POWER OF BLOCKCHAIN TECHNOLOGY: REDEFINING AND DEMOLISHING TRUST IN DIGITAL ECONOMY

Ekaterina M. Konstantinova [1], Aleksandyr S. Bradvarov [2]

[1] *Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Communication and Computer Technologies", katminkova2@gmail.com*
[2] *Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department "Communication and Computer Technologies", alekstefano@abv.bg*

***Abstract**: The biggest advantage of blockchain technology is the ability to build decentralized organizations: organizations that have democratically decentralized governance, keep their data open, public and decentralized, and execute their business processes in a decentralized and public manner on decentralized blockchain platforms. The trend towards building decentralized organizations and economies is expected to intensify in the years to come and continue to change the world we live in. For example, imagine a decentralized ordering platform (Uber decentralized). Such a platform can connect drivers with blockchain passengers through decentralized applications and free of charge. It is a non-proprietary software organization that cannot technically be shut down because it runs at the same time on thousands of machines around the world.*

***Keywords**: Blockchain, Decentralization, Digital economy, International transaction*

СИЛАТА НА БЛОКЧЕЙН ТЕХНОЛОГИЯТА: ПРЕДЕФИНИРАНЕ И РАЗРУШАВАНЕ НА ДОВЕРИЕТО В ДИГИТАЛНАТА ИКОНОМИКА

Екатерина М. Константинова, Александър С. Брадваров

Въведение

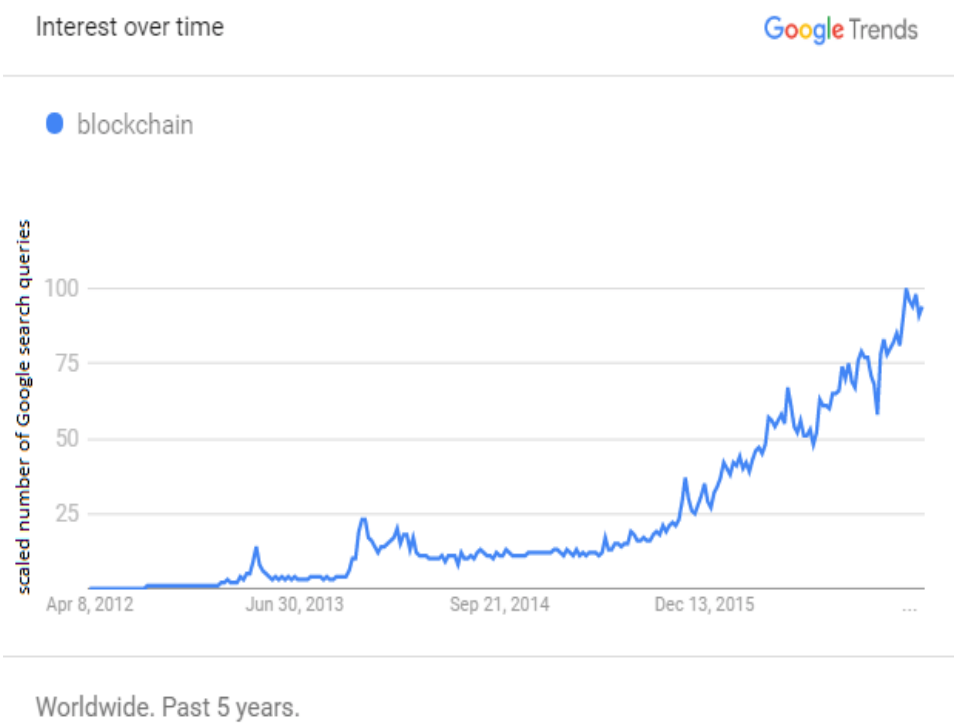
Блокчейн е децентрализирана технология, осъществявана без посредник, която улеснява икономическите транзакции и партньорските взаимодействия. В допълнение към обмена на информация, технологията предоставя и протоколи за обмен на стойност, правни договори и други подобни приложения. Въпреки огромните си преимущества, технологията среща политически предизвикателства, свързани с въпросите за укриването на данъци, прането на пари, финансирането на тероризма и улесненията на много престъпни дейности, като продажба на наркотици и оръжия, както е известно от организираните децентрализирани пазари като Пътят на коприната. Също както и при останалите съвременните комуникационни системи, блокчейн трябва да отговаря на редица технически изисквания. От гледна точка на практическата реализация най-трудно е удовлетворяването на изискванията за висока скорост на предаване на информацията и за осигуряване на надеждна защита на ресурсите на системата от неоторизиран достъп [2], [3], [9], [10], [11], [12], [13], [22], [23], [24].

Изложение

Преимущества на блокчейн

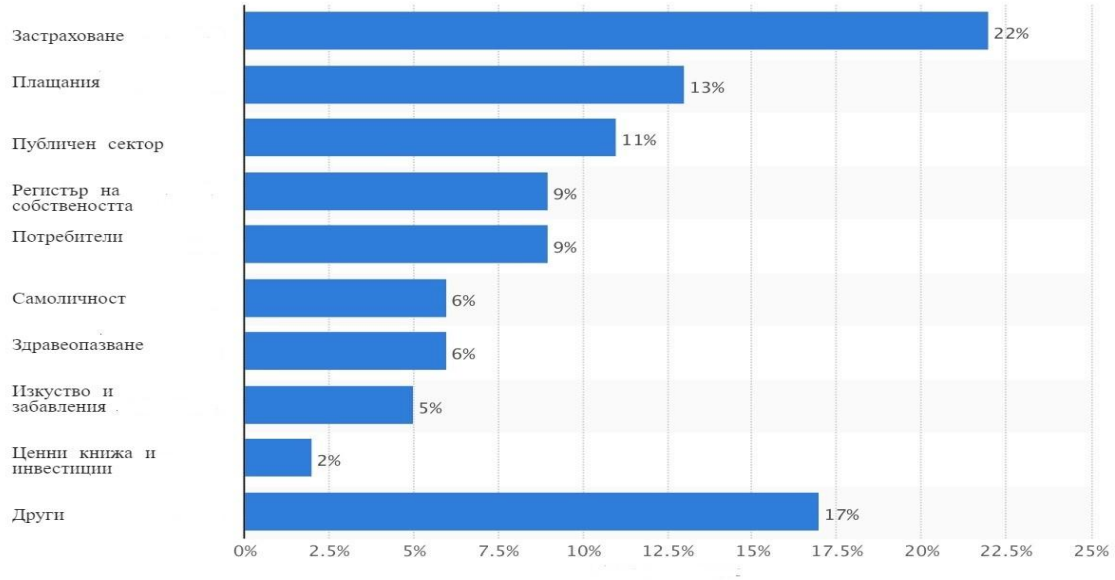
Киберпространството е сложна среда, включваща взаимодействието на хора, софтуер и услуги в Интернет. Блокчейн технологията е децентрализирана база данни, която съхранява регистър на активи и транзакции в P2P, или партньорска мрежа. По същество това е публичен регистър за това кой какво притежава и какви сделки са сключени. Транзакциите са защитени чрез криптография и с течение на времето тази история на транзакциите се заключва в блокове от данни, които след това се свързват и обезпечават чрез криптографски ключове. Това създава неизменен запис на всички транзакции в тази мрежа. Този запис се репликира на всеки компютър, който използва мрежата [1], [2], [9], [10], [11], [12], [13], [14], [15].

Според данни на Google Trends, които показват, че търсенето на думата “blockchain“ се е увеличил експоненциално през последните 5 години, е възможно да навлизаме в пика на използването на блокчейн и регистрите му за документация (Фиг. 1) [8].



Фигура 1: Трендова графика на терминът “blockchain” в глобален мащаб

Това не е приложение, нито компания. Най-близко по функции е до Уикипедия. В тази платформа се вижда всичко в реално време и има достъп до цялата информация. Това се постига чрез списъци от данни за потока на информация, които постоянно се променят и обновяват. Всеки потребител може да проследи тези промени във времето и може да създаде свои собствени уикита, защото в основата си те са просто инфраструктура за данни. Блокчейн е също такава отворена инфраструктура, която съхранява много видове активи. Той съхранява историята на управлението, собствеността и местоположението на различни видове активи като цифровата валута Биткойн, цифрови активи като име на притежател на IP адрес, сертификати, договори, обекти от реалния свят, дори лична информация [9], [10], [11], [12], [13], [14], [15]. Този публичен регистър, който съхранява транзакции в мрежа и се копира многократно, така че да е много сигурен и труден за подправяне (Фиг. 2).



Фигура 2: Приложения на блокчейн, различни от използването на Биткойн

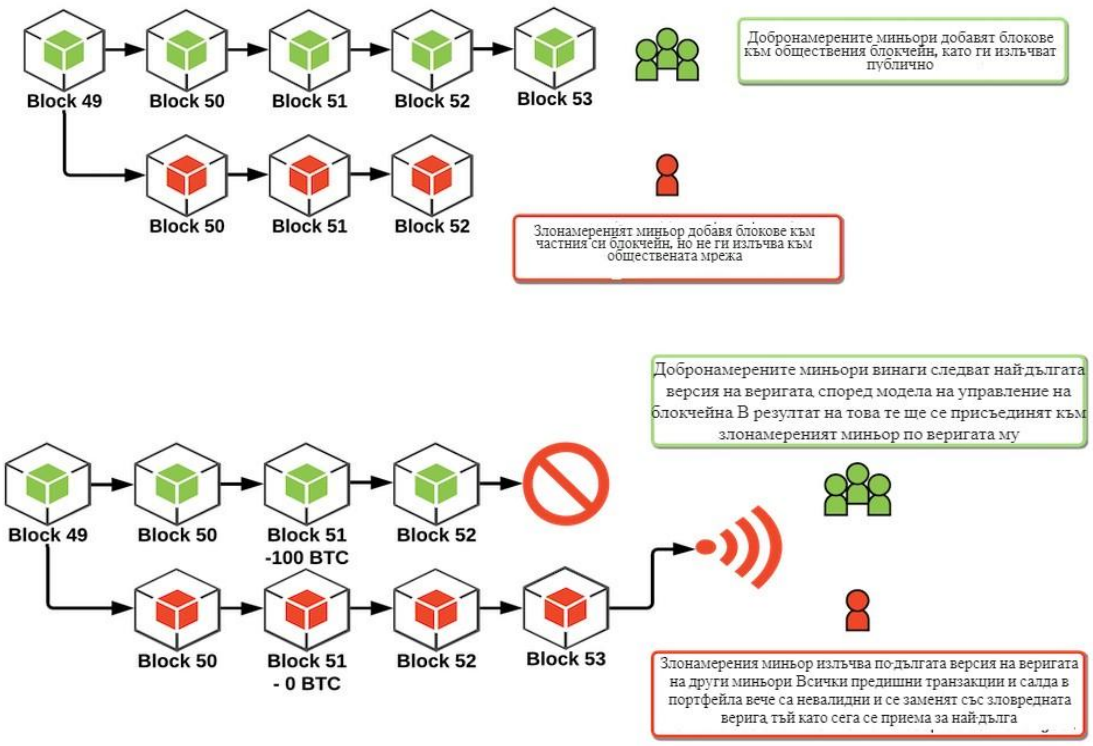
Блокчейн е следващата еволюционна стъпка в развитието на икономиката. Това е така, защото децентрализираният му подход за проверка на промените във важна информация е насочен към многовековния проблем с доверието. Това е социален ресурс, който твърде често се изчерпва, особено на фона на бурните опасения относно сигурността на ценните данни на тази ера [3], [5], [8], [14], [15], [16], [17], [18].

С използването на блокчейн можем да се създаде споделена реалност между субекти, които не са достойни за доверие. Отделните звена в мрежата не е необходимо да се познават или да се доверяват един на друг, защото всеки от тях има възможността да наблюдава и да следи за достоверността на транзакцията. Възможно е създаването на децентрализирана база данни, която има ефективността на монопол, без всъщност да се създава този централен орган. Така че всички тези потребители могат да си взаимодействат, използвайки една и съща база данни, без да се доверяват един на друг. За потребителите това създава пълна прозрачност. Докато обектът в реалния свят се движи по предварително изготвения му път, може да се види неговия цифров сертификат или токен да се движи по веригата. Този процес открива напълно нови възможности на доверие в нашия корумпиран свят.

Недостатъци на блокчейн

Що се отнася до основната блокчейн технология, все още има големи препятствия, които стоят на пътя й, дори и тя да има повече потенциал от криптовалутите. Главно сред тях е, че липсват основните универсални протоколи, които правят Интернет универсално достъпен (TCP-IP, HTML и т.н.). Това дава достъп до информацията само ако потребителят е част от информационната система [2], [6].

Друг потенциално голям недостатък е сигурността на системата. Алгоритъмът за консенсус Proof of Work, който защитава блокчейна на Биткойн, се оказва много ефективен. Има обаче няколко потенциални атаки, които могат да бъдат извършени срещу блокчейн мрежи и 51-процентната атака е сред най-обсъжданите (Фиг. 3).



Фигура 3: 51-процентна атака

Подобна атака може да се случи, ако един субект успее да контролира повече от 50 % от хеширащата мощност на мрежата, което в крайна сметка би позволило нарушаване на хронологията чрез умишлено изключване или промяна на подреждането на транзакциите [8].

Към тези проблеми със сигурността и поради причината, че блокчейн разчита на криптография с публични ключове, една от основните пречки пред масовото използване на технологията е липсата на стандартна система за управление на ключовете, включително механизми за възстановяване и отмяна. Без подходящ механизъм за възстановяване, загубата на частен ключ би възпрепятствал титуляря на акаунта да извърши каквато и да е операция. По същия начин без подходяща система за отмяна на ключ, ако частен ключ е компрометиран всеки потребител притежаващ този ключ може да извършва неоторизирани транзакции от името на акаунта притежател [7].

Друго важно ограничение на технологията е производителността, която е критична в контекста на обществените мрежи. Съществуващите публични мрежи могат да се справят само с ограничен брой транзакции. Например Биткойн системата обработва по-малко от 300 000 транзакции на ден, за разлика от 150 милиона транзакции, обработвани от Visa. Транзакциите с Биткойн се потвърждават на всеки десет минути. Това е значително повече от нужното време, което обикновено отнема за база данни да съхрани и запише информация.

Не на последно място поради анонимността, която съществува в децентрализирания блокчейн и виртуалните валути, те се превръщат във втори дом за всички незаконни транзакции. Един добър пример за това е „Тъмната мрежа“, която по свето същество представлява подземната част на Интернет пространството, която не е индексирана и не може да се достигне чрез стандартните браузъри. Тя разчита на сериозни криптиращи протоколи, като маршрутизатора “Onion” за “Tor” браузър. Всички тези предпазни средства правят „Тъмната мрежа“ център на незаконни и корупционни дейности, като пране на пари, търговия с наркотици и оръжия, трафик на хора, и дори детска порнография. Воденето на кибервойни [9], [10], [11], [12], [13], [17], [18] е съвременен вид война, чрез употребата на Интернет и технологичната база, за превъзходство във военно, икономическо, политическо отношение. Така практически всички водещи държави разработват и из-

ползват собствени кибер оръжия, а човечеството е в началото на кибервойните [2], [14], [15], [16], [19], [20], [21].

Изводи

Както при всички технологии в ранен стадий, предизвикателства има и при блокчейн. Основната инфраструктура трябва да бъде гъвкава с възможност за нарастване, но постигането на консенсус за извършване на такива промени е трудно в работна среда с отворен код. Съществува риск неточна информация трайно да се вмъква в блокчейн. Също така неизменността и необратимостта на транзакциите може да затрудни физическите лица и фирмите да взимат решения, когато има спор [1], [4], [6].

Има голям обществен интерес да се отговори на тези въпроси, но е още твърде рано. Тази технология трябва да се изучава и разбира, за да се увеличат максимално ползите от нея и за постигане на по-добри резултати от развитието ѝ. Със сериозни изследвания може да се открият най-добрите начини при използване на технологията за намаляване на разходите и увеличаване на достъпа до финансови услуги, като същевременно да се защитава социалния капитал, който е жизненоважен за икономическото развитие. В това отношение трябва да се има предвид безпрецедентната конкуренция и предизвикателствата пред действащите финансови институции и регулатори. При колективното вземане на правилно решение, трансформацията може да осигури жизненоважен елемент за постигане на еволюция в глобалната икономическа общност.

References

1. Парашкеванова, Г., Цанков, Ц. (2016). *Киберпрестъпността като основна съвременна заплаха за големите организации*. Научна конференция MATTEX 2016, Шумен, ISSN 1314-3921.
2. Стаменова, А., Диманова, Д., Цанков, Ц. (2014). *Новите войни на XXI век*. Научна конференция MATTEX 2014, Шумен, ISSN 1314-3921.
3. Цанков, Ц. (2012). *Компютърна лаборатория за автоматизиран синтез на сигнали с висока структурна сложност*. Научна конференция MATTEX 2012, Шумен, ISSN 1314-3921.
4. Chang, S.-H., Shih, C.-P. (2018). *The Influence and Application of Artificial Intelligence &Blockchain on Financial Service*. HOLISTICA – Journal of Business and Public Administration, vol. 9, issue 3, pp. 45–54, DOI: 10.2478/hjbpa-2018-0022.
5. Courtois, N., Song, G., Castellucci, R. (2016). *Speed Optimizations in Bitcoin Key Recovery Attacks*. Tatra Mountains Mathematical Publications, vol. 67, pp. 55–68, DOI: 10.1515/tmmp-2016-0030.
6. Jirgensons, M., Kapenieks, J. (2018). *Blockchain and the Future of Digital Learning Credential Assessment and Management*. Journal of Teacher Education for Sustainability, vol. 20, no. 1, pp. 145–156, DOI: 10.2478/jtes-2018-0009.
7. OECD (2017). *OECD Digital Economy Outlook 2017*. OECD Publishing, Paris, 324 p. DOI: 10.1787/9789264276284-en.
8. URL: https://trends.google.com/trends/?geo=US.
9. Фетфов, О., Боянов, П., Ташева, Ж., Трифонов, Т., *Анализ на съвременните видове уязвимости и експлойти в компютърните мрежи и системи*, Annual of Konstantin Preslavsky University of Shumen, Shumen, Университетско идателство „Епископ Константин Преславски“, ISSN 1311-834X, Vol. VI E, 2016, с. 112-122.
10. Савов, И., Боянов, П., *Приложение на кибератаката с отказ на услуги DOS (Denial of Service) срещу информационните ресурси на национални държавни агенции и академични институции*, Politics & Security Journal, Publishing complex HSSE, ISSN 2535-0358, Year III, Issue 1, 2019, pp. 15-20.

11. Фетфов, О., Боянов, П., Ташева, Ж., Трифонов, Т., *Сравнителен анализ на съвременните видове антивирусни програми*, Annual of Konstantin Preslavsky University of Shumen, Shumen, Университетско идателство „Епископ Константин Преславски", ISSN 1311-834X, Vol. VI E, 2016, с. 123-133.
12. Boyanov, P., Hristov, Hr., Fetfov, O., Trifonov, T., *Educational simulation the local area network of academic departments with securely configured FTP server*, International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 31, March 2017, Bulgaria, 2017, pp. 146-154.
13. Boyanov, P., *Unauthorized access attempts to the information resources of private computer networks in academic institutions via network scanning cyber attacks*, Yearbook of Higher School of Security and Economics, Plovdiv, Publishing complex HSSE, ISSN 2367-8798, Vol. XV, 2018, с. 51-58.
14. Камарашев, Г., Димитрова, С., *Финансовия мениджмънт като елемент на военната логистика*, Trans&Motauto 2005 с.37-41.
15. Kamarashev, G., Dimitrova, S., *Outsourcing as a part of the management of resources for security and defense*, SIBIU 2011, pp.643-647.
16. Kamarashev, G., Dimitrova, S., A*spects of defence and security resource allocattion*, Sibiu 2007.
17. Kamarashev, G., Banabakova, V., *Acquisition – theoretical and practical aspects of application in the defense system*, Brno 2005 с.30-37.
18. Савова, Ж., Богданов, Р., *Анонимна система за комуникации в киберпространството, използваща протокол TOR*, Сборник научни трудове на научна конференция на Факултет „А, ПВО и КИС" „Новата парадигма за сигурност в киберпространството" Шумен 2014, стр. 259-265, ISBN 978-954-9681-49-9.
19. Савова, Ж., Богданов, Р., *Оценка на изчислителната сложност на алгоритмите за генериране на големи прости числа за целите на криптографията*, Сборник научни трудове на Научна конференция „Проблеми на информационната сигурност", гр. Шумен, 2010, ISSN 1314-0647.
20. Савова, Ж., Богданов, Р., *Приложение на недвоичните псевдослучайни последователности в криптографията*, Сборник научни трудове Немус'2012. Институт по отбрана Проф. „Цветан Лазаров", 2012, ISSN 1312-2916.
21. Досев, Н., Петров, В., *Съвременни тенденции и аспекти на информационната сигурност в автоматизираните информационни системи и мрежи (АИС/М)*, Научна конференция с международно участие MATTEX 2018 , Шуменски университет „Епископ Константин Преславски", Университетско издателство, Сб. научни трудове том 2, част 1, стр. 85¸95, ISBN 1314-3921.
22. Николов, Л. (2018). *Ролята на Европейския съюз в осигуряването на киберсигурност*. Международна научна конференция „Политиката на европейския съюз по защитата на информацията и личните данни", Сборник научни трудове – ШУМЕН 2018, ISBN 978-954-9681-89-5.
23. Николов, Л., Фетфов, О., Борисова, А. (2018). *Съображения за сигурност при писането на кодове с JavaScript*. Научна конференция с международно участие MATTEX 2018, Шумен, ISSN 1314-3921.
24. Nikolov, L., Slavyanov, V. *Network infrastructure for cybersecurity analysis*. International scientific conference 2018, "Vasil Levski" National Military University - Artillery, Air Defense and CIS Faculty, Shumen, Bulgaria, 2018, ISSN 2367-7902.