ბლოკჩეინი მისი არსი და სტრუქტურა
Blocking his essence and structure

ნანა გულკაშვლი – დოქტორანტი, საქართველოს ტექნიკური უნივერსიტეტი
Nana gulkashvl - PhD student, Georgian Technical University

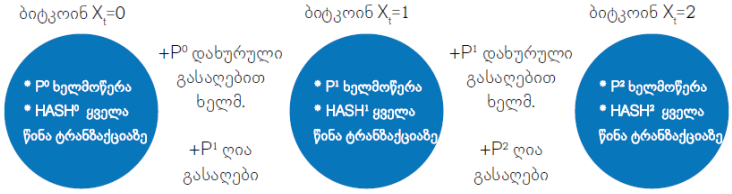
რეზიუმე: წინამდებარე სტატია მიზნად ისახავს გააცნოს მკითხველს კრიპტოგრაფიული ვალუტის ისეთი უმნიშვნელოვანესი სიახლე და მიღწევა როგორიცაა ბლოკჩეინ ტექნოლოგია მისი არსი სტრუქტურა ფუნქციონირების თითოეული დეტალი და ამ ფუნქციების მნიშვნელობა დანერგვა და გამოყენება ისეთ ტექნოლოგიურ მიღწევასთან მიმართებაში როგორიცაა კრიპტოგრაფიული ვალუტა.
საკვანძო სიტყვები: კრიპტოვალუტა. ორადი ჩაწერის სისტემა, ბლოკჩეინ ტექნოლოგია, სწრაფი გადარიცხვა.უნაღდო ანგარიშსწორება. დეცენტრალიზებული. ჰეშირება.

Abstract: This article is aimed at introducing the reader of the cryptographic currency as a crucial novelty and achievement such as blocking technology its essence structure for each detail of the functioning and the importance of these functions to introduce and use the technological achievement such as cryptographic currency.
Key Words: Cryptival. Ordiner recording system, blocking technology, quick transfer.Donce. Hashing.

შესავალი: კრიპტოგრაფიული ფულის გამოჩენა ჩვენს ცხოვრებაში ბევრ პასუხგაუცემელ კითხვასთანაა დაკავშირებული და ამ კითხვების ძირითადი ნაწილი როგორც წესი ეხება, პირველ კრიპტოგრაფიულ ვალუტას ბიტკოინს მის ფუნქციონირებას და ისეთ ულტრათანამედროვე ტექნოლოგიის გამოყენაბსს და მნიშვნელობასმის ფუნქციონირებაში როგორიცააა ბლოკჩეინ ტექნოლოგია სწორედ ამ თემას და ამ კითხვებზე პასუხის გაცემის მცდელობაა ქვემოტ აღნიშნული სტატია.

ძირითადი ტექსტი: კრიპტოგრაფიული ვალუტებიდან დღესდღეობით დღესდღეობით ყველაზე გავრცელებული და წარმატებულია ბიტკოინი. ტექნიკურად ბიტკოინი ემყარება ე.წ. ერთ რანგიან, პირინგულ (Peer-to-Peer, P2P) ქსელს იგივე ბლოკჩეინ სისტემას რომელსაც არ გააჩნია ცენტრალური ადმინისტრატორი. შეტყობინებების მიწოდება ხდება ერთი მონაწილიდან მეორე მონაწილეზე, ამავდროულად შეტყობინების მიმღები თავად ხდება ამავე შეტყობინების გადამცემი ქსელის სხვა მონაწილისთვის. ამის გარდა ანგარიშსწორებები ქსელის მონაწილეებში დენომინირებულია არა რომელიმე რეალურ ვალუტაში, არამედ თავად ბიტკოინებში, ამასთან რომელიმე რეალურ აქტივთან ან ოფიციალურ ვალუტასთან ბიტკოინის ღირებულება არ არის მიბმული, არამედ მისი ღირებულება სხვა ვალუტებთან მიმართებაში განისაზღვრება ღია ბაზარზე მიწოდებისა და მოთხოვნის საფუძველზე. აქედან გამომდინარე, ბიტკოინი დეცენტრალიზებულ ვირტუალურ ვალუტას წარმოადგენს,ოფლაინ სისტემით. ბიტკოინის ქსელის დეცენტრალიზაცია აქტუალურს ხდის ციფრული ვალუტის ფუნქციონირებისათვის საჭირო ზემოთ ჩამოთვლილი მოთხოვნების შესრულებას, რომლებს შორისაც პირველი რიგის მნიშვნელობა ორმაგი გადახდის თავიდან აცილების მოთხოვნას აქვს. ცენტრალიზებულ სისტემაში A და B პირებს შორის ონლაინ ტრანზაქციაში მონაწილეობს მესამე საიმედო პირი მაგალითად ბანკი, რომელიც უზრუნველყოფს გადამრიცხავის მიერ ერთიდაიგივე ციფრული ღირებულების ორჯერ გამოყენების თავიდან აცილებას. მაგრამ თუ ასეთი მესამე მხარე არ იქნება და ციფრული ფული მომხმარებლების კომპიუტერებში, იქნება შენახული მაშინ, მათი მარტივი ასლის აღებით გადამხდელს შესაძლებლობა ექნება ერთი და იგივე ციფრული ფულით ორჯერ გადახდის შესრულება. დეცენტრალიზებული სისტემისთვის ანუ ბლოკჩეინ სისტემისათვის სხვა გამოწვევებს უკვე

განხორციელებული ტრანზაქციების დეცენტრალიზებული შენახვა მომხმარებელთა ანგარიშების განსაზღვრა წარმოადგენს. ბიტკოინის რევოლუციური სიახლე ბლოკჩეინ სისტემაა, რომელიც ორმაგი გადახდის თავიდან აცილებას უზრუნველყოფს. სანდო მესამე მხარის გარეშე როგორც უშუალოდ ტრანზაქციისას , ასევე მისი დასრულების შემდეგ. ტრანზაქციების განსახორციელებლად და ბიტკოინის მისაღებად მომხმარებელმა საკუთარ კომპიუტერში უნდა გადმოწეროს და დააყენოს მიმდინარე ბიტკოინის პროგრამა კლიენტი, რის შემდეგ იგი ქმნის კრიპტოგრაფიული გასაღებების წყვილს დახურულ და ღია გასაღებებს. ღია გასაღები ქვეყნდე ბაბიტკოინის ქსელში (რომლის წევრიც მომხმარებელი პროგრამის საკუთარ კომპიუტერზე დაყენების შემდეგ გახდა), ხოლო დახურული გასაღები კომპიუტერში ფაილის სახით შეინახება.მისი დაკარგვა ან წაშლა ავტომატურად გულისხმობს რომ ამ გასაღებებთან დაკავშირებული მონეტები დაიკარგება. თითოეულ მომხმარებელს შეუძლია შეუზღუდავი ოდენობის გასაღებების წყვილი შექმნას და ისინი მოათავსოს თავის ბიტკოინის საფულეში.ქვემოთ მოცემულ დიაგრამაში ნაჩვენებია ბლოკჩეინ სისტემაში განხორციელებული ოპერაციების თანმიმდევრობა და სტრუქტურა.



ნაკამოტოს მიხედვით ბიტკოინის ელექტრონული მონეტა ციფრული ხელმოწერების ჯაჭვს წარმოადგენს მოცემულია ერთი და იგივე ბიტკოინი არსებობის სხვადასხვა მომენტში. ტრანზაქციის მისაღებად P0 მფლობელს P1–მამომხმარებელმა უნდა მიაწოდოს

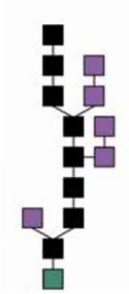
თავისი ღია გასაღები ბიტკოინი. ეს უკანასკნელი თავისი დახურული გასაღებით ციფრულად ხელს აწერს ამ ბიტკოინის „მონეტით“ განხორციელებულ ყველა წინა ტრანზაქციის ჰეშს და მიმღების ღია გასაღებს. ამგვარად თითოეული ბიტკოინი შეიცავს მისი მეშვეობით განხორციელებული ყველა ტრანზაქციის შესახებ ინფორმაციას. პრაქტიკულად მისით განხორციელებული ყველა გადახდა იგივე ტრანზაქცია გადამხდელის ხელმოწერილ შეტყობინებას წარმოადგენს, რომელიც შეიცავს გამოყენებული ბიტკოინების „ისტორიის“ ჰეშს და შესაბამისად ბიტკოინებში გადახდის თანხას და მიმღების ღია გასაღებს. გადამხდელის ლეგიტიმაცია მისი გამოქვეყნებული იგივე ღია გასაღების მეშვეობით მოწმდება, ხოლო შეტყობინებაში განთავსებული მიმღების ღია გასაღები საჯაროდ აფიქსირებს ამ ბიტკოინების ახალ მფლობელს. შემდგომ ტრანზაქციაზე ფიქსირდება დროის აღნიშვნა და ინახება ბლოკჩეინის ინფორმაციული ჯაჭვის ახალ ბლოკში. შემდეგ ბიტკოინის ბლოკჩეინში ჩართული ყველა კომპიუტერი უზრუნველყოფს, რომ ქსელის თითოეულ მონაწილეს განახლებულიი ნფორმაცია ჰქონდეს შესაბამისად ბიტკოინის ახალი მფლობელისა და განხორციელებული ტრანზაქციების შესახებ.როგორც უკვე აღინიშნა ბიტკოინის ქსელს ცენტრალური სანდო პირი არ გააჩნია, რომელიც აწარმოებს და ცენტრალიზებულად აღრიცხავს. ამრიგად საჭიროა მექანიზმი, რომელიც უზრუნველყოფს განხორციელებული ტრანზაქციების დადასტურებას რაც თავიდან აიცილებს გადამხდელის მიერ იგივე ბიტკოინით სხვა ტრანზაქციის განხორიცელებას. და საერთო ბუღალტერიის წარმოებას. რომელიც იმ მომხმარებლებზეა დამოკიდებული, რომლებიც თავიანთი კომპიუტერების გამოთვლითი სიმძლავრეების ნაწილს „გადასცემენ“ ბიტკოინის ბლოკჩეინის ქსელის განკარგულებაში, რადგან მოხდეს განხორციელებული ტრანზაქციების რეკონსილაცია.მათ ხშირად “მომპოვებლებს“– „miner“ უწოდებენ. წარმოდგენილი მონაცემების

სისწორის დადასტურებისა და შენახვა ინფორმაციული ბლოკების ჯაჭვში ანუ ბლოკჩეინში ამისათვის მოცემული ალგორითმით მომხმარებლები ცდილობენ ბიტკოინის პროგრამულ უზრუნველყოფაში ამოხსნან რთული მათემატიკური პრობლემა, რომელიც მოიცავს:

ა) ახალ ბლოკში ტრანზაქციების სისწორის შემოწმებას რაც უზრუნველყოფს გადამხდელების ლეგიტიმაციას, ორმაგი გადახდის თავიდან აცილებას.

ბ) წინასწარ დადგენილი სირთულის ხარისხის დაკმაყოფილებას.

ყველა ახალი ბლოკი უნდა შეიცავდეს ყველა წინა ბლოკების ჯაჭვის ჰეშს,(ჰეშირება ეწოდება მონაცემის გარდაქმნის პროცესს ფიქსირებული სიგრძის ცვლადად,) რითაც უზრუნველყოფილი იქნება საერთო ბუღალტერიის მთლიანობა და უწყვეტობა. ახალი ბლოკი აღიარებული იქნება იმის შემდეგ, რაც მის სისწორეს ბლოკჩეინის ქსელში ჩართული მონაწილეთა უმრავლესობა დაადასტურებს. სქემატურად ბლოკების ჯაჭვი შეიძლება გრაფის ხის (graph tree) მეშვეობით იქნეს წარმოდგენილი



ამასთან დადასტურებულია ბლოკების ჯაჭვი, რომელიც ყველაზე მეტად არის დაშორებული ამ ხის ფესვიდან (Root block). ასევე რომელიმე ბლოკში ცვლილების შეტანისათვის ამ და მის მომდევნო ყველა ბლოკისათვის აუცილებელი იქნებოდა თავიდან იყოს ნაპოვნი შესაბამისი მათემატიკური პრობლემის ამოხსნა და უფრო სწრაფად, ვიდრე ალტერნატიულ ჯაჭვში დანარჩენი მომხმარებლები ახალ

ბლოკებს დაადასტურებენ,რაც პრაქტიკულად შეუძლებელს ხდის უკვე დადასტურებულ ბლოკებში ცვლილებების შეტანას. აღნიშნული ალგორითმი წარმოადგენს ბიზანტიელი გენერლების საომარი ამოცანის ელეგანტურ გადაწყვეტას და საბრძოლო ტაქტიკის ერთ-ერთ უნიკალურ მეთოდს. მიუხედავად დეცენტრალიზაციისა, მომხმარებელთა ჯგუფის ან ცალკეული მომხმარებლების მიერ წინააღმდეგობრივი ტრანზაქციების გენერირების შემთხვევაში ისინი არ დადასტურდება მანამდე, სანამ მიღებულ წესებს ქსელის მომხმარებელთა უმრავლესობა იცავს. შესაბამისად, რაც მეტია ბიტკოინის ქსელის მონაწილეების რაოდენობა, მით უფრო ძნელია თაღლითებისათვის საერთო ბუღალტერიაში თაღლითური ტრანზაქციების შესრულება.

ამგვარად ბლოკჩეინის ბუღალტრული აღრიცხვის სქემა შემდეგნაირია.

1. ახალი, ჯერ კიდევ დაუდასტურებელი ტრანზაქციების გამოქვეყნება.

2. გამოქვეყნებული ტრანზაქციების რთული მათემათიკური ამოცანების გადაჭრის გზით დადასტურება.

3. უმრავლესობის მიერ დადასტურებული ბლოკის არჩევა, ჯაჭვის შემდეგ ბლოკად და ახალი ბლოკების გამოქვეყნება.

დასკვნა: როგორც ზემოთ მოყვანილი ტექსტიდან ჩანს ბლოკჩეინ ტექნოლოგია უნიკალური ინფორმაციის აღრიცხვის სისტემაა რომლის დანერგვა და გამოყენება კრიპტოგრაფიული ვალუტის გარდა ძალიან ბევრ ტრადიციულ სფეროში მოგცემს უამრავ ბენეფიტს ამ სფეროებში და მათ განვითარებას თანამედროვე გამოწვევებისა და პრობლემების გადაჭრის კუთხით.

გამოყენებული ლიტერატურა:

1.https://www.coinfirm.com/products/amlplatform/?utm_source=google&utm_medium=cpc&utm_campaign=AML_Global&gclid=Cj0KCQiA7YyCBhD_

ARIsALkj54p-CSnaOThqGrAqdjKH17CJ15kwVGPd-d0hdzWLVhSmosB8zsjT308aAnWoEALw_wcB

2.https://phemex.com/lpcryptoplatform?group=730&referralCode=DPXAJ&gclid=Cj0KCQiA7YyCBhD_ARIsALkj54qYRB0_9QB1hYhGng97BFP_7rhYTp272S90Njqp9fGohW4WTyBOyXwaAuFKEALw_wcB.

3.https://ka.wikipedia.org/wiki/%E1%83%91%E1%83%9A%E1%83%9D%E1%83%99%E1%83%A9%E1%83%94%E1%83%98%E1%83%9C%E1%83

4. https://www.investopedia.com/terms/b/blockchain.asp