

# MULTIVERSUM

HERE TO STAY

**WHITE PAPER v 1.0.6**

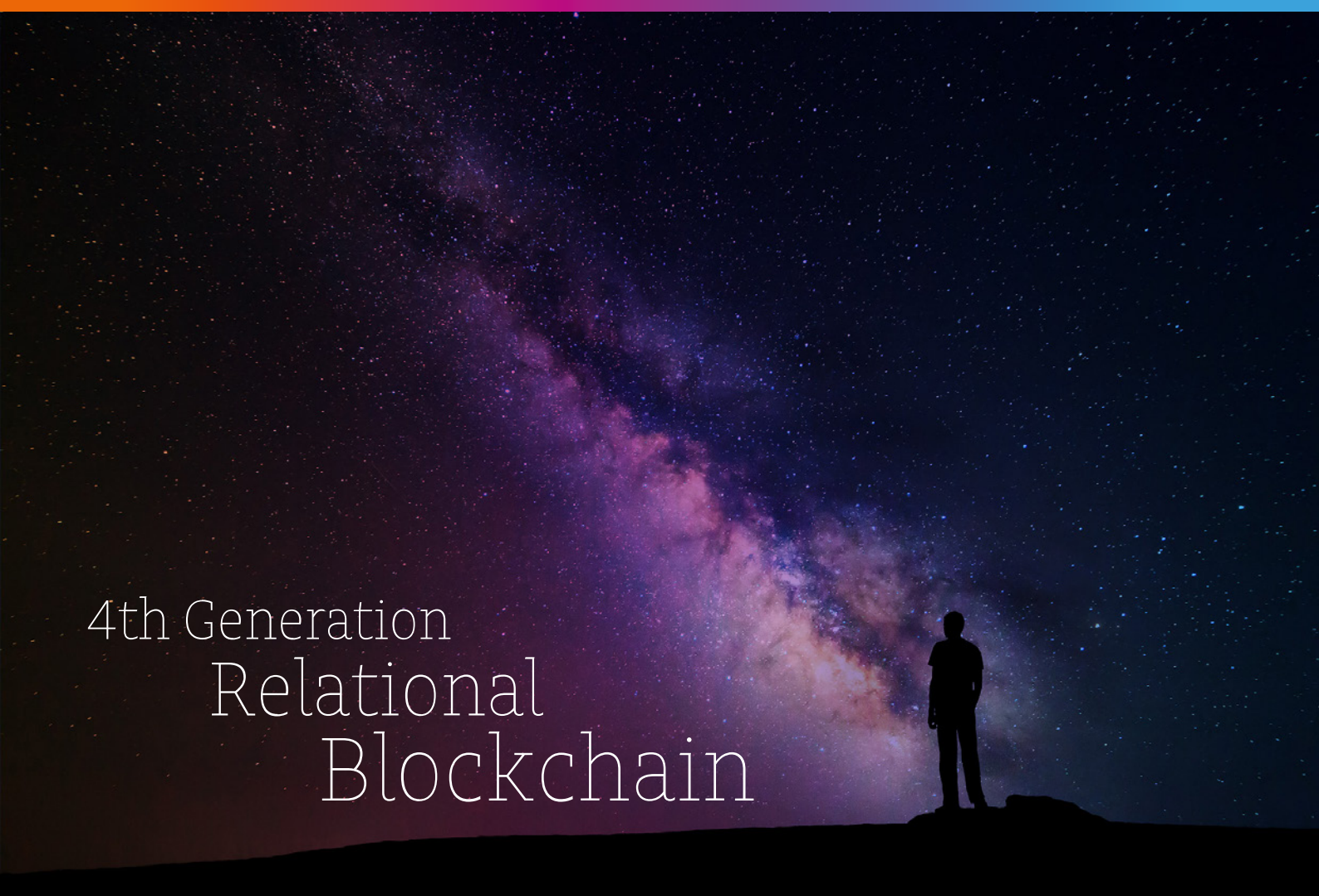
Business | Technical

Hebrew

19.02.2018

Authors: Multiversum Team

[www.multiversum.io](http://www.multiversum.io)



4th Generation  
Relational  
Blockchain

# Multiversum

## זהות ומשימה

ביטקוין, חלוץ המטבעות הקריפטוגרפיים, וכן כל שיבוטיו והתפצלויותיו נחשבים לשרשאות בלוקים מהדור הראשון, והם מבוססים על אלגוריתם הוכחת עבודה בשביל אימות תנועות.

שרשאות בלוקים מהדור השני כאשר Ethereum הובילו את המערכה מבוססות על חוזים חכמים, והן יותר הטרוגניות ומקלות על המרת נכסים לטוקנים.

לשני המודלים הנ"ל יש יעילות אנרגטית נמוכה, הם איטיים למדי בתיקוף בלוקים ומספר תנועות פר בלוק.

המטרה של שרשאות בלוקים מהדור השלישי היא לספק פתרון לסקלביליות, מהירות וצריכת האנרגיה, בעזרת גישות שונות כגון אלגוריתם הוכחת החזקה, ניתוב חוץ שרשרת, גרף שרשאות, ומרכז מוחלט או חלקי.

הדור הרביעי מתקדם אף יותר ומשיג פתרונות סקלביליים ומהירים יותר, ובו בעת מנסה להיות תחרותי מבחינה עסקית שכן שרשאות מידע פשוטות אינן מספיק גמישות כדי לענות לצרכים של סביבה תאגידית, בהן מבני מידע מורכבים צריכים להיות מאורגנים בטבלאות (בדומה לבסיסי נתונים יחסיים).

בו בעת, מבנים אלו צריכים לעבור תיקוף ולהיות בלתי ניתנים לשינוי על ידי טכניקות המבוססות על שרשאות בלוקים, כדי לחזק את יכולת המעקב והאבטחה.

במילים אחרות, הדור הרביעי מנתב את הטכנולוגיה לשימוש יצרני ומרחיב את ההצע למגזר העסקי מבחינת אחסון מידע, ביזור, בקרה, אבטחה ואמינות

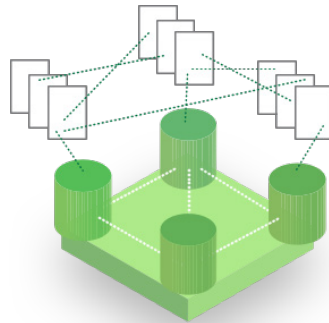
Multiversum מציעה ארגון מידע מורכב במקום ריצוף מידע, פיצול והרכבה מחדש של שרשאות כדי לשפר את הסקלביליות והמקביליות, ו Proof of Integrity (הוכחה קריפטוגרפית של קוד השרת) במקום הוכחת עבודה (Proof of Work) או הוכחת החזקה (Proof of Stake).

זאת ועוד, Multiversum תכלול אינטגרציות ERC20/ERC23, שתאפשר למטבעות וטוקנים ממערכות שונות להיקלט בשרשאות שלנו ולהיפך, באמצעות שירותים נוטריונים לאשרור חוץ מערכת. לצד חידושים אלו, אנו בהחלט נעשה שימוש בפתרונות יעילים שכבר הוטמעו על ידי עמיתינו לתחום.

## Multiversum

### הדור הרביעי של שרשרת הבלוקים היחסית

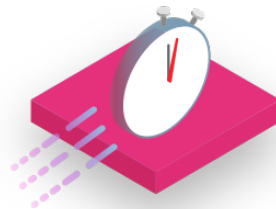
מדוע Multiversum הינה שרשרת בלוקים 4.0?



### שרשראות בלוקים יחסיות

מבנה חדיש של שרשראות בלוקים  
אשר מכיל סוגים שונים של נתונים במבנה רב מימדי

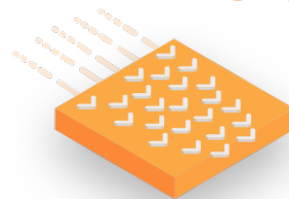
< 0,2 sec



### מהירות תנועות

בתוך פחות מ-0.2 שניות,  
כסף מועבר בין ארנקים, כולל אימות מאובטח של התנועה. מהמהירים בעולם

64000 tps → ∞



### הספק תנועות

סקלביליות מהמעלה הראשונה- עד 64,000 תנועות בשניה (1000 תנועות פר ליבה) על שרת 64 ליבות

POI



## Proof of Integrity

הוכחת החזקה (Proof of Stake) תוחלף ב- Proof of Integrity



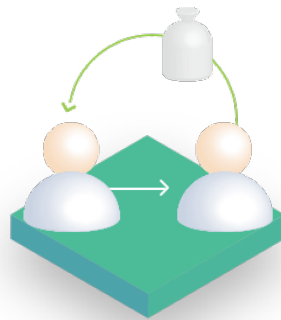
## הדור הבא של הארנק הדיגיטלי

אבטחה חדשנית העושה שימוש בקלט ביומטרי למתן הרשאות ולהעברות כספיות



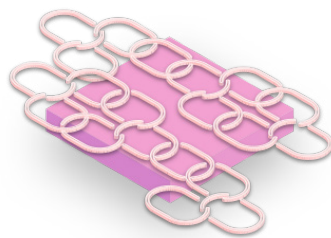
## ידידותי לסביבה

לתנועות Multiversum תהיה עלות זניחה והשפעה סביבתית השואפת לאפס



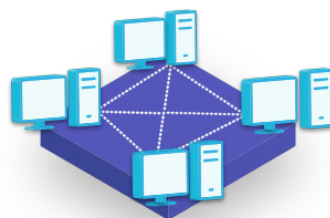
## Rollback

אפשרות לבצע Rollback על טוקנים בפלטפורמת Multiversum



## שרשראות הניתנות לחילוק

אופטימיזציה של משאבים בין הצמתים בשל האפשרות לניתוק השרשרת



## הקצאת צמתי שחזור

צמתי Multiversum יפוזרו בכל העולם ליצירת אמינות ושחזור במקרה של אסון גלובלי

# מצגת ציבורית

## שרשראות בלוקים חדשניות

התכונה המרכזית המשותפת לשרשראות בלוקים היא האבטחה והאמינות יוצאות הדופן שלהן. בו בעת, אנו משלמים מחיר כבד בדמות מעבדים עצומים, זיהום בלתי מתקבל על הדעת, עלות תנועות גבוהה ואיטיות שאינה עולה בקנה אחד עם הסטנדרטים של הקדמה הטכנולוגית העכשווית, ואינה עונה על הצרכים הפיננסיים והציבוריים.

איטיות זו נגרמת על ידי חוסר ב Horizontal scalability<sup>1</sup> (סקלביליות אופקית), כלומר הגדלת יכולת העיבוד על ידי הוספת מעבדים במקום החלפתם בגרסאות מהירות יותר. סיבה נוספת לאיטיות נעוצה בצורת האבטחה שנמצאת כרגע בשימוש בשרשראות בלוקים, שמתוכננת להפוך השתלטות על עיקר ה clusters (מקבצים) על ידי כל אדם ליקרה מדי במונחים של כוח עיבוד ו/או עלות (Proof of Work<sup>2</sup> -

הוכחת עבודה ו Proof of Stake<sup>3</sup> הוכחת החזקה)

זאת ועוד, שרשראות בלוקים עכשוויות הן השתלטות פשוטה של מצבי שינוי בישות נתונים יחידה: הרכבה מחדש של ישויות אלו מצריכה סריקה של כל השרשרת, שגורמת בתורה להאטה נוספת של המערכת וצריכת משאבים מוגברת.

בשל פישוט זה, שרשראות בלוקים אינן מספקות לשימושים מדעיים ותעשייתיים, שמצריכים מבני מידע מורכבים ביותר.

בנוסף, אמצעי האבטחה פועלים רק על הנתונים ואינם מכסים את אבטחת המשתמש, ולכן בלתי אפשרי לשחזר מטבעות וטוקנים שאבדו או נגנבו, גם אם הם נמצאים על השרשרת, או לחסום חשבונות זדוניים. לבסוף, בעיה נוספת היא הפרגמנטציה וחוסר ההומוגניות בין מטבעות קריפטוגרפים, שאינם מסוגלים לתקשר ביניהם ומתקיימים בפלטפורמות נפרדות.

# Multiversum ואימוץ שרשראות בלוקים גלובליות

הטכנולוגיה של Multiversum דוחפת שרשראות בלוקים קלאסיות מעבר למגבלותיהן, על ידי שיפור שכבת הנתונים דרך אימות עצמי ומבנים מופצים של ישויות נתונים מאורגנים, המקושרות זו לזו על ידי קישורים סמליים.

טכנולוגיה זו מניחה את היסודות למערכת מבוצרת ומפוזרת של תנועות בעלות אימות עצמי קוהרנטי: שרשראות הבלוקים של Multiversum

במקום שרשראות בלוקים במודל הקיים של נתונים מופשטים, Multiversum מאפשרת יצירה של Relational Crypto Database (פתרון מתקדם ומאורגן לאחסון נתונים) שיכול להתמודד לא רק עם סוג אחד של נתונים, אלא עם רצף של נתונים המקובץ בגרפים של מבני נתונים מורכבים הקשורים זה בזה. קשרים הם כעת אזרחים מהמעלה הראשונה של שרשרת הבלוקים והם מאובטחים בשיטות קריפטוגרפיות.

במידה ויש צורך בשינוי מצב, לכל אחת ואחת משרשראות הבלוקים תהיה תת שרשרת שתתפצל מממנה, ותחבור מחדש לפעולה כדי לעבור אימות.

משום כך, Multiversum הינה טכנולוגית שרשרת בלוקים מתפתחת, המציעה תכונות ייחודיות להתגברות על מכשולים קודמים, בעזרת סט של טכניקות אימות קריפטוגרפי והפצה המותאמות לכל סביבת עבודה: אדמיניסטרטיבית, תעשייתית, פיננסית וממשלתית.

אחת מהמטרות העיקריות של Multiversum היא להציע לשוק, בכל רגע נתון, את המוצר המתקדם ביותר בנמצא שיתאפשר על ידי אימוץ שיטות AGILE<sup>4</sup> לפיתוח יישומים.

שיטת AGILE מבשרת הפחתה דרסטית של מעורבות ראשונית בעיצוב פרויקט, לטובת גיוון החוויות איתן ניפגש במהלך פיתוח הפרוייקט, שמציגות הזדמנויות וסיכונים שאינם ניתנים לצפיה מראש ובכך מקדמת את השיטות הטובות ביותר וזונחת את אלו שאינן עונות על הצרכים.

AGILE היא תוכנה מבוססת לסטנדרט פיתוחי ומעודדת מפתחים, בעלי מוצרים ומשקיעים לשקול project scopes שיאפשר גמישות ואדפטציה מהירה לצרכי השוק.

זאת ועוד, בסקטור תכנות המתקדם בקצב גבוה שכזה, שחרור מוצר לאחר שישה חודשים של מחקר ושנה של הטמעה, כאשר הוא מתוכנן לתאום לצרכים של השוק מלפני 18 חודשים, משמעותו לספק מוצר לא רלוונטי הנותן מענה לבעיות ישנות שיכול להיות שהמתחרים כבר פתרו ואינו מסוגל להתמודד עם אתגרים שאך זה נוצרו.

ל AGILE, לעומת זאת, יש את האפשרות לספק לשוק את המוצרים החדשניים ביותר בזמן אמת.

## מהירות וטכנולוגיה

אחד מהחוזקות של הטכנולוגיה, היא אכן מהירותה, תודות ליכולת להריץ תנועות שונות במקביל ומכניזם פיצול/הרכבה של שרשראות הבלוקים שלנו. תכונות אלו מאפשרות סקלביליות אופקית גדולה יותר,

ומגדילות את יכולת עיבוד התנועות תוך הוספת כוח מחשוב ליכולות הקיימות, על ידי ניצול יכולת הביצוע של כל צומת וצומת במלואה.

## סקלביליות אפקית

Multiversum נהנית משתי תכונות ספציפיות שמקנות למערכת יעילות מקסימלית:

1. השרשרת המרכזית מסוגלת לבצע אופטימיזציה של מבניה על ידי פיצול עצמוני למספר תת שרשראות, לפי צורך במשאבים ותזרים נתונים ובכך ממקבלת את העבודה על פני מספר נתיבים וצמתים. תהליך פיצול השרשרת מבוצע עד לנירמול עומסי העבודה, כאשר שוב בהליך עצמוני השרשרת תורכב מחדש. תהליך זה מאפשר בזכות טכניקה שמאפשרת לכל בלוק בשרשרת לאמת שתי תת שרשראות שונות משני לינקים נכנסים שונים.
2. Data Sharding טכניקה המאפשרת פיצול מידע בין מספר צמתים. במצב של שרשרת ABC ושלוש מקבצי (clusters) צמתים, נקבל את פיצול המידע הבא:

AB

BC

CA

תת חלוקה זו מאפשר מהירות עיבוד גבוהה יותר של תנועות, משום ששאלות ישפיעו רק על צמתים של תת שרשראות ובכך תיעל כל שלב.

תכונה נוספת חשובה ביותר של הטכנולוגיה שלנו היא High Availability האפשרות להיסתמך על סוג מקבץ שמבטיח המשכיות של סיפוק שירותים במקרה של קריסה של חלק מהצמתים במערכת.

לפי הדוגמה לעיל (צמתים A, B, C), במקרה וצומת C קורס, צמתים A ו B ימשיכו לפעול באופן תקין לחלוטין, ובכך יאפשרו המשך מתן השירות ללא איבוד מידע כלשהוא, כל עוד לפחות 50%+1 מהצמתים עודם פועלים. כך, במקרה של קריסת מספר צמתים, המקבץ באופן עצמוני מארגן מחדש את חלוקת המידע המקושר לכל צומת עד לשחזור תפעול מלא.

## סביבה

Multiversum גם ידידותית לסביבה: אחת ממטרותינו המרכזיות היא להפחית בכוח מחשוב הנחוץ לאימות קריפטוגרפי ובכך למנוע mining (הוכחת עבודה), המהווה בזבוז עצום של כוח מחשוב ומשאבים.

במקום הטכנולוגיה המיושנת הזאת, אנו נטמיע Proof of Integrity, פרוטוקול שמבצע אימות קריפטוגרפי על ידי בדיקת אותנטיות של התוכנה הפותרת את כל ההתמדות (persistence) בתנועה.



## ניהול נתונים

ה Relational Crypto Database של Multiversum מאפשר להרכיב את בסיס הנתונים בקלות וללא מגבלות של קישור נתונים. לכל ארנק דיגיטלי יהיה סדרת מצבים והוא יהיה מקושר לאדם (משתמש), וכל מצב חדש של ארנק דיגיטלי יכיל שתי שדות נתונים: המצב הקודם, כדי לבדוק אימות קישור לתנועה האחרונה (או קישור לחולית השרשרת המרכזית האחרונה) כך שמקור הקישור למצב החדש יהיה ידוע. לאחר מכן, השינוי בתנועה יתווסף והקישור למצב החדש יתחבר מחדש לשרשרת המקורית. על כן, לתנועה החדשה יתווספו שני hashes: אחד מקישור המצב ואחד מהתנועה הקודמת. כך, כל הפעולות יאמתו את אלו שקדמו להן, הקשורות בתנועה עצמה. פתרון מתקדם זה, מסוגל לנהל תרחישי נתונים מורכבים, יאפשר למשתמשים להטמיע כל יישום שהוא על גבי הטכנולוגיה שלנו, יבטיח מיזוג מוסדי, ממשלתי, פיננסי ותעשייתי כלל עולמי ובכך יביא את עולם שרשראות הבלוקים צעד אחד קדימה.

# MULTIVERSUM

HERE TO STAY

## Unique Features !

### **Crypto relational DB**

Autovalidating Complex  
Data structures

### **Proof of Integrity**

(Protocol Innovation)

### **Divisible/Re-joinable chains**

(Parallel Work)

### **Biometric Data integration as Electronic Signature seed**

(User Security)

### **Sharding data**

(Parallel Work)

### **Double Access Lock**

(Structural Security)

### **Minimal ecological footprint**

### **Reverse Access Denial**

(Structural Security)

### **Reciprocal chain confirmation**

(Interoperability with other BC)

### **Rollback**

(User Security)

### **Advanced API offer**

### **Native off-chain adapter for own ERC20**

(Interoperability with other BC)

### **Self managing Crypto-Cluster**

### **Java, Spring and Javascript**

(Libraries for Integration)

### **Native on chain adapter for own ERC20**

(Interoperability with other BC)

### **Freezable wallets**

(User Security)

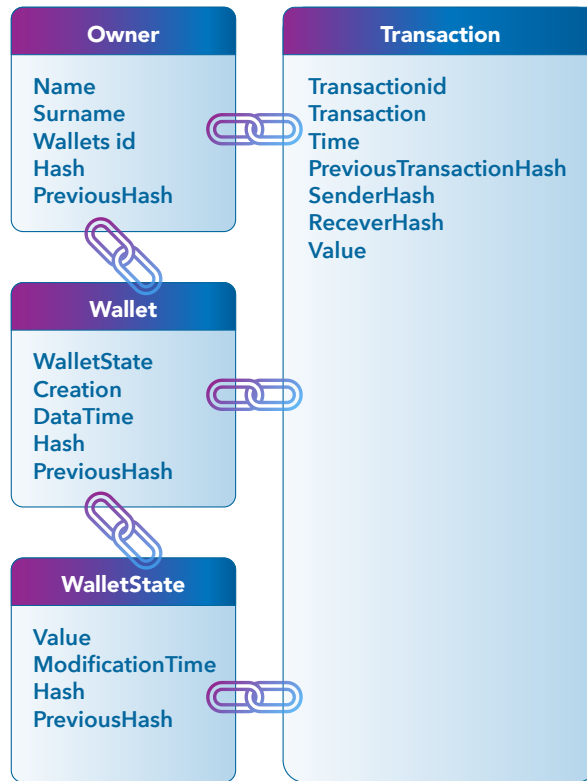
### **ERC23**

(Interoperability with other BC)

## המשימה של Multiversum

Multiversum מבקשת לקדם את עולם שרשראות הבלוק לדור הבא, ולשם כך אנו מציעים את המטרות הבאות:

1. יצירת Crypto Relational DB עם מבני נתונים מורכבים בעלי יכולת אימות עצמי.
2. שרשראות ניתנות לפיצול/ חיבור מחדש בהתבסס על עומסי עבודה נתונים (פעולות ממוקבלות)
3. Data Sharding (פעולות ממוקבלות)
4. API (ממשק תכנות יישומים) מתקדם
5. Rollback (אבטחת המשתמש)
6. Freezable Wallets (אבטחת משתמש)
7. אינטגרציה של נתונים ביומטרים כבסיס לחתימה אלקטרונית
8. ממשק ERC23 (יכולת פעולה הדדית עם שרשראות בלוקים אחרות)
9. Native off-chain adaptors בשביל ERC20/ERC23 פנימיים (יכולת פעולה הדדית עם שרשראות בלוקים אחרות)
10. Native off-chain adaptors בשביל ERC20/ERC23 חיצוניים (יכולת פעולה הדדית עם שרשראות בלוקים אחרות)
11. Proof of Integrity (פרוטוקול חדשני)
12. Double Access Lock (אבטחת המבנה)
13. Reverse Access Denial (אבטחת המבנה)
14. Reciprocal Chain Confirmation (יכולת פעולה הדדית עם שרשראות בלוקים אחרות)
15. אינטגרציה ל Javascript | Java, Spring
16. מודל ACID
17. מודל תנועות
18. שפה תואמת ל SQL
19. Full Route Data Flux



**1. יצירת Crypto Relational DB עם מבני נתונים מורכבים בעלי יכולת אימות עצמי.**

Multiversum מיועדת בעיקר לשימוש תעשייתי וממסדי, אשר משתמשים בנתונים בעלי מבנים מורכבים שאינם יכולים להיות מוצגים בצורה יעילה ומנומלתת בשרשרת פשוטה. אנחנו שמים לנו למטרה להפוך ל crypto relational DB הראשון בשוק, מבוזר או מופץ לפי הצורך.

יכולת זאת מגיעה מ chainable entities conceptualization: בטכנולוגיה שלנו שרשרת מרכזית יכולה להתפצל לשרשראות משניות, המכילות סטים שונים של ישויות ורישומים הישויות יתחברו מחדש במצב ההתמדה (persistence) האחרון, ולאחר השינוי יתחברו מחדש לחוליה האחרונה של השרשרת המרכזית, ובכך יהפכו לשלם שוב. ממשק שרשרתי זה יוצר רישום המכיל שני hashes ויותר של הרישומים הקודמים, ובכך מאמת לא אחת אלא תת שרשראות רבות.

בהטמעה הסטנדרטית של Multiversum, שמשומשת על ידי Versum coins, הישויות בעלות יכולת השרשור המתקיימות במקביל על השרשרת ישתייכו לארבע טבלאות: משתמש, ארנק, מצב ארנק, תנועה, המאשררות את עצמן באופן הדדי.

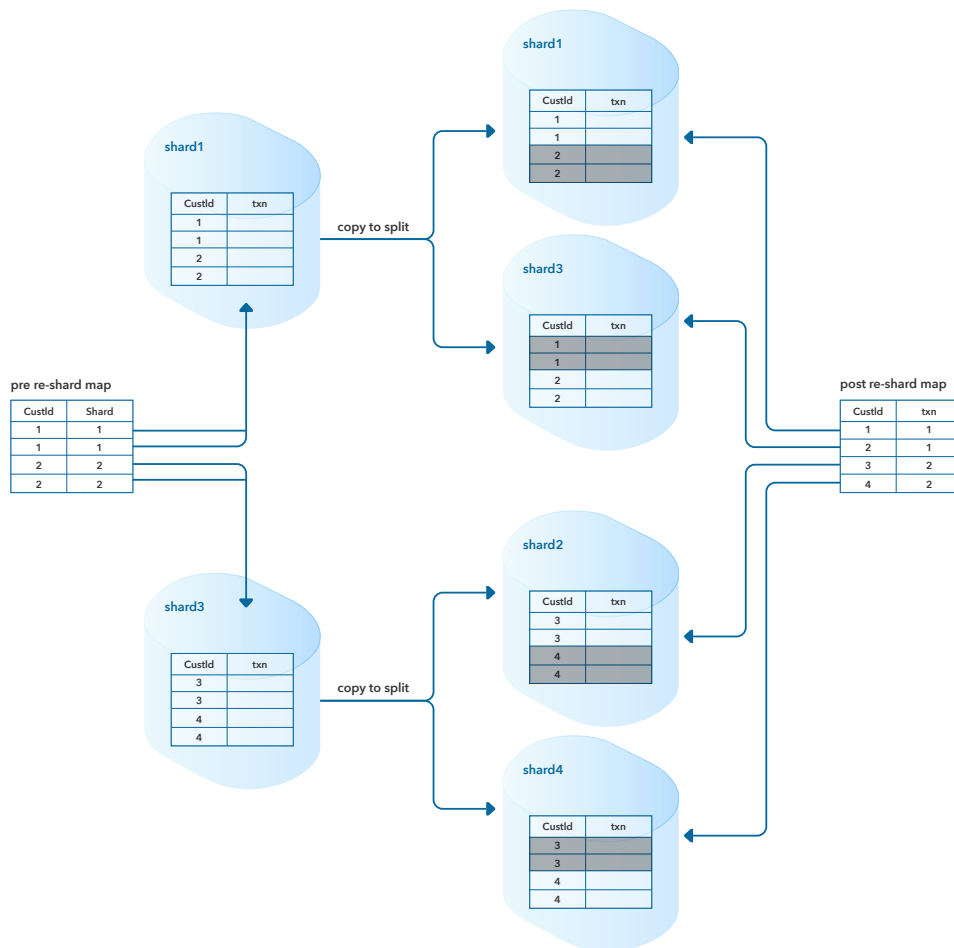
**2. שרשראות ניתנות לפיצול/ חיבור מחדש בהתבסס על עומסי עבודה נתונים (פעולות ממוקבלות)**

אותה היכולת המאפשרת פיצול שרשרת נתונה למספר שרשראות וחיבורן מחדש, מאפשרת לטכנולוגיה זו להשתמש ב workload analyzers שיאותתו למקבץ על הצורך לפצל את השרשרת המרכזית לשתי שרשראות משניות (ולפי הצורך גם את שתי השרשראות האלו שוב ושוב) כאשר יש ביקוש גבוה לביצוע תנועות.

כאשר עומס העבודה יחזור לקדמותו, תת שרשראות מורשות להתחבר מחדש ולעבור אימות. מכניזם זה מאפשר עבודה במקביל על תנועות שונות, תוך שמירת האבטחה של רישומי התנועה.

### 3. Data Sharding (פעולות ממוקבלות)

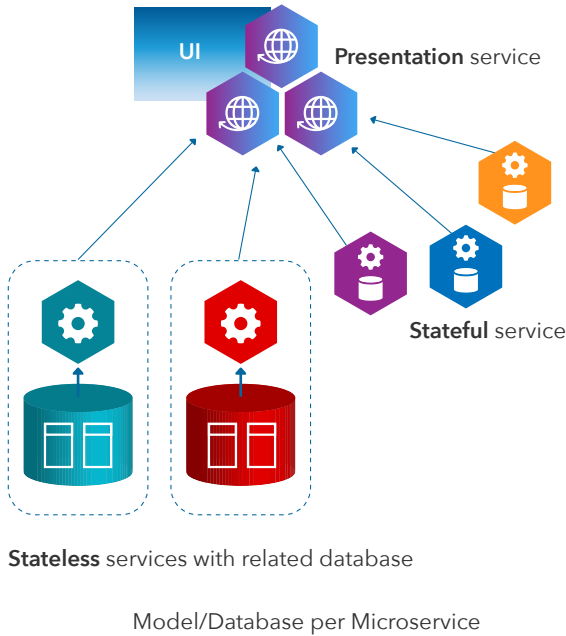
כל צומת יכול את כל השרשרת או רק חלק ממנה. כאשר יש צורך ב Data Sharding, צמתים מתאמים יקבעו data partition modes ספציפיים, בשביל אופטימיזציה של החלוקה בהתאם לעומסי העבודה הנוכחיים. בזכות high availability techniques, אמינות והתמדה יובטחו, גם במקרה של איבוד פתאומי של חלק מהמקבץ, במידה ולפחות 1+50% מהצמתים יישרדו. לאחר קריסה חלקית, צמתים אלו יהיו מסוגלים לפצל ולארגן מחדש את מבני הנתונים, כדי שיוכלו להתמודד עם אפשרות של קריסה חלקית נוספת של המקבץ בהקדם האפשרי. בזכות טכניקות 2 ו 3, שרשראות בלוקים של Multiversum יהיו בעלות יכולות עבודה ממוקבלות ו Data Sharding משופרות, שמשמעותן סקלביליות אופקית, אבטחה מוגברת, זמינות גבוהה, מערכת אמינה, התפטרות מ single point of failure ויכולת התאוששות עצמית מאסונות.



### 4. API (ממשק תכנות יישומים) מתקדם

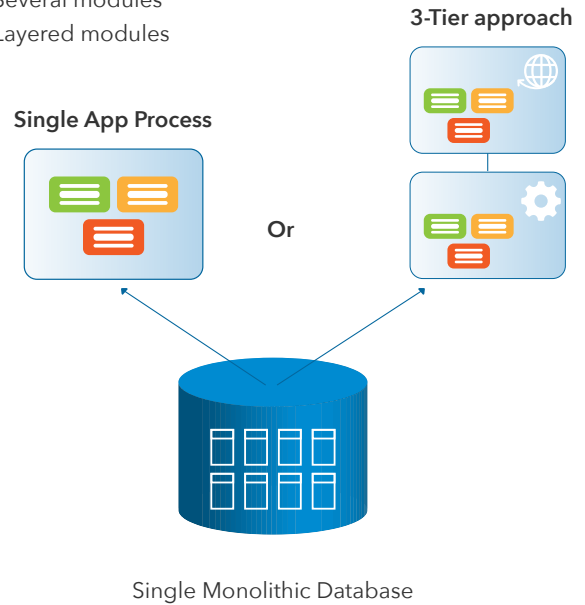
בשל פיתוח על פלטפורמה מבוססת Microservices<sup>9</sup> ו Serverless models<sup>10</sup>, Multiversum תהיה מסוגלת להציע פונקציות API ואבטחה מתקדמות ולהסתגל בשני המבנים השונים.

**Microservice Approach**



**Traditional Application**

- Single app process or 3-Tier approach
- Several modules
- Layered modules

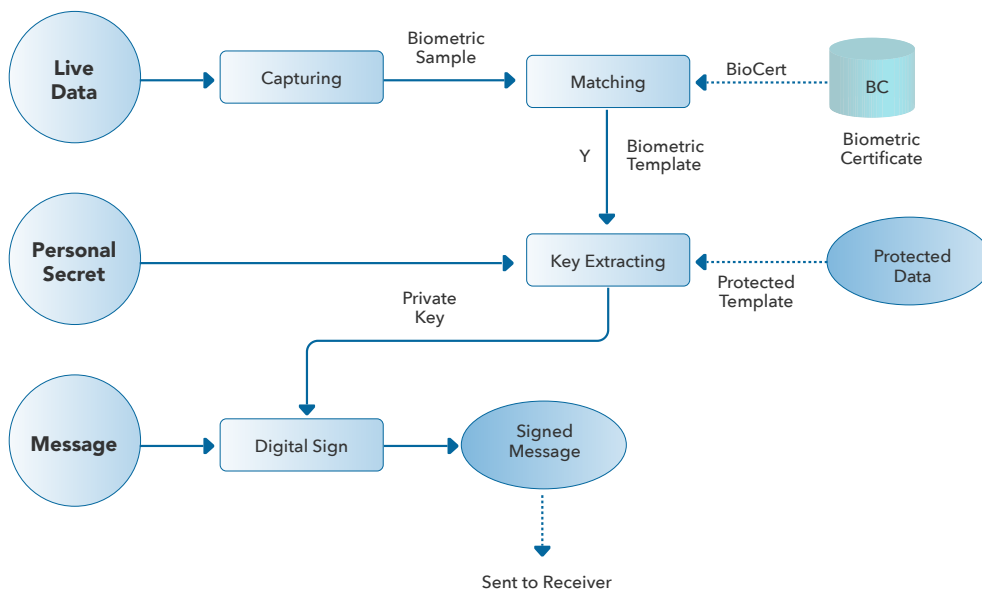


**.5 Rollback (אבטחת משתמש)**

הטכנולוגיה שלנו, בתחום התנועות, תאפשר לבצע Rollback של פעולות בלתי רצויות כלומר שחזור של מצב קודם ללא הפרעה לאמינות של אימות שרשרת, על ידי הטמעה של מספר מצבי שחזור תנועה. תכונה זו, יכולה להיות מופעלת לפי בחירה על כל הטוקנים והיישומים המתארחים על שרשרת הבלוקים של Multiversum

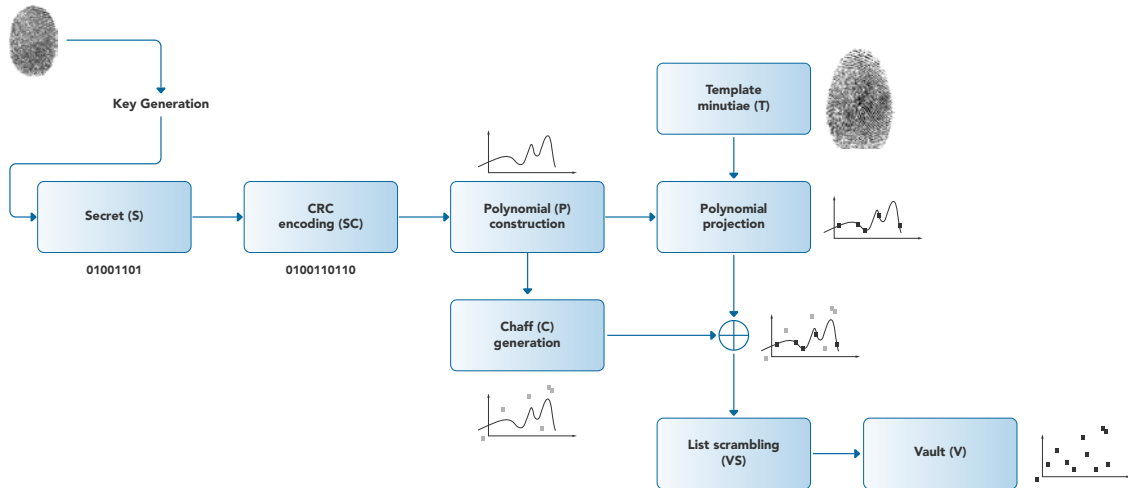
**.6 Freezable Wallets (אבטחת משתמש)**

תכונת הקפאת הארנק במקרה של פעולות לא חוקיות או חשודות, תוטמע במערכת לאחר שתיבדק המעשיות שלה מבחינה עסקית. יישומי קניין, שייבנו על גבי שרשרת הבלוקים של Multiversum יוכלו להטמיע את אופציה זו במידה ויהיו מעוניינות בכך.



**7. הטמעת נתונים ביומטריים כבסיס לחתימה אלקטרונית**

בהתבסס על המחקר שנעשה על ידי Je-Gyeong Jo, Jong-Won Seo and Hyung-Woo Lee's work<sub>11</sub>, הצוות של Multiversum יעריך את המעשיות של שימוש בנתונים ביומטריים כגון טביעת אצבעות, סריקת רשתית ו graphometric signature כמקור למפתח קריפטוגרפי א סימטרי, על מנת להבטיח את אותנטיות זהות המשתמש. כמו כן, יוערכו הבטיחות והיישום של מידע מוצפן למתן תוקף בטיעונים לגאליים. זאת ועוד, מידע ביומטרי יישמש ב Android, IOS ופלטפורמות יישומים נוספות בשביל אבטחת המשתמש.



Fuzzy Vault Scheme for Biometric Digital Key Protection

**8. ממשק ERC23 (יכולת פעולה הדדית עם שרשראות בלוקים אחרות)**

Versum coins יפותחו כדי להטמיע ממשק ERC23 עם תאימות לאחור עם ERC20<sub>12</sub>, כדי להבטיח יכולת פעולה הדדית עם שרשראות אחרות.

```
int totalSupply();
int balanceOf(String walletId);
boolean transfer(String receiverWalletId, int value);
boolean transferFrom(String senderWalletId, String receiverWalletId, int value);
boolean approve(String spenderWalletId, int _value);
int allowance(String walletId, String spenderWalletId);
boolean Transfer(String senderWalletId, String receiverWalletId, int value);
boolean Approval(String walletId, String spenderWalletId, int _value);
```

**9. Native off-chain adaptors בשביל ERC20/ERC23 פנימיים (יכולת פעולה הדדית עם שרשראות בלוקים אחרות)**

Multiversum תפתח native adapter כדי לאפשר תזרים נכנס ויוצא של המטבע והטוקנים שלה לשרשראות חיצוניות למערכת.

**10. Native off-chain adaptors בשביל ERC20/ERC23 חיצוניים (יכולת פעולה הדדית עם שרשראות בלוקים אחרות)**

Multiversum תפתח native adapter כדי לאפשר תזרים נכנס ויוצא של מטבעות וטוקנים משרשראות חיצוניות למערכת על גבי השרשרת שלה.



## Integrity

### 11. Proof of Integrity (פרוטוקול חדשני)

כתחליף להוכחת עבודה והוכחת החזקה, על כל צורתיהן, Multiversum מציעה Proof of Integrity: סדרת אלגוריתמים המסוגלים לאמת תיקוף קריפטוגרפי של צומת ואחדות התגובה מרוב הצמתים. האימות נעשה כנגד random-seed challenge, ביחד עם hash המחושב על ידי רכיב חיצוני (המוגן מ Reverse Engineering, ומתקשר עם תוכנת צומת על גבי ערוץ מוצפן) של התוכנה עצמה עם נתוני התנועה. כדי לאמת תנועה, תוצאת החישוב הזו חייבת להיות זהה לתנועה ספציפית, בכל צומת. פרוצדורה זו, דורשת כוח חישוב נמוך במידה ניכרת ובכך חוסכת בזבז של כוח מחשוב הנפוץ בסוגי אימות בלוקים אחרים (PoW, PoS, DpoS), ומספקת בטחון מבני, שאינו מבוסס על מודלים סטטיסטיים או מודלי <sup>13</sup> Byzantine Consensus, אשר נוטים להיות די פגיעים במקבצים קטנים.



## Access Denied

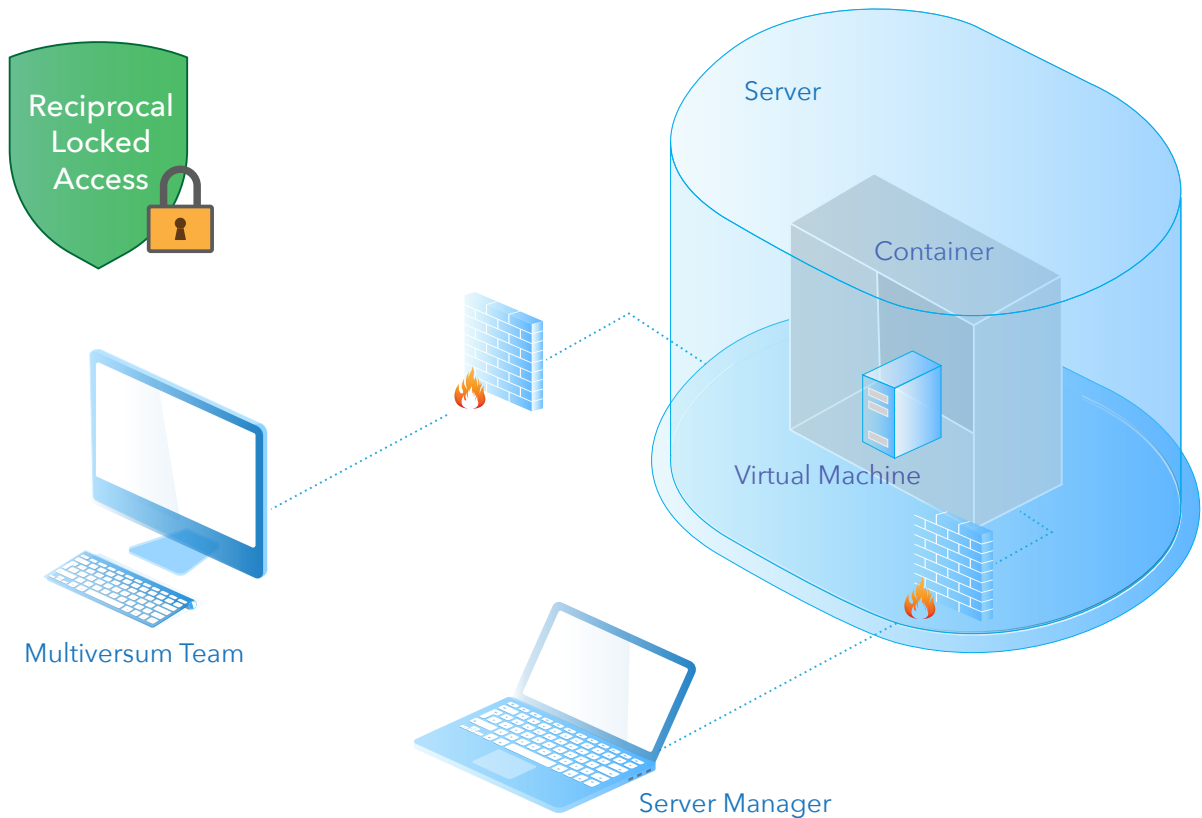
### 12. Double Access Lock (אבטחת מבנה)

צמתים יפוזרו ב Virtual Containers מאובטחים, עם credentials שאינם זמינים למתפעל ה Host machine, ומונעות גישה: משום כך, האבטחה מופנית לפיתוחים מצויינים של Linux Security כגון SeLinux ועוד. בו בעת, גם למשתמש בעל Guest machine credentials לא תהיה גישה ולא יוכל לגשת ל Host machine שמריצה צמתים אלו. הצומת, למעשה, מוגן על ידי Double Access Lock.

### 13. Reverse Access Denial (אבטחת מבנה)

נעילת הגישה המתוארת בנקודה 12 כרוכה במניעה הדדית של גישה לצומת הן למתפעל ה Host machine וכן למי שבסופו של דבר יחזיק ב credentials של הצומת. בכך מובטחת האותנטיות של כל צומת שאינו מנוהלת באופן ישיר על ידי Multiversum על ידי הפיכתו לבלתי נגיש, אוטונומי ומבודד לחלוטין מכל מגע אדם. שלוש מרכיבים פנדמנטלים יופצו בכל Container בנוסף למרכיבים תפעוליים ומרכיבי אבטחה: קוד הידור של שרת Multiversum, תעודת אישור בעלת מפתח א סימטרי כדי לאמת מקבץ Multiversum (שכבר תואר בנקודה 11) שאחראי ל challenge computation המבוסס על hash בקוד השרת, תעודת אישור, challenge seed, ונתוני תנועה. ישנה אפשרות להטמעת טכניקות אבטחה אופציונליות נוספות, כגון עדכון אוטומטי של Container access credentials עם סימא רנדומלית, במהלך שלב ההידור, כדי למנוע גישה חיצונית. מכניזם זה אולי אף יוטמע עבור אישור גישה למקבץ.





**14. Reciprocal Chain Confirmation (יכולת פעולה הדדית עם שרשראות בלוקים אחרות)**  
 Multiversum תבחן את המעשיות של הטמעת רכיב חיצוני לשרשרת, המסוגל לאחסן מצבים של שרשראות בלוקים אחרות (תמורת טוקנים בסופו של דבר) כדי לספק אימות ואמון נוספים. אותה הטכניקה יכולה לשמש את Multiversum כדי לחלוק את אימות המצבים שלה לשרשראות בלוקים אחרות "מיקור חוץ" של שיטת אימות. ממשק ייעודי יספק למען פונקציה זו, שתשווק בין שרשראות בלוקים קיימות ועתידיות. מאפיין זה יסתמך על רכיב ללא שרת שאליו יש גישה גם לאחר הידור ה container, כדי לאפשר הכלת מתאמים לשרשראות אחרות.

**15. אינטגרציה עם Java, Spring ו Javascript**  
 Multiversum תספק ממשקים יוקרתיים מקובצים בספריות פונקציונליות עבור Java, Javascript ואולי אף לשפות תכנות נפוצות נוספות, כדי להקל על אימוץ הטכנולוגיה שלנו ברמה היזמית והממסדית. מודולי הטמעה בעלי תשתית כגון Spring<sup>15</sup> יפותחו גם כן. סוגי ספריות אלו ייסעו בשילוב Multiversum בפתרונות קניין, הן בשרשראות פרטיות והן ב MainNet רשמיות.



## 16. מודל ACID

Multiversum תספק את פרדיגמת ACID<sup>16</sup> ראשי תיבות אלו מזוהים עם המאפיינים הלוגיים הנחוצים לתנועות. כדי להבטיח מודל תנועות בטוח, הטכנולוגיה שתוטמע תצטרך לענות על המאפיינים הבאים:

**Atomicity**: תנועה אינה ניתנת לחילוק בביצועה, ותוצאת היצוע חייבת להיות שלמה או אפסית, ביצוע חלקי אינו אפשרי.

**Consistency**: כל תנועה שהיא תעביר את מאגר הנתונים ממצב מקובל אחד לשני. מידע מתמיד חייב לעלות בקנה אחד עם כל הכללים המוגדרים.

**Isolation**: כל תנועה חייבת להיות מבוצעת בצורה מבודדת: אסור שהכשלון האפשרי של התנועה יפריע לביצוע תנועות אחרות.

**Durability**: ידוע גם כהתמדה (persistence) קובע כי מרגע שתנועה מבוצעת, התוצאה אינה יכולה להיבד מכל סיבה שהיא (קריסת מערכת, שגיאות, הפסקת חשמל).

## 17. מודל תנועות

MULTIVERSUM תתמיד נתוני תנועות במודל transactional<sup>18</sup>, כדי לוודא שכל הנתונים או אף אחד מהנתונים בתת שרשראות הקשורות, יתמידו, כדי להבטיח את קוהרנטיות התנועה המבוצעת ואת שלמות הנתונים.

## 18. שפה תואמת SQL

כדי לפשט את פיתוח היישומים המבוססים על טכנולוגית ה Crypto-Relational Database שלנו וכדי להקל על עקומת הלמידה כנגד טכנולוגיות קיימות, Multiversum תכלול SQL-based<sup>18</sup> syntax לשימוש פונקציות standard persistent-storage (CRUD).

## 19. Full Route Data Flux

תהליך הקבלה, שליטה, אימות והתמדה של תנועה קורה בזכות התהליך המפושט והסכמטי הבא:

התנועה נשלחת ללקוח REST, עם הנתונים הנחוצים חתומים במפתח פרטי: לקוח ה REST שולח את התנועה לצומת מוביל של מקבץ תיאום: הלה יפצל את המשימה בין צמתים בעלי פרוטוקול proprietary coordination:

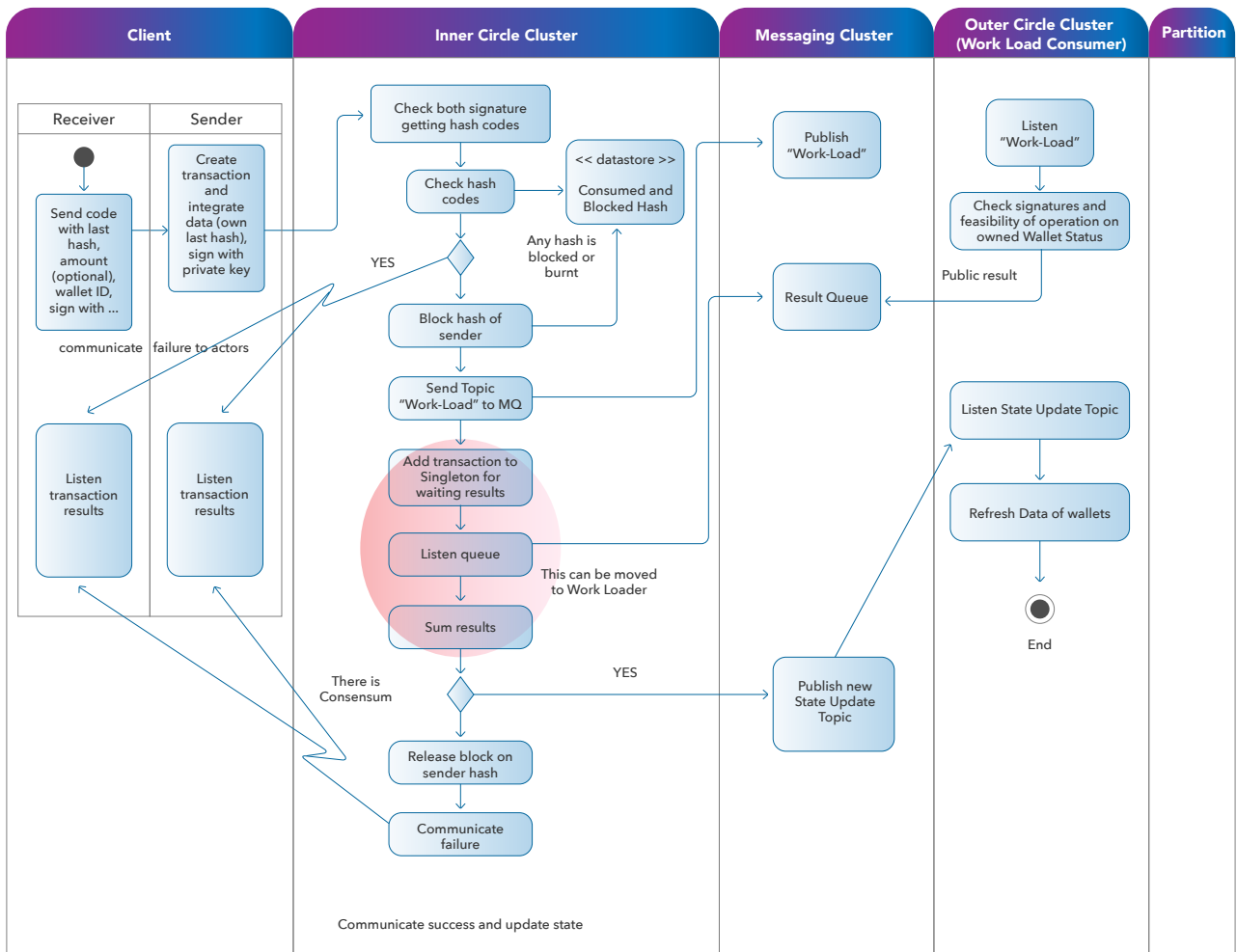
הם יריצו בדיקה ראשונית של שלמות הנתונים, חתימה, הון זמין, hashes שכבר בשימוש, מצבי ארנק לא פעילים, ארנקים או משתמשים חסומים:

כל פעולה נוספת מתעודת הזהות של השולח חסומה כעת בזיכרון הנדיף, בעוד ששדות נתונים ספציפיות מושלמות (כגון תנועות קודמות שיש לקשר, חתימת זמן ו hash קודם)

התנועה נשלחת ל Topic Message Queue<sup>19</sup> עם פרוטוקול שיש להגדיר (AMQP בשביל ה pilot, MQTT ועוד שיש להגדיר) ומופץ לצמתים פועלים מקבילים.

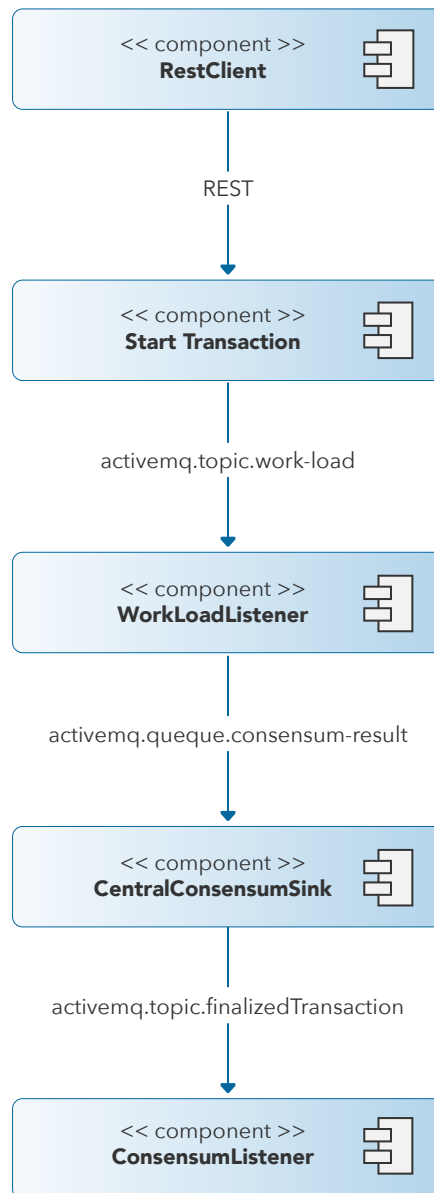
צמתים פועלים מאמתים את האינטרס שלהם בבקשה (יכול להיות שחסר מידע נחוץ, הם עסוקים ועוד תנאים שיש להעריך), וימשיכו כדי ליצור את מצב הארנק החדש, ישחזרו Hashes תואמים של תנועות מקושרות קודמות והוספתן לרישום התנועות. Proof of Integrity מתווספת כעת: Hash התנועה מחושב כעת.

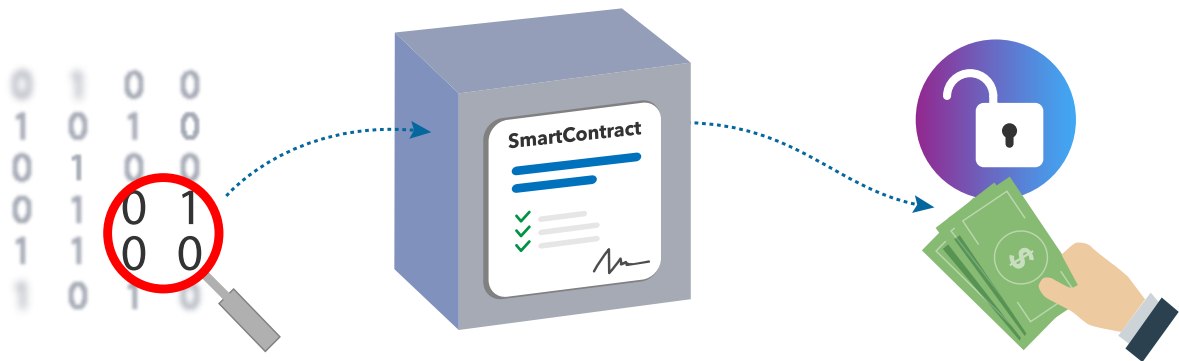
צמתים פועלים מתעדים את התנועה, שולחים הצבעה לצמתים מתאמים דרך Message Queue ואוספים את התוצאות: עם ההצבעות וה hashes קוהרנטים, הצמתים המתאמים יתמידו את התנועה וכל מצב חדש של הארנק, תוך ביטול כל ה Hashes ממצבים קודמים ושידור הצבעת אימות עם מערכת Topic Message Queue נוספת. צמתים פעילים גם יתמידו את התנועה ואת שינויי מצב הארנק. בכך מסתיים התרחיש הטוב ביותר של Full route.



## Logic data flux

*Detail of process flow*





### חוזים חכמים

Multiversum מאמינה בחשיבות של הצעת Smart Contracts<sup>20</sup> משופרים לציבור, אך בזמן כתיבת מסמך זה, אילולא יהיה שינוי בהיקף הממחקר, לא החליטה לחקור את אפשרות זו. לכן, אנחנו מבקשים לשלב ב Multiversum את פתרון הקוד הפתוח שמתאים לצרכינו באופן המיטבי, בהתאם למודל הרשיון שלו.

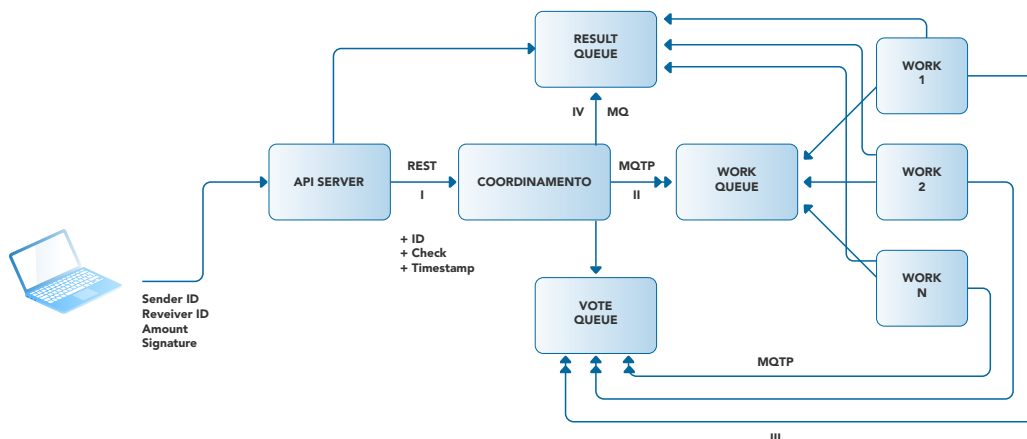
### תשתית

התשתית של Multiversum מעוצבת להבטיח את החוסן וה reachability<sup>21</sup>. מטרה זו הושגה על ידי פיתוח מקבצי צמתים המסוגלים לייעד באופן עצמאי את הצמתים שבתוכם לתפקידים ספציפיים, בהתאם לנתונים הטכניים של כל אחד מהם, אשר כוללים:

- יכולת מחשוב
- נפח זיכרון
- Reciprocal Latency
- שלמות רצף נתונים
- מהימנות החומרה
- ספקות לגבי Proof of Integrity

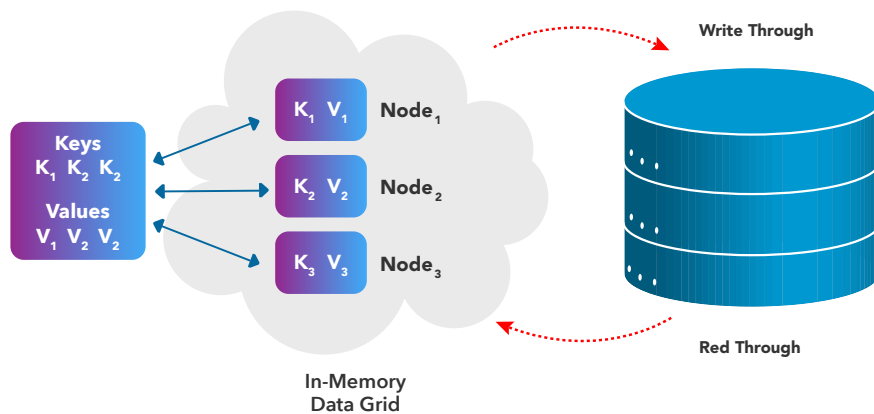
כעת כל צומת יקבל תפקיד אחד או יותר:

- צמתי לקוח
- צמתי תיאום
- צמתים להעברת הודעות
- צמתים פועלים
- צמתי התמדה
- צמתי גיבוי



כעת כל צומת שיספק אישור בר תוקף יוכל להירשם למקבץ ולקבל תפקיד. במקרה של קריסה של אחד או יותר מהצמתים, המקבץ יוכל באופן עצמוני לחלק מחדש את המשימות והתפקידים באופן אופטימלי.

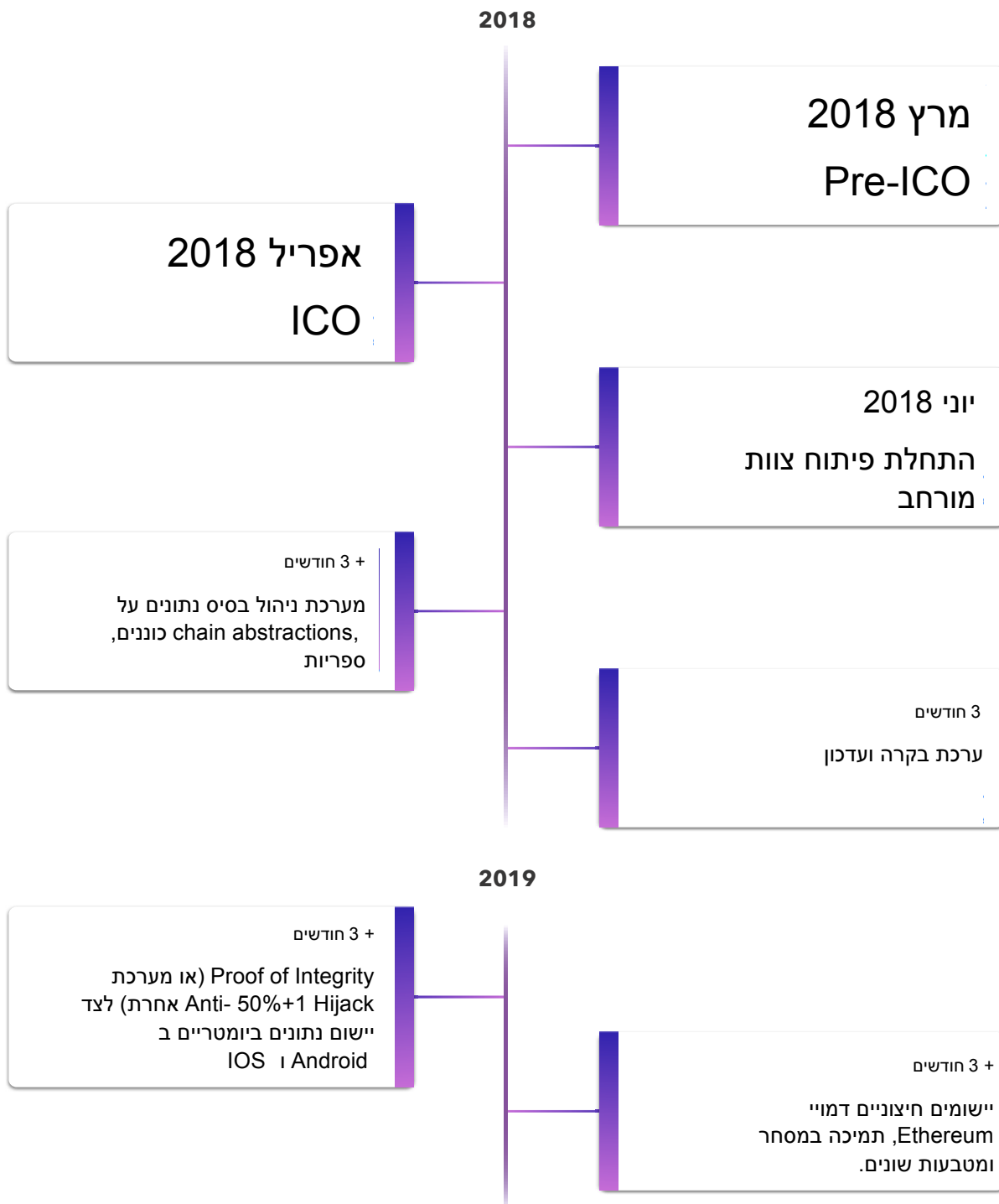
רכיבים של מטמון משותף פנים JVM<sub>22</sub> ישמשו כמאגר נתוני זיכרון ובכך יאפשרו **Read Through**: שאילתות קריאת נתונים מבוצעת באופן ישיר בזיכרון הנדיף לפני שיבדקו זיכרון ממשי. **Write Through**: העלאת נתונים לזיכרון הנדיף לפני ביצוע החדרת מאסה לנתונים מותמדים, כדי לשפר את הביצועים.



## הערות אבטחה

במהלך הפיתוח, "Hacker's bounties" יוצעו למתכנתים שיחשפו נקודות תורפה ויוכלו להציע פתרונות רלוונטיים.

## מפת דרכים טכנית



## אזכורים

- 2 [https://en.wikipedia.org/wiki/Scalability#Horizontal\\_and\\_vertical\\_scaling](https://en.wikipedia.org/wiki/Scalability#Horizontal_and_vertical_scaling)
- 3 [https://en.wikipedia.org/wiki/Proof-of-work\\_system](https://en.wikipedia.org/wiki/Proof-of-work_system)
- 4 <https://en.wikipedia.org/wiki/Proof-of-stake>
- 5 [https://en.wikipedia.org/wiki/Agile\\_software\\_development](https://en.wikipedia.org/wiki/Agile_software_development)
- 6 [https://en.wikipedia.org/wiki/Scope\\_\(project\\_management\)](https://en.wikipedia.org/wiki/Scope_(project_management))
- 7 [https://en.wikipedia.org/wiki/Shard\\_\(database\\_architecture\)](https://en.wikipedia.org/wiki/Shard_(database_architecture))
- 8 [https://en.wikipedia.org/wiki/High-availability\\_cluster](https://en.wikipedia.org/wiki/High-availability_cluster)
- 9 [https://en.wikipedia.org/wiki/Single\\_point\\_of\\_failure](https://en.wikipedia.org/wiki/Single_point_of_failure)
- 10 <https://en.wikipedia.org/wiki/Microservices>
- 11 <http://goo.gl/CVBzJd> Biometric Digital Signature Key Generation and Cryptography Communication Based on Fingerprint"
- 12 <https://en.wikipedia.org/wiki/ERC20>
- 13 [https://en.wikipedia.org/wiki/Byzantine\\_fault\\_tolerance](https://en.wikipedia.org/wiki/Byzantine_fault_tolerance)
- 14 [https://en.wikipedia.org/wiki/Security-Enhanced\\_Linux](https://en.wikipedia.org/wiki/Security-Enhanced_Linux)
- 15 [https://en.wikipedia.org/wiki/Spring\\_Framework](https://en.wikipedia.org/wiki/Spring_Framework)
- 16 <https://en.wikipedia.org/wiki/ACID>
- 17 [https://en.wikipedia.org/wiki/Models\\_of\\_communication#Transactional\\_Model](https://en.wikipedia.org/wiki/Models_of_communication#Transactional_Model)
- 18 <https://en.wikipedia.org/wiki/SQL>
- 19 [https://en.wikipedia.org/wiki/Message\\_queue#Standards\\_and\\_protocols](https://en.wikipedia.org/wiki/Message_queue#Standards_and_protocols)
- 20 [https://en.wikipedia.org/wiki/Smart\\_contract](https://en.wikipedia.org/wiki/Smart_contract)
- 21 <https://en.wikipedia.org/wiki/Reachability>
- 22 [https://en.wikipedia.org/wiki/Java\\_virtual\\_machine](https://en.wikipedia.org/wiki/Java_virtual_machine)



## אסטרטגיית שיווק

פעילות החברה בתחום ה IT שהינו דינמי ומשתנה תמידית, ייעדכן את האסטרטגיה שלנו, שיטות תקשורת ומשימת החברה בהתאם, בדגש על יצירת ערך עבור בעלי מניות והבטחת איזון מתאים בין רעיונות ניהוליים לטווח הקצר ולטווח הארוך.

נקודות המפתח של התכנית שלנו הינן:

- משימת החברה
- מטרות עסקיות
- אסטרטגיות עסקיות
- תיק עבודות של פעילות העסק



אחד מהכלים המרכזיים שבו נעשה שימוש הוא **שיווק במדיה החברתית**: קמפיינים ייערכו ברשתות החברתיות כדי להגדיל את המודעות למוצר, לזהות לקוחות פוטנציאליים, ליצור אנשי קשר וכדי לבנות יחסים משמעותיים עם לקוחות. אסטרטגיית המדיה החברתית שלנו תבצע מספר פעולות שיהוו חלק מתכנית אסטרטגית כוללת, החל מניהול וניטור ערוצים בעזרת כלים ייעודיים, פיתוח קהילה, תוך שימת דגש על תכנים, אינטרקציה והערכת יעילות הטקטיקות בהתבסס על תוצאות שהושגו.



MULTIVERSUM

HERE TO STAY