

פרויקט בחירות בבלוקצ'יין

מגישים:

דור בן ברוך: 307881268

שחר רוזן: 204541791

באגים ידועים:

- הعلاאת פנקס הבוחרים נעשה בקריאה נפרדת בעבר כל בוחר זאת משום שלא נמצא דרך לשולח מערך של כתובות בגלל המגבילות של solidity. אנחנו מניחים שקיים דרך לעשות דבר שכזה אך לא הצלחנו למצאו אותה בגין מגבלות הזמן.
- קיים race condition שגורם לכך שלפעמים לאחר הגדרת חלון זמן העמוד אינו מתעדכן אוטומטית.

מודולים מרכזיים:

Solidity:

- **Migrations.sol** קובץ זה אחראי לעדכון והעלאה של החויזים לבלוקצ'יין.
- **KaiCoin.sol** - ERC20 חואה המייצג את המטבע שלנו בפורמט
- **Functions:**
 - transfer פונקציה להעברת מטבע מכתובת אחת לאחרת
 - approve אישור העברה בין שתי כתובות
 - transferFrom פונקציה להעברת מטבע הפעם עם פרמטר המעביר
- **Election.sol** חואה המנהל את מערכת הבחירות
 - **Functions:**
 - setVotingWindow הגדרת חלון הצבעה ע"י האדמין
 - addCandidate הוספתמועמד ע"י האדמין
 - vote הצבעה לאחד המועמדים
 - submitAllowedVoters העלאת ספ"ר הבוחרים לבלוקצ'יין ע"י האדמין
 - **Modifiers:**
 - onlyOwner בודק שהפעולה מתבצעת ע"י האדמין

JavaScript:

- **readFile** - קורא את תוכן הקובץ הנבחר בספר הבוחרים
 - **initWeb3** - WEB3 מתחל את WEB3
 - **initContract** - מתחל מופעים של החוזים שנטענו
 - **listenForEvents** - מתחל מאזינים ליריעים המופצים ע"י החוזים בבלוקצ'יין
 - **render** - מעדכן את ה- UI בצד הלכה
 - **castVote** - שולח את הבחירה של הלכה לחוזה המתאים ומבצע בחירה
 - **addCandidate** - שולח את פרטי המועמד החדש שנבחרו ע"י האדמין
 - **setVotingWindow** - שולח את פרטי חלון הבחירה שנבחרו ע"י האדמין
 - **convertDateToLocalisedISOString** - פונקציית עזר להתאמת תאריכים מפורט ISO
- למיקום הלכה.

דוגמת ריצה:

1. לאחר הריצת ganache מתחילה את החזים עם .truffle migrate --reset

```
➔ blockchain-elections-app git:(master) ✘ truffle migrate --reset

Compiling your contracts...
=====
> Everything is up to date, there is nothing to compile.


Starting migrations...
=====
> Network name:    'development'
> Network id:      5777
> Block gas limit: 0x6691b7


1_initial_migration.js
=====

  Replacing 'Migrations'
  -----
  > transaction hash: 0xc06a9d61a004fc82b941366591b849a49191d850de1e40f3e817a7e4f012a6ff
  > Blocks: 0          Seconds: 0
  > contract address: 0x17A07cA0034F9b2fa02a9631ee5791a7DDce2e58
  > block number:     68
  > block timestamp:  1583398931
  > account:          0xCf15F23c9b37E0F011d934f0CFeb8A9f1D3a34a8
  > balance:          99.594728424
  > gas used:         263741
  > gas price:        20 gwei
  > value sent:       0 ETH
  > total cost:       0.00527482 ETH

  > Saving migration to chain.
  > Saving artifacts
  -----
  > Total cost:       0.00527482 ETH


2_deploy_contracts.js
=====

  Replacing 'KaiCoin'
  -----
  > transaction hash: 0xbb3dc21cfbdb8dfb701672f4d187a43da67165b366df00f2d0c4ed4474c21551
  > Blocks: 0          Seconds: 0
  > contract address: 0x2394718E9323678A101183092eA277373BE9dd1F
  > block number:     70
  > block timestamp:  1583398932
  > account:          0xCf15F23c9b37E0F011d934f0CFeb8A9f1D3a34a8
  > balance:          99.574585424
  > gas used:         965127
  > gas price:        20 gwei
  > value sent:       0 ETH
```

```

> value sent:          0 ETH
> total cost:         0.01930254 ETH

Replacing 'Election'
-----
> transaction hash: 0x5fa29ac79cfa6ce3f4c1016b80e2aa47d72aaeeee4b1aa99381335b657d6bc03
> Blocks: 0           Seconds: 0
> contract address: 0x1b6a6D1Fbb1C0E996925dD2cFf9552d2523512f9
> block number:      71
> block timestamp:   1583398932
> account:           0xCf15F23c9b37E0F011d934f0CFeb8A9f1D3a34a8
> balance:            99.553224444
> gas used:          1068049
> gas price:          20 gwei
> value sent:         0 ETH
> total cost:         0.02136098 ETH

> Saving migration to chain.
> Saving artifacts
-----
> Total cost:        0.04066352 ETH

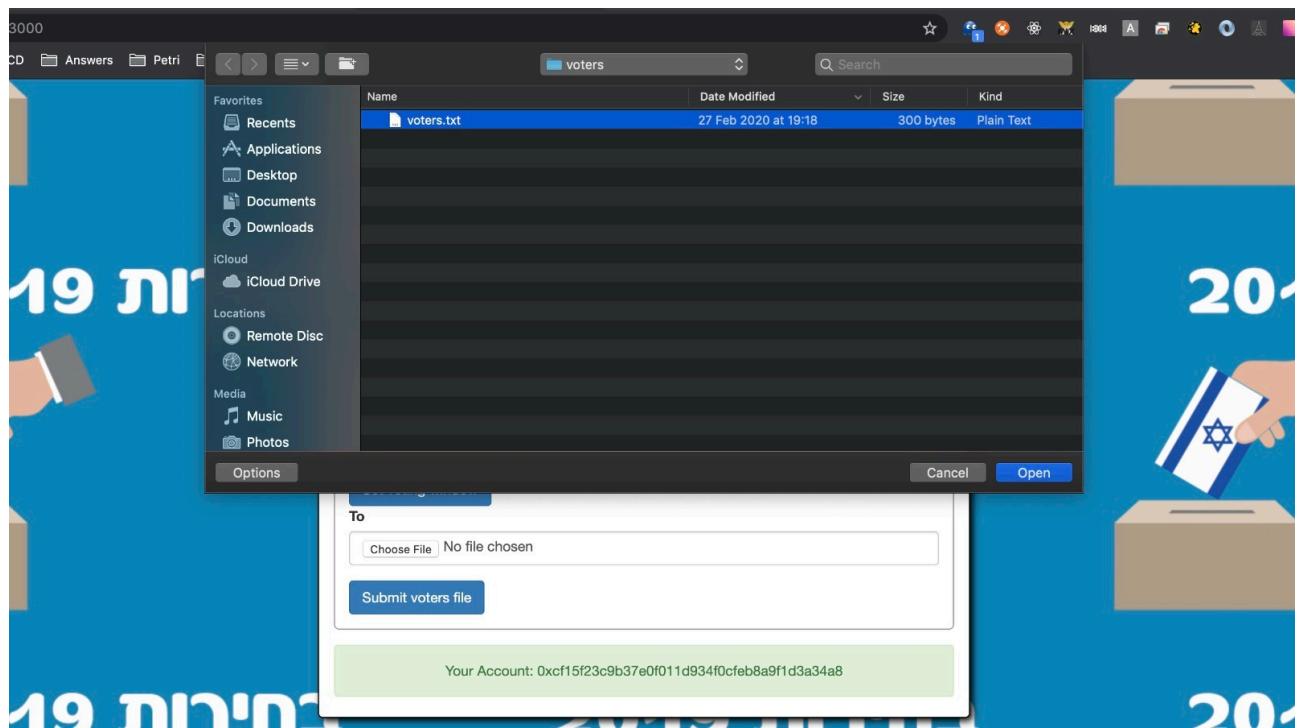
Summary
=====
> Total deployments: 3
> Final cost:        0.04593834 ETH

```

אתר

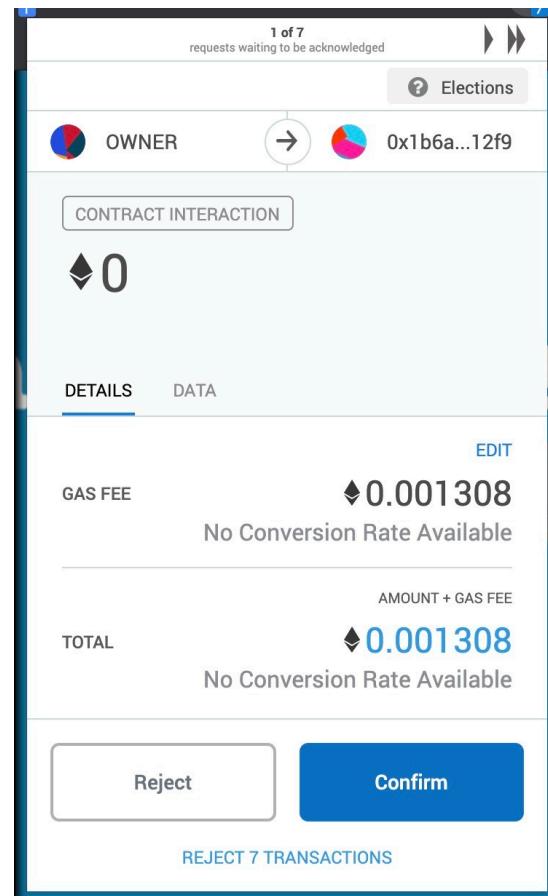
.2

הלקוח עולה ובבחירה משתמש האדמין ניתן להעלות ספר בוחרים.



Choose File voters.txt

Submit voters file



3. הוספה מועמדים (למשתמש האדמין בלבד) נעשית כר:

The image shows a smartphone displaying two screens side-by-side. The left screen displays the election results for the year 2019. It has a table with columns for #, Pic, Name, and Votes. Two candidates are listed: Bibi and Gantz, both with 0 votes. A message at the bottom says "Voting date has not yet been set, please come back at a later time". The right screen shows the "Admin dashboard" with a form to add a candidate named Yair. The right side of the phone has a blue vertical decorative bar.

The image shows a smartphone displaying a transaction confirmation dialog. At the top, it shows the word "Elections" and the address "0x1b6a...12f9". Below that, it says "CONTRACT INTERACTION" and shows a value of "0". There are tabs for "DETAILS" and "DATA", with "DETAILS" currently selected. Under "GAS FEE", it shows "0.002229" with the note "No Conversion Rate Available". Under "TOTAL", it also shows "0.002229" with the note "No Conversion Rate Available". At the bottom are "Reject" and "Confirm" buttons.

בבחירות 2019

#	Pic	Name	Votes
1		Bibi	0
2		Gantz	0
3		Yair	0

Voting date has not yet been set, please come back at a later time

Admin dashboard

Candidate name

Yair

[Add candidate](#)

From

dd/mm/yyyy, --:--

To

dd/mm/yyyy, --:--

4. הגדרת חלון זמני הצבעה - לפני שהחלו נפתח מוצגת הודעה מתאימה והצבעה נחסמת.

בחירה 2019

#	Pic	Name	Votes
1		Bibi	0
2		Gantz	0
3		Yair	0

Voting date has not yet been set, please come back at a later time

Admin dashboard

Candidate name

Add candidate

From

To

Set voting window

The smartphone screen shows a DApp interface titled "Elections". It displays a "OWNER" role with a blue and red circular icon. To the right is a recipient address: "0x1b6a...12f9". Below this is a "CONTRACT INTERACTION" section showing a balance of "0". The interface includes tabs for "DETAILS" and "DATA", an "EDIT" button, and a "GAS FEE" of "0.002042" with a note "No Conversion Rate Available". A "TOTAL" amount of "0.002042" is also shown with the same note. At the bottom are "Reject" and "Confirm" buttons.

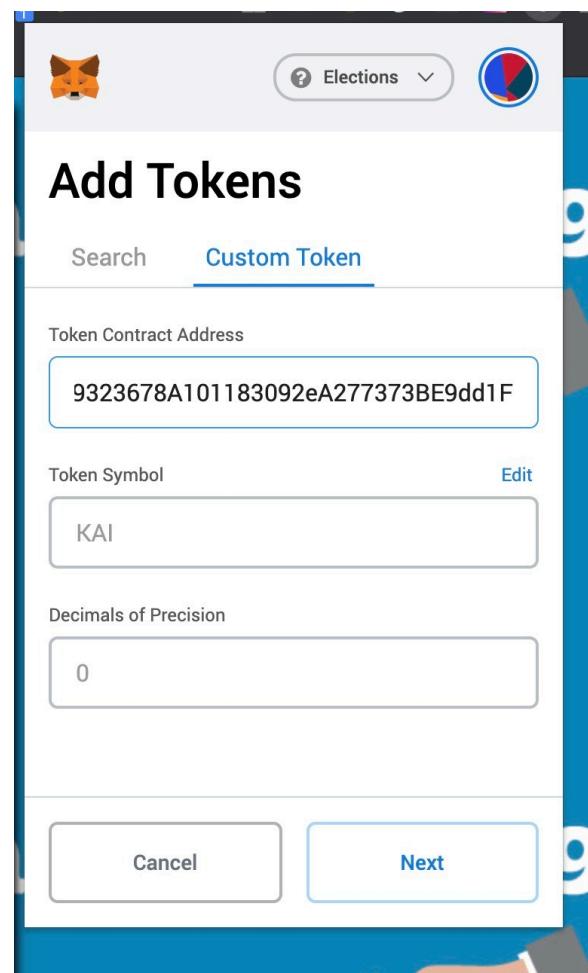
בבחירות 2019

#	Pic	Name	Votes
1		Bibi	0
2		Gantz	0
3		Yair	0

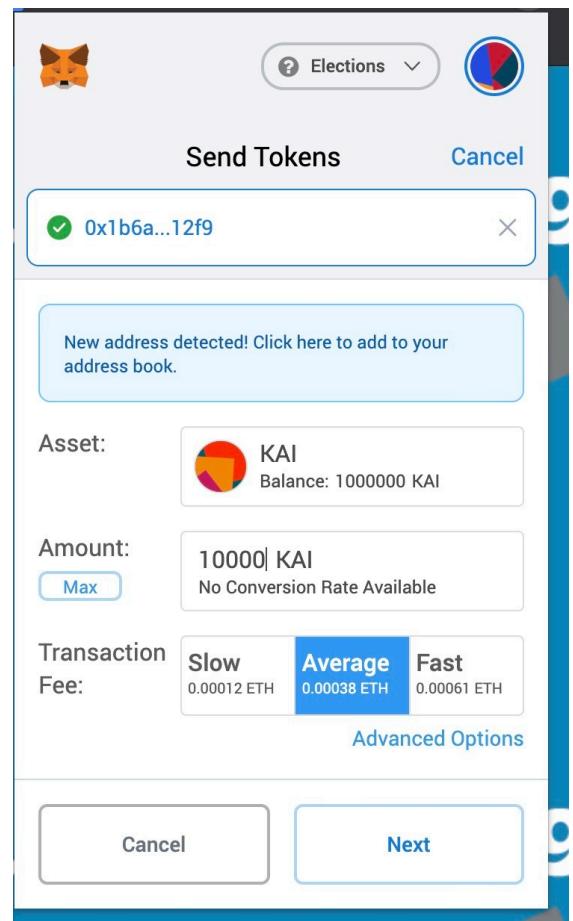
Select Candidate

Vote

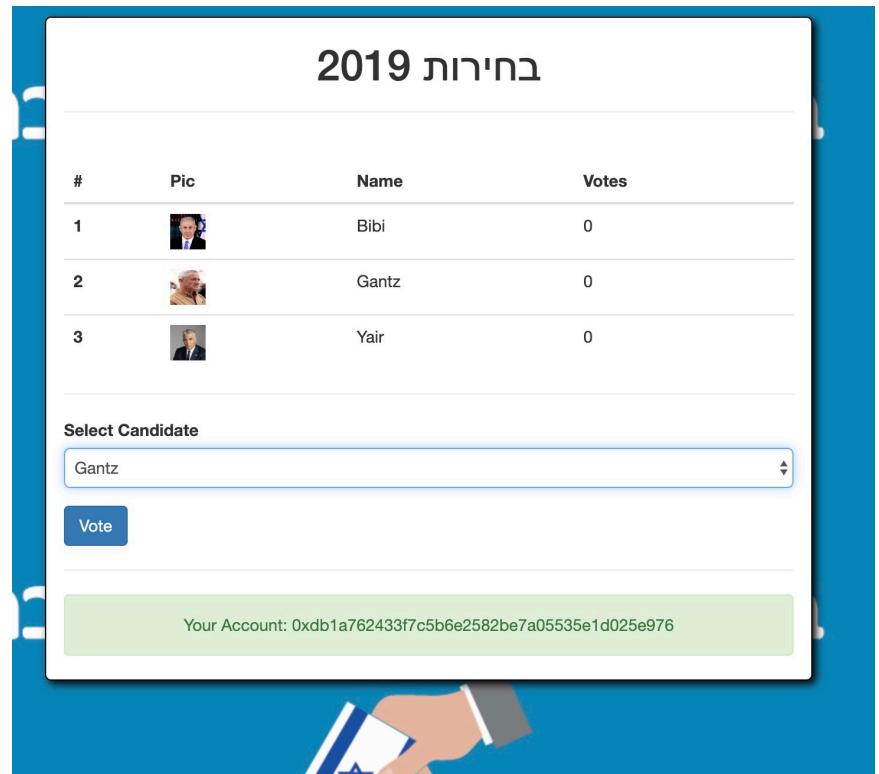
5. יש לטעון את המטבע **ל Metamask** ולהעביר כמות מסויימת לחזזה .Elections

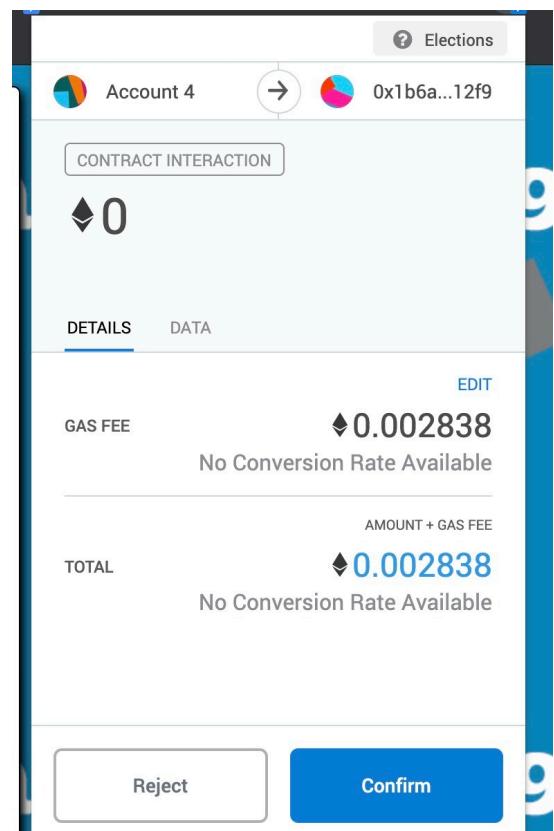


The image shows the Metamask mobile application's "Add Tokens" screen. At the top, there is a navigation bar with a fox icon, a "Elections" dropdown, and a circular profile picture. Below the navigation bar, the title "Add Tokens" is displayed. There are two tabs: "Search" and "Custom Token", with "Custom Token" being the active tab. A field labeled "Token Contract Address" contains the value "9323678A101183092eA277373BE9dd1F". Below this, a "Token Symbol" field contains "KAI" and an "Edit" link. A "Decimals of Precision" field contains "0". At the bottom of the screen are two buttons: "Cancel" and "Next".



6. לאחר הצביעת המצביע יקבל מטבע אחד בעבור הפעולה

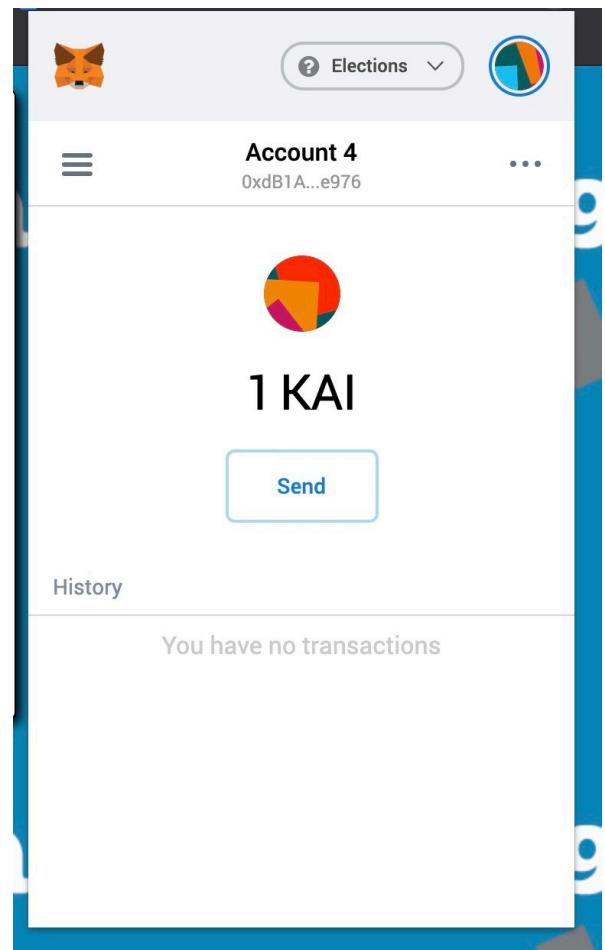




The screenshot shows a voting interface titled "בבחירות 2019" (Elections 2019). It lists three candidates with their names and vote counts:

#	Pic	Name	Votes
1		Gantz	1
2		Bibi	0
3		Yair	0

At the bottom, a green bar displays the account information: "Your Account: 0xdb1a762433f7c5b6e2582be7a05535e1d025e976".



7. בתום חלון הזמן יוצגו התוצאות, יחד עם הودעה מתאימה וביטול אפשרות ההצבעה כנדרש.

#	Pic	Name	Votes
1		Gantz	1
2		Bibi	0
3		Yair	0

Voting has ended, thank you for fulfilling your civil duty!

8. בהינתן מצב בו המשתמש אינו רשום בספר הבוחרים תוצג הודעה מתאימה:

בבחירות 2019

#	Pic	Name	Votes
1		Bibi	0
2		Gantz	0

Voting date has not yet been set, please come back at a later time

The central election committee has not yet registered you as an allowed voter, please contact the relevant authority

Your Account: 0x148de50c0fab9f6a5dd134d1bd238edfc620b6d5