«М.А. Гендельманның 110 жылдығына арналған «Сейфуллин оқулары – 19» халықаралық ғылыми-практикалық конференциясының материалдары = Материалы международной научно-практической конференции «Сейфуллинские чтения – 19», посвященной 110 - летию М.А. Гендельмана» - 2023.- Т.I, Ч.III.- Б. 208-211.

ӘОЖ 004.9

БЛОКЧЕЙН ТЕХНОЛОГИЯСЫ

Гриф М.Г., техника ғылымдарының докторы, профессор
Новосибирск мемлекеттік техникалық университеті, Новосибирск қ., Ресей
Орманша З.Д., 1-курс докторанты
«С.Сейфуллин атындағы Қазақ агротехникалық зерттеу университеті»
КеАҚ, Астана қ.

Блокчейн - (ағылш. *block chain*, blockchain) — биткойн (ағылш. *Bitcoin*) немесе оның баламасы жүйесінде транзакциялары тобын жазуға арналған арнайы құрылым. Қарапайым тілмен айтқанда, сіздің өміріңізге қатысты барлық шынайы дерек, жазбаларды тізбектеп сақтау технологиясы. Туған сәтіңізден бастап ешбір дерек тыс қалмайды. Тіпті бір кезде жол ережесін бұзғаныңыз, досыңызға шотыңыздан ақша аударғаныңыз, интернет дүкеннен жасаған саудаңыз, үйленгеніңіз, барлығы-барлығы блоктарда тізбектеліп сақталады. Қысқаша айтқанда қағазға жазылатын деректердің барлығын блокчейнге де жазуға болады. Айырмасы blockchain-де жазбаны қолдан жасауға, өшіруге, жасыруға болмайды. Өткен күнмен жазба жасай салатын нотариустар, айыппұлыңызды базадан өшіретін пысықайлар, несие тарихын жаңартатын алаяқтар дәурені өтеді. Блокчейн деректерін яғни блоктарды және олардың мазмұнын иесі рұқсат етсе кез-келген адам көре алады. Демек blockchain желісінің пайдаланушысына оның деректерін растайтын нотариус, тіркеуші, аудитор, сақтандыру агенті, бақылаушылар сияқты делдалдар қажет болмайды [1].

Термин алғаш рет Bitcoin жүйесінде енгізілген толығымен қайталанатын таратылатын дерекқордың атауы ретінде пайда болды, бұған блок көбінесе әртүрлі крипто-валютада операциялар деп аталады, бірақ блоктық тізбектер технологиясы қандай да бір өзара байланысты ақпарат блоктарына дейін кеңейтілуі мүмкін.

Блокчейннің ерекшеліктері:

1. Trustworthy - Blockchain сенімді болып табылады, өйткені ол тең рангты желіні пайдаланады, кез келген адам транзакция тарихына кіріп, транзакцияның егжей-тегжейлерімен және кіммен мәміле жасалатынын біле алады. Оның құрамына хэш функциясы кіреді, ол өте қауіпсіз және оны алгоритм арқылы ешкім өзгерте алмайды.

2. Distributed - Blockchain - бұл таратылған жүйе, әрбір түйінде транзакция туралы ақпарат ала алатын бақылаушы орган жоқ.

Орталықтандырылған жүйенің қай жерінде болса да тек орталық орган транзакцияға қол жеткізе алады. Таратылған жүйеде түйіндер сәтсіз болса, ол басқа түйіндерге әсер етпейді және басқа түйіндер қосылады.

3. Hash технологиясы - Хэш ерекшелігі - blockchain-тің маңызды технологиясы, бұл мүмкіндік blockchain технологиясын өте қауіпсіз етеді, өйткені әрбір блокта алдыңғы блоктың хэші бар, егер блокта қандай-да бір өзгеріс болса, ол келесі блоктың хэшімен сәйкес келмейді. . Сонымен, бұзақылық қаупін осында азайтуға болады.

4. Secure- Blockchain өте қауіпсіз және оны оңай бұзуға болмайды. Блоктар Чанға қосылатын болады, егер кімде-кім кез-келген блокты бұзуға тырысса, ол сол блоктың қасындағы блокты жауып тастауы керек және блоктардың жылдамдығына шыдай алмайтын болады.

5. Мәміле үшін комиссия - Орталықтандырылған жүйеде соманы транзакциялау кезінде белгілі бір транзакция үшін банктер алынады, бірақ blockchain технологиясында бұл жойылады.

Транзакциялық блок - Bitcoin жүйесінде транзакциялар тобын жазу үшін арнайы құрылым. Мәміле оның форматы мен қолдары тексерілгенде және транзакция өзі бірнеше басқа адамдармен бірге топтастырылған және арнайы құрылым - блокқа жазылғанда, толық және сенімді («расталды») болып саналады. Блоктың мазмұны тексерілуі мүмкін, себебі әрбір блокта алдыңғы блок туралы ақпарат бар. Барлық блоктар бір дерекқорда жасалады, ол дерекқорда кез келген уақытта орындалатын барлық операциялар туралы ақпараттар қамтылады. Тізбектегі бірінші блок - негізгі блок (ағылшын генезис блогы) - бұл ата-аналар блогы болмағандықтан, бөлек оқиға ретінде қарастырылады.

Блок тақырыптан және транзакция тізімінен тұрады. Тақырып өз кезегінде хештен, транзакциялар хешінен және қосымша ақпараттан тұрады. Биткойн жүйесінде алғашқы транзакция болып құрылған блок үшін берілген комиссия болып табылады, әрі ол қолданушыға жүлде есебінде болады. Әрі қарай, алдыңғы блокқа жазылмаған транзакциялар кезегі бойынша жүйеге келтірілген транзакциялар тізімі болады. Кезектен алу критерийін майнер өзі белгілейді. Оның уақыт хронология кестесі бойынша болуы міндетті емес. Мысалы, жүйеге тек жоғары комиссиясы бар операциялар немесе берілген адрестер тізімі ғана енгізілуі мүмкін. Құрылған блок үшін берілген комиссиядан басқа транзакцияларда input параметрінің ішінде алдыңғы транзакциялардың жағдайына сілтеме болады (Мысалы, биткойндар жүйесінде, сілтеме, жұмсалынған биткойндар алынған транзакцияға сілтеме болады). Құрылған блок үшін берілген комиссия майнерінің операциясында ешқандай "енгізу" транзакциясы болмайды, сондықтан бұл параметрде кез келген ақпарат көрсетіле алады(олар үшін өрістің атауы ағылш. Coinbase parameter).

Бұл жеке тұлғаларға ғана емес, заңды тұлғаларға да қатысты. Blockchain технологиясы арқылы келісімшарттар, сатып алу-сату операцияларын жасауға болады. Еш жасырын схемасыз, айқын түрде мемлекеттік сатып алу операцияларын, тендерлерді өткізіледі. Бұл жүйе

жемқорлықты, бюрократиялық созбалаңды жоюға пәрменді. Банк жүйелеріне енсе, тіпті бірнеше бөлімдерді толығымен қысқартуға, банк операцияларының бірнеше кезеңін азайтуға мүмкіндік береді. Ипотекалық пәтерлер, жылжымалы мүлікті сатып алу-сату кезіндегі алаяқтық мүлдем жойылады дейді мамандар.

Мамандардың айтуынша: «бұл кезінде интернетте революциялық идея болған. Біреу сенсе, біреу сенбеген. Блокчейн технологиясы да өмірімізге енеді. Бұл жүйе арқылы біз қоғамдағы қаржылық айқындылыққа, қаражат пен уақытты үнемдеуге, қоғамның сенімін қалпына келтіруге қол жеткізе аламыз» [2].

Blockchain технологиясы салыстырмалы түрде жаңа зерттеу саласы болып табылады. Бұл технология үлкен үміт күтті, өйткені барлық транзакциялар үшінші тараптың көмегінсіз орталықтандырылмаған режимде жүзеге асырылады. Блокчейн технологиясы туралы білім мен түсініктің жетіспеушілігі бар, бұл оның академиялық зерттеулері мен практикалық қолданылуына кедергі келтіреді. Бұл құжат блокчейн технологиясы туралы қолданыстағы білім қорына қосымша болады деп күтілуде. Бұл құжаттың мақсаты-Blockchain технологиясына шолу жасау, Blockchain технологиясының ағымдағы күйін анықтау және blockchain құнды шешім ұсынатын негізгі қолданбаларды анықтау. Ол сондай-ақ оны қолдануға байланысты негізгі мәселелерді анықтауға тырысады. Қойылған мақсаттарға жету үшін осы мақалада әдебиеттерді шолуға көзқарас қабылданды. Бұл зерттеу құпиялылық, қауіпсіздік, анонимділік, орталықсыздандыру және мөлдірлік сияқты блокчейн технологиясының ерекше сипаттамалары оны әртүрлі салалардағы пайдаланушылар үшін бірегей ететінін көрсетеді. Сондай-ақ, құжатта блокчейн технологиясы өте шектеулі салаларда қолданылатындығы атап өтілген. Ол функционалдылықта кеңейіп, уақыт, тиімділік және дәлдік тұрғысынан көптеген салаларда төңкеріс жасайды деп күтілуде.

Cryptocurrency артындағы технология - бұл blockchain технологиясы. Блокчейн технологиясы идеясы алғаш рет екі зерттеуші Стюарт Хабер мен В. Скотт Сторнетта 1991 жылы сандық құжатты уақытты белгілеудің практикалық шешімін ұсынып, оны кейінге қалдыруға немесе бұзуға жол бермеу үшін пайда болды. Уақыт белгісі құжаттарын сақтау үшін жүйе криптографиялық қорғалған блоктардың тізбегін пайдаланды.

1992 жылы Markle Tree деп аталатын жаңа үлгі пайда болды, ол көптеген блоктарды бір тізбекте қосуға мүмкіндік берді, бірақ бұл технология 2004 жылы қолданылмаған және тоқтап қалған. 2004 жылы компьютер ғалымы және криптографиялық белсенді RPoW жүйесін (қызметтер жұмысының қайталанатын дәлелі) енгізді. айырбастауға болмайтын және қайтарылмайтын хэш-кэш негізіндегі жұмыс токенін алу үшін жұмыс істеді және оның орнына адамнан адамға ауысуға болатын RSA токенін жасады. Ол сонымен қатар сенімді пайдаланушыларға таңбалауыш

белгілердің иелігін сақтап қалу арқылы екі есе шығындалу мәселесін шешті, бұл оның пайдаланушыларына бүкіл әлем бойынша нақты уақыттағы транзакцияның дұрыстығын тексеруге көмектесті. Ол криптографияның прототипі ретінде қарастырылды.

Жаңа технологиялардың дамуы әрдайым жұмысты орындау тәсілдерінің түбегейлі өзгеруіне және қоғамдағы жойқын өзгерістерге әкеледі. Мысалы, бу экономиканы индустрияландыруға алып келді және жұмыс істейтін халықтың едәуір бөлігінің қозғалуына ықпал етті, сонымен қатар қоршаған ортаның тоқтаусыз нашарлауының негізін қалады (Левандовский, 2016; Киттель, 1967). Блокчейн бизнес пен қоғам үшін бірдей таңғаларлық сілкіністерді уәде етеді (Нотон, 2016). Блокчейн-бұл желіде болып жатқан әрбір деректер транзакциясының есебін жүргізуге арналған цифрлық орталықтандырылмаған қоғамдық тізілім. Таратылған кітаптағы әрбір транзакция желі мүшелерінің көпшілігінің консенсусымен тексеріледі. Бір рет енгізілген ақпаратты ешқашан өшіруге болмайды. Блокчейнде бұрын-соңды жасалған әрбір жеке транзакция туралы нақты және тексерілетін жазба бар. Басқаша айтқанда, blockchain деректерді / активтерді бөлісу, бірлесіп жұмыс істеу және транзакцияларды орындау (Allladi және т.б.) үшін көптеген нысандар (жеке тұлғалар да, ұйымдар да) үшін өзгермейтін, сенімді және қауіпсіз платформаны ұсынады. Бұл алаяқтықтың алдын алады және "шектеусіз"тең-теңімен транзакцияларды жүзеге асыруға мүмкіндік беретін тексерудің сандық түрін қамтамасыз етеді. Бұл технология "нарықтық парадигмаларды өзгертеді" дейді (Gumsheimer et al. 2016) "дағдарыстан кейінгі қаржы секторының тағдырын қалпына келтіру" үшін (Grewe & Bosch, 2016) және бұл барлық салаларда "бизнестің келесі онжылдығын өзгерту ықтималдығы жоғары" технология деп болжануда (Tapscott & Tapscott, 2016a). Блокчейндер биткоинмен және Ethereum және Ripple сияқты басқа криптовалюталармен байланысты. Алайда, криптовалюталар блокчейндердің жанама өнімі болып табылатындығын және блокчейндер кез-келген криптовалютадан тәуелсіз өмір сүре алатындығын атап өткен жөн (Гринспан, 2015). Бұл революциялық технология 21 ғасырдағы ұлттық басқаруға, институционалдық функцияларға, іскерлік операцияларға, білімге және күнделікті өмірімізге айтарлықтай әсер етеді. Аққу (2015) блокчейн қосымшаларын әзірлеуді үш кезеңге бөлуге болатындығын көрсетті; Блокчейн 1.0, 2.0 және 3.0. Blockchain 1.0-бұл қолма-қол ақшамен тең-теңімен төлем жүйесі ретінде криптовалюталарды енгізу. Blockchain2.0 - Бұл қарапайым ақша операцияларына, соның ішінде акцияларға, облигацияларға, несиелерге, зияткерлік меншікке және ақылды байланыстарға қарағанда кеңірек блокчейн қосымшалары. Blockchain 3.0 валюта, қаржы және нарықтардан тыс, мысалы, мемлекеттік басқару, денсаулық сақтау, ғылым, сауаттылық, мәдениет және өнер салаларында блокчейн қосымшаларын әзірлейді. Бұрын айтылған қағидаға сәйкес, блокчейннің қазіргі қолданылуы

әлі де 1.0 және 2.0 сатысында. Көптеген адамдар" блокчейн " терминін білмейді, блокчейн технологиясының ықтимал қосымшаларын айтпағанда. Осыған байланысты зерттеу келесі нақты мақсаттарға жету үшін жүргізіледі[2].

Блокчейннің артықшылығы:

Орталықсыздандыру. Желіге қатысушылар тең құқықтарға ие және делдеалдардың ұатысуынсыз бір-бірімен тікелей ақпарат алмасуға қабілетті. Шектелген кілттердің қолданылуына байланысты бұзушылардың хакерлік шабуыл немесе ақпаратты блоктарға ауыстыру ықтималдығы алынып тасталады. Блокчейннің блоктары пайдаланушылар үшін ашық және операцияларды тексеру оңай. Блокчейн – бұл қаржы секторында ғана емес, басқа салаларда да қолдануға болатын ерекше технология. Жоғары жылдамдық бойынша блокчейн технологиясының мүмкіндіктері транзакция уақытын бір минутқа дейін қысқартуы мүмкін. Төмен төлемдер бойынша комиссиялық төлемдердің болмауына байланысты транзакция үшін төлемдер минималды болып табылады.

Блокчейннің кемшілігі:

Қайтымсыздық. Егер қате жасалған болса, сіз операциядан бас тарта алмайсыз. Шабуыл жасау қаупі. Егер Bitcoin тізбегінің 51 пайызы бір пайдаланушыға тиесілі болса, желінің тұтастығына нұқсан келуі мүмкін. Мастабтылық бойынша блокчейн ағымдағы блок өлшемінде жүйе 1 секунд ішінде жеті операцияны өңдейді. Пайдаланушылар өскен сайын бұл көрсеткіш аз болады. Криптографиялық қорғалған блоктағы транзакциялардың жарамдылығы кейіннен желідегі шахтерлердің ұжымдық есептік қуаты арқылы тексеріледі және расталады.

Жеке негізде бұл кеншілер компьютерлер болып табылады, олар күрделі математикалық есептерді шешу үшін өздерінің GPU және / немесе CPU циклдарын қолдана отырып конфигурацияланып, шешім табылғанша блок деректерін хэширлеу алгоритмі арқылы өткізеді. Шешілгеннен кейін блок және оның барлық тиісті операциялары заңды деп тексерілді. Сыйақылар (Bitcoin, осы мысалда, бірақ Litecoin немесе кейбір басқа валюталар) табысты хэшке үлес қосқан компьютер немесе компьютерлер арасында бөлінеді.

Пайдаланылған әдебиеттер тізімі

1 Mukta Sh.N. Blockchain Technology: An Overview // Conference: Blockchain technology. At: Chittagong, 2023. – P. 1-26. – https://www.researchgate.net/publication/

2 Liu H., Zhang B., Huang J., Tian K., Shen Ch. Prospects of Blockchain Technology in China’s Industrial Hemp Industry // Journal of Natural Fibers, 2022. – P. 1-15. - https://www.researchgate.net/publication/366611313