**פרוייקט גמר**

**חברי קבוצת הפרוייקט:**

|  |  |  |
| --- | --- | --- |
| **שם מלא** | **תעודת זהות** | **מייל** |
| **סהר מלחי** | **304850308** | **saharmelechi22@gmail.com** |
| **רזיאל בן-אליהו** | **203019633** | **razielbe@gmail.com** |
| **משה קרופר** | **305257875** | **moshekrupper@gmail.com** |
| **ירון רשף** | **304803877** | **reshefyaron@gmail.com** |

**מנחה פרוייקט גמר:**

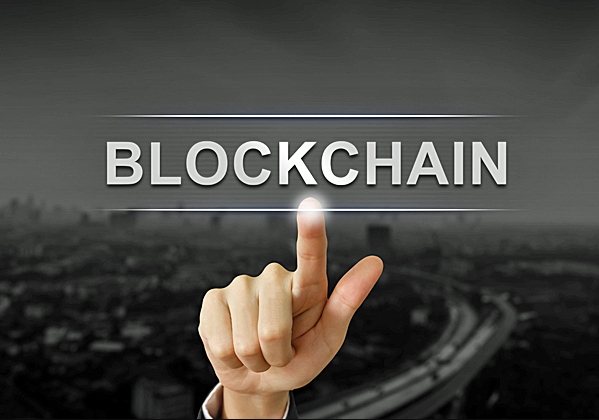
|  |  |
| --- | --- |
| **שם מלא** | **מייל** |
| **כפיר לב** | **kfirb@colman.ac.il** |

**קישור ל-GIT:**

**https://github.com/saharmelechi/VoteChain.git**

**תוכן עניינים:**

1. **תיאור המערכת.**
2. **התבססות טכנולוגית.**
3. **דרישות המערכת.**
4. **ארכיטקטורת המערכת.**
   1. **תיאור מודלים של המערכת.**
5. **תוכנית עבודה.**
6. **צד לקוח (הזנה ואיסוף מידע).**
   1. **הדגמת השימוש במערכת.**
7. **צד שרת (הפצת מידע).**

**מערכת בחירות מבוססת בלוקצ'יין**

# **תיאור המערכת:**

מערכת בחירות מבוססת בלוקצ'יין באה לאפשר תהליך הדורש מצד אחד אנונימיות ופרטיות ומצד שני שקיפות מלאה בתוצאה. הדוגמה הטובה ביותר לבעייה זו הינה תהליך "הבחירות". תהליך זה מצריך מצד אחד חשאיות מלאה בהצבעה, כך שרק המצביע יודע מה הוא הצביע ולמי, אך מן הצד השני ישנו צורך לאגד את תוצאות כל ההצבעות ולא לאפשר בחירה של אדם יותר מפעם אחת.

נחדד קצת את הדברים על ידי דוגמה:

אדם בשם משה קם בבוקר יום הבחירות והולך להצביע, מזדהה בכניסה לקלפי ומכניס את הפתק למעטפה ומשם לקלפי. כאן נגמר תפקידו הלאומי והדמוקרטי לממש את זכות ההצבעה.

מאותו רגע הוא יוצא מהתמונה והצבעתו נתונה בידיו של ה"משקיף על הקלפי" הממונה מטעם משרד הדתות.

השאלות העולות מן המקרה לעיל הן כדלהלן:

1. האם משה יודע בוודאות שהצבעתו באמת משוקללת ונכללת בתוצאות האמת של הבחירות?
2. מי אותו גורם שסופר את הקולות ומכריז על המנצח? האם באמת ניתן לסמוך על הגוף האחראי על ספירת הקולות? האם זוהי באמת דמוקרטיה כאשר יש גוף אחד מנוהל שתפקידו לספור ולהכריז מה המנצח?
3. גם במידה וגוף זה אכן אמין, פסחה הקידמה הטכנולוגית על תהליך חשוב זה, ונשאר התהליך המיושן של "ספירת קולות ידנית"?
4. לא פעם אנחנו שומעים על אנשים המזדהים עם כמה תעודות זהות (כרגע זה הזיהוי היחיד בתהליך הנוכחי) ומצביעים מספר פעמים, מה שכמובן עלול להטות את התוצאה.
5. בתהליך ידני זה נפסלים הרבה קולות מחשש לזיופים וכדומה.
6. ניכר כי הציבור איבד אמון במערכת הבחירות כפי שהיא מתנהלת כיום.

מהשאלות הנ"ל ועוד, נראה שיש צורך רציני באיזושהו תהליך טכנולוגי רציני שיסדיר את הבעיות הנ"ל. במילים אחרות, נדרשת מערכת ממוחשבת מבוזרת שתאפשר, מחד, הצבעה אנונימית לחלוטין, ומאידך, תאפשר לבעל ההצבעה לדעת שקולו נספר בתוצאות ללא חשש לזיופים וללא גוף יחיד שמנהל את התהליך.

מה שמוביל אותנו למסקנה הנדרשת הבאה:

מערכת בחירות מבוססת בלוקצ'יין.

רק נציין שמערכת זו תדע להתמודד גם אם עוד סוגים של בעיות מהסוג הזה כמו מערכת סקרים שגם שם חשובה האנונימיות אך התוצאות אמורות להיות שקופות ללא גוף יחיד מנהל.

**הנחות עבודה:** קיומו של מסד נתונים לזיהוי משתמש בעל זכות הצבעה (טביעת אצבע/ תחנות מאובטחות).

2. **התבססות טכנולוגית:**

בעיה דומה לבעיה המוצגת לעיל קיימת גם בנושא רגיש אחר והוא ה"כסף".

גם שם על מנת לאפשר אמון בסיסי בין שני אנשים זרים שרוצים לקנות ולמכור אחד מהשני, ישנו צורך בגוף מנהל שיאפשר העברת כספים בין אנשים, ניהול החשבון, משיכה הוצאה וכו'.

גוף זה ידוע בכינויו "בנק".

תפקידו של הבנק כפי שהוזכר, הוא לנהל את כספנו ולוודא שבהעברת כסף מאדם אחד לשני, הכסף יירד מחשבונו של האחד ועובר לחשבון השני.

גם בנושא זה ישנן לא מעט בעיות שלא יפורטו במסמך זה, רק נזכיר בקצרה שעבור כל פעולה שאני עושה בחשבוני אני צריך לשלם עמלה. כמו כן כל פעולה שאני מבצע הבנק יודע ורואה כך ששוב אנחנו מגיעים לשאלת השאלות - מה עם פרטיות?

בשנת 2008 הגיח אדם (או קבוצה של אנשים) בשם סאטושי נקמוטו שעד היום לא זוהה (אם כבר מדברים על פרטיות...) והציע פתרון לבעייה זו.

המודל שהוא הציע כלל רשת מבוזרת הנמצאת ב"אין סוף" מחשבים ששומרת טרנזקציות של העברת כסף (ביטקוין). נסביר בקצרה:

1. אדם פותח חשבון (ארנק), כלומר יוצר איזושהי PK ו PBK כך שה-PBK חשוף לכולם ורק בעל PK יכול לאמת את זה שזה אכן ה-PK שלו.
2. מנגון הנקרא בלוקצ'יין מבוזר שתפקידו לשמור את כל העברות הכספים (טרנזקציות) מאז ומעולם.
3. אם ברצוני להעביר כסף לאדם אחר, כל מה שאני צריך לעשות זה לרשום על גבי רשת הבלוקצ'יין ש-PK שלי העביר X כסף ל-PK אחר.
4. בדרך זו על ידי חישוב העסקאות שבוצעו ניתן לדעת בכל רגע נתון כמה כסף יש לכל אחד (לכל PK).

הסבר זה אינו נכנס לכל המנגנון של איך בדיוק נוצר הכסף (הביטקוין) וכיצד מחושבים בלוקים חדשים וכו'. מה שכן חשוב להדגיש הוא, כי נמצא פתרון לבעיה שלא הצליחו לפתור במשך שנים והיא העברת משאב (במקרה הזה כסף) בין אנשים באופן אנונימי לחלוטין תוך וידוא מלא שאדם מסויים, אשר העביר כסף לאדם X, לא יוכל להעביר את אותו כסף לאדם Y וכל זה ללא גוף יחיד המנהל את התהליך.

חשוב לציין שהבעיה שאנחנו באים לפתור (בחירות) שונה באופן מהותי מהבעיה שנפתרה (ניהול כסף) כדלהלן:

1. כיום בטכנולוגיית הבלוקצ'יין כל אחד יכול לפתוח כמות בלתי מוגבלת של ארנקים ולבצע אין סוף טרנזקציות על ארנקים אלו. מה שאין כן אצלנו יש צורך בהצבעה אחת בלבד לכל אדם בעל זכות הצבעה חוקי.
2. במנגנוני בלוקצ'יין יכולים להיווצר שני בלוקים בו זמנית במקומות שונים ברשת. הדבר אמנם נדיר אך יוביל לכך שאחד הבלוקים יפסל בהמשך ואיתו נאבד את ההצבעות הרשומות עליו. יש צורך להתמודד עם האפשרות של פסילת בלוקים.
3. ההצבעה שתירשם בבלוקצ'יין חייבת להיות חתומה אך לא מוצפנת כך שניתן יהיה לוודא שההצבעות לא נערכו על ידי גורם זר. הבעיה היא בבחירת המשתנים שיופיעו בבלוקצ'יין וייחתמו. יותר מדי מזהים עלולים להסגיר את זהות המצביע. פחות מדי מזהים עלולים לתת פתח להצבעות כוזבות מבלי שיהיה ניתן לדעת מי ביצע אותן.
4. כל הצבעה נשענת על הזדהות. פרטי הזהות ניתנים לגניב ועל כן יש צורך להבטיח שפרטי ההזדהות יהיו ברמת אבטחה גבוהה, קשים לזיוף וגניבה ובהינתן שנגנבו, קשים לניצול.
5. מכיוון שמטרת המערכת היא שקיפות, ישנה דרישה שכל מצביע יוכל לזהות את ההצבעה שלו על מנת לוודא שלא גנבו את זהותו. עם זאת, על הבחירות להיות חשאיות ולכן אף אדם או גוף ממשלתי אחר לא צריך להיות עם היכולת לזהות את ההצבעה של אדם פרטי.

3. **דרישות המערכת:**

1. מה קורה אם יש לי אותו HASH בבלוקצ'יין.

הצעה לפתרון: נעשה זיהוי בהתחלה אם היוזר יכול להצביע על ידיי ה API הממשלתי,

לאחר מכן, למסוף יהיה לו מפתח פרטי מתרנדר כל פרק זמן ומביא לנו את המפתח פאבליק קי החדש שככה הבלוקצ'יין יודע שזה סניף נכון על ידיי בדיקת ה HASH (להוסיף תמונה)

שלו, ואם יוזר ירצה לראות מה הוא הצביע הוא יכול לראות באותו מסוף שהוא הצביע.

**כל פקטה בבלוק שנשלח מהמסוף כוללת:**

1. למי הבן אדם הצביע.
2. פרטי המצביע.

**זיהוי יוזר:**

1. תעודת זהות.
2. מסוף הצבעה.
3. למי הצבעתי.
4. טביעת אצבע.
5. מספר סוד פרטי שהוא בוחר על מנת שיוכל לראות את בחירתו במסך השקיפות של הבחירות.

**טכנולוגיות:**

1. בלוקצ'יין.
2. REST API.

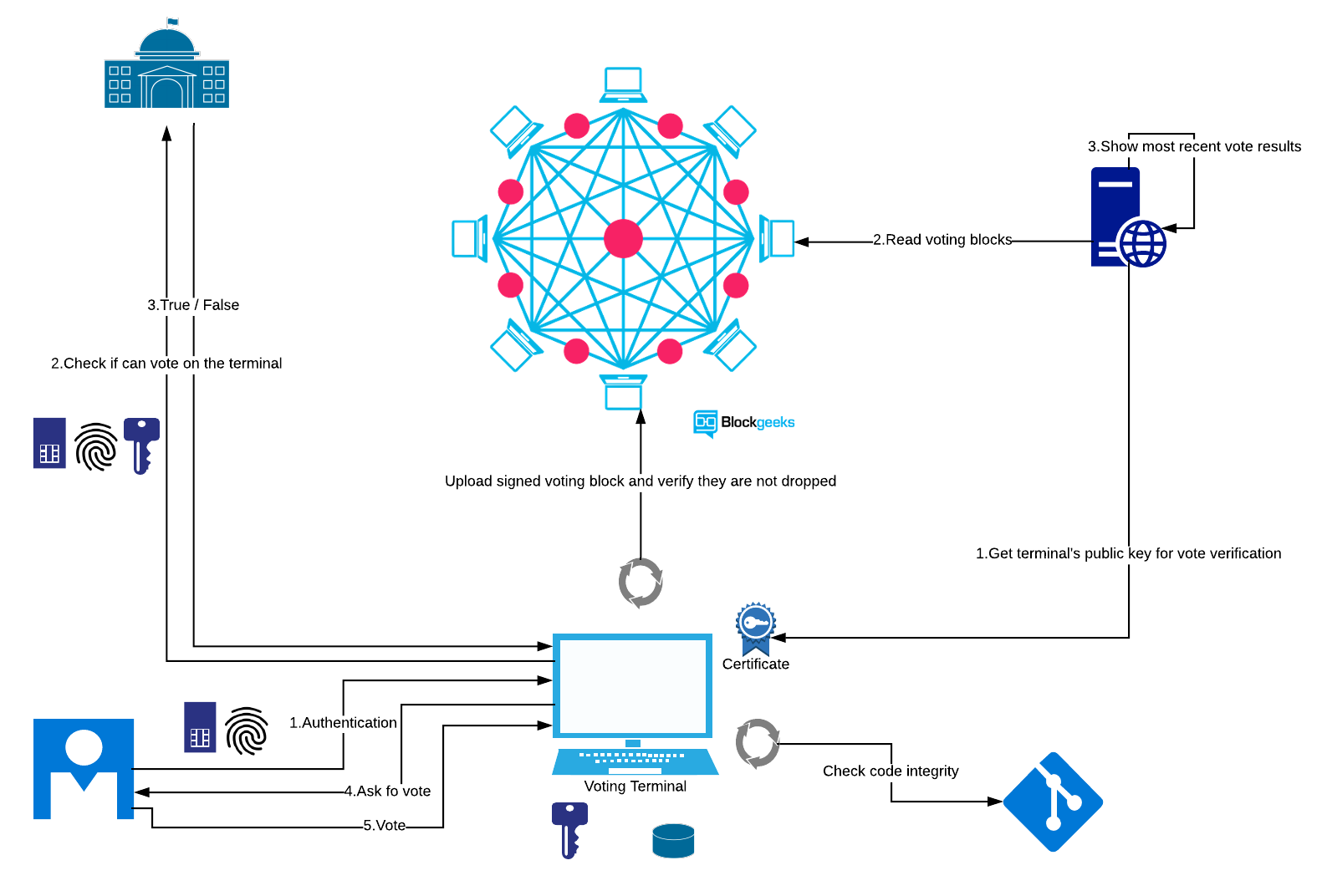
**אתגרים כלליים:**

1. שמירת ההצבעה אנונימית.
2. שקיפות של הבן אדם מה הוא הצביע.
3. טיפול בפסילות של בלוקים שהגיעו ממסופי ההצבעה.
4. טיפול בהצבעות כפולות.
5. אבטחת מסוף ההצבעה.

**תרשים זרימה:**

1. אדם מגיע למסוף הצבעה.
2. אדם מזדהה על ידיי אצבע ותעודת זהות (nfc).
3. API הממשלתי מגדיר את הבן אדם כמזוהה.
4. האדם בוחר הצבעה.
5. ההצבעה נשמרת במסוף ההצבעה, ומועלה לאחר זמן ל- בלוקצ'יין.
6. מסוף ההצבעה מוודא שהבלוק לא נפסל, ואם כן מעלה אותו מחדש.
7. כל אדם יכול לראות מה הוא הצביע, וכן את מצב ההצבעה באתר אינטרנטי או על ידיי בדיקת ההצבעה בבלוקצ'יין.
8. העלאה של מזהי ההצבעה לבלוקצ'יין?.

4. **שרטוט של אופן ביצוע פעולות המערכת:**



## **4.1. פרוט הרכיבים במערכת:**

* מסוף הצבעה רכיב פיזי טאבלט, מבוסס מערכת הפעלה ניידת ומאובטחת בעל יכולות :
  1. חיבור מאובטח לאינטרנט.
  2. קורא טביעות אצבע.
  3. קורא NFC.
  4. יכולת להריץ אפליקציות בסיסיות.
  5. מפתחות PRIVATE PUBLIC צריך להיות צרוב על החומרה.
  6. ארנק של בלוקצ'יין עם סך המקנה לו אפשרות לבצע פעולות.

**המסוף פועל כשרת מקומי המקשר בין משתמש לענן ולו 4 חלקים:**

* מודל בדיקה עצמית - מאפשר בדיקת תקינות מסוף בעל היכולות הבאות:

1. בדיקת המודולים המורצים עליו מול מקור קוד חיצוני (GIT repository) לבדיקה שלא נערכו שינויים בקוד על המסוף והתראה למקרה שכן.

* מודול קישור לבלוקציין - מגשר בין האפליקציה לענן בעל היכולות הבאות:

1. יצירת בלוק לשמירה בלוקצ'יין.
2. שמירה של בלוקי מידע בענן.
3. אימות שמירה של בלוקים בענן.

* מודול קישור ל API ממשלתי:

1. מעביר את הקלט של המשתמש לאימות בשרת,ומקבל ומאשר או דוחה בהתאמה.
2. קורא את אפשרויות ההצבעה.

* מודול קישור ליוזר - מקבל קלט מהיוזר:

1. קורא FNC של זיהוי משתמש.
2. קורא טביעת אצבע של משתמש ומעביר אותם למודול ה-API.
3. קורא הצבעה של המשתמש.

* API ממשלתי חיצוני משמש לשתי מטרות:

1. זיהוי משתמש, המוודא אם לאדם יש יכולת הצבעה במסוף הספציפי שהוא מזוהה בו ברגע הגעתו למסוף והזנת פרטי טביעת אצבע ו NFC.
2. לקבלת מידע פומבי עבור ההצבעה כמו רשימת המועמדים, מועד התחלה וסיום ההצבעה.

* בבלוקצ'יין כשירות ענן:
  + שמירת וקריאה של בלוקי מידע.
  + העברת כסף למסופים על מנת לאפשר את המשך הפעילות שלהם.
* ממשק אינטרנטי להצגת תוצאות הבחירות:
  + אימות תקינות ואבטחת בלוק (ע"י השוואת מפתח הפאבליק קי שהמסוף חושף).
  + ספירת הקולות.
  + הצגת נתוני הבחירות למשתמש בצורה ויזואלית ונוחה.

5. **תוכנית עבודה:**

1. ללמוד בלוקצ'יין.
   1. ארכיטקטורת כללית.
   2. יצירה של בלוקצ'יין פרטי.
   3. כתיבה לבלוקציין באמצעות קוד.
      1. שבועיים, משה מוצא מאמרים וחומרי לימוד ומצוות לכולם .
2. החלטה על כלי הפיתוח האולטימטיביים עבור כל אחד מהרכיבים.
   1. תיעשה ישיבה מסודרת לאחר סעיף 1 .
3. כתיבת ליבת האפליקציה האחראית על כתיבה וקריאה מהבלוקצ'יין.
   1. יחולק בין ירון משה וסהר.
4. יצירת מוקאפ של API ממשלתי.
5. הצלחת מימוש מסוף בחירות על מכשיר בחירות ללא אמצעי אבטחה.
   1. רזיאל.
6. לאבטח את מסוף הבחירות באמצעות מפתחות פומבי/פרטי.
   1. רזיאל.
7. יצירת אתר אינטרנט של נתוני הבחירות אונליין.
   1. סהר / משה.
8. בונוס:

* לבדוק שאדם פרטי יוכל לבדוק דרך אפליקציית המידע שההצבעה שלו נמצאת בענן הבלוקצ'יין והיא אכן תקינה.

# 

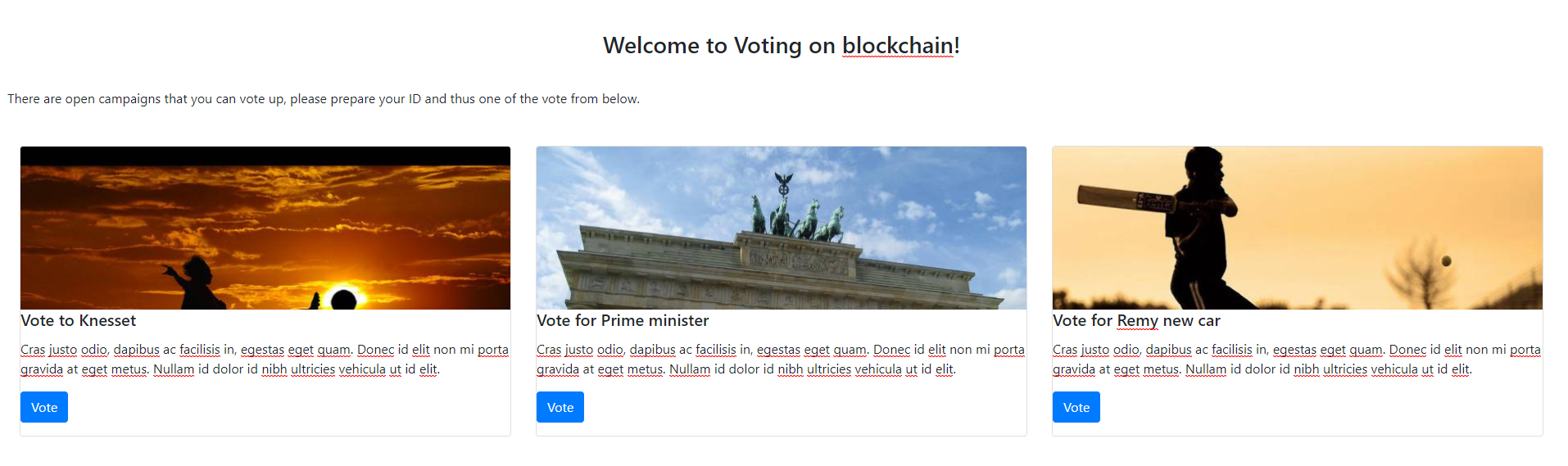
# 

# **6. צד לקוח (הזנה ואיסוף מידע):**

מסוף המשתמש: <http://bit.ly/2Ae1hwc>

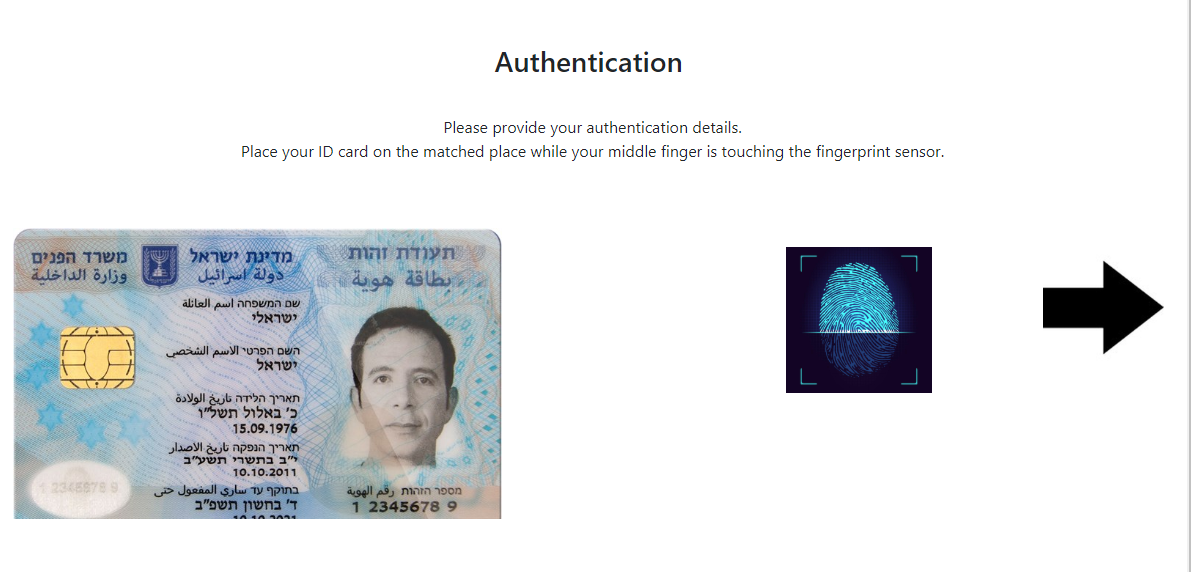
במסוף יהיו 3 מסכים: פתיחה, הזנת פרטים, הצבעה.

מסך פתיחה:

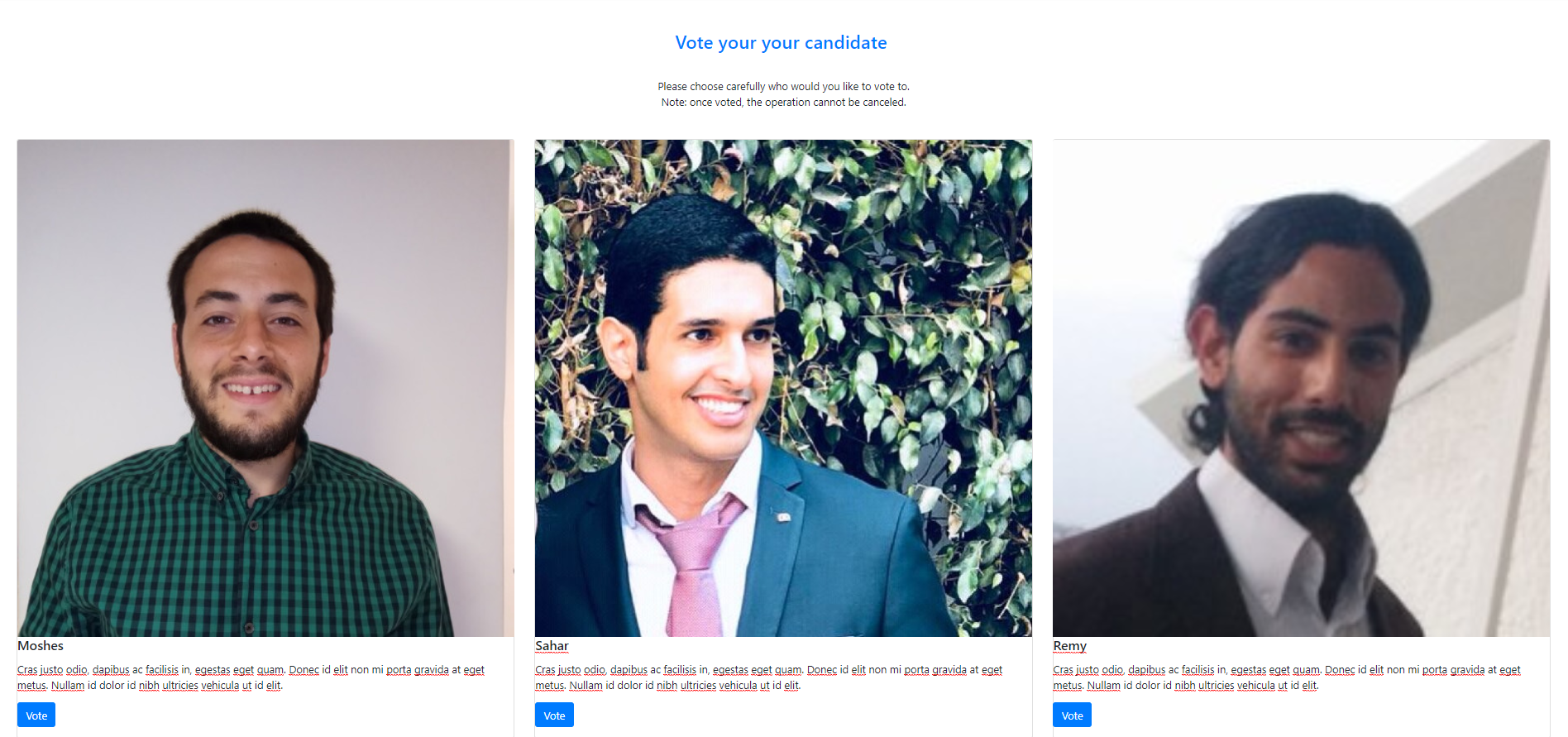


בו משתמש חדש יוכל לבחור את הקמפיין עבורו הוא רוצה להצביע לאחר בחירה, יועבר המשתמש למסך הזנת פרטיו.

**מסך הזנת פרטי המשתמש:**



במקרה שהמשתמש הכניס פרטים שגויים תוצג לו חלונית שתבקש מהמשתמש להזין את פרטיו שנית.

**מסך ההצבעה:**

במסך זה יתבקש המשתמש להזין את המועמד המועדף עליו.

לאחר שיזין, תפתח חלונית אישור שלאחריה הקלט ישמר והמשתמש יקבל הודעה שהצבעתו התקבלה, לאחר כמה שניות הוא יועבר לחלון הראשי.

## 

## 

## 

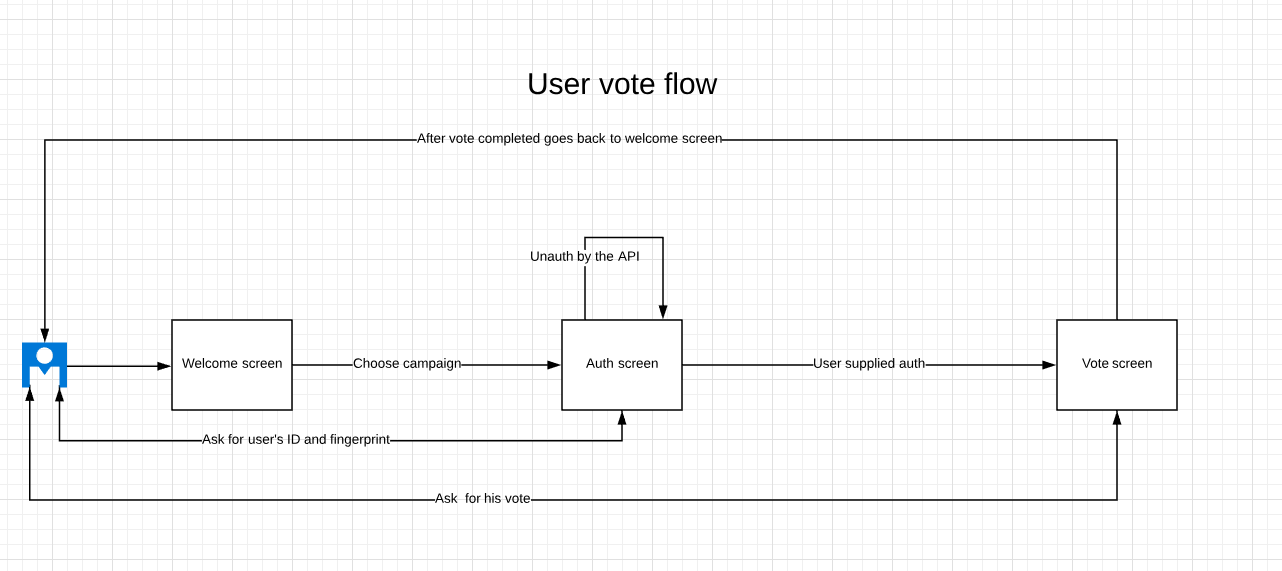
## 

## 

## 

## 

## **6.1. הדגמת מימוש אופן ההצבעה:**



# **7. צד שרת (הפצת המידע):**

אפליקציה שמכילה מסך אחד שבו תינתן בחירה לאיזה קמפיין תינתן ההתפלגות, ולאחר הבחירה תוצג התפלגות ההצבעות הזמן הנתון. המסך יתעדכן כל רבע שעה.