БЛОКЧЕЙН ТЕХНОЛОГИЯТА. ДОКАЗАТЕЛСТВОТО ЗА РАБОТА (PROOF OF WORK - PoW) И ДОКАЗАТЕЛСТВОТО ЗА ЗАЛОГ (PROOF OF STAKE - PoS).

Георги Коджаниколов,

Университет по библиотекознание и информационни технологии, докторант

Резюме: *Бурното развитие на технологиите от последните години донесе не просто нови възможности за комуникация и свързване. Обществените отношения в социален, икономически и културен план са изцяло променени благодарение на новите реалности на дигиталната ера. Като продукт на тези тенденции се появиха и „криптовалутите“. BitCoin ще остане в историята като първата суверенна дигитална валута. Криптовалутите, функциониращи изцяло като дигитална технология без физически аналог и извън контрола на орган на публична власт или регулатор, създават множество нови възможности, но и предизвикателства. Относителната анонимност на използващите ги лица правят криптовалутата привлекателен инструмент за изпирането на пари. Зараждането на феномена, чиято функционалност е обезпечена от блокчейн технология от нов тип (т. нар. технология на разпределния регистър), чертае както хоризонти за иновации и развитие, така и заплахи, непознати до момента за финансовите системи.*

Ключови думи: *криптовалути, биткойн, децентрализация, блокчейн, доказателство за работа (PoW), доказателство за залог (PoS);*

THE BLOCKCHAIN TECHNOLOGY. PROOF OF WORK (PoW) AND PROOF OF STAKE (PoS).

Georgi Kodzhanikolov

University of Library Studies and Information Technology, Ph.D

Abstract: *The rapid development of technologies in recent years has not only brought new opportunities for communication and communication. Public relations in social, economic and cultural terms have been significantly affected thanks to the technological expansion. As a product of this rapid development, "cryptocurrencies" also emerged. Bitcoin will go down in*

history as the first sovereign digital currency. Cryptocurrencies, functioning entirely as a digital technology without a physical counterpart and outside the control of a public authority or regulator, created a host of new opportunities, but also challenges. The relative anonymity of those using them make cryptocurrency an attractive tool for money laundering. The emergence of the phenomenon, the functionality of which is provided by blockchain technology of a new type, draws both horizons for innovation and development, as well as threats unknown to the financial systems.

Key words: *cryptocurrencies, BitCoin, decentralization, financial services, money laundering, digitalisation, proof of work (PoW), proof of stake (PoS);*

Въведение

Случайно или не появата на първата суверенна цифрова валута, извън контрола на публичен орган на власт, Биткойн (BitCoin)[1] се случва в края на 2008г. като отговор на последиците от световната финансова криза. Събитие от естество да преосмисли цялостната структура и функциониране на познатата ни финансова сисмета.

Предложеният модел на безналични, дигитални пари изключва необходимостта от участието на трета доверена страна (банка или друга финансова институция), която да гарантира плащането и интегритета на цялостната система. Криптовалутите, като цяло, и биткойн в частност, са сравнително нови явления. Тяхната популярност е неоспорима и към настоящия момент изчезването им е по скоро хипотетична възможност. Те се превърнаха във функционираща реалност и алтернатива на познатата и утвърдена система на традиционните финанси. В този смисъл, с оглед зачестилите случаи на изпиране на пари или друг вид престъпни деяния, извършвани посредством използването на криптовалути, превръща познаването на функционалната им природа в залог за сигурността и стабилността на финансовата система[2].

Революционно по характер е и технологичното разрешение, което обезпечава фунционирането на системата зад биткойн и криптовалутите като цяло. Чрез създаването и внедряванети на т.нар. „блокчейн“ (Blockchain) технология („технология на разпределения регистър“ според възприетия понятиен апарат на законодателствоот на

[1]Franco, Pedro. Understanding Bitcoin. Cryptography, engineering and economics. John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom, 2015.

[2]Antonopoulos, Andreas. Mastering Bitcoin. Unlocking digital cryptocurrencies. O'Reilly Media, Inc., Sebastopol, 2014, 298 p.;

ЕС[3]) е намерено решение на познатия в компютърните науки проблем на „двойната употреба“. Успоредно с това се елиминира нуждата от участие на трета доверена страна (банка или друга финансова инстируция посредник) в подсигуряване на процеса по транзактиране между участниците в системата. В компютърните науки проблемът на двойната употреба (double spending) се разбира като опасността виртуалните пари да могат да бъдат похарчени повече от веднъж. На практика неограничен брой пъти. Виртуалните пари на езика на компютърната наука представляват файл, точно като дигитален документ.

Изложение

Блокчейн[4] е разпределена база данни или своеобразен счетоводен баланс („public ledger“), споделян и съхраняван от всички участници (nodes) в компютърната мрежа на BitCoin. Като база данни блокчейн съхранява информация по електронен път в цифров формат. Характерно за този тип системи е възможността им да осигурят гаранции за вярността и сигурността на вече верифицирани веднъж и записани в регистъра данни. Отличителна черта на блокчейн технологията в сравнение с типичните бази от данни е начинът на структуриране на данните. Тук те се свързват в поредица от блокове. Всеки от тях има определен капацитет за съхранение на информация и след запълването и верифицирането му се свързва с предходните блокове. Образува се своеобразна верига от данни, известна като блокчейн. На всеки блок във веригата се дава времево клеймо, като изграждането на веригата следва и хронологична последователност. Публичният регистър се съхранява и е на разположение с цялата съдържана информация на участниците в мрежата по всяко време. Не се контролира от определено лице или централен сървър. Даже напротив – контролът е дистрибутиран, което прави и системата децентрализирана. Установените и верифицирани блокове, добавени към веригата, стават неделима част от публичния регистър. Подмяната на записаната вече и съдържана информация става практически невъзможно. Замисълът зад технологичното разрешение е създаването на модел за прозрачното и сигурно съхранение на информация, в частния случай и за целите криптовалутите на историята на транзакциите.

[3] Предложение за Регламент на Европейския парламент и на Съвета относно пилотна уредба на пазарните инфраструктури, основани на технологията на децентрализирания регистър — COM (2020)594;
[4] Making sense of bitcoin, cryptocurrency and blockchain. Bitcoin, cryptocurrency, blockchain... So what does it all mean? (Available on: https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html, 12.11.2022)

BitCoin протоколът и технологията зад него изграждат цялостна и автономна екосистема на дигитална валута от нов тип[5]. Публичният регистър, т.нар. „public ledger“ на направените транзакции и баланси по сметките на всички участници в системата, елиминира необходимостта от участие на трета, независима страна в процеса на транзактирането. BitCoin протоколът децентрализира и дистрибутира тази отговорност към всички участници в мрежата за обмен. Мрежата записва и съхранява цялата история на транзакциите и балансите на всички участници в нея в публичен регистър или блокчейн.

Блокчейнът структурира и подрежда списък от свързани данни и изгражда блокове от транзакции. Блоковете са свързани помежду си, като всеки съдържа препращаща и обвързваща го с предходно генерирания блок информация. Всеки блок в рамките на цялостната структура се идентифицира посредство хеш в началото на блока, генериран с криптографския хеширащ алгоритъм SHA-256. Всеки блок съдържа референция към блока преди него, наричан още „блок родител“. Това създава непрекъсната връзка между вече създадените и новодобавените към веригата блокове. Последователността от хешове, свръзващи всеки блок с неговия родител, създава верига, която може да бъде проследена до първия някога създаден блок, познат като „първичен блок“.

Хеш информацията е интегрална част от всеки блок. Идентичността на новосъздаения блок е невъзможно да бъде потвърдена и верифицирана, ако тази на предходния във веригата бъде изменена. Когато блокът „родител“ бъде модифициран по какъвто и да е начин, хешът му също се променя. Това води до лавинообразен, каскаден ефект, гарантиращ интегритета на цялостанта верига. За да бъде възможна такава промяна във вече установената и закрепена информация по веригата, би било необходима огромна изчислителна мощ. В този ред на мисли, веригата от изградени блокове сама охранява неизменимостта си. Тази инфраструктура гарантира сигурността и прозрачността във функционирането на екосистемата на BitCoin.

Блокчейн е публично достъпен регистър на всички обработени транзкации в мрежата на BitCoin от самото ѝ създаване до момента. Той позволява всеки, използващ софтуерния код зад инфраструктурата, да има достъп до отчетността и съотвено с възможността сам да провери и да се убеди във валидността и легитимността на конкретно събитие. Транзакциите с BitCoin са видими и публични за всички участници в мрежата и се включват в регистрите на blockchain-а само след като бъдат успешно

[5] Godsiff , Philip. Bitcoin: Bubble or Blockchain, Springer International Publishing Switzerland, 2015;

верифицирани и потвърдени от останалите участници. Това създава гаранция, че повторното изпращане или „изхарчване“ на конкретна единица BitCoin няма да бъде възможно. Новите транзакции се подлагат на своеобразна проверка от софтуера преди да бъдат верифицирани и присъединени към публичния регистър с оглед гарантиране, че един и същи BitCoin не може да бъда похарчен повече от веднъж.

Доказателство за работа (Proof of Work (PoW)

Моделът на „доказателството за работа“ (PoW) описва консенсусен механизъм, който изисква значително количество изчислителни усилия от мрежа от устройства[6]. По същество конституира децентрализиран консенсуален механизъм, изискващ членовете на мрежата (nodes) да положат усилие за решаване на криптирано шестнадесетично число, своеобразна математическа задача. Процесът е известен още като „копаене“ (“mining”). Участниците в системата ангажират изчислителната мощ на своите устройства и техният технологичен капацитет за верификация на транзакции, като в замяна получат от системата възнаграждение под формата на новосъздадени единици цифрова валута. PoW способства за сигурната обработка на транзакции от типа peer-to-peer (P2P) без нужда от доверена трета страна. Недостатък на това решение е необходимото голямо количество електрическа енергия, за да бъде поддържана системата, което с времето само ще се увеличава и оскъпява процесът по „добиване“.

Копачите чрез специализиран софтуер и изчислителната мощ на своите компютърни конфигурации валидират новите транзакции и ги записват в глобалния публичен регистър – блокчейн. На всеки средно около 10 минути се „изкопава“ или валидира нов блок, съдържащ в себе данни за валидирани транзакции, извършени след добавянето на последния блок от веригата. Вече добавените транзакции към блокчейна се считат за валидирани, което позволява на новите собственици на биткойн да се разпореждат с получените средства.

За да получат възнаграждение от мрежата, копачите участват в своеобразно състезание в решаването на сложния матемаически проблем въз основа на криптографски хеш алгоритъм. Решението на задачата, известно като „доказателство за работа“ (Proof of work), се включва в новия блок и служи като доказателство, че копачът е допринесъл за фунционирането на системата чрез извършването на множество

[6] Narayanan, Arvind, Joseph Bonneau, Edward Felten. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton, Princeton University Press, 2016;

изчисления. Процесът е познат като „копаене“ (mining) или добив, защото възнаграждението е проектирано да стимулира намаляваща възвръщаемост, характерна за добива на благородни метали. Максималната сума новосъздадени биткойни, следствие на процеса на копаене, е проетирано да намалява приблизително на всеки 4 г. (на всеки 210 000 нововалидирани и добавени към веригата блока).

Водещата цел на добива на биткойн не е създаването на нови единици от криптовалутата. Процесът представлява механизъм, който поддържа сигурността на мрежата и я прави децентрализирана. Възнаграждението за извършена работа от системата към участниците под формата на новогенерирани единици виртуални монети и таксите за транзакциите е схема за стимулиране, която обезпечава сигурността и функционирането на мрежата.

Процесът на добива („mining“) предполага потребителите на BitCoin системата да оперират със специализрания софтуер на специлно пригодени хардуерни компютърни конфигурации. Процесът е важен не просто за създаването на нови BitCoin единици. Чрез включването си в системата за обработка и верификация на транзакции потребителите създават огромна компютърна изчислителна мощ, която се изполава от софтуера за верификация и потвърждаване на плащания. След потвърждаването на тези транзакции, те биват добавени в публичния регстър („blockchain“) и биват валидирани за цялата мрежа. Този процес гарантира, че само легитимните транзакции ще бъдат верифицирани и добавени към блокчейна, като решава double-spending проблема. Цялата мрежа от потребители, осигурява изчислителната мощ и участва в процесите, гарантиращи сигурността на плащанията[7].

Процесът на „добиване“ по същество представлява математически алгоритъм. Софтуерът генерира математическа задача, решаването на която изисква участието на огромна изчислителна мощ. Намирането на решение води до потвърждаване валидността на транзакциите и добавянето им към публичния регистър като легитимни под формата на блок в блокчейна. Софтуерът е предварително програмиран да увеличава сложността на генерирания математически проблем с напредване на времето. Новогенерираните единици BitCoin се разпределят на участниците в мрежата, които с изчислитената мощ на своите компютърни конфигурации са допринесли за нейното функциониране и сигурност. При достигане на крайната точка от добиването на BitCoin,

[7] Lee Kuo Chuen, David. Handbook of digital currency. Bitcoin, Innovation, Financial Instruments, and Big Data. Sim Kee Boon Institute for Financial Economics, Singapore Management University, Singapore, 2015;

т.е. бъдат „изкопани“ приблизително 21,000,000 единици от виртуалната валута, потребителите, които осигуряват функционирането на мрежата, се предвижда да бъдат стимулирани като получават своеобразна такса от всяка обработена транзакция.

Всеки новодобавен блок към блокчейна е свързан с предходните по начин, правещ манипулацията невъзможна. Промяната на вече направен запис в блокчейна би изисквало преизчисляване на всички вече добавени елементи към регистъра, което от технологична гледна точка, граничи с немислимото. В този контекст „копачите“ или потребителите, които участват в процеса на верификация на транзакциите играят фундаментална роля за осигуряването интегритета и сигурността на мрежата. Колкото повече са те, толкова по-непосилна става задачата за потенциално желаещите да манипулират публичния регистър. „Копаенето“ е конкурентен процес, така че може и с времето се превръща в надпревара между тези с най-голяма изчислителна мощност. В този смисъл се създават и т.нар. „миньорски пулове“ (своеобразни общности от копачи), за да увеличат шансовете си за получаване на награда.

Съгласно консенсуса на PoW, хиляди програми за копаене работят върху един блок, докато хешът бъде разрешен, след което се преминава към следващия блок. Доказателството за работа (PoW) е консенсусен механизъм, използван от много криптовалути за валидиране на транзакции в техните блокчейни и присъждане на токени, които да стимулират участието в мрежата.[8]

Доказателство за залог (Proof of stake (PoS)

Моделът на „доказателството за залог“ (PoS) представлява също консенсуален механизъм за обработване и валидиране на плащания и добавяне на нови записи в съответния блокчейн. Той е алтернативен на „доказателството за работа“, залегнало при BitCoin технологията. PoS е предпочитан метод при нововъзникващите криптовалути и се различава съществено от PoW. Втората по пазарна капитализация и популярност криптовалута Ethereum използва именно този механизъм за валидиране на тразакциите в своята мрежа.

При „доказателстовото за залог“ необходимостта от ангажиране на огромна изчислителна мощ под формата на компютърни конфигурации и електрическа енергия

[8] Mullan, P. Carl. A history of digital currency in the United States. New technology in an unregulated market. Palgrave Advances in the Economics of Innovation and Technology, Greensboro, North Carolina, USA, 2016, 285 p. ;

за валидиране на трансакции, механизмът на „доказателството за залог“ предпоставя участниците в процесца да „залагат“ монети от притежаваните криптовалути. С този подход се постига ефект на драстично намаляване на необходимото потребление на енергия, подобряване на децентрализацията, мащабируемостта, адаптивността и сигурността.

Proof of stake променя начина, по който блоковете (структурните единици на блокчейна) се проверяват с помощта на машините на собствениците на монети, така че не е необходимо да се извършва толкова много изчислителна работа. Собствениците предлагат своите монети като обезпечение или своеобразно „залагане“, като по този начин се включват в процеса по верификация и получават шанса да валидират блокове и съответно да станат валидатори. Потребителите, участващи в процеса, трябва да „заключат“ определено количество монети в мрежата като условно ги залагат. Размерът на залозите определя шансовете на потребителя или групата от потребители да бъде избран като следващ валидатор. Пропорционално на големината на залога расте и шансът системата да селектира точно определена група за валидиране на блок в мрежата. В процеса на подбор се добавят и допълнителни уникални критерии, за да се гарантира, че като валидатори няма да бъдат предпочитани само притежателите на най-голям брой единици от съответната монета в мрежата.

Допълнително въведен критерий при избора на валидатори е т.нар. „възраст на монетите“, като мрежата селектира въз основа на това за какъв период от време са били заключени под формата на залог съответните токени (единици криптовалиута). „Възрастта“ на монетите се изчислява, като броят на дните, през които монетите са заложени, се умножи по броя на заложените монети. След като определена група потребители са валидирали и съответно добавили блок към блокчейна възрастта на монетите им се нулира и те трябва да изчакат определен период от време, за да може да валидират друг блок. По този начин се превентира възможността притежателите на голям брой единици, поставени в залог, да доминират в блокчейна и да получават приоритетно възнагражденията под формата на транзакционни такси или новогенерирани единици криптовалута.

Криптовалутите, използващи алгоритъм за доказателство за залог, имат автономията да определят и задават предварително правилата и методите, по които да функционира консесуалният механизъм за верификация и валидиране на транзакции. Ако група потребители бъде избрана да валидира следващ блок, то тя следва да провери

дали трансакциите в блока са валидни. Следва подписването на блока и добавянето му към блокчейна. Стимул за тази дейност е от една страна поддържане и гарантиране на сигурснотта на мрежата, а от друга са присъжданите транзакционни такси или генерирането на нови токени криптовалута.

Към момента някои от най-разпознаваемите и популярни криптовалути на пазара използват именно Proof of stake механизма за валидиране и добавяне на транзакции към техните блокчейни. Такива са например: Ethereum, Cardano, Solana, Polkadot, Avalanche.

Proof of stake протоколът се появява като алтернатива на оригиналния Proof of work механизъм при BitCoin. Целта е да се разреши най вече проблемът с нарастващите разходи по електроенергия и да се ограничат негативните последици за околната среда. И двата механизма имат своите предимства и недостатъци. Тяхното развитие и еволюция са констатен процес, задвижван от екипи от програмисти, икономисти и финансисти. Само по себе това предполага в бъдеще фунционалните им характеристики и приложимост да се разширяват и подобряват.

Заключение

Появата на криптовалутите и блокчейн технологиите безспорно са от естество да поставят под въпрос цялостното функциниране на обществените отношения[9]. Докато утвърждаването на криптовалутата като законно платежно средство, алтернативно на фиатните пари, за момента изглежда утопична идея, то нещата по отношение на блокчейн технологиите стоят на съвсем противоположна равнина. Блокчейн технологиите са предмет на доразвиване и имплементация във всевъзможно сфери от заобикалящата ни действителност – от медицина, през недвижими имоти, търговия до създаването на „умни договори“ без участието на лице с юридическо образование. Безспорен е ефектър и потенциалът на тези чисто технологични достижения, което прави тяхното разбиране и изучаване задължително за стремящите се към просперитет общества[10].

[9] Guttmann, Robert. Cybercash. The Coming Era of Electronic Money. Palgrave Macmillan, 2003;

[10] Kelly, Brian. The BitCoin Big Bang. How alternative currencies are about to change the world. John Wiley & Sons, Inc., Hoboken, New Jersey, 2015, 240 p.

Използвани източници:

1. Franco, Pedro. Understanding Bitcoin. Cryptography, engineering and economics. John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom, 2015.
2. Antonopoulos, Andreas. Mastering Bitcoin. Unlocking digital cryptocurrencies. O'Reilly Media, Inc., Sebastopol, 2014, 298 p.;
3. Предложение за Регламент на Европейския парламент и на Съвета относно пилотна уредба на пазарните инфраструктури, основани на технологията на децентрализирания регистър — COM (2020)594;
4. Making sense of bitcoin, cryptocurrency and blockchain. Bitcoin, cryptocurrency, blockchain... So what does it all mean? (Available on: https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html, 12.11.2022);
5. Godsiff , Philip. Bitcoin: Bubble or Blockchain, Springer International Publishing Switzerland, 2015;
6. Narayanan, Arvind, Joseph Bonneau, Edward Felten. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton, Princeton University Press, 2016;
7. Lee Kuo Chuen, David. Handbook of digital currency. Bitcoin, Innovation, Financial Instruments, and Big Data. Sim Kee Boon Institute for Financial Economics, Singapore Management University, Singapore, 2015;
8. Mullan, P. Carl. A history of digital currency in the United States. New technology in an unregulated market. Palgrave Advances in the Economics of Innovation and Technology, Greensboro, North Carolina, USA, 2016, 285 p.;
9. Guttmann, Robert. Cybercash. The Coming Era of Electronic Money. Palgrave Macmillan, 2003;
10. Kelly, Brian. The BitCoin Big Bang. How alternative currencies are about to change the world. John Wiley & Sons, Inc., Hoboken, New Jersey, 2015, 240p.;