

# מערכת בחירות מבוזרת 2026

Decentralized Election System

פרויקט גמר בקורס בלוקצ'יין – מסלול ברירת מחדל

מגיש: ארבל קורן



# באגים ידועים ומגבלות (Known Bugs & Limitations)



## אבטחה

מפתח האדמין שמור ב-MetaMask מקומי.  
במערכת מבצעת חובה להשתמש בארנק  
MultiSig לאבטחה מוגברת.



## מיון תוצאות

המועמדים מוצגים לפי סדר הוספתם (ID).  
מיון לפי כמות הצבעות דורש מיון בצד הלקוח  
(Frontend) ולא בחוזה.



## Merkle Tree

חישוב ה-Root וה-Proof מתבצע בחוזה  
(On-chain) לצורך הדגמה. בפרודקשן, זה  
אמור להתבצע Off-chain לחיסכון ב-Gas.



# תיאור המערכת וארכיטקטורה



**מטרת הפרויקט:** מערכת בחירות שקופה, אמינה ובלתי ניתנת לשינוי המבוססת על Ethereum Blockchain.

Solidity (ניהול בחירות ומטבע).

**Smart  
:Contracts**



.HTML5, Web3.js **:Frontend**



.Sepolia Testnet **:Network**



.MetaMask Integration **:Wallet**





# החוזים החכמים (Backend Logic)

## 1. BalToken.sol (ERC20)

מטבע דיגיטלי בתקן סטנדרטי. משמש כתמריץ (Incentive): כל מצביע מקבל אוטומטית **10 מטבעות BAL** לאחר ההצבעה.

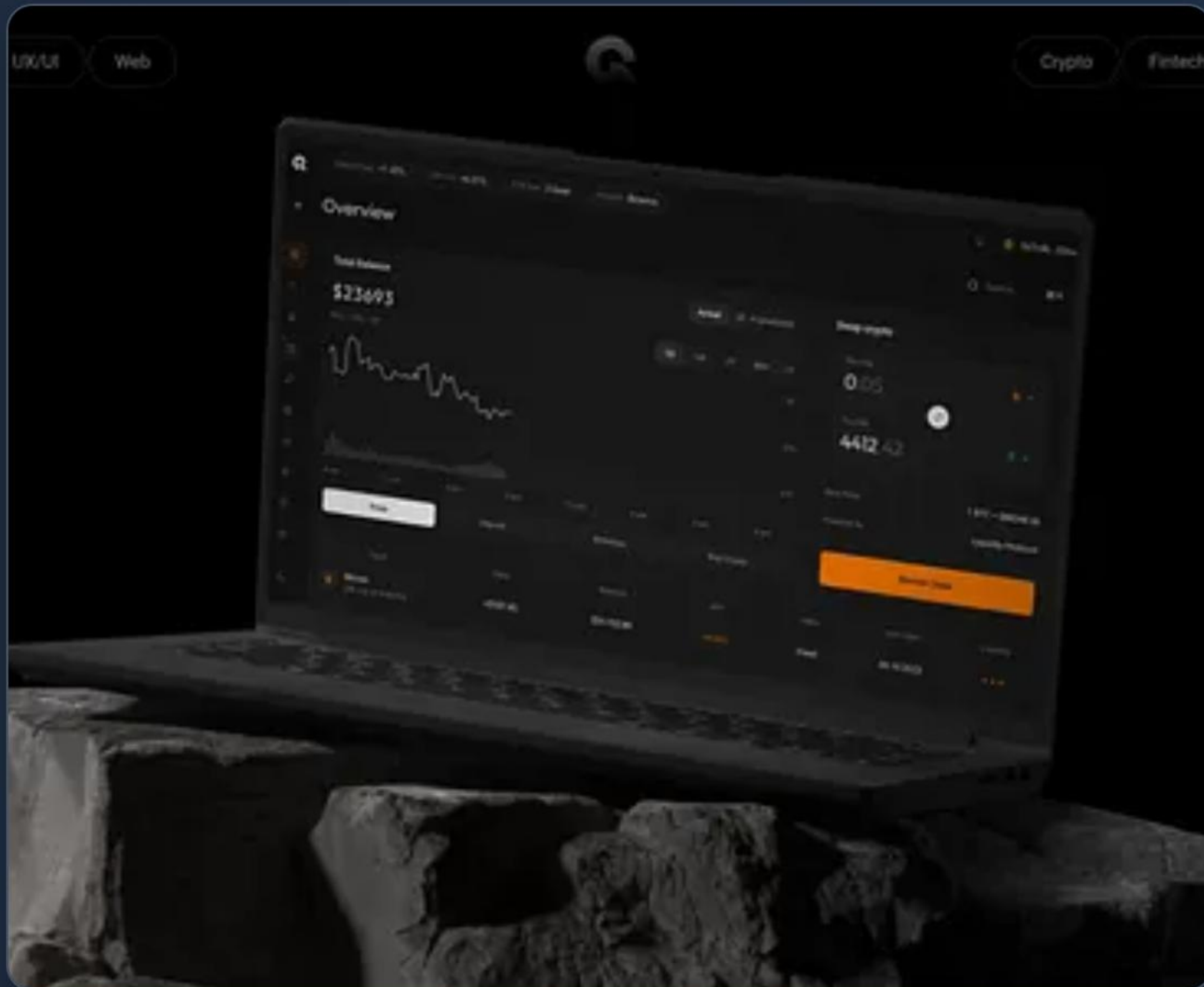
## 2. Election.sol (Core Logic)

- **addCandidate**: הוספת מועמד עם דירוג דעות.
- **startElection**: הפעלת טיימר ונעילת הוספה.
- **vote**: בדיקת זכאות (Merkle), אימות זמן, רישום הצבעה והעברת תשלום.





# ממשק המשתמש (Frontend & Web3)



## חיבור וניהול

זיהוי אוטומטי של חשבון MetaMask והצגת יתרה בזמן אמת.  
פאנל אדמין מאפשר הוספת מועמדים והזנת דעותיהם (1-10).

## תהליך ההצבעה

הצגה דינמית של המועמדים הנמשכת ישירות מהבלוקצ'יין.  
ביצוע הצבעה מאובטחת באמצעות חתימה דיגיטלית על  
טרנזקציה.

כולל טיימר ויזואלי לסיום הבחירות.



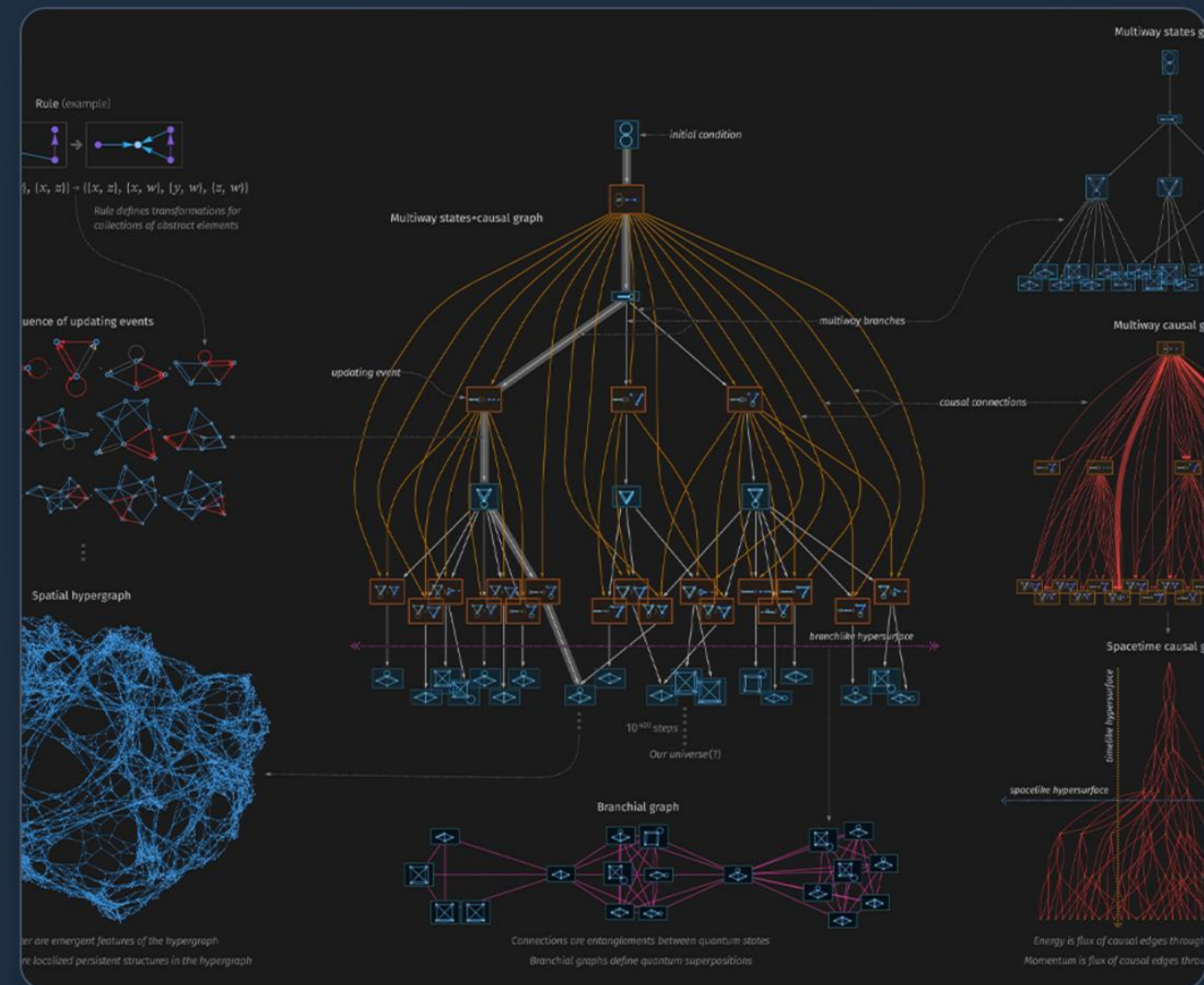
# בנוס: אלגוריתם "הבחירה החכמה"

**הרעיון:** בוחרים מתלבטים יכולים להזין העדפות אישיות ב-3 נושאים (1-10).

**האלגוריתם:** חישוב "מרחק" מתמטי בין דעות הבוחר לדעות המועמד (סכום ההפרשים המוחלטים).

$$\text{Score} = \sum_{i=1}^3 | \text{UserOp}_i - \text{CandOp}_i |$$

המערכת בוחרת אוטומטית במועמד עם הציון הנמוך ביותר (המרחק הקצר ביותר).





# הוראות התקנה והרצה (Deployment)

## Client Config </>

עדכון קובץ **index.html** עם הכתובות החדשות.

עדכון ה-ABI במידת הצורך.

הרצה דרך	<b>Live Server</b>	(VS Code) לתקשורת תקינה.
----------	--------------------	--------------------------

## Remix IDE

Deploy לחוזה **BalToken**.

Deploy לחוזה **Election** (עם כתובת הטוקן).

ביצוע **Transfer** של תקציב לחוזה הבחירות.



# סיכום

- ✓ מערכת Full Stack DApp עובדת על רשת Sepolia.
- ✓ מימוש מלא של דרישות החובה (חוזים, טיימר, תגמול).
- ✓ מנגנון "בחירה חכמה" לשיפור חווית המשתמש.



## !Live Demo Time

נא לפתוח את Remix ואת אתר ההצבעה.



# Image Sources

[https://img.freepik.com/premium-vector/abstract-digital-network-connection-structure-blue-background-artificial-intelligence-engineer\\_230610-1093.jpg](https://img.freepik.com/premium-vector/abstract-digital-network-connection-structure-blue-background-artificial-intelligence-engineer_230610-1093.jpg)

Source: [www.freepik.com](https://www.freepik.com)



[https://coinnews.com/wp-content/uploads/2025/09/ChatGPT-Image-Sep-4-2025-at-04\\_53\\_18-PM-e1757001446202.webp](https://coinnews.com/wp-content/uploads/2025/09/ChatGPT-Image-Sep-4-2025-at-04_53_18-PM-e1757001446202.webp)

Source: [coinnews.com](https://coinnews.com)



<https://cdn.dribbble.com/userupload/42727862/file/still-a875111ed7a9b452046dac2e13a39d6b.png?format=webp&resize=400x300&vertical=center>

Source: [dribbble.com](https://dribbble.com)



<https://content.wolfram.com/sites/43/2020/04/swblog-2036-explainer.png>

Source: [writings.stephenwolfram.com](https://writings.stephenwolfram.com)



[https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-10/AdobeStock\\_615788171\\_cropped.jpg?VersionId=\\_8jtPHTGEJb6wwQ0HzzXnjzJHlcUPbxw](https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-10/AdobeStock_615788171_cropped.jpg?VersionId=_8jtPHTGEJb6wwQ0HzzXnjzJHlcUPbxw)

Source: [www.csis.org](https://www.csis.org)



[https://www.simplilearn.com/ice9/free\\_resources\\_article\\_thumb/What\\_is\\_a\\_Cloud\\_Server.jpg](https://www.simplilearn.com/ice9/free_resources_article_thumb/What_is_a_Cloud_Server.jpg)

Source: [www.simplilearn.com](https://www.simplilearn.com)

