ბიტკოინი როგორც კრიპტოგრაფიული პრობლემების გადაჭრის გზა

მზევინარ ნოზაძე
სტუ ასოც. პროფესორი

არჩილ უნდილაშვილი
სტუ დოქტორანტი

შესავალი

კაცობრიობის ისტორიის ხანგრძლივი პერიოდის განმავლობაში ადამიანები საქონელს, პროდუქტს გაცვლით საშუალებად იყენებდნენ. ხოლო ფიატური, ანუ სახელმწიფო ვალუტა პირველად დაახლოებით 1000 წლის წინ გამოიყენეს. დღეს კი ის ფულადი მასის ძირითად ნაწილს წარმოადგენს მსოფლიო მასშტაბით. მიუხედავად ამისა, თამამად შეიძლება ითქვას, რომ ამ ნაბიჯით არ სრულდება მონტარული ისტორიის განვითარება. კრიპტოვალუტა - ეს არის ახალი სახეობოს ექსპერიმენტული ფული, რომელიც არ წარმოადგენს არც საქონელს და არც სტანდარტულ სახელმწიფოს მიერ ემიტირებულ ვალუტას. კრიპტოვალუტის ექსპერიმენტმა შესაძლებელია ვერ მიაღწიოს განვითარების მაღალ სტადიას, თუმცა აღნიშნულმა ახალმა ფულის სახეობამ მსოფლიო ეკონომიკაში ნამდივლად წარმოაშვა ახალი კითხვები და იდეები, რომელიც კრიპტოვალუტებს ახლავს თან.

ამ სტატიაში ახსნილია, თუ რას წარმოადგენს კრიპტოვალუტა და პასუხები იმ კითხვებზე, რომელიც ახალმა ექსპერიმენტმა წარმოშვა.

საკვანძო სიტყვები: ანონიმურობა; ბიტკოინი, კრიპტოვალუტა; კრიპტოგრაფია; ორმაგი ხარჯვის პრობლემა; ფული; ახალი ფულადი ეკონომიკა; მუშაობის მტკიცებულება; ფსევდონიმი; ბიზანტიელი გენერლების პრობლემა;

ᲢᲔᲥᲜᲘᲙᲣᲠᲘ ᲛᲘᲛᲝᲮᲘᲚᲕᲐ

სახელი კრიპტოვალუტა წარმოშობილია სისტემიდან, რომელიც იყენებს კრიპტოგრაფიას, რათა უზრუნველყოს დაცული გადარიცხვები და ციფრული ფულის გადაცვლა საჯაროდ განაწილებულ და დეცენტრალიზებულ ოპერაციულ სისტემაში. პირველი კრიპტოვალუტაა ბიტკოინი, რომლით ვაჭრობაც დაიწყო 2009 წელს. მანამდეც არსებობდა გარკვეული ტიპის კრიპტოგრაფიული გზით დაშიფრული აქტივები, თუმცა მათ განსხვავებულ ალგორითმებზე აწყობილი სისტემა გააჩნდათ. ორი მნიშვნელოვანი ინოვაცია და პრობლემის გადაჭრის გზა, რომელიც ბიტკოინმა წარმოადგინა, იყო ორმაგი ხარჯვის პრობლემა და „ბიზანტიელი გენერლების პრობლემა“, რომლის არსსაც შედგომში განვმარტავთ.

ᲝᲠᲛᲐᲒᲘ ᲮᲐᲠᲯᲕᲐ

ბოტკოინის შექმნამდე ფაქტიურად შეუძლებელი იყო ორ მხარეს შეორის დადებულიყო ისეთი ტიპის ელექტრონული გზით უზრუნველყოფილი გარიგება, რომელიც წარიმართებოდა მესამე პირის შუამავლობის გარეშე. ამის მთავარ მიზეზს წარმოადგენდა ორმაგი ხარჯვის პრობლემა, რომელიც ყოველთვის ახლდა თან ელექტრონული ფულადი სახსრების შექმნის ყოველ მცდელობას.

ამ ყველაფრის კარგად გასაეგბად ჯერ განვიხილოთ როგორ მუშაობს ფიზიკური ფულადი გარიგებები. მაგალითად თუ ნინო 100 ლარს გადასცემს გიორგის, ნინოს აღარ აქვს ფული, ხოლო გიორგის აქვს 100 ლარი. გიორგის ძალიან მარტივად შეუძლია დაადასტუროს 100 ლარის ქონა, რაც ბუნებრივად ადასტურებს ნინოს თანხის უქონლობასაც, იმ შემთხვევაში, თუ გარიგებაში მხოლოდ მოცემული 2 პირი მონაწილეობს. მოცემული ტიპის მარტივი გარიგების მაგლითი 2 ერთმანეთისთვის უცნობ მხარეს აძლევს შესაძლებლობას მოახდინონ ერთმანეთთან თანხების გაცვლა ნდობის გარეშე თუ შუამავლად არსებობს მესამე მხარე.

ახლა ავსხნათ ის, თუ როგორ მუშაობს გაცვლითი სისტემა

ელექტრონული პრინციპით. ჩვენ შეგვიძლია წარმოვიდგინოთ, რომ ნინო გიორგის 100 ლარის ნაცვლად იმეილის საშუალებით უგზავნის 100 ელექტრონულ ფაილს, რომელსაც ტვირთავს მეილში და შემდეგ აგზავნის. გიორგი 100 ფაილს იღებს იმეილის საშუალებით, თუმცა პრობლემა მდგომარეობს იმაში, რომ ნინოს მიერ გაგზავნილი ფაილები არის მხოლოდ და მხოლოდ ასლები, და ისინი ისევ ინახება ნინოს კომპიუტერში. შესაბამისად ნინოს მათი გაგზავნა კიდევ შეუძლია. შესაბამისად, თუ ჩვენ საქმე გვქენება ფულად აქტივებთან მსგავსი პრინციპი არ გამოგვადება.

აქამდე ორმაგი ხარჯვის პრობლემის გადაჭრის გზას წარმოადგენა გარიგებაში მონაწილე მესამე, „სანდო“ მხარე. ჩვენს მიერ მოყვანილ მაგალითში ნინოსაც და გიორგისაც ანგარიში ჰქონდათ გახსნილი მესამე მხარისთვის, მაგალითად ბანკისთვის ან ისეთი ორგგანიზაციისთვის, როგორიცაა PayPal, რომლებსაც შეუძლიათ გადარიცხვების კონტროლი და ორმაგი ხარჯვის პრობლემის თავიდან არიდება.

2008 წელს სატოში ნაკამატომ (ფსევდონიმი) წარმოადგინა საშუალება, რომელიც მოაგვარებდა ორმაგი ხარჯვის პრობლემას გარიგებაში მესამე პირის მონაწილეობის გარეშე. მისი ქმნილება ბიტკოინი თავისი არსით წარმოადგენს ელექტრნულ ფულს. სისტემა უზრუნველყოფდა ფინანსურ ტრანზაქციებს აქტივების კომპირების გარეშე, სადაც აქტივების რაოდენობის დასაზუსტებლად არ იყო საჭირო მესამე, „სანდო“ მხარის დაქირავება. სისტემა ფუნქციონირებდა კრიპტოგრაფიის გამოყენებით და პირისპირ ქსელური და სამუშაოს მტკიცებულებაზე დამყარებულ მუშაობის პრინცპით.

როგორც PayPal, ბიტკოინის სისტემაც იყენს საჯარო ელექტრონულ დაფთარს, რომელსაც ბლოკჩეინი ეწოდება. ყველა ბიტკოინ ტრანზაქცია ავტომატურად იწერება ბლოკჩეინში., თუმცა PayPal -ისგან განსხვავებით ბლოკჩეინი არ მოიაზრება ცენტრალურ მაკონტროლებლად. საბოლოოდ, ბლოკჩეინი წარმოადგენს საჯარო დკომუნეტს, რომელიც განაწილებულია პირისპირა ათასობით ბოტკოინის ქსელში მოანწიელს შორის. თითოეული

ტრანზაქცია ავტომატურად მოწმდება ბლოკჩეინ სისტემას და არ შეიქმნება ახალი ტრანზაქციის ოპერაცია მანამ, სანამ მის წინ ყველა ტრანზაქციის სისწორეს არ დაამოწმებს სისტემა. სწორედ ამ, ახალმა დამოუკიდებელმა სისტემურმა მოდეალმა უზრუნველყო მესამე, მაკონტროლილებელი პირის „ფულადი“ გარიგებების სისტემიდან ჩამოშორება.

ᲑᲘᲖᲐᲜᲢᲘᲔᲚᲘ ᲒᲔᲜᲔᲠᲚᲔᲑᲘᲡ ᲞᲠᲝᲑᲚᲔᲛᲐ

მიუხედავად იმ ფაქტისა, რომ ბიტკოინის კონცეფცია წყვეტდა ორმაგი ხარჯვის ამოცანას, თავი იჩინა კიდევ ერთმა დამატებითმა პრობლემამ. თუ ქსელში არსებულ ყველა ნოდს გააჩნია სრული ასლი იმ დაფთრისა, რომლებსაც ისინი აზიარებენ იმ მონაწილეებთან, ვისთანაც აქვთ კონტაქტი, მაშინ საიდან უნდა შეიტყოს ახალმა ნოდმა, რომ მას არ მიეწოდება ყალბი დაფთრის ასლი? იმ რთულ ამოცანას, რომლის მთავარი საკითხი არის კონსესუსის მიღწევა ნოდებს შორის, რომლებიც ერთმანეთს არ ენდობიან კომპიუტერულ მეცნიერებათა ლიტერატურაში ცნობილია, როგორ ბიზანტიელი გენერლების პრობლემა. სახელი ბიზანტიელი გენერლების პრობლემა მომდინარეობს ისტორიული გარემოებიდან, როცა ბიზანტიელი გენერალთა გარკვეული რაოდენობა საკუთარი ჯარისკაცებით გარს ერტყა ქალაქს და მათი მიზანი იყოს ქალაქის აღება. მათ იცოდნენ, რომ თუ ისინი ერთდროულად შეუტევდნენ, საკუთარი ძალების ნახევრითაც კი ადვილად შეძლებდნენ ქალაქის აღებას, მაგრამ თუ ისინი ცალცალკე მიიტანდნენ იერიშს მტერი მათ ადვილად დაამარცხებდა. გენერლებს ერთმანეთთან კავშირი მხოლოდ წერილებით ჰქონდათ, რომლის ნამდვილობის დადასტურებაც შეუძლებელი იყო. გენერლები ასევე ეჭვობდნენ, რომ მათ შორის იყვნენ მოღალატეები. როგორ უნდა შეძლებოდათ გენერლების უმრავლესობას შეთანხმება ზუსტ შეტევის დროზე, როცა მათი გზავნილები იყო არააუტენთიფიცირებული, მათ შორს იყვნენ მოღალატეები და არ ჰყავდათ ცენტრალური მაკონტროლებელი?

სინამდვილეში ესაა იგივე პრობლემა, რომელსაც ბიტკოინის

მაინერები ხვდებიან მაშინ, როცა უნდა დაადასტურონ ახალი ტრანზაქცია და დაამატონ ის საერთო დაფთარში.ბიტკოინის მიერ წარმოდგენილი პრობლემის გადაჭრის გზა კი არის ის, რომ ის მიღებულ ტრანაქციას ახვედრებს რთულ მათემატიკურ თავსატეხს, რომლის გაშიფრვაც საკმაოდ რთულია კომპიუტერის მიერ, თუმცა დადასტურება მარტივი. რთული მათემატიკური „ამოცანის“ ამოხსნელად კომპიუტერს სჭირდება დაახლოებით 10 წუთი, შესაბამისად ბლოკჩეინის ქსელში ყოველი ახალი ბლოკი 10 წუთში ერთხელ ემატება, სადაც უკვე გადამოწმებული და დადასტურებულია ყველა ის ტრანზაქცია, რაც კი მანამდე მომხდარა ქსელში.

დასკვნა

მოცემული ორი მნიშვნელოვანი პრობლემის გადაჭრით „სატოშნი ნაკამატომ“ მოახერხა ის, რომ საბოლოოდ ჩამოეყალიბებინა სრულიად ახალი და ინოვაციური საქემა, რომელიც უზრუნველყოფდა ელექტრონული გზით ღირებულებების გაგზავნას მესამე მაკონტროლებელი ძალის ჩარევის გარეშე. სწორედ ამ პრობლემების გადაჭრის შემდგომ შეიქმნა პირველი სრულყოფილი კრიპტოგრაფიულად დაშიფრული დეცენტრალიზებული ციფრული აქტივი ბიტკოინი.

REFERENCES

1. S.Nakamato „Peer-to-peer electronic cash system” 2008, bitcoin.org.

2. J.Kareken and Wallace , On the indeterminacy of equilibrium exchange rates. 1981

Hall, R. E. 1982. Monetary trends in the United States and the United Kingdom: a

review from the perspective of new developments in monetary economics.

BITCOIN AS THE WAY TO SOLVE CRYPTOGRAPHIC PROBLEMS

Mzevinar Nozadze,
Associate Professor of GTU
Archil Undilashvili,
PhD Student of GTU

Resume

Throughout the long history of mankind, people have used goods, products as a means of exchange. Fiat, or state currency, was first used some 1,000 years ago. Today it is a major part of the money supply worldwide. Nevertheless, it is safe to say that this step does not complete the development of monetary history. Cryptocurrencies - this is a new type of experimental money that is neither a commodity nor a standard currency. The cryptocurrency experiment may not reach a high level of development, but the new money has generated new questions and ideas in the world economy that accompany cryptocurrencies.

This article explains what cryptocurrency bitcoin is and the answers to the questions posed by the new experiment.

Key words: Anonymity; Bitcoin, Cryptocurrency; Cryptography; Double spending problem; Money; The new monetary economy; Evidence of work; A pseudonym; The Problem of the Byzantine Generals;