N E W S
OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
SERIES OF SOCIAL AND HUMAN SCIENCES
ISSN 2224-5294
Volume 4, Number 302 (2015), 136 – 141

ECONOMIC INCENTIVES AND TRANSACTION ALGORITHMS IN BITCOIN PAYMENT SYSTEM

Seitim A.
seitima@mail.ru

Turan University, Almaty, Republic of Kazakhstan

Key words: Bitcoin, payment system, crypto currency, transaction algorithms, peering method

Abstract. Paper is about an analyze of Bitcoin crypto currency platform that is widely used in Internet. Direct payments online through peer-to-peer method, the sender and recipient can be linked without the help of financial institutions. Peer-to-peer network is a distributed application architecture that partitions tasks or work loads between peers, where all of the items (peers) are working at one level. Each peer is stored into system of equaly as a client and as a server. In contrast to the monocentralized client-server system the decentralized peer to peer system is more stable and secure. There are no strong conditions for quantity and combination of peers. Any combination and size of online peers can provide the work of Bitcoin system. In the research new payment system internal processes of planning, transaction algorithm and economic incentives were analyzed.

УДК 336.722.117.3

БИТКОИН ТӨЛЕМ ЖҮЙЕСІНІҢ ЭКОНОМИКАЛЫҚ ЫНТАЛАНДЫРУ МЕХАНИЗМІ МЕН ТРАНЗАКЦИЯЛАР АЛГОРИТМІНЕ АРНАЛҒАН ТАЛДАУ ЖҰМЫСЫ

Сейтім А.
Тұран университеті, Алматы қаласы, Қазақстан Республикасы

Түйін сөздер: Биткоин, төлем жүйесі, крипто валюта, транзакциялар алгоритмі, пирингтік әдіс.

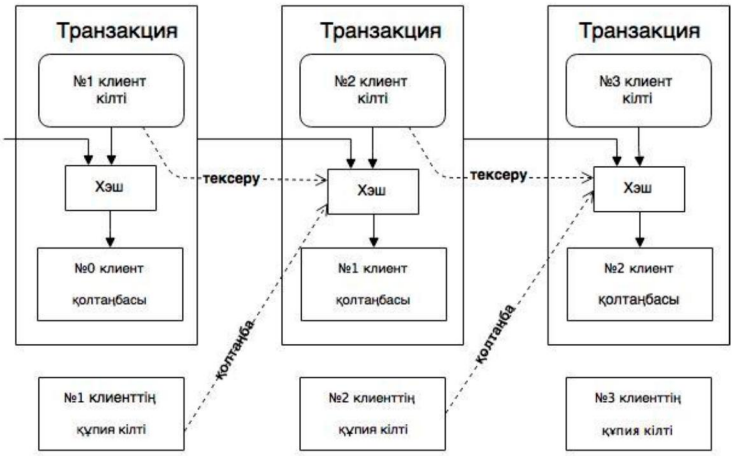
Аннотация. Зерттеуде интернет желісінде кең қолданысқа ие болған Биткоин криптовалютасының платформасына талдау жасалған. Пирингтік әдіс арқылы онлайн төлемдерді тікелей, жіберуші мен қабылдаушыны еш қаржы институтарының көмегінсіз байланыстыруға болады. Пирингтік, яғни тегіс тармақты әдіс дегеніміз (Авторлық анықтама) – (Peer-to-peer network) компьютерлік жүйе ішіндегі барлық тармақтар (пиралар) бір деңгейде жұмыс істейтін әдісті атайды). Қарастырылып отырған жүйеде тармақтардың өзара теңдігі сақталып, әр тармақ клиенттің де, сервердің де функцияларын атқарады. Моно-центрлі клиент-сервер жүйесінен децентрлі тегіс тармақты жүйенің басты айырмашылығы оның жұмыс барысының тұрақтылығында. Жүйенің жұмыс барысын қамтамассыз ету үшін пиралардың мөлшері мен комбинациясына тағылатын міндетемелер болмайды. Олардың кез-келген мөлшері мен үйлесімінде жүйенің жұмыс барысын сақталып тұрады. Биткоин жүйесінің протоколы негізінде жаңа төлем жүйесінің программалық ішкі құрылысы мен экономикалық ынталандыру процесстері қарастырылған.

Бүгінгі таңда электронды ақша аударымдар саласында барлық транзакциялар түрлі төлем жүйелерінің көмегімен, олардың делдалдық қызметтімен жүге асырылып жатыр. Қаржы институттары сол атқарған қызметтері үшін белгілі мөлшердегі сый ақы алып, талабыңызды орындайды. ал клиент өз тарапынан оған өз қаражаттары мен төлқұжаттық мәдіметтерін сеніп тапсыруы тиіс. Осы жерде бірнеше мәселелер көтеріліп жатыр. Қаржы интитуттарының құзырындағы мәліметтер мен тапсырылған қаражаттардың қауіпсіздігі, олардың шоттарды тікелей басқаруы, яғни шоттардың өшіріліп, не болмаса блокталуы үшінші жақтың шешімен жүзеге асырылуы. Және де қаражаттардың шынайы деп қабылдануы, олардың бір реттен артық қолданылмауы төлем жүйесін іске асыратын компаниялардыың қол астында болуы. Зерттеуде біз осы және тағы басқа мәселердің шешу жолдарын ұсынатын, интернет желісінде қарқынды дамып келе жатқан криптография негізінде құрылған Биткоин жүйесіне талдау жасадық. Биткоин протоколы [1] негізінде оның ішкі құрылысына талдай жұмыстарын жасадық. Элетронды жүйеге

қолма-қол төлеу әдісіндегідей, тікелей екі жақты, еш делдалдардға сенім артпай, байланыстыратын криптографияға негізделген әдіс қажет. Транзакциялардың өзгертілмейтін қатаңдығы қабылдаушы жаққа, ал қалыпты тапсырыс беру мехнизмі қаражат жіберушілерге өз ыңғайлығын көрсетер еді. Бұл ғылыми жұмыста Биткоин жүйесінің қайтармалы төлемдер проблемасын шештін әдісін талдаймыз. Пирингтік принцип арқылы бір деңгейлі жүйеде өзара бөлінген уақыт белгілерінің сервері мәліметтердің өңделгенін дәлелдеп, транзакциялардың хронологиясын сақтайды. Жалған түйіндердің қарамағындағы массивке қарағанда адал түйіндердің массивінің көлемі асып тұрғанша, системаның қауіпсіз жұмыс істеуі сақталып тұрады.

Онлайн төлемдер жасалғанда электронды қолтаңбаның маңызы зор. Оның сақтығы ерекше қатаңдықты қажет етеді. Электронды қолтаңба қолданысы бұл жерде көп мәселелелерді шешеді, дегенмен үшінші жақтың жүйені бағдарлауы, ондағы қаражаттың қайта қолданылуын бақылауы, тегі жүйенің бұл жерде осалдығын көрсетіп тұрады. Биткоин жүйесінде пирингтік әдіс арқылы үшінші жаққа мәжбүрлі сенім арту проблемасы шешілді. Жүйедегі әр транзакция уақытысымен хэштеліп тізбекке енеді. Хэштелу дегеніміз (Авторлық анықтама) – енгізілген еркін ұзындықты мәліметтер массивінің белгілі алгоритм арқылы ұзындығы тиянақты биттік жол ретінде түрленуін атайды. Түрлену хэш-функциясы, ал одан шыққан нәтижесін хэш деп атайды. Енді хэштелген транзакцияларға оралатын болсақ олар орындалу дәлелі негізінде аталған тізбектен орын алады. Орындалу дәлелі (Proof-of-Work) деп жүйенің артық қызметтерден қорғау принципін атайды. Принцип бойынша жүйе тарапынан түйіндерге ұзақ уақытты қажет ететін жұмысқа сұраныс беріліп, нәтижесі оңай әрі тез арада тексерілетін болады. Яғни ассиметриялы уақыт шығыны орындалады: сұранысты қанағаттардыратын есептеуді жүргізуге жұмсалатын ұзақ мерзім мен оның нәтижесін тексерілуінің оңай әрі тездігі. Тізбекке қосымша информация енгізу үшін, тізбек бастапқы транзакциядан қайта басталуы тиіс. Сонымен жүйе осындай орындалған жұмыс дәлелі негізінде өзінің қатаңдығын сақтайды. Ең ұзын тізбек бұл жерде реттелген деректердің дәлелі болып әрі, жүйедегі ең үлкен есептік жұмыс атқарған массивтен шыққан тізбек болып табылады. Осы ең үлкен есептік массив шынайы түйіндердің қолында, яғни жұмыс барысын бұзуға бағытталмаған түйіндердің қолында болса, олардың тізбегі ең ұзын болып жалғасып, сонымен қоса жүйеде жалған тізбектер, яғни жалған информациямен залалданған тізбектер болып жатса ондай жалған тізбектерден жылдамдығы мен ұзындығы әрқашан асып тұратын болады. Жүйенің талаптары өте қарапайым. Транзакциялардың жіберіп отырған мәліметтері «үнемділік» принципі арқылы таралады. Түйіндер тізбекті іздеу барысында қосылған жерінен ажырап қайта басқа жүйеге қосыла алады. Ең ұзын тізбекке қосылу арқылы түйіндер қосылуға дейінгі өңделген мәліметердің жүйеде жоғалып кетпеуінен сақтайды.

Жүйе электронды тиынды компютерлік қолтаңбалардың тізбегі деп анықтайды. Жүйенің тұтынушысы, оны клиент деп атайық, тиынды жіберу үшін алдыңғы транзакцияның хэшін және келесі иеленушінің, яғни келесі клиенттің ашық кілтін өзінің компьютерлік қолтаңбасымен белгілейді. Бұл информация тиынмен бірге жіберіледі (Сурет №1).

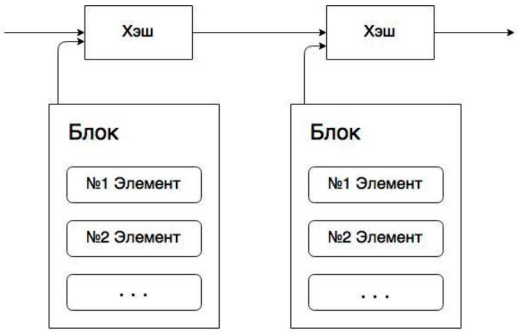


Сурет №1. Транзакцияның ішкі құрылысы мен тізбекке ену механизмі.

Келесі клиент оған жіберілген тиынның қайталанып қолданылмағанын тексере алмайды. Әдетте бұл проблема бақылаушы орталық жақтың әр транзакцияны тексеруімен шешіледі. Тиын эмиссия орталығына қайтарылып, оның орнына жаңа тиын шығарылады, және де тек тікелей эмиссия орталығынынан щыққан тиындар ғана қайта қолданылмағандығын дәлелдейді. Сөйтіп транзакциядағы тиындар тексеру алгоритмінен өтеді. Бұл жағдайдың да өз осал жері бар: жүйенің жұмыс барысы сол эмиссия орталығын бақылайтын органға толығымен тәуелді болып тұр, өйткені ол банк сияқты әр транзакцияны өткізіп, өз бақылауында ұстап тұрады.

Ізделініп жатқан шешім бір тиынның қайта қолданылмауын үшінші жақтың қатысуынсыз жүзеге асырылуында. Бұл үшін, шынайы тиынды анықтау үшін, оның ең алғашқы транзыкциясын рас деп аламыз (өйткені әр тиын тек бірінші рет қолданылған кезінде ғана тексеруді қажет етпейді), одан кейін жасалған транзакцияларды елемейміз. Орындалған транзакцияны анықтау үшін сол тиынмен жасалған барлық транзакцияларды тексеру керек болып тұр. Дәстүрлі эмиссия жүесінде барлық транзакциялар мен олардың реті сол органның қарамағында болады. Ал Биткоин жүйесінде үшінші жаққа сенім артудың орнына, барлық транзакцияларды ашық түрде жариялап [2] және де жүйедегі қатысушыларды транзакциялардың хрологиясын өзара сақтайтын системасы ұсынылады. Болашақ қаражат иеленушіге бұл жерде бар қажеті көпшілік түйіндердің өзара келісімі, яғни сол уақытта жасалған бар транзакциялардың ішінен аталған транзакцияны бірінші деп тану.

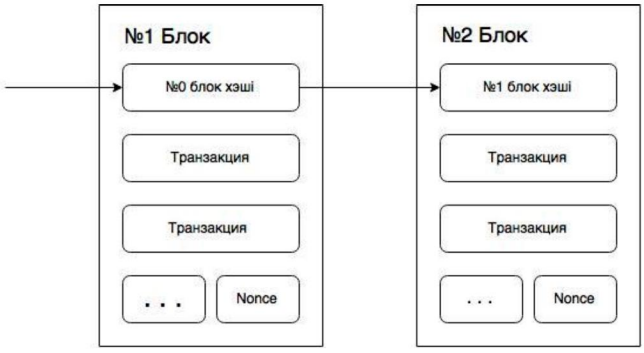
Биткоин программасының ұсынып отырған жүйесі уақыт белгілер серверіне негізделген. Уақыт белгілер Сервері деп блоктарды уақыт белгілерімен хэштеп, оларды газет бетіне шығарғандай, немесе Usenet постына шығарғандай [3-6] ашық түрде жариялайтын платформаны атайды. Уақыт белгісі белгілі бір мәліметтің белгілі бір уақытта орын алғанын дәлелдейді. Бұл шарт хэш-блогына ену үшін қажет. Хэш-блогындағы әр Уақыт белгісі алдыңғысына хронологиясын сақтап жалғасып, реттелген тізбекті құрайды: әр қосылған түйінмен тізбек нығая түседі (Сурет №2).



Сурет №2. Хэш-блогындағы уақыт белгісінің хронологиялы түрде жалғасып ұзаруы.

Уақыт белгілер серверін пиринг негізінде қолдану үшін, жоғарыда айтылғандай газет, не болмаса Usenet постына қарағанда, атқарылған жұмыс дәлелімен жүретін Adam Back-тің Hashcash системасындай [7] жүйе қажет. Дәлелдеу жұмысының мақсаты, SHA-256-дегідей, хэштелген мәліметтердің ішінен белгілі бір нөлдік биттерден басталатын хэшті табу болып тұр. Ол үшін, экпоненционалды түрде нөлдік биттер санына сәйкес көлемдегі тексерулер жасалу қажет, ал табылған мәліметті тексеру үшін бір ғана хэш қажет. Жоғарыда айтылған жұмыс шығыны ассиметриялы болып келеді.

Биткоин жүйесінің ұсынысы бойынша сервердегі атқарылған жұмыс дәлелі негізінде блоктағы ізделінген хэш табылғанша тізбек Nonce мәліметіне жалғаса береді (Сурет №3). Ізделінген хэш табылған соң блок өзгертілмейді. Өзгерістер енгізу үшін, ақарылған жұмыс қайта ең басынан басталуы тиіс, және де одан кейнгі барлық блоктардың да қайта есептелуі қажет. Бұл шарт мәліметтердің көшірме түрінің пайда болуының алдын алу үшін ұйғарылған.



Сурет №3. Блоктың ішкі құрылсы мен қажетті хэшті іздеу барысы.

Атқарылған жұмыстың дәлелдену принципі сонымен қатар көпшіліктің шешім қабылдау проблемасын шешеді. Егер бір IP-адресске бір дауыс тиесілі болса, жүйенің жұмыс барысы ең көп адресстерді бақылайтын жақтың қолында қалып кетеді. Сондықтан, бұл проблеманың алдын алу үшін, «бір процессерден – бір дауыс» шарты енгізілген. Сонда көпшіліктің шешімін жүйедегі ең ұзын тізбек көрсететін болады. Өйткені бұл тізбек ең көп процессерлердің есептеуінен шыққан, яғни атқарылған жұмыс дәлелімен құпталған тізбек болып танылады. Неғұрлым Процессерлердің көпшілігі адал болса, соғұрлым тізбек тез жалғасып (ұзарып) қалған тізбектерден озады. Блоктарға өзгеріс енгізу үшін, ондай жұмыс барысын шабуылдаушы, яғни хакерлік процессерлер жұмысты ең басынан тізбектің соңғы блогына дейін дейін қайта атқарып, жаңа блоктарымен қоса есептегендегі адал тізбектердің ұзындығынан асуы түсуі қажет. Қарастырылған жағдайдың орын алуының мүмкіндігі блоктар санына экспоненциалды түрде кері пропорционал. Кейнгі бөлімдерде бұл заңдылық толығырақ қарастырылатын болады.

Процессорлер мен жүйедегі түйіндер жұмысының қарқыны шамадан тыс асып кетпеуі мақсатында, атқарылған жұмыстың дәлелдену жылдамдығы сағатына пайда болған блоктардың санына тура пропорционал болады. Демек, хэштелу принципі қиындатылады. Жылдамдық көбейе берген сайын, хэштелу қиындай түседі. Сонда блоктардың гернациясы бір келкі жылдамдықпен өтеді. Яғни бұл шарттың мақсаты жүйедегі пайда болған жаңа тиындардың санын қолданушылар қарқынына тура пропорционалды ету. Қолданыс арта бере – желідегі тиындардың генерациялану жылдамдығы кеми түседі. Сонда жүйедегі тиындардың құнсыздану проблемасы, экономикалық тұрғыдан алғанда, криптовалютаның инфляциялану мәселесі шешіледі.

Биткоин системасының процесстік құрылысымен танысамыз. Транзакциялардың орындалуының алгоритмінің механизмі келесі қадамдардан тұрады:

1) Жаңа транзакциялар барлық түйіндерге тарайды
2) Әр түйін жаңа транзакцияны блокқа жинайды
3) Әр түйін қиындатылған хэш блогын қарастырады (іздейді)
4) Хэш табылысымен, бұл блок жүйедегі қалған түйіндерге жіберіледі
5) Блоктағы барлық транзакциялар расталған болса, онда қаражаттың қайта жұмсалуы орын алмаса, түйіндер ол блокты шынайы деп қабылдайды
6) Алдыңғы блоктың расталуымен, қабылданған блок хэшінің негізінде түйіндер жаңа блокпен жұмыс істей бастайды.

Түйіндер тек ең ұзын тізбекті қабылдап, оның үстіндегі жұмысты жалғастырады. Егер екі түйін бір уақыт аралығында келесі блоктың екі түрлі нұсқасын ұсынған болса, қалған түйіндер олардың ең ұзыны анықталғанша екеуімен де жұмысын жалғастырады. Ең ұзыны табылысымен, барлығы сол ұзын тізбекпен жұмыс істеуге көшеді.

Жаңа транзакциялардың барлық түйіндерге жетуі міндетті емес. Блокқа ену үшін оған көпшілік түйіндердің растауы жеткілікті. Блоктарды тарату барысында мәліметтердің жоғалып кетпеуі үшін тағы шарт ойластырылған. Түйін бір блокты қабылдамай кеткен жағдайда, келесі блокты қабылдар алдында ол арада қалып кеткен блокты талап ететіп, оны жоғалған блок деп танып, іске қосады.

Жүйенің тұрақты әрі адал түрде жұмысын сақтау үшін программада экономикалық ынталандыру шарты енгізілді. Шарт бойынша ізделінген хэш тапқаны үшін сол хэш табылған блоктпен жұмыс атқарған бар түйіндерге марапат ретінде биткоиндар берілетін болады. Түйіндер саны ұлғайған сайын сыйақы мөлшері азаяды. Бұл принцип жүйенің құнсықданып кетпеуі үшін ұғарылған шарт.

Платформа негізіндегі блоктағы алғашқы транзакция – маңызы бөлек, бастаушы транзакция болып табылады. Ол транзакция – жаңа тиынды шығарушы транзакция. Тиын блок инициаторының иелігіне түседі. Бұл механизм орталық эмиссия органынсыз, адал түйіндердің жұмысын ынталандыру мақсатында, тиындардың айналымға реттеліп енуін ұйымдастырады. Алтын өндірісінде жұмсалған ресурстар сияқты, бұндай реттелген эмиссияның да қажет ететін ресурстары болады. Тиындардың айналымға бір қалыпты енуі алтынннның айналымға енуіне ұқсайды. Алтын өндірушілер кен іздерде өз адами, қаражаттық және уақыт ресурстарын жұмсаса, Биткоин программасы аналогия бойынша компьтердің процессорлық есептеуге жұмсалған уақыты мен электр қуатын жұмсайды.

Ынталандырудың тағы бір әдісі транзакцияны өткізу үшін алынатын комиссиясы да бола алады. Егер жіберілген тиын мөлшері қабылданған мөлшерден кем болса, арадағы қалдық комиссия болып, бар блоктың жұмысынан пайда болған тиындарға қосылады. Тиындар жиыны программамен орнатылған 21 миллион данаға тең шегіне жеткенде, жұмыс барысын ынталандыратын осы комиссиялар болады.

Ынталандырудың мақсаты – жүйенің тұрақыт түзу жымысын сақтау үшін адал түйіндердің санын арттыру. Алаяқтықты көздеген түйіндер жүйені өз мақсаттарында, яғни төленген тиындарды ұрлау, не болмаса транзакцияларды жаңа тиындар генерациясына жіберу мақсатында қолданғысы келсе, қалған, адал түйіндердің процессорлық қуатынан артық қуат жұмсауы қажет. Бұл мүмкіндік бола тұра, барлық түйіндерге ең пайдалы әрі тиімдісі адал жұмыс атқару болып тұр. Өйткені, бұл жүйеде адал жолмен тиын генерациясы тиімдірек әрі тез жүзеге асырылады, ал жүйені бұзуға бағытталған хакерлік әркеттер жаңа тиындарды табу жолында жетістікке жетпейді, яғни ештеңе ұтпайды. Жалған түйіндер әрекеті көп шығынды әрі ұзақ уақытты қажет етеді. Сондықтан Биткоин жүйесінде хакерлік шаралар уақыт және жұмсалған энергия тұрғысынан тиімсіз болып табылады.

Интернет-коммерцияда орын алатын төлемдердер бүгінгі таңда қаржы институттарының делдалдық қызметтерінің көмегімен жүзеге асырылып отыр. Бұл делдалдық өзіне жүктелген тапсырманы толығымен орындап жатыр, дегенмен сеніп тапсырылған мәліметтердің сақталуы үшінші жақтың қарамағында қалу проблемасы тағы қалып отыр. Бұл жүйенінің бірден бір осалдығын көрсетеді. Қаржы институттарының қарамағында қалып отыратын тағы бір жағдай, ол транзакциялардың қайтарылу мүмкіндігі. Қайтарылмау принципі транзакцияны өткізуде қосымша сервистерді қажет етеді, ал бұл жағдай комиссияның құнын тағы арттырады. Мәліметтердің өзгеру мүмкіндігі қаражат қабылдаушы жақтың сенім артуын қажет етеді. Операцияның орындалуына сенімді болу үшін қабылдаушы жақ қаражат жіберушіден қосымша мәліметтерді талап етуге тура келеді. Дегенмен бұндай жүйедегі жалған транзакциялардың, яғни алаяқтықтың орын алу мүмкіндігі тағы бар. Бұл мәселенің қаржы операцияларында орын алуы қалыпты жағдай болып отыр. Комисияның алынбауынан, қаржы операциясының қайтарылуынан сақтандыратын қолма-қол төлеу әдісі кәзіргі таңда дәстурлі жүйлер ішінде жоқ. Биткоин жүйесі бұл жерде аталған проблемалардың тиімді шешімін ұсынды. Үшінші жақтың қатысуынсыз, тікелеу тегіс тармақты принцип арқылы сенім арту шарты жойылды. Одан шығатын қосымша қызмет көрсету сервистерінің болмауы комиссияларды жойды, ал транзакциялардың қайталанып орындалмауы мәліметтердің өзгертілу қаупін, хакерлік шабуылдардың алдын алды.

ӘДЕБИЕТ

[1] Биткоин – электронды-пирингтік төлем жүйесі // Satoshi Nakamoto // www.bitcoin.org, 2008.

[2] В. Дай // «b-money», http://www.weidai.com/bmoney.txt, 1998.

[3] Г. Массиас, Х. Авила, Дж. Куискуатер // «Минималды шарттарды қажет ететін уақыт белгілерінің қауіпсіз қызметі» // *Информатика теориясына арналған 20-шы Симпозиум, Бенилюкс*, Мамыр 1999.

[4] С. Хабер, В. Сторнетта // «Сандық құжаттарды уақыт шартымен белгілеу амалдары» // *Криптология Журналы*, № 3 (2), 1991, бет. 99-111.

[5] Д. Байер, С. Хабер, В. Сторнетта, D. Bayer, S. Haber, W.S. Stornetta, // «Сандық уақыт белгілер тиімділігін мен сенімділігін арттыру амалдары» // *Sequences II: Коммуникация, Қауіпсіщдік және компьютер ғылымдары,* 1993, бет. 329-334.

[6] С. Хабер, В. Сторнетта // «Биттік жолдар үшін қауіпсіз атаулар» // *4-ші ЕТА Конференциясы: Компьютер және коммуникациялық қауіпсіздік*, Сәуір 1997, бет. 28-35.

[7] А. Бак // «Хэшкэш: қарсы шара қызметінен бас тарту» // http://www.hashcash.org/papers/hashcash.pdf, 2002.

REFERENCES

[1] Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto, www.bitcoin.org, 2008 (Eng)

[2] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998. (Eng)

[3] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999. (Eng)

[4] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991. (Eng)

[5] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping", In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993. (Eng)

[6] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997. (Eng)

[7] Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002. (Eng)

ЭКОНОМИЧЕСКАЯ МОТИВАЦИЯ И АЛГОРИТМ ТРАНЗАКЦИИ ПЛАТЕЖНОЙ СИСТЕМЫ БИТКОИН

Сейтим Айганым
Университет Туран, г. Алматы, Республика Казахстан

Ключевые слова: биткоин, платежная система, криптовалюта, алгоритм транзакций, пиринговый метод.

Аннотация. В работе рассмотрен протокол платежной системы Биткоин. В данный момент эта система пользуется широкой популярностью в Интернет платежах. С помощью пиринговых сетей распространения данных стало возможным связывать отправителя и получателя, минуя посредников. Пиринговая сеть, иначе говоря, одноранговая сеть, это компьютерная сеть, где все участники-узлы (пиры) равны между собой и работают на одной платформе. В рассматриваемой системе платежей узлы, сохраняя равноправие, являются как клиентами, так и сервером сети. Главное отличие такой системы от моноцентровой классической - в устойчивости работы системы. Сеть поддерживается любым положительным количеством и комбинацией подключенных узлов. В данной работе также рассмотрены внутренние механизмы осуществления транзакции и способы материальной мотивации участников сети Биткоин.

Поступила 15.07.2015 г.