

## זהות בריבונות עצמית בעולם גלובלי: מערכות זיהוי מבוססות-אישורים בתור מנוע להכללה חברתית\*

מאת

פאני וונג ופרימברה דה פיליפי\*\*

אחרי הצגת מושגי מפתח והגדרות בסיסיות בתחום הזהות הדיגיטלית, מאמר זה יבחן את היתרונות והחסרונות במערכות זיהוי קיימות בדרך להשיג זהות בריבונות עצמית. הוא יבחן במיוחד את השימוש בטכנולוגיית בלוקצ'יין ובוזיוני ביומטרי בתור אמצעים להבטיח "ייחודיות" (unicity) ו"יחידות" (singularity) של זהויות, ואת האתגרים הקשורים לכך בנוגע לאבטחת מידע אישי וסודיותו. לאחר מכן יתאר המאמר גישה חלופית לזהות בריבונות עצמית שמבוססת על מערכת של הוכחות, של הצהרות, של אישורים ושל הרשאות מבוססי-בלוקצ'יין בעלי ניידות כוללת לאורך חייו של אדם. אומנם אישורים והוכחות אינם תלויים בממשלה כלשהי או בארגון מסוים לצורך ניהול ולגיטימיות, אולם הם עשויים לכלול – בין סימנים רבים לזהות – אמצעי זיהוי וזיהוי ביומטרי שהוציאה מדינה. פתרון כזה – שמבוסס על היסטוריה דיגיטלית

\* תרגום המאמר "Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion", 2 *Frontiers in Blockchain* (2020), <https://bit.ly/31AsWbm>. תרגום: מתן גולדבלט.

\*\* פאני וונג היא עורכת דין ויזמית, מכהנת כיום בתפקיד סגנית ליועץ המשפטי (Associate General Counsel) בקרן Maker, שתומכת במיזם הבלוקצ'יין MakerDAO. היא ממקימי ixo, פרטוקול בלוקצ'יין להפיכת תוצאות השפעה חברתית לנכסים דיגיטליים באסימונים. היא החלה את הקריירה שלה כבול סטריט ואחר כך עבדה בעריכת דין בניו יורק ובלונדון. היא קיבלה תואר במשפטים מאוניברסיטת קולומביה, ואת התארים הראשונים שלה – מאוניברסיטת קליפורניה בברקלי. היא זמינה בכתובת [fennie@makerdao.com](mailto:fennie@makerdao.com). פרימברה דה פיליפי היא חוקרת בתחום המשפט. עבודתה מתמקדת באתגרים המשפטיים שמציבה טכנולוגיית הבלוקצ'יין ובהזדמנויות המשפטיות שהיא מציעה. היא חוקרת קבועה ב-CNRS, עמיתה במרכז ברקמן-קליין לאינטרנט, חברה באוניברסיטת הרווארד וממקימי הקואליציה ליישומים משפטיים ממוכנים (Coalition for Automated Legal Applications) (COALA). היא זמינה בכתובת [pdefilippi@cyber.harvard.edu](mailto:pdefilippi@cyber.harvard.edu). המחברות מודות לקווין או'בריאן (Kevin O'Brien) ולארון גולדסמיד (Aaron Goldsmit) מקיווה (Kiva), להומאן חדד (Houman Haddad) מתוכנית המזון העולמית ולניק ויליאמס (Nick Williams) מסמפו (Sempo) על תובנות ומשוב שלא יסולאו בפז, ולגאורגי ישמאיב (Georgy Ishmaev) על הערותיו לגרסה מוקדמת של המאמר.

מתועדת וחתומה של תכונות ופעילויות – מתקרבת במידה הרבה ביותר לנזילות ולריבוי הפנים של הזהות. הדבר מאפשר לפרטים לבטא רק היבטים מסוימים של זהותם, לפי אלו שעומים ברצונם להתקשר. להדגמת הקשיים שטבועים ביישום זהות בריבונות עצמית בעולם האמיתי, המאמר יתמקד בשני פתרונות זיהוי מבוססי-בלוקצ'יין בתור מקרי מבחן: (1) נוהל הזיהוי קיווה (Kiva) ליצירת היסטוריית אשראי בסיירה לאון; (2) תוכנית "אבני בניין" (Building Blocks) של "תוכנית המזון העולמית" להעברת סיוע במזומן לפליטים בירדן. לסיום, המאמר יבחן כיצד השילוב של מטבעות מבוזרים מבוססי-בלוקצ'יין וזהות בריבונות עצמית עשוי לתרום לקידום הכללה כלכלית רבה יותר. אם עסקאות דיגיטליות יפעלו בתור הצהרות זהות במערכת גומלין המבוססת על זהות בריבונות עצמית, עשויים לצמוח דגמים חדשים לעסקים, כמו תוכניות לביטוח זהות, ולצידם מטבעות מבוזרים בעלי ערך קבוע (מטבעות יציבים) שימשו הליך חוקי מקומי.

**א. הקדמה למערכות לניהול זהות;** 1. הגדרות מקדמיות; 2. יחסי הגומלין בין מזהים, אישיות וזוגות מפתחות ברשת; 3. מערכת זיהוי ריכוזית המבוססת על מזהים ייחודיים לעומת רשת אמון רבת-פנים של מערכת הצהרות אמון ואישורים. **ב. תפקיד הזהות בהכללה חברתית-כלכלית.** ג. יתרונות במערכות זיהוי ביומטריות והסיכונים בהן; 1. תשתית מבוזרת לעומת משמורת ריכוזית על מפתחות; 2. זיהוי לעומת אימות; 3. שליטה אישית במידע אישי לעומת שליטה ארגונית בו; 4. נתונים ביומטריים לעומת סוגי מזהים אחרים. **ד. זהות בריבונות עצמית ומערכות לניהול אישורים;** 1. זהות דיגיטלית בקוד פתוח ותקנים ברשת להצהרות בנות אימות; 2. מפת דרכים לקראת זהות בריבונות עצמית. **ה. מקרה בוחן – קיווה: פתרון לצורך נתוני אשראי;** 1. ארכיטקטורת פרופיל קיווה; 2. לעבוד עם פרופיל קיווה: צעד אחר צעד; 3. שיקולי פרטיות לעומת בעיית הגילוי הֶבְרָתִי. **ו. מקרה בוחן – תוכנית המזון העולמית: פתרון לצורך מיטוב של תוכניות סיוע בין סוכנויות או"ם והתאמתן זו לזו;** 1. אבני בניין; 2. יישום בירדן; 3. הצעדים הבאים. **ז. נקודות מבט עתידיות;** 1. תלות הריבונות העצמית בתשתית טכנולוגית; 2. כסף דיגיטלי והחשיבות של זהות בריבונות עצמית; 3. ביטוח זהות בתור אמצעי ביטחון ומקור הכנסה לספקי זהות? **ח. סיכום.**

## א. הקדמה למערכות לניהול זהות

בחלק זה נציג מערכת עקרונות ומושגים בעולם הזיהוי, בייחוד בנוגע לטכנולוגיות ליישום מערכות לניהול זהות, כמו תקני המרשתת (web standards), קריפטוגרפיה, יומני בלוקצ'יין ויישומי מטבעות מבוזרים.

## 1. הגדרות מקדמיות

בימינו קיים בלבול רב בעולם הזיהוי בנוגע למונחים בסיסיים מסוימים, כמו "זהות" ו"מזהה", "מאפיינים" ו"אישיות". לעיתים קרובות משתמשים בהם לחלופין ובעמימות בלי להגדיר כראוי את המשמעות של כל מונח ואת היקפו. אנו עורכות כאן הבחנה מקדמית בין המונחים הללו ומספקות לצידה הגדרה טנטטיבית שנשתמש בה בהמשך המאמר.

ל"זהות" (identity) ניתנו הגדרות שונות לפי תחום המחקר. בפסיכולוגיה משתמשים במונח זה בדרך כלל לתיאור כל המאפיינים הפסיכולוגיים של אדם, כולל אישיות, אמונות ותכונות אישיות אחרות.<sup>1</sup> בסוציולוגיה הוא כולל את התרבות, ההיסטוריה, הדת והמסורת שאדם משתייך אליהן.<sup>2</sup> מנקודת מבט משפטית זהות עשויה להתקשר למושג של "אדם טבעי" (כלומר בן אדם ממשי) או ל"אישיות משפטית" (שעשויה להיות חברה, נאמנות, שותפות או איגוד אחר של אנשים שמזוהה מבחינה משפטית בתור יחיד).

לצורכי מאמר זה אנו משתמשות במונח "זהות" לתאר את כל התכונות של אדם שמגדירות אותו הגדרה ייחודית במהלך חייו, שמספקות מהות זהה (sameness) והמשכיות למרות שינוי בהיבטים ובתנאים. כך, אנו מבחינות בין המובן "זהות מספרית" (numerical identity), שמתאר את מערכת היחסים שקיימת בבלעדיות בין דבר לעצמו,<sup>3</sup> למובן "זהות איכותית" (qualitative identity), שמתאר רק את התכונות המשותפות לדברים שונים:<sup>4</sup> רק אם שני דברים זהים לחלוטין מבחינה איכותית, אפשר להתייחס אליהם כאל זהים מבחינה מספרית.

אולם גם בהקשר של זהות מספרית חשוב לציין כי מאפייני הזהות עשויים להתפתח במהלך הזמן. גיבוש זהות הוא תהליך מתמשך שבו זהותו של אדם משתנה במהלך השנים ומתפתחת בקביעות בעקבות פעילות הגומלין עם הסביבה.<sup>5</sup> לפיכך הזהות דינמית ורב-פנים, ולכן יש לתכנן כל מערכת לניהול זהות כך שתהיה גמישה, עמידה ודינמית דייה להתאים עצמה לטבע המשתנה והמורכב של הזהות האנושית. אולם על אף התחכום של מערכות אלו שום מערכת לניהול מידע לא תוכל אי פעם לתפוס לחלוטין

- 
- 1 Nina Strohminger, Joshua Knobe & George Newman, "The True Self: A Psychological Concept Distinct from the Self", 12 *Persp. on Psychol. Sci.* (2017) 551
  - 2 James E. Côté, "Sociological Perspectives on Identity Formation: The Culture-Identity Link and Identity Capital", 19 *J. Adolescence* (1996) 417
  - 3 כפי ששמה רומז, זהות מספרית מתארת את היחס שבאמצעותו אפשר למנות דברים: אפשר למנות את א ו-ב בתור אותו דבר רק אם הם זהים מבחינה מספרית. Peter Geach, "Ontological Relativity and Relative Identity", *Logic and Ontology* (Milton K. Munitz ed. 1973) 287
  - 4 Brian Garrett, *Personal Identity and Self-Consciousness* (2002)
  - 5 Paul John Eakin, *How Our Lives Become Stories: Making Selves* (1999)

את כל ההיבטים של הזהות העצמית. אכן, אם אנו מנסות לתכנן מערכת לניהול מגוון זהויות שונות ולסיווגן, חשוב להבין מראש שסיווג זה יהיה בהכרח צמצום של פן מסוים או תרחיש שימוש מסוים של כל זהות.<sup>6</sup>

"אישיות" היא פן מסוים של זהות שבא לידי ביטוי בהקשר מסוים. הזהות מגדירה אדם הגדרה ייחודית, אולם אותו אדם עשוי להיות בעל כמה אישיות לפי ההקשר החברתי הנדון.<sup>7</sup> לדוגמה, אליס היא אם מסורה לבתה ורעיה אוהבת לבעלה. היא חברה נאמנה לכמה מעמיתיה ומנהלת קשוחה לעובדיה. כל האישיות האלו הן חלק מאותה זהות, אולם הן עשויות להציג מאפיינים שונים מעט או תכונות פסיכולוגיות אחרות קמעא. מנקודת מבט טכנית אפשר לתאר אותן בתור שמות עט או זהויות מעשיות.<sup>8</sup> "זהות" היא מושג מופשט שמתייחס לפרט כולו, ואילו אישיות היא מרכיב הכרחי בכל מערכת לניהול זהות משום שהיא מתייחסת לאופן שבו פרטים "מאמתים" עצמם כלפי המערכת.<sup>9</sup>

"מאפיין" מתאר תכונה הכרחית ומגדירה של אדם שמכשירה אותו להיות חבר בקבוצה (או סוג) של אנשים. כך, מאפיין לרוב אינו מיוחד לאותו אדם. לכל אדם עשויים להיות אין-ספור מאפיינים: גורמים – כמו מגדר, גובה, משקל, מוגבלויות ויכולות – שטבועים באותו אדם או גורמים – כמו לאום ואזרחות – שניתנו (ועשויים להילקח) בידי צד שלישי כדי להבחין בין אנשים לפי קטגוריות מסוימות (למשל אזרחות אמריקנית לעומת צרפתית) או לארגן אותם לפיהן. כמובן, רוב הקטגוריות הללו הן סיווגים מופשטים שניתן להגדירם בשרירותיות, גם אם הם מתייחסים לתכונה טבועה. חשבו לדוגמה על המאפיין "גי'נג'יות", שהופך אדם לחבר בקבוצת הג'ינג'ים. כמובן, זה מאפיין טבעי שאינו ניתן לביטול, אולם את הסיווג "גי'נג'ים" אפשר להגדיר בשרירותיות-מה (איזה גוון מדויק של כתום הופך אישה לגי'נג'ית?). בדומה לזה, הקטגוריה "מגדר", שהוגבלה במשך זמן רב ל"גבר" או "אישה", מתרחבת לאחרונה עם התגלותם של אלו שזהותם "לא בינארית". לבסוף, תכונה עיקרית של מאפיינים היא שהואיל ומטרתם לסווג ישות לקטגוריה מסוימת, הם אינם ייחודיים לה: ישויות רבות חולקת אותם מאפיינים.

6 הגורם העיקרי לכך הוא הפער בין ידיעה ממקור ראשון של העצמי לידע מגוף שלישי של אדם באמצעות תיאור.

7 John R. Suler, "Identity Management in Cyberspace", 4 *J. Applied Psychol. Stud.* 455 (2002).

8 John Christman, "Social Practical Identities and the Strength of Obligation", 44 *J. Soc. Phil.* (2013) 121.

9 Kal Toth & Mahesh Subramaniam, "The Persona Concept: A Consumer-Centered Identity Model", 3rd *International Workshop on Emerging Applications for Wireless and Mobile Access (MobEA)* (2003).

לעומת זאת "מזהה" לא נועד לתאר אדם או להכשיר אותו להיות חבר בקבוצה, אלא לשמש "הפניה" לזהות בעולם האמיתי (או לאישיות מסוימת). כך, בדרך כלל צד שלישי מקצה (באקראי) מזהים בהתייחס לתרחיש שימוש או למתחם (למשל שם משפטי של אדם, מספר זהות או שם משתמש). במקרים אחרים מזהים עשויים להיות ייצוג מסוים של תכונה ניתנת להבחנה או של ישות (כמו טביעות אצבע או מידע ביומטרי אחר). חשוב לציין שמנקודת מבט טכנית לחלוטין גם מאפיינים וגם מזהים הם מחרוזות מידע שאפשר להשתמש בהן בתור אמצעי לאימות אדם מסוים (או אישיות מסוימת). לפי המתחם הנדון, אפשר להשתמש באותה מחרוזת מידע כדי להכשיר ישות לחברה בקבוצה, להבחין אותה מחברות בקבוצות אחרות או לזהות אותה זיהוי חד-חד-ערכי באותה קבוצה. אולם מאפיינים ומזהים נבדלים אלה מאלה במטרתם: מאפיין (בהיותו "מכשיר לחברות") נועד לסווג אנשים בקטגוריה מסוימת, ואילו מזהה (בהיותו "הפניה") מיועד לזהות מישהי במתחם מסוים. על כן אף שכמה מערכות לניהול זהות מאפשרות לפרטים רבים לחלוק אותו מזהה (למשל פרטים רבים חולקים שם זהה) או לפרט אחד להיות בעל יותר ממזהה אחד (למשל שמות עט), הרי שכדי להקל את הליך ההזדהות והאימות רצוי לרוב שמזהה יוכל לזהות אדם זיהוי ייחודי ושאינו משתמע לשתי פנים.<sup>10</sup> לכן מערכת לניהול זהות נדרשת למלא שני תנאים בסיסיים לפחות: (1) לשני אנשים לא יהיה אותו מזהה (ייחודיות, unicity); (2) לאדם אחד לא יהיו יותר ממזהה אחד (יחידות, singularity) באותו מתחם.

לנוכח האמור רוב המזהים מורכבים ממחרוזות מקרית של תווים ייחודיים במתחם מסוים. לרוב מפיקה אותם רשות ריכוזית, כגון סוכנות ממשלתית או גוף מנהלי, כמו באשר למספר דרכון או למספר זהות; או חברה או ארגון, כמו באשר לחשבון בנק או לכתובת דוא"ל. בהקשר הזה הריכוזיות מסייעת להבטיח מידה של ביטחון בכך שהמזהה ייחודי (למשל שאותו מספר תעודת זהות לא הוקצה לשתי נשים שונות) ויחיד לזהות אחת (כלומר שלאיש אין יותר ממספר זהות אחד).

לחלופין, אדם יכול להפיק במישרין מזהה, כמו זוג מפתחות קריפטוגרפיים שמאפשרים גישה לארנק של מטבע מבוזר. במקרה זה מבטיחים ייחודיות באמצעות מתמטיקה – לפחות ברמה גבוהה של הסתברות,<sup>11</sup> אבל אי אפשר להבטיח יחידות (כלומר אותו אדם יכול להפיק יותר ממזהה אחד). בדומה לזה, מזהים מבוזרים (decentralized identifiers, DIDs) הם תקן קוד פתוח מבוסס-רשת אשר משתמש בכתובת

Audun Jøsang & Simon Pope, "User Centric Identity Management", *AusCERT Asia Pacific Information Technology Security Conference 77* (A. Clark, K. Kerr & G. Mohay eds., 2005)

Peter Schartner & Martin Schaffer, "Unique User-Generated Digital Pseudonyms", *Unique User-Generated Digital Pseudonyms* (Vladimir Gorodetsky, Igor Kotenko & Victor Skormin eds., 2005) 194

רשת (URL) בתור מזהה ייחודי שמכיל מידע מזהה ציבורי על מושא הזהות או שמפנה למידע זה. המידע המזהה הציבורי שמקושר למזהה המבוזר עשוי לכלול אישורים או הוכחות שזמינים לצפייה ציבורית, או את המפתח הציבורי או הכתובת הציבורית של ארנק של מטבע מבוזר. כך אפשר להשתמש במזהים המבוזרים בצוותא עם טכנולוגיית בלוקצ'יין ועם זוגות מפתחות ציבורי-פרטי.<sup>12</sup>

לסיום, פיתוחים טכנולוגיים מהעת האחרונה אפשרו לפתח מזהים ביומטריים שקשורים במישרין לגשמיות של אדם, כמו טביעות אצבעות, סריקת קשתית העין או זיהוי פנים. בניכוי שגיאות ואי-דיוקים אפשריים שקשורים לטכנולוגיה,<sup>13</sup> למזהים ביומטריים מייחסים לעיתים קרובות **ייחודיות ויחידות** כלפי זהות אחת. אולם תבניות ביומטריות מוגבלות בכך שגם כלי הסריקה המתוחכמים ביותר מספקים רק ייצוגים מקורבים.<sup>14</sup> קושי זה מרוכך במידת מה בכלים ביומטריים רבי-אופנים (סריקת קשתית בשילוב טביעות אצבעות, זיהוי פנים וכולי) שמספקים רמת נדירות גבוהה יותר.<sup>15</sup> בסופו של דבר הכול תלוי בגודל קבוצת האוכלוסייה:<sup>16</sup> אם האוכלוסייה מצומצמת, אפשר לומר שמזהים כאלה ייחודיים אף שעולות בעיות קשות של פרטיות (פרטים נוספים על כך להלן).

## 2. יחסי הגומלין בין מזהים לאישויות ולזוגות מפתחות ברשת

במרשתת המזהה הבסיסי ביותר בשכבת הרשת הוא כתובת ה-IP, שמאפשרת לנתב חבילות מידע ממכונה אחת לאחרת עד שהן מגיעות למכונה הנכונה. כתובת ה-IP אינה מוסרת מידע כלשהו על המכונה שהיא מתייחסת אליה (כלומר היא אינה מאפיין שלה),

Alexander Mühle, Andreas Grüner, Tatiana Gayvoronskaya & Christoph Meinel, "A Survey on Essential Components of a Self-Sovereign Identity", 30 *Computer Sci. Rev.* (2018) 80.

Hugo Proença & Luís A. Alexandre, "Iris Recognition: Analysis of the Error Rates Regarding the Accuracy of the Segmentation Stage", 28 *Image & Vision Computing* (2010) 202; Jim Canham, "Biometrics: Leap of Faith or Fact of Life?", *Biometric Tech. Today* (2018) 8.

Abhishek Nagar, Karthik Nandakumar & Anil K. Jain, "Biometric Template Transformation: A Security Analysis", 2 *Media Forensics and Security* (Nasir D. Memon et al. eds., 2010).

Arun Ross & Anil K. Jain, "Multidimensional Biometrics: An Overview", 3 *12th European Signal Processing Conference* (2004) 1221.

Nicolae Duta, "A Survey of Biometric Technology Based on Hand Shape", 42 *Pattern Recognition* (2009) 2797.

אולם במקרים מסוימים אפשר לקשר כתובת IP לאדם מסוים או לארגון מסוים שאותו זהותם ניתן לגלות באמצעות ספק שירותי האינטרנט (ISP).<sup>17</sup>

בשכבת היישום חשבונות משתמשים וסימאות משמשים לזיהוי אישיות מסוימת (שעשויות להיות אנשים, חברות, מכונות או ישויות אחרות) שפועלות זו מול זו בשירות מקוון. אלו אינם מספקים מעצם טיבם מידע אישי כלשהו על האישיות, אולם ספקי שירות מקוון רבים דורשים מהמשתמשים למסור מאפיינים או מזהים נוספים (למשל שם אמיתי וגיל) כדי להבטיח שרק לפרטים מותרים תהיה גישה לרשת.

עם זאת ראוי לציין שהן באשר לכתובת IP והן באשר לחשבון משתמש, רק חלק מהמזהים הללו יתייחסו לאדם בשר ודם. בפועל המזהים הללו מתייחסים רק לנקודת קצה מסוימת שמתקשרת עם שירות מקוון, אבל לא בטוח שאפשר לקשר את נקודת הקצה הזו קישור ייחודי לזהות מסוימת. למשל אנשים רבים עשויים להשתמש בכתובת IP אחת, ובחשבונות משתמש רבים שולטים היום בוטים ולא אנשים.

בהקשר של מערכת מבוססת-בלוקצ'יין מזהים מנוהלים ככלל באמצעות זוגות מפתחות ציבורי-פרטי, שמזהים את בעל הארנק זיהוי ייחודי.<sup>18</sup> אולם גם הם אינם מוסרים מידע מזהה אישי כלשהו על האדם, אלא אם כן מקשרים אליהם מידע נוסף.<sup>19</sup> לכן אותה ישות (אדם, מחשב או בוט) עשויה להיות בעלים של זוגות מפתחות רבים או לשלוט בהם, שכן זוגות מפתחות אינם מתייחסים בהכרח לזהות מסוימת. למשל, למרי יש זוג מפתחות לארנק הביטקוין שלה וזוג מפתחות אחר לארנק האתר שלה.

מנקודת מבט טכנית זוגות מפתחות ציבורי-פרטי מוכיחים הן החזקה במטבע מבוזר או נכס אסימוני (tokenized asset) שמוחזקים בכתובת דיגיטלית מסוימת או ארנק, והן בעלות בו. המפתח הפרטי הכרחי להוצאתן לפועל של עסקאות לכתובת הבלוקצ'יין שמזוהה בידי המפתח הציבורי, וממנה. עסקה אינה רק העברת נכס מבוזר כמו ביטקוין או אתר, אלא עשויה לייצג גם העברה או הנפקה של אסימון קריפטוגרפי באמצעות עסקה בחוזה חכם.<sup>20</sup> דוגמה לכך היא אסימון לגישה למידע שהבעלים של סל נתונים

17 האסדרה הכללית להגנת מידע של האיחוד האירופי (General Data Protection Regulation, Regulation (EU) No. 2016/679 of the European Parliament and of the Council, 2016 O.J. (L 119) 1) מציינת שיש לראות בכתובות IP מידע אישי במובן שלספק יש תיעוד של כתובת ה-IP והוא יודע למי היא הוקצתה. ראו פרט 30 לפתיח, שמבהיר מהו "מזהה מקוון" (online identifier) הנזכר בהגדרת מידע אישי בסעיף 4: "Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers"

18 Primavera De Filippi & Aaron Wright, *Blockchain and the Law: The Rule of Code* (2018).

19 Elli Androulaki et al., "Evaluating User Privacy in Bitcoin", *Financial Cryptography and Data Security* (Ahmad-Reza Sadeghi ed., 2013) 34

20 Aaron Wright & Primavera De Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia" (2015), <https://bit.ly/338kMb1>

(כמו רשומות רפואיות או נתוני אשראי) מנפיק לצד שלישי המעוניין לגשת לחלק מהמידע. האסימון פועל כמו מפתח לחנות המידע, ועסקאות באסימון הזה נרשמות ביומן בלוקצ'יין כדי לתעד למי ניתנו היתר וגישה.<sup>21</sup>

בבלוקצ'יין ציבורי ונטול הרשאות,<sup>22</sup> כמו ביטקוין או את'ריום, שפועל בלי רשות ריכוזית או מפעיל ביניים,<sup>23</sup> הצמתים שמשמרים את הרשת (למשל ה"כורים") פועלים בלי קשר לזהות נתונה מסוימת.<sup>24</sup> בבלוקצ'יין דורש הרשאות, שבו ישות ריכוזית או מְאָגֵד (קונסורציום) ריכוזי אחראים לזהות את הצמתים (nodes) שמנהלים את יומן הבלוקצ'יין או לפקח עליהם, זוגות המפתחות שנשלטים בידי כל כורה מקושרים בדרך כלל לזהויות בעולם האמיתי.<sup>25</sup> הסתמכות על זהויות בעולם האמיתי מספקת את היכולת הנוספת לפקח (ולהעניש), ובכך מאפשרת לבלוקצ'יינים דורשי הרשאות לוותר על כמה אמצעי אבטחה שבלוקצ'יינים נטולי הרשאות אנונימיים (או בשמות בדויים) חייבים לנקוט, כמו מערכת מבוססת-עבודה (Proof of Work) או מערכת מבוססת-השקעה (Proof of Stake).<sup>26</sup> אזהרה נדרשת היא, שעל המשתמשים לבטוח בנוהלי הממשל של הישות המרכזית או המאגד המרכזי שמפקחים על הבלוקצ'יין דורש ההרשאות.<sup>27</sup>

### 3. מערכת זיהוי ריכוזית המבוססת על מזהים ייחודיים לעומת רשת אמון בת-פנים של מערכת הצהרות אמון ואישורים

כאמור לעיל, עקרונות המפתח של כל מערכת זהות שפועלת כהלכה הם תכונות ה"ייחודיות" וה"יחידות". הייחודיות מתייחסת לעובדה שכל מזהה משמש לזיהוי ייחודי

- 
- Damiano Di Francesco Maesa, Paolo Mori & Laura Ricci, "Blockchain Based Access Control", *Distributed Applications and Interoperable Systems* (Lydia Y. Chen Hans P. Reiser eds., 2017) 206. 21
- בלוקצ'יין "נטול הרשאות" (permissionless) הוא בלוקצ'יין שכל אחת יכולה להצטרף אליו, ושבו כל צימת (node) רשאי לקרוא את המצב העדכני של הבלוקצ'יין ולהוסיף בלוקים חדשים לבלוקצ'יין. לעומת זאת בלוקצ'יין "ציבורי" מתייחס רק ליכולת לקרוא את הבלוקצ'יין, בין שהוא דורש הרשאות ובין שהוא נטול הרשאות, לפי הזכויות להוסיף מידע לבלוקצ'יין. 22
- Primavera De Filippi & Benjamin Loveluck, "The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure", *5 Internet Pol'y Rev.* (2016). 23
- Samia El Haddouti & M. Dafir Ech-Cherif El Kettani, "Analysis of Identity Management Systems Using Blockchain Technology", *2019 International Conference on Advanced Communication Technologies and Networking* (2019). 24
- Thomas Hardjono & Alex Pentland, "Verifiable Anonymous Identities and Access Control in Permissioned Blockchains" (2019), <https://bit.ly/3pR8N9F>. 25
- David Shrier, Weige Wu & Alex Pentland, *Blockchain & Infrastructure (Identity, Data Security)* (Mass. Inst. of Tech. 2016). 26
- Sinclair Davidson, Primavera De Filippi & Jason Potts, "Economics of Blockchain" (2016), <https://bit.ly/3DymLBX>. 27



של פרט אחד (ורק אחד), כלומר לשני אנשים לא יהיה אותו מזהה. יחידות מתייחסת לעובדה שלכל פרט יש מזהה אחד (ורק אחד) במתחם מסוים, כלומר שני מזהים לא יתייחסו לאותו פרט.

אפשר להשיג ייחודיות בלי רשות ריכוזית, משום שפרימיטיביים (primitives) מתמטיים יכולים להבטיח ששני אנשים לא יקבלו אותו מזהה גם אם אין רשות מרכזית שמתאמת את המזהים. כל ספקית זהות רשאית לנפק מזהה בעזרת מספרים מקריים גדולים מאוד, ואף שקיימת אפשרות רעיונית ששני גורמים ינפקו אותו מזהה למוטבות שונות, ההסתברות לכך נמוכה עד כדי זניחה.

לעומת זאת כדי למלא את דרישות היחידות, רוב מערכות הזהות הקיימות מסתמכות על רשות מרכזית כדי לוודא שכל מזהה ייחודי שאינו משתמע לשתי פנים מחובר לזהות יחידה.<sup>28</sup> על הרשות הריכוזית לאסוף מידע אישי כדי להבטיח את היחידות של כל מזהה שהונפק למערכת. מערכת כזו היא לרוב יקרה וביוורוקרטית, ונראה שאינה מעשית מבחינה פוליטית כשמדובר בתרחיש שימוש של מהגרים (בעיקר קבוצות אוכלוסייה פגיעות שנמצאות בתנועה), והיא נתונה לסיכונים חמורים בתחומי הפרטיות, שימוש לרעה במידע ואבטחת מחשבים.<sup>29</sup> לדוגמה, ב-2012 הודו השיקה את מערכת ניהול המידע Aadhaar והשתמשה במידע ביומטרי לזיהוי 1,300,000,000 תושביה – לרבים מהם אין אמצעי זיהוי רשמי.<sup>30</sup> השתתפות במערכת Aadhaar הוצבה בפני ההודים בתור דרישה מוקדמת כדי לקבל קצבאות רווחה, לעשות מגוי לטלפון נייד או להירשם לבית ספר. אולם מערכת כזו העלתה חששות בקרב ארגוני זכויות אדם,<sup>31</sup> והוגשו עתירות רבות לבית המשפט העליון של הודו בשאלה אם המערכת מפירה את הזכות החוקתית לפרטיות.<sup>32</sup>

במצב הרצוי מערכת זהות אמורה להתאים לאופי רב-הפנים של הזהות ולבחון את המאפיינים ואת האישויות השונים, על פי המקרה. בפועל רק מספר קטן מאוד של תרחישי שימוש דורש קשר ייחודי ויחיד בין פרט למזהה שלו (כלומר שפרט יזוהה בידי

- 
- Hemangi Kulkarni et al., "Unique ID Management", 3 *Int'l J. Computer Tech. & Applications* (2012) 520 28
- Edgar A. Whitley & Gus Hosein, "Global Identity Policies and Technology: Do We Understand the Question?", 1 *Global Pol'y* (2010) 209 29
- Swagato Sarkar, "The Unique Identity (UID) Project, Biometrics and Re-Imagining Governance in India", 42 *Oxford Dev. Stud.* (2014) 516 30
- Anil K. Jain & Karthik Nandakumar, "Biometric Authentication: System Security and User Privacy", *Computer* (2012) 87 31
- מאז 2012 הוגשו יותר מ-30 עתירות על מערכת Aadhaar, וחוקתיותה נתקפה שוב ושוב בבתי המשפט. למרות טענות אלו פסק בית המשפט העליון של הודו בספטמבר 2018 ש-Aadhaar כשרה, אולם בהיקף מוגבל ובמגבלות על שמירת מידע. *Puttaswamy v. Union of India* [2018] INSC 838 32

מזהה יחיד וייחודי במתחם מסוים). כך עשוי להיות בבחירות, שבהן אין להתיר לאדם אחד להצביע פעמים רבות באמצעות שימוש במזהים רבים.<sup>33</sup> חלופה למערכת זהות שמבוססת על מזהים ייחודיים ויחידים היא מערכת המבוססת על הצהרות אמן ועל אישורים.<sup>34</sup> במערכת מסוג זה הזהות אינה מתמצית במזהה **מוסמך**, כמו מספרי זיהוי ביומטריים או מטעם הממשלה, אלא הזהות מוגדרת באמצעות רשת של הצהרות אמן ואישורים שמבוססת על אימות מסוג **רשת אמן**.<sup>35</sup> מערכת כזו משקפת טוב יותר את האופי רב-הפנים של הזהות האנושית באפשרה לפרופילים שונים ול**אישויות** שונות להופיע באמצעות שילוב של הצהרות אמן ואישורים לפי תרחישי השימוש. פרופיל שמתאים לבקשה להלוואה עשוי להיות שונה מזה שמשמש בפורומים ציבוריים. מערכת כזו אינה מבטיחה בהכרח שיחידים ישתמשו בה ביחידות, אולם היא מתאימה לרוב הגדול של תרחישי שימוש יום-יומיים.

## ב. תפקיד הזהות בהכללה חברתית-כלכלית

במשך שנים רבות הדגיש הבנק העולמי שצריך להעניק לכל אזרח הוכחה תקפה לזהותו, משום שהזהות הפכה להיות הכרחית לצורך הכללה פיננסית ולצורך גישה לשירותים חיוניים ולזכויות חיוניות. דוח חדש של הבנק העולמי,<sup>36</sup> מזהה שלוש מטרות-על לכל מערכת הזדהות מנקודת מבט של פיתוח:

Clemens H. Cap & Nico Maibaum, "Digital Identity and Its Implication for Electronic Government", *Towards the E-Society* (Beat Schmid, Katarina Stanoevska-Slabeva & Volker Tschammer eds., 2001) 803; R. Michael Alvarez, Thad E. Hall & Alexander H. Trechsel, "Internet Voting in Comparative Perspective: The Case of Estonia", 42 *Pol. Sci. & Pol.* (2009) 497

*Attribute-based Credentials for Trust* (Kai Rannenberg, Jan Camenisch & Ahmad Sabouri eds., 2015)

את המושג "רשת אמן" (web of trust) הציע לראשונה יוצר ה-PGP פיל צימרמן (Phil Zimmermann) ב-1992 במדריך לגרסה 2.0 של ה-PGP: "בחלוף הזמן, תצברו מפתחות מאנשים אחרים שאולי תרצו לקבוע בתור מציגים (introducers) נאמנים. כל אחת אחת תבחר לעצמה מציגים נאמנים. וכולם יצברו בהדרגה – ויפיעו באמצעות המפתח שלהם – אוסף של חתימות מאשרות מאנשים אחרים, בציפייה שכל מי שתקבל אותן תבטח בחתימה אחת או שתיים לפחות. כך תיווצר רשת מבוזרת וסובלנית-לתקלה של ביטחון בכל המפתחות הציבוריים"; 2, Rohit Khare & Adam Rifkin, "Weaving a Web of Trust", *World Wide Web J.* (1997) 77

יוזמת ההזדהות לשם פיתוח של הבנק העולמי פרסמה ב-2016 מסמך מסגרת אסטרטגי שמכיר ביכולתן של מערכות הזדהות מודרניות להביא לשינוי בהספקת שירותים בסיסיים וזכויות לעניים. *Strategic Framework for Dev.*, World Bank Grp., (2016), <https://bit.ly/31rvV6p>.

**הכללה וגישה לשירותים חיוניים**, כמו טיפולים רפואיים וחינוך, זכויות הצבעה, שירותים פיננסיים ותוכניות לרשת ביטחון חברתית; **מנהל תקף ועיל של שירותים ציבוריים**, החלטות מדיניות שקופות ומשילות משופרת – בעיקר כדי לצמצם כפילות ובזבוז; **אמצעי מדידה מדויק יותר של התקדמות בפיתוח בתחומים כגון הפחתת תמותת אימהות ופעוטות.**

אולם גם היום, יותר מ-1,500,000,000 בני אדם מודרים מגישה לשירותים בסיסיים וזאת משום שהם אינם מסוגלים להוכיח את זהותם.<sup>37</sup> רוב גדול של אותם אנשים מתגוררים באסיה ובאפריקה באזורים שאין בהם תשתית הולמת לרישום לידות ואירועים אחרים במהלך החיים (למשל בדרום אסיה ובאפריקה שמדרום לטהרה, בהתאמה, רושמים את לידתם של רק 39% ו-44% מהילדים<sup>38</sup>), ושככלל הם חלק מהפליטים העניים ביותר באוכלוסייה.

כמו כן, לפי נציבות האו"ם לפליטים,<sup>39</sup> יש כעת בעולם יותר מ-70,000,000 בני אדם שעזבו בכפייה את מקום מגוריהם בשל מלחמה או רדיפה; 25,000,000 מהם פליטים – בעיקר מסוריה, מאפגניסטן ומדרום סודן. יש גם כ-4,000,000 חסרי מדינה, שנשללה מהם אזרחות, ולכן גם גישה לשירותים בסיסיים ולזכויות בסיסיות. המספרים הללו צפויים לגדול בשנים הבאות, בעיקר בשל ההשפעה המתגברת של שינויים באקלים, שהשפעתם המכרעת על מאבקים פוליטיים<sup>40</sup> והיותם גורם ממשי להגירה פנימית ולהגירה חיצונית,<sup>41</sup> מוכרים.

לפיכך, השיק האו"ם לאחרונה את "ברית ID2020" (ID2020 Alliance),<sup>42</sup> שותפות בין גופים רבים שמאחדת ארגונים, גופים שלא למטרות רווח, עסקים וממשלות מלאומים

37 רוח ההזדהות לשם פיתוח של הבנק העולמי משנת 2016 הראה שכ-1,500,000,000 בני אדם ברחבי העולם (יותר מ-21% מאוכלוסיית העולם) אינם יכולים להוכיח את זהותם. ראו שם.

38 שם.

39 *Figures at a Glance*, UNHCR, <https://bit.ly/3pBGxra>

40 ראו למשל, Peter H. Gleick, "Water, Drought, Climate Change, and Conflict in Syria", 331 *Weather Climate & Soc'y* (2014) 6 (הבצורת הקיצונית בסוריה מתוארת בתור גורם מניע למלחמת האזרחים ב-2011); Michael Werz & Laura Conley, *Climate Change, Migration, and Conflict in Northwest Africa* (2012) (קישור ההצלחה של אסטרטגיות הגיוס של אל-קאעידה לירידה הכללית ביכולת להתפרנס מחקלאות וממרעה).

41 החוזה העולמי של האו"ם בעניין פליטים הכיר בכך ש"אקלים, הידרדרות באיכות הסביבה ואסונות טבע פועלים בהשפעה הדדית עם גורמים לתנועת מהגרים". לפי המרכז לניטור עקירה פנימית, היו ב-2017 1,800,000 עקירות פנימיות חדשות שקשורות לאסונות. רוב העקירות בשל אסונות שקשורות לסכנות טבע ולהשפעה של שינויי אקלים הן פנימיות, אולם מתרחשת גם עקירה חוצת גבולות, והיא עשויה להיות קשורה למצבי מלחמה ואלמות.

42 ID2020, <https://id2020.org>

רבים, וכולם פועלים להבטיח שהזהות הדיגיטלית תיושם באחריות ותהיה זמינה בתפוצה רחבה. לברית שתי מטרות: מצד אחד היא ממונה על הגדרת אמות המידה למערכות זיהוי דיגיטליות טובות ומוסריות, ומצד אחר היא אחראית לממן מיזמים לזהות דיגיטלית בחשיבה של טובין חברתיים וליישם. ברית ID2020 יצרה בין היתר סימן אישור (Certification Mark),<sup>43</sup> שמשמש לסמן פתרונות טכנולוגיים העומדים באמות המידה הטכניות ובדרישות הטכניות שהברית קבעה והמקיימים את עקרונות הניידות, ההתמדה, הפרטיות והשליטה בידי המשתמש.

מוסדות ציבוריים ופרטיים מפתחים כעת הוכחות היתכנות רבות כדי לספק זהות דיגיטלית לאלו שאין להם כעת אמצעי זיהוי רשמיים.<sup>44</sup> בתכנון פתרונות זהות הללו חשוב להבטיח ששחקן יחיד לא יחזיק ברישומי הזהות האישיים של כל אדם מזוהה וישלוט בהם, מה שעלול להעלות חששות ניכרים בתחום הפרטיות. אפשר להשתמש בזהות דיגיטלית בעיקר כשמדובר בפליטים שאין ברשותם אמצעי זיהוי הולמים, לצורך זיהוי אנשים מסוימים או משפחות מסוימות שזכאים לסיוע כספי או להטבות מסוג אחר. אולם בשל המצב הפגיע של קבוצות אוכלוסייה אלו, חשוב במיוחד למצוא דרכים לזהות את האנשים הללו זיהוי ייחודי שאינו משתמע לשתי פנים, וכך בכך להבטיח הגנה על פרטיותם. נדרש לתכנן מערכת לניהול זהות שממזערת את השליטה של גורם יחיד במידע אישי של אוכלוסיית פליטים.

לכן אף שהיא נותרת אדישה לטכנולוגיה, ברית ID2020 מתעניינת במיוחד בטכנולוגיית בלוקצ'יין בתור פתרון אפשרי להענקת זהויות דיגיטליות שאפשר להתחקות עליה, שאינה משתנה, ושאינה בשליטת חברה אחת בלבד או ארגון אחד בלבד, גם לא בכוח. אחת הדרישות היסודיות ש-ID2020 הגדירה לזהויות דיגיטליות היא למעשה שהזהויות יישארו ניידות ושאנשים יותירו בידיהם את השליטה על המידע האישי שלהם בכך שיבחרו עם מי לחלוק אותו ולאילו מטרות.

ישנם מספר ארגונים שלא למטרת רווח במגזר ההומניטרי, המעורבים אף הם בהגדרת נהגים מיטביים (best practices) וקווים מנחים וזאת במטרה להבטיח שהמטפלים במהגרים ובפליטים יכבדו את זכותם הבסיסית לפרטיות ולהגנת מידע. הם אף פיתחו מסמכי ליבה בסוגיה זו, ובכללם "המדריך לניהול מידע",<sup>45</sup> הרוח של ארגון

<sup>43</sup> ID2020 Certification Mark Application Form, ID2020, <https://bit.ly/31C55cu>

<sup>44</sup> ראו למשל Greg McMullin, Primavera De Filippi & Constance Choi, *Blockchain Identity Services: Technical Benchmark of Existing Blockchain-Based Identity Systems* (2019) (ניתוח יוזמות שונות מבוססות-בלוקצ'יין לזהות דיגיטלית והדרגות השונות בהן של ביזור והתאמות לפרטיות).

<sup>45</sup> *Handbook on Data Management in Information Systems* (Jacek Błazewicz, Wiesław Kubiak, Tadeusz Morzy & Marek Rusinkiewicz eds., 2012).

Privacy International (2018) על "בעיית המטה-דאטה ההומניטרית"<sup>46</sup> והמדריך של הוועד הבין-לאומי של הצלב האדום על "הגנת מידע בפעולה ההומניטרית",<sup>47</sup> שעוסק במיוחד בדרישות הפרטיות הנוספות שיש ליישם ביחסים עם אנשים פגיעים. כל הקווים המנחים הללו מזמינים ארגונים שמעניקים סיוע ההומניטרי לנקוט את כל הצעדים ההכרחיים להגן על המידע האישי של כל המעורבים, ולהתמקד בעקרונות ההומניטריים הבסיסיים שעניינם "לא להזיק" וקידום כבוד האדם.

אולם, גם אם הארגון שאוסף את המידע מכבד את כל הקווים המנחים בעניין פרטיות, כל ארגון ריכוזי שמחזיק בכמות גדולה כזו של מידע אישי הוא בהכרח נקודת כשל יחידה שעלולה לגרום בלי משים לדליפות מידע חמורות. פתרון מבוזר אמיתי יאפשר לאנשים לשמור על שליטה מלאה במידע האישי שלהם (בפתרון זהות בריבונות עצמית אמיתי), אבל היעדר מאגר מידע ריכוזי של זהויות יקשה להבטיח את הייחודיות ואת היחידות של זהויות אלו.

פתרון שזוהה ושמציע זהות קבועה מלידה בלי צורך ברשות ריכוזית שאחראית להקצות מזהה מסוים לכל אדם, הוא להסתמך על מידע ביומטרי כדי לחולל מזהה ייחודי (פונקצייה קריפטוגרפית ביומטרית) שמקושר לכל אדם. אכן, בהיעדר רשות ריכוזית שמסוגלת להבטיח שאדם אחד לא יירשם פעמיים לקבלת זהות, הדרך היחידה להבטיח את יחידות המזההים בלי לגלות לציבור מידע רגיש על האדם הנדון היא שהמזההים הללו יקושרו למידע ביומטרי מגובב קריפטוגרפית. הפונקצייה הביומטרית יכולה לשמש אמצעי לאימות, שכן אפשר לאמתה בקלות באמצעות השוואתה לפונקצייה ביומטרית אחרת, אבל אי אפשר לגלות באמצעותה את המידע הביומטרי של מושאה.

עם זאת אף שדגם כזה צפוי להניב יתרונות חשובים לפרטיות, צמודה לו אזהרה ולפיה יחידות המזהה מצויה ביחס הפוך למהימנות המערכת.<sup>48</sup> אכן, ייחודיות וייחודיות הן עניין שבמידה: מזהים שונים בעלי תכונות שונות מתמקמים בנקודות שונות על פני רצף. אף שבמידע ביומטרי אפשר ליצור מזהים ייחודיים שאינם משתמעים לשתי פנים,

Privacy Int'l & Int'l Comm. of the Red Cross, *The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Era* (2018), <https://bit.ly/338bkED>

Int'l Comm. of the Red Cross, *Handbook on Data Protection in Humanitarian Action* (2017).

48 מידע ביומטרי מאוחסן בדרך כלל בצורתו הגולמית ואינו מגובב, משום שפונקציות גיבוב דורשות את אותו קלט בכל פעם. גיבוב מתאים לקלטים זהים מטבעם, כמו סיסמאות, ואילו קלטים ביומטריים משתנים מטבעם. לכן אי אפשר להבטיח קלטים זהים. למשל קשתית שמצולמת בתנאי תאורה שונים במקצת תפיק קלט שונה שבו תוצאות מגובבות אינן זהות זו לזו. קלטים ביומטריים מושוים לתבניות באמצעות השוואת מספר הסיביות היציבות (stable bits) שמופקות מכל סריקה ביומטרית. אפשר לגבב קלט ביומטרי באמצעות מזעור מספר הסיביות היציבות הנדרשות, אך האימות הביומטרי יהפוך למהימן פחות. אם מספר הסיביות היציבות שנדרש להתאמה עולה, המהימנות משתפרת, אולם יהיה קשה יותר לאמת זאת, בשל התגברות הקושי להגיע למספר הסיביות היציבות.

השאלה אם הם עומדים ברף יחידות מספיק תלויה בסופו של דבר בדרגת התחכום הטכנולוגי ובגודל האוכלוסייה.<sup>49</sup> להלן ננתח את היתרונות שבמערכות אלו ואת הסיכונים בהן כדי להעריך עד כמה מותר להשתמש בהן למטרות זיהוי פליטים וחלוקת סיוע להם.

### ג. יתרונות במערכות זיהוי ביומטריות והסיכונים בהן

לשימוש בנתונים ביומטריים במערכת לניהול זהות נודעים כמה יתרונות. אם אנשים יכולים להזהה את עצמם באמצעות נתונים הביומטריים, הם אינם נזקקים עוד לסיסמאות (לרוב סיסמאות חלשות שקל יותר לזכור – וקל מאוד לפצח). מאחר שנתונים ביומטריים קשים יותר לזיוף (או יקרים לזיוף יותר מאשר לפיצוח סיסמאות חלשות), נתונים ביומטריים עשויים להיות בטוחים ממערכות אימות קיימות. אולם השימוש בנתונים ביומטריים במערכת לניהול זהות עלול ליצור קשיים ניכרים בתחומי האבטחה והפרטיות, לפי אופן השימוש בהם, אחסונם והענקת אישור לשימוש בהם.<sup>50</sup> לדוגמה, נתונים ביומטריים שמאוחסנים במערכות ריכוזיות בלי אמצעי ביטחון בדמות מדיניות גישה למידע או צעדים לעיצוב אבטחה, עשויים להיות בסיכון רב יותר מאשר במקרים שבהם היה המידע מאוחסן אחסון מקומי במכשיר של המשתמש.<sup>51</sup>

לכן בשנים האחרונות הולכים ומתרבים מחקר ויוזמות לבחינת השימוש בתשתיות מבוזרות, בעיקר מבוססות-טכנולוגיית-בלוקצ'יין, כדי ליצור סוגים חדשים של מערכות ניהול זהות בריבונות עצמית<sup>52</sup> ולצורך להן נתונים ביומטריים כדי להבטיח את יחידות הזהויות במערכות הללו.<sup>53</sup>

- 
- Abhilasha Bhargav-Spantzel et al., "Biometrics-Based Identifiers for Digital Identity Management", *Proceedings of the 9th Symposium on Identity and Trust on the Internet* (Carl Ellison, Neal Burnett & Sara Caswell eds., 2010) 84; J.A. Unar, Woo Chaw Seng & Almas Abbasi, "A Review of Biometric Technology Along with Trends and Prospects", 47 *Pattern Recognition* (2014) 2673 49
- Salil Prabhakar, Sharath Pankanti & Anil K. Jain, "Biometric Recognition: Security and Privacy Concerns", *IEEE Security & Privacy* (2003) 33 50
- Benjamin J. Muller, *Security, Risk and the Biometric State* (2010) 51
- Djuri Baars, "Towards self-sovereign identity using blockchain technology" (2016) 52 (unpublished M.A. thesis, University of Twente); Ori Jacobovitz, *Blockchain for Identity Management* (Lynne & William Frankel Ctr. for Comput. Sci. Dep't of Comput. Sci., Ben-Gurion Univ., Tech. Report No. 16-02, 2016); Andrew Tobin & Drummond Reed, Sovrin Found., *The Inevitable Rise of Self-Sovereign Identity* (2016); Paul Dunphy & Fabien A.P. Petitcolas, "A First Look at Identity Management Schemes on the Blockchain", *IEEE Security & Privacy* (2018) 20
- J.S. Hammudoglu et al., "Portable Trust: Biometric-Based Authentication and Blockchain Storage for Self-Sovereign Identity Systems" (2017), 53

בלי לדון בפתרונות אלו לגופם, נתאר להלן את הפעולות הבסיסיות של מערכות ניהול הזהות הללו ואת היבטי הנוהל שלהן, ונתמקד בסוגיות העיקריות שיש להתחשב בהן בעיצוב מערכת זהות שמסתמכת על תשתית מבוססת-בלוקצ'יין ועל מידע ביומטרי בתהליכי ההזדהות והאימות.

### 1. תשתית מבוזרת לעומת משמורת ריכוזית על מפתחות

כל המערכות המבוססות-בלוקצ'יין מסתמכות על זוג מפתחות ציבורי-פרטי לתעד מידע (בין היתר עסקאות פיננסיות) ביומן משותף ומבוזר. לכן היבט חשוב של כל מערכת זהות מבוססת-בלוקצ'יין הוא השאלה מי בסופו של דבר מחזיק במפתחות הפרטיים שנחוצים להוציא לפועל עסקה, או שולט בהם. בעניין זה חשוב להבחין בין תשתית מבוססת-בלוקצ'יין מבוזרת למנגנון שבאמצעותו מערכת הזהות המבוססת-בלוקצ'יין מנהלת את המפתחות שמקושרים לכל ישות וישות.

בלוקצ'יין מבוזר כשנתוני העסקאות בו מתועדים בלי שינוי ומתופעלים ברשת מפולגת של צומתי מחשבים כדי למנוע גנבה שיטתית (כלומר רישום מחדש של נתוני העסקאות כדי לאפשר הוצאה כפולה). אולם האופי המבוזר של רשת בלוקצ'יין אינו נכון למשמורת על המפתחות ששולטים בארנקים האישיים ברשת זו ולאחסונם המאוכלס.<sup>54</sup> שליטה ריכוזית במפתחות אלו ואחסון ריכוזי שלהם הם פרצת אבטחה חמורה שיש בה כדי להסביר מקרים מפורסמים רבים של שוד זירות מסחר במטבע מבוזר. מנקודת מבט טכנית טהורה (בהתעלם מהתחייבויות משפטיות וחוזיות) הבעלות בנכסים בבלוקצ'יין מושווית לשליטה בנכסים שמנוהלת באמצעות המפתחות הפרטיים שקשורים לארנק שמכיל את הנכסים. אם זירות מסחר במטבע מבוזר שולטות במפתחות הפרטיים המקושרים לארנקים (או לחשבונות פנימיים בזירת המסחר) שבהם כספי הלקוחות, הן שולטות בפועל גם בכספים אלו משום שהמשמורת על אותם המפתחות משמיעה בסופו של דבר שליטה מלאה בכספים המאוחסנים בחשבון – כמעט כמו שטרות גשמיים.<sup>55</sup> לכן מאחר שהמפתחות הפרטיים של הלקוחה לא אוחסנו ואובטחו במבוזר כראוי, זירות

<https://bit.ly/3osPiVk>; Paco Garcia, "Biometrics on the Blockchain", *Biometric Tech. Today* (2018) 5; Asem Othman and John Callahan, "The Horcrux Protocol: A Method for Decentralized Biometric-based Self-sovereign Identity", *2018 International Joint Conference on Neural Networks (IJCNN)* (2018).

Garrick Hileman & Michel Rauchs, *2017 Global Cryptocurrency Benchmarking Study* (2017), <https://bit.ly/338rCgH>

Primavera De Filippi, "Bitcoin: A Regulatory Nightmare to a Libertarian Dream", 3 *55 Internet Pol'y Rev.* (2014).

המסחר הריכוזיות הללו הפכו במהירות ל"מלכודות דבש" בעלות ערך שמושכות תוקפים.<sup>56</sup>

בשלבנו נתונים ביומטריים ומטבע מבוזר, חשוב שלא להשתמש בנתונים ביומטריים בתור המקור למפתח הפרטי שמאפשר גישה לעתודות המטבע המבוזר. שאם לא כן, כל מי שיכולה לקבל גישה לנתונים הביומטריים של אדם תוכל להפיק את המפתח הפרטי שלו וכך לגשת לעתודות המטבע המבוזר. בהיבטי האבטחה והפרטיות מערכת כזו מסוכנת מזירת מסחר ריכוזית רגילה במטבע מבוזר, שכן נתונים ביומטריים מכילים את המידע המזהה האישי הרגיש ביותר והמקובע ביותר.<sup>57</sup> בקיצור, גם אם משתמשים בתשתית בלוקצ'יין מבוזרת כמו ביטקוין או את'ריום בתור עמוד התווך של מערכת זהות,<sup>58</sup> יתרונות האבטחה שבביזור אינם עוברים אליה אם המשמורת על המפתחות נשארת ריכוזית בלי גורמי עיצוב אבטחה שיפצו על כך.

## 2. זיהוי לעומת אימות

בשלב הבא בהערכת מערכת זהות חשוב לזהות מהם סוגי המידע שחובה למסור בשלבים השונים של התהליך, כאשר אנשים נרשמים למערכת זהות מסוימת וכשהם מאמתים את זהותם במערכת. ננתח להלן את הצעדים השונים במערכת זיהוי מבוססת-ביומטריה.

### רישום

רישום (enrollment) הוא תהליך יצירה של זהות משתמש חדשה במערכת הביומטרית. על כל משתמשת למסור דגימות ביומטריות נדרשות (למשל טביעת אצבע, קשתית או פנים) שיינטלו בסורק ביומטרי או במכשיר דומה. המידע הביומטרי שנאסף ישמש ליצירת תבנית ביומטרית ומזהה ביומטרי שמקושרים למידע האישי (כמו נתונים דמוגרפיים) למטרת זיהוי בעתיד.<sup>59</sup>

David Gerard, Attack of the 50 Foot Blockchain: Bitcoin, Blockchain, Ethereum & Smart Contracts (2017) 56

Irma van der Ploeg, "Biometrics and the Body as Information", *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination* (David Lyon ed., 2003) 57

Primavera De Filippi & Raffaele Mauro, "Ethereum: The Decentralised Platform that Might Displace Today's Institutions", *Internet Pol'y Rev.* (Aug. 25, 2014), <https://bit.ly/3dpDBbw> 58

Livia C. F. Araújo et al., "User Authentication Through Typing Biometrics Features", *53 IEEE Transactions on Signal Processing* (2005) 851 59



## אימות

אימות (authentication) הוא תהליך שבו לאחר שפרטים נרשמו למערכת המערכת בודקת – באמצעות השוואת דגימה ביומטרית חדשה לדגימה הביומטרית שנוצרה ברישום – אם יש להם הרשאות מתאימות לגשת לשירות מסוים או ליהנות מסיוע מסוג מסוים.<sup>60</sup> את שלב האימות אפשר לחלק לשני צעדים שונים: זיהוי (identification) ווידוא (verification).

## וידוא



וידוא הוא תהליך שבו מוודאים את זהותו של אדם. הוא עונה על השאלה: האם את מי שאת טוענת שאת? מדובר בתהליך השוואה אחד לאחד שבו דגימה ביומטרית חדשה משווית לרישום מאומת. כך גם בשימוש בטביעת אצבע או בסריקת פנים כדי לגשת למכשירים כמו מחשב או טלפון נייד. כיום מקובל שהרישום הביומטרי מאוחסן אחסון מקומי ובתצורה מוצפנת במכשיר ממשי.<sup>61</sup> כך למפתחות יישומנים לטלפונים ניידים וליצרניות מכשירים אין גישה לתבנית. הסריקה המקורית ששימשה ליצירת התבנית למטרות התאמה מושמדת, ועם השלמת תהליך ההשוואה, זהו גם גורלן של הסריקות החדשות שנוצרות בכל כניסה חדשה למערכת.<sup>62</sup> אחסון מקומי של תבנית ביומטרית במכשיר (ולא בשרת מרכזי) הוא אחסון מבזר של מידע, ואפשר לבזרו עוד בשבירת התבנית הביומטרית לחתיכות רבות שחייבות להצטרף זו לזו כדי שיוכלו לקרוא אותן. שיטה זו מגינה על הפרטיות ומשפרת את האבטחה.<sup>63</sup>

- 
- Lawrence O’Gorman, “Comparing Passwords, Tokens, and Biometrics for User Authentication”, 91 *Proc. IEEE* (2003) 2021 60  
 Bruce Schneier, “Inside Risks: The Uses and Abuses of Biometrics”, 42(8) *Comm. ACM* (1999) 136 61  
 Umut Uludag, Arun Ross & Anil Jain, “Biometric Template Selection and Update: A Case Study in Fingerprints”, 37 *Pattern Recognition* (2004) 1533 62  
 Minhaz Fahim Zibran, *Biometric Authentication: The Security Issues* (Univ. of Sask. Dep’t of Comput. Sci. No. 2012–02, 2012) 63

## זיהוי



זיהוי הוא תהליך אחזור הזהות של אדם מסוים בהתבסס על מזהה. הוא עונה על השאלה: מי את? מדובר בתהליך השוואה של אחד לרבים, ובו דגימה ביומטרית חדשה מושווית לתבניות רבות במאגר מידע של זהויות כדי לאחזר את הזהות המסוימת שקשורה אליה.<sup>64</sup>

במצב מושלם סריקת הדגימה תושמד עם תום התהליך. אולם למטרת השוואה יש לאחסן את התבנית הביומטרית המקורית בשרת או להפוך אותה לזמינה בדרך אחרת למפעילת מערכת הזהות. לכן – בניגוד לתהליך הווידוא, שניתן לעשותו בוידוא מקומי במכשיר המשתמשת – בתהליך הזיהוי נדרשת נגישות מקוונת של התבניות הביומטריות. על כן כדי למזער סיכוני אבטחה חשוב לזהות מנגנונים לאחסון מבוזר מאובטח ולעיבוד מידע,<sup>65</sup> כגון חישוב רב-צדדי מאובטח,<sup>66</sup> או פתרונות חדשניים המבוססים על הצפנה הומומורפית.<sup>67</sup>

### 3. שליטה אישית במידע אישי לעומת שליטה ארגונית בו

להוציא מקרה שבו תבנית ביומטרית מאוחסנת במכשיר של המשתמשת (בעיקר למטרות וידוא), ביתר המקרים המתוארים לעיל המידע המזהה הביומטרי והאישי אינו בחזקתו של מושא המידע אלא של הארגון שאוסף את המידע עבור מערכת זהות מסוימת, מאחסן אותו ומנהל אותו. אף שתקנות לניהול מידע – בעיקר באירופה – מאפשרות למושא המידע להגביל איסוף מידע אישי ועיבודו,<sup>68</sup> עם איסופו המידע עשוי להישאר בשליטת בעלי החומרה (שרתים ומכשירים) שהמידע מאוחסן בה. כך גם בנוגע למידע התנהגותי

<sup>64</sup> *Handbook of Biometrics* (Anil K. Jain, Patrick Flynn & Arun A. Ross eds., 2007)  
<sup>65</sup> Vignesh Ganapathy et al., "Distributing Data for Secure Database Services", *Proceedings of the 4th International Workshop on Privacy and Anonymity in the Information Society* (Traian Marius Truta et al. eds., 2011)  
<sup>66</sup> Oded Goldreich, *Secure Multi-Party Computation* (1998), <https://bit.ly/3IrxGkB>  
<sup>67</sup> Craig Gentry, "A Fully Homomorphic Encryption Scheme" (Sept. 2009) (unpublished Ph.D. dissertation, Stanford University)  
<sup>68</sup> Christina Tikkinen-Piri, Anna Rohunen & Jouni Markkula, "EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies", 34 *Computer L. & Security Rev.* (2018) 134

ולמידע חברתי שתאגידים אוספים על משתמשותיהם ושנערך סטטיסטית בתור פרופיל זהות שעשוי לשמש למטרות פרסום, דירוג אשראי חלופי, וידוא זהות וכדומה.<sup>69</sup> חוקי פרטיות ותקנות הגנת מידע מעניקים הגנה מסוימת בנוגע לאופני אחסון המידע, לשימוש בו או לאיסופו. אולם תקנות להגנת מידע רק מטילות חובה על אוספי מידע ועל מעבדי מידע לקבל הסכמה מודעת ומפורשת של מושא המידע לפני שיתחילו לאסוף מידע אישי או להשתמש בו למטרה מסוימת.<sup>70</sup> בכמה תחומי שיפוט – כמו באירופה לאחר חקיקת האסדרה הכללית להגנת מידע<sup>71</sup> – נוספו זכויות, לרבות הזכות לניידות מידע<sup>72</sup> וזכות המחיקה<sup>73</sup> (שידועה בשם הזכות להישכח). אולם אם הגנות אלו אינן קיימות, יש סיכון שמידע אישי (כולל תבניות ביומטריות ודגימות ביומטריות) יישאר מבודד בידי הארגונים ששולטים בו, ולמושא המידע לא תהיה אפשרות ממשית לבקש למחוק אותו או לניידו אלא אם כן אותם ארגונים מיישמים מדיניות משלהם שאוכפת דרישות אלו.

#### 4. נתונים ביומטריים לעומת סוגי מזהים אחרים

נתונים ביומטריים מקנים יתרונות למערכת לניהול זהות, אולם הם אינם חפים מחסרונות. ראשית, שימוש במידע ביומטרי כדי ליצור מזהה ייחודי ויחיד, מחייב פרטים להזדהות בתור אישיות אחת ורק אחת – גם אם אין הכרח בכך לתרחיש שימוש מסוים,<sup>74</sup> והדבר עלול להציב קשיים ממשיים בתחום הפרטיות, בעיקר מבחינתם של פליטים פוליטיים. נתונים ביומטריים גם עלולים להיות בעייתיים מדרכי אימות מסורתיות (למשל סיסמאות ומזהים אחרים כמו מספרי PIN ומכשירי חומרה) משום שאין ביכולתנו לשנות את נתונינו הביומטריים.<sup>75</sup> חשוב לציין שמידע ביולוגי הוא למעשה מידע ציבורי: אנו

- 
- Lee A. Bygrave, "The Data Difficulty in Database Protection" Univ. of Oslo Faculty 69  
of Law Research Paper No. 2012-18 (2012) <https://bit.ly/3GmxS2Q>
- Eleni Kosta, Consent in European Data Protection Law (2013) 70
- האסדרה הכללית להגנת מידע (לעיל, הערה 17) היא אסדרה בדיני האיחוד האירופי על 71  
הגנת מידע ופרטיות לכל האנשים בתחומי האיחוד האירופי והאזור הכלכלי האירופי.
- סעיף 20 לאסדרה קובע: "למושא המידע נתונה הזכות לקבל את המידע האישי עליו או 72  
עליה שהוא או היא מסר/ה לשולט [במידע], בתצורה מובנית שנמצאת בשימוש נפוץ  
ושקריאה במכונה, ונתונה לו או לה הזכות להעביר את המידע האמור לשולט אחר בלי  
הפרעה מהשולט שהמידע האישי סופק לו..."
- סעיף 17 לאסדרה קובע: "למושא המידע נתונה הזכות שהשולט [במידע] ימחק את המידע 73  
האישי בנוגע אליו או אליה בלי דיחוי בלתי נחוץ, והשולט מחויב למחוק מידע אישי בלי  
דיחוי בלתי נחוץ אם חלה אחת העילות הללו: (א) המידע האישי אינו נחוץ עוד למטרות  
שלשמן הוא נאסף או עובד בדרך אחרת..."
- Anil K. Jain, Arun Ross & Salil Prabhakar, "An Introduction to Biometric 74  
Recognition", 14 *IEEE Transactions on Circuits & Sys. for Video Tech.* 4 (2004)
- Prabhakar, Pankanti & Jain (לעיל, הערה 50). 75

מותירות אחריו מידע ביולוגי בכל מקום, למשל טביעות אצבעות, די-אן-איי, דפוס הליכה, תמונות פנים או קשתית, ואלגוריתמים מתקדמים במחשבים מסוגלים לחלץ ממנו תבנית ביומטרית.<sup>76</sup> אפשר בקלות לגנוב טביעות אצבעות, להעתיקן ו"להרים" (lift) אותן. על תוכנה לזיהוי פנים אפשר להערים בקלות באמצעות תמונות או סרטוני וידאו. קשה יותר לזייף טביעות קשתית ונתונים ביומטריים התנהגותיים, כמו הליכה, ולהעתיקם, אולם גם הם אינם פשוטים ובטוחים (לדוגמה עדשות מגע עלולות להטעות סורקי קשתית). לפיכך, בשל האופי הציבורי הטבוע בהם, ניתן להשתמש בנתונים ביומטריים רק בתור שם משתמש (כלומר מפתח ציבורי) ולא בתור סיסמה (כלומר מפתח פרטי). אם משתמשים בנתונים ביומטריים, יש לדרוש אימות באמצעות גורם שני כלשהו, כמו PIN או אסימון גשמי, וידוא תמונה בתעודת זהות או נוכחות בפועל של אדם.<sup>77</sup>

יתרה מזאת, גופנו נתון לשינוי. סריקות קשתית הופכות לעכורות בשל קטרקט. טביעות אצבע עשויות להיעלם בעקבות עבודה קשה או כוויות. ההליכה עשויה להשתנות בגלל זקנה, תאונות או מחלה. לפי מחקר<sup>78</sup> של המכון הלאומי לתקנים וטכנולוגיה, גם כשמדובר באנשים בריאים שיעור השגיאה בסריקת קשתית אחת עשוי לנוע בין 2.5% עד ל-20% במקרים מסוימים – שיעור ניכר בהתחשב בעובדה שאוכלוסיית העולם מונה 7,500,000,000 נפש. כפי שטוענים אנשי מקצוע בתחום ההזדהות כמו וינאי גופטה (Vinay Gupta), מחמת המגוון המורכב של צורות ביולוגיות והגונויות (ניאונסים) שביניהן אי אפשר כלל להסתמך על מדדים ביומטריים בתור מזהים יחידים וייחודיים של בני אדם.<sup>79</sup> אכן, אם נתונים ביומטריים משמשים מזהה כללי לזהות אדם ולזכויותיו, מבחינתם של הנקלעים לשיעור הטעות הבסיסי בן שלושת האחוזים התוצאות עלולות להיות משתקות וחמורות. לדוגמה, מחקר על מערכת תעודת זהות הביומטרית בהודו הראה ש-20% ממשקי הבית בג'הרקאנד (Jharkhand) מסרו שלא הצליחו לקבל את הקצבות המזון שלהם בגלל טעויות ביומטריות – פי חמישה משיעור הכשל בכרטיסי הקצבה רגילים.<sup>80</sup>

לבסוף, התפיסה הציבורית שלפיה הנתונים הביומטריים "מדעיים" יותר ולכן מהימנים יותר, מביאה הלכה למעשה להתעלמות מהחסרונות הטמונים בהם. אולם אם מזהה ביומטרי משמש עמוד התווך של מערכת לניהול זהות, שמשמשת להגנה על

Emilio Mordini & Sonia Massari, "Body, Biometrics and Identity", 22 *Bioethics* 76 (2008) 488.

Shantanu Rane et al., "Secure Biometrics: Concepts, Authentication Architectures, and Challenges", *IEEE Signal Processing Mag.* (2013) 51.

George W. Quinn & Patrick J. Grother, Nat'l Inst. of Standards & Tech., *NIST Interagency Report No. 7853, IREX III, Supp. I: Failure Analysis* (2012).

Vinay Gupta, A Blockchain Solution for Identity?, *Medium* (July 7, 2017), <https://bit.ly/3dq1pw3>.

Vindu Goel, Indian "Big Brother" Using Fingerprint Identification System for Food, Benefits and Bank Accounts, *Independent* (Apr. 10, 2018), <https://bit.ly/338gCjt>.

זכויות בסיסיות והטבות, אי אפשר שהוא ייכשל כישלון הרה אסון, גם אם ההסתברות לכשל נמוכה מאוד. בעולם מושלם מערכת זהות שמתפקדת כהלכה חייבת להיות עמידה בפני אירועים שליליים שהסתברותם נמוכה אך תוצאותיהם חמורות. היא תרוויח מקלָט מוגבר ומקשרי גומלין עם העולם. אולם מערכת זהות שנסמכת על נתונים ביומטריים בתור המזהה המהימן היחיד אינה רק מערכת פגיעה ושברירית,<sup>81</sup> אלא גם בעייתית מאוד בהיבטי אבטחת רשת ופרטיות<sup>82</sup> – והדבר נוגע בעיקר לעניין קבוצות אוכלוסייה פגיעות כמו מהגרים ופליטים.

#### ד. זהות בריבונות עצמית ומערכות לניהול אישורים

המושג "זהות בריבונות עצמית" (self-sovereign identity) צמח בשנים האחרונות אף שעדיין אין הגדרה מוסכמת למובן האמיתי של מושג זה.<sup>83</sup> מבחינה כללית, זהות בריבונות עצמית נועדה לשמר את הזכות לגילוי פרָרְתִי (סלקטיבי) של היבטים שונים בזהות ושל רכיביה השונים במתחמים שונים ובהקשרים שונים. זכות זו חלה בלי תלות בשאלה האם את ההיבטים והרכיבים האלו הנפיקו ממשלה מסוימת, חברה כלשהי או ארגון פלוני. זהות בריבונות עצמית עניינה גם הרעיון שלבני אדם נתונה שליטה במידע האישי שלהם, ובמידה מסוימת – גם בייצוגים של הזהויות (או האישויות) שלהם במערכת מסוימת לניהול זהות. מכאן נדרש שתינתן להם היכולת לקבוע במידה גבוהה של פירוט למי יש זכות גישה לפרטי מידע מסוימים עליהם (ולשלוט בכך).<sup>84</sup> מנקודת מבט טכנית, בדרך כלל רואים בזהות בריבונות עצמית אב-דגם (מסגרת חשיבה) חדש לניהול זהות מקוון. באב-דגם זה פרטים וישויות יכולים לנהל את המידע שקשור לזהותם (כלומר מזהים, מאפיינים ואישורים או מידע אישי אחר) באמצעות אחסון מקומי שלו במכשיריהם (או אחסון מרחוק ברשת מבוזרת), ולהעניק לצדדים שלישיים מאושרים גישה בררנית למידע זה בלי צורך לפנות לרשות נאמנה או למפעיל ביניים מהימן כדי לספק את ההצהרות הללו או לאשרן.<sup>85</sup> כך מתאפשרת שליטה רבה יותר במידע מזהה אישי או במידע אחר הצריך לעניין בנוגע לפרט או לישות. מאחר

81 Allan Friedman, Patrick Crowley & Darrell West, Ctr. For Tech. Innovation at Brookings, *Online Identity and Consumer Trust: Assessing Online Risk* (2011).

82 Prabhakar, Pankanti & Jain (לעיל, הערה 50); *Security and Privacy in Biometrics* (Patrizio Campisi ed., 2013).

83 M.E.M. van Wingerde, "Blockchain-Enabled Self-Sovereign Identity" (Dec. 13, 2017) (unpublished M.A. thesis, Tilburg University).

84 Uwe Der, Stefan Jähnichen & Jan Sürmeli, "Self-sovereign Identity – Opportunities and Challenges for the Digital Revolution" (2017), <https://arxiv.org/abs/1712.01767>.

85 Alexander Mühle et al., "A Survey on Essential Components of a Self-Sovereign Identity", 30 *Computer Sci. Rev.* (2018) 80.

שמזהים דיגיטליים יכולים ללבוש צורות שונות, דרישה חשובה ממערכת זהות כוללת היא לקבוע תקנים לתפעוליות בינית.\* להלן נתאר את התקן הנפוץ ביותר, המזהה המבוזר (DID) שנזכר לעיל.

## 1. זהות דיגיטלית בקוד פתוח ותקנים ברשת להצהרות בנות-אימות

מאגד המארג הכלל-עולמי (World Wide Web Consortium, W3C) הוא גוף לתקינה טכנית למען מרשתת פתוחה שפועלת בתקן המזהה המבוזר.<sup>86</sup> מזהים מבוזרים הם סוג חדש של מזהה לזהות דיגיטלית בת-אימות ובריבונות עצמית שניתן לגילוי ולתפעוליות בינית במגוון מערכות.<sup>87</sup> בתקן מזהה מבוזר תומכת הקרן לזהות מבוזרת (Decentralized Identity Foundation), מאגד חברות שמפתחות – ובנות – יישומים באמצעות תקן מזהה מבוזר, ובהן מיקרוסופט, איי-בי-אם, Hyperledger, Accenture, מאסטרקארד ו-RSA וכל החברות הגדולות בתחומי זהות בלוקצ'יין ומידע, כמו Civic, uPort, BigChainDB, Sovrin ורבות אחרות.<sup>88</sup>

מזהים מבוזרים הם מעני משאבים אחידים (URLs), כלומר כתובות ייחודיות במרשתת) שמתייחסים למסמך מזהה מבוזר אשר מספק מידע כיצד להשתמש באותו מזהה מבוזר.<sup>89</sup> לדוגמה, מסמך מזהה מבוזר עשוי לפרט ששיטת וידוא מסוימת (כגון מפתח ציבורי קריפטוגרפי או פרוטוקול ביומטרי בשם בדוי) יכולה לשמש לאימות. מסמך המזהה המבוזר עשוי גם להפנות לסדרת נקודות קצה לשירות ולאפשר פעולות גומלין נוספות עם השולט במזהה המבוזר. לדוגמה, מזהה מבוזר יכול להפנות למיקום של מידע אישי קשור שכדי לגשת אליו על הפונה לבקש רשות מהשולט במזהה המבוזר.<sup>90</sup>

מזהה מבוזר לעצמו מועיל רק לאימות. הוא מועיל בייחוד בצירוף הצהרות בנות-אימות או אישורים בני-אימות – תקני W3C נוספים שיכולים לשמש להוכחות אין-ספור של מושא המזהה המבוזר.<sup>91</sup> עם הוכחות אלו נמנים אישורים ותעודות שמעניקים למושא המזהה המבוזר זכויות גישה או הטבות גישה. לדוגמה, הצהרה

\* הערת המתרגם: תפעוליות בינית (interoperability) היא היכולת של כמה מערכות או רכיבים להחליף ביניהם מידע ולהשתמש במידע שהוחלף.

86 את W3C מוביל חלוץ תעשיית המרשתת טים ברנרס לי (Tim Berners-Lee), שהמציא את המארג הכלל-עולמי. ב-W3C יש 479 חברות, כולל כל החברות הגדולות בתחומי המרשתת והטכנולוגיה כמו אמזון, אפל, בואינג, סיסקו, מיקרוסופט, גוגל, פייסבוק, עליבאבא, טנסנט ובאידו, לצד אוניברסיטות מחקר וממשלות. ראו W3C, <https://www.w3.org>.

87 הכרת המונח ב-3rITLp0, *GitHub*, <https://bit.ly/3rITLp0>, *A Primer for Decentralized Identifiers*.

88 .DIF, <https://identity.foundation>.

89 .Decentralized Identifiers (DIDs) v1.0, W3C (May 4, 2020), <https://bit.ly/3otVeNG>.

90 McMullin, De Filippi & Choi (לעיל, הערה 44).

91 Dunphy & Petitcolas (לעיל, הערה 52).

בת-אימות יכולה להוכיח שאדם אושר באישור "דע את לקוחך" (Know-Your-Customer, KYC), ולכן הוא כשיר לפתוח חשבון בנק, שאותו אדם מתועד בתור זכאי לנהוג או מורשה לגשת לתוכניות מסוימות בתור מנהל מערכת.<sup>92</sup> הצהרה בת-אימות מכילה את המזהה המבוזר של מושאה (למשל לקוחת בנק) ואת ההוכחה (למשל אישור "דע את לקוחך") והיא חייבת להיות חתומה בידי האדם או הישות שמצהירים אותה באמצעות המפתחות הפרטיים המקושרים למזהה מבוזר של מנפיק ההצהרה (למשל הבנק). הצהרות בנות-אימות הן אפוא שיטות שבהן רשויות מהימנות, כמו בנקים, מנפיקות בהנפקה בת-הוכחה אישור מתועד שקשור למזהה מבוזר מסוים. הצהרות מזהה מבוזר נותרות בשליטת מושא המזהה המבוזר ואפשר להשתמש בהן להוכיח מאפיין מסוים של מושא המזהה המבוזר בלי תלות ברשות מתעדת, בספקית זהות או במרשם ריכוזי.<sup>93</sup> אם תוכיח שהיא המושא האמיתי של אותו מזהה מבוזר (בשיטת אימות מפורטת מראש), אישה או ישות תוכל ליהנות מזכויות הגישה המקושרות לאותן טענות.

אף שמזהים מבוזרים אינם תלויים בטכנולוגיית בלוקצ'יין ואינם דורשים אותה, הם עוצבו כך שיתאמו לכל יומן מבוזר ורשת בלוקצ'יין. הואיל ומזהה מבוזר עשוי להיות מקושר לזוג מפתחות פרטי-ציבורי מסוים שמשמש לחתימת הצהרות זהות, אפשר לקשר את אותו זוג מפתחות (כלומר זוג המפתחות שמקושר למזהה מבוזר) לזוג מפתחות שמשמש לחתום על עסקאות פיננסיות בבלוקצ'יין. חשוב מכך, מפרט המזהה המבוזר מאפשר גם לקשר שיטות מסוימות למזהה מבוזר שמפרט את הנהלים לרישום מפתחות, להחלפתם, לסיבובם, לשחזורם ולפקיעתם. כבר יושמו כמה תוכניות שיטה שממנפות את החוסן של טכנולוגיית הבלוקצ'יין ואת עמידותה בפני שיבוש כדי לנהל מזהים מבוזרים (למשל BCR DID, Blockstack DID, Ethereum ERC725 DID).<sup>94</sup> קבוצת W3C פועלת להבטיח תפעוליות בינית בין שיטות מזהה מבוזר שונות. עם זאת, חשוב לציין בהתחשב בשקיפות הבלוקצ'יין ובהיותו בלתי ניתן לשינוי, לעולם אין לאחסן מידע אישי בבלוקצ'יין עצמו.<sup>95</sup> אולם, ניתן להיעזר בו למטרות מעקב אחר הענקת אישורים וגישה למידע המזהה זיהוי אישי שמאוחסן מחוץ לו, ובכך ליצור שובל בר-ביקורת של גישה למידע. לכן נוסף על שיטות מזהה מבוזר תקניות אפשר להשתמש בבלוקצ'יין לתיעוד הצהרות או הוכחות ולביטולן בסופו של דבר; להענקת

92 Mehmet Aydar & Serkan Ayvaz, "Towards a Blockchain Based Digital Identity Verification, Record Attestation and Record Sharing System" (2019), <https://bit.ly/3IJdFwe>.

93 Baars (לעיל, הערה 52).

94 רשימה של תוכניות שיטת מזהה מבוזר שזמינות כעת נמצאת ב- DID Method Registry, W3C, <https://bit.ly/3IJ33NH>.

95 Primavera De Filippi, "The Interplay Between Decentralization and Privacy: The Case of Blockchain Technologies", 9 *J. Peer Production* (2016) 18.

גישה למחסני מידע אישי ולביטולה;<sup>96</sup> ולמטרות אחרות שעשויות להידרש למערכת זהות מסוימת (למשל תביעות שהוגשו ויושבו במערכת ליישוב סכסוכים בנוגע להוכחות שווא).

## 2. מפת דרכים לקראת זהות בריבונות עצמית

הדרך לזהות בריבונות עצמית אמיתית עודה ארוכה, שכן אנו רק בשלבים המוקדמים של הבנה כיצד ליישם מערכת זהות דיגיטלית שמעניקה לפרטים שליטה מלאה ואוטונומיה. עם זאת בשל משבר הפליטים באירופה והעלייה במספר העקורים שאין להם אמצעי זיהוי רשמי, היום – אולי יותר מתמיד – למסע לעבר ריבונות בזהות עצמית נודעת חשיבות מכרעת.

כמתואר לעיל, פתרונות של זהות בריבונות עצמית נועדו להעניק לאנשים שליטה בזהותם, כלומר הם יוכלו להחליט במדויק איזה מידע לגלות על עצמם, למי לגלותו ובאילו נסיבות. בדגם של זהות בריבונות עצמית ספקיות זהות לא יוכלו למנוע מאנשים לממש זכויות אדם בסיסיות, כמו הזכות להיות עצמי, הזכות לחופש ביטוי והזכות לפרטיות. אין הכרח כי אנשים יהיו המחזיקים היחידים בכל המידע על עצמם. אולם תנאי מוקדם חשוב לזהות בריבונות עצמית הוא שזהויות דיגיטליות לא יהיו נעולות במסגרת (פלטפורמה) מסוימת או בשליטת מפעיל כלשהו, אלא יישארו ניידות ובנות-תפעוליות בינית במסדות שונות. כך אנשים יהיו חופשיים לבחור את זהות המפעיל שהם בוטחים בו ביותר ולעבור בין מפעיל למפעיל לפי רצונם.

אך שאין כיום הגדרה מדויקת של זהות בריבונות עצמית, מזהים כמה תבחינים בתור העקרונות שבבסיס הזהות בריבונות עצמית.<sup>97</sup> אפשר לראות בעקרונות אלו נקודת התייחסות ראשונית להערכת פתרונות קיימים לזהות בריבונות עצמית:

1. **קיום** – לבני אדם צריך להיות קיום עצמאי, בלי תלות במזהים הדיגיטליים שמשמשים רק הפניה אליהם.
2. **שליטה** – לבני אדם צריכה להיות שליטה בזהותם, הם יוכלו תמיד להפנות אליה, לעדכן אותה ואף להסתיר אותה – גם אם אחרים יכולים להצהיר הצהרות בנוגע אליה.
3. **גישה** – לבני אדם צריכה להיות גישה לכל המידע בנוגע לזהותם, והם יוכלו לשחזר את הצהרותיהם בעת הצורך.
4. **שקיפות** – מערכות ואלגוריתמים שמנהלים זהויות דיגיטליות ומפעילים אותן חייבים להיות פתוחים ושקופים הן בנוגע לפעולותיהם הן בנוגע לתחזוקתם.

96 סקירה כללית על פתרונות זהות בריבונות עצמית מבוססי-בלוקצ'יין שונים ועל מאפייניהם נמצאת אצל McMullin, De Filippi & Choi (לעיל, הערה 44).

97 Chris Allen, "The Path to Self-Sovereign Identity", *GitHub* (Apr. 19, 2017), <https://bit.ly/3pypR3T> (מאת כריס אלן (Chris Allen) וקהילת (Rebooting Web of Trust)).



5. **התמדה** – זהויות יהיו ארוכות טווח, מוטב שיהיו לנצח, ולפחות כל עוד המשתמשת מעוניינת לשמור אותן.
6. **ניידות** – מידע בנוגע לזהות ושירותים בנוגע אליה, חייבים להיות עבירים ולא יוחזקו בידי צד שלישי יחיד, גם אם מדובר בישות מהימנה.
7. **תפעוליות בינית** – היכולת להשתמש בזהויות תהיה רחבה ככל האפשר, בניגוד לעיצובה לעבודה רק בסביבות מבודדות.
8. **הסכמה** – נדרשת הסכמה של בני אדם לשימוש בזהויותיהם, ושיתוף מידע על משתמשת יהיה רק בהסכמת מושא המידע.
9. **מזעור** – גילויי הצהרות יוגבל למידה המזערית הנדרשת להשגת המטלה הנדונה.
10. **הגנה** – יש להגן על זכויות המשתמשים בכל מחיר, גם אם הדבר מנוגד לאינטרסים של ספקיות הזהות.

רוב מיזמי הזהות הדיגיטלית לא יעמדו בכל התבחינים הללו – ורבים אינם מתיימרים כלל להיחשב למיזמי זהות "בריבונות עצמית". במאמר זה נדון בשני מקרי בוחן שבהם משתמשים בנתונים ביומטריים בשילוב טכנולוגיית בלוקצ'יין כדי להעניק למשתמשים מידה מסוימת של ריבונות בזהויותיהם הדיגיטליות. מקרה הבוחן הראשון הוא **נוהל קיווה** (Kiva Protocol), שמתמקד בזהות לצורך דירוג אשראי ושיתוף מאובטח של נתוני אשראי בין מוסדות מיקרו-מימון. מקרה הבוחן השני הוא תוכנית **אבני בניין** (Building Blocks) של תוכנית המזון העולמית ופתרון הזהות הביומטרי שלה להספקת שירותים למוטבים נצרכים, בעיקר הספקה משופרת של שירותים למוטבים של סוכנויות רבות של האו"ם.

בחרנו בשתי היוזמות הללו משום שדרגת המוכנות הטכנולוגית שלהן גבוהה מזו של חלופותיהן, בשל אמינותן, בשל השפעתן האפשרית בהיבט של פריסה בהיקף נרחב בעתיד ולבסוף בשל הניסויים הקודמים שהן ערכו, ושאפשרו לנו לאסוף פרטי מידע רבי-ערך בשאלה עד כמה היישום הנוכחי שלהן מקיים את התבחינים לזהות בריבונות עצמית.

כמתואר בחלקים הבאים, שני המיזמים האלו נתנו עדיפות לעקרונות מסוימים של זהות בריבונות עצמית שהולמים ביותר את תרחישי השימוש שלהם. בשני המקרים נראה שפתרונות הזהות מתמקדים בראש ובראשונה בעקרונות שעניינם תפעוליות בינית ושיתוף מאובטח של הצהרות זהות בין צדדים. גם עקרונות המזעור, ההסכמה, הניידות וההתמדה זכו לחשיבות רבה. השימוש ביומן בלוקצ'יין מועיל מפני שהוא מאפשר לחלוק מידע בבטחה בין צדדים רבים, והצדדים נדרשים לקבל רשות כדי לגשת למידע וכדי להוסיפו לבלוקצ'יין. מנקודת מבט של זהות, לזהות דיגיטלית מתמדת וניידת ולהיסטוריה דיגיטלית מתמדת וניידת יש ערך רב בקרב קבוצות אוכלוסייה פגיעות

בתנועה מתמדת. תוקף ההוכחות, בייחוד מארגונים מהימנים כמו קיווה וסוכנויות או"ם, חשוב כדי שמושא המידע תוכיח אמינות שוב ושוב ותקבל גישה למשאבים. עם זאת את עקרונות השליטה והגישה עדיין קשה להגשים מבחינה טכנית בכלכלות מתפתחות, משום שתפוצת השימוש בטלפונים חכמים והידע הטכני הנדרש למשמורת עצמית (self-custody) עודם בחיתוליהם. היעדר קישוריות הולמת ותשתית חומרה (למשל לרוב הפליטים יש טלפון נייד, אבל לא תמיד יש להם טלפון חכם) הוא אבן נגף עיקרית שיש לסלקה ממפת הדרכים לקראת זהות בריבונות עצמית. לכן יוזמות קיווה ואבני דרך נדרשו שתיהן ליישם דגמי משמורת בפתרונות הזהות שלהן ולצמצם מאוד את מידת השליטה של אנשים בזהויותיהם הדיגיטליות. עם זאת אפשר שיחול שינוי בכך בעתיד ככל שהטלפונים החכמים יוולו ומשתמשים ירחיבו את ידיעותיהם הטכניות. מכל מקום, שני מקרי הבוחר מלמדים לקחים חשובים בדבר המכשולים הרבים שבפני יישום פתרונות זהות בריבונות עצמית בהקשר ההומניטרי, ובדבר הגישות השונות שנקטה כל אחת מהיוזמות בניסיון להתגבר על מכשולים אלו בטווח הקצר, אגב התמקדות בצרכים המידיים של המשתמשים.

## ה. מקרה בוחן – קיווה: פתרון לצורך נתוני אשוראי<sup>98</sup>

קיווה<sup>99</sup> בונה פרוטוקול זהות שצפוי להיפרס בכל רחבי סירה לאון – עדות לחזון התוכנית ולחשיבות הספקת מערכת זיהוי דיגיטלית לקבוצות אוכלוסייה פגיעות. מנגנון קיווה מבוסס על דגם המזהה המבוזר והאישורים שתואר לעיל ומשתמש ב-Hyperledger Indy בתור שכבת הבלוקצ'יין הבסיסית. הוא מסתמך על מערכת זהות מבוססת-אישורים שבה המזהה הבסיסי הוא זוג מפתחות ציבורי-פרטי שאפשר לקשר אליו הוכחות רבות ואימותים רבים. מנפיקי אישורים בני אימות מכונים בפרוטוקול קיווה "עוגני אמון" (trust anchors), והם מסכנים את המוניטין שלהם בעולם האמיתי. פרוטוקול הזהות קיווה מעוצב כעת בתור מערכת מורשית פרטית שבה כל עוגני האמון זקוקים להיתר מקיווה או מממשלת סירה לאון כדי להנפיק אישורים, לחתום על הוכחות ולקרוא הצהרות זהות. בעתיד עשויים להיות עוגני אמון נוספים, למשל ארגונים לא ממשלתיים, חברות טכנולוגיה כמו פייסבוק וגוגל וארגונים אחרים שיוכלו לספק מידע שנדרש לזהות מסוימת.<sup>100</sup>

98 רוב המידע בחלק זה התקבל בשיחות ובראינות עם קווין או'בריאן וארון גולדסמית' מקיווה.

99 Kiva, <https://www.kiva.org/protocol>.

100 פרוטוקול זהות עתידי עשוי לאפשר עוגני אמון חסרי רישיון שאינם נזקקים להיתר ריכוזי מראש. לחלופין, עוגני אמון יקבלו היתר אוטומטי לפי מערכת של תנאים בני תכנות, למשל

כיום עוגני אמון מוגבלים לגופים ממשלתיים בסירה לאון ולגופי מיקרו-מימון משום שהמטרה המיידית היא לפתור בעיה שניצבת בפני תעשיית ההלוואות הקטנות – גורמים רבים אינם זכאים להלוואה משום שאין להם זהות רשמית ונתוני אשראי (מידע לאישור הלוואות). למעשה, ממשלת סירה לאון – באמצעות השפעת הבנק המרכזי שנותן רישיונות בנקים – תדרוש שכל גופי המיקרו-מימון, הבנקים והמוסדות הפיננסיים האחרים ישתתפו במערכת הזיהוי של קיווה בתור מנפיקי אישורים. הדבר נוגע בעיקר להלוואות קטנות בכלכלות מתפתחות שאין בהן סוכנויות אשראי לאומיות, מה שמקשה על מלוות לבדוק חבות צולבת. היעדר יכולת לבחון את כלל החובות של לווה, מקשה את קביעת מחיר הסיכון לאי-פירעון החוב ואת ביטוח ההלוואות הללו.

פרוטוקול קיווה פועל כמו סוכנות אשראי ומעניק ללקוחה פרטיות ושליטה רבות משמעניקות סוכנויות אשראי מסורתיות. אדם יכול לנייד את פרופיל האשראי, שמורכב מהוכחות אשראי ומהצהרות אשראי מקושרות, חלף נעילת הפרופיל בסוכנות אשראי ריכוזית. חשוב לציין שלקוחות קובעים מי רשאי לגשת לפרופיל שלהם, ואילו כיום כל אדם יכול לערוך בדיקת אשראי בלי רשות. בדגם קיווה לווה יכולה להחליט אם להעניק למלווה גישה לנתוני האשראי שלה.

כל אורח סירה לאון שזכאי לתעודת זהות ממשלתית יקבל מקיווה מזהה מבוזר וזוג מפתחות ציבורי-פרטי שקשור אליו כדי לחתום על הצהרות זהות, לצד הוכחה ראשונה ממשלת סירה לאון (בדמות אישור בר אימות שמכיל גיבובים של הנתונים הביומטריים של אותו אורח ומזהים אחרים שהממשלה הנפיקה). במסגרת של קיווה נתונים ביומטריים הם רק מאפיין נוסף שמקושר למזהה מבוזר, בדומה לתאריך לידה, מקום לידה וכל פרט מידע מזהה אחר. כך מצטמצם חלק גדול מהסיכון השיטתי לשימוש בנתונים ביומטריים בתור אמצעי בלעדי לזיהוי, כמתואר לעיל. מאחר שמידע ביומטרי אינו מזהה בשיטה זו, הנתונים הביומטריים ישמשו בעיקר למטרות וידוא ולא לזיהוי.

כל מי שמעוניינת לגשת למידע שמקושר לאותו פרופיל חייבת לבקש ממושא המזהה המבוזר (כלומר אותה אורחית) לתת רשות. בלוקצ'יין Hyperledger מתעד שצד שלישי (שמזוהה באמצעות המפתח הציבורי המקושר למזהה מבוזר) ביקש גישה לאותם הצהרות ואישורים בני-אימות, קיבל אותה ולבסוף ביטל אותה, לפי חותמות זמן. לכל אורח יהיה מזהה מבוזר בסיסי שממפה אין-סוף מזהים מבוזרים משניים שנוצרים עבור כל עסקת הלוואה חדשה או מערכת יחסים עם מלווה. אפשר גם ליצור מזהים מבוזרים משניים למטרות מגוונות, כלומר כל מזהה מבוזר משני מייצג אישיות אחרת או פרופיל

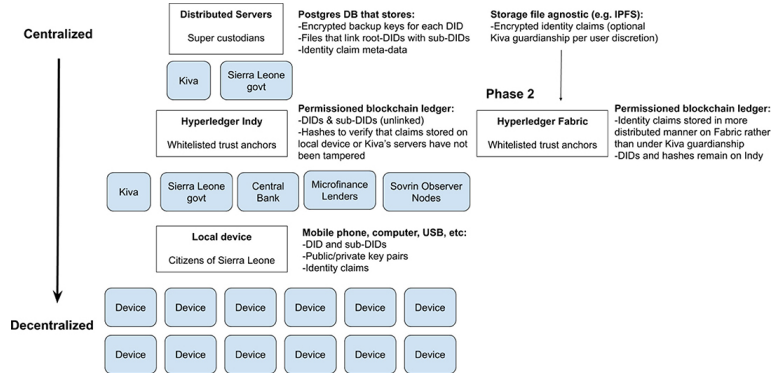
---

מספר האישורים או סוגי האישורים שמקושרים לעוגן אמון מסוים כדי להוכיח את המוניטין שלו.

שונה. השימוש במזהים מבוזרים משניים מאפשר מידה של פרטיות (ראו החלק על פרטיות להלן).

### 1. ארכיטקטורת פרופיל קיווה

זו הארכיטקטורה ברמה גבוהה (high-level architecture) של פרופיל הזהות קיווה:



בדגם רצוי כל המידע הרגיש – כגון מפתחות אישיים, הקבצים שמקשרים מזהים מבוזרים בסיסיים למזהים מבוזרים משניים, הצהרות זהות ומידע אחר – מאוחסן רק בתוך מכשירים שמושא הזהות שולט בהם, כמו טלפונים ניידים ומחשבים. כך השליטה במידע אישי ואחסונו מבוזרים מבחינה מבנית. אולם במדינות מתפתחות מצב זה יתקיים רק בעתיד, מפני שתפוצת השימוש בטלפונים חכמים עדיין קטנה (אולם היא גדלה במהירות בשווקים רבים) ולרבים אין בהכרח מכשיר אישי, למשל אפשר שבני משפחה חולקים מכשיר טלפון אחד. כיום אי אפשר לאחסן בבטחה מפתחות פרטיים בטלפונים "טיפשיים". לכן סביר שצדדים שלישיים, כמו ארגונים שלא למטרת רווח ועסקים, יהיו גורמי ביניים שמסייעים לנהל מפתחות פרטיים או מכשירים משותפים. בעולם מושלם לעולם אין חולקים מפתחות פרטיים, הם נותרים נעולים בארנקים במכשירים משותפים, וכשהמשתמש נכנסת למכשיר המשותף, היא יכולה לבטל את נעילת המפתחות הפרטיים שלה באמצעות נתונים ביומטריים, PIN או סיסמה.

גם אם ארגונים שלא למטרת רווח וארגונים קהילתיים אחרים משמשים נאמנים או גורמי ביניים שמסייעים למשתמשים לנהל את המפתחות הפרטיים שלהם, נחוץ לגבות את הצהרות הזהות ואת המפתחות הפרטיים. בשל הקשיים המעשיים בניהול זוגות מפתחות ציבורי-פרטי המקושרים למזהה מבוזר מסוים, פרופיל הזהות קיווה פורס דגם אפוטורפוסות שבו קיווה וממשלת סירה לאון הם משמורני-על במערכת. קיווה יפקיד בנאמנות את זוג המפתחות בשם מושא הזהות, שרשאי להוציא את המפתחות מחשבון

הנאמנות בכל עת. בדגם האפוטרופוסות של קיווה מפתחות גיבוי במשמורת מוצפנים, ואפשר לשחזר אותם רק בתהליך רב-גורמי, למשל נתונים ביומטריים, PIN או שניהם. שרתי קיווה מאחסנים גם קובצי מידע שממפים את הקשרים בין מזהים מבוזרים בסיסיים למזהים מבוזרים משניים קשורים, ומגבים עותקים של הצהרות זהות מוצפנות (בצירוף מטה-דאטה נלווה) בהתקן אחסון מידע נפרד כמו IPFS. בשלב הבא של הפרופיל יוכלו לאחסן את הצהרות הזהות המוצפנות אחסון מבוזר יותר ביומן מורשה, כמו Hyperledger Fabric, שעיצבו הולם אחסון מידע יותר מעיצובו של Hyperledger Indy, שהותאם לאימות מזהים מבוזרים. המידע הפרטי ביותר והרגיש ביותר מוחזק באפוטרופוסות בשרתים המבוזרים של קיווה במאגר הנתונים Postgres. ממשלת סיריה לאון עשויה לתחזק עותק מקומי של מאגר הנתונים (או מאגר נתונים מקביל) לפי תקנות המקומיות של סיריה לאון, שדורשות כי מידע רגיש על אזרחיה יאוחסן במדינה.

מתחת לשכבת האפוטרופוסות של קיווה נמצא יומן בלוקצ'יין מורשה פרטי שפועל על Hyperledger Indy. הבנק המרכזי של סיריה לאון יהיה צומת מורשה, לצד קיווה וממשלת סיריה לאון. מאחר שהבנק המרכזי דורש מכל המוסדות המלווים לדווח על עסקאות הלוואה בפרופיל, מלוות מיקרו-מימון ומוסדות פיננסיים נוספים שנתונים לסמכות הבנק המרכזי יידרשו להירשם בתור צמתים. נוסף על זה, צדדים אחרים, כמו ארגונים שלא למטרת רווח, רשאים לבקש להיות עוגני אמן או סוכנים (stewards, צמתים משקיפים של Sovrin). הדבר מסייע להגביר את האבטחה של היומן ואת חוסנו באמצעות גיוון צמתים הרחק מישויות שממוקמות בסיירה לאון.

הצמתים מאחסנים עותקים של המזהים המבוזרים ושל המזהים המבוזרים המשניים שאינם מקושרים אלו לאלו, ושל גיבוי הצהרות הזהות הקשורות אליהם. כמצוין לעיל, Hyperledger Indy לא נועד לאחסן מידע ממשי על הצהרות שמושאי הזהות יכולים לבחור לאחסן באפוטרופוסות של קיווה. לאחר מכן אפשר להעביר את אותן הצהרות ל-Hyperledger Fabric, שנבנה לתמוך במידע על הצהרות, כמתואר לעיל.

## 2. לעבוד עם פרופיל קיווה: צעד אחר צעד

נתאר כאן את הפעולות בפרופיל קיווה בסדר הצעדים המתוכנן, וכיצד אזרחית סיריה לאון תעבוד עם פרופיל קיווה כשיפרס במלואו. ממשלת סיריה לאון תקיים מבצעים לרישום אזרחים לפרופיל הזהות. אזרחים יירשמו בעמדות הצבעה, שם יקבלו תעודת זהות גשמית, ועליה נתונים ביומטריים, ותעודת זהות דיגיטלית בדמות מזהה מבוזר ומפתחות פרטיים מקושרים ומאוחסנים בארנק, רצוי במכשיר של האזרחית. במקרים רבים, כמתואר לעיל, לאזרחית אין מכשיר טלפון כלל או מכשיר שמסוגל להכיל מפתחות פרטיים בארנק. במקרה זה המפתחות והצהרות הזהות העתידיות יישמרו

באפוטרופסות אצל קיווה. ממשלת סיירה לאון תיתן את ההוכחה הראשונה באמצעות חתימה על הצהרת זהות שלפיה מדובר באזרחית סיירה לאון בעלת מידע מזהה רשמי, כגון מחרוזת ביומטרית או תאריך לידה.

כשהאזרחית, שנכנה אותה מרי, תלך למלוות מיקרו־מימון לבקש הלוואה, הבנק יבקש תחילה את הצהרת הזהות של מרי שחתומה בידי ממשלת סיירה לאון (תעודת הזהות הרשמית של המדינה). מרי תיכנס ליישומון (במכשיר הטלפון שלה או במכשיר בבנק) שמעניק לבנק רשות לאמת את ההצהרה החתומה של הממשלה. כדי להגן על הפרטיות רצוי שהבנק לא יקרא בפועל את תוכן ההצהרה (למשל נתונים ביומטריים ותאריך לידה) אם מידע זה אינו נדרש למטרות "דע את לקוחך" או אישור אשראי. הבנק צריך לדעת רק שהממשלה חתמה על הצהרה תקפה שמוכיחה את זהותה של מרי, מה שממלא את המחויבויות המזעריות של הבנק לצורך "דע את לקוחך".

לאחר מכן הבנק יבקש ממרי רשות לגלות את נתוני האשראי שלה. אם תשובתה של מרי היא "כן", היא תפתח את הצהרות הזהות שלה באמצעות המפתח הפרטי שלה. הבנק יאמת את הצהרות הזהות למול הגיבוכים ב־Hyperledger Indy כדי לאשר שהצהרות הזהות מלאות ומקוריות. אם נפלה בהן שגיאה, הבנק יקבל הודעת כישלון.

אם מרי אינה יכולה להשתמש במכשיר שלה לניהול הצהרות זהות ומפתחות, הבנק יבקש רשות לאחזר את הצהרות הזהות משרתי קיווה במישרין. כדי לחתום על האישור באמצעות מפתחותיה שברשות קיווה, יהיה על מרי לספק אימות באמצעות גורם שני, כמו נתוניה הביומטריים או PIN.

עם אישור ההלוואה יחתום הבנק על הצהרות זהות בנוגע לתשלומי ההלוואה ולהחזרים. מרי תקבל ביישומון בטלפון הנייד שלה הודעות המבשרות על כך שהבנק כותב הצהרה, למשל בנוגע להחזרים, ומרי תוכל לאשר את הפעולה.<sup>101</sup> ההצהרה תישלח למכשירה של מרי אם היא בוחרת לשמור מידע רק במכשיר המקומי שלה; או שהצהרה תוצפן ותאוחסן בארנקה של מרי באפוטרופסות בשרתי קיווה (קיווה עשוי לאחסן גם עותק לגיבוי אם מרי בוחרת בכך, גם אם היא מנהלת את המידע שלה במכשירה).

מרי יכולה גם לפתוח הליך ליישוב סכסוכים אם לדעתה הבנק כתב הצהרה שגויה או לא סיפק הצהרה על תשלום. הליך יישוב הסכסוכים יהיה כנראה מחוץ לבלוקצ'יין. מרי תגיש כרטיס ובו העובדות שגוף בורר יחליט בהן. אם הגוף הבורר יפסוק לטובת מרי ויקבע שהיא אכן שילמה לבנק את התשלום החודשי במזומן, ידרוש הגוף הבורר מהבנק לחתום על הצהרה כאמור, וְלא – הגוף הבורר יוכל לחתום עליה באמצעות המפתחות שלו.

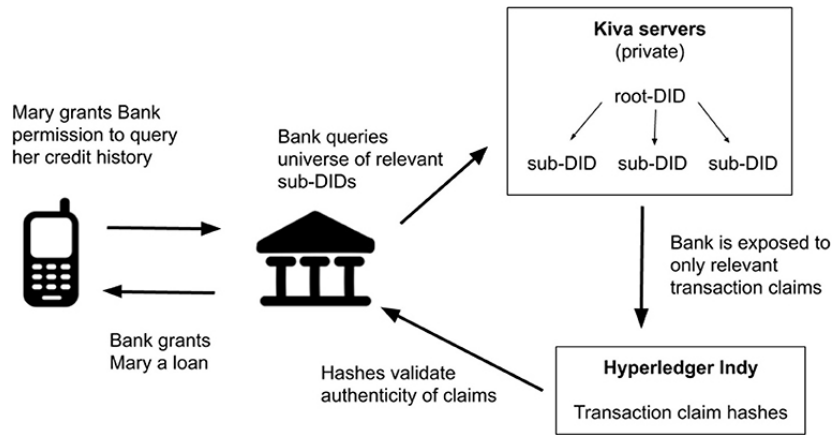
101 בשלב הראשון מרי תיתן בתחילת התהליך רשות לבנק לכתוב את כל ההצהרות שקשורות להלוואה שלה עד לפירעונה. קיווה מקווה להעניק בעתיד למשתמשת שליטה עוד יותר (בעיקר ככל שתפוצת השימוש בטכנולוגיה תגדל), ומרי תוכל להעניק **בנפרד** רשות לכל הצהרה שהבנק מעוניין לצרף למתאר שלה.

אם ההלוואה ופירעונה הם במזומן, יהיה על מרי לבטוח בבנק שישלח את הצהרת התשלום. היא תקבל כנראה קבלה גשמית על התשלום במזומן ותוכל להציג אותה לבנק ולבקש הצהרת תשלום (או לבוררת אם הבנק לא יעשה זאת). לפי דגם עתידי, אם ההלוואה ניתנת במטבע דיגיטלי, אפשר לתעד תיעוד אוטומטי את תשלומי ההלוואה והפירעון בתביעות זהות, ועסקאות הבלוקצ'יין יצורפו בתור הוכחת תשלום.

### 3. שיקולי פרטיות לעומת בעיית הגילוי הבררתי

כדי להגן על הפרטיות ולצמצם נזקים מפרצות אבטחה, פרופיל קיווה שואף לפעול לפי עקרונות ההוכחה באפס ידיעה (zero knowledge proofs), שלפיהם חושפים רק את המידע הנחוץ בהחלט ונוקטים צעדים להבטיח שאיש לא יוכל לחפש מידע במערכת בלי רשות. לפיכך כל הלוואה שמרי תקבל תקושר למזהה מבוזר משני חדש, ולא תחובר במישורין למזהה המבוזר הבסיסי שלה. הדבר ימנע מבנקים את היכולת לנטר פעילות אשראי עתידית שמחוברת למזהה המבוזר הבסיסי בלי לבקש רשות ממושא המידע, שכן עסקאות אשראי עתידיות יקושרו למזהה מבוזר משני חדש שייווצר, ולבנקים אין גישה לקובץ שממפה מזהים מבוזרים משניים ואת המזהה המבוזר הבסיסי שלהם.

הפרטיות מנוגדת לבעיית הגילוי הבררתי, שבו מלוות חייבות לבדוק אם קיים מינוף צולב. בתהליך האישור הבנק של מרי יכול לראות את מלוא נתוני האשראי שלה במזהים המבוזרים המשניים שלה, משום שאת תהליך האימות יפתח הבנק בשליחת שאילתה לשרתי קיווה כדי לקבל את כלל המזהים המבוזרים המשניים שמחוברים למזהה המבוזר הבסיסי של מרי. כמתואר לעיל, הקובץ שממפה מזהים מבוזרים משניים למזהה מבוזר בסיסי זמין רק בשרתי קיווה. אולם בשום שלב הבנק אינו נחשף למזהים המבוזרים המשניים עצמם או למזהה המבוזר הבסיסי גופו; הבנק נחשף רק להצהרות העסקה שמקושרות למזהים המבוזרים המשניים. לאחר מכן הבנק יעבור להשוואת הצהרות העסקה לגיבובים ב-Hyperledger Indy כדי לאמת את ההצהרות, כמתואר לעיל.



גם כשמדובר במערכת זהות בריבונות עצמית, לא כל הנתונים יהיו שייכים לאדם וגם לא יהיו בשליטתו, מפני שחלק מהנתונים יופקו בידי צדדים שלישיים יצרני הוכחות, ויישמרו בידיהם. לדוגמה, הבנק ימשיך לשלוט ברשומותיו בנוגע להיסטוריית ההלוואות שלקוחה קיבלה ממנו. אולם לעומת סוכנות אשראי ריכוזית, המידע לא ייאסף במרוכז ולא יישלח למפעיל יחיד. הנתונים יישארו בידי צד שלישי, ואילו ההוכחה המקושרת אליהם (בדמות הצהרה בת אימות) מוקצית בידי הלקוחה, נשלטת על ידיה ומאוחסנת בבלוקצ'יין. לכן אף שאזרחי סיירה לאון אינם שולטים בכל המידע עליהם, הם כן שולטים בצבר אישורים בני אימות שמייצגים את מאפייניהם, והם יכולים לצרף אותו בחופשיות לכדי זהות שמישה או לכדי צבר פרופילים ואישויות.

לבסוף, חשוב לציין שמערכת הזהות של קיווה היא בבסיסה מאגר של נתוני הצהרות בנות-אימות שאינן מפלה לרעה הצהרות זהות בעלות רגישות פוליטית. הוא תוכנן עבור סיירה לאון, אולם אפשר ליישם את אותה מערכת זהות עבור פליטים סורים למשל ולאפשר לממשלת סוריה להנפיק הוכחות לזהות של פליטה מסוימת באמצעות חתימה וחותמת זמן. גם אם ממשלת סוריה שהנפיקה את הזהות אינה קיימת עוד, הפליטה תוכל להוכיח את זהותה באותו מועד.

נחזור לרשימת עקרונות הזהות בריבונות עצמית. מערכת הזהות של קיווה מתמקדת ראשית בהסכמה, בתפעוליות בינית ובמזעור. זאת לצורך תרחיש השימוש העיקרי שלה – לאפשר למוסדות מיקרו-מימון לחלוק מידע וליצור תרשומת מתמדת של נתוני אשראי אגב שמירה על פרטיות הלווה (מוסד מיקרו-מימון יקבל רק את המידע הנחוץ להחלטתו). מלכתחילה בשל קשיים טכניים רוב המשתמשים לא ישמרו בעצמם את המידע בנוגע לזהותם, אולם המערכת מתוכננת להרשות למשתמשים לבחור שקיווה לא



יהיה משמורן-על בעניינם. במהלך הזמן תגדל תפוצת המשמורת העצמית והשליטה, והזהויות יישארו בניידות כללית ומתמידות.

## ו. מקרה בוחן – תוכנית המזון העולמית: פתרון לצורך מיטוב תוכניות סיוע בין סוכנויות או"ם והתאמתן זו לזו<sup>102</sup>

תוכנית המזון העולמית<sup>103</sup> היא זרוע הסיוע במזון של האו"ם וארגון הסיוע הגדול בעולם לטיפול ברעב ולקידום ביטחון תזונתי. תוכנית המזון העולמית מספקת סיוע במזון ליותר מ-80,000,000 איש ביותר מ-80 מדינות.

המגמה בשנים האחרונות היא לאפשר למקבלי הסיוע להחליט בעצמם מה לרכוש באמצעות התערבות על בסיס מזומן (Cash-Based Interventions) חלף חלוקת מזון ממש. בשנת 2018 חילקה תוכנית המזון העולמית יותר מ-1,700,000,000 דולר בהתערבות על בסיס מזומן, יותר ממחצית הסיוע הכספי שחולק במזומן בכל העולם.<sup>104</sup> בתנאים מתאימים תוכניות התערבות על בסיס מזומן יכולות להיות יעילות יותר, להיטיב יותר עם הכלכלות המקומיות ולהעניק מידה נוספת של כבוד האדם למקבלי הסיוע.

תוכנית המזון העולמית יזמה חדשנות בקרב סוכנויות האו"ם והכירה בארבע תרומות אפשריות של טכנולוגיית בלוקצ'יין להתערבות על בסיס מזומן: (1) הגברת יעילות, למשל הפחתת עלויות וסיכונים ושיפור אחריותיות ושליטה; (2) יצירת תמונת מצב מאוחדת של מקבלי הסיוע, ובאמצעות זאת הפחתת כפילויות ופיצול, יצירת אפשרויות למיטוב ולהתאמה וקישור גורמי סיוע שונים בחיבור אחד לבלוקצ'יין; (3) ריבוי אפשרויות הפדיון (כמו כספומטים, חנויות מזון, רשתות בריאות ובתי ספר) שזמינות לארגונים המעורבים ולמקבלי הסיוע; (4) סלילת הדרך לזהויות דיגיטליות מבוססות-בלוקצ'יין באמצעות הדגמה מעשית של הטכנולוגיה שבבסיסן ואיגוד בעלי עניין עיקריים על בסיס רשת בלוקצ'יין ניטרלית.

### 1. אבני בניין

בחלק זה נתאר מיזם מבוסס-בלוקצ'יין להתערבות על בסיס מזומן של תוכנית המזון העולמית שמכונה "אבני בניין".<sup>105</sup> מיזם אבני בניין נולד בינואר 2017 בהוכחת היתכנות

102 רוב המידע בחלק זה התקבל בשיחות ובראיונות עם הומאן חדר מתוכנית המזון העולמית.

103 Overview, World Food Programme, <https://bit.ly/31A6q2j>

104 World Food Programme, Giving Generously, Economist (Mar. 3, 2014), <https://www.economist.com/3d0kEpM>

105 Building Blocks: Blockchain for Zero Hunger, World Food Programme, <https://bit.ly/31A6H51>

של מאה אנשים בכפר אומרקוט (Umerkot) שבפקיסטן. המטרה אז הייתה להדגים שבלוקצ'יין יכול לשמש גם שלא ביישומי מטבע מבוזר. לצורך הוכחת ההיתכנות יצרו בבלוקצ'יין חשבונות מוטבים וטענו לתוכם אסימונים שמייצגים כסף מזומן או מזון. לכל מוטבת הוקצה מזהה אקראי בין 1 ל-100, שקושר בקשר אחד לאחד למפתח הציבורי שלה. כדי לממש את זכאותה נדרשה המוטבת להציג את עצמה לפני סוחרת מזון ולמסור את המזהה האקראי שלה. הסוחרת הזינה את המזהה של המוטבת ואת סכום המימוש ליישומן ברשת. יישומן הרשת שלח את הבקשה לאבני בניין, וזה שלח במסרון סיסמה חד-פעמית לטלפון ה"טיפש" של המוטבת בתור מנגנון אימות. המוטבת מסרה את הסיסמה החד-פעמית לסוחרת, וזו הזינה אותה ליישומן הרשת ושלחה אותה לאבני בניין. אם הסיסמה החד-פעמית הייתה תקפה, אבני בניין בחן את סכום המימוש המבוקש כנגד הזכאויות הקיימות בבלוקצ'יין. אם אלו הספיקו, הוא הפעיל את המפתח הפרטי של המוטבת המוחזק במשמורת, כדי לתעד עסקה ולשלוח בחזרה אישור לסוחרת. בראותה את האישור חילקה הסוחרת למוטבת כסף מזומן או מזון בכמות המבוקשת. לאחר מכן קבעה תוכנית המזון העולמית, על סמך נתוני אבני בניין, כמה היא חייבת לכל סוחרת, ושילמה לה במישרין.

לצורך הוכחת ההיתכנות השתמש אבני בניין בבלוקצ'יין הציבורי את/ריום. כך הוחלט בשל העובדה שבלוקצ'יינים ציבוריים מקיימים את עצמם באמצעות תמריצים קריפטו-כלכליים ורשת ציבורית של מאמתים, ולכן אינם תלויים בתוכנית המזון העולמית או באו"ם. אולם צוות המיזם שם לב שלבלוקצ'יינים ציבוריים מרכזיים יש ספיקת עסקה (transaction throughput) נמוכה ועלויות עסקה גבוהות בשל התפוצה הגבוהה של מנגנון ההסכמה המבוסס-עבודה (Proof-of-Work), שמבוסס על כוח חישוב כדי להבטיח עסקאות ביומן הציבורי שבו מתועדות העסקאות.

## 2. יישום בירדן

לאחר שהדגים את רעיון השימוש ביומן בלוקצ'יין ושילב את הלקחים מהוכחת ההיתכנות, במאי 2017 פתח אבני בניין בתוכנית הרצה רחבת היקף בהשתתפות 10,000 פליטים סורים בירדן. הרעיון דמה לזה בפקיסטן. עם זאת בתוכנית ההרצה בירדן עבר אבני בניין לבלוקצ'יין פרטי ומורשה, תוכנת הקצה Parity Ethereum עם אלגוריתם הסכמה של הוכחת סמכות (Proof-of-Authority). רשת הוכחת הסמכות הפרטית סיפקה לאבני בניין ספיקת עסקה גבוהה מאוד בלי עלות לפי עסקה. הרשת הפרטית סיפקה גם ערובות טובות יותר לפרטיות בהגנת המידע. החיסרון העיקרי של הרשת הפרטית הוא שאינה מקיימת את עצמה, אולם קוד החוזה החכם זהה ברשתות הפרטית והציבורית. לכן, כשהרשתות הציבוריות יפתרו כראוי את בעיות הספיקה, העלות והפרטיות, יוכל מיזם אבני בניין לעבור אליהן באמצעות "העתק-הדבק" לקוד שלו ותו לא. חיסרון נוסף הוא, שהואיל ויש בה צמתים מעטים

יותר, הרשת הפרטית עמידה פחות מהרשת הציבורית וחסונה פחות ממנה בפני חבלות. אולם כל צומת עצמאי נוסף בבלוקצ'יין מקרב את הבלוקצ'יין הפרטי לתכונות של אלו הציבוריים בהיבטי העמידות והמקובעות.

בניגוד להוכחת ההיתכנות בפקיסטן, שבה האימות נערך באמצעות מסרוני סיסמה חד-פעמית, בירדן השתלב מיזם אבני בניין במערכת האימות הביומטרית הקיימת המבוססת על זיהוי קשתית שנציבות האו"ם לפליטים מפעילה.<sup>106</sup> באבני בניין פליטה נדרשת רק לסרוק את קשתית הנקודת המכירה כדי לקבל סיוע במזון. כל העסקאות מתועדות בתשתית מבוססת-בלוקצ'יין-פרטי, שמשמשת מרשם לחישוב היתרה שעומדת לרשות כל פליטה וסכום הכסף שעל תוכנית המזון העולמית לשלם לסוחרות הנוגעות בדבר.<sup>107</sup> היתרון במערכת נעוץ ביכולתם של המוטבים לגשת לכספים ולהעביר אותם באמצעות התייצבות פשוטה לפני מערכת ההזדהות המבוססת על הנתונים הביומטריים, בלי צורך במכשיר כמו טלפון נייד. אכן, בהתחשב במצב הלא מבוסס של הפליטים בירדן קשה להניח קיומה של קישוריות קבועה למרשתת או שלכל המוטבים יהיה טלפון מתוחכם דיו לניהול מפתחות. הספקת גישה קלילה למוצרים חיוניים כמו מזון וכסף חשובה במיוחד לפליטים במצב קשה.

בדומה לקיווה, תוכנית המזון העולמית ניצבת בפני קשיים שעניינם בעלות משתמשי הקצה בטלפונים חכמים וקישוריות נתונים. לכן גם לאבני בניין יש דגם אפוטרופוסות למשמורת המפתחות שמשמשים לסמן עסקאות. תוכנית המזון העולמית היא המשמורנית של המפתחות הפרטיים של המוטבים, ואלו מופעלים באמצעות אימות קשתית ביומטרי כדי לסמן עסקאות בלוקצ'יין שקשורות להתערבות על בסיס מזומן. כמו בדגם קיווה, גם הדגם של תוכנית המזון העולמית מתוכנן לאפשר משמורת עצמית אם משתמשת תבחר בכך כשתונח תשתית מספקת לאפשר זאת, למשל זמינות של טלפונים חכמים, בעלי יכולת ניהול מפתחות, במחיר שווה לכל נפש. בסופו של דבר המטרה היא לספק לכל המוטבים מערכת חדשה של זוגות מפתחות ציבורי-פרטי (שהם יצרו וישלטו בהם שליטה מלאה) ולהעביר לארנקים הללו את אשראי הסיוע.

כמצוין לעיל, מנגנון אבני בניין של תוכנית המזון העולמית משתמש במערכת הביומטרית לניהול זהו<sup>108</sup> של נציבות האו"ם לפליטים לצורך אימות. נתונים ביומטריים במערכת זו כוללים למשל סריקות דיגיטליות מקוריות (כמו תמונות קשתית), ערכות תכונות (כלומר תבנית ביומטרית מופשטת מסריקות דיגיטליות) וצמצום של ערכות תכונות למחרוזת נתונים שמשמשת מזהה ייחודי. במהלך תהליך הרישום סוכנות האו"ם לפליטים אוספת את הנתונים הביומטריים של הנרשמת ומקשרת את המידע

.UNHCR, <https://www.unhcr.org/en-us> 106

Russ Juskalian, "Inside the Jordan Refugee Camp that Runs on Blockchain", *MIT Tech. Rev.* (Apr. 12, 2018), <https://bit.ly/3pvuYC1> 107

.UNHCR, Biometric Identity Management System, <https://bit.ly/3EAnx2O> 108

הביומטרי (שצומצם למחרוזת מידע) למזהה אקראי ייחודי במאגר המערכת הביומטרית לניהול זהות. אנשים מקובצים ליחידות משפחתיות (הפשטה ברמה שנייה), ולכל יחידה מזהה ייחודי (מחרוזת בת 12 תווים).

אימות במערכת הסיוע הכספי של נציבות האו"ם לפליטים דורש שהמוטבת תספק סריקת קשתית בנקודת המכירה עבור כל עסקה. התהליך פועל כך: תחילה, במערכת הביומטרית בנקודת המכירה אוספים את המידע הביומטרי באמצעות סריקת קשתית. הסריקה מומרת לתבנית, נשלחת לנציבות האו"ם לפליטים ונבחנת מול כלל התבניות במאגר המערכת הביומטרית לניהול זהות כדי למצוא את המזהה הייחודי שקשור ליחידה המשפחתית של המוטבת. המזהה נשלח למערכת אבני בניין של תוכנית המזון העולמית כדי לשלוף את זוגות המפתחות הציבורי-פרטי שקשורים לאותו מזהה. במפתח הציבורי יבדקו אם היתרה שעומדת לזכות המוטבת מספיקה לעריכת העסקה. אם היתרה מספיקה לממן את העסקה, המפתח הפרטי יופעל ויסמן את העסקה בבלוקצ'יין בשם המוטבת. כל שלב תקשורת בתהליך כולו מוצפן מקצה לקצה.

לעת עתה, הטמיעה המערכת סדרת נהגים מיטביים כדי להפחית את הסיכון בנתונים ביומטריים ריכוזיים, באמצעות הפרדת המשמורת על המפתחות (שבידי תוכנית המזון העולמית) מרישום המידע הביומטרי המקושר לזהות המוטבת (שנציבות האו"ם לפליטים מנהלת). לכן מנקודות המבט של פרטיות ואבטחת מידע אבני בניין של תוכנית המזון העולמית משלב את אמצעי הביטחון הנחוצים להבטיח שהסוחרת, הבנק, מעבד התשלום, רשת התשלום וגורמי ביניים נוספים לא ייחשפו למידע שאינו נדרש למילוי תפקידם. אכן, מעבד התשלום בנקודת המכירה נדרש לדעת רק אם הרוכשת נרשמה למערכת ואם היתרה בחשבונה מספיקה. הוא אינו נדרש לדעת מה הזהות שלה בעולם האמיתי ואפילו לא מהו סכום היתרה בחשבונה.<sup>109</sup>

יתרה מזאת, כדי לצמצם סיכוני אבטחה נציבות האו"ם לפליטים אינה מאחסנת מידע מזהה אישי כלשהו (כמו שם, אזרחות, תאריך לידה, מין ויחסים משפחתיים) עם המידע הביומטרי במאגר המערכת הביומטרית לניהול זהות. כל הנתונים הביומטריים מאוחסנים בבטחה ונפרדים לחלוטין מכל מידע אישי אחר. בדומה לזה, המערכת הביומטרית לניהול זהות אינה מאחסנת מידע על המפתחות האישיים של המוטבת – שניתן לגשת אליהם רק במערכת אבני בניין של תוכנית המזון העולמית. פרטיות הפליטים מוגנת אפוא היות שתוכנית המזון העולמית אינה יודעת את הזהות האמיתית של אלו שהיא מעבדת עת עסקאותיהם, ולנציבות האו"ם לפליטים אין גישה לעסקאות של אלו שהיא מזהה.

109 שימו לב שבמערכת אבני בניין היתרה מודפסת בתחתית קבלות העסקה של המוטבת. המוטבים מעריכים מאוד את המאפיין הזה. אולם מאחר שהמוטבת נדרשת לאשר את העסקה אישור ביומטרי, הקופאית אינה יכולה לחפש באקראי יתרות של מוטבים, אלא אם כן מוטבת הפעילה עסקה.

על בסיס הצלחת תוכנית ההרצה הוגדל מיזם אבני בניין בינואר 2018 כדי לשרת את כל 106,000 הפליטים הסורים שתוכנית המזון העולמית מסייעת להם במחנות בירדן. כעת מדובר ביישום הנרחב ביותר בעולם של טכנולוגיית בלוקצ'יין למטרת סיוע הומניטרי. עד היום התערב אבני בניין על בסיס מזומן בשווי 60,000,000 דולר ב-3,000,000 עסקאות וחסך עמלות בנקאיות בשווי 900,000 דולר.<sup>110</sup>

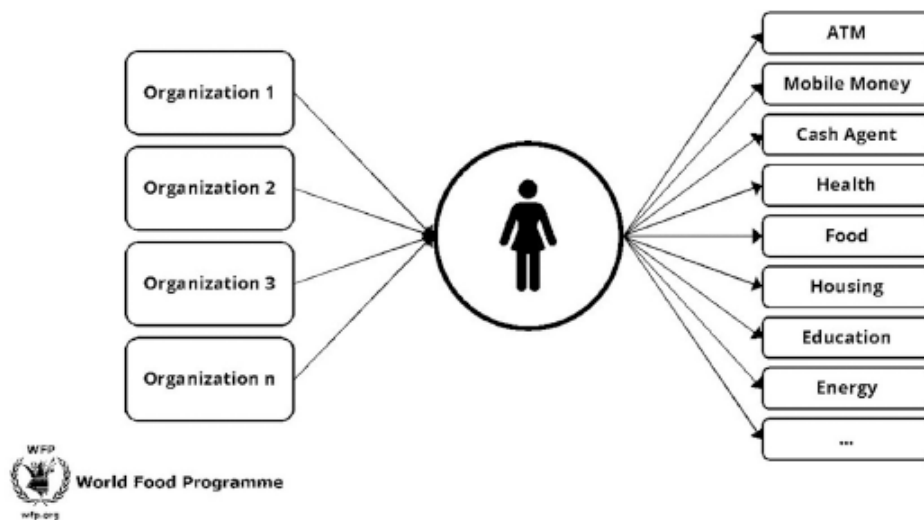
### 3. הצעדים הבאים

את כל מה שתואר בחלקים הקודמים אפשר להשיג במאגרי מידע מסורתיים. אולם מאחר שבלוקצ'יין הוא מושג חדש למדי, ולעיתים קרובות הוא תאורטי בעולם הסיוע ההומניטרי, אבני בניין הוא הצעד הראשון להסרת הערפל מכמה היבטים של טכנולוגיית הבלוקצ'יין בהדגימו כיצד הטכנולוגיה עובדת בהיקף נרחב בהקשר הומניטרי. בהיבט זה תוכנית אבני בניין היא מהראשונות מסוגה.

לאחר שהשיג את מטרתו העיקרית, אבני בניין מתכוון לצעוד כעת את הצעד הבא ולקבל לרשת חברים חדשים כדי לאפשר התקשרויות קלות עם מגוון סוכנויות שונות. לארגונים לא ממשלתיים יש דרישות אבטחה מיוחדות בהקשרים הומניטריים. ארגונים לא ממשלתיים בין-לאומיים מתקשים לעיתים קרובות להשלים איסוף מידע אישי בכמויות גדולות לצורך הנפקת זהויות דיגיטליות משותפות לכמה סוכנויות. במחנות הפליטים בירדן, לדוגמה, יותר מ-45 סוכנויות מסייעות לאותם מוטבים. אולם המערכות השונות אינן מקושרות קשר ממשי ואין ביניהן תפעוליות בינית. התוצאה היא כפל מאמץ ותמונת מצב מפוצלת למדי של מקבלי השירותים, שנאלצים לחשוף שוב ושוב מידע אישי בעוברם בין סוכנויות.

אם הארגונים הללו ינתבו את הזכאויות מהם למפתח הציבורי של כל מוטבת, תופיע תמונת מצב מאוחדת של מקבלי השירות וייווצרו הזדמנויות למיטוב ולהתאמה הדדית. תכנון תוכניות ומיקוד צרכים יהפכו לשוויוניים יותר. נוסף על זה, אפשר לקשר את כל הגורמים בקשר אחד לבלוקצ'יין ולחבר את השווקים השונים (כמו מזון, כסף מזומן, בריאות וחינוך). זהו פתרון אלגנטי משום שכל ארגון יכול לשמר את המערכות שבבעלותו לרישום, למיקוד ולניהול זכאויות, ובה בעת להימנע מפיצול.

110 החיסכון הושג כשכל ה"התחשבנויות" נערכו בבלוקצ'יין והבנקים רק שילמו לסוחרים. חיסכון דומה יושג בהקשרים אחרים או לא יושג בהם, לפי מציאות הביצוע בשטח.



או"ם נשים (UN Women)<sup>111</sup> הוא הארגון הראשון שהצטרף לרשת אבני בניין. תוכנית הרצה משותפת הושקה ביוני 2019 כדי להדגים בדיוק כיצד שני ארגונים או יותר יכולים לשתף פעולה בסיוע לאותם אנשים ברשת בלוקצ'יין משותפת. הדגם מיועד להיות תוכנית אב לשתוף פעולה נרחב יותר.

או"ם נשים (וכל חבר חדש נוסף) פועל בצומת אבני בניין עצמאי, וכל צומת מאמת כל עסקה ברשת ומתעד אותה. מאחר שכעת אי אפשר להניח שלכל המוטבים יש טלפון חכם וקישוריות, אבני בניין פיתח פתרון חדשני שמאפשר לכל ספק הומניטרי באבני בניין להיות משמורן של המפתחות הפרטיים שקשורים לזכאיות שלו, ובד בבד לשמור על תמונת מצב מאוחדת של מקבלי השירותים בבלוקצ'יין. אבני בניין אינו שומר מידע מזהה אישי כלשהו בבלוקצ'יין.

כשרעיון איחוד הזכאיות בבלוקצ'יין יודגם היטב ויתקבל, הצעד הקל הבא יהיה מעבר להוכחות זהות. ארגון אחד יוכל, למשל, להוכיח שמפתח פרטי נמצא בבעלות אם מיניקה. ארגון אחר יוכל לחפש את כל המפתחות הציבוריים להוכחת "אם מיניקה" ולמקד שירותים עבור מוטבות שלו – בלי שיצטרך לדעת מידע אישי רגיש עליהן.

החלקים השונים בתצורה הזוהו של אדם נמצאים בידי גורמים שונים. לכן, השגת שיתוף פעולה על סמך הבנה משותפת של הטכנולוגיה ושל כוחה להעצים את מקבלי השירות, חיונית כדי להשיג זהות מבוססת-בלוקצ'יין ממשיית באמצעות איסוף כל החלקים במקום אחד. אבני בניין נוקט גישה שלפיה את הדרך למערכת זוהו

<sup>111</sup> UN Women, <https://www.unwomen.org/en>

מבוססת-בלוקצ'יין מן המניין מוטב להתחיל ברכיבי הזהות הרגישים פחות. לדוגמה, אם זכאיות להתערבות על בסיס מזומן נקבעות ומופצות במבודד, פרטי העסקה הקשורים מפוזרים אף הם בין מערכות שונות וכן בין ספקי שירותים פיננסיים שונים. בתרחיש זה אם סוכנות אשראי תבקש לנתח את נתוני העסקה כדי להקצות דירוג אשראי לצורך אישור הלוואה, תהיה לה ודאי גישה רק לחלק מהמידע. על בסיס פרטי מידע מעטים יותר אפשר לקבוע את הסתברות הסיכון במידת דיוק פחותה, ולכן מקבלי השירות יחויבו בריבית גבוהה יותר. חלף זאת, אם כל הזכאיות ינותבו לארנק בלוקצ'יין מאוחד עבור כל מוטבת, ואישור העסקאות יגיע משם – גם נתוני העסקאות הפיננסיות יהיו מאוחדים. בהתבסס על זה ארגון כמו קיווה, שמשמש בפרופיל הוכחה באפס ידיעה למשל, יכול לקבוע למוטבת דירוג אשראי על בסיס המידע כולו, והתוצאה היא שיעור ריבית נוח יותר על הלוואה. יתרה מזאת, בעזרת אבני בניין המידע ניד, ולכן אם פליטה סורית תשוב לביתה, היא תוכל להשתמש במידע שהופק בירדן כדי לקבל בסוריה הלוואה להקמת עסק קטן ולשוב להתקיים בכוחות עצמה. שאם לא כן, המידע יישאר כנראה בידי ספקיות השירותים הפיננסיים בירדן ולא יהיה זמין לה בסוריה (או ביעד החדש שלה).

כמו פרופיל קיווה, גם אבני בניין מתמקד בראש ובראשונה בעקרונות התפעוליות הבינית והמזעור. לפיהם, סוכנויות או"ם רבות יכולות לשתף פעולה בבטחה כדי להשיג תמונה מאוחדת על אותה מוטבת, אולם שום מידע מזהה אישי אינו נחשף בבלוקצ'יין, ופרטיותה של מושא המידע אפוא מוגנת. עוד בדומה לקיווה, בהתחשב בתנאים באוכלוסיית המשתמשים קשה לנקוט משמורת עצמית, ולכן היא אינה בעדיפות ראשונה בשלב ראשון. בשני המקרים תשתית זהות מבוססת-בלוקצ'יין מאפשרת ניידות הוכחות לאוכלוסייה מהגרת. במהלך הזמן אפשר לבנות תרחישי שימוש נוספים על גבי מערכת הזהות, כגון שימוש בפרטי עסקאות התערבות על בסיס מזומן ברחבי סוכנויות או"ם רבות בתור פרטי מידע לניבוי איכות אשראי.

שאלה לעתיד היא אם פרופיל קיווה עשוי לפעול בתפעוליות בינית עם אבני בניין. עד עתה התמקדה תפעוליות בינית בשחקנים באותו תרחיש שימוש, למשל מוסדות למיקרו-מימון בסיירה לאון לגבי קיווה וסוכנויות או"ם לגבי אבני בניין. המשתמשים בכל מערכת זהות עשויים לחפוף זה את זה בעתיד מפני שהמיזמים הללו מתרחבים. לדוגמה, משתתפת (או משתתפת לשעבר) בתוכנית אבני בניין עשויה לבקש הלוואת מיקרו-מימון בתחום שיפוט שמשמש בפרופיל קיווה. באתחול בדיקת נאותות האשראי שלה, האם מוסדות המיקרו-מימון המשתתפים בתוכנית קיווה יכירו בעסקאותיה ובהוכחותיה מאבני בניין לעניין התערבות על בסיס מזומן? הכרה דורשת הן הסכמי מדיניות מחוץ לבלוקצ'יין והן תפעוליות בינית של תקנים טכניים בבלוקצ'יין. ולהפך, משתתפת בפרופיל קיווה עשויה להפוך למשתתפת באבני בניין. האם אפשר להשתמש באבני בניין בהוכחותיה מפרופיל קיווה כדי שלסוכנויות או"ם שונות יהיה מענה טוב יותר לצרכיה? האם שתי המערכות הללו מסוגלות לאפשר לצדדים מהימנים אחרים

מחוץ לקבוצה הראשונית של צמתים מורשים להפוך למוכיחים ולצמתים? תפעוליות בינית איתנה, תקנים טכניים והתאמות מדיניות יאפשרו למערכות הזרות הללו להשיג יכולת הרכבה (composability) ויכולת להיערם (stackability), כלומר יוכלו להרכיב יישומים חדשים על גבי שכבת הזרות הבסיסית.

## ז. נקודות מבט עתידיות

ככל שאנשים הופכים להיות יותר ויותר ניידים, כך מערכת זהות שימושית שמסוגלת לפעול בכל העולם הופכת להיות תנאי מקדים להבטחת הזדמנויות שוות בכלכלה הגלובלית. כלכלות מתפתחות בונות מחדש את מערכות הזהות שלהן, וחשוב לשים לב לתוצאות שמערכת בתכנון לקוי עלולה לגרום. לגישות הנוכחיות של מערכות זהות ריכוזיות מבוססות-ממשלה שמסתמכות על נתונים ביומטריים, יש מגבלות חמורות בהיבטי האבטחה והפרטיות.<sup>112</sup> מערכת זהות מבוזרת יותר ובריבונות עצמית שמשמשת באישורים בני-אימות ובפקדי גישה, אינה רק גמישה יותר ויעילה יותר, אלא גם עשויה לתרום להבטחת זכויות אדם בסיסיות, בייחוד במדינות שבהן הממשלה לא יציבה והמוסדות שבריריים.<sup>113</sup> בהתחשב במצבם החמור מהגרים, פליטים וקבוצות אוכלוסייה פגיעות אחרות עשויים לצאת נשכרים ממערכת שמאפשרת להם לגלות בבררתיות כמה מאפיינים ולא אחרים, לפי תרחישי השימוש.

### 1. תלות הריבונות העצמית בתשתית טכנולוגית

מערכת זהות בריבונות עצמית אמיתית דורשת רמת תשתית מסוימת, בעיקר חדירה גבוהה של טלפונים חכמים במחיר שווה לכל נפש שמסוגלים לאחסן בבטחה מפתחות פרטיים, וקישוריות מהימנה. גורמי מקצוע בתחום, כמו קיווה ותוכנית המזון העולמית, מכירים את תנאי החיים של לקוחותיהם: קבוצות אוכלוסייה פגיעות בסביבה שבה תשתית דלה, ורבים מהם חיים מתחת לקו העוני. לכן אי אפשר להניח זמינות גבוהה של התשתית הטכנולוגית ושל התחכום הטכני הדרושים לניהול עצמי של מפתחות פרטיים. בעיה נוספת באחסון מקומי של מפתחות – נוסף על זמינות חומרה – היא השבת מפתחות בכלל משום שבסביבה בניהול עצמי איבוד מכשיר הטלפון הפרטי גורר איבוד

112 Prabhakar, Pankanti & Jain (לעיל, הערה 50).

113 Victoria L. Lemieux, "In Blockchain We Trust? Blockchain Technology for Identity Management and Privacy Protection", *CeDEM17: Proceedings of the International Conference for E-Democracy and Open Government* (Peter Parycek, Noella Edelmann eds., 2017) 57



המפתח הפרטי. לכן המכשול הקשה ביותר אולי להשגת ריבונות עצמית מלאה הוא בעיית השבת המפתחות, בצירוף מחיר החומרה. לנוכח סוגיות אלו מוסכם שהנוהג המיטבי כעת הוא דגם משמורת או אפוטרופוסות שבו מנהלני תוכניות כמו קיווה או תוכנית המזון העולמית מנהלים מפתחות עבור המשתמשים, אבל המשתמשים יכולים לצאת מהאפוטרופוסות אם הם בוחרים בניהול עצמי.

כדי לעמוד באתגרים אלו החלו כמה חברות לבנות את הדור הראשון של טלפונים חכמים בבלוקצ'יין. אייץ'-טי-סי אקסודוס (HTC Exodus),<sup>114</sup> אחד ממכשירי טלפון הבלוקצ'יין הראשונים בשוק, יצא באוקטובר 2018. לטלפון אקסודוס יש סביבת ביצוע בטוחה (trusted execution environment) משלו לניהול מפתחות מאובטח ולחתימת עסקאות מאובטחת. הוא מפעיל מנגנון השבת מפתחות חברתי להשבת מפתחות פרטיים אם המכשיר או ביטויי הסיסמה (passphrases) אבדו; המשתמשת מחלקת את המפתח הפרטי בין שלושה לחמישה אנשי קשר.<sup>115</sup> אייץ'-טי-סי הוציאה ברבעון השלישי של 2019 טלפון בלוקצ'יין זול יותר בשם Exodus 1s, שמחירו יהיה בערך 250 דולר.<sup>116</sup> עבור רבים מלקוחות קיווה ותוכנית המזון העולמית המחיר עודו גבוה מכפי שידם משגת, אולם זהו צעד בכיוון הנכון.<sup>117</sup>

## 2. כסף דיגיטלי והחשיבות של זהות בריבונות עצמית

לשימוש ביומני בלוקצ'יין להעברת כסף מעמית לעמית (peer-to-peer) יש השפעות רבות בכלכלת פיתוח. הדבר מדגיש עוד את הצורך בפתרונות זהות בריבונות עצמית. יישום מעניין של טכנולוגיית בלוקצ'יין הוא ספרות (דיגיטיזציה) של מטבעות מקומיים או משלימים לכדי מטבע מבוזר דיגיטלי מראשיתו. בדרך כלל שער החליפין של מטבעות קהילתיים מקובע לזה של המטבע הלאומי בקיבוע רך (softly pegged), ולכן הם משמשים בעיקר אמצעי חליפין ולא מאגר ערך או יחידת חשבון. לדוגמה, "כלכלה מלמטה" (Grassroots Economics)<sup>118</sup> הוא ארגון שלא למטרת רווח בקניה שמנהל עם חקלאים כפריים תוכנית למטבע מקומי ששמו אשראי סרפופו

<sup>114</sup> Exodus, <https://www.htcexodus.com>

<sup>115</sup> Brian Barrett, Review: HTC Exodus 1, Wired (Feb. 26, 2019), <https://bit.ly/3EspZYW>

<sup>116</sup> Stan Schroeder, HTC's New, Cheaper Blockchain Phone Will Run a Full Bitcoin Node, Mashable (May 11, 2019), <https://bit.ly/304zcYA>

<sup>117</sup> לשם השוואה, הטלפון הסלולרי הראשון של "מוטורולה" נמכר ב-1982 תמורת 3,995 דולר. בימינו אייץ'-טי-סי, סמסונג וחברות אחרות מוכרות טלפונים חכמים חזקים הרבה יותר תמורת פחות מ-200 דולר. jimmy0209, History of Cellphones Prices, Timetoast, <https://bit.ly/3rMfwnE>

<sup>118</sup> Grassroots Econ., <https://www.grassrootseconomics.org>

(Sarafu Credit) מאז 2010. המטבע סרפו מקובע בקיבוע רך לשילינג הקנייתי, וחקלאים, סוחרים ובתי ספר בקהילה המקומית מכבדים אותו. בקהילות שבהן הגישה לכסף מזומן (שילינג קנייתי) מצומצמת, אין גישה לחשבונות בנק בגלל היעדר מסמכי זיהוי, וספקי כסף נייד כמו M-Pesa גובים עמלות גבוהות במידה מופרזת – חקלאים הולכים ומסתמכים על מטבעות קהילתיים מקומיים בתור פתרון משלים למטבע המקומי.<sup>119</sup> מאז אוקטובר 2018 הפכה כלכלה מלמטה את אשראי סרפו למטבע יציב (stablecoin) שניתן לשימוש באמצעות טלפונים "טיפשים". מטבע יציב הוא מטבע מבוזר שמשמש ביומן בלוקצ'יין ושערכו מקובע למטבע מקומי או לסל נכסים מובטחים (reference basket of assets). בעקבות הספרות של אשראי סרפו לכדי מטבע יציב שמקובע לשילינג הקנייתי, עלויות העסקה נמוכות במידה רבה הן מגרסת הנייר של סרפו והן מעסקאות M-Pesa. לדוגמה, העמלה לעסקה בשווי 101 שילינג קנייתי היא 11 שילינג ב-M-Pesa, אולם רק שני שילינג בסרפו (עלות שני מסרונים, קישור USSD ועמלות זניחות בגין הרצת עסקאות קריפטו בבלוקצ'יין צדדי של את'ריום).

מעניינת מאוד העובדה שמידע על עסקאות – שבתנאים אחרים היה בבעלות M-Pesa ובשליטתה או שבעסקת מזומן לא היה ניתן להתחקות עליו – אפשר לתעד כעת בבלוקצ'יין. הנתונים כוללים מידע סטטיסטי על סוגי הסחורות והשירותים שכל ארנק מנצל כסף עבורם, על היקף העסקאות וכדומה. בהיקשרם לזהות בריבונות עצמית, נתוני עסקה כאלו בקוד פתוח יספקו מידע התנהגותי עשיר למטרות אישור הלוואות קטנות, מיקרו-ביטוח ובקשות הומניטריות אחרות, כמו תכנון הערכת צרכים כדי לקבוע כמה סיוע במזומן להעניק למוטבים. בדרך כלל הערכת צרכים נעשית באמצעות קבוצות מיקוד וסקרים. נתונים דינמיים מעסקאות אמת מדויקים יותר באים בעיתם ומעלים תובנות רבות יותר כדי להבטיח שהמוטבים יקבלו כמות מספיקה של סיוע במזומן. יתרה מזאת, כמתואר בעניין דגם קיווה, אם מעניקים הלוואות במטבע מבוזר ופורעים אותן כך, הצהרות הלוואה ופירעון מתווספות מעצמן לפרופיל הזהות של קיווה. הדבר מחזק את פרופיל האשראי של המשתמש ומגביר את עושר הזהויות הדיגיטליות שלהן.

כלכלה מלמטה, סמפו (Sempu, חברת הזנק אוסטרלית) והצלב האדום עובדים כעת יחדיו ליצור מיזם בשם מטבעות הכללה קהילתיים (Community Inclusion Currencies), דגם לניתוב סיוע במזומן ומקורות אחרים של כסף מזומן מהמגזר השלישי ומהמגזר הפרטי בתור עתודות שמנפיקות את המטבעות המקומיים הללו בסכומים קטנים. באמצעות דגם של עתודה בסכום קטן אפשר למנף בייעילות תרומות במזומן וסיוע במזומן. לדוגמה, אפשר להנפיק תרומה במזומן בשווי 100 דולר בתור מטבעות הכללה

Tristan Dissaux, & William O. Ruddick, "Challenges of Collective Organization and Institution Building Around Community Currencies in Kenyan Slums", *Presentation at the 4th International Conference on Social and Complementary Currencies* (May 11, 2017).

קהילתיים בשווי 120 דולר. אם מטבעות הכללה קהילתיים נכנסים למחזור בקהילה במהירות גבוהה, ההשפעה הראשונית של אותו סיוע כספי בשווי 100 דולר גדלה עוד יותר. כדי לשמור על יציבות מחיר מטבעות ההכללה הקהילתיים, אפשר להציב סכר אלגוריתמי בפני פדיון מטבעות ההכללה הקהילתיים תמורת מזומן – בהתחשב בהיצע הקיים של מטבעות הכללה קהילתיים, בשערי הנפקתם של מטבעות הכללה קהילתיים ופדיונם ובחלק היחסי של העתודות. את מטבעות ההכללה הקהילתיים ינפיקו בתור מטבעות יציבים המקובעים למטבע הלאומי, ורצוי גם לאחסן את העתודה בתור מטבע יציב שמקובע להליך החוקי במדינה, ואילו ההנפקה והפירעון יהיו ממוכנים באמצעות חוזים חכמים. דגם מטבעות ההכללה הקהילתיים יאפשר מנגנון הניתן להרחבה ואף חלופי לבנקים קהילתיים. לדוגמה, קבוצות נשים לחיסכון והלוואה יפקידו את החסכונות השיתופיים שלהן בעתודה, וכשחברה תזקק להלוואה, החוזה החכם ינפיק מטבעות הכללה קהילתיים חדשים. במהלך הזמן יתווספו שיעורי ריבית וחסכון כדי להפוך מיזמים שונים של מטבעות הכללה קהילתיים לבני-קיימה מבחינה כלכלית. לפני שנתיים זכה מיזם מטבעות ההכללה הקהילתיים במענק מ"חדשנות נורווגיה", זרוע של ממשלת נורווגיה, כדי לערוך תוכנית הרצה ולהתרחב בקניה ובמקומות נוספים ברחבי העולם.<sup>120</sup> מטבעות יציבים מורים על עתיד שבו כסף יהיה בעיקרו כלל-עולמי ודיגיטלי אולם נטול בנקים.<sup>121</sup> עד להופעת המטבעות המבוזרים השמיע כסף דיגיטלי בהכרח עסקאות באמצעות בנקים, ובנקים או מוסדות פיננסיים אחרים (השערים למסילות הבנקים) ערכו בדיקות "דע את לקוחך" ובדיקות למניעת הלבנת כספים. כך, אלו שאין להם מסמכי זהות נותרו מחוץ לכלכלה העולמית הדיגיטלית.<sup>122</sup> מאחר שכסף הולך והופך להיות כלל-עולמי, עשויה להתפתח הזדמנות מקבילה להקים מערכת לניהול זהות כלל-עולמית באותה מידה ודיגיטלית שמגינה על פרטיות המשתמשים,<sup>123</sup> ושכד בכד עונה על דרישות משטרי האסדרה הכלל-עולמיים של "דע את לקוחך" ושל מניעת הלבנת כספים. בין כסף דיגיטלי לזהות דיגיטלית עשוי להתפתח אגבור (סינרגייה) בתיווך תשתית מבוססת-בלוקצ'יין, ובו נתוני עסקה ישמשו הוכחות שמגבירות את עושר פרופיל הזהות הדיגיטלי. הדבר עשוי לתרום לשיפור באישור בקשות אשראי ובהערכת צרכים הומניטריים ולהערכת סיכונים מדויקת יותר (ובסופו של דבר מכלילה יותר) לדרישות "דע את לקוחך" ומניעת הלבנת כספים.

Laurie Goering, Red Cross Boosts Disaster-Prone Communities with Blockchain 120  
"Cash", Thomson Reuters Found. (Nov. 26, 2019), <https://tmsnrt.rs/302x1EX>

Ronald J. Balvers & Bill McDonald, "Designing a Global Digital Currency" (2017), 121  
<https://bit.ly/3psjajG>

Claudio Borio & Piti Disyatat, "Global Imbalances and the Financial Crisis: 122  
Reassessing the Role of International Finance", 5 *Asian Econ. Pol'y Rev.* (2010) 198

Paul Vigna & Michael J. Casey, *The Age of Cryptocurrency: How Bitcoin and the 123  
Blockchain Are Challenging the Global Economic Order* (2016)

### 3. ביטוח זהות בתור אמצעי ביטחון ומקור הכנסה לספקי זהות?

רעיונות חדשניים בנוגע לזהות דיגיטלית ושווקים חדשים בנושא זה טרם התממשו. הצעה מעניינת בוחנת אפשרות ליצירת שוק ביטוח לנזקי הצהרות זהות,<sup>124</sup> שאפשר להקים על גבי מערכת לניהול זהות דיגיטלית בדומה לארכיטקטורת קיווה. שוק כזה יספק ביטחון ב"קילומטר האחרון" נגד שגיאות זהות (למשל הזנת נתונים שגויים למערכת הזהות) וייצור מנגנון שוק להערכת הדיוק של הצהרות שונות בקשר לזהות, לאמינותן ולשימושיותן.<sup>125</sup> מלוות יוכלו לאשר הלוואות בתחושת נוחות רבה יותר, בעיקר למי שאין לה נתוני אשראי רשמיים, אם ההצהרות שמקושרות לפרופיל שלה מבוטחות מפני נזקים בגין עלות ההלוואה. במהלך השנים יצמיח המשך פעולות ההלוואה הוכחות חדשות מהמלווה ובכך יגביר את האמון ויפחית את דמי הביטוח שלוה משלמת.

ביטוח זהות עשוי להפוך גם למקור הכנסה חדש לספקי זהות, כמו בנקים ומוסדות מיקרו-מימון, שנדרשים ממילא לערוך בדיקות "דע את לקוחך". במערכות ניהול זהות מעין-מבוזרות כאלו בנקים ומלוות יוכלו לבטח את הסיכון שבהנפקת אישור זהות בבלוקצ'יין. כך הם יסייעו למלוות עתידיות לבטל סיכונים וייצרו תמריצים כלכליים עבור מלוות שב"אפשרות ראשונה" (כלומר מלוות שמוכנות להלוות או להנפיק הצהרות זהות בשלב מוקדם בהיסטוריה הדיגיטלית של הלווה).

מהגרות שבידיהן הוכחות מעטות או שאין בידיהן הוכחות כלל, ישלמו דמי סיכון גבוהים יותר (משום שאין נתונים קודמים עליהן) עד שלמהגרות יהיו הוכחות איכותיות רבות יותר שיהפכו אותן למהימנות יותר. דגם כזה עשוי לעודד פליטים לפנות ככל האפשר למוסדות מסוימים או לארגונים מסוימים כדי לאסוף רשימה חיובית של אישורים בני-אימות, ובכך להפחית את דמי הביטוח שמקושרים לזהותם. במקרים מסוימים יכול להיות שסוכנויות, כמו נציבות האו"ם לפליטים וארגונים דומים אחרים, ישלמו חלק מדמי הסיכון. אף שדגם ביטוח כזה עשוי להועיל בסופו של דבר לפליטים ולעקורים שאין ממשלה חזקה שתערוב לזהותם, יש לנסות אותו רק לאחר מחקר נרחב שנועד לצמצם כל חיסרון אפשרי וסיכונים מערכתיים של ביטוח זהות כזה, כמו הכנסת הטיות לרעה לא חוקיות, הפליה ושיפוט ערכי שרירותי למערכת הזהות שבבסיסו.

124 Identity Ins. Consortium, <https://identityinsurance.org>

125 Fang-Fang Tang et al., "Using Insurance to Create Trust on the Internet", 46 *Comm. ACM* (2003) 337

## ח. סיכום

זהות בריבונות עצמית היא תחום מחקר חדש יחסית, ורק כעת היא מתחילה להתממש לכדי יישומים בעולם האמיתי של מערכות חדשות לניהול זהות דיגיטלית. יש לכך ערך בעיקר ביישומים שעשויים להרחיב הכללה חברתית והכללה כלכלית של קבוצות אוכלוסייה פגיעות ולשפר מאוד הכללות אלו.<sup>126</sup> אולם חשוב לזכור כי אף שמתפתחות אמות מידה ופרימיטיבים לנהגים מיטביים בתחום הזהות בריבונות עצמית,<sup>127</sup> אין פרוטוקול זהות כללי שפותר את כל תרחישי השימוש. כפי שמדגימים מקרי המבחן של קיווה ותוכנית המזון העולמית, הזהות תלויה מטיבה בתרחיש השימוש. תפעוליות בינית ותקנון חשובים לתפוצה, אולם הצלחתו של יישום זהות פלוני תלויה בהתאמה מדויקת של פריסתו לתרחישי השימוש ולתנאים המקומיים. מערכת מצליחה לניהול זהות נדרשת אפוא לגמישות מספקת כדי להסתגל לאופייה הגמיש מטבעו של הזהות האנושית.

פיתוח מטבעות מבוזרים בתור סוג חדש של כסף נייד בקוד פתוח, במיוחד מטבעות יציבים, יאפשר למשתמשים ליהנות מטווח נרחב של הזדמנויות עסקיות שמקורן בשירותים פיננסיים חדשים שנבנים על גבי אותן מערכות.<sup>128</sup> אישורים בני-אימות של גורמים מהימנים יכולים לשמש הצהרות זהות. כמתואר לעיל, אישורים חתומים בידי תוכנית המזון העולמית לטובת מוטבות מסוימות עשויים לשמש דירוג אשראי חלופי, וארגונים כמו קיווה יוכלו לספק הוכחות זהות. בדומה לזה, כלכלה מלמטה, שמנהל כעת את תוכנית סרפו בקניה, יוכל לחתום על הצהרות זהות בשם משתמשיו על סמך עסקאות סרפו, והדבר עשוי לסייע להם להשתדרג לפרוטוקול הזהות ומערכת הגומלין של מיקרו-מימון מבית קיווה.

בסופו של דבר קיווה תוכל לספק לשותפיה בתחום המיקרו-מימון הון להלוואות במטבע יציב בעסקה מעמית לעמית הזולה יותר מהעברת כסף בין-לאומית דרך בנקים ומהירה ממנה.<sup>129</sup> מלוות מיקרו-מימון יעניקו במישרין הלוואות במטבע יציב שערכו נקוב במטבע המקומי של הלווה. מלוות מיקרו-מימון בפרוטוקול הזהות של קיווה יחתמו חתימה אוטומטית על הצהרות זהות בעניין הענקת הלוואות ופירעונן היות שעסקאות כאלו הן כעת בנות-אימות בבלוקצ'יין, וכך יפחתו סכסוכים אפשריים. לאחר מכן יוכלו הלוות להשתמש בהלוואות הללו לצורכי מסחרן: רכישת מלאי לחנותן,

Sofie Blakstad & Robert Allen, *FinTech Revolution* (2018) ch. 7 126

McMullin, De Filippi & Choi (לעיל, הערה 44). 127

Jane Thomason et al., "Blockchain—Powering and Empowering the Poor in Developing Countries", *Transforming Climate Finance and Green Investment with Blockchains* (Alastair Marke ed., 2018) 137

Jake Darlington, "The Future of Bitcoin: Mapping the Global Adoption of World's Largest Cryptocurrency Through Benefit Analysis" (Apr. 21, 2014) (unpublished Honors Thesis Project, university of Tennessee) 129

תשלום משכורות לעובדיהן וכדומה. בעקבות זאת ישמשו הלוואות קודמות שנפרעו בהצלחה הוכחות זהות, יעשירו עוד את הנתונים הדיגיטליים של הלוות ואת פרופיל האשראי שלהן וייצרו מעגל קסמים חיובי למען הכללה פיננסית. דגמי עסקי זהות חדשים כאלו, כמו ביטוח זהות, יוצרו כנראה במערכת הגומלין האמורה של כסף נייד וזהות ניידת ובכך יגבירו את החוסן של המערכת כולה. ואף שעוד רחוקה הדרך למערכת זהות דיגיטלית, כלל-עולמית ובריבונות עצמית אמיתית, אנו מאמינות שטכנולוגיית הבלוקצ'יין עשויה להיות אחת מאבני הבניין העיקריות להוצאת החזון האמור מהכוח אל הפועל.