

Използване на блокчейн приложения и иновации в киберсигурността

Татяна Дочева*

Резюме: Разработката извежда необходимостта от киберзащита и прилагане на нови технологии в киберсигурността, във все по-дигитализирания ни свят. Разглежда развитието, приложението и потенциала на блокчейн технологията до настоящия момент, както и нейната същност. Представя възможните предимства и предизвикателства от прилагането на блокчейн приложения и иновации в киберсигурността, изведени от опита на вече въведени блокчейн иновации и приложения в други сектори на нашия живот. Разработката има по-скоро обзорен, отколкото аналитичен характер.

Ключови думи: киберсигурност, иновации, блокчейн.

JEL: L86, O31.

Актуалност

Обществото ни става все по-зависимо от глобалната информационна и комуникационна инфраструктура, но като всяко общо благо, наред с предимствата киберпространството доказано може да се използва като поле за злоупотреби.

Годишната цена на киберпрестъпността за световната икономика се

оценява на 5,5 трилиона евро в края на 2020 г., което е два пъти повече в сравнение с 2015 г. С повече от 10 терабайта данни, откраднати месечно, рансъмуерът е една от най-големите киберзаплахи в ЕС, като фишингът сега се определя като най-често срещаният първоначален вектор на такива атаки. Разпределените атаки тип „отказ на услуга“ (DDoS атаки) също се нареждат сред най-големите заплахи (<https://www.consilium.europa.eu/bg/infographics/cyber-threats-eu/>).

Броят и сложността на кибератаките и киберпрестъпността се увеличават в цяла Европа. Тази тенденция ще продължи да се засилва в бъдеще, тъй като до 2025 г. се очаква 41 милиарда устройства в световен мащаб да бъдат свързани с интернет на нещата.

Военната агресия на Русия срещу Украйна промени положението със заплахи в Европа през 2022 г. Конфликтът мобилизира много хактивисти, киберпрестъпници и държавно спонсорирани групи.

Еднакво засегнати от случайни киберинциденти или целенасочени кибератаки са публичният и частният сектор, както и цялото общество. По своята природа кибератаките са „асиметрични“ – с малки усилия и инвестиции могат да бъдат нанесени огромни поражения.

* Татяна Дочева е докторант в катедра „Национална и регионална сигурност“ на УНСС.

Това е причината, поради която гнес киберсигурността има толкова голямо значение. Кибератаките са сериозен и общ проблем в киберпространството и организациите по целия свят се напреварат да премахнат съществуващите слабости в своите мрежи и да ги укрепят срещу бъдещи кибератаки.

С приетите на 22 март 2021 г. заключения на ЕС относно Стратегията за киберсигурност, се подчерта, че киберсигурността е от съществено значение за изграждането на устойчива, екологична и цифрова Европа. Целта на Стратегията е да се засили устойчивостта на Европа срещу киберзаплахи и да се гарантира, че всички граждани и предприятия могат да се възползват в пълна степен от надеждни услуги и цифрови инструменти.

Република България участва активно във формирането и осъществяването на политиките за киберсигурност в рамките на ЕС и НАТО и се стреми към постигане на киберустойчивост на цялото общество и държава. Със Закона за киберсигурност (ЗКС) киберсигурността се определя като състояние на обществото и държавата, при което чрез прилагане на комплекс от мерки и действия киберпространството е защитено от заплахи, свързани с неговите независими мрежи и информационна инфраструктура или които могат да нарушат работата им.

Киберсигурността е от критично значение както за нашето благополучие, така и за сигурността ни. Бъдещата ни сигурност зависи от реформирането на способността ни да се защитим от киберзаплахи, като разчитаме на надеждни цифрови системи.

С реализирането на нови идеи и технологии се създават нови канали за достъп до пазара и се увеличава производителността, при това с относително ниски разходи. Три от тях: интернет на нещата, изкуственият интелект и блокчейн технологиите, имат изключителен трансформиращ потенциал.

Блокчейн технологията и криптовалутите въвежда иновативни решения в различни индустрии, включително киберсигурността. Използвайки децентрализираната и неизменна природа на блокчейна и криптографските характеристики на криптовалутите, тези иновации имат потенциал за подобряване на сигурността на данните, управление на идентичността, сигурни транзакции и смекчаване на киберзаплахите.

Блокчейн иновации

Наричана революционна, блокчейн е една от новите технологии, които дефинират Web 3.0 и Индустрия 4.0. Днес, в масовото съзнание тя все още се асоциира с биткойн, както и с другите криптовалути и дигитални активи, което е естествено следствие от бързия ръст на цените на криптоактивите през 2020 – 2021 г., подпомогнат в голяма степен от пандемията. Но освен представата и разбирането за блокчейн технологията като спекулативна търговия с криптовалута, тя има и много други приложения извън сектора на търговията и постепенно се превръща в иновация с много по-голямо влияние.

Блокчейн технологията позволява на хора и организации, които може да не се познават или да се доверяват един на друг, да се споразумеят и постоянно да записват информация без

посредничеството на трета страна. Създавайки доверие в данните по начини, които не са били възможни преди, блокчейн има потенциала да революционизира начина, по който споделяме информация и извършваме транзакции онлайн.

Технологията носи много предимства, които са от значение за днешния бизнес свят. Тези предимства включват сигурност, скорост, лекота, намаляване на разходите и прозрачност. Тези характеристики на блокчейн технологията я правят подходяща в много индустрии.

Вече има много успешни примери за блокчейн приложения, като интелигентните договори (smart contracts) и набирането на капитал онлайн (crowdfunding) са сред най-известните. Технологията е основата на цяло поколение от иновативни децентрализирани приложения (DApp), с различни случаи на употреба. Сектори, в които вече се прилага блокчейн технологията, са: Плащания, Финанси, Застраховане, Управление на веригата на доставки, Здравеопазване, Енергийният сектор, Управление на интелектуалната собственост, недвижимите имоти, гариелство, гласуване, социални помощи, хазарт, игри, хонорари на артисти и др. Такова приложение във веригата на доставки се наблюдава в селското стопанство и дори в бижутерския сектор, част от промишлените производители и др.

Блокчейн технологията е изминала дълъг път от появата на криптовалутите преди 13 години. Всяка една криптовалута е базирана на блокчейн, но това е само едно от приложенията на технологията. Разглеждайки нейното развитие, на което е основана криптовалута, тя преминава през четири основни цикъла до този момент, всеки от които продължава 3-4

години. Според етапите на крипто цикъла, растежът продължава около година и половина, след което настъпва корекция: цената на биткойн започва да пада и говоренето за него спира. За първите три цикъла е валидно: краят на всеки цикъл провокира началото на нов.

В първия крипто цикъл (2009-2012 г.) дори посветените крипто ентусиасти се отнасят към криптовалутите като към експеримент. Те дори не могат да си представят, че тяхната стойност може да се доближи до стойността на акциите на традиционните компании, а в бъдеще може напълно да промени финансовата система (фигура 1).

В първия крипто цикъл са създадени Litecoin и Namecoin през 2011 г., като могава стартират и първите крипто портфейли и майнинг пулове.

Във втория крипто цикъл (2012-2016 г.) притокът на нови лица е 10 пъти по-висок, отколкото в първия. Този цикъл дава живот на крипто индустрията, появяват се „второто поколение“ криптовалути, които имат функции като прикрити агресии, умни договори, странични вериги или активи: Monero, Ethereum, Ripple, Dash и NXT (фигура 2).

Третият крипто цикъл (2016-2019 г.) бе запомнен от цялата крипто общност и с право може да се нарече най-значимият: Появяват се ICO (Initial coin offering) – първоначално публично предлагане на токени (фигура 3).

В четвъртия цикъл (2021 г.-) всичко е същото както и в миналите цикли: Вегнага щом цената на BTC (Bitcoin) започва да расте импулсивно, за това се заговорва навсякъде (фигура 4). Участниците на пазара отгавна са забелязали, че колкото повече се спекулират определени

цифрови активи в мрежата, толкова по-бързо нараства стойността им.

Заслужава да се отбележи обаче, че в този крипто период наблюдавахме историческо събитие: институционалните инвеститори започнаха да инвестират в криптовалути, съответно с много по-големи инвестиции и това доведе цифровото злато към голямо увеличение: На 11 декември 2020 г. биткойнът струваше 17 800 долара, а на 14 април 2021 г. актуализира рекордното си ниво от 64 600 долара. Погледнато в проценти, този ръст е много по-малък отколкото в предишните цикли, както се вижда на фигурите по-долу. Но ако разглеждаме основната криптовалута на фона на цялостната картина, няма по-скъп актив на финансовия пазар.

В допълнение, традиционните финансови компании, които предоставят своите услуги по целия свят, или вече са внедрили технологията, или активно работят по нея, предлагайки многообразни крипто услуги. Сред тях са: Visa, MasterCard, PayPal, JP Morgan Chase, Goldman Sachs Group, Tesla, Citigroup и други. Също така много централни банки прилагат блокчейн за създаване на собствени централни банкови цифрови валути (CBDC).

Въпреки че DeFi и NFT не са нови насоки в крипто индустрията, те получиха активно развитие само от началото на четвъртия крипто цикъл. Появиха се много проекти, които се определят като нови области на сектора. В резултат на това крипто индустрията вече има огромна подкрепа от традиционния финансов сектор.

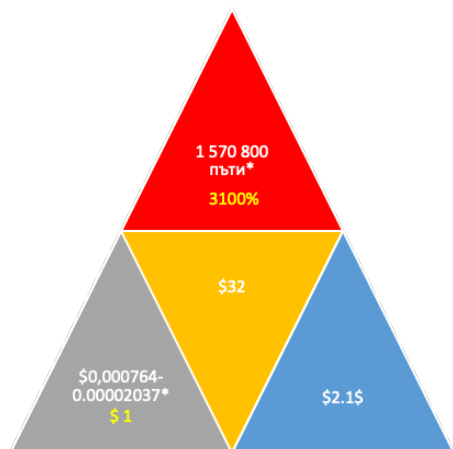
Едно от най-значимите събития през 2023 година, според крипто общностите,

е все по-голямата яснота от регулаторните органи за блокчейн и дигиталните активи. Бяха предприети действия, като освобождаване на регулаторните рамки, които ще насърчат иновациите, вместо да ги възпрепятстват. Не само правителствата и регулаторите вече се убеждават в истинския потенциал на Блокчейн технологията, но и институционалните инвеститори приемат криптовалутите като един висок клас активи и допринасят за реализиране на потенциала на технологията.

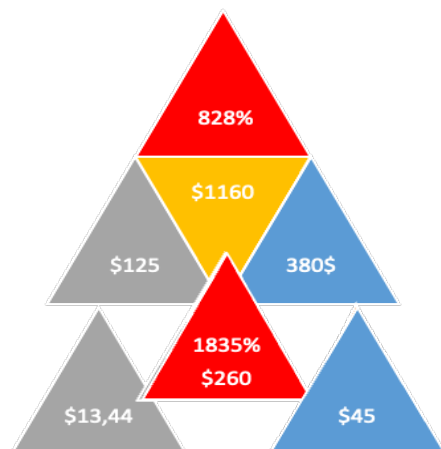
ЕС прие Европейска блокчейн стратегия и лансира Европейска програма за блокчейн инфраструктура за публичния сектор, чиито приоритетни и основни приложения и насоки са:

- Екологична устойчивост: блокчейн технологията трябва да бъде устойчива и енергийно ефективна;
- Защита на данните: блокчейн технологията трябва да е съвместима и, когато е възможно, да поддържа строги европейски разпоредби за защита на данните и поверителността;
- Дигитална идентичност: блокчейн технологията трябва да зачита и подобрява развиващата се рамка за дигитална идентичност на Европа;
- Киберсигурност: блокчейн технологията трябва да може да осигури високи нива на киберсигурност;
- Оперативна съвместимост: блокови вериги трябва да са оперативно съвместими помежду си и с наследени системи във външния свят.

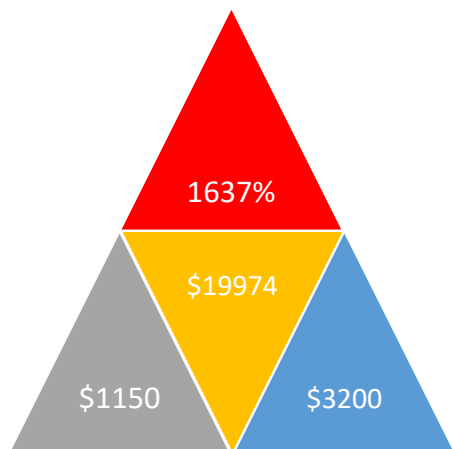
Европейската комисия постави и сериозен акцент върху насърчаването на блокчейн технологията в борбата с климатичните промени, за устойчиво



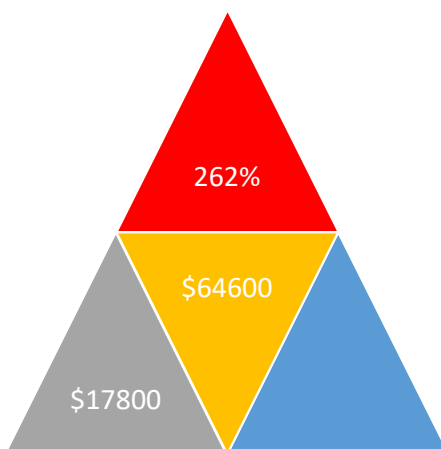
Фигура 1. 2009-2012 г.



Фигура 2. 2012-2016 г.



Фигура 3. 2016-2019 г.



Фигура 4. 2021 г.

Легенда: Преглед на историята на цената на биткойна | Binance Academy
(Сколько стоил Биткойн в начале (prostocoin.io))



икономическо развитие и за реализацията на Европейската зелена сделка.

Европейската комисия силно подкрепя блоковата верига на политическите, правните и регулаторните и финансиращите фронтове. Най-важните части на блокчейн стратегията му включват: Изграждане на общоевропейски блокчейн за обществени услуги; Насърчаване на правната сигурност; Увеличаване на финансирането за научни изследвания и иновации; Насърчаване на блокчейн за устойчивост; Подкрепа за оперативната съвместимост и стандартите; Подкрепа за развитието на блокчейн умения; Взаимодействие с общността.

Какво е Blockchain?

Блокчейн (Blockchain) или Блокова верига, известен още като DLT, е метод за съхранение на информация в компютърна мрежа, който представлява непрекъснато растящ списък от компютърни записи, наречени „блокове“, свързани помежду си и кодирани криптографски. Всеки блок съдържа информация за предходния и е удостоверяван за време, което гарантира хронологична цялост. След като се валидира и запише, за да се промени един блок се изисква консенсус на мнозинството в мрежата. Ако един блок данни се промени, всички следващи блокове ще бъдат анулирани. Информацията е криптирана в дигитална таблица и може да бъде достъпена от всеки. *Hash function* (хаш функцията) осигурява неизменчивостта на данните – тя преобразува данните в код, според вида на алгоритъма, който съдържа точно определен брой символи, независимо от големината на информацията, и ги имплементира в блокчейна. Хашът е низ от букви и цифри, който

не може да се повтори и може да бъде разпознат по него. Първият блок и начинът за добавяне на последващи такива се обуславят от хашинг алгоритъма и вида на консенсуса. Те са заложили в кода на блокчейна, познат още като консенсуален алгоритъм (*consensus algorithm*). Участниците в мрежата се наричат възел или нод (*node*).

Видовете блокчейн мрежи са публични, частни, хибридни и консорциумни. За разлика от публичните, частните блокчейни са притежание най-често на един субект (например на една компания) и са с точно определени разрешения и правила, и съответно не са отворени за обществеността и не са децентрализирани, но могат да бъдат разпределени. Хибридните блокчейни комбинират характеристиките на публичните и частните блокчейни в гъвкава мрежа, която решава кои потребители да допусне до какви данни и кои транзакции да бъдат публични. Консорциумните блокчейни обединяват множество организации в една обща споделяна мрежа, която се управлява съвместно от няколко равноправни субекта и има гъвкави правила относно видимостта на мрежата, промените и дали да бъде отворена или затворена (Какви са основните типове блокчейн мрежи?

<https://studioweb.bg/post/kakvi-sa-osnovnite-tipove-blokcheyn-mreji-9898#:>

Как Blockchain може да стимулира киберсигурността

Блокчейн приложенията и иновациите в киберсигурността имат потенциала да революционизират начина, по който подхождаме към сигурността на данните, управлението на идентичността, сигурните транзакции и споделянето на

информация за заплахи. Като се възползват от децентрализирания характер на блокчейн технологията и криптографските характеристики на криптовалутите, тези иновации осигуряват подобрена защита срещу киберзаплахи, подобрена цялост на данните и повишена прозрачност. Тъй като блокчейн технологията и криптовалутите продължават да се развиват, тяхната роля в укрепването на практиките за киберсигурността ще стане още по-видна, създавайки по-сигурна цифрова екосистема както за физически лица, така и за организации.

Въпреки че блокчейн е отворен регистър, предаването на данните се провежда стриктно и се осъществява с използване на най-силните криптографски методи. При широко внедряване на тази технология, която се счита за по-надеждна от традиционните системи, вероятността за осъществяване на взлом съществено намалява. Нивото на киберсигурност се повишава и благодарение на почти пълното елиминиране на посредничеството на хора при реализация на процесите. Неговите характеристики – *децентрализация, неизменчивост и прозрачност*, го правят отлично решение за проблемите на киберсигурността.

Децентрализация: Децентрализацията на Blockchain би намалила значително шансовете за подправяне на базите данни, дава възможността да се преодоляват големи хакерски атаки като DDoS, DoS или кражба на лична информация.

Тъй като цялата информация се съхранява в мрежа на блокчейн и всяка промяна на блокчейна е видима за всички, както и че тя трябва да бъде потвърдена от мнозинството, подобна атака би взела необичайна изчислителна сила, която

значително би обезсърчила всеки да направи подобен опит.

Начинът, по който киберпрестъпниците успяват да се сдобият с информация, обикновено е да атакуват мястото, където всички данни са групирани – традиционно данните се записват на централен сървър, който е уязвим на атаки. На блокчейн това е изключително непрактично, ако не и почти невъзможно. Тъй като цялата информация се съхранява в мрежа на блокчейн, не съществува артерия за данни, към която престъпниците да се насочат. Вместо това, те ще трябва да корумпират същите данни за всеки блок. Естествено винаги съществува възможност отделен потребител да бъде атакуван, но това застрашава само него, не цялата мрежа. В достатъчно голяма мрежа с отворен код, както и достъпните за четене транзакции, несъдържащи лични данни, осигуряват прозрачност, защита и свобода за потребителя.

Прозрачност и непроменливост: Обществената мрежа има предимството да съхранява всичките си данни в очите на обществеността. Всяка промяна, направена в нея, лесно се открива и проследява. Вероятността да остане незабелязана промяна също може да бъде равна на нула. Освен това, благодарение на хеширането, когато се добавя или модифицира низ за данни, записът и на актуализацията, и на неговото предишно състояние остават видими, нито един от които не може да бъде изтрит. По този начин кибернашествениците се сблъскват с допълнителното предизвикателство на ясно видим маркер, който показва всяка стъпка от тяхната атака.

Това би означавало, че кибернападателят ще трябва да влезе незабелязано в блокчейна, да направи промени, без да го разкрият и да се измъкне без да бъде забелязан. Ако добавим и по-горе споменатата трудност за достъп до всеки блок получаваме задача, която е твърде неосъществима за почти всеки да я изпълни ефективно.

Силата на блокчейн технологията:

Предимствата и недостатъците на блокова верига с и без криптовалута

Непрекъсваемост и сигурност: При блокчейн данните се съхраняват на хиляди устройства и всеки мрежов възел може да репликира и съхранява копие на базата данни и поради това един възел, който излиза, не засяга наличността или сигурността на мрежата. Докато при традиционите бази данни се разчита на един или няколко сървъра, което ги прави по-уязвими към технически повреди и злонамерени атаки. Сриът на един сървър може да свали цялата информация извън линия и да разчитаме единствено, че последното архивиране е било сравнително скоро.

Защита на цялостта на данните: Присъщите свойства на Blockchain, като неизменност и механизми за консенсус, го правят ефективен инструмент за гарантиране на целостта на данните. Блокчейн технологията може да предложи на компаниите алтернативен метод за съхраняване на техните данни, които ще осигури повече защита срещу пробиви.

Чрез съхраняване на данни в разпределена книга, всякакви промени или опити за подправяне са лесно откриваеми, като се запазва целостта на критичната

информация. Това приложение е особено ценно в сектори, където целостта на данните е от решаващо значение, като управление на веригата за доставки, здравеопазване и финансови услуги.

Децентрализирано управление на идентичността: Защитата на личните данни придобива все по-голяма важност в днешно време. Базираните на блокчейн системи за управление на идентичността осигуряват сигурно и защитено от фалшифициране решение за проверка и управление на цифрови идентичности. Индивидите могат да контролират своите лични данни и да предоставят достъп до тях само на тези, на които имат доверие, намалявайки риска от кражба на самоличност, неотризиран достъп и от изтичане на лична информация. Базираното на блокчейн управление на самоличност също позволява безпроблемни и надеждни процеси на проверка, без да се разчита на централизиран посредници.

Сигурни транзакции и умни договори: Блокчейн ни дава прозрачност и сигурност по отношение на съхранението и обработката на транзакциите. Транзакциите с криптовалута използват криптографски техники, гарантиращи поверителността и целостта на финансовите трансфери.

Интелигентните договори, съхранявани в блокчейна, позволяват автоматизирани и сигурни споразумения, без да се разчита на посредници. Това елиминира риска от измами и повишава ефективността на финансовите транзакции.

Намалено време и разходи: След като блокчейн технологията може да валидира транзакции и да показва историята, то тя може да премахне необходимостта от посредници и служители,

които валидират и проверяват информацията. Това не само намалява вероятността от човешка грешка, но и спестява време чрез автоматизиране на процеса.

Неизменни одитни следи и криминалистика: Прозрачната и неизменна природа на Blockchain позволява създаването на защитени от подправяне одитни пътеки и възможности за криминалистика. Блоквите вериги позволяват проследяване на транзакции и запис на метаданни, осигурявайки незаличим запис на дейностите. Тази функция подобрява прозрачността, опростява усилията за съответствие и позволява ефективни разследвания в случай на кибер инциденти или измамни дейности.

Финансовите одити в голям мащаб могат да станат много по-прости и ефективни във времето, тъй като всички транзакции на една компания (или дори на цяло правителство) могат да бъдат проследени и валидирани.

Децентрализирано разузнаване и споделяне на заплахи: Базираните на блокчейн платформи и криптовалутите улесняват децентрализираното разузнаване на заплахи и мрежи за споделяне. Тези мрежи позволяват на професионалистите и организациите по киберсигурност да си сътрудничат, да споделят информация за заплахи и колективно да се защитават срещу киберзаплахи. Децентрализираният характер гарантира надеждността и целостта на споделяните данни за заплахи, насърчавайки по-стабилна екосистема за киберсигурност.

Проследяване на престъпни сделки: Най-голямото погрешно схващане за криптоактивите продължава да е, че те са непроследими и че се използват

основно за измами. При транзакциите в криптовалутите всяка една от тях се записва в блокчейн, оставяйки след себе си видима следа за всеки. Това дава възможност на блокчейн анализаторските фирми да проследят движението между незаконни адреси. Вече има и специални крипто криминалистки компании, които помагат на правоохранителните органи да проследяват престъпни групи, като анализират потока на криптовалутите. Някои от тях са Chainalysis в Ню Йорк, британската Elliptic и CipherTrace, подкрепена от правителството на САЩ.

На първо място, проследяването на движенията на средства от една сметка към друга е доста лесно при блокчейн технологията. Също така няма и достатъчно ликвидност, за да могат например руските олигарси да си местят парите по този начин. Ликвидността в крипто все още е част от световния валутен пазар и следователно преместването на големи финансови средства с помощта на криптовалута е трудно.

Борсите за криптовалути също така ще обръщат повишено внимание на подобен тип дейност, особено ако оперират под американска юрисдикция, защото са длъжни да спазват законите на САЩ. Няма значение дали компанията борава с долари, криптовалути, злато, недвижими имоти или нефинансови активи. Законите за санкциите се прилагат за всички хора и фирми в САЩ.

Токенизация и стимули за киберсигурност: Токенизация и стимулите за киберсигурност са ключови елементи в екосистемата на криптовалутата, които допринасят за подобряване на мерките за сигурност и насърчаване на стабилна среда за киберсигурност.

Токенизация: Токенизацията се отнася до процеса на преобразуване на реални или цифрови активи в цифрови токени, които могат да бъдат представени и прехвърлени в блокчейн. Могат да се създават всевъзможни токени, които да бъдат персонализирани за нуждите на всеки бизнес, приложим във всяка обществена или частна мрежа. В контекста на кибер защитата, токенизацията осигурява средство за подобряване на сигурността чрез намаляване на излагането на чувствителни данни. Вместо директно съхраняване на чувствителна информация, токениите се използват за представяне на данните и действителната информация остава сигурно съхранена и защитена. Този подход минимизира риска от нарушения на данните и подобрява поверителността.

Стимули за киберсигурност: Криптовалутите предлагат уникални възможности за стимулиране на усилията за киберсигурност чрез използването на токени. Тези стимули са предназначени да възнаграждат лица или организации за принос към сигурността и целостта на екосистемата на криптовалута. Чрез съгласуване на икономическите стимули с целите на киберсигурността, тези стимули насърчават проактивни отбранителни мерки и насърчават участниците да се ангажират активно в осигуряването на мрежата. Днес блокчейните използват много различни консенсусни алгоритми, всеки със своите собствени механизми. Те играят неразделна роля в защитата на мрежата.

Алгоритъмът за консенсус Доказателство-за-работа (Proof-of-Work) е процес на математически изчисления и се прилага в копаенето (*mining*) на

криптомонети. За всеки валиден блок, който се „изкопава“, има автоматично възнаграждение от системата с криптовалута, която се копае. Честотата на хешрейта в Proof of Work често се използва като мярка за здравословното състояние на мрежата на криптовалутите. Колкото по-висока е скоростта на хеширане, толкова по-трудно е да се осъществи 51% атака.

При консенсуса Доказателство-за-дял (Proof-of-Stake) мрежата се подsigурява и се постига разпределен консенсус чрез използване на трудни хеширащи алгоритми за валидиране на електронните транзакции. При Proof-of-Stake потребителите залагат собствените си средства, за да участват в генерирането и проверката на блока. Правейки това, те печелят лихва/допълнителни жетони като награди за тяхното активно участие и принос към мрежовата сигурност.

Награди за бъгове и идентификация на уязвимости: Един често срещан стимул за киберсигурност е прилагането на програми за награди за откриване на грешки. Проектите за криптовалута предлагат награди, обикновено под формата на токени, на лица, които идентифицират и докладват уязвимости или грешки в техните системи. Това насърчава общността за киберсигурност или т.нар. „бели хакери“ активно да търси слабости, което в крайна сметка води до подобрена устойчивост и сигурност на системата.

Децентрализирано споделяне на разузнавателни данни за заплахи: Токенизацията може също така да улесни споделянето на информация за заплахи в рамките на екосистемата на криптовалута. Чрез токенизирани платформи

участниците могат да допринасят и споделят информация за възникващи заплахи, уязвимости или злонамерени участници. Стимули, като символични награди, могат да бъдат предоставени на тези, които допринасят с ценна информация или откриват нови заплахи. Този децентрализиран подход към споделянето на информация за заплахите подобрява колективната защита срещу кибернетични заплахи.

Децентрализирани услуги за сигурност: Токенизацията отваря пътища за развитие на децентрализирани услуги за сигурност в екосистемата на криптовалутата. Тези услуги могат да включват децентрализирани антивирусни решения, сигурни многофакторни протоколи за удостоверяване и децентрализирани системи за проверка на самоличността. Базираните на токени модели позволяват на потребителите достъп до тези услуги и стимулират доставчиците на услуги непрекъснато да подобряват функциите за сигурност.

Предизвикателства и съображения

Блокчейн технологията, осигурявайки повишена сигурност, донесе редица предимства в различни индустрии, но наред с тях, в практиката са открити и някои негативи.

Тъй като технологията е напълно нова, подготвените специалисти са малко на брой, което прави блокчейн базираните приложения **скъпи за разработване и поддръжка**, а това влиза в противоречие с рекламираното предимство, че технологията намалява разходите. От другата страна: сложността на технологията поставя **барьера**, която

възпрепятства много потребители да използват блокчейн услуги.

Блокчейн-базираните приложения са трудни за **интеграция** с данните, които не са на блокчейн и дори да интегрират своите приложения с други такива и услуги, които са на други блокчейни, което не отговаря на приоритетните приложения и насоки за оперативна съвместимост.

Въпреки че една от основните насоки за приложение на блокчейн технологията е ефективно преструктуриране на икономиката и дигитализацията, засега нейното функциониране все още се определя като **силно енергийноемко** (особено в блокчейни, използващи алгоритъма Доказателство-за-работа). Това налага да се търсят и нови решения на енергийния аспект, едновременно с възможните приложения, за да не се стигне до ситуация, в която използването на технологията може да влезе в противоречие с целите, в името на които тя е използвана.

В сравнение с традиционните централизирани бази данни, блокчейните имат **ограничена ефективност** (най-разпространените блокчейни – Bitcoin и Ethereum поддържат по-малко от 50 транзакции в секунда) и изискват **увеличен капацитет за съхранение** (в момента блокчейнът на Bitcoin изисква около 200 GB) (<https://kriptomat.io/bg/blockchain/plyusove-i-minusi-na-blokchein-tehnologiyata>).

Частните ключове и стабилността са две от предимствата на блокчейн, но могат да бъдат и недостатъци. Ако някой потребител загуби своя ключ, то той може да загуби и достъп до всичките си активи, защото няма да има гореща линия, която да напомни за паролата. Ако направим грешка, като извършваме

трансфер, няма да можем да го отменим. *Ние сме самата банка.*

Внедряването на **стимули за токенизация** и киберсигурност в криптовалутите също представлява предизвикателство. Осигуряването на справедливост и ефективност на механизмите за стимулиране, предотвратяването на злоупотреби или фалшиви доклади и избягването на централизацията на властта са важни съображения. Освен това, постигането на баланс между стимулирането на практиките за сигурност и поддържането на аспектите на децентрализацията и поверителността на криптовалутите е от съществено значение.

За много хора гумата блокчейн се асоциира с криптовалутите и на практика се е превърнала в синоним на финансови машиниции и откупи за дешифриране на криптирани дискове. И това донякъде е съвсем очаквано и не без основание, предвид множеството атаки над криптоборси и рансъмуер-а. Криптовалутите позволяват на престъпници лесно да прехвърлят незаконни средства през стотици портфейли, преди да ги депозират и да ги осребрят на криптоборса, особено в началото на криптоиндустрията, когато липсваха регулация, законодателство и международни стандарти. За последните няколко години криптовалутите се превърнаха и в предпочитания начин за плащане сред онлайн престъпниците.

Дискусиите за **сигурността** на блокчейн са двустранни:

От една страна са защитниците на технологията: „Блокчейнът като технология досега никога не е бил „хакван“. Според тях, многото случаи на атакувани криптоборси и потребители, загубили своите средства, се дължи на пробииви в

софтуерните системи на самите борси, а не на блокчейна на криптовалутата.

От другата са критиците: „Недопустима небрежност/измама“. В много от случаите разработчиците не осигуряват достатъчно защита на личните ключове и пароли, като така допускат пробив. Липсват задълбочени одити и застраховки като решаващи елементи за възвръщане на доверие в такива продукти.

И поддръжниците, и критиците обаче са на едно мнение: Макар че представлява голямо подобрение в сигурността на данните, блокчейн не е сигурен безопасен вариант. Тя може да бъде злоупотребена и манипулирана, въпреки че отнема много повече време, ресурси и усилия, отколкото традиционните технологии. Координираната атака все още може да се случи на самия блокчейн, при което една единица или група, притежаваща по-голямата част от миннодобивната сила, създава притискане на споменатия блокчейн, което в крайна сметка ще им позволи да нарушат мрежата. Това се нарича **51% атаката** и може да причини сериозни щети, както се вижда при Bitcoin Gold.

Въпреки това, количеството на организацията и ресурсите, необходими за този вид операция, го прави много малко вероятен за големите платформи с блокчейн с много по-висок процент на хеширане като оригиналния Bitcoin, чийто блокчейн е много устойчив и бързо се адаптира като отговор на атака.

Някои от последствията от приложението на Блокчейн технологията са по-трудно доловими. Както и при изкуствен интелект, ефективните блокчейн-базирани приложения могат да намалят броя или да премахнат напълно необходимостта от заети в някои сектори, което

естествено ще доведе до нарастване на равнището на **безработицата**. Интелигентните договори, които премахват необходимостта от посредници, са пример за това: не се нуждаете от брокер на недвижими имоти, за да закупите, продадете или наемете имот, не се нуждаете от застраховател, за да си получите обезщетението при настъпване на събитието, няма нужда и от нотариус, който да потвърди сделката. При децентрализираните финансови приложения няма нужда от банкови служители и финансови брокери, всеки сам управлява своите средства. Също така и **Волатилността** на крипто пазара има все по-голямо влияние върху световните финансови пазари, след като криптото е все по-широко приемано, което естествено води и до високи рискове за спестяванията и вложенията на инвеститорите.

Заклучение

Колкото по-мощна става дигитализацията, толкова по-уязвими стават и държавата, и икономиката, и обществото. И толкова по-високи са изискванията за сигурност. Най-голямата защита е превенцията: изисква инвестиции в решения за сигурност, но преди

всичко – осъзнаване на мащабите на проблема. Добрата киберсигурност може да не струва малко, но не трябва да се правят компромиси с нея.

Блокчейн технологията има потенциала да увеличи радикално безопасността на данните, тъй като показва характеристики, които са много по-подходящи, за да издържат на твърде честите атаки на киберпрестъпността. Нейните предимства, въпреки недостатъците, я правят широко предпочитана във виртуалната сигурност, както и от все повече фирми и дори правителства, които предприемат стъпки за подобряване на своите системи що се отнася до прозрачност, ефективност и намаляване на разходите. При все че много сектори се справят с предимствата и недостатъците на блокчейн системите, все още има дълъг път към масовото приемане, отстраняване или минимизиране на негативите, както и търсене на нови приложения, за да се открие къде блокчейн технологията добавя най-голяма стойност. Дали предимствата на блокчейн технологията ще вземат превес над недостатъците е просто въпрос на време.

Цитирани източници (References):

1. 4-те основни цикъла на крипто пазара до този момент <https://kryptonovini.com/news/4-te-osnovni-tsikala-na-kripto-pazara-do-tozi-moment/> (последно достъпен 07.02.2024 г.)
(4-te osnovni tsikala na kripto pazara do tozi moment <https://kryptonovini.com/news/4-te-osnovni-tsikala-na-kripto-pazara-do-tozi-moment/> (posledno dostapen 07.02.2024 g.)
2. Актуализирана Национална стратегия за киберсигурност „Киберустойчива България 2023“, Решение № 301 на Министерския съвет от 02.04.2021 г.
(Aktualizirana Natsionalna strategia za kibersigurnost „Kiberustoychiva Bulgaria 2023“, Reshenie № 301 na Ministerskia savet ot 02.04.2021 g.)

3. Блокчейн технологията може да улесни внедряването и функционирането на кръговата икономика <https://nauka.offnews.bg/zemiata/blokchejn-tehnologiyata-mozhe-da-ulesni-vnedriavaneto-i-funktcioniranet-187378.html> (последно достъпен 07.02.2024 г.).
(Blokcheyn tehnologiyata mozhe da ulesni vnedryavaneto i funktsioniraneto na kragovata ikonomika <https://nauka.offnews.bg/zemiata/blokchejn-tehnologiyata-mozhe-da-ulesni-vnedriavaneto-i-funktcioniranet-187378.html> (posledno dostapen 07.02.2024 g.)
4. Георгиев, Иван, Цветан Цветков и Димитър Благоев (2013). Мениджмънт на фирмените иновации и инвестиции: Част V. Иновации и иновационен процес. Издателски комплекс – УНСС.
(Georgiev, Ivan, Tsvetan Tsvetkov i Dimitar Blagoev (2013). Menidzhmant na firmenite inovatsii i investitsii: Chast V. Inovatsii i inovatsionen protses. Izdatelski kompleks – UNSS)
5. Европейска Дигитална стратегия, Блокчейн стратегия <https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy> (последно достъпен 07.02.2024 г.).
(Evropeyska Digitalna strategia, Blokcheyn strategia <https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy> (posledno dostapen 07.02.2024 g.)
6. ЕС решава да укрепи киберсигурността и устойчивостта в целия Съюз: Съветът приема ново законодателство <https://www.consilium.europa.eu/bg/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/> (последно достъпен 07.02.2024 г.).
(ES reshava da ukrepi kibersigurnostta i ustoychivostta v tselia Sayuz: Savetat priema novo zakonodatelstvo <https://www.consilium.europa.eu/bg/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/> (posledno dostapen 07.02.2024 g.)
7. Закон за киберсигурност, Обн. ДВ бр. 94 от 13 Ноември 2018 г., изм. ДВ бр. 25 от 29 Март 2022 г.
(Zakon za kibersigurnost, Obn. DV br. 94 ot 13 Noemvri 2018 g., izm. DV br. 25 ot 29 Mart 2022 g.)
8. Инфографика — Най-големите киберзаплахи в ЕС <https://www.consilium.europa.eu/bg/infographics/cyber-threats-eu/> (последно достъпен 07.02.2024 г.).
(Infografika — Nay-golemite kiberzaplahi v ES <https://www.consilium.europa.eu/bg/infographics/cyber-threats-eu/> (posledno dostapen 07.02.2024 g.)
9. Какво представлява Блокчейн технологията? <https://investinblockchain.bg/kakvo-e-blockchain-tehnologiyata/> (последно достъпен 07.02.2024 г.).
(Kakvo predstavlyava Blokcheyn tehnologiyata? <https://investinblockchain.bg/kakvo-e-blockchain-tehnologiyata/> (posledno dostapen 07.02.2024 g.)
10. Киберсигурност: как ЕС се бори с киберзаплахите <https://www.consilium.europa.eu/bg/policies/cybersecurity/> (последно достъпен 07.02.2024 г.).
(Kibersigurnost: kak ES se bori s kiberzaplahite <https://www.consilium.europa.eu/bg/policies/cybersecurity/> (posledno dostapen 07.02.2024 g.)

11. Национална програма „Цифрова България 2025“, Последно обновяване 10.02.2023 г. https://www.mtc.government.bg/sites/default/files/uploads/it/09-12-2019_programa_-_cifrova_bulgariya_2025.pdf (последно достъпен 07.02.2024 г.).
(Natsionalna programa „Tsifrova Bulgaria 2025“, Posledno obnovyavane 10.02.2023 г. https://www.mtc.government.bg/sites/default/files/uploads/it/09-12-2019_programa_-_cifrova_bulgariya_2025.pdf (posledno dostapen 07.02.2024 g.)
12. Предимства и недостатъци на блокчейна <https://academy.binance.com/bg/articles/positives-and-negatives-of-blockchain/> (последно достъпен 07.02.2024 г.).
(Predimstva i nedostatatsi na blokcheyna <https://academy.binance.com/bg/articles/positives-and-negatives-of-blockchain/> (posledno dostapen 07.02.2024 g.)
13. Силата на блокчейн технологията и нейните неограничени възможности <https://investinblockchain.bg/blockchain-power-and-use-cases/> (последно достъпен 07.02.2024 г.).
(Silata na blokcheyn tehnologiyata i neynite neogranicheni vazmozhnosti <https://investinblockchain.bg/blockchain-power-and-use-cases/> (posledno dostapen 07.02.2024 g.)
14. Топ 4 предимства на блокчейн технологията <https://startupfactory.bg/blogbg/blokcheyn-tehnologia/4-predimstva-na-blcokchain/> (последно достъпен 07.02.2024 г.).
(Top 4 predimstva na blokcheyn tehnologiyata <https://startupfactory.bg/blogbg/blokcheyn-tehnologia/4-predimstva-na-blcokchain/> (posledno dostapen 07.02.2024 g.)
15. 7 Ways The Blockchain Can Save The Environment and Stop Climate Change, <https://futurethinkers.org/blockchain-environment-climate-change/> (последно достъпен 07.02.2024 г.).
(7 Ways The Blockchain Can Save The Environment and Stop Climate Change, <https://futurethinkers.org/blockchain-environment-climate-change/> (posledno dostapen 07.02.2024 g.)
16. Harnessing Blockchain Applications And Cryptocurrency- Based Cybersecurity Innovations <https://bitcoinworld.co.in/harnessing-blockchain-applications-and-cryptocurrency-based-cybersecurity-innovations/> (последно достъпен 07.02.2024 г.).
(Harnessing Blockchain Applications And Cryptocurrency- Based Cybersecurity Innovations <https://bitcoinworld.co.in/harnessing-blockchain-applications-and-cryptocurrency-based-cybersecurity-innovations/> (posledno dostapen 07.02.2024 g.)

Izpolzvane na blokcheyn prilozhenia i inovatsii v kibersigurnostta

Tatyana Docheva

Using Blockchain Applications and Innovations in Cybersecurity

Tatyana Docheva

Abstract: This paper highlights the need for cyber protection and application of new technologies in cyber security in our increasingly digitalized world. It examines the development, application and potential of blockchain technology to date, as well as its nature. It presents the possible benefits and challenges of implementing blockchain applications and innovations in cybersecurity, drawn from the experiences of blockchain innovations and applications already implemented in other sectors of our lives. The work is of a review rather than analytical nature.

Key words: cybersecurity, innovation, blockchain.

JEL: L86, O31.