהיא מבוססת קוד סגור ובתשלום, וגם מסתמכת על אבטחת התשתית של Guardtime.**

### 3.1.2. מחקרים קודמים מאמר 3

לפי מאמר [3], בהשוואה לגישות אחרות, BlockAudit מציע מספר יתרונות.
הגישה של שנייר וקלסי [17] לרישום ביקורת מאובטח כוללת יצירת ערכי יומן ביקורת לפני התקפה. עם זאת, משמעות הדבר היא שאם התקפה מתרחשת לפני יצירת ערכי יומן הביקורת, המערכת שלהם לא תזהה את ההתקפה. בנוסף, המערכת שלהם אינה מספקת דרך למנוע מתוקף למחוק או להוסיף רשומות ביקורת, אשר ניתן לזהות בקלות על-ידי BlockAudit.
סאטון וסמבי [7] הציעו גישה מבוססת בלוקצ'יין המאחסנת את תקציר הוכחת השלמות לבלוקצ'יין של ביטקוין. בעוד שגישה זו משתמשת במאפייני האבטחה של בלוקצ'יין כדי לשפר את האבטחה של יומני הרישום שאינם ניתנים לשינוי, **היא אינה מספקת דרך ליצור יומני ביקורת בזמן אמת כאשר מתרחשות עסקאות, כפי שעושה BlockAudit.**
בסך הכל, בעוד שלגישות אלה יש חוזקות משלהן והן עשויות להיות שימושיות במצבים ספציפיים, הן אינן מציעות את אותו פתרון מקיף לרישום ביקורת מאובטח כמו שהחוקרים ב BlockAudit הציעו, המשלב מערכות OLTP עם בלוקצ'יין כדי ליצור יומני ביקורת בזמן אמת ומספק מצב חסין מפני חבלה של יומן הביקורת העמיד בפני התקפות.

## 3.2. חשיבות יומני ביקורת

### 3.2.1. חשיבות יומני ביקורת מאמר [1]

במאמר [1] החוקרים עומדים על החשיבות בניתוח באופן שוטף את נתוני היומן המיוצרים על ידי מערכות המידע של הארגון על מנת למנוע פרצות אבטחה ולזהות התקפות פוטנציאליות על תשתית הארגון. במקרה של פריצה, חיוני לזהות את התוקף בחקירה פורנזית ולהעמידו לדין. עם זאת, התוקפים עשויים לנסות לשנות או למחוק ערכי יומן שיכולים לשמש כראיות, מה שמקשה על הוכחת מעשיהם הפסולים בבית המשפט. **כדי להבטיח שראיות יומן יישארו קבילות, על הארגון להיות מסוגל לספק הוכחה לשלמותו, ולהבטיח כי לא התרחשו שינויים במהלך העיבוד**. השימוש במערכות כמו SIEM יכול לסייע בניתוח זה ובשימור נתוני יומן.
כשמדובר בשימוש בראיות דיגיטליות בהליכים משפטיים, ישנן דרישות מסוימות שיש לעמוד בהן על מנת שהראיות ייחשבו קבילות מבחינה משפטית. דרישות אלה הן **רלוונטיות ואותנטיות**. על מנת שפיסת ראיה דיגיטלית תהיה רלוונטית, עליה להיות קשורה ישירות למקרה הנדון ולהיות מסוגלת לספק מידע שימושי לבית המשפט. בנוסף, הראיות חייבות להיות אותנטיות, כלומר הן חייבות להיות אמיתיות ולא טופלו שלא כדין בשום צורה.

#### 3.2.1.1. חשיבות שרשרת מתמשכת של משמורת [1]

החוקרים במאמר [1] מראים שאחת הדרכים להבטיח את האותנטיות של ראיות דיגיטליות היא לשמור על שרשרת מתמשכת של משמורת. משמעות הדבר היא שיש ליצור, להעביר ולאחסן את הראיות באופן שניתן לאמת ולהסתמך עליו.

טכנולוגיית הבלוקצ׳יין מציעה גישה חדשנית להבטחת שלמות ואי-התכחשות לאירועי יומן באופן מאובטח. **על ידי שימוש בבלוקצ׳יין מורשה, ניתן לפתח תשתית מאובטחת שאינה דורשת ספק שירות מהימן.** תשתית זו משתמשת בשכבת ביקורת מבוזרת כדי לאחסן הוכחות תקינות עבור כל ערך יומן, אשר ניתנות לאימות על ידי מבקרי המערכת. רשת הבלוקצ׳יין המאחסנת את ההוכחות הללו מתוחזקת על ידי קונסורציום של מפעילים עצמאיים, מה שמבטיח שהנתונים יישארו עמידים בפני חבלה וזמינים.

### 3.1.1.1. תכנון מערכת ביקורת בלוקים [3]

במאמר [3] החוקרים מראים שהשלב הראשון בעיצוב Block Audit הוא לגשת למערכת יצירת יומן ביקורת בקנה מידה גדול שנמצאת כעת בשימוש על-ידי הארגון. במקרה זה, המחברים השתמשו בשירותים המסופקים על ידי ClearVillage Inc. המציעה תוכנה עבור ערים ומחוזות ומנהלת יומן ביקורת ניתן לחיפוש ומתמשך כדי לעקוב אחר שינויים במסד הנתונים. כחלק מהתכנון של Block Audit, מסד הנתונים משמש לאחסון טרנזקציות, בעוד יומן הביקורת הניתן לחיפוש מועבר לבלוקצ׳יין. הדבר מאפשר ליישומים להמשיך להשתמש בשאילתות מסד נתונים פשוטות, לקבל זמני תגובה של תת-שניות וליהנות מהתכונות של הבלוקצ׳יין על-ידי שימוש בו לאחסון יומן הביקורת. שינויים אלה יכולים להתבצע עם שינויים מינימליים ביישומים קיימים.

על-ידי שילוב יומן הביקורת עם הבלוקצ׳יין Block Audit. הפתרון של החוקרים שואף לשפר את האבטחה והתקינות של מסד הנתונים ויומן הביקורת, ובכך להקשות על תוקף להשחית את הנתונים או לשנות אותם.

#### 3.1.1.1.1. יומני ביקורת ופגיעויותיהם [3]

במאמר [3] החוקרים, מסבירים על יומני ביקורת אשר משמשים במערכות עיבוד טרנזקציות מקוונות כדי לעקוב ולנטר את פעילות המשתמשים, לספק תובנות לגבי העיבוד הרציף של טרנזקציות ולזהות אי-התאמות, חריגות או פעילויות זדוניות. יומני רישום אלה נוצרים כאשר משתמש מורשה מבצע טרנזקציה למסד הנתונים, דבר הגורם לשינוי בערך של אובייקט. השינוי נרשם ביומן הביקורת, שבו ניתן להשתמש לאחר מכן כדי לאמת את הגודל המצטבר של עסקאות ואת סך התשלום שבוצע במהלך השנה. יומני ביקורת חשובים למטרות ביקורת והבטחת מקור, והם חייבים להיות נגישים וניתנים לחיפוש בקלות מהיישום.

**בקצרה, יומני ביקורת משמשים כתיעוד של שינויים שבוצעו במסד הנתונים והם חיוניים להבטחת השלמות והאבטחה של עסקאות מקוונות.**

בעוד שיומני ביקורת שימושיים למעקב אחר שינויים שבוצעו במסד הנתונים ולהבטחת נכונות המערכת, הם גם **פגיעים** להתקפות שעלולות לפגוע בתקינות של מערכות עיבוד טרנזקציות מקוונות. התקפות אלה יכולות לבוא בצורה של וקטורים התקפה שונים המנצלים חולשות ידועות במערכת. **כדי להגן על נתוני ביקורת**, ניתן להשתמש בשיטות קונבנציונליות כגון שימוש בהתקן הוספה בלבד או בהתקן אופטי מסוג כתיבה לאחר קריאה מרובה (WORM). עם זאת, מערכות אלו מסתמכות על ההנחה שלא ניתן לפגוע באתר הרישום, מה שלא תמיד קורה. תוקפים יכולים לעתים קרובות לנצל פגיעויות במערכות הרישום כדי לטפל שלא כדין בנתונים ביומני הביקורת, מה שהופך אותם ללא אמינים. לכן, חשוב שיהיו אמצעי אבטחה חזקים כדי להגן על יומני ביקורת ולהבטיח את שלמותן של מערכות עיבוד טרנזקציות מקוונות. אם התוקף מצליח להשיג את האישורים של משתמש מורשה, הוא יכול להשתמש באישורים אלה כדי להשחית הן את מסד הנתונים והן את יומן הביקורת. הדבר יכול לאפשר להם לטפל במסד הנתונים ואולי למנוע ממנו לאכלס את יומני הביקורת. לחלופין, אם התוקף מצליח לסכן את מסד הנתונים עצמו, הוא יכול לחבל במסד הנתונים וגם להפוך את תהליך הביקורת ללא זמין על-ידי מניעת תאימות לאחור של יומני הביקורת עם מסד הנתונים. משמעות הדבר היא שיומני הביקורת לא ישקפו בצורה נכונה את מצב מסד הנתונים, מה שיקשה על זיהוי אי התאמות או חריגות.

**לכן חשוב לנקוט באמצעי אבטחה חזקים כדי להגן מפני סוגים אלה של התקפות ולהבטיח את שלמות מסד הנתונים ויומני הביקורת.**

### 3.1.1.1.2. שימוש בטכנולוגיית בלוקצ׳יין להתגבר על החולשות [3]

בכדי לתת מענה הולם לחולשות הנ״ל של אבטחת יומני ביקורת, ניתן להשתמש בטכנולוגיית בלוקצ׳יין אשר תוכל לספק לנו הגנה ויכולת אי-הכחשה ברמה גבוהה שתאפשר לארגונים לסמוך על המידע שנשמר ברשת הבלוקצ׳יין בזכות מהימנות רשת הבלוקצ׳יין אשר היא מערכת מבוזרת אשר מפחיתה ריכוזיות של גורם עניין יחיד אשר יש לו שליטה על המידע ויכול לשנות אותו במידה והוא שולט היחיד במערכת.

#### 3.1.1.1.1.1. מודל האיום במערכת OLTP[3]

במאמר [3], המחברים מניחים כי לתוקף יש הן גישה פיזית לבסיס המחשוב המהימן (TCB) במערכת והן היכולת לחדור מרחוק למערכת עיבוד הטרנזקציות המקוונת (OLTP) על ידי ניצול באגים בתוכנה. מערכת OLTP הנבחנת דומה למאגר מכירות קמעונאיות, מיישמת פרוטוקולי תקשורת מאובטחים כגון SSL/TLS, ומתחזקת מסד

נתונים של רשומות מכירות ויומן ביקורת מרוחק העוקב אחר שינויים שבוצעו באמצעות עסקאות. תחת הנחות אלה, התוקף יכול להפעיל **שתי סוגי התקפות: התקפת גישה פיזית והתקפת פגיעות מרחוק.**

#### 3.1.1.1.1.1.1 התקפת הגישה הפיזית

**בהתקפת הגישה הפיזית**, התוקף משיג את האישורים של משתמש עם הרשאה ליצור עסקאות חדשות ומשתמש בהם כדי להתחזות למשתמש הלגיטימי כדי להשחית את מסד הנתונים ואת יומן הביקורת. התוקף יכול לטפל בנתונים בתוך מסד הנתונים ולטפל שלא כדין בהיסטוריה המתוחזקת על-ידי יומן הביקורת כדי להשחית את תהליך הביקורת. התקפה זו מניחה שהתוקף הוא מאוד מתקדם ומתוחכם עם גישה לרכיבי מערכת מרכזיים.

#### 3.1.1.1.1.1.2 התקפת הפגיעות מרחוק

בהתקפת הפגיעות מרחוק, התוקף מנצל פגיעויות ברירת מחדל ביישום OLTP, כגון תקלות תוכנה, התקפות של תוכנות זדוניות או התקפות של הצפת מאגר. בעוד תוקף זה אינו חזק כמו בהתקפת הגישה הפיזית, הם עדיין יכולים לזהם את מסד הנתונים ואת יומן הביקורת עם מידע שגוי. עם זאת, המחברים מניחים כי יישום OLTP מאובטח מפני התקפות מסד נתונים ורשת קונבנציונליות, כגון הזרקת SQL ואימות חלש.

#### 3.1.1.1.1.1.3 התמודדות עם התקפות יומן ביקורת

כדי לנטרל את ההתקפות על יומני ביקורת שתוארו בסעיפים הקודמים, המחברים מציעים מערכת בשם Block Audit המשלבת מערכות עיבוד טרנזקציות מקוונות (OLTP) עם בלוקצ׳יין כדי לשפר את האבטחה. Block Audit שואפת לטפל בפגיעויות ביומני ביקורת ולספק פתרון מאובטח למעקב אחר שינויים שבוצעו במסד הנתונים ולהבטחת שלמות העסקאות המקוונות. על-ידי שימוש בבלוקצ׳יין, הוא יכול ליצור תיעוד ברור מפני פתיחה לא מורשית של כל השינויים שבוצעו במסד הנתונים, ובכך להקשות על תוקף להשחית את יומני הביקורת או לטפל במסד הנתונים.

## 3.3. סיכום שמירת ואחזור מידע של יומני הביקורת ברשת בלוקצ׳יין

לסיכום, בחלק זה עמדנו על תהליך וחשיבות שימוש בטכנולוגיית בלוקצ׳יין לצורך שמירת יומני ביקורת, בצורה מאובטחת, המספקת פתרון מאובטח למעקב אחר שינויים שבוצעו במערכות המיחשוב השונות ובמסד הנתונים, ובכך להקשות על תוקף להשחית את הנתונים או לשנות אותם.

# 4. הצגה והסבר של פתרונות העושים שימוש ברשת הבלוקצ׳יין, כפי שמובא במאמרים

## 4.1. פתרונות מוצעים מאמרים [5],[3],[1]

במאמרים הבאים נראה ששימוש ברשת בלוקצ׳יין מאפשרת הבטחה שנתוני היומן יאוחסנו בצורה מאובטחת ומאומתת באופן שיכול לשמש כראיה במקרה של תקרית אבטחה, חלק מהחוקרים מציעים שימוש ברשת בלוקצ׳יין ציבורית וטכנולוגיה משלימה של מערכת מבוזרת לשמירת נתונים, אחרים מציעים שימוש בשילוב של רשתות בלוקצ׳יין פרטית וציבורית כדי להתגבר על מספר חסרונות ולמעשה לתת פתרון מעשי, כפי שנראה בהמשך יש עדיין לא מעט אתגרים במימוש מערכת לניהול יומני בקורת בצורה מאובטחת ואמינה, תחום זה ימשיך להתפתח ולהשתפר.

### 4.1.1. פתרון מוצע מאמר [1]

כדי להבטיח את הרלוונטיות והאותנטיות של נתוני יומן, חשוב ליישם אמצעים המונעים חבלה ומבטיחים את שלמות הנתונים. גישה אחת שהוצעה למטרה זו היא השימוש בטכנולוגיית בלוקצ׳יין.

כדי להעריך את היעילות של מערכת הרישום המאובטחת המוצעת שלהם [1] המבוססת על בלוקצ׳יין מורשה, המחברים יצרו אב טיפוס כחלק מפרויקט DINGfest (detection, visualization, forensic processing of security incidents)

פרויקט DINGfest הוא תשתית SIEM בקוד פתוח המורכבת משלושה מרכיבים עיקריים: **איסוף נתונים, ניתוח נתונים וזיהוי פלילי ודיווח על תקריות**. המחברים הוסיפו **רכיב רביעי**, **ביקורת נתונים**, כדי להבטיח יכולת ביקורת משפטית ולהעריך את מערכת הרישום המאובטחת המוצעת.

אב הטיפוס נבנה בתוך תשתית DINGfest ונבדק לאבטחה וביצועים. תוצאות הערכה זו הראו כי מערכת הרישום המאובטחת המוצעת הייתה יעילה בהבטחת שלמותם ואי-התכחשותם של אירועי יומן, תוך מתן ביצועים טובים.

### 4.1.2. מערכת לאחסון מאובטח של נתוני יומן באמצעות רשת בלוקצ׳יין [1]

מחברי מאמר [1] מתארים מערכת לאחסון מאובטח של נתוני יומן באמצעות רשת בלוקצ׳יין. המערכת נועדה להבטיח זמינות, שלמות ואי-התכחשות לקבצי יומן. היא מורכבת ממספר שלבים: **יצירת ראיות, העברת ראיות, אחסון ראיות ויישוב סכסוכים**. בשלב **יצירת הראיות**, נתוני יומן נוצרים על מקורות יומן (כגון מערכות המחוברות לרשתות חיצוניות) וכוללים חתימות דיגיטליות וחותמות זמן. במהלך שלב **העברת הראיות**, נתוני היומן מועברים למערכת האחסון באמצעות חיבור מוצפן. בשלב **אחסון הראיות**, נתוני היומן מאוחסנים באופן השומר על זמינות ותקינות, כגון שימוש ברשת בלוקצ׳יין. בשלב **יישוב המחלוקות**,

המבקר יכול לאמת את האותנטיות של נתוני יומן הרישום על-ידי בדיקת החתימות הדיגיטליות והוכחות התקינות.
בסך הכל, מטרת המערכת היא להבטיח שנתוני היומן יאוחסנו בצורה מאובטחת ומאומתת באופן שיכול לשמש כראיה במקרה של מקרה של פריצה וחבלה במערכות.

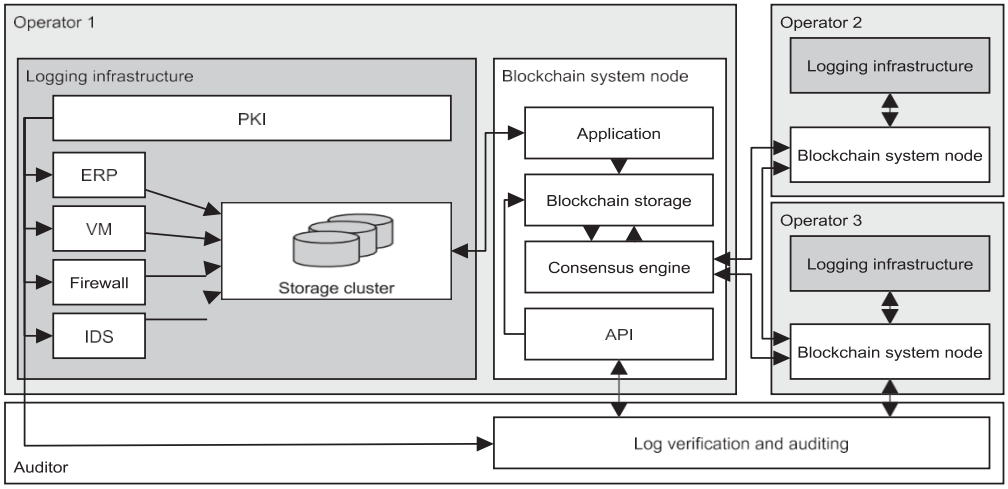
### 4.1.3. שימוש ברשתות בלוקצ'יין מורשות להבטחת שלמות ואי-התכחשות [1]

בנוסף החוקרים במאמר [1] מראים כיצד בלוקציינים מורשים, שבהם קבוצת המשתתפים מאומתת, רלוונטיים במיוחד ליישומים ארגוניים. בהתבסס על בלוקצ׳יין מורשה, ניתן לפתח תשתית מאובטחת המבטיחה את שלמותם ואי-התכחשותם של אירועי יומן ללא ספק צד שלישי מהימן. תשתית זו נועדה להוכיח את קיומו של ערך יומן בעת יצירתו באמצעות הוכחות שלמות המאוחסנות בשכבת ביקורת מבוזרת. רשת הבלוקצ׳יין המאחסנת את ההוכחות הללו מתוחזקת על ידי קונסורציום של מפעילים עצמאיים. מבקרים יכולים לאמת את שלמות הראיות שהוגשו בעבר על ידי יצירת קשר עם כל צומת ברשת. יצירה אוטומטית של חתימה, אחסון והוכחת תקינות עבור כל אירוע יומן רישום מספקת את האימות הדרוש ואת אי-ההתכחשות.

### 4.1.4. ארכיטקטורת המערכת - אחסון ואימות מאובטחים מאמר 1

ארכיטקטורת המערכת **איור 6,** במאמר [1] מתמקדת באחסון ואימות מאובטחים של ראיות שנוצרו על ידי מקורות שונים, כגון יישומי מבוססי קונטיינר, חומות אש או מערכות לגילוי חדירות. מידע זה מועבר למערכת אימות יומן באמצעות פרוטוקולים קיימים, כגון syslog, המיועדים לשידור מאובטח.
לאחר קבלת הראיות על ידי מערכת אימות היומן, היא מנוטרת על ידי אפליקציה נפרדת ונוצרת עסקה עבור כל ראיה חדשה. עסקה זו כוללת גיבוב של הראיות וחותמת זמן. עסקאות אלה מקובצות לאחר מכן לבלוקים ומתווספות לבלוקצ׳יין, יחד עם עסקאות מצמתים אחרים במערכת המבוזרת. זה מבטיח שהראיות יאוחסנו בצורה מאובטחת ועמידה בפני חבלה.
במועד מאוחר יותר, מבקרים יכולים לאמת את שלמות הראיות על ידי בדיקה ראשונה של החתימה מול אישורי מפתח ציבורי חוקיים מתשתית מפתח ציבורי (PKI) פעולה זו מבטיחה שניתן יהיה לאתר את קובץ יומן הרישום בחזרה למקור שלו. לאחר מכן, המבקר יכול להגיש את הגיבוב של הראיות לצומת בלוקצ׳יין לצורך אימות. אם ערכי הגיבוב המאוחסנים בעסקאות הבלוקצ׳יין תואמים את הגיבוב של הראיות המוצעות, ניתן להוכיח שהנתונים הוגשו במועד מוקדם יותר. כדי להבטיח את שלמות התהליך, ניתן לבקש את ההוכחה גם ממספר צמתי בלוקצ׳יין באופן עצמאי, במקרה שאחד הצמתים פגום.

ארכיטקטורת מערכת זו נועדה לספק דרך מאובטחת ואמינה לאחסן ולאמת ראיות ממקורות שונים, תוך שימוש בטכנולוגיית בלוקצ׳יין כדי להבטיח את שלמותם ואי-התכחשותם של הנתונים.




*איור 6 מערכת שחוקרי מאמר 1 מימשו*

*.Fig. 2. Proposed design for a secure and auditable logging infrastructure*

### 4.1.5. יצירת עסקאות בלוקצ'יין הליך רישום רשמי [1]

המחברים מתארים הליך רישום רשמי עבור מערכת הרישום המאובטחת שלהם, הכולל שלושה שלבי עיבוד: S1, S2 ו- S3.

- **שלב S1**: **עיבוד יישומי לקוח**: בשלב זה, כל ערך יומן חדש (Ljk) מנותח כדי ליצור נתוני טרנזקציות (Pji). נתוני העסקאות כולל את ערך יומן הרישום, כמו גם את הזהות (IDj) והמפתח הציבורי (Kj) של הארגון שיצר את ערך היומן. נתוני העסקה נכלל בעסקה חדשה (Tji) יחד עם hash (Hji) של ערך היומן וחתימה דיגיטלית (Sji) שנוצרה באמצעות מפתח החתימה הפרטי של הארגון (Zj). העסקה מועברת לצומת בלוקצ'יין דרך ערוץ מוצפן כדי למנוע התקפות אדם בתווך.
- **שלב S2**: **עיבוד צומת בלוקצ'יין**: בשלב זה, העסקה מעובדת בכל צומת ברשת הבלוקצ'יין. כל צומת כולל חותמת זמן המבוססת על קונצנזוס מבוזר ומאמת את הייחודיות של ערך היומן על ידי בדיקה שהוא עדיין לא חלק מהמערכת. אם ערך יומן הרישום הוא ייחודי, מיפוי של קוד ה- Hash של התוכן לקוד ה- Hash של עסקת הבלוקצ'יין מתווסף למילון כדי לאפשר בדיקות מידע יעילות במהלך האימות. לאחר שיותר משני שלישים מכל הצמתים עיבדו בהצלחה את העסקה, היא מחויבת באופן בלתי הפיך לפנקס התנועות.
- **שלב S3**: **אימות**: בשלב אופציונלי זה, משתמש יכול לשלוח ערך יומן רישום ליישום הלקוח, המבקש הוכחה מרשת הבלוקצ'יין על-ידי שליחת הגיבוב של ערך יומן הרישום. אם העסקה המתאימה נמצאה והוחזרה, החתימה והגיבוב מאומתים באמצעות המפתח הציבורי המתאים ופונקציית גיבוב עמידה בפני קדם-תמונה. אם החתימה והגיבוב נכונים, קיימת הוכחה שאינה ניתנת לדחייה לכך שערך יומן הרישום נשלח במועד מוקדם יותר.

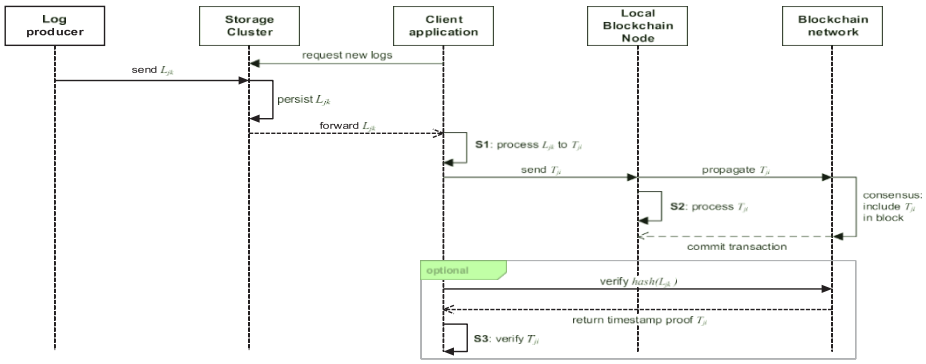



**Fig. 3.** Sequence diagram of log entry processing data flows.

איור 7: יצירת עסקאות בלוקצ'יין *הליך רישום רשמי* [1]

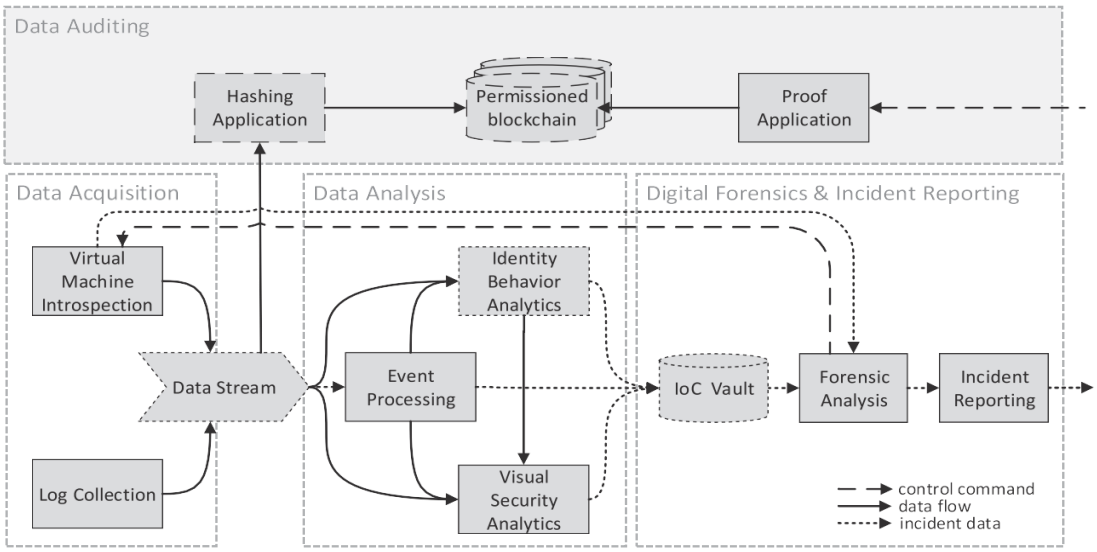
### 4.1.6. תפעול רשת בלוקצ׳יין ועיגון לרשת ציבורית

המחברים במאמר [1] דנים תפעול רשת הבלוקצ׳יין במערכת הרישום המאובטחת שלהם. הם מציעים כי הרשת צריכה להיות מורכבת **מארבעה צמתים לפחות**, המופעלים על ידי ארגונים נפרדים או בתוך ארגון יחיד אך מפוזרים על פני מספר מיקומים או יחידות. **זה עוזר להקשות על הארגון או על התוקף לשנות את הנתונים בבלוקצ׳יין**. עם זאת, אם הרשת מופעלת **בתוך ארגון יחיד, קיים סיכון שהארגון עלול ליזום החלפה מתואמת של נתוני בלוקצ׳יין כדי להסתיר פרצה בתשתית שלו**. כדי למתן את הסיכון הזה, המחברים מציעים להוסיף **מנגנון עיגון לבלוקצ׳יין המורשה**, הכולל את גיבוב הבלוקים האחרון בעסקה במערכת ללא הרשאות כמו **ביטקוין**. זה מאפשר למבקרים חיצוניים לאמת בפומבי את מצב הבלוקצ׳יין הפרטי בזמן העגינה, אך הוא גם כרוך **בעמלות עסקה**. תדירות העיגון צריכה להיות מאוזנת בקפידה כדי למזער עלויות, אך גם כדי למנוע מהארגון להחליף את נתוני הבלוקצ׳יין בחלון הזמן שבין הבלוקים.

### 4.1.7. תכנון ובניית אב טיפוס [1]

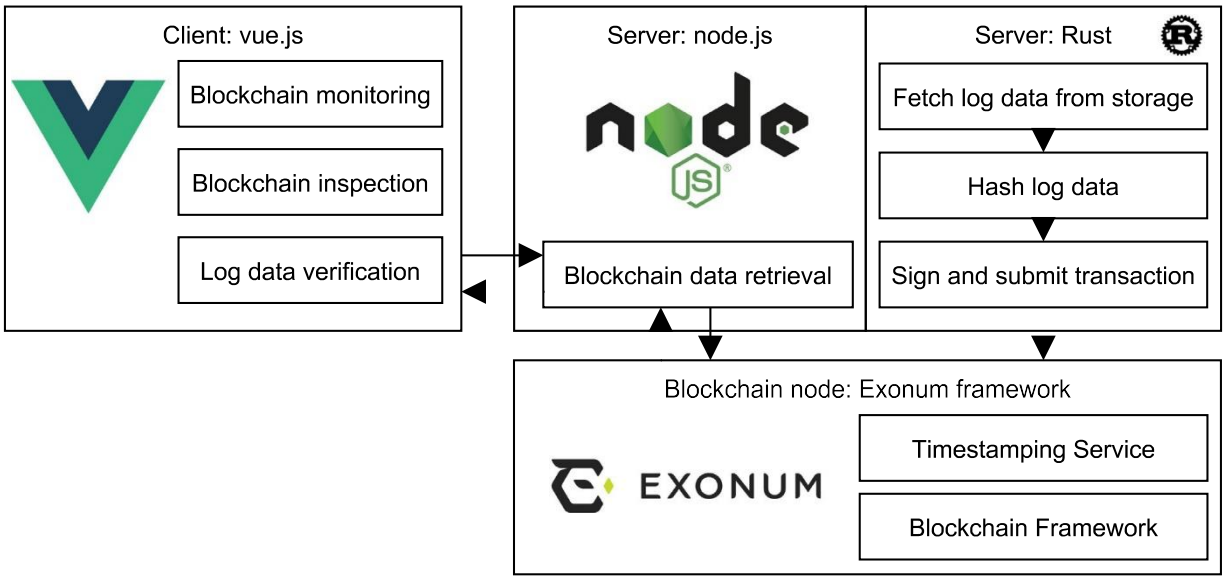
מערכת אב-טיפוס לשירות ביקורת יומנים מבוזרת המשתמשת בבלוקצ׳יין כדי להבטיח את שלמותן, יכולת הביקורת ואי-התכחשותן של רשומות יומן. אב הטיפוס בנוי על גבי תשתית קיימת בשם:

DINGfest (detection, visualization, forensic processing of security incidents), הכוללת אשכול אחסון אך חסרה את היכולת להבטיח את שלמות רשומות היומן. כדי לטפל בכך, אב הטיפוס מוסיף יישום גיבוב המחשב את הגיבוב SHA256 עבור כל רשומת יומן, יחד עם חתימתו, ושולח את הגיבוב לבלוקצ׳יין בעסקה חתומה. הבלוקצ׳יין, המיושם באמצעות רשת Exonum, משמש לאימות קודי הגיבוב ולחותמת הזמן שלהם בקונצנזוס עם מאמתים אחרים. אב הטיפוס כולל גם יישום המספק ממשק אינטרנט למבקרים לשליחת רשומות יומן לאימות. Exonum נבחר בזכות אלגוריתם הקונצנזוס הסובלני לתקלות הביזנטי המוכן לייצור ותמיכה בחותמות זמן מבוזרות ובעיגון ביטקוין. אב הטיפוס נועד להתגבר על חששות אבטחה ומדרגיות במונחים של תפוקה ואחסון.




איור 8: ארכיטקטורה של המערכת ממאמר [1]

**Fig. 4.** The DINGfest SIEM architecture extended with an auditing layer (based on Menges et al., 2018).




איור 9א: ממאמר 1 ארכיטקטורה של המערכת שבנו

Client-server architecture of the application prototype

#### 4.1.7.1. הערכת אב הטיפוס [1]

הערכה של אב טיפוס עבור שירות ביקורת יומן מבוזר המשתמש בבלוקצ׳יין כדי להבטיח את השלמות, יכולת הביקורת ואי-ההתכחשות לרשומות יומן. ההערכה מתמקדת הן באבטחה והן בביצועים.

#### 4.1.7.2. אבטחת מערכת [1]

כדי להעריך את האבטחה של אב הטיפוס, ארבעה איומים בסיסיים נחשבים: **יירוט, הפרעה, שינוי וייצור**.

כדי למנוע **יירוט**, אב הטיפוס מגדיר ערוצי תקשורת מאומתים ומוצפנים בין צמתים.

כדי למנוע **הפרעה**, אב הטיפוס משתמש באלגוריתם קונצנזוס סובלני לתקלות ביזנטי שדורש יותר משני שלישים מהצמתים כדי להסכים לבצע עסקה, ומעוגן לבלוקצ׳יין ללא הרשאה כדי למנוע מהתוקף להשיג שליטה על הרשת.

כדי למנוע **שינויים**, אב הטיפוס משתמש בגישה דו-שכבתית המגנה על הזמינות של רשומות יומן הרישום עם אשכול אחסון משוכפל ועל שלמות רשומות היומן עם הוכחות בבלוקצ׳יין.

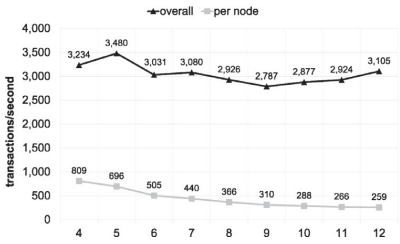
כדי למנוע **ייצור**, אב הטיפוס מסתמך על אמצעים משפטיים כדי לשלול את האפשרות של ייצור ארגוני וממליץ לאמת את היומנים לאותנטיות לפני הפשרה. הערכת הביצועים מתמקדת במדדי תפוקה ואחסון בפריסה מבוססת ענן של אב הטיפוס. אב הטיפוס נבדק על יכולתו להתמודד עם הכנסת רשומות יומן לבלוקצ׳יין בקצב של 1000 רשומות בשנייה, ועל יכולתו לטפל באחזור רשומות יומן מהבלוקצ׳יין בקצב של 100 רשומות בשנייה. אב הטיפוס נבדק גם ביכולתו לאחסן רשומות יומן בבלוקצ׳יין לתקופה של שנה לפחות. תוצאות ההערכה מראות כי אב הטיפוס יכול להתמודד עם הכנסה ואחזור של רשומות יומן בקצב הנדרש, ויכול לאחסן רשומות יומן בבלוקצ׳יין למשך פרק הזמן הנדרש.

### 4.1.7.3. ביצועי מערכת [1]

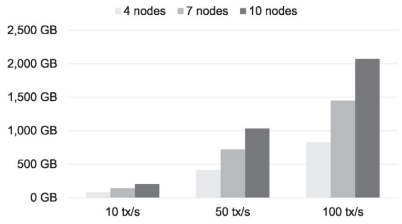
הביצועים של אב טיפוס עבור שירות ביקורת יומן מבוזר המשתמש בבלוקציין כדי להבטיח את השלמות, יכולת הביקורת ואי-ההתכחשות לרשומות יומן. הביצועים של אב הטיפוס מוערכים במונחים של תפוקת העסקה, מדרגיות הצומת ודרישות האחסון. כדי להעריך את תפוקת העסקה, אב הטיפוס נבדק על יכולתו להתמודד עם הכנסת רשומות יומן לבלוקציין בקצב של 5000 עסקאות בשנייה. התוצאות מראות כי אב הטיפוס יכול להתמודד בממוצע עם 3000 עד 3500 עסקאות בשנייה, מה שמניב בין 250 ל-800 עסקאות מעובדות לכל צומת. כדי להעריך את **מדרגיות הצומת**, אב הטיפוס נבדק עם מספר שונה של צמתים והתוצאות מראות שביצועי הצומת יורדים ככל שמספר הצמתים גדל, אך הביצועים הכוללים נשארים יציבים. כדי להעריך את **דרישות האחסון**, אב הטיפוס נבדק על יכולתו לאחסן רשומות יומן בבלוקציין לתקופה של **חודש** לפחות והתוצאות מראות כי מסד הנתונים גדל באופן **ליניארי** הן עם התפוקה והן עם מספר הצמתים.

אב הטיפוס כולל גם פתרון **להפחתת דרישות האחסון** על ידי **קיבוץ רשומות יומן לעסקאות**, אך לפתרון זה יש את החיסרון של התייחסות לרשומות המקובצות כיחידת שלמות אחת והפיכת זה **לבלתי אפשרי להוכיח את שלמותן של רשומות בודדות**.

אב הטיפוס מציע גם שימוש במערכת בלוקציין מתגלגלת להשלכת בלוקים שאינם נחוצים עוד על בסיס מדיניות שמירת הלוגים הארגונית, אך לא קיים כיום יישום קוד פתוח של מערכת זו.




(a) Transactions per second for varying node counts.




(b) Storage requirements for varying average throughput and node counts.

איור 9ב ביצועי אב-הטיפוס - ממאמר [1]

**Fig. 6.** Prototype performance benchmark results.

### 4.1.7.4. השוואה עם גישות אחרות לרישום מאובטח המבוססות על בלוקצ'יין [1]

הביצועים והתכונות של אב טיפוס עבור שירות ביקורת יומן מבוזר המשתמש בבלוקצ'יין עם גישות אחרות המבוססות על בלוקצ'יין לרישום מאובטח. אב הטיפוס מושווה לגישות אחרות המשתמשות הן בבלוקצ'יין ללא הרשאה (למשל ביטקוין) והן בבלוקצ'יין מורשה (למשל Fabric). ההשוואה מדגישה כי אב הטיפוס מבוסס על בלוקצ'יין מורשה (Exonum) וכוללת אפשרות לעיגון מבוסס קונצנזוס לבלוקצ'יין של ביטקוין כדי להעלות את רמת העמידות לחבלה. אב הטיפוס כולל גם אמות מידה למגבלות תפוקה ואחסון, ומציע פתרונות להגדלת המדרגיות באמצעות קיבוץ רשומות יומן ושימוש בבלוקצ'יין מתגלגל. לשם השוואה, הגישות האחרות מפרידות בין הוכחת השלמות לנתוני היומן (למשל גישות מבוססות ביטקוין) או מאחסנות נתוני יומן חלקיים או מלאים בבלוקצ'יין (למשל גישות מבוססות רשת פבריק), מה שמגביל את המדרגיות שלהן. אב הטיפוס מציע גם אי-השתנות לפי כניסה על ידי שימוש בבלוקצ'יין מורשה ואי-התכחשות ציבורית על ידי פרסום בלוקים לבלוקצ'יין ללא הרשאה.

| מאמר | בלוקצ'יין | רשת מורשית? | BFT | כולל בדיקות ביצועים? | הוכחה/נתונים | תמיכה באי-השתנות ברמת רשומה |
|---|---|---|---|---|---|---|
| Cucurull and Puiggalí (2016) | Bitcoin | - | n.a. | - | ✓ | - |
| Sutton and Samavi (2017) | Bitcoin | - | n.a. | - | ✓ | ✓ |
| Ahmad et al. (2018) | Fabric | ✓ | - | - | - | ✓ |
| Shekhtman and Waisbard (2018) | Fabric | ✓ | - | - | - | ✓ |
| [1] Present work | Exonum | ✓ | ✓ | ✓ | ✓ | (✓)[a] |

[a] Without log grouping from Section 5.2

טבלה 1 משווה את התכונות של גישות שונות מבוססות בלוקצ'יין לרישום מאובטח, כולל אב הטיפוס שתואר בסעיפים הקודמים מאמר [1].

הסבר של העמודות בטבלה 1:

- **מאמר**: שם המאמר או העבודה המתארת את הגישה.
- **בלוקצ'יין**: שם טכנולוגיית הבלוקצ'יין המשמשת בגישה.
- **רשת מורשית:** האם הגישה משתמשת בבלוקצ'יין מורשה.
- **BFT**: האם הגישה משתמשת באלגוריתם קונצנזוס סובלני לתקלות ביזנטיות (BFT) מה מאפשר יכולת מדרגיות גבוהה יותר וגם רמת אי-השתנות גבוהה יותר, לעומת השימוש בפרוטוקול Kafka שהמאמרים שהשתמשו בפבריק עשו. יש לציין שכיום פבריק תומך גם בBFT.
- **ביצועים**: האם הגישה כוללת התייחסות למגבלות תפוקה ואחסון. בניגוד למאמרים אחרים, מאמר זה כולל בדיקות ביצועי תפוקה ואחסון שהם בסיסיים עבור פלטפורמות רישום בתדירות גבוהה.

- **הוכחה/נתונים** : האם הגישה מפרידה בין הוכחת התקינות לבין נתוני יומן הרישום. בשל מגבלות אחסון בעסקאות ביטקוין, שיטות ממוקדות ביטקוין מפרידות את נתוני היומן מהוכחת השלמות. מחקרים מבוססי Hyperledger Fabric, לעומת זאת, משלבים באופן חלקי או מלא נתוני יומן בבלוקצ'יין, מה שעלול להגביל את רמת המדרגיות.
- **תמיכה באי-השתנות ברמת רשומה** : זה למעשה יצירת עסקת בלוקצ'יין אחת עבור כל אירוע רישום. בעוד Sutton and Samavi (2017) השתמשו בשיטה זו עם הבלוקצ'יין של ביטקוין, אשר כרוכה בעלויות עסקה גבוהות. Cucurull and Puiggalí (2016) בחרו לפרסם נקודות ביקורת (checkpoints) ולא יומנים בודדים, אך הדבר חושף את היומנים להתקפות חיתוך פוטנציאליות.

אב הטיפוס שתואר בסעיפים הקודמים משתמש בבלוקצ'יין המורשה של Exonum, כולל אלגוריתם קונצנזוס של BFT, כולל התייחסות לאילוצי תפוקה ואחסון, מפריד בין הוכחת התקינות לנתוני היומן, ומציע אי-השתנות לפי ערך (למעט כאשר רשומות יומן מקובצות כמתואר בסעיף 5.2). גישות אחרות, כגון אלה המשתמשות בבלוקצ'יין של ביטקוין או פבריק, מפרידות בין הוכחת התקינות לנתוני היומן או שאינן כוללות התייחסות לאילוצי תפוקה ואחסון.

#### 4.1.7.5. בחירת פרוטוקול קונצנזוס מתאים [3]

**שלב נוסף בתכנון** של ביקורת בלוקים הוא לבחור פרוטוקול קונצנזוס בין העמיתים כדי להגיע להסכמה על רצף העסקאות ומצב הבלוקצ'יין. ישנם אלגוריתמים שונים של קונצנזוס שניתן להשתמש בהם בבלוקצ'יין, כגון הוכחת עבודה (PoW), הוכחת החזקה (PoS), הוכחת ידע (PoK) ועמידות בפני תקלות ביזנטיות (BFT). לכל פרוטוקול קונצנזוס יש יתרונות וחסרונות משלו. לדוגמה, אלגוריתמי PoW ניתנים להרחבה למספר רב של צמתים, אך יש להם השהיה גבוהה (זמן שלוקח להכניס בלוק חדש). לעומת זאת, פרוטוקולי BFT הם בעלי השהיה נמוכה, אך עלולים לסבול מבעיות מדרגיות.

עבור מערכת ביקורת הבלוקים, המחברים בוחרים להשתמש ב- Hyperledger, המשתמש בגרסאות של פרוטוקול BFT כדי להשיג קונצנזוס. Hyperledger הוא ספר חשבונות מבוזר מורשה ארגוני שפותח על ידי קרן לינוקס ומתוחזק על ידי ועדת היגוי חזקה. יש לה קהילת פיתוח הולכת וגדלה התורמת לאימוץ רחב היקף של הטכנולוגיה כתחליף לפתרונות קיימים. המחברים בחרו להשתמש ב- Hyperledger עבור מערכת ביקורת הבלוקים בשל מפרטי התכנון של יישומי יומן ביקורת, הדורשים קונצנזוס מהיר תוך שמירה על גודל רשת קטן יותר. בסך הכל, השימוש בקונצנזוס במערכת ביקורת הבלוקים מסייע להבטיח את האבטחה

והשלמות של מערכת עיבוד העסקאות המקוונת על ידי יצירת הסכמה בין העמיתים על מצב הבלוקצ׳יין.
עבור מערכת ביקורת הבלוקים, המחברים החליטו להשתמש ב- Hyperledger Fabric, בעל ארכיטקטורה ניתנת להגדרה ומודולרית שניתן לייעל אותה למגוון רחב של מקרי שימוש. הוא גם תומך בפריסה של חוזים חכמים על גבי בלוקצ׳יין באמצעות שפות תכנות למטרות כלליות כגון Java, Go ו- Node.js.
Hyperledger Fabric הוא בלוקצ׳יין מורשה, כלומר כל משתתפי הרשת ידועים זה לזה ויש תפיסה חלשה של אנונימיות במערכת. המשתתפים עשויים שלא לסמוך לחלוטין זה על זה, מכיוון שהם עשויים להיות מתחרים, אך ניתן להגביר את האמון באמצעות שימוש בבלוקצ׳יין ללא צורך בצד שלישי. בנוסף, Hyperledger Fabric מציע קונצנזוס הניתן לחיבור, ניהול זהויות, ניהול מפתחות וספריות הצפנה שניתן להתאים אישית על פי צרכי היישום.

### 4.1.8. פתרון מוצע מאמר 5

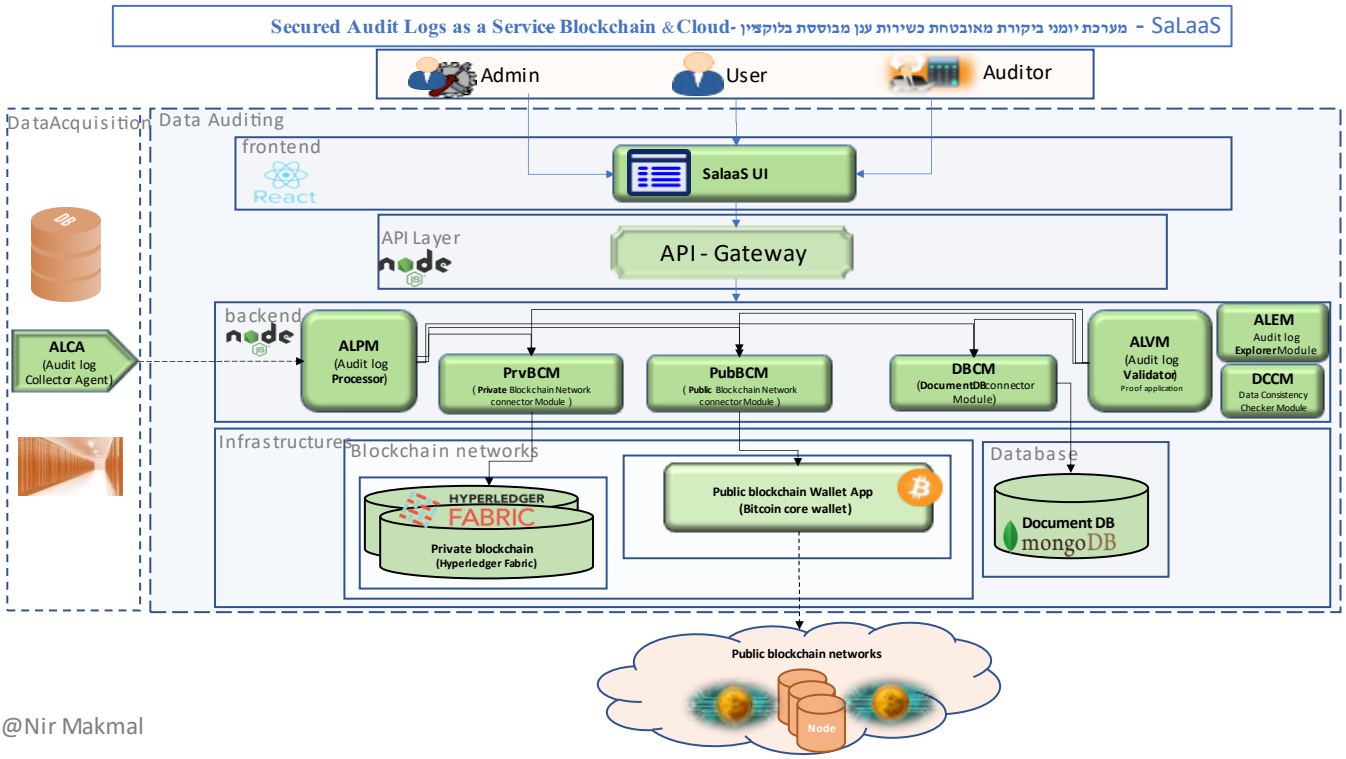
במאמר [5] החוקרים, סוקרים כיצד קבצי יומן רישום ממלאים תפקיד מכריע בשמירה על אבטחה ואמינות בכל מערכת. הם עוזרים לזהות כל פעילות זדונית או עקבות של תוקפים. עם זאת, התוקפים מנסים לעתים קרובות לשנות או לחבל בקבצי יומן הרישום כדי לכסות את עקבותיהם. בענן ציבורי, כל השותפים אחראים לתחזוקת הענן ולהבטחת זמינותו. עם זאת, אם צד כלשהו עושה טעות, זה עלול להוביל לחבלה בקבצי יומן. באופן דומה, בענן ציבורי, ספק השירות אחראי לספק את כל השירותים ברשת ציבורית. אם משתמש נתקל בבעיות ביצועים כלשהן ומבקש דוח מפורט מספק השירות, הספק עשוי לנסות לחבל עם יומני הרישום כדי להוכיח את צדקתו. במקרים כאלה, המצב הופך למקרה קר, שכן קשה להוכיח את החבלה של קבצי יומן. כדי לטפל בבעיה זו, המחברים מציעים להשתמש בטכנולוגיית בלוקצ׳יין כדי לאבטח קבצי יומן באופן מבוזר. **במערכת המוצעת במאמר, המחברים מציעים להשתמש בבלוקצ׳יין ציבורי כגון אתריום כדי לאחסן קבצי יומן בצורה מאובטחת.** ארגונים רבים ברחבי העולם מאמצים את טכנולוגיית הבלוקצ׳יין בגלל תכונות האבטחה והזמינות ברמה הגבוהה שלה. עם זאת, **יש כמה בעיות בשימוש בבלוקצ׳יין לאחסון קבצי יומן. בעיה אחת היא שזה דורש עסקאות מרובות כדי לאחסן קבצים גדולים.** כדי להתגבר על בעיה זו ולהשיג תפוקה גבוהה, המחברים מציעים את השימוש בפרוטוקול **IPFS** (מערכת קבצים בין-פלנטרית). IPFS היא מערכת אחסון קבצים מבוזרת המאפשרת אחסון של קבצים גדולים בעסקה אחת. ראשית, הנתונים מאוחסנים ב- IPFS, ולאחר מכן נוצר גיבוב בגודל קבוע עבור הנתונים שנשלחו. גיבוב זה מאוחסן לאחר מכן בבלוקצ׳יין אתריום.

# 5. דיווח קצר על הפרויקט המעשי בו מימשתי מערכת מבוססת רשת בלוקצ'יין לאבטחת יומני ביקורת.

## 5.1. ארכיטקטורת מערכת - הפרויקט המעשי

המערכת שפיתחתי מורכבת מהחלקים הבאים (איור 10):

1. ממשק גרפי שבו נוכל להגדיר ולראות את נתוני המערכת בשם- SalaaS UI
2. מודל איסוף נתונים בשם - Audit log collector agent -**ALCA**
3. שכבת צד שרת עם מודלים שונים אשר מאפשרים:
   3.1. מידול והכנסת נתונים של יומני מערכת לתוך המערכת שלנו **(Audit log Processor) ALPM**.
   3.2. חיבור לבסיס נתונים (Database connector module) **DBCM**- לצורך שמירת יומני ביקורת.
   3.3. חיבור לרשת בלוקצ'יין פרטית (פבריק) Private blockchain connector module **PrvBCM** אשר תאמת את הנתונים ותוסיף בלוקים חדשים למערכת.
   3.4. חיבור לרשת בלוקצ'יין ציבורית (ביטקוין) public blockchain connector module **PubBCM** אשר תספק עוגן לנתונים ותעלה את רמת האמינות של המערכת. (לצורך הפרויקט אשתמש ברשת ביטקוין testNet , עקב עלויות של רשת ביטקוין הראשית)
   3.5. איתור נתונים של יומני מערכת.(Audit log Explorer Module) **ALEM**
   3.6. אימות נתונים של יומני מערכת (Audit log Validator) **ALVM** .
   3.7. מודל בדיקת תקינות הנתונים שנשמרו במערכת Data Consistency Check **DCCM** Module.
4. שכבת התשתיות:
   4.1. רשת בלוקציי'ן מסוג פבריק
   4.2. תוכנת ארנק ביטקוין קור המחוברת לרשת ביטקוין הציבורית.
   4.3. שרת בסיס נתונים – MongoDB.
5. המערכת מבוססת טכנולוגיית קונטיינר (docker containers) היכולה להיות מותקנת על ענן ציבורי לפי בחירה.

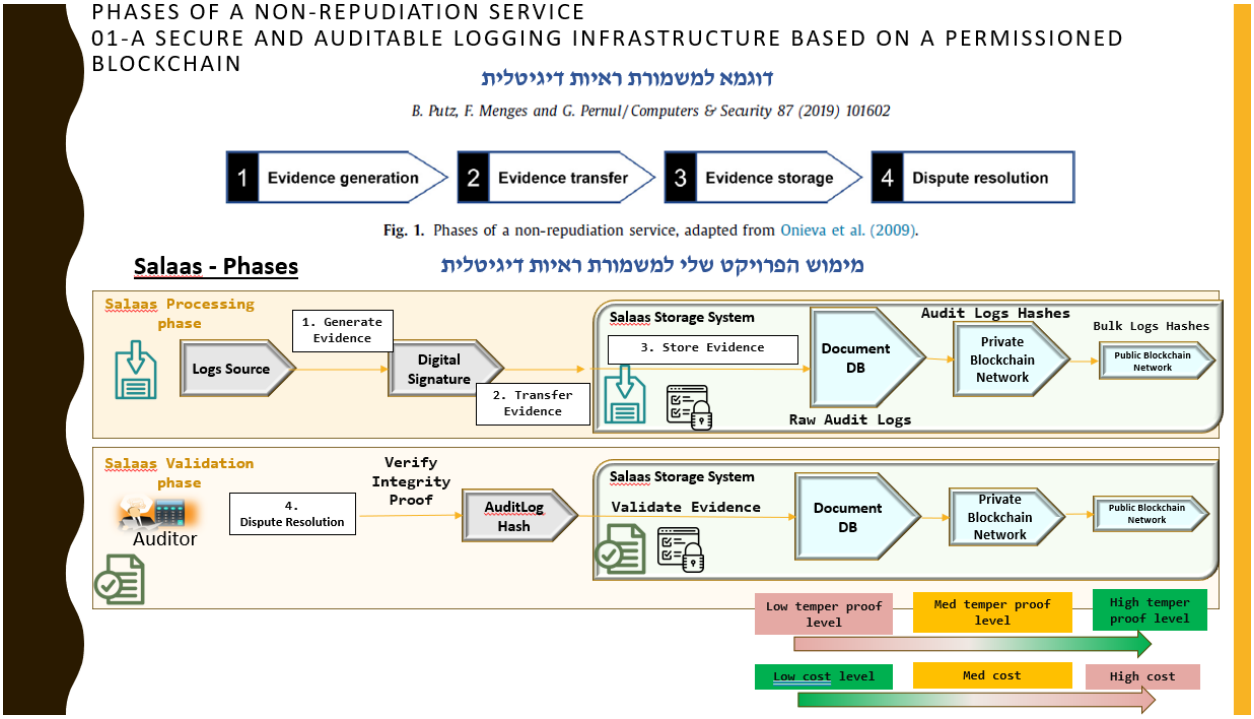



*איור 10 ארכיטקטורה שיצרתי שמתארת הפרויקט - SaLaaS מערכת יומני ביקורת מאובטחת כשירות ענן מבוססת בלוקצ'יין & Secured Audit Logs as a Service – Blockchain & Cloud-*

## 5.2. תיאור שלבי המערכת שפיתחתי

לפי מאמר [1] משמורת ראיות דיגיטליות דורשת את השלבים הבאים: שלב איסוף הראיות, שלב העברת הראיות שהוא צריך להתבצע בצורה מאובטחת, שלב שמירת הראיות שצריך להישמר בצורה מאובטחת כדי שלא יחבלו בראיה, ושלב הוכחה שהראיה תקפה.

בפרויקט שלי אני מממש את תהליך משמורת הראיות של יומני ביקורת בצורה שעולה על תנאי שמירת הראיות בצורה בטוחה, ע"י שימוש בפרוטוקולי הצפנה ושמירת המידע על גבי רשת בלוקצ'יין פרטית ורשת בלוקצ'יין ציבורית. ראוה איור 11.

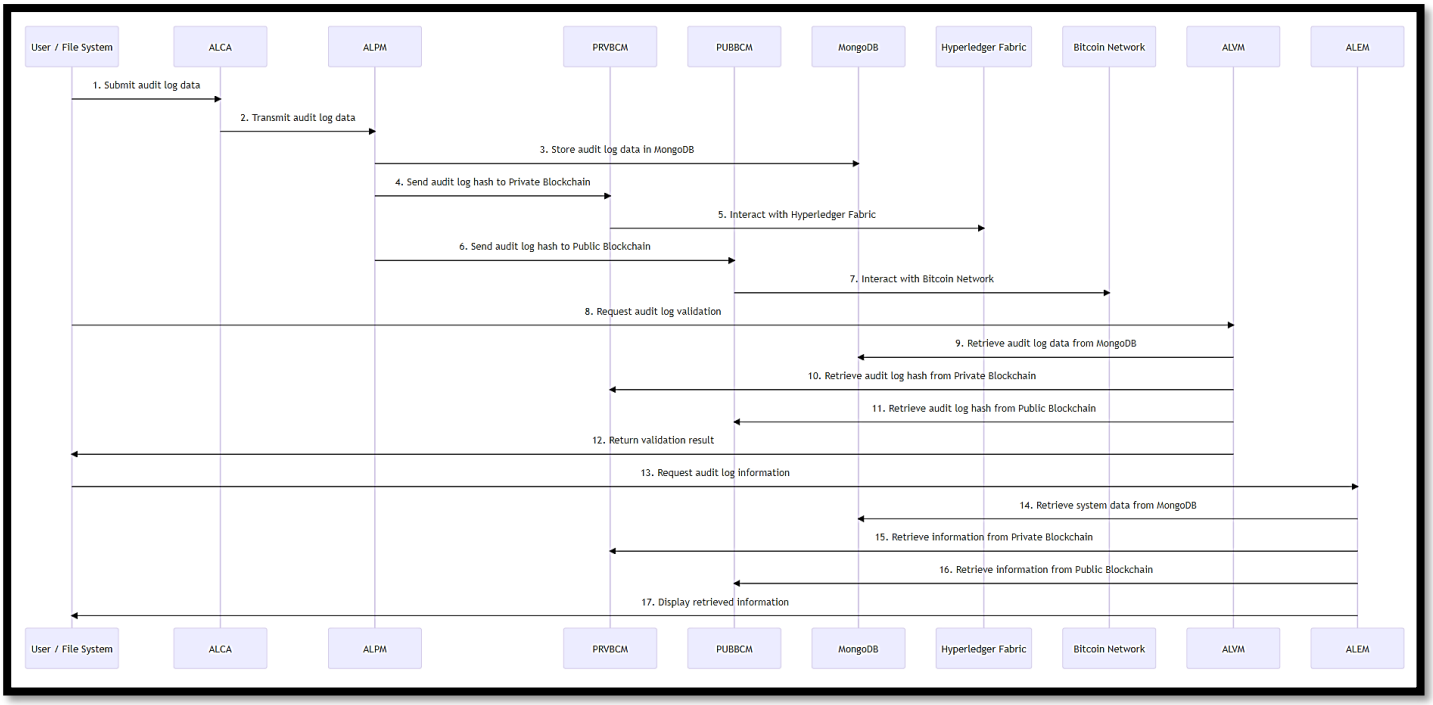



*איור 11 תיאור של הכנסה של יומני מערכת ואימות שלהם*

## 5.3. תיאור הפונקציונליות של המערכת

הפרויקט מאפשר איסוף, אחסון ותיקוף של יומני ביקורת באמצעות רכיבים שונים, המערכת כוללת ממשק משתמש גרפי (GUI), מסד הנתונים MongoDB ורשתות בלוקציין פרטיות וציבוריות. תהליך זה מורכב מסדרה של מודולים, כל אחד עם התפקידים והפונקציות הספציפיים שלו.

בדיאגרמה זו ניתן לראות את הפעולות העיקריות של המערכת. איור 12.




*איור 12 קשרים בין המודלים - SaLaaS מערכת יומני ביקורת מאובטחת כשירות ענן מבוססת בלוקצ'יין Secured Audit Logs as a Service – Blockchain & Cloud-*

להלן שלבי המערכת:

1. **<u>שלב ההכנסה - קריאת נתוני יומן ביקורת גולמי</u>**: נקודת המוצא של המערכת כוללת את המשתמש השולח יומני ביקורת או את היומנים המתועדים במערכת קבצים. סוכן אוסף יומני הביקורת (ALCA) קורא את יומני הרישום, שיכולים לכלול יומני פעילות משתמשים, יומני אירועי מערכת או נתונים רלוונטיים אחרים.

2. **שידור יומן ביקורת**: סוכן אוסף יומני הביקורת (ALCA) שהוא תוכנה המותקנת במערכת של המשתמש, הסוכן אוסף את יומני הביקורת ושולח אותם למודול עיבוד יומני הביקורת (ALPM).

3. **אחסון במסד נתונים**: לאחר מכן, ה-ALPM מאחסן את נתוני יומן הביקורת הגולמיים במסד נתונים של MongoDB. מסד נתונים NoSQL זה יעיל במיוחד לאחסון נתונים בנפח גבוה. השימוש ב-MongoDB הוא קריטי לשמירה על יומני הביקורת הגולמיים הנתונים שלהם לצורך חיפושים

מהירים, **במיוחד מכיוון שהבלוקצ'יין הפרטי או הציבורי אינו יכול לתמוך באחסון של יומני ביקורת נרחבים בשל מהירויות חיפוש והכנסה איטיות יותר ועלויות גבוהות יותר**.

4. **גיבוב יומן הביקורת לרשת בלוקצ'יין הפרטית** : ה-ALPM משפר את האבטחה על ידי יצירת גיבוב, ייצוג קריפטוגרפי ייחודי של יומן הביקורת, והעברתו לבלוקצ'יין פרטי באמצעות מודול מחבר רשת הבלוקצ'יין הפרטי (PRVBCM). **גישה זו משפרת את הקביעות והאבטחה של המערכת, מקשה על חבלה ביומנים ומספקת ראיות משפטיות תקפות במידת הצורך.**

5. PRVBCM: **Hyperledger Fabric Interaction** מקיים אינטראקציה עם Hyperledger Fabric, מודול המתחבר לרשתות בלוקצ'יינים פרטיות.

6. **גיבוב יומן הביקורת לרשת בלוקצ'יין הציבורי** : ה-ALPM מוסיף שכבת אבטחה נוספת על ידי גיבוב יומן הביקורת לבלוקצ'יין ציבורי באמצעות מודול מחבר רשת הבלוקצ'יין הציבורי (PUBBCM). תכונת ביזור זו של רשת הבלוקצ'יין הציבורית הופכת את יומני הביקורת לכמעט בלתי אפשריים לחבלה או שינוי, ומספקת סביבה מאובטחת יותר וראיות טובות יותר לכך שהיומנים נשארים שלמים בבלוקצ'יין הפרטי או MongoDB. **חשוב להדגיש את הצורך בשימוש ברשת בלוקציי'ן ציבורית, אני עושה שימוש בבלוקציין ציבורי כדי להעלות את רמת האמינות של המערכת** מכיוון שרשת בלוקציין פרטית נשלטת ע"י הארגון או החברה והם יכולים לשנות נתונים לטובתם, להסתיר או לשנות נתונים, ברגע שאנו מעלים לדוגמא כל 5 יומני ביקורת שנכתבו לרשת הפרטית גם לרשת הציבורית, אז החברה תוכל לשנות נתונים ברשת הפרטית רק לחמשת יומני הביקורת שלא נרשמו עדיין לרשת הציבורית.

7. **אינטראקציה ברשת ביטקוין** : PUBBCM מתממשק לרשת ביטקוין, המייצגת את הבלוקצ'יין הציבורי בהקשר זה.

8. **<u>שלב האימות - בקשת אימות יומן ביקורת</u>** : בעת הצורך לאמת את יומני הביקורת, המשתמש או מערכת אוטומטית (לדוגמה, מערכת קבצים, דרך ממשק הודעות או דרך REST API) שולחים בקשת אימות למודול אימות יומן הביקורת (ALVM).

9. **אחזור נתוני יומן ביקורת מ- MongoDB** : ה- ALVM מאחזר את נתוני יומן הביקורת המאוחסנים ממסד הנתונים MongoDB.

10. **אחזור גיבוב מבלוקצ'יינים פרטיים** - ה-ALVM גם מאחזר את הגיבובים של יומני הביקורת הן מהבלוקצ'יין הפרטי.

11. **אחזור גיבוב מבלוקצ'יינים ציבוריים** : ה-ALVM גם מאחזר את הגיבובים של יומני הביקורת הן מהבלוקצ'יין הציבורי.

12. **תוצאת אימות**: ה-ALVM משווה את נתוני יומן הביקורת שאוחזרו ואת קוד הגיבוב המתאים להם עם קודי הגיבוב המאוחסנים בבלוקציינים. אם מתרחשת התאמה, משמעות הדבר היא שהנתונים לא שונו מיומן הביקורת המקורי, ותוצאות האימות מועברות לצד המבקש (משתמש, מערכת קבצים או באמצעות הודעת REST/הודעות).

13. **<u>בקשה למידע על יומן ביקורת</u>**: אם משתמש או מערכת קבצים צריכים לבדוק מידע הקשור ליומני הביקורת, בקשה זו נשלחת למודול סייר יומן הביקורת (ALEM) באמצעות ממשק המשתמש הגרפי או ממשקי ה- API.

14. **אחזור נתונים מ MongoDB** - ה- ALEM מושך את נתוני המערכת המבוקשים מ- MongoDB

15. **אחזור נתונים מרשת בלוקציי'ן פרטית** – ה- ALEM מושך את נתוני המערכת המבוקשים הרלוונטיים מהבלוקציינים הפרטיים.

16. **אחזור נתונים מרשת בלוקציי'ן ציבורית**: ה- ALEM מושך את נתוני המערכת המבוקשים הרלוונטיים מהבלוקציינים הציבוריים.

17. **הצגת המידע המבוקש**: ה- ALEM מציג לבסוף את המידע המאוחזר למשתמש או למערכת אחרת.

ניתן לראות שהמערכת די מורכבת ומנסה להתגבר על כשלי מערכת ולהעלות את רמת האמינות של המערכת, המערכת מבטיחה את שלמות יומני הביקורת באמצעות יישום טכנולוגיית בלוקציין. בתחילה היא מאחסנת את היומנים ב-MongoDB ושומרת את הגיבובים של היומנים בבלוקציין פרטי וציבורי כאחד. השוואת הגיבוב מאמתת את שלמות היומנים: **התאמה מרמזת על האותנטיות של היומן, ואילו אי-התאמה מרמזת על חבלה. בנוסף המערכת תומכת גם בחקירה והצגה של נתוני יומן ומידע.**

## 5.4. מגבלות המערכת שפתחתי ועבודה עתידית

### 5.4.1. סוגי יומני ביקורת וביצועים:

מכיוון שהמטרה הראשית של המערכת היא לצורך הדגמה של אפשרות לשמירה מאובטחת של יומני ביקורת, **המערכת יכולה לטפל רק בסוגים מסוימים של יומני מערכת ותוכל לעבד אותם בקצב עיבוד נמוך יחסית**. אך ממשק המשתמש ביחד עם צד השרת שבניתי, מאפשרים לעמוד על האתגרים השונים בבניית מערכת כזאת. מכיוון שהמערכת בנויה בצורה מודולרית, היא ניתנת להרחבה וטיפול במקרים נוספים בעתיד יחסית בקלות.

### 5.4.2. שימוש ברשת ביטקוין testNet

המערכת מעוגנת לבלוקצ'יין ציבורי מסוג ביטקוין, **לצורך הפרויקט השתמשתי ברשת testNet** כדי להימנע מעלויות גבוהות של שמירת מידע ברשת הביטקוין הראשית. מכיוון שהמערכת מודולרית שמירה בbitcoin testnet היא זהה לשמירה ברשת ביטקוין הראשית, ולכן בקלות ניתן לשנות את ההגדרה שלה שהשמירה תתבצע ברשת ביטקוין ולכן המעבר לרשת הראשית יהיה עם שינוי קוד מינימלי.

### 5.4.3. יתירות המערכת

במהלך העבודה זיהיתי נקודת כשל אפשרית. אם רשת הביטקוין לא זמינה , **תהיה לנו תקופת זמן שבה לא נוכל לאמת את התנועות**, לכן למערכת שתפעל בפועל יש צורך בשמירת חתימות יומני המערכת למערכת נוספת, מכיוון שהמערכת מודולרית, אחת מהאפשרויות היא להוסיף תמיכה ברשת בלוקצ'יין מסוג **אתריום**, לצורך זאת יש רק צורך להוסיף את המימוש של אתריום למודול PubBCM .

### 5.4.4. התמודדות עם ייצור יומני מערכת חדשים זדוניים

בכדי לתת מענה גם למניעת יצירה של יומני מערכת חדשים שנוצרו בכדי לסתור ראיות, במאמר [1] עלתה אפשרות להסתמך על אמצעים משפטיים כדי לשלול את האפשרות של ייצור יומני מערכת ע"י הארגון, זה נותן מענה ברמה מסוימת. לדעתי בנוסף לזה, **בעתיד** הייתי מוסיף **למערכת יכולת של זיהוי אנומליות של יצירת יומני מערכת חדשים**, לדוגמא ניתן להשתמש בלמידת מכונה שתזהה תבנית ובמידה ויש חריגה היא תתריע עליה ובכדי למנוע מהארגון להתעלם ממנה, נשמור את ההתרעות ברשת ביטקוין הציבורית, כך שנעלה את רמת אמינות המערכת.

### 5.4.5. התקנה על ענן ציבורי

עקב עלויות של התקנת המערכת בענן הציבורי, במסגרת הנוכחית הפרויקט הותקן בסביבה מקומית, אבל מכיוון שהמערכת מודולרית ומבוססת קונטיינרים ניתן להתקינה בקלות יחסית בענן ציבורי לפי בחירה.

### 5.4.6. עמידות להתקפת ע"י מחשב קוונטי

יש לציין שחלק מהמערכת של הפרויקט כגון שימוש במפתח ציבורי להצפנה, לא בעל עמידות גבוהה כנגד התקפה ע"י מחשב בעל כוח קוונטי [23]. לצורך העלאת עמידות המערכת להתקפה ע"י מחשב קוונטי, יש צורך להשתמש בפרוטוקולי הצפנה עמידים להתקפה כזאת, כגון הצפנה מבוססת פונקציות גיבוב, הצפנה מבוססת פולינומים מרובים משתנים [24] ושיטות אחרות.

# 6. סיכום ומחקרים עתידיים

## 6.1. סיכום גישות המאמרים העיקריים

שלוש הגישות המוצגות במאמרים 1,3,5 משתמשות כולן בטכנולוגיית בלוקצ׳יין כדי לשפר את השלמות והאבטחה של מערכות ביקורת יומנים.

**הגישה הראשונה** [1] מציעה תשתית לביקורת יומנים באמצעות בלוקצ׳יין מורשה לאחסון הוכחות שלמות. הוא נועד לעמוד בדרישות החוק לראיות קבילות ומציע חלופה מקומית לפתרונות של צד שלישי. ניתוח האבטחה של גישה זו מראה כי היא מסוגלת לעמוד בניסיונות ליירט, להפריע או לשנות את נתוני היומן המעובדים שלה, אם כי לא ניתן לשלול לחלוטין ייצור באמצעים טכניים. אמות מידה של ביצועים מראות כי יישום הבלוקצ׳יין מסוגל להתמודד עם קצב עיבוד גבוה של אירועי יומן, אך דרישות האחסון הן משמעותיות בשל שכפול מלא ושמירה של כל הנתונים ההיסטוריים. במחקר עתידי, אב טיפוס משופר יוכל ליישם סיבוב יומן כדי להפחית את עלויות האחסון.

**הגישה השנייה** [3] מציגה מערכת יומן ביקורת מבוססת בלוקצ׳יין בשם BlockAudit, המשתמשת בתכונות האבטחה של טכנולוגיית הבלוקצ׳יין כדי ליצור יומני ביקורת בגישת הוספה בלבד בכדי לספק הגנה מפני חבלה ושינוי מידע. הוא מדגיש את פגיעויות האבטחה ביישומי יומן ביקורת קיימים ומציע עיצוב חדש המרחיב את ORM ליצירת יומני ביקורת תואמי בלוקצ׳יין. המערכת מתוכננת להיות מהירה, מאפשרת שיטת הכנס-הפעל ומאובטחת מפני התקפות פנימיות וחיצוניות. בעתיד, המחברים מתכננים להרחיב את היכולות של BlockAudit על ידי פריסתו בסביבת ייצור וחקירת צווארי בקבוק ואופטימיזציה שונים של ביצועים.

**הגישה השלישית** [5] משתמשת בטכנולוגיית בלוקצ׳יין כדי לשמור על שלמות קבצי יומן על ידי שילוב IPFS עם טכנולוגיית בלוקצ׳יין אתריום כדי להמיר מערכות אחסון מרכזיות למערכות אחסון מבוזרות. המערכת המוצעת מסוגלת לאחסן מספר רב של קבצי יומן עם עלויות עסקה מינימליות וערך גז, והיא מאובטחת, ניתנת להרחבה ומבטיחה ביצועים גבוהים. עם זאת, המערכת הנוכחית תלויה ב- CSPs כדי לאסוף קבצי יומן, ובעתיד המחברים מציעים כי ניתן להגדיל את האמון ב- CSPs על ידי הפחתת התלות בהם.

## 6.2 סיכום

בעבודה זו, ראינו שאחת הדרכים להבטיח את האותנטיות של ראיות דיגיטליות היא שמירה על שרשרת מתמשכת של משמורת. משמעות הדבר היא שיש ליצור, להעביר ולאחסן את הראיות באופן שניתן לאמת ולהסתמך עליו. זה חשוב במיוחד במקרה של נתוני יומן, אשר יכול לספק מידע רב ערך על אירועים שהתרחשו על מערכות המידע של הארגון. **על מנת שנתוני יומן אלה ייחשבו קבילים בבית המשפט, על הארגון להיות מסוגל לספק הוכחה לכך שהם נוצרו, הועברו ואוחסנו באופן אמין וניתן לאימות.**

בעבודה זו סיפקתי סקירה מפורטת של המצב הנוכחי של אבטחת מערכות מידע והטכנולוגיות השונות המשמשות להגנה על נתונים ומערכות מפני גישה לא מורשית או התקפות זדוניות. הדגשתי את חשיבות יומני הביקורת במערכות המידע והצורך המתמשך בניטור רציף, כאשר מאמר [1] מדגיש את החשיבות של שרשרת משמורת מתמשכת כדי להבטיח את שלמות הנתונים. בנוסף, בעבודה זו  דנתי בחשיבות מחשוב הענן ובסיכוני האבטחה הפוטנציאליים הכרוכים בו. פתרונות כגון פתרונות מבוססי סוכן ומבוססי יומן הוצעו כדי להפחית סיכונים אלה.

בין היתר, בעבודה זו סיפקתי סקירה של טכנולוגיית ההצפנה וטכנולוגיית הבלוקצ'יין. הוסברה עבודתה של טכנולוגיית ההצפנה וחשיבותה בשמירה על אבטחת המפתחות הציבוריים והפרטיים. כמו כן נדונו אבני הבניין הבסיסיות של טכנולוגיית הבלוקצ'יין, ובפרט עסקאות, וכיצד הן פועלות ברשת בלוקצ'יין.

בנוסף, סקרתי בעבודה זו את נושא זיהוי פלילי דיגיטלי וזיהוי פשעים דיגיטליים, במיוחד בסביבת הענן. הסוגים השונים של שיטות זיהוי פורנזיות דיגיטליות, כגון פתרונות מבוססי סוכן ומבוססי יומן. בעבודה זו הראיתי את חשיבות הערך של מחשוב ענן במערכות מידע מודרניות. מחשוב ענן מספק מספר יתרונות כגון מדרגיות, אבטחה, אמינות וחיסכון בעלויות. עם השימוש במחשוב ענן, ארגונים יכולים בקלות להגדיל או להקטין את משאבי המחשוב שלהם לפי הצורך, ללא צורך בהשקעות יקרות בתשתית. לספקי ענן יש בדרך כלל מרכזי נתונים בקנה מידה גדול עם שכבות אבטחה מרובות, מה שמבטיח שהנתונים מוגנים מפני גישה לא מורשית והתקפות זדוניות. זה גם מאפשר לארגונים להתמקד בפעילויות הליבה העסקיות שלהם, במקום לדאוג לאבטחה ולתחזוקה של תשתית ה IT-שלהם. בנוסף, מחשוב ענן מספק גישה אמינה לנתונים וליישומים, גם במהלך עליות חדות בלתי צפויות בתעבורה או שיבושים אחרים.

בנוסף, מחשוב ענן יכול גם להפחית את העלויות הכרוכות בחומרה, תוכנה ותחזוקה. כמו כן, מחשוב ענן מאפשר לארגונים לשלם רק עבור המשאבים הדרושים להם, במקום להשקיע בחומרה ותוכנה יקרות מראש. זה מספק לארגונים את הגמישות להרחיב או לצמצם את משאבי המחשוב שלהם כאשר הצרכים העסקיים שלהם משתנים. באופן כללי, מחשוב ענן הוא חשוב עבור מערכות מידע מודרניות ומציע יתרונות רבים, כולל מדרגיות, אבטחה, אמינות וחיסכון בעלויות, וע״י זה אנו יכולים לבנות מערכת לשמירת יומני ביקורת בדרך חסכונית ואמינה.

בעבודה דנתי בחשיבותם של מנגנוני קונצנזוס בטכנולוגיית הבלוקצ׳יין, במיוחד בהתמודדות עם בעיית ההוצאות הכפולות והבטחת סובלנות התקלות של מערכות מבוזרות.
**ועמדתי על טכנולוגיית בלוקצ׳יין שונות המאפשרות לבנות מערכת לשמירת יומני ביקורת בצורה טובה יותר מאשר פתרונות חומרה או תוכנה לא מבוזרים אשר נותנות מענה לאתגרי הזיהוי הפלילי הדיגיטלי.**

## 7. רשימת מקורות


1. Putz, B., Menges, F., & Pernul, G. (2019). A secure and auditable logging infrastructure based on a permissioned blockchain. Computers & Security, 87, 101602.
2. Ahmad, A. (2019). Blockchain-Driven Secure and Transparent Audit Logs. Electronic Theses and Dissertations, 2004-2019. 6778 - https://stars.library.ucf.edu/etd/6778
3. Ahmad, A., et al. (2018). Towards blockchain-driven, secure and transparent audit logs. Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services.
4. Kumar, M., Singh, A. K., & Suresh Kumar, T. V. (2018). Secure log storage using blockchain and cloud infrastructure. 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE.
5. Jain, P. (2020). Decentralize Log File Storage and Integrity Preservation using Blockchain. International Journal of Computer Science and Information Technologies, 11(2), 21-30.
6. Anderson, J. (2018). Securing, standardizing, and simplifying electronic health record audit logs through permissioned blockchain technology. Dartmouth College Undergraduate Theses. 135. https://digitalcommons.dartmouth.edu/senior_theses/135
7. Sutton, A., & Samavi, R. (2017). Blockchain enabled privacy audit logs. International Semantic Web Conference. Springer, Cham.
8. Sharma, S. G., Ahuja, L., & Goyal, D. P. (2018). Building secure infrastructure for cloud computing using blockchain. 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS). IEEE.
9. Nakamoto, S. (2009). Bitcoin: a peer-to-peer electronic cash system.
10. Bitcoin.org. (n.d.). [Online]. Available: http://www.bitcoin.org/bitcoin.pdf
11. Nguyen, H.-L., et al. (2018). Blockchain-Based Auditing of Transparent Log Servers. IFIP Annual Conference on Data and Applications Security and Privacy. Springer, Cham.
12. Zhou, X., et al. (2019). Towards blockchain-based auditing of data exchanges. International Conference on Smart Blockchain. Springer, Cham.
13. Li, S., et al. (2020). A blockchain-based public auditing scheme for cloud storage environment without trusted auditors. Wireless Communications and Mobile Computing, 2020.
14. Sahlin, E., & Levenby, R. (2018). Blockchain in audit trails: An investigation of how blockchain can help auditors to implement audit trails.
15. Buterin, V. (2015, August 7). Ethereum - On Public and Public Blockchains. Ethereum.org.

16. Desai, H., Kantarcioglu, M., & Kagal, L. (2019). A Hybrid Blockchain Architecture for Privacy-Enabled and Accountable Auctions. 2019 IEEE International Conference on Blockchain (Blockchain).
17. Schneier, B., & Kelsey, J. (1999). Secure audit logs to support computer forensics. ACM Transactions on Information and System Security, 2(2), 159-176.
18. Buterin, V. (2017). A Next-Generation Smart Contract and Decentralized Application Platform. https://ethereum.org/en/whitepaper/
19. Merkle, R. C. (1988). A Digital Signature Based on a Conventional Encryption Function. Advances in Cryptology — CRYPTO '87. Lecture Notes in Computer Science, 293, 369-378. https://doi.org/10.1007%2F3-540-48184-2_32
20. Brown, D., & Mandalia, H. (2017). Corda An Introduction.
21. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Vukolic, M. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains.
22. Enterprise Ethereum Alliance. (2017). Enterprise Ethereum Alliance Permissioned Blockchains Specification V3.
23. Fernández-Caramés, T. M., & Fraga-Lamas, P. (2020). Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. IEEE Access, 8, 21091-21116.
24. Buhrman, H., Cleve, R., Watrous, J., & de Wolf, R. (2010). Quantum lower bounds by polynomial degrees. Journal of the ACM (JACM), 48(4), 778-797.
25. Grover, L. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, 212-219.

# Abstract

In this work we will review the importance of audit logs in information systems, we will explain what a blockchain network is, and the types of blockchain networks such as private, public and federal networks.

A detailed explanation is given on how to save and retrieve information of the audit logs in the blockchain network, we will go through an explanation of solutions that make use of the blockchain network, as presented in the following articles: General information about Bitcoin [9], we will review in detail the articles on the topic of audit logs on Blockchain network [1], [3] and [4], we will briefly review the articles regarding the use of cloud technology for blockchain networks [8] and [2] and in addition other articles that will give us another look.

In this work we will see an innovative way to deal with the immutability of audit logs which is one of the tools in the field of digital forensics, a field for finding legal evidence in the digital world. In order to trace digital traces, it is necessary to read system logs and other sources of information in order to perform a digital identification that can also be used for forensic evidence, one of the challenging problems is: how organizations can comply with internal and/or government regulations, regulations, legal civil contracts if and when they are required to perform prove evidence that is also valid in the courts for the purpose of suing an attacker or user who maliciously infiltrated/sabotaged the system or for the purpose of investigating malfunctions that were not done maliciously.

One of the innovative ways is by building a system as a blockchain-based cloud service that provides a system for saving and analyzing audit logs in a secure and immutable way.
The applied part of the work includes the development of a secure audit log system as a blockchain-based cloud service, which was done as part of the final project, the system will include several components, a component that receives the information into the system and transfers the audit data through a verification, signing and saving process in the blockchain network. The system will use cloud infrastructures and blockchain networks for accessibility, security, dynamic growth capabilities according to the required information. The system will allow authorized users the ability to retrieve and retrieve audit logs required for an information security audit or a request by company managers or government organizations for investigation or prosecution purposes.

**The Open University of Israel**

**Department of Mathematics and Computer Science**


# Secured Audit Logs as a Service - Blockchain & Cloud (SALaaS)

Thesis (Final Paper) submitted as fulfillment of the requirements

towards an M.Sc. degree in Computer Science

The Open University of Israel

Department of Mathematics and Computer Science

By

**Nir Makmal**

Prepared under the supervision of Prof. Ehud Gudes

October 2023