המכללה לביטחון לאומי

מחזור מ"ז 2019-2020

**טכנולוגיית בלוקצ'יין בשוק הביטוח**

ציון סופי 90

מגיש: הראל שרעבי ת"ז 034494229

מרצה: פרופ' דני רז

אפריל 2020

**רקע**

בשווקים הפיננסיים שונים, יש שחקנים שתפקידם המרכזי הוא לייצר אמון בין משתמשים בשוק הפיננסי. כך למשל בורסות ברחבי העולם מבטיחות כי עסקאות, לרבות חוזים פיננסיים, שמבוצעות בין קונים למוכרים יכובדו על ידי שני הצדדים. ללא קיומה של הבורסה, צד א לא היה נותן אמון שצד ב יקיים את חלקו בעסקה. גם מוסדות בנקאיים נותנים פתרון לבעיית האמון כדי שכסף פנוי שיש לאדם אחד יוכל להינתן כהלוואה לאדם אחר מבלי שהמלווה (המפקיד) יצטרך לתת אמון בלווה. הבנק מבצע שתי עסקאות אחת מול המפקיד/המלווה והשנייה מול הלווה וכך נפתרת בעיית האמון באמצעות גורם מתווך.

**תיאור הטכנולוגיה**

בלוקצ'יין (Blockchain) היא תפיסה טכנולוגית במחשוב המאפשרת פעילות עסקית מאובטחת באינטרנט ואימות של טרנזקציות עסקיות בין צדדים שונים ללא צורך בישות ניהול מרכזית. את הגורם המנהל מחליפים "בלוקים" מוצפנים של מידע הנוצרים באמצעות שיתוף מבוסס רשת תקשורת מסוג עמית לעמית (P2P).

בלוקצ'יין מיועד להגיע להסכמה בין גורמים שונים ובלתי תלויים על בלוקים של מידע שמחוברים בשרשרת. כל בלוק כולל מזהה וגיבוב של תוכן הבלוק הקודם וכן מתחבר אליו. כך נוצר מבנה נתונים מבוזר שעל תוכנו (תוכן השרשרת הראשית) יכולים להסכים כל הגורמים המעורבים. אין אפשרות לשנות את תוכן הבלוקים מרגע שהם נקבעו.

הרעיון המרכזי מאחורי בלוקצ'יין הוא יצירת מערכת לניהול עסקאות כספיות ללא גורם מרכזי מנהל. באופן מסורתי, בסיס הנתונים המרכזי של גורם מנהל מהווה את החוליה החלשה באבטחת מידע, שניתן לחדור אליה, לשנותה או לפגום ברשומותיה. הבלוקצ'יין, לעומת זאת, מנוהל באופן מבוזר, בתפיסת קוד פתוח. אנשים שונים במחשבים שונים בונים מעין סולם דיגיטלי של טרנזקציות, הכולל נתונים מוצפנים. אחת ליחידת זמן נכתבים הנתונים לבלוק. בתום זמן מסוים, ננעל הבלוק, ומצטרף כמעין שרשרת לבלוקים הקודמים.

הבלוקים מוצפנים באמצעות שילוב של מפתחות פרטיים ומפתחות ציבוריים. שינוי מחייב שחזור כל הבלוקים הקודמים, מטלה שהיא באופן מעשי בלתי אפשרית, כיוון שכל אחד ממשתמשי הרשת מחזיק העתק של הבלוקצ'יין. על הנתונים צריך להריץ אלגוריתם, המאמת את הטרנזקציה החדשה. אימות מחייב אישור של רוב נקודות הקצה, המחזיקות בנתונים ולכן שינוי מידע קיים הוא כמעט בלתי אפשרי.

בשורה התחתונה, בלוקצ'יין היא טכנולוגיה שמאפשרת לנו לסחור אחד עם השני בלי לסמוך אחד על השני.

**הרעיון**

עסקת ביטוח היא עסקה שבה הלקוח מעוניין להעביר סיכון מסוים לגורם מבטח, בדרך כלל חברת ביטוח, תמורת תשלום למבטח, ואם מתממש הסיכון, המבטח משלם ללקוח את הפיצוי/השיפוי המוסכם. חברת הביטוח מצדה מפזרת את הסיכונים באמצעות העובדה שיש לה הרבה לקוחות שרק לגבי מיעוטם יתממש הסיכון. גם בעסקת ביטוח, חברת הביטוח מהווה גורם מייצר אמון. במקום שכל לקוח ייתן אמון בשאר הלקוחות שהם יפצו אותו אם יתממש לגביו סיכון, חברת הביטוח מבטיחה לכל לקוח פיצוי ללא תלות בלקוחות האחרים.

באמצעות טכנולוגיית בלוקצ'יין ניתן להתקשר בעסקאות ביטוח ולהבטיח קיום של העסקה על ידי הצדדים ללא צורך בחברת ביטוח כגורם מתווך. למותר לציין ששוק הביטוח בישראל בלבד מגלגל עשרות מיליארדי ש"ח בשנה וחלק ניכר מהסכומים משמש לכסות את הוצאות התיווך ואינו משמש את עלויות הסיכון.

**ההישג המצופה**

ההישג המצופה הוא כתיבת קוד לשימוש בטכנולוגיית בלקוצ'יין שיבטיח שוק ביטוח הדדי אמין בעלויות מינימאליות. הקוד צריך לשקף חוזה ביטוח בין מבוטח לבין כל שאר המבוטחים באופן שיבטיח כי במקרה של אירוע ביטוחי למבוטח מסוים יבוצע התשלום המוסכם מכל שאר המבוטחים למבוטח שקרה לו האירוע והאופן שיבטיח אמינות של התרחשות האירוע שמזכה בתשלום.

**הסיכונים**

* הגנת פרטיות - בחלק מתחומי הביטוח, כמו לדוג' ביטוחי בריאות, יש צורך בהצפנת מידע רפואי לצורך הגנת הפרטיות.
* הטיות ומניפולציות טכנולוגיות - קיים סיכון שהקוד שנכתב מוטה וכולל מניפולציות שיתגלו רק אחרי שכבר מבוטחים יפגעו.
* שינויים בקוד - הקוד מגדיר את תנאי העיסקה. קיים סיכון שמישהו יעשה שינויים בקוד באופן שיפגע באחרים.

**אתגרים טכנולוגיים**

* אתגר כתיבת הקוד - באופן בסיסי עסקת ביטוח מורכבת מהגדרת האירוע הביטוחי שאותו מעוניינים לבטח (לדוגמא, מוות, תאונה, ניתוח וכדו'), קביעת הפיצוי שישולם בהתרחש האירוע הביטוחי, וקביעת הפרמיה שמשלם המבוטח עבור הכיסוי הביטוחי.

כתיבת הקוד שיהיה למעשה "פוליסת ביטוח" חכמה, צריך לכלול את כל מרכיבי עסקת ביטוח וכן צריך להיות כזה שלא יתאפשרו בו מניפולציות ביטוחיות. מאחר שפוליסות ביטוח רגילות כבר קיימות אז צריך "לתרגם" אותן לקוד. עם זאת יש לבחון אלו התאמות יש לעשות בקוד לאור העובדה שהפוליסה כתובה כקוד. בין אם מדובר בוויתור על תנאים שאינם נדרשים עוד בשת השימוש בטכנולוגיה או בצורך להוסיף תנאים אחרים בשל כך.

* אימות טכנולוגי להתרחשות אירוע ביטוחי - האמון שנדרש בתהליך בין הצדדים לעסקה הוא גם האמון הנדרש להבטחת קבלת הפיצוי כשמתרחש אירוע ביטוחי, אבל גם אמון על כך שבכלל התרחש אירוע ביטוחי. יש ביטוחים שבהם ניתן לאמת באופן פשוט יחסית את התרחשות האירוע, כמו לדוגמה אירוע מוות, שניתן לאמתו באמצעות מרשם האוכלוסין. לכן יש אתגר טכנולוגי לאמת התרחשות אירוע ביטוחי.
* סטנדרטיזציה של מידע - המעבר לטכנולוגיה דורש יצירת פרוטוקול אחיד להעברת מידע רלוונטי לחוזה הביטוח, בין אם זה מידע רפואי לצורך ביטוחי בריאות או מידע על מאפייני רכב ונהגים. ככל שהמידע יהיה יותר מפורט ניתן יהיה לייצר עסקאות יותר מדויקות ומגוונות.
* הבטחת תשלום עתידי - כאשר מתממש הסיכון הביטוחי צריך להתבצע תשלום של המשתתפים למבוטח שאירע לו האירוע הביטוחי המזכה בתשלום. כיצד מבטיחים שכל הצדדים לעסקה אכן יבצעו את התשלום במועד העתידי שבו יתרחש האירוע.

**לקחים ותובנות מהתהליך**

* שפה משותפת - צריך שלאנשי התוכן ולאנשי התוכנה תהיה שפה משותפת. לכל אחד מהצדדים צריכה להיות הבנה בסיסית של הצד השני כדי שהשיח יהיה יעיל ויצרני.
* להתחיל בקטן - מדובר במהפכה של ממש בעולם הביטוח ולכן חשוב להוכיח היתכנות במוצר מוגמר. ולכן צריך להתחיל בחוזה ביטוח פשוט שהאתגרים הטכנולוגיים בו פשוטים יחסית ורק אחר כך לעבור לחוזים המורכבים יותר.