

ОСНОВНИ ХАРАКТЕРИСТИКИ НА БЛОКЧЕЙН ТЕХНОЛОГИИТЕ В КОНТЕКСТА НА СИГУРНОСТТА¹

Д-р Александър Янков, Катедра „Национална сигурност и публична администрация”, Правно-исторически факултет, Югозападен университет „Неофит Рилски”

Резюме: Настоящата статия разглежда блокчейн като децентрализиран цифров регистър, състоящ се от записи, наречени „блокове”, които се използват за отразяване на определени действия или транзакции, извършвани на неопределен брой компютри. Данните са хронологично последователни, тъй като не е възможно да се изтрият или внасят промени, без това да се одобри или поне да стане известно на всички участници в мрежата. В този смисъл блокчейн е система от бази данни, технологията за работа с които определено променя начина, по който се развива светът. Още повече, че от управленска и правна гледна точка блокчейн е уникален поради своята децентрализирана същност, както и поради факта, че предоставя напълно равни първоначални възможности на всеки участник. Анализирани са блокчейн технологията като основа за развитието на биткойн и другите криптовалути.

Ключови думи: блокчейн технология, биткойн, „златен стандарт”, криптовалути.

MAIN CHARACTERISTICS OF BLOCKCHAIN TECHNOLOGIES IN THE CONTEXT OF SECURITY

Aleksandar Yankov, PhD, Department of National Security and Public Administration, Faculty of Law and History, South-West University “Neofit Rilski”

Abstract: This article examines blockchain as a decentralized digital ledger consisting of records called ‘blocks’ that are used to record certain actions or transactions performed on an indefinite number of computers. The data is chronologically consistent, as it is not possible to delete or make changes without approval or at least becoming known to all network participants. In this sense, blockchain is a system of databases, the technology for working with which is definitely changing the way the world develops. Moreover, from a managerial and legal point of view, blockchain is unique due to its decentralized nature, as well as the fact that it provides completely equal initial opportunities to each participant. Blockchain technology is analyzed as the basis for the development of Bitcoin and other cryptocurrencies.

¹ Докладът е представен на кръгла маса, проведена на 22 май 2024 г., на тема: „ИЗКУСТВЕН ИНТЕЛЕКТ, СИГУРНОСТ И ДЕЗИНФОРМАЦИЯ - СЪВРЕМЕННИ ТЕНДЕНЦИИ И ПРЕДИЗВИКАТЕЛСТВА“, която се организира от Правно-историческия факултет на Югозападния университет „Неофит Рилски“, гр. Благоевград в рамките на научноизследователски проект № RP-C1/24 на тема: „Изкуствен интелект, сигурност и дезинформация - съвременни тенденции и предизвикателства“.

Keywords: blockchain technology, bitcoin, 'golden standard', cryptocurrencies.

Според повечето известни в литературата определения blockchain (блокчейн) представлява неподдаваща се на промени система за споделяне, която има за цел записване на определени действия и ли транзакции или проследяване на активи в бизнес мрежа. На практика това е децентрализиран цифров регистър, състоящ се от записи, наречени „блокове“, които се използват за отразяване на определени действия или транзакции, извършвани на неопределен брой компютри. Данните са хронологично последователни, тъй като не е възможно да се изтриват или внасят промени, без това да се одобри или поне да стане известно на всички участници в мрежата. В този смисъл блокчейн е система от бази данни, технологията за работа с които определено променя начина, по който се развива светът. Още повече, че от управленска и правна гледна точка блокчейн е уникален поради своята децентрализирана същност и липса на център на власт, както и поради факта, че предоставя напълно равни първоначални възможности на всеки участник, с което се подхранват идеите за възможността на утопичното общество.

Обикновено, когато се говори за блокчейн се изтъкват следните негови преимущества. На първо място, **невъзможността за внасяне на промени** – след като бъдат направени веднъж, записите не могат да бъдат променени. На второ място, както вече бе изтъкнато, blockchain е **децентрализирана система** - той може да работи без регулации и намеса, без значение на човешки фактор или на изкуствения интелект. На трето място следва да се отбележи **възможността за достъп** на всеки участник до всички записи. На следващо място, това е технология, която предполага **наличието на консенсус**, тъй като всички транзакции се проверяват и актуализират с консенсус. И не на последно място по значение е **сигурността**, която ни предлага blockchain поради простия факт, че цялото записано съдържание е индивидуално криптирано. Цифровите транзакции се съхраняват в цифров „блок“ (нещо като запис в книга), който се добавя към предишна „верига“ от блокове; оттук и терминът блокчейн.

Начинът на **функциониране** на блокчейн, заложен в самото му наименование, е изключително прост - всеки блок има уникален „хеш“, като подпис или идентификационен код, и времева щампа, за да покаже точното време, когато е валидиран или създаден. Всеки блок съдържа хеша на предишния блок, образувайки веригата. Този

хеш се използва не само за свързване на блоковете, но и за проверка на целостта на данните. Ако някой се опита да промени информацията в блока, ще се промени и хешът, което няма да остане незабелязано. Това позволява надеждност, автентичност и идентифицируемост на информацията в самата система, но същевременно стабилност и устойчивост на системата към външни влияния. Или накратко казано, блокчейн има потенциала да революционизира почти всяка цифрова операция, която познаваме днес, от извършване на плащания и сключване на договори до поддържане на сложни промишлени и правителствени структури.

Сред потенциалните **ползи**, които води след себе си прилагането на блокчейн технологията, е на първо място, елиминирането на възможностите за противоправно вмешателство, на подправянето или фалшифицирането на данни. Блокчейнът използва криптография, всяка транзакция се записва в блок и се свързва с предишния блок, образувайки верига. Това гарантира, че информацията остава непроменена. Технологията допринася за това транзакциите да бъдат видими и прозрачни, тъй като всички участващи в мрежата компютри имат достъп до една и съща база данни, а хеш хронологията прави всеки запис проследим. Блокчейн е сигурна технология, тъй като не е необходимо съответният участник да се доверява на останалите, за да е убеден, че дадено действие е точно записано. Поради това често блокчейн технологията е наричана „мрежа без доверие“ между участниците, но същевременно с увеличено доверие в самата система, тъй като всеки участник може да види и потвърди данните. Тъй като блокчейн е автоматизирана мрежа, тя премахва необходимостта от посредници, такси за определени услуги, както и забавяне на процесите поради човешки фактор или документация на хартиен носител.

Но както всяка друга технология, блокчейн също може да е съпроводен от определени **рискове**. Тъй като това е технология, базирана в интернет, самата тя не може да бъде предмет на незаконно посегателство, но това едва ли се отнася за необезопасени системи около нея. Друг възможен риск, свързан с криптовалутите, е възможността един субект да получи контрол върху повече от половината от целия „майнинг“ или залагане на криптовалута, тъй като това би му предоставило възможността да променя бъдещи „блокове“. На практика, за големи мрежи като Bitcoin и Ethereum подобна атака би била трудно изпълнима, но за по-малки мрежи е напълно реална заплаха.

През 2016 г. Централната банка на Канада публикува проучване, според което последиците от развитието на криптовалутите водат до формирането на нов „златен стандарт”. Това, което днес наричаме криптовалута/и, всъщност има редица аналогии със златото. На първо място, както при златните залежи, криптовалутите също са в ограничено „количество“, поради което не съществува сериозен риск от ерозия на стойността им. В конкретния случай, ако говорим за алгоритъма на биткойн, границата на му е някъде в района на 21 милиона части - точно това количество в крайна сметка ще бъде „добито“ в съответствие с настоящите алгоритми за емисии, които увеличават трудността при добиването му на всеки четири години. Протоколите за повечето други криптовалуди като цяло са подобни.

Следващата прилика между златото и криптовалутите е самият процес на добиване. При това във втория случай хората изразходват значителни ресурси, за да „извлекат“ актив, който сам по себе си няма физическа стойност. Стойност се появява само когато определена критична маса от хора започне да използва този продукт като средство за разплащане и спестяване. Тази „златна“ аналогия, която на пръв поглед изглежда като предимство, всъщност носи определени рискове, ако този актив се използва като пари. Тези рискове са типични за „златния стандарт” и са свързани с дефлационния характер на икономиката, изградена върху ограничен актив. Ако има продукт - мярка за стойността, който също непрекъснато расте в цената поради своята ограниченост, тогава в крайна сметка за икономическите играчи става нецелесъобразно да го харчат - те преминават от режим на потребление към спестяване и икономиката стагнира. Това е и сериозен недостатък на криптовалутите, свързан с невъзможността на държавата да контролира предлагането на пари.

Друг недостатък е невъзможността да говорим за търсене на децентрализирано платежно средство, което може да подкопае функцията на парите като средство за съхранение на стойност. По време на „златния стандарт” държавите можеха да имат различни лихвени проценти, дори и тяхната валута да е тясно обвързана със златото. Разходите за транспортиране на златото са високи и следователно този актив не може да преминава свободно през границите, за да следва по-благоприятните финансови условия. Докато електронните пари могат да се прехвърлят навсякъде по света за частица от секундата практически без разходи и по отношение на криптовалутите държавата не може

да провежда самостоятелна лихвена политика, което опеделено затруднява регулаторните органи.

Освен това следва да имаме предвид, че блокчейн технологията и базираните на нея криптовалюти са много повече от просто средство за плащане. Всъщност това е криптографска регистрация на правата на собственост. Например, в биткойн мрежата има т. нар. цветни монети (coloured coins), които са свързани със собственост. Субектът, който може да харчи биткойни (т.е. притежава съответния частен ключ), се счита за собственик на имуществото. В същото време „цветните монети“ могат да се прехвърлят, както и да се извършват обикновени операции с тях. В случая с биткойн тази идея е слабо приложима, но има други по-напреднали и ефективни методи за записване на правото на собственост, базирано върху блокчейн технологията. Теоретично, тези методи могат да бъдат приложени и за приписване на стойността на обикновените аналогови пари на криптовалутите. В този случай подобна валута ще бъде дигитализиран аналог на обикновените пари, като същевременно ще има всички предимства на виртуалните пари - скорост и прозрачност на транзакциите. Както вече добре знаем, Bitcoin не е единствената опция за криптовалута.

Както стана ясно, блокчейн технологията представлява хранилище на информация относно всички операции в системата. Това е вид регистър, който записва движенията на биткойните. За първи път тази технология беше използвана за емитиране на криптовалутата Bitcoin. Или казано накратко, дефиницията за блокчейн е картотека, в която няма контролен орган, и съответно, веднъж въведената информация е почти невъзможна за промяна. Използването на криптиране гарантира, че потребителите могат да променят само онези части от блоковата верига, които „притежават“ в смисъл, че имат частни ключове, без които записът във файла е невъзможен. В допълнение, криптирането гарантира, че копията на разпределения блокчейн са синхронизирани между всички потребители. Представете си цифрово медицинско досие - всеки запис всеки запис представлява отделен блок. Този запис има етикет: дата и час на влизане. Забранено е модифицирането на записи със задна дата, тъй като е необходимо записите за диагноза, лечение и др. да останат в първоначалния си вид. Записите могат да бъдат достъпни само за лекаря, който притежава единия частен ключ, и за пациента, който има другия. След това тази информация ще бъде достъпна само за тези, на които един от тези двама

потребители е споделил своя частен ключ (например, болницата като цяло или отделен специалист). Така, блокчейн технологията по своята същност е защитена на ниво база данни.

Концепцията за блокчейн е предложена през 2008 г. от Сатоши Накамото. За първи път е внедрена през 2009 г. като компонент на цифровата валута биткойн, където блокчейнът играе ролята на главна картотека за всички транзакции. Благодарение на блокчейн технологията биткойнът се превърна в първата цифрова валута, която решава проблема с двойното харчене (за разлика от физическите монети или токени, електронните файлове могат да бъдат дублирани и изразходвани два пъти) без използването на какъвто и да е орган или централен сървър. Сигурността в блокчейн технологията е осигурена чрез децентрализиран сървър за маркиране на времето и мрежовите връзки между партньори. В резултат на това се формира база данни, която се управлява автономно, без единен център. Това прави блокчейните много полезни за записване на определени събития (като медицински досиета) и операции с данни, управление на самоличността и проверка на източника. Блокчейн технологията понякога е наричана „Интернет на стойността“ и това е добра метафора. Всеки може да пусне информация в интернет и след това други хора да имат достъп до нея от всяка точка на света. Блоките вериги ви позволяват да изпращате всякаква стойност навсякъде по света, където файлът на блоквата верига е наличен. Но трябва да имате частен ключ, създаден с помощта на криптографски алгоритъм, за да ви позволи достъп само до блоковете, които „притежавате“. Давайки на някого вашия личен ключ, вие по същество давате на това лице парична сума, която се съхранява в съответния раздел на блоквата верига. В случая с биткойн такива ключове се използват за достъп до адреси, които съхраняват определени количества валута, които имат пряка финансова стойност. На практика технологията изпълнява функцията за регистриране на прехвърлянето на средства, обикновено изпълнявана от банките.

Освен това при биткойна блокчейн технологията изпълнява и друга важна функция, а именно установяване на доверителни взаимоотношения и потвърждаване на автентичността на самоличността на участниците, тъй като никой не може да промени блоквата верига без съответните ключове. Промените, които не са потвърдени от тези ключове, се отхвърлят. Разбира се, ключовете (подобно на истинските пари) теоретично

могат да бъдат откраднати, но защитата на няколко реда компютърен код обикновено не струва много. Това означава, че основните функции, изпълнявани от банките като проверка на самоличността за предотвратяване на измами и последващо записване на транзакциите, след което те стават легални, могат да се изпълняват по-бързо и по-точно от блокчейн технологията, което ще вероятно ще доведе в бъдеще до изчезването на банките като центрове за разплащания.

Какво е значението на блокчейн технологията? Днес ние сме свикнали да споделяме информация чрез децентрализираната интерактивна платформа на Интернет. Но когато става въпрос за прехвърляне на ценности (пари), обикновено сме принудени отново да използваме услугите на старите централизирани финансови институции, каквито са банките. Вярно е, че методите за онлайн плащане се появяват почти едновременно с Интернет, но те обикновено изискват интеграция с банкова сметка или кредитна карта, в противен случай не могат да бъдат използвани напълно. Блокчейн технологията предлага примамлива възможност за освобождаване от тази „допълнителна връзка“. Тя може да поеме и трите важни роли, традиционно изпълнявани от сектора на финансовите услуги: регистриране на транзакциите, проверка на самоличността и сключване на договори. Именно това демонстрира най-важния икономически и правен ефект от същността на блокчейн технологията. В конкретния случай това ще бъде от съществено значение, тъй като пазарът на финансови услуги е най-големият в света по пазарна капитализация. Прехвърлянето на поне част от тази система към блокчейн технологията би довело до прекъсване на голям брой връзки в областта на финансовите услуги, но в същото време значително ще повиши ефективността на подобни услуги.

Друга потенциална роля за тази технология е че тя би могла да бъде изключително полезна извън финансовия сектор. В допълнение към въвеждането на още една валута (биткойн), блокчейн технологията може да се използва за съхраняване на всякакъв вид цифрова информация, включително компютърен код. Този код може да бъде програмиран да се изпълнява само когато и двете договарящи страни въведат ключовете си, като по този начин приемат условията на договора. Същият код може да взема информация от външни потоци от данни (цени на акции, прогнози за времето, заглавия на новини и всичко друго, което може да бъде анализирано от компютър) и „да сключва“ договори, които ще бъдат автоматично регистрирани, когато са изпълнени определени условия. Този

механизъм се нарича „умни договори“, а възможностите за неговото приложение са почти безкрайни.

Всичко гореизложено ни позволява да направим единственото възможно заключение: блокчейн технологията и нейното внедряване е невъзможна (или поне неефективна) без интернет.

В заключение, както е известно, правната сигурност е едно от основните свойства на правото и неговите норми. Според представителите на доктрината той представлява точно, пълно и последователно консолидиране и прилагане на нормативната правна воля, присъща на закона и е насочена към поддържане на разумна стабилност на правното регулиране, създаване на доверие на частните лица в държавата и закона. Европейският съд по правата на човека също приема, че сигурността на правните норми е един от най-важните признаци за качеството на законите. Според него „качеството на въпросния закон изисква той да бъде достъпен за засегнатите лица и формулиран с достатъчна точност, за да позволи на тези лица, с помощта на съвет, да предвидят в разумна степен, с оглед на конкретните обстоятелства, последиците, до които може да доведе определено действие. Законът трябва да бъде изготвен с достатъчно ясни формулировки, за да даде на гражданите правилно разбиране на обстоятелствата и условията, при които публичните власти имат право да прибегват до оспорваните мерки”². Може би именно блокчейн технологията ще ни помогне да постигнем така желаната правна сигурност и предвидимост.

Библиография:

1. [Antonopoulos, A. Bitcoin Security Model: trust by computation. 2014. O'reilly-Radar. http://radar.o'reilly.com/2014/02/bitcoin-security-model-trust-bycomputation.html.](http://radar.o'reilly.com/2014/02/bitcoin-security-model-trust-bycomputation.html)
2. [Champagne, Phil The Book of Satoshi, 2014, e53 Publishing LLC, ISBN 9780996061322, \[PDF\] The Book Of Satoshi by Phil Champagne eBook | Perlego](#)
3. Drescher, Daniel Blockchain Basics A Non-Technical Introduction in 25 steps, Apress, 1st Ed., 2017, ISBN 9781484226032.

² GORZELIK AND OTHERS v. POLAND, Решение от 17 февруари 2004 г., Жалба № 44158/98), [Права на човека | GORZELIK AND OTHERS v. POLAND BG \(Горзелик и други срещу Полша\) \(humanrights.bg\)](#), §64.

4. Szabo N. Smart contracts: formalizing and securing relationships on public networks. 1997. First Monday 2(9). DOI: 10.5210/fm.v2i9.548.
5. Tapscott, Don & Alex Tapscott Blockchain Revolution. How the Technology Behind Bitcoin and Other Cryptocurrencies Is changing the World, 2018, Penguin Publishing group, ISBN 9781101980149.
6. Zheng, Zibin, Shaoan Xie, Hong-Ning Dal, Xianping Chen & Huamin Wang An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, 2017 6th IEEE International Congress on Big Data. DOI: [10.1109/BigDataCongress.2017.85](https://doi.org/10.1109/BigDataCongress.2017.85).
7. GORZELIK AND OTHERS v. POLAND, Решение от 17 февруари 2004 г., Жалба № 44158/98), [Права на човека | GORZELIK AND OTHERS v. POLAND BG \(Горзелик и други срещу Полша\) \(humanrights.bg\)](https://www.humanrights.bg/en/cases/gorzelik-and-others-v-poland), §64.
8. Димитрова В. и М. Семова Блокчейн и умните договори в ритейлинга, 2018, Conference: COMMERCE 4. 0 – SCIENCE, PRACTICE AND EDUCATION Varna, Bulgaria [_\(17\) \(PDF\) БЛОКЧЕЙН ТЕХНОЛОГИЯТА И УМНИТЕ ДОГОВОРИ В РИТЕЙЛИНГА \(researchgate.net\)](https://www.researchgate.net/publication/328111111).
9. Максуров А.А. Возможности правового регулирования сети Интернет. — URL: Правовые вопросы связи. — 2011. — № 1 — С. 14.
10. Максуров А.А. Блокчейн, криптовалюта, майнинг: понятие и правовое регулирование. — М.: Издательско-торговая корпорация «Дашков и К°», 2020. — 198 с., ISBN 978-5-394-03262-2.