БЕЗБЕДНОСТ ЕЛЕКТРОНСКИХ КОНТРОЛНИХ ЈЕДИНИЦА ВОЗИЛА ЗАСНОВАНА НА БЛОКЧЕЈН ТЕХНОЛОГИЈИ

Ђорђе Карић[1]

Резиме: Све већа приутност нових технологија у превозним средствима и све више аутоматизације процеса доводи до заначајних бенефита у виду бољих возних карактеристика, безбедности саобраћаја и смањењу саобраћајних гужви. Са повећањем броја мехатроничких система повећава се и ризик од напада малициозних програма. Компромитујући електронске контролне јединице смештене у возилу злонамерни софтвер може да пласира лажне информације у рачунарску мрежу и да утиче на одлуке које возило самостално доноси у току вожње. У овом раду обрађује се тема заштите података у паметним возилима, где би се комуникација између возила у циљу безбедности била омогућена само возилима са верификованим записима у блокчејну.

Кључне речи: мехатроника, рачунарске мреже, базе података, електронске контролне јединице, моторна возила. блокчејн технологија, децентрализација

SAFETY OF VEHICLE ELECTRONIC CONTROL UNITS BASED ON BLOCKCHAIN TECHNOLOGY

Abstract: The increasing presence of new technologies in vehicles and the increasing automation of processes lead to significant benefits in the form of better driving characteristics, traffic safety and reduced traffic congestion. As the number of mechatronic systems increases, the risk of malicious attacks also increases. By compromising electronic control units housed in a vehicle, malicious software can insert false information on a computer network and influence decisions that the vehicle makes on its own while driving. The focus of this paper is the topic of data protection in smart vehicles, where communication between vehicles for security purposes would be enabled only to vehicles with verified records in the blockchain.

Key words: mechatronics, computer networks, databases, electronic control units, motor vehicles. blockchain technology, decentralization

1. УВОД

Са развојем технологије у аутомобилској индустрији, у данашње време нова возила се не израђују више искључиво од механичких делова, него такође и од склопа комплексних елктронских уређаја под називом електронске контролне јединице (EKJ) које обезбеђују напредне функције вожње и олакшавају независно доношење одлука. Електронске контролне јединице добијају улазне податке од сензора и обављају прорачуне за задате наредбе. Оваква „паметна“ возила имају велики број осетљиве опреме уз помоћ које возило доноси самостално одлуке у току вожње, као и опреме која аутомобил чини свесним свог окружења. Малициозни упади могу да убаце малвер, односно злонамерни софтвер у електронску контролну јединицу и компромитују рачунарску мрежу возила. Унутрашња рачунарска мрежа возила заснива се на комуникацији између великог броја електронских контролних јединица преко сабирница као што је *CAN* магистрала. Компромитујући електронске контролне јединице смештене у возилу злонамерни софтвер може да пласира лажне информације у рачунарску мрежу и да утиче на одлуке које возило самостално доноси у току вожње. Овај рад се бави спречавањем злоупотребе електронских контролних јединица праћењем стања унутрашње рачунарске мреже уз помоћ блокчејн технологије.

[1] Ђорђе Карић, Машински факултет, Универзитет у Београду, e-mail: djordje.karic@yahoo.com

2. БЕЗБЕДНОСТ ЕЛЕКТРОНСКИХ КОНТРОЛНИХ ЈЕДИНИЦА

2.1. Електронске контролне јединице

Савремени аутомобил се не може замислити без мноштва електронских система. Развој у дизајну возила довео је до појаве електронских контролних јединица. Електронска контролна јединица добија податке са сензора и на основу унапред дефинисаних алгоритама шаље наредбе актуаторима. Електронска контролна јединица је главно „регулаторно тело“ сваке операције мотора. Рецимо, један од главних задатака електронске контролне јединице је контрола убризгавања горива. Користећи улазне податке са сензора, микропроцесор врши калкулације излазне вредности, након чега се те вредности претварају у одговарајуће сигнале. Основни подаци које електронска контролна јединица добија са сенора су брзина мотора и брзина возила, позиција мотора у циклусу рада, притисак пумпе горива, температура спољашњег ваздуха, температура расхладне течности, сигнал са квачила, количина убризгавања ваздуха, сигнали са кочионог система, паркинг сензори и мноштво других информација. Пристигли сигнали се обрађују у електронској контолној јединици и складиште у меморији. Након тога електронска контролна јединица контролише рад мотора, убризгавање горива током паљења и током вожње, лимитира максимално убризгавање и максималну брзину, контролише хлађење мотора, систем темпомата, издувне гасове и остало. [1]

2.2. Безбедност рачунарских мрежа у возилима

Системи безбедности рачунарских мрежа у возилима фокусирају се на неауторизован приступ систему и уочавање аномалија у раду система, као и одступања од прихватљивог понашања возила [2]. Поред свих напора, поједини безбедносни изазови и даље постоје. Системи који се тренутно користе базирају се на централизованом дизајну који се ослања на главну електронску контролну јединицу, односно мастер електронску контолну јединицу унутар возила. Ова решења су рањива јер је напад усмерен на главну електронску контролну јединицу, односно централни компјутер. Из овог закључујемо да је децентрализација електронских контролних јединица унутар возила неопходна ради боље сигурности целокупног система.

3. БЕЗБЕДНОСТ ВОЗИЛА ЗАСНОВАНА НА БЛОКЧЕЈН ТЕХНОЛОГИЈИ

3.1. Блокчејн технологија

Блокчејн технологија има потенцијал да реши горе поменуте проблеме и безбедоносне изазове укључујући централизацију система, доступност и поузданост података. Блокчејн је непромењив запис, односно неизмењива књига, листа података која обезбеђује поверљиве трансакције у форми међусобно повезаних блокова података. Технологија је први пут предложена у научном раду „Bitcoin: Peer–to-Peer Electronic Cash System“ Satoshi Nakamoto 2008. [3]. Иницијално је представљена као безбедно решење за систем трансакције крипто валуте биткоин, док је данас распрострањена технологија за немонетарне апликације које се користе у разним областима. Заснива се на серији блокова (записа), међусобно повезаних криптографијом, који носе потребне податке као и информације о валидацији и генерисању новог блока. Основи механизам иза ланца блокова је ткз. консензус механизам који обезбеђује поузданост, верификује информације и ажурира податке између корисника. Користи криптографију да обезбеди сигурност за трансфер и приступ подацима. Може да буде јаван или приватан, да има могућност да одлучи ко може да учествује у мрежи [4].

Он замењује централни систем поверљивим консензусом који обезбеђује да ни једна, у овом случају електронска контролна јединица, не преузима потпуну контролу. Такође, децентрализован консензус блокчејн технологије је сигуран систем за заштиту унутрашње рачунарске мреже јер редовно записује све операције извршене у возилу од електронске контролне јединице и тако лако може да закључи који запис је одговоран за коју промену стања. Блокчејн је привлачно решење уколико постоји намера или потреба да база података буде децентрализована.

Децентрализована мрежа не може бити хакована, манипулисана или подложна нападу као што традиционалне базе података јесу.

Блокчејн технологију чине четири кључне особине :

- Транспарентност – сви учесници могу да виде све записе који су унети у блокове
- Децентрализација – постојање већег броја рачунара који заједно учествују у мрежи, док свако од њих има могућност увида у податке који су унети, као и могућност уношења нових података
- Неповратност – једном унети податак у блок тамо остаје заувек
- Нема посредника, односно централног тела који би управљало и регулисало трансакције које се дешавају на мрежи

Функционисање сваке блокчејн мреже (била она намењена само одређеном броју људи или свима) регулисано је тачно одређеном процедуром. Пошто су блокови нераскидиво повезани захваљујући коду (сваки од њих има свој свој уникатни ИД који се назива хеш помоћу кога можемо пронаћи претходни блок из низа), било која промена података о обављеним трансакцијама, укључујући њихово брисање, додавање и било који други вид фалсификовања, није могућа.

3.2. Хеш функција

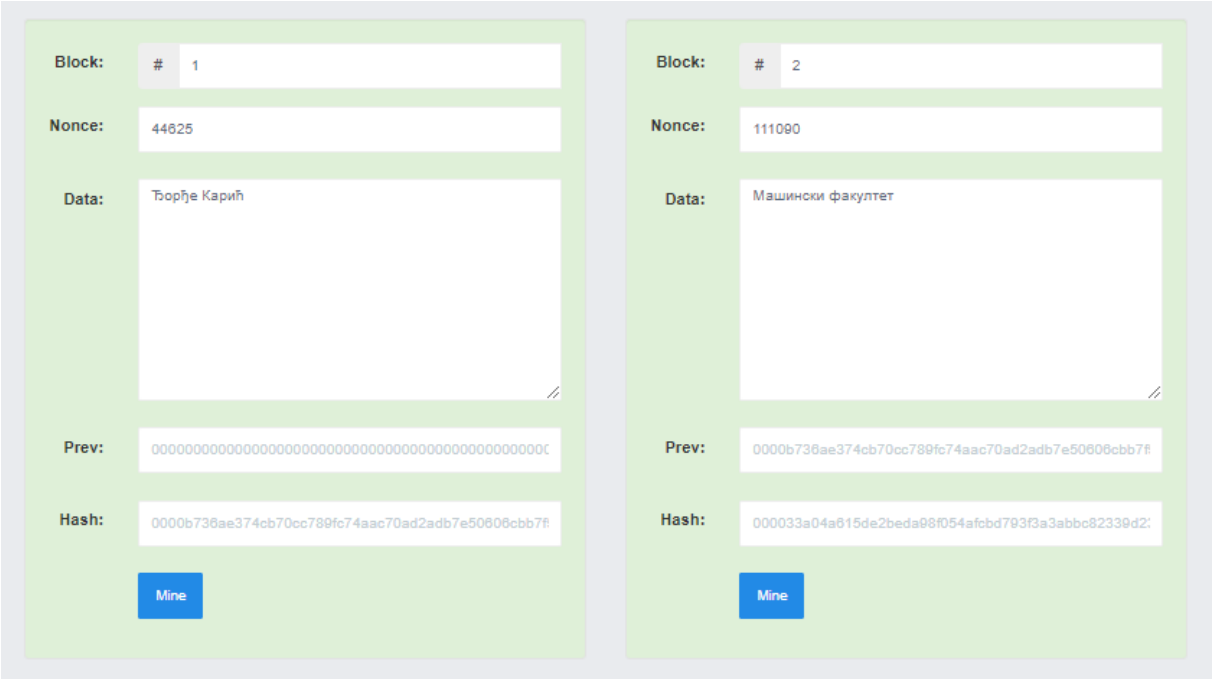
Хеш функција је математички модел који мапира податке произвољне дужине у податак фиксне дужине. Ако желите да представите речи различитих дужина, хеш функција би сваку од тих речи представила као јединствени низ бројева и слова.

Управо тај низ је познат као хеш. Хеш функција ће вратити исти хеш без обзира колико пута унели исте податке. Ако промените макар мало унете податке, хеш ће се у потпуности изменити. У блокчејну се користи механизам консензуса, где рачунари у мрежи погађају хеш. Први који погоди податке из хеша верификоваће блок.

СХА-256 (*SHA-256*) је сигурносни хешинг алгоритам који се налази иза биткоин протокола. Уређује креирање и управљање адресама, а такође се користи и за верификацију трансакција. Криптографске хеш функције су математичке операције које се врше над дигиталним подацима. Он узима улазни податак и конвертује га у алфанумерички низ фиксне дужине. Ово значи да колико год био дугачак улазни податак (стринг ограничен на 2^{256} -1 бит) излазна вредност ће бити низ од 256 бита [5].

Табела 1 – Пример промене Хеш функције услед промене улазног фајла

Редни број	Улазни податак	Излазни податак :
1.	Машински факултет	5ce1954e05a9074794d7756866a12e17b18a4a1d1676d3de2f6ff7cea7fdd265
2.	Машински факултеТ	c3cbb5f2b50009375f8a528886b5fb42cf29e0ab09eaf00b29dad03b7dcdbd50



Слика 1 - Пример блокчејна [6]

3.3. Потенцијалне претње за рачунарску мрежу у возилу

Изложеност возила интернету доводи до разних претњи по безбедност. У потенцијалном нападу на мрежу могу бити послати лажни подаци о стању на путу, лажни аларми о квару возила, могу бити измењени подаци о стварној брзини и брзини која се приказује на брзинометру, лажирање извештаја о судару до озбиљних безбедносних претњи као што је потпуно преузимање возила. Такође, безбедоносни изазов је и крађе података о возилу и кориснику.

Постоје различите врсте напада на рачунарске мреже. Неки од основних су :

- пресретање (engl. interception),
- пресецање, прекидање (engl. interruption),
- измена (engl. modification)
- фабриковање (engl. fabrication).

Пресретање је пасиван напад на поверљивост података. Може бити спроведено као прислушкивање саобраћаја, надзирање интезитета или увид у информације. Обично је припрема за неки озбиљнији напад.

Пресецањем се прекида ток неких информација и спречава пружање услуга и нормално функционисање система. Измена је активан напад на интегритет система. У рачунарском свету се може испољити као измена података, приступних права или начина функционисања програма.

Фабриковање је активан напад на аутентичност. Нпр. нападач генерише лажне податке, лажни саобраћај или издаје неовлашћене наредбе. У ове нападе спада и лажно представљање корисника, услуга, сервера или неког другог система [7].

3.4. Предложено решење заштите информација у мрежи засновано на блокчејн технологији

Примена блокчејн технологије односила би се на интеракцију, размену информација, од почетне када је возило регистровано на мрежи и како је запис креиран за то возило (генесис блок), како је електронска контролна јединица ажурирана и како врши проверу интегритета.

Због потребе да се прате промене стања електронских контролних јединица и да се прати понашање возила док је у функцији, предложен систем би се састојао од два главна блокчејна, два нивоа.

Ова два нивоа појашњавају улогу разних чинилаца у интеракцији и осигуравају да су чиниоци упознати са информацијама које је потребно да знају. Први ниво обухвата произвођача возила, техничке сервисере, осигуравајуће куће, правне и саобраћајне органе. Интеграција ових чинилаца у први ниво олакшава праћење извршених акција над електронским контролним јединицама као што је ажурирање или друге промене стања извршене од поверљивих субјеката.

Интеракције између чинилаца у овом нивоу имају фокус на регистрацији возила и на његовом одржавању. Иницијална регистрација података возила служи да се креира записа (блока) у првом нивоу. Овај запис чува податке о стању возила и вредности хеша свих електронских контролних јединица у возилу и користи се као валидација возила у другом нивоу. Ово се постиже тако што компјутер компарира тренутно стање возила и хеш фирмвера за сваку електронску контролну јединицу у другом блокчејну. Такође, први ниво чува записе о распореду одржавања и дијагностичих прегледа који показују шта се радило на возилу. Задатак другог нивоа је да идентификује када је електронска контролна јединица компромитована. Да би остварио ово, други ниво проверава интегритет електронске контролне јединице. Поред овога, други ниво прати и ситуацију у саобраћају, док податке добија искључиво од поузданих извора.

Децентрализацијим односно чувањем података у вези са возилом, као и радњи које изводе произвођачи и сервисери, у блокчејну, обезбеђујемо да ниједан ентитет не може модификовати било коју од ових радњи или података. Тим такође чувамо и безбедност мреже возила. Ограничавањем приступа информацијама само ауторизованим ентитетима обезбеђујемо приватност података, док верификовањем тренутног стања возила и упоређивањем са записом у блокчејну, осигуравамо да се комуникација дешава само између валидних страна.

4. ЗАКЉУЧАК

Рапидан напредак дигиталних технологија довео је до нових изазова у вези са заштитом података и заштитом рачунарских мрежа. Разне компаније и државне установе имају потребу за имплементирањем механизама за криптовање података и аутентификацију корисника. Блокчејн је веома функционална и позудана технологија, која може да реши изазове безбедности података и превенције злонамерних упада. Захваљујући њеној архитектури која осигурава да нико не може да мења податке у мрежи, она је тренутно најбољи вид заштите података који се међусобно размењују.

Решење изложено у раду предлаже идентификовање возила које је компромитовано и обезбеђује возило од могуће злоупотребе. На основу свега горе изложеног, безбедност рачунарских мрежа и њихова децентрализација у аутомобилској индустрији заснована на блокчејн технологији је нешто чему треба тежити у области заштите података и превенцији незаконитог уласка у систем.

Будуће примене ове технологије, могле би да се односе на примену блокчејна у аутономној вожњи и размени информација од сигурних извора са другим учесницима у саобраћају.

5. ЛИТЕРАТУРА

[1] Петровић, С.; Јанковић, Б.; Гроздановић, З.; Брацановић, Ђ. Борак, Б.: Теоретска верификација подсистема на возилу помоћу CAN бус и мониторинг електронске контролне јединице мотора, James F. Kurose, Keith W. Ross Умрежавање рачунара, ЦЕТ, Београд, 2018.
[2] Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto
[3] Tapscott, Don, and Alex Tapscott. Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world. Penguin, 2016.

[4] The Mathematics of Bitcoin — SHA-256, Toby Chitty
[5] https://andersbrownworth.com/blockchain/
[6] Плескоњић, Д.; Мачек, Н.; Ђорђевић, Б.; Царић, М.: *Сигурност рачунарских система и мрежа,* Микро књига, Београд,2007-