ՀՏԴ 336.74

ԿՐԻՊՏՈԱՐԺՈՒԹԱՅԻՆ ՀԱՄԱԿԱՐԳԻ ՀԱՍԿԱՑՈՒԹԱՅԻՆ ՇՐՋԱՆԱԿԻ ԶԱՐԳԱՑՄԱՆ ՄՈՏԵՑՈՒՄՆԵՐԸ

ՌՈԲԵՐՏ ԽԱՉԱՏՐՅԱՆ, ՍԱՄՎԵԼ ՀՈՎՀԱՆՆԻՍՅԱՆ, ԱՐՓԻՆԵ ԳԵՎՈՐԳՅԱՆ

Վ. Բրյուսովի անվան պետական համալսարան

Ժամանակակից ֆիզիկական և թվային տիրույթներում կրիպտոարժութային համակարգի ներդրման փորձերը նպաստում են տնտեսական զարգացման հնարավորությունների բացահայտմանը, ինչպես նաև մրցակցային առավելության ձեռքբերմանը: Հոդվածն անդրադառնում է «կրիպտոարժութային համակարգի» հասկացության ընդհանուր հայեցակարգային շրջանակին, արտաքին և ներքին գործոնների վերլուծությանը՝ ներկայացնելով տվյալ ոլորտի պատմական ակնարկը, հիմնական դրույթները, որոնք ապահովում են ուսումնասիրության արդիականությունը:

Բանալի բառեր. կրիպտոարժույթ, կրիպտոարժութային համակարգ, բիթքոին, բլոկչեյն, թոքեն, կրիպտոհանքափոր (մայներ), գրանցամատյան, արձանագրություն, մասնակիցը մասնակցին ցանց:

Ներկայում կրիպտոարժույթները լայն տարածում ունեն միջազգային շուկաներում: Սա մեծապես պայմանավորված է տեղեկատվական տեխնոլոգիաների շարունակական զարգացմամբ և ֆիզիկական սահմանների աստիճանական ձևափոխմամբ: Կրիպտոարժութային համակարգը հիմնվում է այնպիսի դինամիկ գործոնների վրա, ինչպիսիք են՝ բլոկչեյն համակարգերի միջոցով փոխադարձ վստահության կառուցակարգերի առկայությունը, պլատֆորմի ռիսկերի նվազեցումը և վերացումը[1], առցանց հարթակների առաջացումը (օրինակ՝ կրիպտոբորսաներ), առցանց վճարումների հարմարավետությունը, գործարքների արագությունը, գործարքների անվտանգությունն ապահովող ժամանակակից տեխնոլոգիաների կիրառումը, գործարքների ապակենտրոնացումը, միջնորդների վերացումն ու միջնորդավճարների էական նվազեցումը:

Նմանաբովանդակ գործոնները հանգեցրել են կրիպտոակտիվների (օրինակ՝ կրիպտոարժույթ՝ էլեկտրոնային փողեր, բլոկչեյն համակարգով գործառվող պայմանագրեր և պահվող տեղեկություն) առաջացմանը և կիրառման լայն տարածմանը: 2008 թ. Սատոշի Նակամոտոն գործառեց

[1] Օգտագործվող ենթակառուցվածքներից կախվածության նվազեցում կամ վերացում (օրինակ՝ վճարման համակարգեր):

ապակենտրոնացված ցանցերի տեխնոլոգիաներ, ինչից հետո կրիպտոարժույթները զբաղեցրեցին իրենց դիրքը շուկայում և սկսեցին օգտագործվել տարբեր նպատակներով թե՛ ֆիզիկական և թե՛ իրավաբանական անձանց կողմից: Ավելին, եթե մեկնարկային շրջանում գոյություն ունեին սահմանափակ քանակությամբ կրիպտոարժույթներ, ապա այժմ առկա են բազմաթիվ տեսակներ: Ըստ www.coinmarketcap.com կայքի՝ ներկայում գոյություն ունի կրիպտոարժույթների մոտ երկու հազար երեք հարյուր հիսուն տեսակ: Ըստ կիրառության՝ ամենատարածվածը, թերևս, դասական բիթքոինն է:

Սույն հոդվածի **նպատակն** է կրիպտոարժույթների վերաբերյալ մասնագիտական գրականության և էլեկտրոնային աղբյուրների ուսումնասիրության արդյունքների հիման վրա վերլուծել կրիպտոարժույթների հասկացութային շրջանակի զարգացումը, բացահայտել կրիպտոարժութային համակարգի առավելությունները, թերությունները, ռիսկերը, հնարավոր զարգացումները, ինչպես նաև հաշվի առնելով ոլորտում հայալեզու մասնագիտական գրականության սակավությունը՝ նպաստել ոլորտային գրականության ստեղծմանը:

Առաջնորդվելով 21-րդ դարի տեղեկատվական և ֆինանսական տեխնոլոգիաների զարգացման միտումներով՝ իրավաբանական և ֆիզիկական անձիք գործարկում են կրիպտոարժութային վճարային համակարգը որպես իրենց ապրանքների գնման և ծառայությունների վճարման միջոց: Այս ընդլայնման հիմնական պատճառը ֆինանսական գործարքներում և միջազգային վճարային համակարգերում բլոկչեյն համակարգի լայն կիրառումն է [1]: Նմանատիպ նորարարական տեխնոլոգիաների ներդրումը կարող է նպաստել, ինչպես առանձին կառույցների, կազմակերպությունների, անհատների, այնպես էլ տնտեսական համակարգի զարգացմանը՝ պայմանավորված փոխադարձ վստահություն ապահովող տեղեկատվական տեխնոլոգիաների ներդրմամբ և կիրառմամբ, գործարքային ծախսերի նվազեցմամբ, ապահով, չմիջնորդավորված վճարային համակարգի գործառմամբ, շահույթի ավելացման հնարավորությունների ստեղծմամբ, միջազգային շուկայում մրցակցային առավելության ձեռքբերմամբ և պահպանմամբ:

Յուրաքանչյուր նորարարության առաջացման հիմքում ընկած է կա՛մ որևէ գործոն, որի հիման վրա ստեղծվում կամ ստեղծվել է տվյալ նորարարությունը, կա՛մ որևէ երևույթի անհրաժեշտությունը հասարակության համար: Այս հարցին անդրադարձել է Մարսել Մորիսն իր «Կրիպտոարժույթներ և Բիթքոին՝ ոլորտի քարտեզագրում» աշխատությունում [2]: Տնտեսագետներն ու հասարակագետները միշտ չէ, որ համակարծիք են այն հարցում, թե ինչպես է փողը դարձել հասարակության ամենօրյա գործարքների անբաժանելի մասը [3], սակայն նման ֆինանսադրամական

համակարգը, այնուամենայնիվ, ապրանքների փոխանակման, արժեքի չափման և պահպանման կարևոր միջոց է [4]: Կառավարության և այլ կառույցների՝ դրամաշրջանառության ոլորտային քաղաքականությունները խիստ սահմանափակումներ և կանոնակարգավորումներ են առաջադրել, այդ թվում, թե ինչպես են փողի միավորները (օրինակ՝ դրամանիշները) թողարկվում, շրջանառվում և փոխակերպվում այլ արժույթների: Այդ սահմանափակումների կիրառման համապատասխանությունն ապահովելու համար անհրաժեշտ է, որ կենտրոնական կառույցները կարգավորեն և վերահսկեն դրամաշրջանառության համակարգը: Արժույթների համակարգերում այդ կենտրոնական հաստատությունները կենտրոնական բանկերն են: 2007-2008 թթ. ֆինանսական ճգնաժամի արդյունքում ֆինանսական հաստատությունների նկատմամբ վստահությունը նվազեց, և մարդիկ ամբողջ աշխարհում սկսեցին կորցնել իրենց վստահությունը դեպի կենտրոնացված ֆինանսական հաստատությունները [5]: Այնուհետև ապակենտրոնացված, այլընտրանքային արժութային համակարգի գործառման անհրաժեշտություն առաջացավ [6], որի արդյունքում ստեղծվեցին կրիպտոարժույթները՝ ապակենտրոնացված թվային արժութային սխեմաները՝ հիմնված մասնակիցը մասնակցին (peer-to-peer/P2P) ցանցի և գաղտնագրային (կրիպտոգրաֆիկ) գործիքների վրա: Կրիպտոարժութային համակարգի օգտատերերը կարող են վիրտուալ գումար փոխանցել այլ օգտատերերին և այդպիսով վաճառել կամ գնել ապրանքներ ու մատուցել ծառայություններ: Բիթքոինը (Bitcoin BTC) կրիպտոարժույթների ամենահայտնի և ամենամեծ շրջանառություն ունեցող օրինակն է: Կրիպտոարժույթները, հատկապես բիթքոինը, մեծ ուշադրություն են գրավել գործնականում: Մի կողմից, կրիպտոարժույթներն ունենալով ցածր միջնորդավճարներ դիտարկվում են որպես բանկերի և վճարային քարտերի գործուն այլընտրանք [7]: Մյուս կողմից, պետական կառույցները և կենտրոնական մարմինները զգուշացնում են, որ կրիպտոարժույթները փողերի լվացման և անօրինական ապրանքների (օրինակ՝ թմրանյութ, ապօրինի զինամթերք) առևտրի իրականացման համար հեշտ գործիք են [8]: Այսպիսով, կրիպտոարժույթները հնարավորություն են տալիս ստեղծել նոր գործարարության (բիզնես) մոդելներ էլեկտրոնային առևտրի և ֆինանսների ոլորտներում՝ հնարավորություն տալով իրականացնել չմիջնորդավորված համաշխարհային փոխանցումներ ցածր ծախսերով [9]: Սակայն մինչ օրս կրիպտոարժույթների ուսումնասիրությունը հատուկ ուշադրություն չի գրավել միջգիտակարգային ոլորտներ ուսումնասիրող հետազոտողների շրջանում, հետևաբար առկա է ավելի խորը քննարկման անհրաժեշտություն [2, p. 2]:

1997 թ. Ադամ Բակովն առաջին անգամ կիրառեց HashCash տեխնոլոգիան, որը հնարավորություն էր տալիս դիմակայել DDoS-հարձակումներին[1], պահպանել ֆինանսական պաշարները և ապակենտրոնացված համակարգի աշխատանքը: Այդ տեխնոլոգիան հետագայում դարձավ բլոկչեյն համակարգի հենքերից մեկը: Այսպիսով, 1998թ. HashCash տեխնոլոգիայի ալգորիթմի հիման վրա Նիկ Սաբոն և Վեյ Դեյը մեկմեկու անտեղյակ, սակայն միաժամանակ, ստեղծում են B-money և Bit-Gold թվային ծրագրերը [10]: Նրանք հիմնվում էին գնաճի կառավարման համար անհրաժեշտ ապակենտրոնացման համակարգերի վրա, որոնք ներկայիս կրիպտոարժութային համակարգի նախատիպերն էին: Ի վերջո այս ամենի հիմքում ստեղծվեց մի տեխնոլոգիա, որը միավորեց իր մեջ այնպիսի հատկանիշներ, ինչպիսիք են՝ անանունությունը, անվտանգությունը, ինչպես նաև անկախությունը:

2008 թ. Սատոշի Նակամոտոն աշխարհին ներկայացրեց ապակենտրոնացված ցանցերի տեխնոլոգիան՝ բլոկչեյնը, ապա վիրտուալ արժույթի ծրագիրը, որը գործառվում է այս տեխնոլոգիայի հիման վրա [10, p. 2]: 2009 թ. հոկտեմբերի 5-ին հաստատվեց քոինի (coin՝ մետաղադրամ) նախնական արժեքը: Առաջին առևտրային փոխանակումը տեղի ունեցավ New Liberty Standart սակարանում (բորսայում), որտեղ ընդամենը 1 դոլարով հնարավոր էր գնել 1,309.03 Bitcoin, ինչից անմիջապես հետո նկատելի դարձան բիթքոինի[2] շարունակական կտրուկ տատանումները:

Կրիպտոարժութային համակարգի առանձնահատկությունները և հնարավոր կիրառությունները հստակեցնելու համար նախևառաջ անհրաժեշտ է հասկանալ կրիպտոարժութային համակարգերի ոլորտում կիրառվող հիմնական հասկացությունները: *Կրիպտոարժույթը բացառապես թվային եղանակով հասանելի ակտիվ է:* Ակնհայտ է, որ այս սահմանումը թերի է և ամբողջությամբ չի ներկայացնում «կրիպտոարժույթ» հասկացությունը, ըստ այդմ՝ ներքոնշյալ ներկայացվում են առավել ընդգրկուն սահմանումներ:

- Կրիպտոարժույթները թվային արժույթների ենթաբազմություն են, որոնք կարող են ունենալ կա՛մ կենտրոնացված ենթակառույցներ, կա՛մ հիմնված լինել ապակենտրոնացված ցանցի վրա [11]: Կենտրոնացված արժութային համակարգում թվային արժույթը թողարկվում է մեկ ենթա-

[1] DDoS attack (անգլերեն՝ Distributed Denial-of-Service Attack): Ցանցին կատարվում են անթիվ հարցումներ, որոնք հնարավոր չէ հաղթահարել և անհրաժեշտ է մերժել սպասարկումը կամ սպասեցնել բավականին երկար ժամանակ:

[2] Բիթքոին թվային կամ վիրտուալ արժույթ, որն իրացվում է մասնակիցը մասնակցին (peer-to-peer/P2P) տեխնոլոգիայի միջոցով և ապահովում վճարումների արագությունը:

կառույցի կողմից, որն երաշխավորում է թվային մետաղադրամների/թոքենների[1] փոխանակումը ֆիատների (իրական փողերի) կամ օգտագործումը թվային ապրանքների գնման և վաճառքի ժամանակ [12]:

• Կրիպտոարժույթները համակարգեր են, որոնք հնարավորություն են տալիս կատարել ապահով վճարում (գործարք) առցանց առևտրային գործունեության շրջանակում, որոնք և կոչվում են վիրտուալ թոքեններ ու ներկայացնում են տվյալների գրանցամատյանը (ledger) համակարգի ներսում [13]:

• Կրիպտոարժույթը վճարման միջոց է, որը կարող է փոխանակվել առցանց ապրանքների և ծառայությունների դիմաց: Մի շարք ընկերություններ թողարկել են իրենց սեփական արժույթները (հաճախ կոչվում են թոքեններ), որոնք կարող են օգտագործվել որպես ապրանքների կամ ծառայությունների դիմաց վճարման միջոց [14]:

• Կրիպտոարժույթը գաղտնագրված թվային ակտիվ է, որը, շնորհիվ իր հիմքում ընկած բլոկչեյն տեխնոլոգիայի, դժվար է կեղծել [15]: Հետևաբար կրիպտոարժույթը թվային ակտիվ է, որը փոխանցումների միջավայրի գործառման համար գաղտնագրման (կոդավորման) տեխնոլոգիա և միջոց է: Այդ միջոցները թույլ են տալիս ապահովել գործարքները[2], որոնք սովորաբար թափանցիկ բնույթ են կրում: Կրիպտոարժութային համակարգի մասնակիցները երաշխավորում են գործարքի հավաստիությունը և արժույթի լրացուցիչ միավորների ստեղծումը: Կրիպտոարժույթները վերահսկվում են կրիպտոարժութային համակարգի մասնակիցների՝ մայներների[3] ընդհանուր հանրության կողմից, որոնք մասնակցություն ունեն գործարքում: Գործարքները մշակվում, հաստատվում ու ստուգվում են մայներների կողմից, և հաջողված գործարքները գրանցվում են հանրային, բաշխված գրանցամատյանում, որը կոչվում է բլոկչեյն [15, p. 3]: Կրիպտոարժույթներն իրացվում են բլոկչեյն տեխնոլոգիայի միջոցով: Ըստ այդմ, անհրաժեշտություն է առաջանում ուսումնասիրել ոլորտում շրջանառվող «բլոկչեյն» հասկացության սահմանումները: Ըստ Սատոշի Նակամոտոյի [10, p. 2] աշխատության՝ բլոկչեյնը գործարքների և տվյալների ապակենտրոնացված կառավարման միջոց է, որը հայտնի է որպես

[1] Թոքենը (token) կրիպտոգրաֆիկ առևտրային ակտիվ կամ գործիք է, որը հաճախ հանդիպում է բլոկչեյն համակարգում:

[2] Բլոկչեյն համակարգում գործարքը փոխանցման, ստուգման, գրանցման և պահպանման ընդհանուր գործընթացների ամբողջությունն է:

[3] Մայնինգը (կրիպտոհանքափորություն) բաշխված և ապակենտրոնացված կոնսենսուսի արձանագրություն է, որը պայմանավորված է մաթեմաթիկական հավասարումների և տվյալների կոդավորմամբ: Մայներ՝ մայնինգը իրականացնող մասնակից:

բիթքոինի՝ գաղտնի արտարժույթի հաջողության հիմքում գտնվող տեխնոլոգիա: Դրա հիմնական նպատակն է ստեղծել ապակենտրոնացված միջավայր, որտեղ որևէ երրորդ կողմ չի վերահսկում գործարքները և տվյալները [16]:

• Բլոկչեյնն ապակենտրոնացված տեխնոլոգիա է՝ հասանելի բազմաթիվ համակարգիչների վրա, որոնք վերահսկում և արձանագրում են գործարքները [14, p. 2]: Բլոկչեյնը թվային, ապակենտրոնացված, հանրային կերպով հասանելի գրանցամատյան է, որտեղ մայնինգով (կրիպտոհանքափորությամբ) զբաղվող անհատները ժամանակագրական հաջորդականությամբ գրանցում են բոլոր գործարքները[1]:

• Բլոկչեյնը թույլ է տալիս պահպանել տվյալները համացանցի միջոցով պաշտպանված, թափանցիկ եղանակով, առանց կենտրոնական կառավարման մարմնի: Հետևաբար բլոկչեյնը տեխնոլոգիա է, որը կոլեկտիվ համաձայնության (կոնսենսուսի) ու գրանցամատյանի բաշխված ապակենտրոնացվածության միջոցով ստեղծում է վստահություն, պատասխանատվություն և թափանցիկություն բոլոր մասնակիցների միջև [17]:

• Բլոկչեյնը տվյալների շտեմարանի ստեղծման տեխնոլոգիա է, որը հիմնվում է համացանցի վրա և լիովին օգտագործում է իր բոլոր առավելությունները, ներառյալ բաց արձանագրությունը, հաշվարկների և կոդավորման ներունակությունը: Բաշխված գործարքների տվյալների շտեմարանում յուրաքանչյուր նոր գործարք գրանցվում է նախորդներից հետո, առանց նախորդ գրառումները փոխելու կամ ոչնչացնելու հնարավորության: Տվյալների շտեմարանը կազմված է ժամանակագրական կարգով, բաշխված է, ստուգված և պաշտպանված է կեղծումներից համակարգի մասնակիցների (հանգույցների) միջև վստահության և համաձայնության (կոնսենսուսի) բաշխվածության միջոցով [17, c. 19]:

• Կրիպտոարժույթներն առաջացել են որպես բլոկչեյնի վրա հիմնված ծրագրերի առաջին սերունդ և որպես թվային արժույթներ, որոնք հիմնված են կրիպտոգրաֆիայի և մասնակիցը մասնակցին ցանցի վրա: Առաջին և ամենատարածված օրինակը բիթքոինն է [18]:

• Բլոկչեյն համակարգում ցանցի պաշտպանությունը և փոխանցումների մշակումն իրականացվում է մայնինգի (կրիպտոհանքափորության) միջոցով: «Կրիպտոարժույթի մայնինգ» նշանակում է գործողություններ, որոնց արդյունքում կրիպտոարժույթի ձեռքբերման գործարքը ստուգվում և գրանցվում է բլոկչեյնում: Մայնինգը հանրային գրանցամատյանում գործարքների ավելացման և վավերացման գործընթացն է [19]:

[1] «Թվային տեխնոլոգիաների զարգացման մասին» ՀՀ օրենքի նախագիծ, Պ-253-05.02.2018-ՖՎ-011/0:

Ոլորտում շրջանառվող վերոնշյալ սահմանումների վերլուծությունից բխում է սահմանման հնարավոր մեկ այլ՝ ընդհանրացված տարբերակ՝ կրիպտոարժույթը ծածկագրված (կոդավորված) թվային ակտիվ է, որն օգտագործվում է որպես գործարքների գրանցման և փոխանցումների իրականացման այլընտրանքային տարբերակ: Այն գոյություն ունի միայն էլեկտրոնային ցանցում թվային տվյալների (վիրտուալ գումար) տեսքով, որոնք պահպանվում են մեկ ընդհանուր ցանցին միացված մեծաքանակ համակարգիչներում: Այսպիսով, ամփոփելով և ամբողջացնելով վերոնշյալ սահմանումները, առաջ է գալիս հետևյալ համապարփակ սահմանումը.

Կրիպտոարժույթը թվային միավոր է, որն իրացվում է ապակենտրոնացված, չմիջնորդավորված, թափանցիկ և կեղծիքները կանխարգելող բլոկչեյն տեխնոլոգիայի միջոցով և նպատակ ունի իրականացնելու փողի գործառույթ:

Կրիպտոարժույթը վճարային համակարգի վիրտուալ՝ էլեկտրոնային այլընտրանքային տարբերակ է, որն իրացվում է բլոկչեյն համակարգում: Կրիպտոարժույթի միավորը քոինն է: Բլոկչեյն համակարգը, իր հերթին լինելով գործարքների դաշտ, պահպանվում է յուրաքանչյուր մասնակցի համակարգչում և ապահովում է տվյալ թվային միավորի անվտանգությունը, ապահովությունը, չմիջնորդավորվածությունը և ապակենտրոնացվածությունը: Հարկ է նշել նաև կրիպտոարժութային համակարգի գաղտնիության մասին, որն ապահովվում է բանալիների առկայությամբ, վեջիններս էլ փոխարինում են օգտատերերի անձնական տվյալները: Բանալիները երկուսն են՝ հանրային (public) և անձնական (private) (հանրայինը կարող է հասանելի դառնալ բոլորին, իսկ անձնականի մասին գիտի միայն օգտատերը): Սա կարելի է նույնականացնել էլեկտրոնային հարթակներում մուտքանվան և գաղտնաբառի հետ. մուտքանունը կարող է հասանելի լինել բոլորին, իսկ գաղտնաբառը հասանելի է միայն օգտատիրոջը համակարգ մուտք գործելու համար:

Գործարքի ամբողջականությունը ստուգվում է ալգորիթմներով և կրիպտոգրաֆիկ մեթոդներով: Գործարքը, որը վավերացնում է գործարքի նախաձեռնողը, ուղարկվում է բլոկչեյն համակարգին միացված հանգույցին (մասնակցին), որը հաստատում է գործարքը և տարածում է այն ցանցում այլ հանգույցների միջև: Այս մասնակիցները ստուգում և տարածում են գործարքն իրենց մասնակիցների միջև, մինչև այն հասանելի կլինի ցանցի բոլոր հանգույցներին [20]: Գործարքները խմբավորված են բլոկերով, որոնք կցվում են գոյություն ունեցող շղթաներին և այդ գործընթացը հայտնի է որպես մայնինգ: Ցանցի աշխատանքն ուղղված է հաջորդ բլոկի վերաբերյալ կոնսենսուսի ձեռքբերմանը, որը ներառվում է բլոկչեյնում

կոնսենսուսի արձանագրության միջոցով: Վերջինս էլ ներառում է ապակենտրոնացված կառավարման ապահովում, իսկություն, ամբողջականություն և համակարգի մասնակիցների միջև վստահություն (BFT) [21]: Դեֆակտո կոնսենսուս արձանագրությունը կատարված գործարքի ապացույցն է [22], որը ստիպում է մայներներին հաշվարկել Hash գործառույթը[1], որն իր հերթին պետք է արդյունավետորեն ստուգելի լինի: Հաշվի առնելով Proof-of-Work-ի հսկայական էներգիայի սպառումը՝ այլ բլոկչեյնները կիրառում են ավելի թեթև տարբերակներ, ինչպիսիք են՝ Proof-of-Stake-ը կամ վերոնշյալ երկուսի համադրությունը [23]: Բլոկչեյնի հիմքում ընկած է համակարգի անվտանգությունը, որը պայմանավորված է գործարքի ողջ գործընթացով, այսինքն՝ Ա անձի կողմից Բ անձին կատարվող փոխանցումը, ստուգվում, գրանցվում և պահպանվում է համակարգի բոլոր մասնակիցների մոտ (առօրյայում յուրաքանչյուր ֆինանսական գործարք կատարվում և գրանցվում է առևտրային բանկերի կամ այլ ֆինանսական հաստատությունների կողմից՝ միջնորդավորված գործողություն), իսկ հաշվի առնելով միլիոնավոր մասնակիցների քանակը, գոյություն չունի այնպիսի ծրագիր կամ մեթոդ, որ կարող է կեղծել կամ կոտրել համակարգը միաժամանակ միլիոնավոր համակարգիչներում: Հետագայում բլոկչեյն համակարգի յուրաքանչյուր մասնակցի մոտ պահպանվում է այն տեղեկատվությունը, որ օրինակ՝ X օրը Y ժամին Ա-ն Բ-ին փոխանցեց Z քանակությամբ բիթքոին (bitcoin), էֆիրիում (ethereum) կամ կրիպտոարժույթի որևէ այլ տեսակ: Այս տեղեկատվությունը պահպանվելու է յուրաքանչյուր մասնակցի մոտ. հետագայում այլ փոխանցումների ժամանակ այս տեղեկատվությանը ավելանալու են այլ փոխանցումների տվյալներ, օրինակ՝ X^N օրը Y^N ժամին Գ-ն Դ-ին փոխանցեց Z^N քանակությամբ բիթքոին: Այսինքն՝ համակարգում պահպանվում է կատարված փոխանցումների, գործարքների բոլոր տվյալները, սակայն այս ամենով հանդերձ համակարգի որևէ մասնակից չի կարող տեսնել մյուս մասնակցի կրիպտոդրամապանակի պարունակությունը: Այսպիսով, փոխանցման գործընթացը թափանցիկ է, սակայն անձնական ակտիվների գաղտնիությունը պահպանվում է՝ տեսանելի չէ երրորդ անձանց, որից էլ բխում է անհատի սեփականության գերակայությունն իր ակտիվների նկատմամբ:

Սույն հոդվածում կրիպտոարժութային համակարգի առանցքային ուսումնասիրության համար անհրաժեշտություն է առաջանում կատարել ընդհանուր կրիպտոարժութային համակարգի սահմանափակումների և հնարավորությունների վերլուծություն, որի իրականացման համար կիրառվում է SWOT վերլուծության գործիքը: Այս պարագայում վերլուծության

[1] Hash գործառույթն իրականացնում է որոշակի ալգորիթմի կողմից կատարված կամայական երկարության տողի տվյալների վերափոխումը:

գործիքը ծառայում է կրիպտոարժութային համակարգի առավելությունների ու թերությունների, ինչպես նաև հնարավորությունների ու վտանգների բացահայտման և վերլուծության համար, որոնց շնորհիվ հնարավոր է դառնում հասկանալ ոլորտի բացերը, հնարավոր խնդիրները ու զարգացման միտումները:

Կրիպտոարժութային համակարգի ուժեղ կողմեր

<u>Ապակենտրոնացում</u>: Կրիպտոարժութային համակարգում իրականացվող գործարքների վերահսկողությունը կենտրոնական մարմնի կողմից բացառվում է: Առօրյայում յուրաքանչյուր գործարք վերահսկվում է որևէ կենտրոնական մարմնի կողմից, սակայն կրիպտոարժութային համակարգում նման իրավասությունների և հնարավորությունների կենտրոնացումը բացառվում է. այն բաշխված է մասնակիցների միջև, որոնք վերահսկում են կատարվող գործարքները՝ ապահովելով համակարգի վստահելիությունը և արժանահավատությունը գրանցամատյանի միջոցով:

<u>Չմիջնորդավորվածություն</u>: Կրիպտոարժութային համակարգի այս գործոնը հնարավորություն է տալիս բացառել կենտրոնական մարմնի կամ այլ նմանատիպ գործառույթ իրականացնող մարմնի ներգրավվածությունը գործարքի իրականացման ընթացքում: Գործարքի ընթացքում փոխանցումը կատարվում է բացառապես երկու օգտատիրոջ միջև, իսկ փոխանցման գործընթացի իրականացումը փաստում են համակարգի մյուս մասնակիցները:

<u>Թափանցիկություն:</u> Բլոկչեյն համակարգը պահպանում է կատարված գործարքների ողջ պատմությունը, դրանով իսկ ապահովելով համակարգի թափանցիկությունը մասնակիցների միջև և ըստ այդմ՝ բացառում կեղծելու հնարավորությունները, քանի որ մեկ համակարգչում կամ համակարգիչների խմբում կեղծված բլոկերի շղթան կհակասի ցանցի մնացած բոլոր համակարգիչներում առկա բլոկերի ճիշտ շղթաներին և դուրս կմղվի ընդհանուր համակարգից մայներների կողմից:

<u>Անանունություն:</u> Թեպետ առաջնորդվելով թափանցիկությամբ՝ համակարգն ապահովում է օգտատիրոջ ամբողջական անանունությունը: Յուրաքանչյուր օգտատեր կարող է ստեղծել անսահմանափակ քանակությամբ հասցեներ առանց անուն, հասցե կամ որևէ այլ տեղեկատվություն նշելու:

<u>Կեղծելու անհնարինություն</u>: Առցանց գնումների կամ գործարքների համար հաճախ պահանջվող քարտերի և անձնական տվյալների մուտքագրումը ներկայումս խարդախության, ֆինանսական պաշարների կորստի արդյունք կարող է դառնալ: Կրիպտոարժութային համակարգն

առաջնորդվում է բանալիների առկայությամբ, որոնք փոխարինում են բոլոր անձնական տվյալները: Գործարքը հաստատվում է համագործակցող անձնական ու հանրային բանալիների և ալգորիթմների կիրառմամբ:

Ապահովություն և սեփականության գերակայություն: Կրիպտոարժութային համակարգում կատարված վճարումները հնարավոր չէ չեղարկել, ինչպես նաև կրիպտոմետաղադրամները չեն կարող կեղծվել, կրկնօրինակվել կամ կրկնակի ծախսվել: Հենց այս հնարավորությունները երաշխավորում են համակարգի ամբողջականությունը: Կրիպտոդրամապանակի պաշարները պատկանում են և հասանելի են միայն օգտատիրոջը, հետևաբար հաշվի սառեցում կամ այլ ազդեցություն բացառվում է, որով և պայմանավորված է օգտատիրոջ՝ իր պաշարների նկատմամբ սեփականության գերակայությունը:

Կրիպտոարժութային համակարգի թույլ կողմեր

Իրավական համակարգի անպատրաստականություն: Որոշակի գործողությունների արդյունքում, որոնք հանգեցրել են կրիպտոակտիվների կորստին հնարավոր չէ դիմել որևէ համակարգի (մարմնի) ակտիվները վերականգնելու կամ գործարքները չեղարկելու համար, ինչը պայմանավորված է կրիպտոարժութային համակարգում իրավական կարգավորումների բացակայությամբ:

Ստվերային շուկայի զարգացում: Թեև համակարգը թափանցիկ է, սակայն այն դեռևս մնում է գրավիչ հանցագործների և ստվերային գործունեություն ծավալողների համար՝ պայմանավորված ապակենտրոնացվածությամբ և անանունությամբ: Այս պարագայում կրիպտոարժութային համակարգը լավ հնարավորություն է համակարգչահեների (հակերների) և հանցագործների լայն շրջանում անհրաժեշտ ռեսուրսների շրջանառությունն ապահովելու համար:

Կրիպտոարժութային համակարգի հնարավորություններ

Անսահմանափակ գործարքների հնարավորություն: Յուրաքանչյուր օգտատեր կարող է վճարել որևէ այլ օգտատիրոջը, ցանկացած վայրում որտեղ առկա է հասանելի համացանց, անկախ մյուս օգտատիրոջ գտնվելու վայրից: Սա հատկապես հնարավորություն է թերզարգացած ֆինանսական համակարգերի կատարելագործման համար, մասնավորապես՝ ձեռնարկատիրության և էլեկտրոնային առևտրի ոլորտներում:

Արագություն: Համակարգը հնարավորություն է տալիս կատարել փոխանցում ցանկացած վայրից մեկ այլ վայր մի քանի րոպեների ընթացքում (BTC համակարգի մշակումից հետո): Սա հնարավորություն է ստեղծում հատկապես միջազգային գործարքների և միջազգային առևտրի հետագա զարգացման համար:

Կրիպտոարժութային համակարգի վտանգներ

Սեփականության գերակայություն: Բանալիների կորցնելու կամ մոռանալու պարագայում կրիպտոհաշիվը հնարավոր չէ վերականգնել, հետևաբար գոյություն չունի նաև համապատասխան կառուցակարգ բանալիների կորստի դեպքում սեփական հաշիվը վերականգնելու համար:

Գների համակարգի անկայունություն: Համակարգին բնորոշ են գների կտրուկ տատանումները, որոնք կարող են հանգեցնել ինչպես շահութաբեր ներդրումների, այնպես էլ կորուստների:

Այսպիսով, կրիպտոարժույթների առաջացումը պայմանավորված էր էլեկտրոնային փողերի առավել կատարելագործված տարբերակի ստեղծմամբ: Կրիպտոարժույթների տատանումները և պետական կառավարման մարմինների կողմից անվերահսկելիությունը հիմնական խոչընդոտող գործոններն են թե՛ պետությունների, թե՛ անհատների համար, սակայն շնորհիվ թվային ակտիվների համակարգի ապակենտրոնացվածության և չմիջնորդավորվածության, կրիպտոարժութային համակարգը շուկայում ապահովում է իր մրցակցային առավելությունն այլ արժույթների և ակտիվների նկատմամբ: Ներկայումս գոյություն ունեն մի շարք կազմակերպություններ, ծառայություններ մատուցող ընկերություններ, որոնք ընդունում են կրիպտոարժութային վճարային համակարգը որպես այլընտրանք ավանդական արժութային վճարային համակարգին: Այդ շարքը համալրող կազմակերպություններն են Wikimedia, Microsoft, Expedia, Amazon և այլն: Վերոնշյալ կազմակերպությունները և ընկերությունները շուկայում կազմում են բլոկչեյն համակարգի շրջանառությունն ապահովող սեգմենտների մի մասը: Նկատելի է, որ այս կազմակերպությունների շարքում գլխավորապես ընդգրկված են մասնավոր կազմակերպությունները, սակայն անհրաժեշտ է փաստել, որ կրիպտոարժութային համակարգն իրականում ավելի լայն կիրառում ստանալու հնարավորություն ունի նաև պետական ոլորտում, սկսած թվային փողերի թողարկումից [24], մինչև առևտրի, առողջապահության, կառավարման, փաստաթղթաշրջանառության ապահովման համակարգերը:

Հոդվածի շրջանակներում իրականացված վերլուծությունը փաստում է, որ դեռևս գոյություն չունի մեկ միասնական և/կամ ընդհանրական մոտեցում կրիպտոարժութային համակարգի վերաբերյալ, ինչպես նաև մեկ միասնական դիրքորոշում համակարգի ներդրման, իրագործման կամ կանխարգելման շուրջ:

Կրիպտոարժույթների վերաբերյալ հասկացությունների ուսումնասիրության հիման վրա հոդվածում առաջարկվել է *կրիպտոարժույթ* եզրույթի առավել համապարփակ սահմանում: Հոդվածում առաջարկված հայերեն եզրույթները կարող են հիմք հանդիսանալ տեղեկատվական և ֆինանսա-

կան տեխնոլոգիաների ոլորտներում հետագա տերմինաստեղծ գործունեության համար, ինչպես նաև կրիպտոարժութային համակարգերի հետագա կիրառության դեպքերի և դրանց առևտրայնացման կառուցակարգերի մշակման ու զարգացման համար:

ՕԳՏԱԳՈՐԾՎԱԾ ԱՂԲՅՈՒՐՆԵՐ

1. ***Hileman G., & Rauchs M***., (2017) *Global Cryptocurrency Benchmarking Study*. Cambridge Centre for Alternative Finance, 33.

2. ***Morisse M***., (2015). *Cryptocurrencies and Bitcoin: Charting the Research Landscape.* Twenty-First Americas Conference on Information Systems, Puerto Rico. (pp. 1-2).

3. ***Graeber D***., (2011). *Debt: The First Five Thousand Years* (Brooklyn, NY: Melville House).

4. ***Greco T***., (2001). Money: *Understanding and Creating Alternatives to Legal Tender.* Chelsea Green Publishing.

5. ***Teigland R., Yetis-Larsson Z., & Larsson T. O.,*** (2013). *Breaking Out of the Bank in Europe - Exploring Collective Emergent Institutional Entrepreneurship through Bitcoin*. SSRN 2263707.

6. ***Bollen R.,*** (2013). The Legal Status of Online Currencies: Are Bitcoins the Future? *Journal of Banking and Finance Law and Practice* (24:4), pp. 272–293.

7. ***Brito J., & Castillo A.,*** (2013). *Bitcoin: A Primer for Policymakers*. Arlington: Mercatus Center at George Mason University.

8. ***Brezo F. & Bringas P. G.,*** (2012). *Issues and Risks Associated with Cryptocurrencies Such as Bitcoin*. In SOTICS 2012 The Second International Conference on Social Eco-Informatics, L. Berntzen and P. Dini (eds.), Venice, Italy, pp. 20–26.

9. ***Kelly B.,*** (2015). *The Bitcoin Big Bang: How Alternative Currencies are about to Change the World*, Hoboken: Wiley.

10. ***Nakamoto S.,*** (2008). *Bitcoin: A Peer-To-Peer Electronic Cash System.*

11. ***Trautman L.,*** (2014). Virtual Currencies; Bitcoin & What Now After Liberty Reserve, Silk Road, and MT Gox? *Richmond Journal of Law & Technology* (20:4), pp. 1–108.

12. ***Bryans D.,*** (2014). Bitcoin and Money Laundering: Mining for an Effective Solution. *Indiana Law Journal* (89:1), pp. 441–472.

13. ***Frankenfield J.,*** *"Cryptocurrency" Investopedia* Financial Dictionary www.investopedia.com/terms/c/cryptocurrency.asp (15.09.2019).

14.***Royal J., Voight K.,*** (2019*). What Is Cryptocurrency? Here's What You Should Know.* www.nerdwallet.com/blog/investing/crypto currency-7-things-to-know/ (10.10.2019)

15.***Shrivas M.K. & Yeboah T.,*** (2017). *The Disruptive Blockchain: Types, Platforms and Applications.*

16.***Yli-Huumo J., Ko D., Choi S., Park S., & Smolander K.,*** (2016). *Where is current research on blockchain technology? A Systematic Review*. 11(10).

17. ***Лелу Л.,*** (2018). *Блокчейн от А до Я. Все о технологии десятилетия.* Litres.

18. ***Alharby M. & Moorsel V. A.,*** (2017). *Blockchain-Based Smart Contracts: A Systematic Mapping Study*.

19.***Techopedia Dictionary.*** *IT Education Website*, www.techopedia. com/definition/32530/mining-blockchain (28.09.2019)

20. ***Xu X., Weber I., Staples M., Zhu L, Bosch J., Bass L., Pautasso C., & Rimba P.,*** (2017). *A Taxonomy of Blockchain-Based Systems for Architecture Design*. In Software Architecture (ICSA), IEEE International Conference on. IEEE, 243-252.

21.***Mattila J.,*** (2016). *The Blockchain Phenomenon–The Disruptive Potential of Distributed Consensus Architectures* (No. 38). ETLA Working Papers.

22.***Back A.,*** (2002). *Hashcash – A Denial of Service Counter-Measure*. www.hashcash.org/papers/hashcash.pdf. (05.09.2019).

23.***Kiayias A., Russell A., David B., & Oliynykov R.,*** (2017). A Provably Secure Proof-Of-Stake Blockchain Protocol. In *Annual International Cryptology Conference* (357-388).

24.***Cukierman A.,*** (2019). *Welfare and Political Economy Aspects of a Central Bank Digital Currency.*

ПОДХОДЫ К РАЗВИТИЮ КОНЦЕПТУАЛЬНЫХ РАМОК КРИПТОВАЛЮТНОЙ СИСТЕМЫ

РОБЕРТ ХАЧАТРЯН, САМВЕЛ ОВАННИСЯН, АРПИНЕ ГЕВОРГЯН

Государственный университет имени В. Я. Брюсова

Попытки внедрения криптовалютной системы в современную реальность способствуют выявлению и реализации возможностей экономического развития и достижения конкурентного преимущества. Статья затрагивает рамки общего понятия криптовалютной системы, анализ внешних и внутренних факторов среды криптовалютной системы; таким образом, представляя исторический очерк данной сферы и основные положения, обеспечивающие актуальность данного исследования.

Ключевые слова: криптовалюта, криптовалютная система, биткоин, блокчейн, токен, майнинг, леджер, пиринг.

APPROACHES TO THE CONCEPTUAL FRAMEWORK OF CRYPTOCURRENCY SYSTEM

ROBERT KHACHATRYAN, SAMVEL HOVHANNISYAN, ARPINE GEVORGYAN

Brusov State University

The targeted attempts to implement the cryptocurrency system in modern realities contribute to the identification and implementation of opportunities for economic development and achieving a competitive advantage. The article touches upon the framework of the conceptual notions of the cryptocurrency system, the analysis of the external and internal environmental factors; thus, presenting both a historical outline of the field and the main provisions that ensure the relevance of this study.

Keywords: cryptocurrency, cryptocurrency system, bitcoin, blockchain, token, mining, miner, ledger, peer-to-peer.

Ներկայացվել է խմբագրություն 17.02.2020
Երաշխավորվել է տպագրության 12.03.2020