ბლოკჩეინი

პრინციპები და საფუძვლები

ალექსანდრე ციხილოვი

თბილისი • 2020

Alexander Tsikhilov. Blockchain — principles and fundamentals
ალექსანდრე ციხილოვი. ბლოკჩეინი — პრინციპები და საფუძვლები

რედაქტორი ზურაბ აბაშიძე
ყდის დიზაინი ირმა ლიპარტელიანი

ISBN 978-9941-9686-5-5
978-1-913340-90-2 (English Edition. 2020)

საგა — საქართველოს აკადემიური გამომცემლობა
დავით აღმაშენებლის გამზირი. #181-2, თბილისი, 0102
ტელ.: (+995 32) 234.04.32
ელ-ფოსტა: pressacademic@gmail.com
www.apgeorgia.com
FB: Academic-Press-of-Georgia

შინაარსი

ნაწილი III
ბლოკჩეინ-ინდუსტრია

ნაწილი I

როგორ არის მოწყობილი ბლოკჩეინი

შესავალი

„თავიდან ვერ გამჩნევენ, შემდეგ დაგცინიან,
მერე იწყებენ ომს, სურთ, რომ გადაგბუგონ,
და ბოლოს, გიდგამენ ძეგლს...“

ეს არის ციტატა ამერიკელი პროფკავშირული ადვოკატის ნიკოლას კლაინის გამოსვლიდან, რომელსაც, ოდნავ შეცვლილი სახით, შეცდომით მიაწერენ მახათმა განდის. კლაინმა წარმოთქვა ეს სიტყვა ასი წლის წინ სრულიად სხვა საბაბით, თუმცა ეს სიტყვები, როგორც არც ერთი სხვა, საუკეთესოდ ერგება სიტუაციას, რომელიც რაღაც მოვლენის გარშემო წარმოიქმნა. ის ჩვენს ცხოვრებაში ცოტა ხნის წინ, მაგრამ იმდენად სწრაფად შემოიჭრა, რომ თავის ირგვლივ პოლარული აზრების შეხლა-შემოხლა წარმოშვა: კატეგორიული მიუღებლობიდან მოწინააღმდეგეებში, მგზნებარე აღფრთოვანებამდე აპოლოგეტებში. მსგავსი დისკურსის თვით ფაქტი ნიშნავს, რომ მოვლენა, რომელსაც ამდენი შუბი შეელეწა, თავისთავად არაორდინარულია და ღრმად შესწავლას იმსახურებს. ეს მოვლენაა ბლოკჩეინ-ტექნოლოგია და მის საფუძველზე აგებული პროექტები.

მართლაც, ბლოკჩეინი და, კერძოდ, მისი პრაქტიკული რეალიზაცია კრიპტოვალუტის სახით არის ცხარე დისკუსიების საგანი როგორც კომპიუტერული ტექნოლოგიების სამყაროში, ასევე ფინანსურ ინდუსტრიაში. შედარებითი ტექნიკური სირთულე ქმნის გარკვეულ წინააღმდეგობებს ამ არატრივიალური ტექნოლოგიის ყველა უპირატესობისა და ნაკლოვანების სწრაფად აღსაქმელად. ისინი კი, რომლებმაც შეძლეს ბლოკჩეინ-ქსელების მუშაობის პრინციპების ძირითად ასპექტებში ჩაწვდომა, საკმაოდ სწრაფად მიდიან იმ დასკვნამდე, რომ ამ ტექნოლოგიის წარმოშობამ და შემდგომმა განვითარებამ შეიძლება, მნიშვნელოვნად შეცვალოს თანამედროვე მსოფლიო მოწყობის სურათი. ამ აზრს ზოგი აღტაცებაში მოჰყავს, სხვებს კი გულს უტეხს. ვიღაცას ამ ტექნოლოგიის გაჩენა ახალ დარგში თვითრეალიზაციის შანსს აძლევს, ხოლო ვიღაც სერიოზუ-

ლად შიშობს დაკარგოს არსებული პოზიციები იმ დარგებში, რომელთა შემდგომი არსებობისათვის ბლოკჩეინი შეიძლება საფრთხეს წარმოადგენდეს.

ვინმე სატოში ნაკამოტოს ავტორობით 2008 წელს შექმნილი დოკუმენტი და ბლოკჩეინ-ტექნოლოგიის ბაზაზე მას მიდევნებული პირველი პრაქტიკული რეალიზაცია – ბიტკოინ-პროექტი – იმდროინდელი მსოფლიო საზოგადოებისათვის შეუმჩნეველი დარჩა. თუკი ვინმემ შენიშნა ეს პროექტი, ეს იყვნენ მხოლოდ სპეციალისტი-კრიპტოგრაფები, რომელთაც ძირითადად, პროფესიული ასპექტები აინტერესებდათ. მოგვიანებით, როდესაც ინფორმაცია ნელ-ნელა გავრცელდა, პროექტს ღიად დაცინვა დაუწყეს, – თვით იდეა იმის შესახებ, რომ არსებობს რაღაც ელექტრონული ვალუტა, ბევრს სასაცილოდ ეჩვენებოდა. მაგრამ როდესაც ბიტკოინის ერთი მონეტის ღირებულებამ ათასობით დოლარს მიაღწია, ბევრს უკვე აღარ ეცინებოდა.

ბლოკჩეინ-პროექტებისადმი ინტერესის ნამდვილი გამოვლინება 2016 წლის პირველ ნახევარში დაიწყო. ჰოდა, მაშინ, თუ კლაინის ციტატას მივყვებით, ბლოკჩეინ-ინდუსტრია თავისი ევოლუციის შემდეგ ეტაპზე გადავიდა, – მას წინააღმდეგობის გაწევა დაუწყეს. ბლოკჩეინის პროექტებმა სერიოზული საფრთხეები და ინტერესთა კონფლიქტები შეუქმნა ეროვნულ მთავრობებს, ფინანსურ რეგულატორებს, ტრადიციულ ფინანსურ ინსტიტუტებსა და მსხვილ საშუამავლო სერვისებს. სამართლიანობისათვის უნდა აღვნიშნოთ, რომ ბევრი ამ საფრთხეებიდან უსაფუძვლო არ არის და ამ წიგნის რამდენიმე თავი მოცემული პრობლემატიკის აღწერასა და ანალიზს დაეთმობა.

რაც შეეხება მთლიანობაში ტექნოლოგიისადმი კრიტიკულ და ნეგატიურ დამოკიდებულებას, აშკარაა, რომ ძნელი იქნებოდა იმ მოვლენის დადებითად შეფასებისა და მხარდაჭერის მოლოდინი, რომლის მუშაობის პრინციპებიც თავისთავად, საკმაოდ რთული გასაგებია. წიგნის ამოცანაა, რამდენადაც შესაძლებელია მოცემულ კონტექსტში, ტექნოლოგიურად რთული კონცეფციები გასაგები ენით ახსნას ანუ ისე, რომ მკითხველმა, რომელიც საკმაოდ შორსაა კომპიუტერული და ფინანსური ტექნოლოგიებისაგან, ბლოკჩეინის არსსა და მის ბაზაზე აგებული პროექტების მუშაობაზე ნათე-

ლი წარმოდგენა შეიქმნას. წიგნი არ შეიცავს რთულ მათემატიკურ აპარატს ჩახლართული ფორმულებით ან ალგორითმების ზედმეტად დაწვრილებით აღწერას. ბევრი შედარებით რთული კონცეფცია გადამუშავებულია მათი გაგების გასამარტივებლად და წიგნში „მსხვილი შტრიხებითაა“ დასურათხატებული. თავიდანვე გვინდოდა აღგვენიშნა, რომ წიგნის ავტორი არც მათემატიკოსია, არც ფიზიკოსი, არც ისტორიკოსი, არც ეკონომისტი და, უკვე ორი ათეული წელია, აღარც პროგრამისტი. ავტორი მეწარმეა, კრიპტოენთუზიასტი და გარკვეულწილად, ბლოკჩეინ-ევანგელისტი, და სწორედ აქედან გამომდინარე უნდა განვიხილოთ წიგნში გადმოცემული სამყაროს აღქმის პოზიციები ისეთი მასშტაბური და მომაჯადოებელი მოვლენისადმი, როგორიც ბლოკჩეინია.

ახლა წიგნის სტრუქტურის შესახებ. იმ გამოგონებათა ისტორიაში მოკლე ისტორიულ ექსკურსს, რომლებმაც თავის დროზე სერიოზულად შეცვალა სამყარო, მოსდევს თავი, რომელიც ბლოკჩეინ-ტექნოლოგიების დაწვრილებით აღწერას ეთმობა. შემდეგ განხილული იქნება ყველაზე პოპულარული პროექტები, რომლებიც ბლოკჩეინით განხორციელდა, საუბარი ძირითადად, კრიპტოვალუტებზე იქნება. შემდეგი თავი ეძღვნება ტექნოლოგიის გამოყენებას სხვადასხვა დარგში: აღწერილია როგორც არსებული პროექტები, ასევე პროექტები, რომლებიც ჯერ კიდევ იგეგმება სარეალიზაციოდ. იმ თავზე, რომელიც ბლოკჩეინ-პროექტებისა და სახელმწიფოთა ურთიერთობების პრობლემატიკას ეძღვნება, საუბარი უკვე იყო. და ბოლოს, მოდის თავი კრიპტოაქტივებში ინვესტიციების შესახებ, რომელიც მკითხველებში განსაკუთრებული მოთხოვნით სარგებლობს. ბევრი ოცნებობს მნიშვნელოვანი მოგების მიღებას კრიპტოინვესტიციებიდან, თუმცა, ყველა ინვესტორი საკმარისად როდია გარკვეული ამ პროცესებთან დაკავშირებულ რისკებში და იმაშიც, თუ როგორ შეიძლება ამ რისკების მართვა. წიგნის დასკვნითი თავი ბლოკჩეინ-ტექნოლოგიების განვითარების პერსპექტივას ეხება.

დასასრულ, რამდენიმე სიტყვა გვინდა ვთქვათ წიგნში მოცემული ინფორმაციის აქტუალობაზე. ბლოკჩეინ-ინდუსტრია და მასში მიმდინარე პროცესები საკმაოდ დინამიკურად ვითარდება. ამის გამო, გამორიცხული არ არის, რომ ამ წიგნის წაკითხვის მომენტისთვის მასში გადმოცემული გარკვეული ფაქტები ცოტათი მოძვე-

ლებულადაც მოგვეჩვენოს, ხოლო დაუსრულებელი ისტორიები გაგრძელდეს. ამავდროულად, წიგნში წარმოდგენილია ფუნდამენტური ხასიათის ინფორმაცია, რომელიც ძნელად თუ შეიცვლება დროთა განმავლობაში. ამასთანავე, ამგვარი განსაზღვრებები ჭარბობს ავტორის მიერ წარმოდგენილ ბლოკჩეინ-ტექნოლოგიების შემადგენელი სხვადასხვა ცნების გადმოცემისას. ზემოთქმულის გათვალისწინებით, შეიძლევა, იმედი ვიქონიოთ, რომ წიგნის გამოსვლიდან გარკვეული დროის გასვლის შემდეგაც მისი შინაარსი საინტერესო იქნება მკითხველთათვის, რომლებსაც სურთ გაეცნონ ისეთ საინტერესო საგანს, როგორიც ბლოკჩეინია.

ავტორი გულითად მადლობას უხდის მეგობრებსა და კოლეგებს დახმარებისა და მხარდაჭერისათვის, რომლის გარეშეც ამ წიგნის შექმნა შეუძლებელი იქნებოდა.

აღმოჩენები, რომლებმაც სამყარო შეცვალა

ცივილიზაციის ისტორია ათასწლეულებს ითვლის. ამ დროის განმავლობაში კაცობრიობამ დიდი გზა განვლო უძველეს დროში გამოყენებული პრიმიტიული მეთოდებიდან და პრაქტიკებიდან, ურთულეს თანამედროვე ტექნოლოგიებამდე. ცივილიზაციის ევოლუციის უკან დგას უმნიშვნელოვანეს გამოგონებათა ჯაჭვი, რომლებმაც თავის დროზე დიდი გავლენა მოახდინა ადამიანთა ცხოვრებაზე და ხელი შეუწყო განვითარების შემდეგ საფეხურზე გადასვლას. 6000 წლის წინ შექმნილმა ჩვეულებრივმა ბორბალმა მნიშვნელოვნად გააადვილა ადამიანებისა და ტვირთების გადაადგილება. ეს კი განაპირობა ინტუიციურ დონეზე აღქმულმა ფაქტმა, რომ შედარებით სწორ ზედაპირზე გორების ხახუნის ძალა საგრძნობლად ნაკლებია, ვიდრე სრიალის ხახუნის ძალა. საბოლოოდ აღმოჩნდა, რომ ტვირთის გაგორება ბორბლებზე გაცილებით იოლია, ვიდრე მისი მიწაზე გახოხება. დაახლოებით იმ დროს გამოჩნდა მეტყველებითი ინფორმაციის ნახატებისა და ნიშნების სახით დაფიქსირების პირველი მცდელობები მათი შემდგომი შენახვის მიზნით. ასე გაჩნდა დამწერლობის ადრეული ჩანასახები, ხოლო მასთან ერთად, ადამიანის ცოდნის კომპონენტების დაგროვებისა და გავრცელების შესაძლებლობა. გარკვეული დროის შემდეგ, ადრეული სახელმწიფოებრივი წარმონაქმნების გაჩენასთან ერთად, კაცობრიობას დასჭირდა ესწავლა მისთვის ხელმისაწვდომი რესურსების გათვალისწინება და განაწილება, ასე გაჩნდა ციფრები და მათი საშუალებით ელემენტარული მათემატიკური მოქმედებები.

ჩვენი წელთაღრიცხვის პირველი ათასწლეულის დასაწყისი აღინიშნა რომის იმპერიის სამხედრო, პოლიტიკური და კულტურული დომინირებით ევროპის, ჩრდილოეთ აფრიკისა და ახლო აღმოსავლეთის ტერიტორიებზე. როგორც შედეგი, რომაული თვლის სისტემამ ფართო გამოყენება პოვა და კვლავაც გამოიყენებოდა V საუკუნეში იმპერიის დაცემის შემდეგაც. მაგრამ რიცხვთა ჩაწერის არაპოზიციური სისტემა ძალზე მოუხერხებელი იყო, განსაკუთრებით, რთუ-

ლი არითმეტიკული ოპერაციების, მაგალითად, გაყოფისას და გამრავლებისას. ზუსტი მეცნიერებების განვითარებამ, მათი მათემატიკური აპარატების გართულებამ და რესურსების აღრიცხვის უფრო თავსატეხმა ფორმებმა და მათმა მოძრაობამ წარმოქმნა საზოგადოებრივი ინტერესი თვლის უფრო პროგრესული – პოზიციური სისტემის შექმნისა. X და XI საუკუნეების მიჯნაზე ფრანგი მეცნიერი (შემდგომში რომის პაპი) ჰერბერტ ავრილაკელი გახდა ასეთი სისტემის ერთ-ერთი პირველი პოპულარიზატორი, რომელიც შეიმეცნა ესპანეთში სწავლისას მაშინ, როცა ამ ქვეყნის დიდი ნაწილი არაბთა ბატონობის ქვეშ იმყოფებოდა. ახალმა სისტემამ ევროპაში მაშინვე ვერ დაიმკვიდრა ადგილი და მხოლოდ XIII საუკუნის შუა ხანებში, იტალიელი მეცნიერი ფიბონაჩის წყალობით, „არაბული ციფრების“ შედარებით ფართოდ გავრცელება დაიწყო. ამან მნიშვნელოვანი ბიძგი მისცა ევროპაში ფინანსური მომსახურების ინდუსტრიის შექმნასა და განვითარებას, პირველ რიგში – იტალიაში, რომელიც შუა საუკუნეების დამლევისთვის, ფინანსური ტექნოლოგიების ფლაგმანი გახდა.

სწორედ იმ დროის იტალიაში, ბოლოს და ბოლოს, მნიშვნელოვანწილად გადაიჭრა სასაქონლო-ფულადი ფასეულობების მოძრაობის ამოცანა, სახელდობრ, გამოგონებული იქნა ორმაგი საბუღალტრო ჩანაწერი. ორმაგი ჩანაწერის მეთოდის არსი აქტივებისა და პასივების ბალანსში ძევს. სხვაგვარად რომ ვთქვათ, მათ ოდენობათა ცვლით საჭიროა მათი შენარჩუნება მუდმივ ერთობლივ ტოლობაში. გაჩნდა პირველი სააღრიცხვო წიგნები, რომლებიც შეიცავდა ბუღალტრულ გატარებებს (ტრანზაქციების წინამორბედებს) ორმაგი ჩანაწერის ბაზაზე, გაჩნდა პირველი ბალანსები და ანგარიშები მოგება-წაგების შესახებ. ამ ყველაფრის შედეგად გაჩნდა შესაძლებლობა, საფუძვლები ჩაყროდა უფრო რთულ სამეწარმეო საქმიანობას, ასევე – საშუალება, წარმოქმნილიყო პირველი საკრედიტო ინსტიტუტები. ითვლება, რომ სწორედ შუა საუკუნეების იტალიაში გაჩნდა პირველი ბანკები, კერძოდ – წმინდა გიორგის ბანკი 1407 წელს გენუაში. ორმაგი ჩაწერის პრინციპმა, რომელიც საშუალებას იძლეოდა, შეგვეჯერებინა სახსრების წყაროები და მათი ხარჯვის მიმართულებები, ხელი შეუწყო საბანკო დაკრედიტების სისტემის განვითარებას. ბანკები აქტიურად გასცემდნენ ფულს ვაჭრებზე, დიდგვაროვნებსა და ევროპელ სუვერენებზეც კი. სამაგიეროდ, ბანკირები არა მარტო იღებდნენ მნიშვნელოვან მოგებას კრედიტების პროცენტებიდან,

არამედ შეძლეს მნიშვნელოვნი პოლიტიკური გავლენის მიღწევა, როგორც, მაგალითად, მედიჩების ოჯახი ფლორენციიდან, რომლის წარმომადგენლებიც საბოლოოდ, ტოსკანის ჰერცოგები და მთელი ოლქის მემკვიდრეობითი მმართველები გახდნენ.

ადამიანის ცოდნის შენახვისა და გავრცელების სფეროში მორიგი რევოლუცია 1448 წელს, საბეჭდი დაზგის გამოგონებით, იოჰან გუტენბერგმა მოახდინა. სიზუსტისათვის, ტექსტების ქაღალდსა და ქსოვილზე ბეჭდვის პრინციპები მანამდეც, დაახლოებით IX საუკუნიდან, ცნობილი იყო ჩინეთში. განსხვავება მხოლოდ ის გახლდათ, რომ ქაღალდზე ანაბეჭდის მისაღებად, ტექსტს ცალკეული ლიტერებისგან კი არ აწყობდნენ, არამედ სპეციალურ დაფაზე მთლიან გრავიურას დაატანდნენ. მაგრამ სწორედ ასაწყობი შრიფტის გაჩენამ შექმნა ის აუცილებელი მოქნილობა, თავისუფლება და მოხერხებულობა, რომელიც საჭირო იყო წიგნის ბეჭდვის განსავითარებლად. საბეჭდი დაზგის გამოგონებამ საშუალება მოგვცა გაგვევრცელებინა მეცნიერული ცოდნა აქამდე არნახული სისწრაფით, რამაც საბოლოოდ, კაცობრიობა ახალი დროის სამეცნიერო რევოლუციამდე მიიყვანა. წინაპრებისაგან მემკვიდრეობით მიღებული მსოფლიო მოწყობის ტრადიციული ხედვა ძირეულად გადაიხედა ისეთი მეცნიერების მიერ, როგორებიც იყვნენ კოპერნიკი, გალილეი და ნიუტონი.

ადამიანები დიდი ხანი ფიქრობდნენ, როგორ შეექმნათ მექანიზმები, რომლებსაც არ დასჭირდებოდა ადამიანის ან ცხოველის კუნთების ძალის გამოყენება. ჩვენი წელთაღრიცხვის I საუკუნის მეორე ნახევარში ბერძენმა მათემატიკოსმა და მექანიკოსმა ჰერონ ალექსანდრიელმა (უფრო ცნობილია როგორც „მექანიკის ოქროს წესის“ გამომგონებელი) ორთქლის ძრავას პირველი მოდელი შექმნა. მიუხედავად აპარატის უკიდურესი პრიმიტიულობისა, მის საფუძველაზე ჰერონმა ისეთი მოწყობილობები ააგო, როგორებიც იყო: წყლის ორთქლით მბრუნავი სფერო, კარის ავტომატურად გაღების მექანიზმი და „წმინდა“ წყლის გასაყიდი ავტომატიც კი. იმ დროს ცოდნის გავრცელების ძალზე დაბალი დონის გამო, ჰერონის მართლაც რომ რევოლუციური გამოგონება დავიწყებას მიეცა თითქმის ჩვიდმეტი ასწლეულით, თუ არ ჩავთვლით XVI-XVII საუკუნეებში წყლის ორთქლზე ჩატარეულ ცალკეულ ექსპერიმენტებს, რომლებსაც ეგვიპტელი და იტალიელი ინჟინრები აწარმოებდნენ. მხოლოდ 1781 წელს შოტლანდიელმა ინჟინერ-გამომგონებელმა ჯეიმს უატმა დააპატენტა

საკუთარი ორთქლის ძრავა, რომელიც ხელახლა იქნა აღმოჩენილი და ფაქტობრივად, ინგლისურ სამრეწველო რევოლუციას ჩაუყარა საფუძველი. ჰერონის ორთქლის ძრავა ასე დიდი ხნით რომ არ დაევიწყებინათ, ტექნოლოგიური რევოლუცია შეიძლება, ბევრად უფრო ადრე შემდგარიყო, და ვინ იცის, უკვე IX საუკუნისათვის, ანუ კარლოს დიდის ეპოქაში, კაცობრიობას შეიძლება, კოსმოსური სივრცის ათვისების პროცესიც დაეწყო. თუმცა, სამწუხაროდ, ეს ერთადერთი სერიოზული გამოგონება როდია, რომელიც დავიწყებული იქნა კაცობრიობის ისტორიის ძალზე ხანგრძლივი პერიოდით.

1936 წელს ავსტრიელმა არქეოლოგმა ვილჰელმ კიონინგმა ბაღდადის გარეუბანში აღმოაჩინა უცნაური საგანი – დაახლოებით 13 სანტიმეტრის სიმაღლის კერამიკის მომცრო ჭურჭელი, რომელსაც ყელი ფისით ჰქონდა ამოვსებული და საიდანაც რკინის ღეროს ბოლო იყო ამოჩრილი. კერამიკის სტილის მიხედვით, ნაპოვნი ნივთი სასანიდთა იმპერიის ეპოქას (ა.წ. 224-651 წლები) მიაკუთვნეს. არქეოლოგმა ივარაუდა, რომ ეს ჭურჭელი არის გალვანური ელემენტის პრიმიტიული ფორმა, სხვაგვარად რომ ვთქვათ, ბატარეა, რომელიც ელექტროდენის გამოსამუშავებლად იყო განკუთვნილი. ზუსტად არ არის ცნობილი, გამოიყენებოდა თუ არა „ბაღდადის ბატარეა“, როგორც მას უწოდეს, ამ დანიშნულებით. ცნობილია რიგი სკეპტიკოსების აზრები, რომ ეს ნაკლებსავარაუდოა, რადგან ნაპოვნი არ ყოფილა რაიმე თანმდევი ნივთი, რომელსაც მოცემული „ბატარეა“ გამოკვებავდა. მაგრამ ზოგიერთი მეცნიერი მაინც თვლიდა, რომ, მაგალითად, გალვანიზაციის პროცესი (ერთი მეტალის დაფარვა მეორე მეტალის თხელი ფენით ელექტროლიზის ხერხით) ცნობილი იყო მინიმუმ 2000 წლის წინ. ასეა თუ ისე, ძველ საბერძნეთში ადამიანებმა ყურადღება მიაქციეს იმას, რომ შალზე ქარვის ხახუნის შედეგად ის მსუბუქ ნივთებს იზიდავდა. ამგვარად, კაცობრიობა ჯერ კიდევ გაუაზრებლად გადააწყდა მოვლენას, რომელსაც შემდგომში „ელექტრობას“ დაარქმევენ, რაც პირდაპირ თარგმანით, სწორედ „ქარვიანობას“ ნიშნავს. ისევე, როგორც ორთქლის ძრავას შემთხვევაში, ელექტრობის შესწავლისადმი სისტემური მიდგომა მხოლოდ XVIII საუკუნის მეორე ნახევარში დაიწყო, ხოლო მასთან დაკავშირებული მეცნიერული კანონები კიდევ ერთი საუკუნის შემდეგ ჩამოყალიბდა. კაცობრიობის სამსახურში ჩაყენებულმა ელექტრობამ ცივილიზაციის სახე შეცვალა. განათება, გათბობა, მექანიზმების ამოძრავება, ინფორმაციის გადა-

ცემა – ეს ყველაფერი ელექტრობის საშუალებით ხორციელდება და თანამედროვე ადამიანს ვერც კი წარმოუდგენია ამ ძალზე ფასეული სამეცნიერო მიღწევის გარეშე ცხოვრება, რომელმაც გზა გაგვიხსნა უფრო მნიშვნელოვანი გამოგონებებისკენ.

ფარადეის, მაქსველისა და ჰერცის მიერ ელექტრომაგნიტური გამოსხივების კვლევებმა გამოიწვია ისეთი მოწყობილობების შექმნა, რომლებიც საშუალებას იძლეოდა, ინფორმაცია გადაეცათ მანძილზე – ჯერ ტელეგრაფით (სადენების საშუალებით), შემდეგ შეიქმნა რადიო (უსადენოდ). გაჩნდა რეზისტორები, კონდენსატორები, ტრანსფორმატორები, ელექტრონულო გასაღებები, ვაკუუმის ელექტროლამპები და სხვა ელექტროკომპონენტები. მათ ბაზაზე შეიქმნა და განვითარდა სხვადასხვა სახის ელექტროხელსაწყოები – როგორც სამრეწველო, ისე საყოფაცხოვრებო დანიშნულებისა. 1946 წელს აშშ-ში გამოჩნდა პირველი ელექტროგამომთვლელი მანქანა ENIAC, რომელიც ელექტროლამპებზე მუშაობდა. მისი წონა 27 ტონას შეადგენდა, ხოლო გამოთვლითი სიმძლავრე წამში 5 000 ოპერაციას აღწევდა. შემდგომში კომპიუტერების დამზადებისას უარი თქვეს უზარმაზარ და ექსპლუატაციაში ჭირვეულ ელექტროლამპებზე და ნახევარგამტარების ტექნოლოგიებზე გადავიდნენ. კომპიუტერები ძალზე შემცირდა ზომებში, ამავდროულად, საგრძნობლად იზრდებოდა მათი გამოთვლითი სიმძლავრეები. 1971 წელს მიკროპროცესორის გამოგონებამ უკვე რამდენიმე წელიწადში პერსონალური კომპიუტერების შექმნას შეუწყო ხელი. დაახლოებით იმავე დროს დაიწყო ელექტრონული საფოსტო შეტყობინებების გაცვლისათვის საჭირო გლობალური სატელეკომუნიკაციო ქსელის შექმნის პირველი ექსპერიმენტები. შემდგომში ეს წამოწყება იმაში გადაიზარდა, რაც ახლა ჩვენთვის ინტერნეტის ქსელად არის ცნობილი. მისი საშუალებით კაცობრიობამ მიიღო უნიკალური შესაძლებლობა, განსაკუთრებულად სწრაფად და მნიშვნელოვანი მოცულობებით დააგროვოს, გაავრცელოს და მიიღოს ინფორმაცია ადამიანის ცოდნის ყველა სფეროში. მსოფლიოში მორიგი ტექნოლოგიური რევოლუცია მოხდა, რომელმაც კვლავ დაუჯერებლად შეცვალა გარემო და ადამიანს საშუალება მისცა, ცივილიზაციის განვითარების ახალი ფურცელი გადაეშალა.

XX საუკუნის 90-იანი წლებიდან ინტერნეტი საკმაოდ ფართოდ გავრცელდა, ხოლო XXI საუკუნის დასაწყისისთვის ადამიანებისათვის

პრაქტიკულად პირველი მოთხოვნილების საგანი გახდა, რომელსაც აქტიურად იყენებენ. კომერციული საწარმოებისა და სახელმწიფო სამსახურების უდიდესმა ნაწილმა შექმნა საკუთარი წარმომადგენლობა ინტერნეტში, უმარტივესი „საშინაო გვერდებიდან“ – მასშტაბურ პორტალებამდე, რომლებშიც შესაძლებელია აუცილებელი ინფორმაციის მიღება, მომსახურების შეკვეთა ან რაიმე პროდუქტის შეძენა. სოციალური ქსელების განვითარებასთან ერთად, ინტერნეტის შეჭრა ყოველდღიურ ცხოვრებაში მრავალჯერ გაიზარდა. დაიწყო მასობრივი ინფორმაციის ტრადიციული საშუალებების – ბეჭდვითი გამოცემების, ტელევიზიის, რადიოს შევიწროების პროცესი. ინტერნეტ-მაღაზიებმა მნიშვნელოვანი კონკურენცია გაუწიეს ჩვეულებრივ მაღაზიებს, ხოლო უმრავლესობა ფინანსური ოპერაციებისა საბანკო ოფისებში მისვლის გარეშე ტარდება, ამის მაგივრად, საბანკო ინტერნეტ-დანართებით სარგებლობენ. საფინანსო ბროკერებთან სატელეფონო ზარები შეცვალა ოპერაციებმა ინტერნეტ-პლატფორმების საშუალებით. მომხმარებლებს გაუჩნდათ შესაძლებლობა, გაეერთიანებინათ და თვალსაჩინო გაეხადათ მთელი აუცილებელი ინფორმაცია საინვესტიციო გადაწყვეტილების კომფორტულად მისაღებად, რადგან ახლა მათ წვდომა აქვთ კოტირებებზე, საფინანსო ინსტრუმენტების გრაფიკებზე, ანალიტიკურ ანგარიშებსა და საბაზრო პროგნოზებზე.

ლოგიკურია ვიფიქროთ, რომ ყოველი ახალი რევოლუციური გამოგონება ცარიელ ადგილზე არ ჩნდება, მას წინ უსწრებს ისეთივე მასშტაბური და მნიშვნელოვანი აღმოჩენები, რომლებიც ქმნის უწყვეტ ჯაჭვს, გაჭიმულს საუკუნეთა სიღრმეში, თანამედროვე სამყაროდან – უძველეს დრომდე. ყოველი ტექნოლოგიური რევოლუცია ხდებოდა თავისებური პასუხი ცივილიზაციის მოთხოვნაზე, რომელიც ისტორიული ვითარებების ზემოქმედებით ყალიბდებოდა. ამ წიგნის ერთ-ერთი მიზანია, მკითხველამდე მიიტანოს აზრი, რომ ბლოკჩეინი წარმოადგენს კაცობრიობის ისტორიისათვის არანაკლებ მნიშვნელოვან მოვლენას, ვიდრე ნებისმიერი ზემოთ ჩამოთვლილი გამოგონება. განაწილებული რეესტრის ტექნოლოგიის ბაზაზე კრიპტოვალუტების შექმნა – ესეც ცივილიზაციის პასუხის თავისებური ფორმაა ვითარებათა იმ კომპლექსზე, რომელიც თანამედროვე საფინანსო სამყაროში ჩამოყალიბდა, ამდენად, მომდევნო თავებში მოტანილი არგუმენტების მიზანია, ამ დებულების სამართლიანობაში დაარწმუნოს მკითხველი.

ბლოკჩეინის სტრუქტურის შესავალი

თავისთავად ბლოკჩეინ-ტექნოლოგია არ შეიცავს პრინციპულად რაღაც ახალს ან მეცნიერებისათვის აქამდე უცნობს. ბლოკჩეინის ფუნქციონირების მოდელის ღირებულება სხვადასხვა ინსტრუმენტის, ტექნოლოგიებისა და პრინციპების კომბინირებაშია, რომლებიც გარკვეული სახით შეთავსებისას აყალიბებს ლოგიკურ და დაცულ სტრუქტურას მონაცემთა განაწილებული შენახვისათვის. რას წარმოადგენს ბლოკჩეინი? ფაქტობრივად, ის შეიძლება შევადაროთ დიდ საბუღალტრო წიგნს, რომლის გვერდებზეც იწერება კონტრაგენტებს შორის ჩატარებული ფინანსური ოპერაციები. ოღონდ ეს წიგნი ისეა შედგენილია, რომ ყოველი ჩანაწერი, რომელიც მასში ხვდება, შემდგომში არანაირად არ შეიძლება წაიშალოს ან შეიცვალოს, ამას ხელს შეუშლის ტექნოლოგიაში ინტეგრირებული სერიოზული კრიპტოგრაფიული ალგორითმები. თვით მონაცემები კი ინახება არა კონკრეტულად მმართველი ცენტრის სტატუსის მქონე რომელიმე ადგილზე, არამედ კოპირდება და სინქრონიზდება ან, სხვაგვარად რომ ვთქვათ, მეორდება (რეპროდუცირდება) და ნაწილდება სისტემის ყველა მონაწილეს შორის – ქსელის კვანძებს შორის. ამგვარად, ვინმემ რომც მოინდომოს თავისთან შენახული მონაცემების შეცვლა, სისტემის სხვა მონაწილენი უბრალოდ, ყურადღებასაც არ მიაქცევენ ამ ცვლილებებს, რადგან ისინი სისტემაში მიღებული წესების საწინააღმდეგოდაა განხორციელებული.

როგორ არის მოწყობილი ასეთი „საბუღალტრო წიგნი“? მის „გვერდებს“ ეწოდება ბლოკები. ისევე, როგორც გვერდები ჩვეულებრივ წიგნში, ბლოკები მისდევს ერთმანეთს მკაცრად დანომრილი მიმდევრობით. მაგრამ, თუ ჩვეულებრივ წიგნში გვერდი შეიძლება ამოვიღოთ, ან გადავაადგილოთ, ან საერთოდაც გადავაგდოთ, ბლოკებს ასე ვერ მოვეპყრობით. ყველა ბლოკი ხისტად არის მიბმული ერთმანეთზე სპეციალური კრიპტოგრაფიული „ბოქლომებით“, რომელთა გატეხაც, თუნდაც თეორიულად, განსაკუთრებულად რთულია. სწორედ აქედა-

ნაა წარმომდგარი „ბლოკჩეინის“ ტექნოლოგიის სახელწოდება, ინგლისურად blockchain „ბლოკების ჯაჭვს“ ნიშნავს. იმისათვის, რომ მონაცემთა საიმედო საცავი იყოს, ნებისმიერმა ბლოკჩეინ-სტრუქტურამ უნდა დააკმაყოფილოს შემდეგი კრიტერიუმები:

- უნდა ჰქონდეს დეცენტრალიზებული ტექნოლოგიური საფუძველი, ანუ უნდა შეეძლოს აუცილებელ მონაცემთა ქსელის ყველა კვანძში გავრცელება და მათი ქმედით მდგომარეობაში შენარჩუნება რეპროდუცირებისა და სინქრონიზაციის პროცესების საშუალებით.
- შეინარჩუნოს უწყვეტი კავშირი მონაცემთა ბლოკებს შორის ყოველ ახალ ბლოკში მის მიმართ წინამდებარე ბლოკზე ბმულის შექმნის გზით.
- შეეძლოს მონაცემთა ნაკრებების დაშიფვრა სტანდარტული ზომის უნიკალურ საინფორმაციო ბლოკებში, სხვაგვარად რომ ვთქვათ – მონაცემთა ჰეშირება.
- გამოიყენოს გატეხისადმი განსაკუთრებულად მედეგი კრიპტოგრაფიული ალგორითმები, რომლებიც აუცილებელია ბლოკებში ჩაწერილი მონაცემების დასაცავად.
- გამოიყენოს მათემატიკის სპეციალური ქვეთავი – თამაშთა თეორია – იმისათვის, რომ სისტემის ყველა კვანძმა დაიცვას დადგენილი წესები და ემსახუროს საერთო კონსენსუსის მიღწევას ახალი ბლოკების შექმნისას და მათში მონაცემთა ჩაწერისას.

ყველა ზემოთ ჩამოთვლილი ამოცანა შეადგენს ხუთ ძირითად „სვეტს“, რომელზეც დაფუძნებულია ბლოკჩეინ-ტექნოლოგია. შემდგომში ყოველ მათგანს საკმაოდ დაწვრილებით განვიხილავთ. მკითხველებს შეიძლება გაუჩნდეთ კითხვა: მაინც სად არის ბლოკჩეინში საკუთრივ ფული? როგორ ხვდება იქ, სად ინახება, როგორ მივიღოთ და შემდეგ როგორ დავხარჯოთ? და მთავარი, როგორაა ეს ფული დაცული ბოროტმოქმედთა ხელყოფისაგან? ყველას ყურში ჩაესმის „კრიპტოვალუტა“, რომელიც მტკიცედ ასოცირდება ბლოკჩეინ-ტექნოლოგიასთან. უფრო მეტიც, ბლოკჩეინის მიმართ ადამიანთა წმინდა ტექნოლოგიური ინტერესი, როგორც წესი, მეორადია. მაგრამ იმის საცდელად, რომ კრიპტოვალუტაში ინვესტიციების შედეგად

მოგება მივიღოთ, აუცილებელია თუნდაც საბაზო დონეზე გვესმოდეს მისი მუშაობის პრინციპი.

სინამდვილეში კრიპტოვალუტები არის მხოლოდ ერთ-ერთი შესაძლო „ზედნაშენი“ ბლოკჩეინ-სტრუქტურებზე, უფრო ზუსტად, მისი უტილიტარული გამოყენების ერთ-ერთი ფორმაა. ისტორიულად ასე ჩამოყალიბდა, რომ ამ ბაზაზე რეალიზებული პირველი პროექტი, ბიტკოინი, წარმოადგენს კრიპტოვალუტით გადახდის სისტემას, თანაც, საკმაოდ ღარიბს თავისი ფუნქციური შესაძლებლობებით, რაც შეიძლება შევუნდოთ როგორც სიახლის შემომტან პროექტს. მიუხედავად იმისა, რომ ცნებები – „ბიტკოინი“ და „ბლოკჩეინი“ – ერთდროულად გაჩნდა, მათი მნიშვნელობა სინონიმური სულაც არ არის, რადგანაც პირველი აღნიშნავს კრიპტოვალუტას, ხოლო მეორე – საკუთრივ ტექნოლოგიას, რომელიც ამ კრიპტოვალუტის ხორცშესხმის შესაძლებლობას იძლევა. უნდა ითქვას, რომ ტერმინი „კრიპტოვალუტა“ გაჩნდა რამდენიმე წლით გვიან, ვიდრე საკუთრივ ბიტკოინის პროექტი – 2011 წელს ჟურნალ Forbes-ში სტატიაში CryptoCurrency. თვით ბიტკოინის ავტორი სატოში ნაკამოტო მას e-cash-ს ან „ელექტრონულ ფულს“ უწოდებდა. ბიტკოინის პროექტს ვრცლად სასაუბროდ დავუბრუნდებით იმ თავში, რომელიც ბლოკჩეინ-ტექნოლოგიის პრაქტიკულ რეალიზებას ეთმობა.

მართვის დეცენტრალიზაცია

ურთიერთდაკავშირებულ და ურთიერთმოქმედ კომპონენტთა ნებისმიერ წყებას მართვა ესაჭიროება. ეს ნამდვილად, ნებისმიერ სისტემას ეხება – საზოგადოების სხვადასხვა სოციალური ორგანიზაციის ფორმებიდან დაწყებული, აპარატულ-პროგრამული ტექნოლოგიური კომპლექსებით დამთავრებული. უამისოდ, მათი პროექტირებისა და შექმნისას დაგეგმილი ფუნქციურობის რეალიზება გარანტირებული ვერ იქნება, რადგან სისტემების უმრავლესობას ეფექტიანი თვითორგანიზების უნარი არ გააჩნია. მმართველობის პრობლემატიკას კაცობრიობა მთელი თავისი ისტორიის მანძილზე აწყდებოდა.

მართვის სისტემების სხვადასხვა ფორმის განხილვისას, მისი ორი ძირითადი სახეობა შეიძლება გამოვყოთ: ცენტრალიზებული და დეცენტრალიზებული.

ისტორიულად, საზოგადოების მართვის ყველაზე ადრეული ფორმა ბუნებრივად ჩამოყალიბდა პირველყოფილი ადამიანების დროს, როდესაც გვაროვნულ და ტომობრივ ჯგუფებს ჰქონდათ მკაცრი მმართველობითი იერარქია, რაც შეეხება მთელი მოსახლეობის მართვას, აქ მხოლოდ უკიდურეს დეცენტრალიზაციაზე შეიძლება ლაპარაკი. უფრო მეტიც, უმრავლეს შემთხვევაში, თითოეული ჯგუფი განსხვავებულ მმართველობით გაერთიანებას წარმოადგენდა, ამიტომ სახეობა Homo Sapiens-ის მოსახლეობის მთელი ერთობლიობა ძნელია წარმოვიდგინოთ ერთიან, თუმცა დეცენტრალიზებულ სისტემად. მართლაც, ჯგუფებს შორის მმართველობითი კავშირები არ არსებობდა, ხოლო თუკი ურთიერთქმედება ხდებოდა, ის მხოლოდ დესტრუქციულ ხასიათს ატარებდა. ჩვეულებრივ, ის მიმართული იყო უფრო ძლიერი ჯგუფების მხრიდან უფრო სუსტების განადგურებისაკენ ან საუკეთესო შემთხვევაში მათი ასიმილაციისაკენ. ჯგუფებს შორის სოციალური ურთიერთდამოკიდებულების განვითარებასთან ერთად, მათ შორის გაჩნდა მყარი კავშირები, რომლებმაც საბოლოოდ წარმოშვა უფრო რთული იერარქიული სისტემები, სათავეში არსებული მადომინირებელი ელემენტებით. როგორც კი ურთიერთ-

დაკავშირებული ჯგუფების რაოდენობა იერარქიების შიგნით შედარებით დიდი ხდებოდა, სისტემა ცენტრალიზებული მოდელის სახეს იღებდა. სხვაგვარად რომ ვთქვათ, ადამიანებმა შექმნეს ცნება „მმართველობა“ („მთავრობა“), რომლის სათავეშიც ერთპიროვნული – არჩევითი ან მემკვიდრეობითი – მმრთველი დადგა. მმართველობის ასეთი ფორმა სავსებით სიცოცხლისუნარიანი აღმოჩნდა, რადგან ჩვენს დრომდე მოაღწია, თუმცა, მრავალგვარი ცვლილება განიცადა.

ამგვარად, დადასტურებულად შეგვიძლია ვთქვათ, რომ საზოგადოების ორგანიზების აუცილებელმა დეცენტრალიზებულმა ფორმებმა ჩამოყალიბების ადრეულ სტადიებზე ევოლუცია განიცადა იმ მომენტისათვის უფრო პროგრესული ცენტრალიზებული მიდგომის მიმართულებით. ცენტრალიზაციამ წარმოშვა რესურსების თავმოყრის შესაძლებლობა, რომელმაც მართვადი პროექტების – დაპყრობითი ომების ან მასშტაბური მშენებლობების, ზოგჯერ კი, ორივეს – განხორციელების საფუძველი შექმნა. ისეთი უძველესი სახელმწიფოების ისტორია, როგორებიცაა ბაბილონი ან ეგვიპტე, ამის თვალსაჩინო მაგალითებს წარმოადგენს. ამასთანავე, უკვე შუა საუკუნეებში, მმართველობის სხვა ფორმებიც გაჩნდა. თუმცა, ცვლილებები მმართველობითი პრინციპების ევოლუციის შედეგი როდი იყო; ნაცვლად ამისა, გარკვეულ შემთხვევებში, პოლიტიკური გარემოებები ხელს არ უწყობდა ეფექტიანი ცენტრალიზებული მმართველობითი მოდელების შექმნას.

ამის კარგი მაგალითია კათოლიკური ეკლესია, რომელმაც – მართალია, მრავალსაუკუნეობრივი ბრძოლის შედეგად, – შუა საუკუნეების ევროპაში დამოუკიდებელი ზესახელმწიფოებრივი ინსტიტუციის დე ფაქტო როლი მოირგო. და თუმცა საკუთრივ კათოლიკური ეკლესიის სისტემა მკაცრად იერარქიული, ხოლო მასში მმართველობა მნიშვნელოვანწილად ცენტრალიზებული იყო, ეკლესიის მღვდელმთავრების არჩევა უდიდეს ევროპულ სახელმწიფოებს შორის პოლიტიკური კონსენსუსის შედეგად ხდებოდა. ახალი ეპოქის დასაწყისში წარმოქმნილმა პროტესტანტობამ თავისი კონფესიური სტრუქტურის ორგანიზაციაში ნამდვილი დეცენტრალიზაცია შემოიღო. პონტიფიკატის ზედამხედველობის ტრადიციული ცენტრალიზებული მართვის საპირისპიროდ, საეკლესიო თემების მართვის პრესვიტერიანული ფორმა გაჩნდა.

სახელმწიფოებიც არ ჩამორჩებოდნენ პროგრესს თავისი მოწყობის ორგანიზაციის ნაწილში: 1291 წელს შუა საუკუნეების ევროპის რუკებზე გაჩნდა ნამდვილად დეცენტრალიზებული სახელმწიფო – შვეიცარიის კონფედერაცია – რამდენიმე დამოუკიდებელი კანტონის კავშირი ცენტრალური მმართველობითი პოლიტიკური ინსტიტუტის ფაქტობრივი არარსებობის პირობებში. ამჟამად, ეს ძველი მოვლენა ღირსეულად შეგვიძლია შევაფასოთ – შვეიცარიამ საუკუნეების მანძილზე არა მარტო არ დაკარგა საკუთარი სუვერენიტეტი, არამედ შეძლო გამხდარიყო მსოფლიოს ერთ-ერთი განვითარებული ქვეყანა. მეორე მხრივ, ისტორიამ იცის არცთუ ცოტა მაგალითი იმისა, რომ დეცენტრალიზაციას სახელმწიფოების ფეოდალური დაქუცმაცების შედეგად, ისინი დასუსტებამდე, ზოგჯერ კი დაღუპვამდეც მიჰყავდა.

ეს მაგალითები მეტყველებს იმ დებულების პირობითობაზე, რომ მართვის ერთ-ერთი ფორმა მეორეზე უკეთესია. რა თქმა უნდა, ორივეს აქვს პლუსები და მინუსები. ვცადოთ გადავიტანოთ ჩვენი ანალიზი საზოგადოებრივი მოწყობის ფორმებიდან ტექნოლოგიურ სისტემებზე. მმართველობის საზოგადოებრივი და ტექნოლოგიური ფორმების მსგავსება ეფუძნება ზოგად პრინციპს, რომელიც სუბიექტის მიერ ობიექტზე მმართველობით ზემოქმედებაზე ვრცელდება. ტექნოლოგიურ მაგალითად განვიხილოთ გლობალური კომპიუტერული ქსელის მართვა. როდესაც ინტერნეტმა ადამიანთა ცხოვრების ყველა სფერო მოიცვა, მისი აქტიური გამოყენება დაიწყეს სხვადახვა სახის – კომერციული, სახელმწიფო, საზოგადოებრივი – ორგანიზაციის სერვისებისათვის. საინტერესოა, რომ ინტერნეტი თავისთავად, დეცენტრალიზებული სტრუქტურაა, თუმცა მას აქვს იერარქიული არსი, განსაკუთრებით – გამოყენების ქვედა დონეებზე.

საბოლოო მომხმარებელი ქსელში ერთვება თავისი პროვაიდერის საშუალებით, მას კი თავის მხრივ, თუ მცირე ორგანიზაციას წარმოადგენს, აქვს მხოლოდ ერთი საგარეო არხი, უფრო მსხვილ ოპერატორთან დასაკავშირებლად. რაც უფრო მსხვილია ქსელის სუბიექტი, მით მეტი კავშირი აქვს სხვა მსხვილ სუბიექტებთან როგორც პირდაპირი შეერთებების, ასევე ქსელური ტრაფიკის გაცვლის პუნქტების საშუალებით. მთელ მსოფლიოში ქსელის ყველაზე მსხვილ ოპერატორებს აქვთ მაგისტრალური არხების საკუთარი ინფრასტრუქტურა და უზრუნველყოფენ ყველაზე მნიშვნელოვან გამტარუნარიანობას გადა-

საცემი მონაცემებისათვის. მიუხედავად ამისა, ინტერნეტს არ აქვს ერთიანი „უარის წერტილი“ ანუ სისტემის ერთი, თუნდაც საკმაოდ მსხვილი მონაწილის გამორთვა არ გამოიწვევს მთელი ქსელის მუშაობის გაჩერებას, გარდა იმ სეგმენტისა, რომელიც მთლიანად იყო „მიბმული“ ქსელიდან ამოვარდნილ მსხვილ კვანძთან. ამასთანავე, ამ სეგმენტის კომპონენტები შეიძლება გადაერთოს სარეზერვო არხებზე და ამგვარად დაბრუნდეს ონლაინ.

სწორედ უარის წერტილის არარსებობაა დეცენტრალიზებული სისტემის ერთ-ერთი მთავარი უპირატესობა. დავუბრუნდეთ შვეიცარიის მაგალითს: ცნობილია, რომ ამ სახელმწიფოს პრეზიდენტს ან სხვა რომელიმე პოლიტიკურ ინსტიტუტს არ აქვს უფლება, გასცეს კაპიტულაციის ბრძანება გარედან საომარი შემოჭრის შემთხვევაში. თუ მაინც გაიცა ასეთი ბრძანება, კანონი ადგილობრივ მცხოვრებლებს კატეგორიულად უკრძალავს მის შესრულებას. ამგვარად, აგრესორს საქმე ექნება ლამის თითოეულ შვეიცარიელთან, ცალ-ცალკე. იგივე ეხება ინტერნეტის ქსელსაც. თუკი რომელიმე ქვეყანა თავისი პოლიტიკური გადაწყვეტილებით მოინდომებს ინტერნეტის გამორთვას, დიდი ალბათობით, ტექნოლოგიურად ამის განხორციელება შესაძლებელი იქნება მხოლოდ საკუთარ ტერიტორიაზე (გარდა კვანძებისა, რომლებიც ინტერნეტს მიერთებულია თანამგზავრული კავშირით, იმ პირობით, რომ თანამგზავრი სხვა სახელმწიფოს ეკუთვნის). შეიძლება დაზარალდნენ სხვა ქვეყნის მომხმარებლებიც, რომელთა მაგისტრალური არხები ჩართულია იმ ქვეყნის სატრანზიტო კვანძებში, რომელმაც გლობალური ქსელიდან გამოთიშვა გადაწყვიტა, მაგრამ მსოფლიოს მთელი დანარჩენი ქსელი ქმედუნარიანობას შეინარჩუნებს.

რეალურად, ინტერნეტის გასანადგურებლად აუცილებელია ყველა მისი კვანძის გამორთვა, რაც თავისთავად, ორგანიზაციულ და ტექნოლოგიურ სირთულეს წარმოადგენს, ეს კი ჩანაფიქრის პრაქტიკულად განხორციელების შეუძლებლობას ესაზღვრება. ამგვარად, შეგვიძლია ვთქვათ, რომ ქსელი თეორიულად არ გამოირჩევა მოწყვლადობით, რაც ერთიანი მმართველობითი ცენტრის გარეშე განაწილებულ ტოპოლოგიას ემყარება. არადა, თუ ინტერნეტქსელის ბაზაზე აგებული სერვისების დონეს გადავხედავთ, დავინახავთ, რომ მათი დიდი უმრავლესობა დაფუძნებულია „კლიენტი-სერვერის“ ტექნოლოგიაზე ანუ – ცენტრალიზებულ ტექნოლოგიაზე.

ყველანი დიდი ხანია შევეჩვიეთ სხვადასხვა ინტერნეტსერვისით სარგებლობას. ელექტრონული ფოსტის სერვისების საყრდენი პორტალები, მონაცემთა (მაგალითად, დოკუმენტებისა და ფოტოების) შენახვის ღრუბლოვანი სისტემები, „ბანკი-კლიენტის“ სისტემაზე წვდომა საკუთარი ანგარიშების სამართავად და გადახდების განსახორციელებლად, სასტუმროებისა და ავიაბილეთების დაჯავშნა, სავაჭრო პლატფორმები საფინანსო ბაზრებზე გარიგებების განსახორციელებლად და ბევრი სხვა მსგავსი სერვისი აგებულია ცენტრალიზებული ინფრასტუქტურის ბაზაზე. ყოველი ასეთი სისტემით სარგებლობისას, იმისათვის, რათა მივიღოთ წვდომა რესურსებსა და მომსახურებაზე, აუცილებელია ვეწვიოთ კონკრეტული მომსახურების მომწოდებლის სოციალურ საიტს, შევიყვანოთ ჩვენი სახელი და პაროლი და შევუერთდეთ ცენტრალურ სერვერს, სადაც ინახება კლიენტის მონაცემები ან მისი აქტივები. მაგრამ, თუ მომწოდებლის ცენტრალური სერვერი რაიმე მიზეზის გამო გაითიშა, აღნიშნული მომსახურებით ვერ ვისარგებლებთ და მოგვიწევს მოცდა, სანამ სერვერი კვლავ ამუშავდება. მსგავს შემთხვევაში ვაწყდებით ცენტრალიზებული სისტემების მთავარ პრობლემას – „უარის წერტილის“ არსებობას. მომსახურებაზე უარის თქმა შეიძლება იყოს სხვადასხვა ფაქტორის მოქმედების შედეგი: ტექნოლოგიური პრობლემების, მოწყობილობის მწყობრიდან გამოსვლის, პროგრამულ უზრუნველყოფაში შეცდომების, თვით მომსახურების სტრუქტურის შიგნით მომწოდებლის მიერ ჩადენილი დარღვევების, ჰაკერთა სხვადასხვა სახის შეტევების ან კომპიუტერული ვირუსების მოქმედების. უკანასკნელ როლს არც სახელმწიფოს ძალოვანი ან მარეგულირებელი სტრუქტურების რეპრესიული ზემოქმედება ასრულებს, იმ სამართლებრივ ტერიტორიაზე, სადაც ფიზიკურადაა განლაგებული მომსახურების მომწოდებელი.

ყველა ეს ფაქტორი, რომლის ზემოქმედების შედეგიც არის მომსახურებაზე უარის თქმა, გვაიძულებს იმაზე დაფიქრებას, თუ როგორ შეგვიძლია ტექნოლოგიურად ან ორგანიზაციულად თავიდან ავიშოროთ მსგავსი სიტუაციები. ამ კითხვაზე პასუხი გაგვცა ბლოკჩეინ-ტექნოლოგიების გაჩენამ, რომელიც აგებულია დეცენტრალიზებულ სისტემაზე მონაცემთა შენახვისა და გაცვლისათვის, რაც გამორიცხავს ყველა ნეგატიურ ფაქტორს, სერვისების ცენტრალიზაციისას ბუნებრივად რომ წარმოიქმნება. ნაცვლად ქსელური ტოპოლოგია „ვარსკ-

ვლავისა“, რომლის სხივებიც ყველა მომხმარებლის კვანძებიდან აუცილებლად მიდის ცენტრალურ წერტილში – სერვერში, – გაჩნდა ორგანიზაციული ფორმა, რომელშიც თვით ცნება „ცენტრალური სერვერი“ არ არსებობს, ხოლო ყველა ურთიერთქმედება პირდაპირ კლიენტების კვანძებს შორის ხორციელდება. ასეთ ქსელებს ასევე „ერთრანგიანს“ ან „პირინგულს“ უწოდებენ. ყველა კვანძი ასეთ ქსელში უმრავლეს შემთხვევაში, თანაბარუფლებიანია, და ყოველ მათგანს შეუძლია შეასრულოს როგორც კლიენტის, ასევე სერვერის ფუნქციები. ქსელის ასეთი დეცენტრალიზებული ტოპოლოგია თავიდან გვაცილებს „უარის წერტილის“ ფაქტორს, ზრდის სისტემის საიმედოობისა და შრომისუნარიანობის ხარისხს აბსოლუტურთან ახლოს მდგომ სიდიდემდე.

მკითხველს შეიძლება გაუჩნდეს სავსებით სამართლიანი კითხვა: თუ სერვერები თავისთავად, ქსელში არ არსებობს, მაშ, როგორ ინახება ასეთ სისტემაში საერთო მონაცემები, როგორ ვრცელდება ისინი ქსელით და როგორ არის ისინი დაცული არასანქცირებული წვდომის ან ცვლილებებისაგან? და კიდევ, როგორ ხდება ასეთი სისტემების მომსახურება და განვითარება, თუკი ქსელის ყველა მონაწილეს თანაბარი უფლებები აქვს? ბლოკჩეინ-ტექნოლოგია უზრუნველყოფს ამ კითხვათა უმრავლესობაზე პასუხის გაცემას. მონაცემები კოპირდება სისტემის ყველა კვანძს შორის. ცვლილებებისა და არასანქცირებული წვდომისაგან დაცვას უზრუნველყოფს ასიმეტრიული კრიპტოგრაფიის მათემატიკური ალგორითმები. მთელი სისტემა ფუნქციონირებს მოცემული წესების წყებაზე დაყრდნობით, რომელსაც სისტემის ყველა მონაწილე ეთანხმება. იმ შემთხვევაში, როდესაც აუცილებელია მნიშვნელოვანი ცვლილებების შეტანა, გადაწყვეტილება მიიღება სისტემის მონაწილეთა საერთო კენჭისყრით.

უნდა აღინიშნოს, რომ დეცენტრალიზებული სისტემების ადმინისტრირება გაცილებით რთულია, ვიდრე ცენტრალიზებულების. მაგრამ ეს შეიძლება განვიხილოთ როგორც იმ უპირატესობების საფასური, რომლებსაც დეცენტრალიზაცია იძლევა. სადღეისოდ, კიდევ ბევრი პრობლემა რჩება, რომლებიც დეცენტრალიზებული სისტემების მართვისას შეიძლება წარმოიშვას. ჩვენც არაერთხელ დავუბრუნდებით ამ პრობლემატიკის განხილვას მომდევნო თავებში.

ინფორმაციის ჰეშირება

მონაცემთა ჰეშირების ინსტრუმენტი ბლოკჩეინ-ტექნოლოგიის მნიშვნელოვან და განუყოფელ ნაწილს წარმოადგენს. ჰეშირება გამოიყენება ბლოკჩეინ-სისტემებში მისამართების თავმოყვრისთვის, შეტყობინებების ციფრული ელექტრონული ხელმოწერის შესაქმნელად, აგრეთვე კრიპტომონეტების საწარმოებლად (ე.წ. მაინინგისათვის) ზოგიერთ ბლოკჩეინ-პროექტში, რომლებიც აგებულია პრინციპზე „მუშაობის დადასტურება“. სანამ განვიხილავდეთ ბლოკჩეინ-სისტემების ზემოთ ხსენებულ კომპონენტებს, მოგვიწევს იმის გარკვევა, თუ მაინც რას წარმოადგენს მონაცემთა ჰეშირება და რა პრინციპების საფუძველზე მუშაობს ეს პროცედურა.

დავიწყოთ განმარტებით. ჰეშირება არის ნებისმიერი ზომის მონაცემთა ერთობლიობის გარდაქმნის მეთოდი ფიქსირებული სიგრძის სტანდარტიზებულ სტრიქონად სპეციალური ალგორითმის საშუალებით. ანუ, თუ ავიღებთ მონაცემთა რაღაც ერთობლიობას, მაგალითად, ამ წიგნის მთელ ტექსტს, მაშინ შეიძლება მისი ციფრული ანაბეჭდის შექმნა, ვთქვათ, ათი სიმბოლოს სიგრძისა. ამასთან, უნდა განვსაზღვროთ შემომავალ მონაცემთა ზუსტი ალგორითმი და უცვლელად გამოვიყენოთ ის ყველა სხვა ნებისმიერი ზომის მონაცემისთვის, რომ მივიღოთ გამოსვლისას ათი სიმბოლოსაგან შემდგარი სტანდარტული სტრიქონი. ასევე ამბობენ, რომ ასეთ შემთხვევაში გამოიყენება „დეტერმინირებული ალგორითმი“ იმიტომ, რომ ის ყოველთვის იძლევა წინასწარ განსაზღვრულ შედეგს. ფაქტობრივად მისაღები შედეგი უნდა გახდეს გარდასასახი შემომავალი მონაცემების უნიკალური ასახვა. ამისათვის უნდა შევქმნათ გარდასახვის ისეთი ალგორითმი, რომელიც არც ერთ შემთხვევაში არ დაუშვებს გარდასახვის ერთნაირ შედეგებს შემომავალი მონაცემების სხვადასხვა ერთობლიობისათვის ანუ არ შექმნის ე.წ. „კოლიზიებს“. ამასთან, უმცირესმა – თუნდაც ერთბიტიანმა – ცვლილებამ შემომავალ მონაცემებში აბსოლუტურად უნდა უცვალოს სახე გამომავალ ჰეშს. აი, მაგალითი ჰეშირების ერთ-ერთი ყველაზე მარტივი ალგორითმის (SHA-1)

მუშაობისა, სადაც ჰეშების პირველსახეებს წარმოადგენს ინგლისური სიტყვის – „დეცენტრალიზაცია“ ორი ვარიანტი, ამასთან, მეორე სიტყვაში შეცვლილია მხოლოდ ერთი ასო:

Decentrali**z**ation	9ffefb933ed06a04b99dd172c8ee73f59ac7fc3d
Decentrali**s**ation	10406aa1f6c0c1610fa15455a6e43c73484dda32

როგორც მიღებული შედეგებიდან ჩანს, მეორე ჰეშს საერთო არაფერი აქვს პირველთან, თუმცა ამოსავალ პირველსახეებში განსხვავება მინიმალურია. მკითხველი ალბათ დასვამს კითხვას: საერთოდ, რისთვისაა ეს საჭირო? სინამდვილეში ჰეშირება განსაკუთრებულად სასარგებლო ფუნქციაა, რომელიც საკმაოდ ფართოდ გამოიყენება კომპიუტერულ ტექნოლოგიებში.

წარმოვიდგინოთ სიტუაცია, რომ აუცილებლად გვჭირდება, კავშირის არხების მეშვეობით გადავცეთ მონაცემთა მნიშვნელოვანი მოცულობა, რომლებშიც ამა თუ იმ მიზეზით შეიძლება წარმოიშვას დაბრკოლებები და ხარვეზები. როგორ უნდა შევამოწმოთ, მივიდა თუ არა მონაცემები საბოლოო მომხმარებლამდე საწყისი სახით? სანამ არ შევადარებთ საწყისი ინფორმაციის ყოველ ბიტს მიღებულთან, დანამდვილებით ვერ ვიტყვით, რომ მონაცემთა გადაცემა შეუცდომლად მოხდა. გარდა ამისა, იქნებ მონაცემთა გადაცემისას ვიღაც უცხო ჩაერია და განგებ შეცვალა ინფორმაცია? კიდევ, როგორ მოვიქცეთ, თუ ინფორმაციის მოცულობა გიგაბაიტებით იზომება? ორი უზარმაზარი საინფორმაციო ბლოკის შედარების პროცესმა შეიძლება ბევრი დრო წაიღოს. უფრო მარტივი ხომ არ იქნება, თუ მონაცემთა გადასაცემ ბლოკს დავურთავთ ჰეშირების საყოველთაოდ ცნობილი ალგორითმის ბაზაზე შექმნილ უნიკალურ მოკლე „ციფრულ ანაბეჭდს“? მაშინ მიღებისას შეგვიძლია კიდევ ერთხელ გავუშვათ იგივე ალგორითმი, შესასვლელში მივაწოდოთ მიღებული მონაცემები და შემდეგ უბრალოდ შევადაროთ მიღებელი ჰეში გადასაცემ მონაცემებზე დართულ ჰეშს. თუ ისინი ზუსტად დაემთხვევა, ეს ნიშნავს, რომ გადაცემა მოხდა დამახინჯების გარეშე და გვაქვს მონაცემები, რომლებიც გადასაცემის სრული ანალოგია. ამგვარად ვამოწმებთ მონაცემთა მთლიანობას. ამგვარი შემოწმების ალგორითმის გამოყენე-

ბის პოპულარული ვარიანტია ე.წ. „საკონტროლო ჯამის“ მნიშვნელობის მიღება, რომლის გაანგარიშებაც ეყრდნობა მონაცემთა შემავალი ბლოკის ჰეშირების ალგორითმს.

ლოგიკური მსჯელობით ვასკვნით, რომ სრულიად შეუძლებელია მონაცემთა დიდი ბლოკის გარდაქმნა განსაკუთრებულად მცირედად, საწყისი ინფორმაციის რაღაც ნაწილის დაკარგვის გარეშე. მართლაც ასეა. ჰეშირების ალგორითმი წარმოადგენს ცალმხრივ მათემატიკურ ფუნქციას, რომლის მოქმედების შედეგი პრაქტიკულად შეუძლებელია ვაქციოთ საწყის მონაცემებად გარდაქმნამდე, ანუ გამოთვლითი თვალსაზრისით, ჰეშისაგან ძალზე ძნელია მისი პირველსახის მიღება. თეორიულად ამის განხორციელება შესაძლებელია მხოლოდ ვარიანტთა მიმდევრობითი გარდაქმნით – ე.წ. „უხეში ძალის“ მეთოდის საშუალებით. ეს მეთოდი ეყრდნობა პრინციპს „დაშიფრე და შეადარე“: რომელიღაც ნაგულისხმევი საწყისი მონაცემები ჰეშირდება და შედარდება არსებულ ჰეშთან. თუ ეს ორი ჰეში არ დაემთხვა, მაშინ მოცემული ნაგულისხმევი პირველსახე არ გამოგვადგება. ვცვლით მას და ხელახლა ვაჰეშირებთ, და ასე შემდეგ, უსასრულობამდე მანამ, სანამ ჰეშები მოულოდნელად დაემთხვევა. მხოლოდ მაშინ შეგვეძლება ვთქვათ, რომ „გავშიფრეთ ჰეში“, მაგრამ ასეთი შედეგის მისაღებად საჭირო განსახილველი ვარიანტების რაოდენობა, გადაჭარბების გარეშე, ასტრონომიული სიდიდეებით იზომება.

სიტყვაზე, მოცემული მეთოდი ფართოდ გამოიყენება სხვადასხვა სერვერზე შენახული საიდუმლო პაროლების დასაცავად. ინტერნეტ-საიტებზე მომხმარებელთა პაროლების ღიად განთავსება აშკარად საფრთხის შემცველია, ისინი შეიძლება, ბოროტმოქმედებმა მოიპარონ და შემდეგ სცადონ, სისტემასა და მის მონაწილეებს მატერიალური ზარალი მიაყენონ. მაგრამ თუ პაროლები ინახება დახურული სახით ანუ ჰეშების სახით, მაშინ არასანქცირებული წვდომა მნიშვნელოვნად რთულდება. თუ პაროლი შეჰყავს მის მფლობელს, მაშინ სისტემა აჰეშირებს პაროლს და ადარებს მოცემული მომხმარებლის პაროლის შენახულ ჰეშს. თუ ისინი დაემთხვევა, ეს ნიშნავს, რომ სწორი პაროლია შეყვანილი, და სისტემა მომხმარებელს აძლევს წვდომას. თუ ჰეშები არ დაემთხვევა, მაშინ პაროლი არასწორია. მოპარული ჰეშის ქონა ბოროტმოქმედს სულაც არ უადვილებს ამოცანას, რადგან მისთვის აუცილებელია საწყისი პაროლის აღდგენა ვარიანტების მასშტაბური

გადასინჯვის მეთოდით. გასაგებია, რომ რაც უფრო გრძელია საწყისი პაროლი, მით უფრო მეტია გადარჩევის მაქსიმალურად შესაძლო ვარიანტი. ამიტომ საწყისი პაროლის მისაღებად აუცილებელია, საქმეში ჩავრთოთ განსაკუთრებული გამოთვლითი სიმძლავრეები, რაც საბოლოოდ აისახება შეტევის საერთო ღირებულებაზე, რომელიც უფრო ძვირი შეიძლება იყოს, ვიდრე კონკრეტული პაროლის მორგებით მიღებული შესაძლო მატერიალური სარგებელი.

ჰეშირების ალგორითმით სარგებლობის კიდევ ერთი პოპულარული მეთოდი გამოიყენება ე.წ. ტორენტ-ტრეკერებში. ტორენტები ფაილების გაცვლა-გამოცვლის ტექნოლოგიაა, როგორც წესი – მედიაფაილების (დიდი უმრავლესობა ვიდეოფაილებია). თვით ტექნოლოგიას აქვს ჰიბრიდული მოდელი, როდესაც ტექნიკური ინფორმაციის შემცველი ტორენტ-ფაილები ცენტრალიზებულად ვრცელდება სპეციალური ტორენტ-ტრეკინგული პორტალების საშუალებით. ამასთან, ძირითადი ფაილების უშუალო გაცვლა-გამოცვლა ხდება დეცენტრალიზებულად, „სიდერებს“, რომლებიც იძლევიან ფაილებს, და „ლიჩერებს“, რომლებიც იღებენ ფაილებს, შორის პირდაპირი შეერთების ორგანიზაციის საშუალებით. ინტერნეტქსელით გადასაცემი ინფორმაციის მოცულობის გამო (ზოგიერთ ვიდეოფაილს შეიძლება ჰქონდეს გიგაბაიტებით გასაზომი მოცულობა), მისი გადაცემა ხორციელდება ფრაგმენტებით. მიმღები მხარის ამოცანაა დაუკავშირდეს ერთი და იმავე ფაილის ფრაგმენტების სხვადასხვა გამომგზავნს და მიიღოს თავის მოწყობილობაზე ყველა ნაწილი.

საბოლოო მიზანია, ამ პატრა ნაჭრებით სწორი წესით აეწყოს საწყისი ფაილი ისე, რომ არ დაირღვეს ყველა მონაცემის მთლიანობა და მედიაგამშვებმა არ გვიჩვენოს შეცდომა ფაილის სანახავად გაშვების მცდელობისას. მოცემული ტექნოლოგიის ერთ-ერთი ძირითადი პროცედურაა მონაცემთა მნივნელოვანი ბლოკების მუდმივი შედარება მათი მთლიანობისა და მათი ფრაგმენტების სწორი იდენტიფიკაციის კონტროლის მიზნით. სწორედ აქ დასახმარებლად მოდის ჰეშირების ფუნქციონალი. როგორც მთელი ფაილების, ისე მათი ფრაგმენტების ჰეშებით ხორციელდება მონაცემთა ბლოკების სწორედ იმისადმი შესაბამისობის იდენტიფიკაცია, რაც იყო მოთხოვნილი. თუ ყველა ჰეში ემთხვევა, ეს ნიშნავს, რომ საბოლოოდ, გარანტირებულად „შევაწებებთ“ საჭირო ფაილს შეცდომების გარეშე. ამიტომ სწორედ ჰეში-

რების ტექნოლოგია გვაძლევს საშუალებას, სწრაფად და საიმედოდ შევადაროთ მონაცემთა სხვადასხვა ბლოკი და მივცეთ გადაცემისას მათი მთლიანობის დაცვის გარანტია.

დაბოლოს, ჰეშირების ტექნოლოგია აქტიურად გამოიყენება მონაცემთა ძიების დასაჩქარებლად. ამისათვის ფორმირდება ე.წ. „ჰეშ-ცხრილები“, რომლებიც სხვადასხვა საინფორმაციო ბლოკის ჰეშებს შეიცავს. მათ გარკვეული წესით ახარისხებენ, რათა ძიებისას შესაძლებელი იყოს მონაცემთა სწრაფი პოვნა მათივე ჰეშების მიხედვით, რათა მაშინვე მივმართოთ საჭირო თავს, მთელ ბაზაში ძიების მაგივრად.

ახლა განვიხილოთ საკითხი, თუ რომელი მათემატიკური და ლოგიკური ოპერაციები გამოიყენება ჰეშების გამოსათვლელად. ჰეშირების ალგორითმი საკმაოდ ბევრია, შედარებით მარტივებიდან დაწყებული – საკმაოდ რთულებით დამთავრებული. ჩვეულებრივ, ალგორითმის მათემატიკური მოდელის შექმნისას მიზნად ისახავენ ჰეშიდან პირველსახის უკუაღდგენის ამოცანის გართულებას და პირველსახიდან მიღებული ჰეშების მაქსიმალურად შესაძლო დიაპაზონის გაფართოებას. ეს აუცილებელია იმისათვის, რომ კოლიზიების წარმოშობის ალბათობამ, ანუ ორი სხვადასხვა პირველსახიდან ერთნაირი ჰეშების მიღებამ, შეადგინოს განსაკუთრებულად მცირე სიდიდე. გასაგებია, რომ ჰეშის თანრიგობრიობის (ზომის) ზრდასთან ერთად, კოლიზიის წარმოქმნის ალბათობა თვალსაჩინოდ მცირდება. თუმცა, რიგ შემთხვევებში საჭიროა შედარებით მცირე ზომის ჰეშების ამოცანის გადაჭრა, რადგან ეს გავლენას ახდენს შენახული ინფორმაციის ერთობლივ მოცულობაზე და შედეგად, მისი შენახვის ღირებულებაზე.

ჰეშირების ალგორითმის მუშაობის მაგალითად მოვიყვანთ რამდენიმე ყველაზე პოპულარულ პროცედურას, მათ შორის მათაც, რომლებიც გამოიყენება ბლოკჩეინ-ტექნოლოგიებზე დაფუძნებულ სხვადასხვა პროექტში, როგორებიცაა, მაგალითად, Bitcoin (SHA-256) ან Ethereum (SHA-3). მოცემული ალგორითმები შედგება გარკვეული რაოდენობის ნაბიჯებისაგან (იტერაციებისაგან), ყოველ მათგანზე ატარებენ რაიმე სახის ლოგიკურ ოპერაციებს შემდეგი ერთობლიობიდან.

- **„კონკატენაცია“** (ანუ მონაცემთა ორი ბლოკის „გადაბმა“ ან „შეწებება“, როდესაც მეორე ხდება პირველის გაგრძელება,

მაგალითად, „1111“-სა და „2222“-ის კონკატენაცია იძლევა შედეგს „11112222“).

- **„შეკრება“** (ჩვეულებრივი არითმეტიკული მოქმედება ორი და მეტი რიცხვისათვის).
- **„კონიუნქცია“** (ანუ **„ლოგიკური „და“**): ამ ბიტობრივი ოპერაციის შედეგი იქნება ჭეშმარიტი (1), თუ ორივე ბიტი არის ერთიანი, წინააღმდეგ შემთხვევაში შედეგი იქნება მცდარი (0).
- **„დიზიუნქცია**“ (ან **„ლოგიკური „ან“**): ამ ოპერაციის შედეგი იქნება ჭეშმარიტი (1), თუ არგუმენტთაგან ერთი მაინც არის ჭეშმარიტი (1), წინააღმდეგ შემთხვევაში შედეგი იქნება მცდარი (0).
- **„ლოგიკური გამომრიცხავი „ან“ („XOR“)**: ამ ოპერაციის შედეგი ორი ბიტისათვის იქნება ჭეშმარიტი (1) მხოლოდ მაშინ, როდესაც მხოლოდ ერთი არგუმენტი იქნება ჭეშმარიტი (1), ხოლო მეორე – მცდარი (0), წინააღმდეგ შემთხვევაში შედეგი იქნება მცდარი (0).
- **„ლოგიკური უარყოფა“ „არა“:** ბიტობრივი ინვერსია, უნარული ოპერაციის შედეგი, სადაც მიღებული ბიტი მნიშვნელობით ყოველთვის იქნება შემომავალი ბიტის საწინააღმდეგო, ანუ ერთიანები ხდება ნულები და – პირიქით).
- **„ბიტობრივი წანაცვლებები“:** როდესაც ბიტების მნიშვნელობები წანაცვლების მიმართულებით გადაადგილდება მეზობელ რეგისტრებში, მაგალითად, „10100110“ ბლოკისათვის მარცხნივ ლოგიკური წანაცვლების შედეგი იქნება „01001100“.

ბიტობრივი წანაცვლებები შეიძლება იყოს ლოგიკური (როდესაც უკანასკნელი ბიტი წანაცვლების მიმართულებით იკარგება, ხოლო პირველი ხდება ნული) და ციკლური (როდესაც წანაცვლების მიმართულებით უკანასკნელი ბიტი დგება პირველის ადგილზე). ზემოთ მოყვანილ მაგალითში განიხილებოდა სწორედ ლოგიკური წანაცვლება, რადგან მარცხნივ ციკლური წანაცვლების შედეგი ამ შემთხვევაში იქნებოდა „01001101“. გარდა ამისა, ყოველ იტერაციაში შეიძლება გამოყენებული იქნას დამხმარე კონსტანტების ერთობლიობები, მიმაგრებული ყოველ ალგორითმზე. ეს კონსტანტები ზემოთ აღწერილ

სხვადასხვა ოპერაციაში გამოიყენება. ამგვარად, ალგორითმის ყოველი ნაბიჯის შემდეგ შედეგი უფრო და უფრო შორდება საწყის მონაცემებს. ხდება მონაცემთა რთული ციკლური „შერევა“, შესაძლოა, სწორედ ამიტომ ამ პროცედურას უწოდეს „ჰეშირება“, რომლის ინგლისურიდან თარგმანიც ნიშნავს „არეულ-დარეულს“, „დომხალს“ და ხშირად ჰქვია წვრილად დაჭრილი ხორცის ან ბოსტნეულის კერძს. ამგვარი კერძების ინგრედიენტები, როგორც ჰეშირების შედეგი, შეუძლებელია მივიყვანოთ საწყის სახემდე (პირველსახემდე). თუმცა სხვადასხვა მაჰეშირებელი ალგორითმისათვის პირველსახეების აღდგენის ეფექტიანი მეთოდების მოძიების მცდელობები არსებობდა მათი წარმოქმნისთანავე.

იმისათვის, რომ წარმოვიდგინოთ პრობლემატიკა, რომელიც დაკავშირებულია ჰეშირების ყველაზე პოპულარული ალგორითმების კრიპტომედეგობასთან, შევაფასოთ ჰეშების ვარიანტების მრავალფეროვნებისა და მათთვის კოლიზიების მოძიების ალბათობათა გაანგარიშებული მაჩვენებლები. თანაფარდობა ჰეშის n თანრიგობრიობასა (ზომას) და შესაძლო გამოსვლების (ჰეშის გენერაციის ვარიანტების) რიცხვს შორის ტოლია 2 ხარისხად n-სა. თუ ჰეშის საშუალო სიგრძე ძირითად პოპულარულ ბლოკჩეინ-პროექტებში შეადგენს 256 ბიტს, ეს ნიშნავს, რომ გამოსასვლელთა რიცხვი ტოლია 2^{256} ან დაახლოებით 1.2×10^{77}, ანუ მნიშვნელობისა, რომელიც შედარებადია სამყაროში არსებული ატომების რაოდენობის შეფასებასთან. თუმცა, კოლიზიის მოსაძებნად სავალდებულო არ არის ყველა ვარიანტის განხილვა.

არსებობს შეტევის ცნობილი ალგორითმი, ე.წ. „დაბადების დღის შეტევა“, რომელიც ეფუძნება პარადოქსს, რაც დაკავშირებულია N ადამიანისაგან შემდგარ ჯგუფში, თუნდაც ორი ადამიანის დაბადების დღეების დამთხვევის ალბათობაზე ამოცანის ამოხსნასთან. პარადოქსი მდგომარეობს იმაში, რომ ფასდება არა იმის ალბათობა, რომ რომელიღაც კონკრეტული ადამიანის დაბადების დღე ვიღაცისას ემთხვევა (ეს ალბათობა მცირე ჯგუფებისათვის ძალზე დაბალია), არამედ ამ ჯგუფის ადამიანთა ნებისმიერი წყვილის დაბადების დღეების დამთხვევის ალბათობა. ეს კი ალბათობის უკვე სრულიად სხვა დონეა. მაგალითად, 23-კაციანი ჯგუფისათვის ასეთი ალბათობა აღემატება 50%-ს, ხოლო 60-კაციანისათვის 99%-ზე მეტი ხდება. ჰეშირების ალგორითმების კოლიზიებთანაც ასევე შესაძლებელია ანა-

ლოგიების გატარება, მაგრამ ბევრად დიდ რიცხობრივ მნიშვნელობებზე დაყრდნობით. თუმცა, ზოგადი აზრი ამით არ იცვლება: იმისათვის, რომ ვიპოვოთ კოლიზია ალბათობის რომელიღაც მნიშვნელოვან სიდიდესთან, უნდა გადავარჩიოთ ვარიანტთა ბევრად ნაკლები რაოდენობა, ვიდრე შესაძლო გამოსავლების მაქსიმალური რიცხვია. 256-ბიტიანი გასაღებისა და კოლიზიის პოვნის 75%-იანი ალბათობისას ეს მნიშვნელობა იქნება 5.7×10^{38}, რაც 39 თანრიგით მცირეა გამოსავალთა მაქსიმალურ მათემატიკურად შესაძლო გასავლის რიცხვზე. როგორც ხედავთ, ალბათობის მსგავსი, არსებითად მცირე სიდიდეც კი მაინც ინარჩუნებს ვარიანტთა გადარჩევის ამოცანის სირთულეს, განსაკუთრებით – მაღალ გამოთვლით დონეზე. ამიტომ ბლოკჩეინ-ტექნოლოგიებში გამოიყენება მაღალი თანრიგიანობის ჰეშირების ალგორითმები, რათა დაცული იქნას შენახული მონაცემები ბოროტმოქმედთა ხელყოფისაგან მინიმუმ იმ მომენტამდე, სანამ გამოთვლითი სიმძლავრეები ამ სირთულის დაბრკოლებათა გადალახვის საშუალებას მოგვცემს.

შევეცადეთ განგვეხილა ძირითადი მომენტები, რომელთა ცოდნაც ჰეშირების პრონციპებზე აუცილებელია. ამ პროცედურის უშუალო გამოყენებას კიდევ დავუბრუნდებით წიგნის სპეციალურ ნაწილებში, რომლებიც ბლოკჩეინ-პროექტების პრაქტიკულ განხორციელებას ეძღვნება.

კრიპტოგრაფიის ისტორია

ბლოკჩეინ-ტექნოლოგიის დეტალებში განხილვისას, სრულიად შეუძლებელია გვერდი აუარო მის ერთ-ერთ ყველაზე მნიშვნელოვან ელემენტს – კრიპტოგრაფიულ ნაწილს. ბლოკჩეინში კრიპტოგრაფია წარმოადგენს უძლიერეს დამაკავშირებელ ელემენტს, რომელსაც მთლიანობაში ეფუძნება განაწილებული რეესტრის ძირითადი ღირებულება. სწორედ კრიპტოგრაფია დგას მონაცემთა მთლიანობის დაცვისა და გადაცემის სადარაჯოზე, უზრუნველყოფს მფლობელობის უფლებას და იცავს სისტემის მომხმარებელთა აქტივებს, პირველ რიგში – ფინანსურს. კრიპტოგრაფიის გარეშე ბლოკჩეინ-ტექნოლოგია უბრალოდ ვერ იარსებებდა, ის დაკარგავდა ყველა უპირატესობას და მის გამოყენებას არავითარი აზრი არ ექნებოდა. მაშ, რატომ არის კრიპტოგრაფია ასეთი მნიშვნელოვანი? მოდი, ვცადოთ გავერკვეთ, მაინც რა არის კრიპტოგრაფია და როგორ გახდა ის ბლოკჩეინ-ტექნოლოგიის ფაქტობრივი ბირთვი.

კრიპტოგრაფიის ისტორია ათასწლეულების სიღრმეებში მიდის. ყოველ დროში ადამიანებს ჰქონდათ აუცილებლობა, საიდუმლო ინფორმაცია გადაეცათ გარკვეულ მანძილებზე. ჩვეულებრივ, პირველ რიგში, საქმე ეხებოდა სამხედრო მნიშვნელობის ინფორმაციას. იმ ეპოქაში, როდესაც სამყაროში არ არსებობდა კოლექტიური უსაფრთხოების სისტემები, სამხედრო თვალსაზრისით უფრო სუსტი სახელმწიფოები მუდმივად ხდებოდნენ აგრესიული მეზობლების მსხვერპლნი. მცირე სახელმწიფოებისათვის საკუთარი თავისუფლებისა და დამოუკიდებლობის შენარჩუნების ერთადერთი შანსი იყო ძლიერი მოკავშირეების პოვნა. მაგრამ ასეთი ხელშეკრულებების დასადებად აუცილებელი იყო ინფორმაციის გაცვლა, რომელიც პოტენციური მოწინააღმდეგისათვის არავითარ შემთხვევაში არ უნდა გამხდარიყო ცნობილი. იგივე ეხებოდა სამხედრო მეთაურების ბრძანებებს იმ ქვედანაყოფებისათვის, რომლებიც ძირითადი ძალების დისლოკაციის ადგილიდან შორს იმყოფებობდნენ: მუდმივი კოორდინაციის განსახორციელებლად საჭირო იყო ინფორმაციის გადაცემა და მიღება მო-

მავალი საომარი მოქმედებების ადგილმდებარეობაზე, რაოდენობაზე, მომარაგებაზე, ასევე – ტაქტიკასა და სტრატეგიაზე.

ინფორმაცია გადაეცემოდა სპეციალურად მომზადებული ადამიანების (შიკრიკების ან ჯაშუშების) მეშვეობით, რომელთა ამოცანაც იყო მაქსიმალურად სწრაფად და მოწინააღმდეგისთვის შეუმჩნევლად მიეტანათ გზავნილი ადრესატისათვის. მიუხედავად ამისა, არსებობდა არც ისე მცირე რისკი, რომ ასეთ შიკრიკს დაიჭერდნენ, ხოლო მის ხელთ არსებულ ინფორმაციას მტრები მოიპოვებდნენ. შეტყობინებების შედგენისას ამ რისკებს მუდამ ითვალისწინებდნენ, ამიტომ ინფორმაცია არასდროს არ იწერებოდა ღია ტექსტით, არამედ გარკვეული სახით მის დაშიფვრას ცდილობდნენ. მსგავსი პრაქტიკა გულისხმობდა, რომ ტექსტის გასაშიფრი გასაღები იცოდნენ მხოლოდ გამგზავნმა და გზავნილის მიმღებმა. ეს კი ნიშნავს, რომ შეტყობინებების გაცვლამდე აუცილებელი იყო გარკვეული ძალისხმევის დახარჯვა დასაშიფრი გასაღებების გასავრცელებლად ცენტრსა და მის პოტენციურ ადრესატებს შორის, რაც, თავის მხრივ, შეიცავდა რისკს, რომ მტერი ამ ინფორმაციასაც ხელში ჩაიგდებდა (ან იყიდდა) და შემდგომში, შეტყობინების წასაკითხად გამოიყენებდა. რა თქმა უნდა, თავად გამგზავნს არავითარი წარმოდგენა არ ექნებოდა ამის შესახებ, რამდენადაც საიდუმლო გასაღების ფლობის ფაქტს მოწინააღმდეგე არასდროს გაამჟღავნებდა.

პრინციპს, როდესაც შეტყობინებები დაიშიფრება და გაიშიფრება ერთი და იმავე გასაღებით, რომელსაც ინფორმაციის გაცვლაში მონაწილე ორივე მხარე ფლობს, ეწოდება სიმეტრიული კრიპტოგრაფია, რადგანაც მოცემულ შემთხვევაში საქმე გვაქვს გასაშიფრი გასაღებების აშკარა სიმეტრიასთან. სწორედ ეს პრინციპი გამოიყენებოდა ადამიანთა ცივილიზაციის არსებობის ყოველ დროში, უძველესი ხანებიდან – გასული საუკუნის 70-იან წლებამდე. დაშიფვრის რა მეთოდები გამოიყენებოდა იმ დროში? როგორც ადამიანის ცოდნის სხვა სფეროებს, კრიპტოგრაფიულ ტექნოლოგიებსაც ჰქონდა თავისი ევოლუციური გზა. ყველაფერი დაიწყო შეტყობინებაში ერთი ასოების ჩასმით მეორეს მაგიერ. მაგალითად, რომაელი მხედართმთავარი გაიუს იულიუს კეისარი გენერლებისათვის შეტყობინებებს კოდირებას უკეთებდა ლათინურ ანბანში ასოთა წანაცვლებით სამ პოზი-

ციაზე ანუ: ასო B ხდებოდა ასო E, C – F და ასე შემდეგ. მსგავს ჩანაცვლებით შიფრებს ასევე უწოდებენ მონოალფაბეტურს. შემდგომში მონოალფაბეტური შიფრები განდევნა პოლიალფაბეტურმა – მაშინ დასაშიფრი ტექსტის ასოებზე გამოიყენებოდა რამდენიმე მონოალფაბეტური შიფრი. ეს მეთოდი სხვადასხვა ვარიაციით გამოიყენებოდა თითქმის 1000 წლის განმავლობაში, XX საუკუნის დასაწყისამდე, როდესაც ხმარებაში შემოვიდა შეტყობინებების დასაშიფრი ელექტრომექანიკური მოწყობილობები. ალბათ ასეთი მეთოდის ყველაზე ცნობილ რეალიზებას წარმოადგენს გერმანული როტორული საშიფრი მანქანა „ენიგმა“, რომლის შიფრები გაუხსნელად ითვლებოდა.

დღევანდელი გადასახედიდან, „ენიგმას“ შიფრი სუსტად გამოიყურება. არადა, მეორე მსოფლიო ომის დროს ამ დასაშიფრმა მანქანამ ბევრი სიძნელე შეუქმნა გერმანიის მოწინააღმდეგეებს. საომარი მოქმედებების დაწყებამდე ჯერ კიდევ დიდი ხნით ადრე, 1932 წელს, პოლონურმა დაზვერვამ თავისი გერმანელი აგენტების ინფორმაციაზე დაყრდნობით შეძლო მიეღო მანქანის მოწყობილობის ზოგიერთი კოდი და პრინციპი. ამან პოლონელებს საშუალება მისცა, აღედგინათ მანქანა თავიანთ ლაბორატორიაში და ეცადათ მისი მუშაობის ალგორითმში გარკვევა. 1939 წელს გერმანია პოლონეთში შეიჭრა, მაგრამ ცოტა ხნით ადრე, „ენიგმაზე“ შესრულებული ყველა სამუშაო გადაეცა ბრიტანულ დაზვერვას, რომელმაც სპეციალური შეტყობინებების გასაშიფრად ჯგუფი შექმნა და თავისთან მიიწვია ნიჭიერი მათემეტიკოსი და კრიპტოგრაფი ალან ტიურინგი. 1940 წლისთვის ტიურინგის გუნდმა შეძლო აეგო დაახლოებით ორასი კრიპტოანალიტიკური მანქანა, რომლებიც „ენიგმას“ შიფრით მუშაობდა, მაგრამ გასაშიფრად საჭირო გადარჩევის განსაკუთრებულად მრავალფეროვანი ვარიანტები დიდი ხნის მანძილზე საშუალებას არ იძლეოდა, გაეტეხათ კოდი. მიუხედავად ამისა, ტიურინგმა შეძლო გამოევლინებინა განმეორებადი ფრაზები დაშიფრულ შეტყობინებებში. ერთ-ერთი ასეთი აღმოჩნდა თითქმის ყველა ტექსტში არსებული ნაცისტური მისალმება, რამაც საშუალება მისცა, მნიშვნელოვნად შეევიწროებინა ვარიანტთა გადარჩევის დიაპაზონი და საბოლოოდ გაეტეხა შიფრი. ითვლება, რომ სწორედ ამ მოვლენამ იქონია მნიშვნელოვანი ზეგავლენა გერმანიის დამარცხებაზე, ხოლო ომის დასრულება, ზოგიერთი სპეციალისტის აზრით, არანაკლებ ერთი წლით დაჩქარდა.

XX საუკუნის მეორე ნახევრის დასაწყისისათის მეცნიერები უფრო და უფრო ხშირად მიდიოდნენ დასკვნამდე, რომ სიმეტრიული კრიპტოგრაფიის შესაძლებლობები აშკარად არასაკმარისი იყო რიგი თანამედროვე ამოცანების ამოსახსნელად. კომპიუტერების წარმოქმნისა და მათი გამოთვლითი სიმძლავრეების ზრდასთან ერთად, იმ დროს არსებული თვით ყველაზე რთული სიმეტრიული შიფრების გატეხაც სერიოზული პრობლემა აღარ იყო. ამიტომ მსოფლიომ თანდათანობით დაიწყო გადასვლა მათემატიკურ კრიპტოგრაფიაზე. ამ გადასვლის შედეგი გახდა ნამდვილი რევოლუცია, რომელიც კრიპტოგრაფიის პრინციპულად ახლებური ნაწილის გამოჩენით გამოიხატა. საუბარია ასიმეტრიულ კრიპტოგრაფიაზე ან, როგორც მას კიდევ უწოდებენ, ღია გასაღების კრიპტოგრაფიაზე.

1976 წელს ორმა კრიპტოგრაფმა – უიტფილდ დიფიმ და მარტინ ჰელმანმა გამოაქვეყნეს ნაშრომი სახელწოდებით „ახალი მიმართულებები თანამედროვე კრიპტოგრაფიაში“. სტატიაში გადმოცემული მთავარი იდეა ის იყო, რომ გარდა ერთი საიდუმლო გასაღებისა, ყალიბდებოდა მეორეც – ღია, რომელიც მათემატიკურად დაკავშირებული იყო საიდუმლო გასაღებთან. ამასთან, საიდუმლო გასაღების ღიადან აღდგენის პროცესი წარმოადგენს განსაკუთრებულად რთულ მათემატიკურ ამოცანას. ამ იდეის საბოლოო შედეგი განხორციელდა საიდუმლო გასაღების ღია არხებით გავრცელების შესაძლებლობაში ისე, რომ არ არსებობს მესამე პირების მიერ მისი გახსნის საშიშროება. ამისათვის მხარეებს სჭირდებოდათ, მხოლოდ ღია გასაღებები გაეცვალათ დამხმარე საანგარიშო ინფორმაციის დამატებით, ხოლო შემდეგ, მათემატიკური ოპერაციის საშუალებით აღედგინათ საერთო საიდუმლო გასაღები მიმღების მხარეს. ამ ალგორითმმა მიიღო „დიფი-ჰელმანის“ სახელი – მისი შემქმნელების გვარების მიხედვით და სათავე დაუდო ახალ კრიპტოგრაფიულ ეპოქას, რომელშიც ჩნდებოდა და ვითარდებოდა დაშიფვრის განსაკუთრებულად კრიპტომედეგი ალგორითმები, რომლებიც გამოიყენება, კერძოდ, ბლოკჩეინ-ტექნოლოგიაში.

როგორ ხდება ღია გასაღებით დაშიფვრა? სინამდვილეში პრინციპი საკმაოდ მარტივია – ყოველი მომხმარებელი თავისთვის აგენერირებს ღია გასაღებს, თუნდაც შემთხვევითი გზითაც კი. შემდეგ, დაშიფრვის კონკრეტულ ალგორითმზე დამოკიდებული მათემატი-

კური ოპერაციების დახმარებით, ამ საიდუმლო გასაღებიდან იღებს მეორე გასაღებს, რომელსაც აქვს საჯარო სტატუსი – ანუ საჯარო გასაღების მფლობელს შეუძლია ღიად გაავრცელოს ის: მოათავსოს საიტზე, საფოსტო შეტყობინებაში ან სულაც დაბეჭდოს გაზეთში. საკუთარი საჯარო კოდის გახსნა აუცილებელია, რადგან ეს შეტყობინების დასაშიფრად უეჭველად დასჭირდებათ მათ, ვისაც ამ ორი გასაღების მფლობელისათვის შეტყობინების გაგზავნის სურვილი ექნება. საქმეც ისაა, რომ საჯარო გასაღებით კოდირებული შეტყობინების გაშიფრვა შესაძლოა მხოლოდ მისი შესაბამისი საიდუმლო გასაღების დახმარებით. როგორც ვხედავთ, ამგვარი სისტემა ბევრად უფრო მოსახერხებელია, ვიდრე კრიპტოგრაფიის სიმეტრიული ფორმა, სადაც საერთო საიდუმლო გასაღების დაუცავი არხებით მუდმივად გავრცელების აუცილებლობა ქმნის სერიოზულ მოწყვლადობას მთლიანად დაშიფვრის ტექნოლოგიისათვის.

და მაინც, უნდა აღინიშნოს, რომ დაშიფვრის სიმეტრიული სისტემების გამოყენება კვლავაც გრძელდება. საქმე ისაა, რომ სიმეტრიულ ალგორითმებს აქვს დაშიფვრისა და გაშიფვრის ძალზე მაღალი სიჩქარეები. იმ სისტემებში, სადაც ეს პარამეტრი კრიტიკულია, და ასევე იმ პირობით, რომ მხარეებს შეუძლიათ უზრუნველყონ საიდუმლო გასაღებების ერთმანეთში უსაფრთხოდ გაცვლა, სიმეტრიული დაშიფვრის გამოყენება სავსებით გამართლებული და ეფექტიანი შეიძლება აღმოჩნდეს. საკმაოდ ხშირად, ინტერნეტის ქსელით მონაცემების გადაცემისას, სიმეტრიული და ასიმეტრიული კრიპტოგრაფიის ალგორითმების კომბინაციით სარგებლობენ. კერძოდ, შეერთების დაყენებისას გამოიყენება საერთო საიდუმლოს გადაცემა დიფი-ჰელმანის ალგორითმის საშუალებით, ხოლო შემდეგ ეს საერთო საიდუმლო ორივე მხარის მიერ გამოიყენება როგორც მონაცემთა პაკეტების სიმეტრიული ალგორითმებით დაშიფვრისა და გაშიფვრის გასაღები. მაგრამ მაინც, დიდი რაოდენობის მომხმარებლის მქონე განაწილებულ სისტემებში განუყოფლად ბატონობს ასიმეტრიული კრიპტოგრაფია და ბლოკჩეინ-პროექტები გამონაკლისი არ არის. მაშ, ასიმეტრიული დაშიფვრის რომელი მეთოდებია ამჟამად ყველაზე პოპულარული?

ასიმეტრიული კრიპტოგრაფია

ასიმეტრიული დაშიფვრის ალგორითმი საკმაოდ ბევრია. მაგრამ ამ წიგნში შევჩერდებით მხოლოდ რამდენიმე მათგანზე, გადავალთ შედარებით მარტივებიდან შედარებით რთულებზე. ასიმეტრიულ ალგორითმებს შორის პირველად გაჩენილი დიფი-ჰოლმანის ალგორითმი არ ჭრიდა იმ მხარეთა აუტენტიფიკაციის ამოცანას, რომლებიც ერთობლივად ახდენდა საიდუმლო გასაღების გენერირებას. თუმცა, უკვე 1977 წელს გამოჩნდა ალგორითმი, რომელიც უზრუნველყოფდა არა მარტო დაშიფვრის პროცესს, არამედ გამოსადეგი იყო სისტემის სუბიექტის აუტენტიფიკაციის შესაქმნელადაც ციფრული ელექტრონული ხელმოწერის საშუალებით. მოცემული ალგორითმი ეყრდნობოდა ე.წ. დიდი რიცხვების „ფაქტორიზაციის“ ამოცანას და სახელად მიიღო აბრევიატურა RSA – მისი შემქმნელი მეცნიერების – რონალდ რივესტის, ადი შამირისა (ინგლისურად – Shamir) და ლეონარდ ადელმანის – გვარების მიხედვით. ფაქტორიზაცია ეწოდება ნატურალური რიცხვის მარტივ თანამამრავლებად განშლის პროცესს. ალგორითმ RSA-ში საიდუმლო გასაღები წარმოადგენს ორ დიდ მარტივ რიცხვს, ხოლო საჯარო გასაღები – ამ ორი რიცხვის ნამრავლს. კრიპტოგრაფიაში ამ მეთოდის გამოყენება განპირობებულია მისი თვისებით, რომლის მეშვეობითაც რამდენიმე რიცხვის ერთმანეთზე გამრავლების ამოცანა საკმაოდ მარტივია, მათ შორის – ძალზე დიდი რიცხვებისაც. ამავდროულად, მიღებული რიცხვის საწყის თანამამრავლებად უკუგანშლა გამოთვლითი თვალსაზრისით განსაკუთრებულად რთულია.

ავხსნათ მაგალითზე. დავუშვათ, გვაქვს სამი მარტივი რიცხვი – 3, 5 და 7. მარტივი ის რიცხვებია, რომლებიც ნაშთის გარეშე იყოფა მხოლოდ ერთიანზე და საკუთარ თავზე. გავამრავლოთ ეს რიცხვები ერთმანეთზე, მივიღებთ 105-ს. ახლა წარმოვიდგინოთ, რომ გვაქვს მხოლოდ საბოლოო შედეგი – 105 და გვჭირდება მისი უკუგანშლა მარტივ მამრავლებად, ანუ რომ მივიღოთ 3, 5 და 7. ამ ამოცანის ამოხსნისას ასეთი არცთუ ისე დიდი სამნიშნა რიცხვისათვისაც კი სიძნელეებს ვაწყდებით, ხოლო ამოცანა ათეულობით პოზიციიანი თანრიგიანობის მქონე რიცხვების ფაქტორიზაცია თანამედროვე კომპიუტერისთვისაც შეიძლება სავსებით არატრივიალური იყოს. რა თქმა

უნდა, არსებობს ალგორითმები, რომლებიც საშუალებას გვაძლევს, რამდენადმე უფრო ეფექტიანად განვახორციელოთ ფაქტორიზაცია, ვიდრე გამყოფთა უბრალო გადარჩევით, მაგრამ ერთმნიშვნელოვანი ოპტიმალური ალგორითმი, რომელიც ამ ამოცანის სწრაფად ამოხსნის საშუალებას მოგვცემს, ჯერჯერობით არ გამოუგონიათ.

რიცხვების ფაქტორიზაციის პრობლემაზე მეცნიერები ასეული წლების წინაც ფიქრობდნენ. ამ პრობლემის შესწავლა ერთ-ერთმა პირველმა ფრანგმა მათემატიკოსმა პიერ დე ფერმამ დაიწყო. ჯერ კიდევ 1643 წელს მან შემოგვთავაზა ფაქტორიზაციის საკუთარი მეთოდი, რომელიც RSA შიფრების კრიპტოანალიზისათვის ჩვენს დროშიც გამოიყენება. გასაგებია, რომ დაშიფვრის ნებისმიერი ალგორითმისათვის ყოველთვის მოიძებნებიან ადამიანები, რომლებიც მონახავენ შესაძლებლობას მასზე ეფექტურად შესატევად, ზოგი – დანაშაულის ჩასადენად, ზოგი – მეცნიერული მიზნებით, იმისათვის, რათა გამოვიკვლიოთ ალგორითმის კრიპტომედეგობა და დავიცვათ პროექტები, რომლებიც ამ ამოხსნას ეფუძნება. ჯერ კიდევ 2000 წლის შუა პერიოდში გაჩნდა შეტყობინებები იმის შესახებ, რომ ამა თუ იმ უნივერსიტეტის მეცნიერებმა გატეხეს RSA-ს ჯერ 512-ბიტიანი და შემდეგ 1024-ბიტიანი გასაღები. ამასთან, მათ გამოიყენეს რომელიღაც განსაკუთრებული გამოთვლითი სიმძლავრე, ხოლო ამოცანის გადასაჭრელად სავსებით გონივრული დრო დასჭირდათ. რა თქმა უნდა, ვერც ერთი, თუნდაც ყველაზე მძლავრი კომპიუტერი ასეთ გამოთვლით დატვირთვას მარტო ვერ გაუმკლავდება, ამიტომ ამგვარი ამოცანების ამოსახსნელად, კომპიუტერებს ჩვეულებრივ, გამომთვლელ კლასტერებად აერთიანებენ.

უკანასკნელი ათი წლის განმავლობაში კომპიუტერების სიმძლავრეები საგრძნობლად გაიზარდა. „მურის კანონის“ თანახმად, კომპიუტერების პროცესორების წარმადობა ყოველ 18 თვეში ორმაგდება, ამიტომ RSA ალგორითმის კრიპტომედეგობის შესანარჩუნებლად სხვადასხვა ტექნოლოგიურ გადაწყვეტაში აუცილებელია მუდმივად ვზარდოთ ღია გასაღების სიგრძე. რადგან უსასრულობამდე ამ პროცესის გაგრძელება შეუძლებელია, ამ ალგორითმზე უარის თქმა და უფრო პროგრესულებზე გადასვლა დაიწყეს, რომლებშიც საკმარისი კრიპტომედეგობა ნარჩუნდება გონივრული თანრიგის მქონე გასაღებებისათის – 256-1024 ბიტის ფარგლებში. ერთ-ერთი ასეთი გახდა DSA-ს ციფრული ხელმოწერის ჩამოსაყალიბებელი ალგორითმი, რო-

მელიც დისკრეტული გალოგარითმების მოდელზეა აგებული. მოცემულ ალგორითმში გამოყენებულია ეგრეთ წოდებული მოდულური არითმეტიკა, რომელიც იმ ხარისხის მიგნების ამოცანაა, რომელშიც უნდა ავიყვანოთ მოცემული რიცხვი, რათა სხვა მოცემულ რიცხვზე შედეგის მოდულის გაყოფისას, გაყოფის სასურველი ნაშთი მივიღოთ. უფრო გასაგები რომ გახდეს, განვიხილოთ შემდეგი მაგალითი:

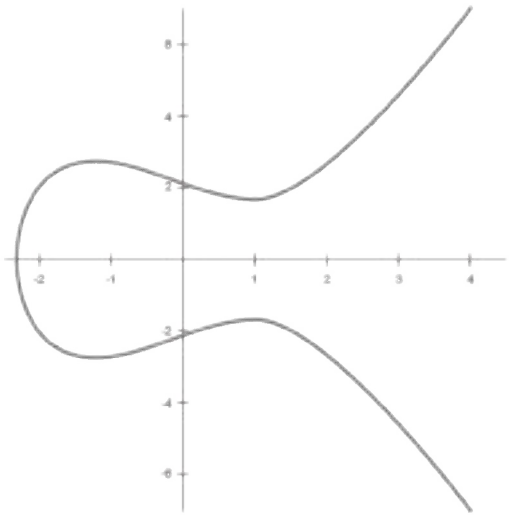
$$3^x \bmod 17 = 13$$

მოდულზე გაყოფა მთელი რიცხვების ჩვეულებრივი მთელნაშთიანი გაყოფაა ერთმანეთზე. ასეთ არითმეტიკულ ოპერაციას სკოლაში დაბალ კლასებში, უშუალოდ წილადების ათვისებამდე სწავლობენ. ამის შემდეგ, ნაშთით გაყოფას მშვიდად ივიწყებენ და აღარ იხსენებენ უმაღლესი მათემატიკის საუნივერსიტეტო კურსამდე, სადაც მოულოდნელად ირკვევა, რომ ნაშთიანი გაყოფა სინამდვილეში, საკმაოდ მნიშვნელოვან როლს თამაშობს ალგებრაში რიცხვთა თეორიაში. ჩვენს მაგალითში უნდა განვსაზღვროთ, რომელ ხარისხში უნდა ავიყვანოთ სამიანი, რომ შემდეგ, მიღებული შედეგის მოდულის 17-ზე გაყოფისას, 13 გაყოფის ნაშთად მივიღოთ. სწორი პასუხია: $x = 4$ ანუ $3^4 = 81$, $81/17 = 4$ + ნაშთი 13 (შემოწმება: $4 \times 17 = 68 + 13 = 81$). საკმაოდ მარტივია, არა? სამის ერთზე და ერთზე მეტ სხვადასხვა *x* ხარისხში აყვანისას, შემდეგ კი შედეგის მოდულის 17-ზე გაყოფისას ყოველთვის სხვადასხვა ნაშთს მივიღებთ. მაგრამ მათ ექნება ერთი საერთო თვისება, ყველა ეს ნაშთი იქნება 1-დან 16-ის ჩათვლით, ოღონდ მიმდევრობით (*x* ხარისხის ზრდასთან ერთად) არ დალაგდება. ამ რიცხვთა სიმრავლეს გამოკლებათა რგოლს უწოდებენ. რგოლს იმიტომ, რომ ნაშთები მუდმივად გამეორდება ხარისხის სხვადასხვა მაჩვენებლისათვის, რომლებშიც საწყისი რიცხვი აგვყავს. ახლა წარმოვიდგინოთ, რომ ვოპერირებთ არა ერთ-ორთანრიგიანი რიცხვებით, არამედ ძალზე დიდი რიცხვებით. ამ შემთხვევებში, თუ მოცემული რიცხვის ხარისხი წინასწარ არ ვიცით, მაშინ მისი პოვნის ამოცანა ნაშთთა კონკრეტული სიდიდეებისათვის ძალზე რთული ხდება. სწორედ ეს სირთულე ძევს DSA ალგორითმის საფუძველში.

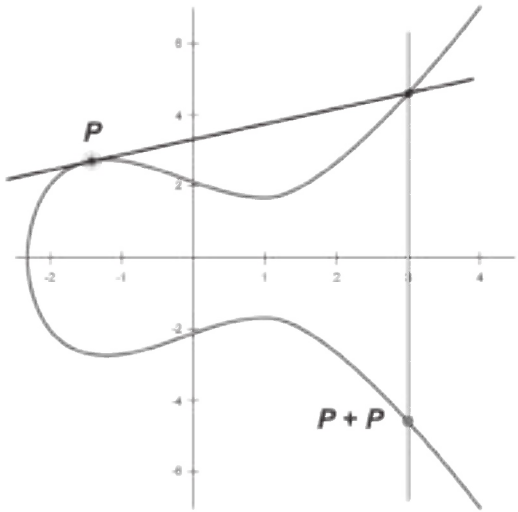
როგორც უკვე ნახსენები იყო, დაშიფვრის ყველა მსგავსი ალგორითმი აგებულია პრინციპზე, რომ ამოცანა ერთი მხრიდან იხსნება

ძალზე სწრაფად და მარტივად, ხოლო უკუმიმართულებით – ძალზე რთულად. DSA ალგორითმიც გამონაკლისი არ არის. თუ ამოცანას დიდი რიცხვებისათვის სხვადსხვა მნიშვნელობის უბრალო გადარჩევით ამოვხსნით, მაშინ ეს მეთოდი ძალიან ნელა იმუშავებს. ამიტომ ჩვეულებრივი გადარჩევის მაგივრად, შემუშავებული იქნა ალგორითმები, რომლებიც ამ ამოცანას ბევრად ეფექტიანად ჭრის, იმდენად ეფექტიანად, რომ, თუ მხედველობაში მივიღებთ თანამედროვე კომპიუტერების მწარმოებლობის მუდმივ ზრდას, მათემატიკოსები დაშიფვრის ალგორითმების სირთულის ზრდის აუცილებლობაზე უნდა დაფიქრებულიყვნენ, წინააღმდეგ შემთხვევაში, ისინი შიფრების მასობრივი გატეხის პრობლემის წინაშე უკვე არცთუ ისე შორეულ მომავალში შეიძლება დამდგარიყვნენ.

ამოცანის მნიშვნელოვნად გასართულებლად, 1985 წელს შემუშავებული იქნა დისკრეტული გალოგარითმების ალგორითმი ელიფსური მრუდების ბაზაზე (ალგორითმი ECDSA). რაზეა ამ შემთხვევაში საუბარი და რა მრუდია ეს? ელიფსური მრუდი არის წერტილთა სიმრავლე, რომელიც $y^2 = x^3 + ax + b$ განტოლებით აღიწერება, ანუ DSA ალგორითმისგან განსხვავებით, ოპერაციები ტარდება არა მთელი რიცხვების რგოლზე, არამედ ელიფსური მრუდის წერტილთა სიმრავლეზე, რაც მნიშვნელოვნად ართულებს ღია გასაღებიდან დახურული გასაღების აღდგენის ამოცანას. აი, ჩვეულებრივი ელიფსური მრუდის მაგალითი:



ელიფსური მრუდის წერტილთა სიმრავლიდან შეიძლება ამოირჩეს ისეთი წერტილები, რომლებიც შეიძლება მივამატოთ საკუთარ თავს და შედეგად მივიღოთ სხვა წერტილი იმავე მრუდზე. სხვაგვარად რომ ვთქვათ, გავაფართოოთ განტოლება $X = nP$-ის, სადაც $n = 2$-სა და მეტს, ხოლო X და P არის წერტილები მოცემულ მრუდზე კოორდინატებით x და y ღერძებზე. კონსტანტა n-ზე გამრავლება სხვა არაფერია, გარდა n-ჯერ მიმდევრობით შეკრება. ამგვარად, ვიწყებთ იმით, რომ აუცილებლად უნდა მივამატოთ საწყისი წერტილი მასცე და შედეგად მივიღოთ ისეთივე წერტილი, ოღონდ – საკუთარი განსხვავებული კოორდინატებით. გეომეტრიულად, ელიფსური მრუდის წერტილის საკუთარი თავისთვის მიმატება ამ წერტილის მხების აგებას ნიშნავს. შემდეგ ვპოულობთ მხების გადაკვეთის წერტილს მრუდის გრაფიკთან, იქიდან ვაგებთ ვერტიკალურ წრფეს და ამგვარად ვპოულობთ მისი გადაკვეთის წერტილს მრუდის საწინააღმდეგო მხარეს. ეს წერტილი იქნება მიმატების შედეგი. აი, როგორ გამოიყურება წერტილის საკუთარი თავისთვის მიმატების ოპერაცია გეომეტრიულად:



ამის შემდეგ, უკვე მომდევნო იტერაციისას, საწყისი წერტილი იქნება ის, რომელიც წინა ნაბიჯის დროს, შეკრების შედეგად მი-

ვიღეთ. სწორედ მისგან ვაგებთ ახალ მხებს და ა.შ. n რაოდენობით ამოცანის სირთულეს წარმოადგენს n-ის უკუძიება X და P ცნობილი წერტილებისათვის და ამ ამოცანას არ აქვს სწრაფი ამოხსნა. ამ შემთხვევაში n იქნება დახურული გასაღები, ხოლო X – ღია. გასაგებია, რომ კომპიუტერი გაანგარიშებისას შეკრების ოპერაციას ახდენს არა გეომეტრიულად, არამედ სუფთად ალგებრულად, რისთვისაც ყოველი წერტილისათვის x და y ღერძებზე არსებული კოორდინატების ბაზაზე სპეციალური ფორმულები არსებობს.

ცალკე უნდა აღვნიშნოთ, რომ ელიფსური მრუდების ყველა ფორმა როდი გამოდგება მათ საფუძველზე კრიპტოგრაფიული ალგორითმების ფორმირებისათვის. არსებობს ამ ასპექტში საკმაოდ „სუსტი“ ელიფსური მრუდები, რომლებიც დისკრეტული გალოგარითმების ამოცანების ამოხსნის სხვადასხვა სახის ალგორითმების მიმართ არამდგრადია. ამიტომ, იმისათვის, რომ ელიფსური მრუდი გამოსადეგი იყოს რთული კრიპტოგრაფიული ამოცანებისათვის, ის უნდა აკმაყოფილებდეს სხვადასხვა პირობას, რომლებსაც აქ არ განვიხილავთ, რათა ზედმეტად არ გავართულოთ ზოგადი პრინციპების აღწერა.

ალგორითმების თეორიაში გამოყოფენ მათემატიკური ამოცანების ამოხსნის სხვადასხვა სირთულის კატეგორიებს: პოლინომურს, სუბექსპონენციურს და ექსპონენციურს. ელიფსურ მრუდებზე დაფუძნებული დისკრეტული გალოგარითმების ალგორითმების სირთულე ექსპონენციური (თვალსაჩინო) სისწრაფით იზრდება. აქამდე არ არის შემუშავებული ამ ამოცანის არც ერთი გადაჭრა სუბექსპონენციურ დროშიც კი ანუ დროში, რომელიც პროპორციულია ფუნქციისა, რომელიც იზრდება უფრო ნელა, ვიდრე ნებისმიერი ხარისხოვანი ფუნქცია. სწორედ ამიტომ, ამ ალგორითმმა ყველაზე ფართო გამოყენება პოვა ჩვენს დროში, როგორც საკმარისად კრიპტომედეგმა მოდელმა, რომელიც იყენებს შედარებით მცირეთანრიგიან გასაღებებს. თუ ზემოთ აღწერილ ლოგარითმებს ერთმანეთს შევადარებთ, მაშინ, იმ შემთხვევისათვის, როდესაც ღია RSA ან ჩვეულებრივი DSA გასაღებების სიგრძე, მაგალითად, არის 1024 ბიტის ტოლი, ელიფსური მრუდების გამომყენებელი ალგორითმისათვის შესაბამისი კრიპტომედეგობის მისაღწევად საკმარისი იქნება სულ რაღაც 160 ბიტი. ეფექტიანობაში სხვაობა აშკარაა, ამიტომ ყველაზე პოპულარული

ბლოკჩეინ-პროექტები, როგორებიცაა Bitcoin ან Ethereum (და მრავალი სხვა), იყენებს სწორედ ელიფსურ მრუდებზე დაფუძნებულ კრიპტოგრაფიას, რომელიც ამჟამად ყველაზე საიმედოდაა აღიარებული.

გარდა საკუთრივ მონაცემთა დაშიფვრისა, ბლოკჩეინ-ტექნოლოგიაში დაშიფვრასთან დაკავშირებულ უმნიშვნელოვანეს ელემენტს წარმოადგენს ციფრული ელექტრონული ხელმოწერა (ЦЭП). რა არის ეს და როგორ გამოიყენება იგი?

ციფრული ელექტრონული ხელმოწერა

ჩვენთვის ჩვეული ცნება „ხელმოწერა“ სამყაროსავით ძველია, დოკუმენტთა ნამდვილობის შემოწმების ამოცანა უძველესი დროიდან იდგა კაცობრიობის წინაშე. დოკუმენტების გაყალბების გასართულებელ ელემენტებად გამოიყენებოდა საკუთრივ მოხელეთა, ვაჭართა, ფეოდალთა და თვით მონარქთა ხელით შექმნილი გვარ-სახელების უნიკალური ფორმები. ეს ხანდახან კეთდებოდა ხელმომწერის სახელმწიფო ან გვარეულობის დამადასტურებელი გერბების ანაბეჭდის მქონე ლუქის ან ცვილის ბეჭედთან ერთობლიობაში. ითვლებოდა, რომ ეს კომბინაცია მყარად იცავდა დოკუმენტს არასანქცირებული შეცვლისაგან მონაცემთა გამყალბებლის სასარგებლოდ. უმრავლეს შემთხვევაში, დაცვის ეს ზომები ამართლებდა. და მაინც, არ არსებობდა არავითარი გარანტია, რომ ასეთი შემთხვევებისათვის კარგად შეიარაღებული რომელიღაც შუასაუკუნეობრივი ბოროტმოქმედი ვერ შეძლებდა დოკუმენტის ისეთი ასლის შექმნას, რომელიც საკმაოდ ახლოს იქნებოდა ორიგინალთან.

კომპიუტერული ტექნოლოგიების განვითარებასთან ერთად სატელეკომუნიკაციო არხებით გადაცემული ინფორმაციის ავთენტურობის პრობლემა განსაკუთრებით მწვავედ დადგა. რა თქმა უნდა, დაუცველი ციფრული დოკუმენტის გაყალბება ბევრად უფრო ადვილია, ვიდრე ხელნაწერისა. ამიტომ დიდი ხნის მანძილზე კომპიუტერულ დოკუმენტებს ხსნიდნენ, ადასტურებდნენ ხელმოწერით და უმეტეს შემთხვევაში, მასზე მელნის ბეჭედს ურტყამდნენ; შემდეგ დოკუმენტს ასკანირებდნენ და გადასცემდნენ როგორც გრაფიკულ გამოსახულებას, რომელიც შეიცავდა როგორც ნაბეჭდ მონაცემებს, ისე ხელით შექმნილ რეგალიებს. მაგრამ ასეთ შემთხვევებში გაყალბების საწინააღმდეგო რაიმე გარანტიის არსებობაც კი წარმოუდგენელი იყო – ყოველ შემთხვევაში, სანამ ტექნოლოგიები არ გადავიდა სრულიად ახალ ხარისხობრივ დონეზე, დოკუმენტების შექმნაზე

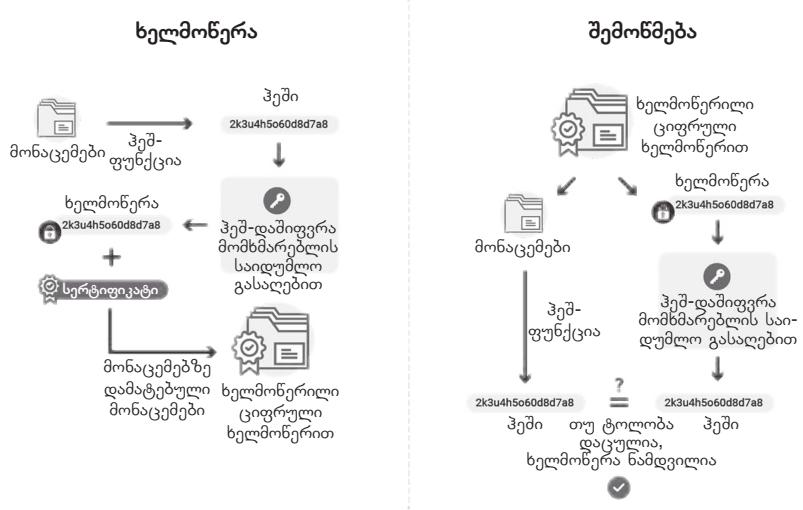
ციფრული ელექტრონული ხელმოწერით, რომელიც ასიმეტრიული კრიპტოგრაფიის ალგორითმების ბაზაზე ჩამოყალიბდა.

ციფრული ელექტრონული ხელმოწერა არის გარკვეული კრიპტოგრაფიული ალგორითმის მუშაობის შედეგი, რომელსაც შესავალზე მიეწოდება ორი აუცილებელი ელემენტი: მონაცემთა ერთობლიობის ჰეში, რომელიც აღწერას ექვემდებარება, და ხელმოწერის მფლობელის საიდუმლო გასაღები. ციფრულ ხელმოწერას აქვს მთელი რიგი სასარგებლო თვისებებისა, რომელთა შორის მთავარია, რომ ხელმოწერის შექმნა შეუძლია მხოლოდ საიდუმლო გასაღების მფლობელს და სხვას არავის. უფრო სწორად, შეიძლება იყოს ღიადან საიდუმლო გასაღების აღდგენის გამოთვლითი მცდელობები, მაგრამ, როგორც უკვე დავრწმუნდით, ამის გაკეთება ძალზე რთულია და ამგვარი შედეგის მიღების ალბათობა ძალზე მცირეა. ციფრული ხელმოწერის ნამდვილობის შემოწმება შეგვიძლია, თუ ვიცით ხელმოწერის მფლობელის ღია გასაღები. ამასთან, კონკრეტული ხელმოწერით დამოწმებული დოკუმენტი ველარ შეიცვლება ვერც ერთ თავის ბიტში, რადგან ხელმოწერა ამ შემთხვევაში მაშინვე დაკარგავს თავის ვალიდურობას. ეს მოხდება იმიტომ, რომ შეიცვლება ხელმოწერილი დოკუმენტის ჰეში, რომელზეც პირდაპირ არის დამოკიდებული საკუთრივ ხელმოწერის ფორმირება, ანუ ციფრული ელექტრონული ხელმოწერა არა მარტო ავტორის იდენტიფიცირებას ახდენს, არამედ იმ დოკუმენტის უცვლელობის გარანტიასაც იძლევა, რომელიც ხელმოწერილია.

ციფრული ელექტრონული ხელმოწერის ფორმირებისათვის პირველ რიგში აუცილებელია ავირჩიოთ ასიმეტრიული კრიპტოგრაფიის საკმარისად კრიპტომედეგი ალგორითმი; შემდეგ მის საფუძველზე შევქმნათ გასაღებთა წყვილი – საიდუმლო და საჯარო; შემდეგ გამოვთვალოთ ხელმოსაწერ მონაცემთა ბლოკის ჰეში – მაგალითად, რომელიღაც დოკუმენტისა, რომლისთვისაც წინასწარ გვაქვს არჩეული ჰეშ-ფუნქციის შესაბამისი ალგორითმი. ჰეშირებას აქვს ორი მიზანი: საწყისი მონაცემების მთლიანობის დაცვა და მათი ციფრული ანაბეჭდის შექმნა სტანდარტიზებული ფორმით. ამის შემდეგ, რაკიღა გვაქვს მონაცემთა ჰეში და დახურული გასაღები, გავუშვებთ ფორმირების ალგორითმს და გამოსავალში მივიღებთ შედეგს მონაცემთა სტრიქონის სახით. ხელმოწერის ნამდვილობისა და ხელმოწერილი მონაცემების მთლიანობის შემოწმება სხვადასხვა დასაშიფრ ალგორითმში მათემატიკურად ერთმანეთისაგან განსხვავდება. თუმცა შემოწმების

ზოგად პრინციპს წარმოადგენს ორი შედეგის გამოთვლა, რომელიც სხვადასხვა მეთოდით ხდება, ამასთან, ერთ-ერთი მათგანის მისაღებად აუცილებლად გამოიყენება ხელმომწერის ღია გასაღები. შემდეგ ეს შედეგები დარდება და მათი სხვადასხვაობის შემთხვევაში კეთდება დასკვნა, რომ ხელმოწერა გაყალბებულია ან საწყისმა მონაცემებმა ხელმოწერის შემდეგ ცვლილება განიცადა.

მაგალითის სახით განვიხილოთ ალგორითმი RSA. აქ დარდება ხელმოწერილ მონაცემთა ბლოკების ჰეშები, სადაც პირველი ჰეში მიიღება სტანდარტული მეთოდით როგორც ჰეშ-ფუნქციის მოქმედების შედეგი საწყის მონაცემებზე, ხოლო მეორე გამოითვლება ღია გასაღების საშუალებით. შემდეგ, მიღებული ორი ჰეში ერთმანეთს დარდება, რის შემდეგაც შეგვიძლია გავაკეთოთ დასკვნა ხელმოწერის ნამდვილობაზე ანუ მის მათემატიკურ შესაბამისობაზე ხელმოწერილ დოკუმენტებთან. საჭიროა კიდევ ერთხელ გავუსვათ ხაზი, რომ ЭЦП-ის ფორმირება ან მისი შემოწმება ტარდება მათემატიკური ოპერაციების საშუალებით, რომელიც ახასიათებს მხოლოდ კონკრეტულ, წინასწარ არჩეულ დაშიფვრის ალგორითმს. როგორც წესი, ამისათვის გამოიყენება ფაქტორიზაციის ან დისკრეტული გალოგარითმების ალგორითმები, მათ შორის ელიფსური მრუდის წერტილების სიმრავლეზეც. ძირითადად სწორედ უკანასკნელი მეთოდი გამოიყენება ბლოკჩეინ-გარემოებში როგორც ყველაზე კრიპტომედეგი. RSA ალგორითმის საშუალებით ხელმოწერის მაგალითისა და ხელმოწერის შემოწმების სქემა ნაჩვენებია სქემაზე:



ასევე უნდა აღინიშნოს, რომ ციფრული ელექტრონული ხელმოწერა სულაც არაა სავალდებულო, ეყრდნობოდეს ასიმეტრიული დაშიფვრის ალგორითმებს. არსებობს მისი გამოყენების მეთოდიკა სიმეტრიული სისტემებისათვის. ამ შემთხვევაში საჭიროა კიდევ ერთი სუბიექტი, მესამე პირი არბიტრის სახით, რომელსაც ორივე მხარე ენდობა და რომელიც ინახავს საერთო საიდუმლო გასაღებს. აშკარაა, რომ ეს სქემა გამოიყენება საკმაოდ იშვიათად, ეფექტიანი ალგორითმების არარსებობისა და მესამე მხარისადმი უპირობო რწმენის არსებობის აუცილებლობის გამო. ამიტომ უმრავლეს შემთხვევებში გამოიყენება ასიმეტრიული კრიპტოგრაფიის ალგორითმები, ხოლო ბლოკჩეინ-პროექტებში მას ყველგან იყენებენ.

გარდა სტანდარტული ციფრული ხელმოწერისა, ბლოკჩეინ-პროექტების სხვადასხვა რეალიზაციაში გამოიყენება მისი ეგზოტიკური ფორმები. მაგალითად, „ბრმა ხელმოწერა“, რომელსაც კიდევ უწოდებენ „სამტკიცს ნულოვანი გამჟღავნებით“. „ბრმა ხელმოწერის“ ალგორითმი მარტივია: სისტემის ერთი წევრი შიფრავს თავის შეტყობინებას და უგზავნის მას მეორე წევრს, რომელიც წარმოადგენს სანდო კვანძს (სანდოს სხვა კვანძების რომელიღაც სიმრავლისა) სისტემაში. ეს სანდო წევრი სვამს თავის ხელმოწერას დაშიფრულ შეტყობინებაზე, ამ დროს წარმოდგენა არ აქვს მის შინაარსზე. ამის შემდეგ, ხელმოწერილი შეტყობინება უბრუნდება საწყის გამგზავნს, რომელიც ახდენს მის უკუგაშიფვრას, ტოვებს მხოლოდ სანდო კვანძის ხელმოწერას. ეს შეგვეძლო შეგვედარებინა სიტუაციისათვის, როდესაც სანდო წევრი იღებს დაწებებულ კონვერტს, რომლის შიგნითაც, შეტყობინების ფურცლის გარდა, არის ასევე გადასაღები ქაღალდი. მიმღები კონვერტის გაუხსნელად სვამს მასზე ხელმოწერას, რომელიც გადასაღები ქაღალდის საშუალებით ავტომატურად აისახება შეტყობინების ფურცელზე. გამგზავნისათვის კონვერტის დაბრუნების შემდეგ, ის იღებს შიგნიდან ხელმოწერილ შეტყობინებას და ამგვარად აღწევს სასურველს, იღებს სანდო კვანძის ხელმოწერას ისე, რომ არ გაანდობს კვანძს თვით შეტყობინებას. მსგავსი ოპერაციის ჩატარება შეიძლება სუფთა მათემატიკურადაც, თუ გამოვიყენებთ ასიმეტრიული კრიპტოგრაფიის პროტოკოლებს – მაგალითად, ფაქტორიზაციის ალგორითმი RSA-ის დახმარებით.

რისთვის გამოიყენება ასეთი თავსატეხი ხერხები? სინამდვილეში, ვარიანტი საკმარისზე მეტია. მაგალითის სახით მოვიყვანოთ არჩევნე-

ბზე ფარული კენჭისყრის სისტემა. იმისათვის, რომ მიიღოს ბიულეტენი, ამომრჩეველი იდენტიფიცირებული უნდა იქნას საარჩევნო კომისიის წევრის მიერ, რომელიც არ უნდა ხედავდეს, ვის მისცა ხმა ამომრჩეველმა. „ბრმა ხელმოწერის“ ტექნოლოგიის გამოყენება გარანტიას იძლევა, რომ ბიულეტენებს მიიღებენ მხოლოდ იდენტიფიცირებული ამომრჩევლები, რომელთაც აქვთ ხმის უფლება. შედეგად, შეიძლება ვენდოთ არჩევნების შედეგებს, რადგან საზოგადოებას აქვს საარჩევნო კომისიის თანამშრომელთა მიმართ ნდობა. ანალოგიური პრინციპით მუშაობს ელექტრონული ხმის მიცემის სისტემა, სადაც შემმოწმებელი კვანძი მის მიერ იდენტიფიცირებული ამომრჩევლის შეტყობინებას (რომელიც შეიცავს დაშიფრულ ინფორმაციას მისი არჩევანის შესახებ) აწერს ხელს, რის შემდეგაც უბრუნებს მას ხელმოწერილ შეტყობინებას. ხელმოწერა ამ შემთხვევაში ნიშნავს, რომ ხმის მიცემაში მონაწილეობის უფლების ფაქტი შემოწმებული იქნა ქსელის სანდო კვანძის მიერ. ამომრჩეველი, რომელმაც მიიღო ხელმოწერილი შეტყობინება, გზავნის მას სპეციალური მრიცხველის მისამართზე, რომელიც მას ითვალისწინებს როგორც ერთ-ერთი კანდიდატის მხარდამჭერ ლეგიტიმურ ხმას. მსგავსი ალგორითმები უკვე გამოიყენება ზოგიერთი ქვეყნის ხელისუფლების სხვადასხვა ორგანოს არჩევნებში, დაწყებული მუნიციპალური სტრუქტურებიდან – დამთავრებული სახელმწიფოს პარლამენტებით. ყველაზე ცნობილი ქვეყანა, რომელიც იყენებს ინტერნეტკენჭისყრას ეროვნული საიდენტიფიკაციო ბარათების ბაზაზე, არის ესტონეთი, რომელმაც პირველმა მიმართა ამ პროცედურას 2007 წლის საპარლამენტო არჩევნებში.

ᲪᲔᲮ-ის ჩამოყალიბების კიდევ ერთ საინტერესო მეთოდს წარმოადგენს ე.წ. „რგოლური ხელმოწერა“. ჯერ კიდევ XVII საუკუნეში ბრიტანელი სამხედროები, რომლებიც სხვადასხვა სახის საჩივრებს უგზავნიდნენ უფროსობას, ხელს აწერდნენ მასზე ტექსტის გარშემო, წრიულად. ხელმოწერის ასეთი უცნაური ფორმა გამოიყენებოდა იმისათვის, რომ შეუძლებელი ყოფილიყო პირველი ხელმომწერის ვინაობის ამოცნობა, რომელსაც სარდლობა მაშინვე დააბრალებდა ამ საქმის მოთავეობას. შემდგომში ეს მეთოდი ამერიკელმა სამხედროებმაც გადაიღეს, კერძოდ, XIX საუკუნის ბოლოს, ესპანეთთან ბრძოლისას კუბაზე. როდესაც გაჩნდა ელექტრონული სისტემები, რომლებიც საშუალებას იძლეოდა მონაცემთა სხვადასხვა ბლოკის

ხელმოწერისა, იმავდროულად გაჩნდა აუცილებლობა, ზოგიერთ შემთხვევაში სხვა პოტენციურ კანდიდატთა სიაში შენიღბულიყო კონკრეტული ხელმომწერი. ამისათვის შეიმუშავეს სპეციალური მათემატიკური ალგორითმი, რომელიც ქმნიდა საჯარო გასაღებების გარკვეულ ერთობლიობას, რომელიც დაკავშირებული იყო სისტემის სხვადასხვა მონაწილესთან.

ქსელის მონაწილეთა დიდი ნაწილი ჩვეულებრივ, თავადაც ვერ ხვდება, რომ მისი ღია გასაღებით შეიძლება ისარგებლონ რგოლური ხელმოწერის შესაქმნელად. ღია გასაღებების ამგვარად მიღებულ ერთობლიობაში მხოლოდ ერთს აქვს წყვილში მისი შესაბამისი საიდუმლო გასაღები, რადგანაც მისით ოპერირებს პირადად ხელმომწერი, რომელსაც სურდა, ყველა დანარჩენისათვის უცნობად დარჩენილიყო. თვით რგოლური ხელმოწერა იქმნება ალგორითმის შესავალში ღია გასაღებების (ერთი საკუთარი და მრავალი სხვისი) ერთობლიობის, საკუთარი საიდუმლო გასაღებისა და თვით ხელმოსაწერი შეტყობინების მიწოდების გზით, რის შემდეგაც ხელმომწერი გამოსავალზე იღებს რგოლური ხელმოწერის მონაცემთა სტრიქონს. ამ ხელმოწერის შემოწმება სისტემის სხვა ნებისმიერ წევრს შეუძლია სპეციალური ალგორითმით, რომელიც იყენებს იმავე მონაცემებს, გარდა, რა თქმა უნდა, საიდუმლო გასაღებისა, რადგან ის შეიძლება ცნობილი იყოს მხოლოდ პირადად ხელმომწერისათვის. რგოლური ხელმოწერის შექმნის ალგორითმები ჩვეულებრივ გამოიყენება ბლოკჩეინ-სისტემებში დამატებითი ანონიმიზაციისათვის იმ შემთხვევაში, თუ ტექნოლოგიურად ჩადებული საწყისი გასაიდუმლოება მომხმარებელს არ აკმაყოფილებს. კრიპტოვალუტის მსგავს პროექტებს ჩვენ კიდევ განვიხილავთ ბლოკჩეინში ანონიმურობის პრობლემატიკისადმი მიძღვნილ ნაწილში.

დაბოლოს, არსებობს ელექტრონული ხელმოწერების კონსოლიდაციის სისტემა, რომელსაც „მულტიხელმოწერა“ ეწოდება. იქმნება სიტუაციები, როდესაც წარმოიშობა ერთდროულად სისტემის რამდენიმე წევრის მიერ მიღებული გადაწყვეტილების საფუძველზე ციფრული აქტივების მართვის აუცილებლობა. მაგალითად, არსებობს რაღაც ელექტრონული ანგარიში, რომელზეც დევს მნიშვნელოვანი თანხა, რომელიც ეკუთვნის მონაწილეთა ჯგუფს ან იურიდიულ პირსაც კი. სისტემის წესებით მოცემულია ანგარიშის მმართველთა

რაოდენობა, ასევე – თითოეული მათგანის ხელმოწერის წონის პროცენტული მნიშვნელობა. როგორც ვარიანტი, ნაგულისხმევია, რომ ნებისმიერი გადარიცხვა ამ ანგარიშიდან დადასტურებული უნდა იქნას ყველა მმართველის წონითი მონაწილეობის არანაკლებ 60%-ით. ერთნაირი წონის მქონე სამი მმართველის შემთხვევაში (თითოეულს აქვს 33,3%), აუცილებელია არანაკლებ ორი მონაწილისა, რათა მათ ელექტრონულად მოაწერონ ხელი ტრანზაქციას, რომელიც გადარიცხავს თანხებს (33,3% × 2 = 66,6% > 60%) ისე, რომ ზღვრული პირობა შესრულებულად ითვლებოდეს. მსგავსი პრაქტიკა ბლოკჩეინ-სისტემებში განპირობებულია შესრულებული ტრანზაქციების უკან გამოთხოვების ტექნოლოგიური შეუძლებლობით. ამიტომ კოლექტიურ მფლობელობაში მყოფი მნიშვნელოვანი თანხების გადარიცხვაზე მიღებული ყოველი გადაწყვეტილება უნდა გამორიცხავდეს მის ბოროტად გამოყენებას რომელიმე კონკრეტული პირის მხრიდან, რომელიც დაშვებულია ანგარიშის მართვაში. მულტიხელმოწერა ბლოკჩეინ-პროექტებში შეიძლება განხორციელებული იქნას სხვადასხვა მათემატიკური მეთოდით, ასიმეტრიული კრიპტოგრაფიის ალგორითმების საფუძველზე.

ელექტრონული ხელმოწერის მაიდენტიფიცირებელი და დამცავი ფუნქციონალი ძალზე ფართო შესაძლებლობებს იძლევა მის გამოსაყენებლად ყოველდღიურ პრაქტიკაში, პირველ რიგში – იურიდიულსა და ბიზნესის სფეროებში. ამჟამად ციფრულმა ელექტრონულმა ხელმოწერამ გამოყენება პოვა როგორც კონტრაგენტთა დაშორებული იდენტიფიკაციის საშუალებამ სხვადასხვა შეთანხმების დადებისას, ახალი საწარმოების დაარსებიდან – მსხვილი აქტივების, მათ შორის უძრავი ქონების შეძენამდე. რიგ სახელმწიფოებში ციფრული ელექტრონული ხელმოწერა იურიდიულად გათანაბრებულია ჩვეულებრივთან. საკმაოდ ხშირად ᲑᲔᲭ-ტექნოლოგია, უფრო სწორად კი – მულტიხელმოწერის ალგორითმი გამოიყენება ე.წ. „პირობითი დეპონირების სერვისებში“. მსგავსი მომსახურება აუცილებელია მნიშვნელოვანი გარიგებების დასადებად, რომლისთვისაც იწვევენ მესამე საარბიტრაჟო მხარეს, რომელიც თავისი ხელმოწერით, გარიგებაში მონაწილე კონტრაგენტთა მიერ ვალდებულებების სათანადო შესრულების გარანტიას იძლევა. ᲑᲔᲭ-ის შესაქმნელმა ალგორითმებმა მნიშვნელოვანი გავრცელება პოვა სწორედ ბლოკჩეინ-გარემოში. როგორც მთელი

ტექნოლოგიური პროცესის ქვაკუთხედი, ციფრული ხელმოწერები განაწილებული ქსელის მომხმარებლებს კრიპტოაქტივების საკუთრების უფლების გარანტიას აძლევს, რადგან სისტემაში ჩადებული ინფორმაციის მთლიანობის დაცვას ახორციელებს. რა თქმა უნდა, ინფორმაციის დაცვის ამ მეთოდის გატეხის მიმართ უსაფრთხოებისა და მოუწყვლელობის საკითხები ყოველთვის წინა პლანზე დგას.

წინა თავში აღინიშნა, რომ პირველად შემოთავაზებულ ღიაგასაღებიან დაშიფვრის ალგორითმს (დიფი-ჰელმანის ალგორითმს) არ ჰქონდა ციფრული ხელმოწერის ფორმირების საშუალება, მაგრამ მისი მომდევნო ფაქტორიზაციის ან დისკრეტული გალოგარითმების ალგორითმები, ელიფსური კრიპტოგრაფიის ჩათვლით, საუკეთესოდ გამოდგება ამ მიზნისათვის. მიუხედავად ამისა, არ შეიძლება დარწმუნებულნი ვიყოთ, რომ ისეთ კრიპტომედეგ ალგორითმებსაც კი, როგორიცაა ECDSA, ნათელი მომავალი ელოდება, რადგან მეცნიერები მთელი კრიპტოგრაფიული სამყაროსათვის სიურპრიზს ამზადებენ ე.წ. კვანტური კომპიუტერების სახით. არატრივიალური გამომთვლელი მოწყობილობების სწორედ ასეთ ტიპს შეუძლია საფრთხე შეუქმნას დაშიფვრის ყველა პოპულარულ ალგორითმს. რას წაროადგენს ისეთი მოვლენა, როგორიცაა კვანტური კომპიუტერი, და რატომ უნდა უფრთხოდეს მას კრიპტოგრაფიული ალგორითმები?

კვანტური გამოთვლები

კრიპტოგრაფიული ალგორითმების გატეხის შესაძლებლობა და სახელდობრ ღია გასაღებიდან საიდუმლო გასაღების აღდგენის მცდელობები ყოველთვის შეზღუდული იყო კომპიუტერების გამომთვლელი სიმძლავრეებით. პროცესორების წარმადობა წლებთან ერთად მუდმივად იზრდებოდა, მაგრამ მასთან ერთად იზრდებოდა ალგორითმების კრიპტომედეგობაც. სხვა სიტყვებით რომ ვთქვათ, გატეხის ამოცანა ყოველდღიურად, პროპორციულად რთულდებოდა და ისე ჩანდა, რომ ამ რბოლა-დევნას ბოლო არ ექნებოდა. მაგრამ ბოლო წლებია, ინტეგრალურ სქემებზე აგებული ელექტრონული კომპონენტების, პირველ რიგში მიკროპროცესორების, მწარმოებელ ტექნოლოგთა წინაშე აშკარად გამოისახა ტრანზისტორის როგორც ელექტრონული სქემის საბაზო ელემენტის ზომის შემდგომი შემცირების ფიზიკური საზღვრები. 2018 წლის მდგომარეობით, შემუშავებები ნახევრადგამტარული ტექნოლოგიების დარგში საშუალებას იძლევა, მასობრივად ვაწარმოოთ მიკროპროცესორები 10-ნანომეტრიანი ტექნოლოგიური პროცესების ბაზაზე. სხვა თუ არაფერი, კომპანია Samsung უკვე იყენებს ამ ტექნოლოგიას თავის სმარტფონებში, როცა იმავდროულად, კომპანია Intel ჯერ კიდევ აგრძელებს პროცესორების კეთებას პერსონალური კომპიუტერებისათვის 14 ნმ-იანი ტექნოლოგიით. ნებისმიერ შემთხვევაში, ტრანზისტორის დამზადების ტექნოლოგია თანდათან უახლოვდება ატომურ განზომილებებს, მიუხედავად იმისა, რომ ერთი ატომი აშკარად არ არის საკმარისი მისგან ტრანზისტორის გასაკეთებლად.

სამეცნიერო სამყაროდან მოსული ბოლო ცნობები გვატყობინებს, რომ მეცნიერებმა შეძლეს ტრანზისტორის შექმნა მხოლოდ შვიდი ატომისაგან და ამ რიცხვის შემდგომი შემცირება თითქმის შეუძლებელია. საქმე ისაა, რომ კაჟის ერთ ატომს აქვს 0,2 ნანომეტრი ზომა, მაგრამ ამასთან ერთად ითვლება, რომ ფიზიკური შეზღუდვების გამო კაჟის ტრანზისტორის ჩამკეტის შესაძლო ზომა შეადგენს 5 ნანომეტრს. რას გვეუბნება ეს? იმას, რომ მურის სახელგანთქმულმა კანონმა, რომლის თანახმადაც პროცესორების წარმადობა ორმაგდე-

ბა ყოველ 18 თვეში, პრაქტიკულად მიაღწია თავის ფიზიკურ ზღვარს, რაც, თავის მხრივ, აისახება კომპიუტერების მაქსიმალურად შესაძლო სიმძლავრეზე, რომელიც ასევე შეწყვეტს პროპორციულად ზრდას ისე, როგორც ეს ადრე ხდებოდა. შედეგად, დაშიფვრის კრიპტომედეგი ალგორითმების გატეხაში პროგრესი ნულამდე დავა და ყველა მიმდინარე პროექტი, რომლებიც ამ ალგორითმებზეა დაფუძნებული, ბოლოს და ბოლოს შეძლებს თავი იგრძნოს უსაფრთხოდ. და მაინც, მართლაც ასეა ეს თუ არა?

თუ კომპიუტერების შექმნის კლასიკური ტექნოლოგია მიადგა განვითარების ზღვარს, ეს ნიშნავს, რომ წარმადობის შემდგომი ზრდისათვის გადაწყვეტა უნდა ვეძებოთ პრინციპულად ახალ სამეცნიერო-ტექნოლოგიურ მიმართულებებში. გამოთვლების წარმადობის მნიშვნელოვანი ზრდის შესაძლებლობის ძიებისას ყველაზე პერსპექტიულ სფეროდ ამჟამად ე.წ. კვანტური კომპიუტერები ითვლება.

კვანტური კომპიუტერები არის ჩვენთვის ჩვეულებრივი ორობითი ლოგიკის არქიტექტურისაგან მნიშვნელოვნად განსხვავებული გამომთვლელი მოწყობილობები. კლასიკური წარმოდგენით, მეხსიერების უმცირეს უჯრედს ეწოდება ბიტი, რომელსაც შეუძლია ჰქონდეს მდგრადი მნიშვნელობა ან ნული, ან ერთი. კვანტურ კომპიუტერში კი ბიტს აქვს კვანტური ბუნება და ეწოდება „კუბიტი“. ასეთი კუბიტების როლი შეიძლება შეასრულოს, მაგალითად, სუბატომური ნაწილაკების სპინების მიმართულებებმა, ასევე გარე ელექტრონებისა და ფოტონების სხვადასხვა მდგომარეობამ. კვანტური მექანიკის საფუძვლებს რომ არ ჩავუღრმავდეთ, დაწვრილებით არ განვიხილავთ კვანტური კომპიუტერის ფიზიკურ მოწყობას, არამედ აღვნიშნავთ მხოლოდ ზოგიერთ თვისებას, რომელიც მას კლასიკური კომპიუტერისაგან განასხვავებს.

1931 წელს ავსტრიელმა მეცნიერმა ერვინ შრედინგერმა განახორციელა გონებრივი ექსპერიმენტი, რომელშიც ის ფოლადის კამერაში, სადაც იდგა რადიოაქტიური ატომის ბირთვიანი მოწყობილობა და ასევე შხამიანი გაზით სავსე კოლბა, ათავსებდა პირობით კატას. ექსპერიმენტის პირობების მიხედვით, ატომ-ბირთვს ერთი საათის განმავლობაში ელის დაშლა 50%-ინი ალბათობით. თუ ასე მოხდა, მაშინ ამოქმედდება მექანიზმი, რომელიც კოლბას გატეხს, რის შემდეგაც კატა დაიღუპება. მაგრამ თუ ბირთვის დაშლა მაინც არ მოხდა, მაშინ კატა უვნებელი დარჩება. ამ ექსპერიმენტის აზრი იმაშია,

რომ გარე დამკვირვებელმა ზუსტად არასდროს იცის, დაიშალა თუ არა ბირთვი, ცოცხალია თუ არა კატა მანამ, სანამ თვითონ არ გახსნის ყუთს, ხოლო ამ მომენტამდე ითვლება, რომ კატა ერთდროულად ცოცხალიც არის და მკვდარიც.

გასაგებია, რომ არც ერთ არსებას ჩვენს სამყაროში არ შეუძლია ერთდროულად ორ სხვადასხვა მდგომარეობაში ყოფნა დროის ერთსა და იმავე მონაკვეთში. ამიტომ უფრო სწორი იქნებოდა გვეთქვა, რომ კატა არის ე.წ. „სუპერპოზიციის“ მდგომარეობაში, რომელშიც მდგომარეობის ყველა შესაძლო ვარიანტი მიიღება ალბათობის სხვადასხვა ხარისხით. ამასთან, ყველა შესაძლო მდგომარეობის ალბათობათა ჯამი აუცილებლად 100%-ის ტოლი უნდა იყოს. იგივე შეიძლება ვთქვათ კვანტური კომპიუტერის კუბიტის მუშაობის პრინციპზეც – ის ამგვარადვე შეიძლება იმყოფებოდეს სუპერპოზიციის მდგომარეობაში და ერთდროულად იღებდეს ლოგიკური ნულისა და ერთიანის მნიშვნელობებს. კუბიტის მდგომარეობის გაზომვის უშუალო მომენტამდე მისი ზუსტი მნიშვნელობა დამკვირვებლისათვის უცნობია, ხოლო გაზომვისა და შედეგის მიღების შემდეგ კუბიტი მაშინვე ფიქსირდება დანამდვილებით, ნულის ან ერთიანის მდგომარეობაში. კუბიტების ეს პირველი შეხედვით უცნაური თვისება ძალზე სასარგებლო აღმოჩნდა რთული გამოთვლითი ამოცანების პარალელური ანგარიშის ორგანიზაციაში, კრიპტოგრაფიული ალგორითმების ჩათვლით.

კუბიტების კიდევ ერთი საინტერესო თავისებურებაა, რომ ერთად მათ შეუძლია ყოფნა ე.წ. „კვანტური დახლართულობის“ მდგომარეობაში, როდესაც ერთი კუბიტის მდგომარეობის შეცვლა ავტომატურად იწვევს მასთან დაკავშირებული მეორის მდგომარეობის შეცვლას საწინააღმდეგო მდგომარეობით. დიდი რაოდენობის კუბიტების ერთმანეთში კვანტური დახლართულობის ორგანიზება ტექნოლოგიურად ძალზე რთულია, რადგან მათ აუცილებლად საგულდაგულოდ უნდა გავუკეთოთ იზოლირება გარემოში ნებისმიერი სახის დაბრკოლებისაგან. ამჟამად კვანტური კომპიუტერების წამყვანმა მწარმოებლებმა, მაგალითად, ისეთებმა, როგორიცაა Google, შეძლეს შეკრულ მდგომარეობაში მთელი 72 კუბიტის დაჭერა, რაც ჯერჯერობით მსოფლიო რეკორდია მსგავს შემუშავებებს შორის. ბევრია თუ ცოტა 72 კუბიტი გატეხის ამოცანების გადასაჭრელად, თუნდაც, მაგალითად, ფაქტორიზაციის RSA ალგორითმისათვის? თუ განვიხილავთ n ჩვეულებრივ

ბიტს, მაშინ 2^n შესაძლო მდგომარეობიდან დროის ერთ მომენტში შეიძლება ამოვირჩიოთ მხოლოდ ერთი, ამ დროს n კუბიტი სუპერპოზიციის მდგომარეობაში იქნება ერთდროულად 2^n მდგომარეობაში. როგორც შედეგი, კუბიტების რაოდენობის წრფივი ზრდისას შესაძლო მდგომარეობების რაოდენობა გაიზრდება ექსპონენციურად. ეს კი, თავის მხრივ, ნიშნავს, რომ დიდი რაოდენობის კუბიტების მქონე კვანტურ კომპიუტერს ექნება განსაკუთრებული გამომთვლელი სიმძლავრე. კვანტური გამოთვლების სფეროში უახლესი შემუშავებების გათვალისწინებით, სპეციალისტების შეფასებით, ჩვეულებრივი კომპიუტერებისა და კვანტური კომპიუტერების სომძლავრეებს შორის სხვაობა არანაკლებ მილიარდჯერადია. ამასთან, კვანტურ კომპიუტერს მთავარი უპირატესობა ექნება სწორედ ვარიანტების გადარჩევასთან დაკავშირებული მათემატიკური ამოცანების ამოხსნისას.

მიუხედავად ამისა, ასეთი მნიშვნელოვანი გამომთვლელი სიმძლავრეც კი შეიძლება საკმარისი არ აღმოჩნდეს ღია გასაღების მქონე კრიპტოალგორითმების ადვილად გასატეხად. ამისათვის აუცილებელი კუბიტების რაოდენობა ბევრად უფრო მაღალი სიდიდეებით განისაზღვრება: მაგალითად, 2048-ბიტიანი ფაქტორიზაციის ალგორითმ RSA-სთვის საჭირო იქნება ზუსტად ორჯერ მეტი კუბიტი. ეს მონაცემები ნაანგარიშებია ჰიბრიდული (შეიცავს როგორც კლასიკურ, ისე კვანტურ ნაწილებს) ალგორითმის გამომთვლელი მოთხოვნების საფუძველზე, რომელიც 1994 წელს წარმოადგინა ამერიკელმა მეცნიერმა, კვანტური ინფორმატიკის სფეროს სპეციალისტმა პიტერ შორმა, ხოლო ელიფსური კრიპტოგრაფიის გასატეხად კუბიტების აუცილებელი რაოდენობა, რაოდენ საკვირველიც უნდა იყოს, ნაკლებია: 256-ბიტიანი გასაღებებისთვის საჭირო იქნება 1536 კუბიტი, ხოლო 512-ბიტიანისთვის – 3072. კვანტური კომპიუტერების წარმადობის ზრდის სიჩქარის გათვალისწინებით (ხოლო ამჟამად ის აჭარბებს მურის კანონს), იმ მომენტამდე, როდესაც ყველაზე პოპულარული კრიპტოალგორითმები დათმობს საკუთარ პოზიციებს, შესაძლოა, თითებზე ჩამოსათვლელი წლები დარჩა. ამგვარად, ამ პოტენციური საფრთხის გადაჭრაზე სპეციალისტმა-კრიპტოგრაფებმა აუცილებლად ახლავე უნდა იზრუნონ.

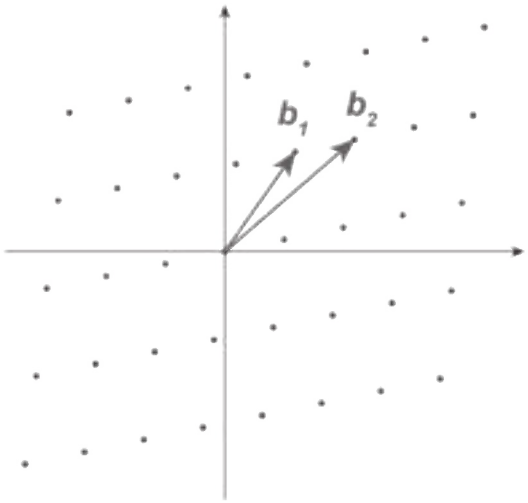
ყველაფერი ეს არც ისე საშიშია, როგორც ერთი შეხედვით შეიძლება მოგვეჩვენოს. უკვე შემუშავებულია ასიმეტრიული კრიპტო-

გრაფიის რიგი ალგორითმებისა, რომლებიც კვანტური გადარჩევისადმი მდგრადი რჩება საკმაოდ დიდი რაოდენობის კუბიტების გამოყენების შემთხვევაშიც კი. ასეთ ალგორითმებს „პოსტკვანტურებს“ უწოდებენ, და სწორედ ზოგიერთ მათგანზე ვისაუბრებთ. კერძოდ, ლემპორტის ხელმოწერაზე, ცხაურებზე აგებულ კრიპტოგრაფიასა და ელიფსური მრუდების იზოგენიებზე.

ციფრული ელექტრონული ხელმოწერის შექმნა ლემპორტის ალგორითმის ბაზაზე არის კრიპტოგრაფიის ჰეშ-ფუნქციისა და შემთხვევითი რიცხვების გენერატორის გამოყენება. იქმნება 256 წყვილი შემთხვევითი რიცხვი, თითოეული 256 ბიტის სიგრძით. ჯამური 16 კილობაიტის მოცულობის მქონე მონაცემთა ეს ერთობლიობა იქნება საიდუმლო გასაღები. ყოველი 256-ბიტიანი წყვილი ჰეშირდება და ეს 512 ჰეში იქნება ღია გასაღები. შემდეგ საიდუმლო გასაღების საფუძველზე გასაგზავნი შეტყობინებისათვის შეიქმნება ელექტრონული ხელმოწერა. როგორც ცნობილია, ელექტრონული ხელმოწერით შეტყობინების დასადასტურებლად, თავდაპირველად მისი ჰეშირება უნდა მოხდეს. შემდეგ დგება ელექტრონული ხელმოწერა, რომელშიც შეტყობინების ბიტის ჰეშის ყოველი მნიშვნელობისათვის (ნულის ან ერთიანისთვის) ამოირჩევა ან პირველი, ან მეორე რიცხვი საიდუმლო გასაღების იმ წყვილიდან, რომელიც შეესაბამება ჰეშში ბიტის რიგით ნომერს.

ამ ალგორითმის კრიპტომედეგობა დამოკიდებულია გამოყენებული ჰეშ-ფუნქციის ტიპზე. იმის გათვალისწინებით, რომ ჰეშირების პროცედურას აქვს მკაცრად ცალმხრივი ხასიათი, და ასევე იმ ფაქტიდან გამომდინარე, რომ ჰეშირდება მონაცემთა მნიშვნელოვანი რაოდენობა (256 წყვილი), საიდუმლო გასაღების ღიადან უკუაღდგენის ამოცანის გადაჭრა კვანტურ კომპიუტერსაც კი არ შეუძლია. მაგრამ ეს ალგორითმიც არ არის სრულყოფილი. ჯერ ერთი, გასაღებებს აქვს მნიშვნელოვანი ზომა (16 კილობაიტამდე). მეორეც, ამ ალგორითმით ელექტრონული ხელმოწერის შექმნისას საიდუმლო გასაღების ნახევარი ფაქტობრივად, საჯარო ხდება. ამიტომ ერთი გასაღების საფუძველზე ხელმოწერა უმჯობესია გამოვიყენოთ მხოლოდ ერთხელ, რაც ასევე ქმნის მნიშვნელოვან მოუხერხებლობას ამ ალგორითმის საფუძველზე სისტემების პროექტირებისათვის.

შემდეგი ალგორითმი, რომელიც ასევე პოსტკვანტურად ითვლება, არის ე.წ. „ცხაურებზე აგებული კრიპტოგრაფია“. ცხაურებს მათემატიკაში უწოდებენ წერტილთა პერიოდულ ბადეს კოორდინატთა n-განზომილებიან სისტემაში, სადაც მოცემულია „საბაზო ვექტორების“ რიცხვი n, რომლებიც ქმნის თვით ცხაურს. აი, ცხაურის მარტივი მაგალითი კოორდინატთა მართკუთხა სისტემისათვის, ორი მოცემული საბაზო ვექტორით.



ამ ალგორითმში გამოსათვლელად რთული ამოცანაა ე.წ. SVP-ის (Shortest Vector Problem) პოვნა ანუ „ყველაზე მოკლე ვექტორის“ პოვნა მოცემული საბაზო ვექტორებისათვის n სივრცის განზომილების მნიშვნელოვანი გაზრდის პირობით. თუ განვიხილავთ ჩვეულებრივ ბრტყელ ორგანზომილებიან ცხაურს, მაშინ თვალით ამ კვანძთან ყველაზე ახლოს მყოფი წერტილის პოვნა ადამიანისათვის არავითარ სირთულეს არ წარმოადგენს. მაგრამ თუ ამას კომპიუტერი აკეთებს, მაშინ საქმეში არცთუ ისე მარტივი მათემატიკური გამოთვლები ერთვება, ხოლო თუ დავიწყებთ სივრცული განზომილებების რაოდენობის ზრდას, მაშინ პროცესი ძალზე სერიოზულ გამოთვლით ამოცანად გადაიქცევა. ითვლება, რომ ამჟამად ასეთი ამოცანის სირთულე აჭარბებს კვანტური კომპიუტერის შესაძლე-

ბლობებს, მაგრამ ცხაურებზე აგებულ კრიპტოგრაფიაზე დაფუძნებული ალგორითმებიდან, მოუწყვლადად ჯერჯერობით ითვლება მხოლოდ უშუალოდ დაშიფვრა. ციფრული ელექტრონული ხელმოწერა გატეხეს უკვე 1999 წელს, ხოლო მისი მოდიფიცირებული ვერსია – 2006 წელს. ამჟამად მათემატიკოსები მუშაობენ ᲐᲔᲖ-ის შემდგომ განვითარებაზე, რათა ეს პრობლემა გადაჭრან და ინდუსტრიას კრიპტოგრაფიული უსაფრთხოების ახალი, უფრო სრულყოფილი სტანდარტი შესთავაზონ.

დაბოლოს, განვიხილოთ, შესაძლოა ამ მომენტისათვის ყველაზე პერსპექტიული ალგორითმი – ელიფსური მრუდების იზოგენიებზე დაფუძნებული კრიპტოგრაფიის გამოყენება. იზოგენია არის მეთოდი, რომელიც საშუალებას იძლევა, ერთ ელიფსურ მრუდზე მდებარე წერტილი ავსახოთ მეორე მსგავსი ტიპის მრუდზე მდებარე წერტილში. წერტილების გარდასახვის ალგორითმი წარმოადგენს ორი პოლინომის (მრავალწევრის) თანაფარდობას წერტილის ყოველი კოორდინატისათვის x და y ღერძებზე. იმ შემთხვევაში, თუ ასეთი ასახვის მიღება მათემატიკურად შესაძლებელია, ეს ორი მრუდი ერთმანეთის მიმართ იზოგენური იქნება. თითოეული მრუდისათვის შეიძლება გამოვთვალოთ ე.წ. „j-ინვარიანტი“, რომელიც ელიფსური მრუდის გარკვეულ „კლასიფიკატორად“ ითვლება და წარმოდგენილია ჩვეულებრივი რიცხვების სახით. j-ინვარიანტის გამოსათვლელად გამოიყენება ელიფსური მრუდის განტოლების კოეფიციენტები. კოეფიციენტთა სხვადასხვა მნიშვნელობის გამოყენებით, გამოითვლიან მრავალ ვარიანტს, რომლებიც შემდეგ აისახება დიაგრამის სახით. მიღებულ დიაგრამაში ინვარიანტები ხდება მისი წვეროები, ხოლო დიაგრამის წიბოები არის იმ ინვარიანტთა შეერთება, რომელთა ელიფსური მრუდები იზოგენურია ერთმანეთის მიმართ. სწორედ დიაგრამაში წვეროებს შორის გზების პოვნა ანუ, სხვა სიტყვებით რომ ვთქვათ, სწორედ იზოგენიების გამოთვლა სხვადასხვა ელიფსურ მრუდს შორის არის ის რთულად გამოსათვლელი ამოცანა, რომლის საფუძველზეც იგება ეს კრიპტოგრაფიული ალგორითმი. ელიფსური მრუდების ერთმანეთზე მიმდევრობით დადებული გრაფების საფუძველზე აგებული სტრუქტურები წარმოადგენს ძალზე ლამაზ გეომეტრიულ ობიექტებს, როგორიცაა, მაგალითად, სურათზე ნაჩვენები რთული „იზოგენური ვარსკვლავი“:

აშკარაა, რომ იზოგენიების გამოყენება მნიშვნელოვნად ართულებს ელიფსურ კრიპტოგრაფიას. თუ კლასიკურ ვარიანტში საქმე გვაქვს მხოლოდ ერთ ელიფსურ მრუდთან, მაშინ იზოგენიების შემთხვევაში საქმე გვაქვს მათ მთელ „ოჯახთან“, რაც ამოცანას კიდევ უფრო ართულებს. კვანტურ კომპიუტერსაც კი არ ძალუძს ამ ამოცანის ამოხსნა სუბექსპონენციურ დროში, რაც ალგორითმის კრიპტომედეგობაზე მეტყველებს და რომელიც სავსებით დარწმუნებით შეიძლება ჩაითვალოს „პოსტკვანტურად“. ალბათ ეს ალგორითმი ამჟამად ყველაზე გამოსადეგია მის საფუძველზე ბლოკჩეინ-პროექტების ასაგებად, რომლებიც ისწრაფვის თავისი მომხმარებლებისათვის მონაცემთა მაქსიმალური უსაფრთხოების უზრუნველყოფისაკენ. კვანტური გამოთვლების აქტიურად განვითარებადი ინდუსტრიის ფონზე ეს პრობლემა მართლაც აქტუალური ხდება.

თამაშის თეორია და ბლოკჩეინი

როდესაც განვიხილავდით დეცენტრალიზაციას როგორც მართვის მეთოდს, ყურადღება გავამახვილეთ სისტემებში ერთნაირი უფლებების მქონე სუბიექტების ურთიერთქმედების სირთულის პრობლემატიკაზე, სადაც მაკონსოლიდირებელი და მმართველი ცენტრი არ არსებობს როგორც კლასი. და მართლაც, მაინც რომელი ყველაზე ეფექტიანი მეთოდით უნდა მივიდნენ სისტემის ერთნაირი უფლებების მქონე სუბიექტები ერთობლივ გადაწყვეტილებებამდე, რომლებიც ხელს აძლევს თუ ყველას არა, უდიდეს უმრავლესობას მაინც? აშკარაა, უნდა არსებობდეს საზოგადოებრივი თანხმობის რაღაც პროცედურულად განპირობებული ფორმა, რომელიც იმ გადაწყვეტილების მიღების საშუალებას იძლევა, რომელიც სავალდებულოდ შესასრულებელი იქნება მთელი საზოგადოებისათვის. ამასთან, მან არ უნდა შექმნას გადაუჭრელი კონფლიქტები, რომლებიც მთელი სისტემის დანგრევას გამოიწვევს. ზომების ამ კომპლექსს ეწოდება წესების ჩამოყალიბება კონსენსუსის მისაღწევად ანუ ერთსულოვნება დაინტერესებულ პირთა აზრებს შორის სისტემისათვის მნიშვნელოვანი გადაწყვეტილებების მისაღებად, რესურსების თვალსაზრისით დანახარჯებიანი პირდაპირი კენჭისყრის გარეშე.

სისტემის წევრთა მისწრაფებების ერთობლიობა, ნახონ საკუთარი ან საზოგადოებრივი ხეირი, ამავდროულად გადალახონ სხვა საწინააღმდეგო ინტერესების მქონე წევრთა აშკარა თუ ფარული წინააღმდეგობა, შეიძლება სიტყვა „თამაშით“ გადმოვცეთ. რა თქმა უნდა, საკუთარი მიზნების რეალიზებისათვის ყველა წევრი ოპერირებს სპეციალურად შექმნილი ამა თუ იმ სტრატეგიით, რომელიც დასახული ამოცანების გადაჭრაში მაქსიმალური ეფექტის მიღწევას ესწრაფვის. მათემატიკაში არსებობს სპეციალური თავი, მიძღვნილი თამაშებში ოპტიმალური სტრატეგიების შესწავლისადმი. მას ასევე ჰქვია – „თამაშის თეორია“, და ჩვენ განვიხილავთ მის ცალკეულ ელემენტებს, რადგანაც ისინი წარმოადგენს მნიშვნელოვან რგოლს ბლოკჩეინ-სისტემების აგებისას, რომლებიც თითქმის ყოველთვის დეცენტრალიზებულია, ხოლო მისი წევრები თანაბარუფლებიანები არიან. საუბარია

პირველ რიგში, ქსელის კვანძებს შორის კონსენსუსის ჩამოყალიბების მეთოდებზე ბლოკების ჯაჭვის, ასევე, მათში ტრანზაქციათა ნაკრების შექმნისას. ოღონდ, ამაზე – ცოტა მოგვიანებით. თავიდან ვეცადოთ, ცხადი გავხადოთ ჩვენთვის, თუ რა არის ეფექტიანი ან არაეფექტიანი სტრატეგია საერთო თანხმობის მიღწევისას.

სტრატეგიის ეფექტიანობა უწყვეტადაა დაკავშირებული წევრთა რაციონალური ქცევის ცნებასთან. იმისათვის, რათა დავრწმუნდეთ, რომ „თამაშის“ მონაწილეთა შორის თანამშრომლობა ყოველთვის გარანტირებული არ არის, თუნდაც ეს მათ საერთო ინტერესებს ეთანადებოდეს, განვიხილოთ ცნობილი „პატიმრის დილემა“. ის წარმოდგენილი იყო ამერიკელი მათემატიკოსების – მერილ ფლადისა და მელვინ დრეშერის მიერ. ციხეში ერთდროულად და ერთი და იმავე საქციელისთვის მოხვდა ორი დამნაშავე. პოლიციამ არცთუ უსაფუძვლოდ ივარაუდა მათ შორის პირის შეკვრის შესაძლებლობა და ისინი ერთმანეთისაგან გააცალკევა, შემდეგ თითოეულს გამოძიებასთან თანამშრომლობის ერთნაირი პირობები შესთავაზა. თანამშრომლობის ფორმა გულისხმობდა ერთი პატიმრის ჩვენებას მეორეს წინააღმდეგ და სანაცვლოდ, დაუყოვნებლივ გათავისუფლებას. ისიც ნაგულისხმევია, რომ, თუ მეორე პატიმარი პოლიციასთან თანამშრომლობაზე უარს იტყვის, მას პატიმრობის მაქსიმალურ ვადას მიუსჯიან. თუ ორივე პატიმარი უარს იტყვის თანამშრომლობაზე, მაშინ ორივეს მინიმალურ ვადას მიუსჯიან. თუკი ორივე მოწმედ დადგება ერთმანეთის წინააღმდეგ, ორივეს მიუსჯიან საშუალო ხანგრძლივობის ვადას. გასაგებია, რომ ერთმანეთისაგან იზოლაციაში მყოფმა პატიმრებმა ერთმანეთის გადაწყვეტილების შესახებ არაფერი იციან. მაშ, როგორი უნდა იყოს ყველაზე ეფექტიანი სტრატეგია თითოეული პატიმრისათვის?

ამ სიტუაციას დილემა ეწოდება იმიტომ, რომ თითოეული ცალკე აღებული პატიმრისთვის და მათი ჯგუფად განხილვის შემთხვევაში, უპირატესი სტრატეგიები აზრობრივად, დიამეტრულად საწინააღმდეგოა. კონკრეტული პატიმრისთვის უმჯობესია, მთელი დანაშაული მეორეს გადააბრალოს და მაშინ მას აქვს შანსი, დაუყოვნებლივ გამოვიდეს ციხიდან. მაგრამ ორივე პატიმრისთვის, როგორც ჯგუფისთვის, უმჯობესია გაჩუმდეს, რადგან პატიმრობის ჯამური ვადა ორივე პატიმრისათვის მინიმალური იქნება ყველა შესაძლებელს შორის.

ამგვარად, თუ ცალ-ცალკე ორივე სუბიექტი რაციონალურად იქცევა, მაშინ ერთობლიობაში შედეგი ხდება არარაციონალური გადაწყვეტა. მსგავსი სიტუაცია გარკვეული აზრით ასახავს პრობლემატიკის სირთულეს, რომელსაც თამაშის თეორია სწავლობს, როდესაც ერთი მონაწილე ცდილობს საკუთარი ინტერესის მაქსიმალურად დაცვას საერთო ხეირის საწინააღმდეგოდ. მსგავსი პრაქტიკა ბლოკჩეინ-სისტემებში შემდეგი თვალსაჩინო მაგალითით ხორციელდება.

დავუშვათ, ფულადი ეკვივალენტის მქონე ციფრული აქტივების შესანახ დეცენტრალიზებულ სისტემაში (მაგალითად, კრიპტოვალუტაში) მოიძებნა რაღაც კვანძი, რომელმაც სხვადასხვა არაკეთილსინდისიერი პრაქტიკების დახმარებით მოახერხა, მთელი ქსელისთვის თავს მოეხვია ხელოვნური ტრანზაქცია, რომლის შედეგადაც ციფრული მონეტების უზარმაზარი რაოდენობის მფლობელი გახდა. კითხვა: ვინ მოიგებს ამ აქციით? ვინმემ შეიძლება იფიქროს, რომ მოიგებს ბოროტმოქმედი, რადგან მისი ქმედების შედეგი პირდაპირი გამდიდრება გახდა. რა თქმა უნდა, წააგეს აქტივების ყოფილმა მფლობელებმა, რომლებმაც ქსელსა და მათ პერსონალურ ანგარიშებზე შეტევის შედეგად ისინი დაკარგეს. სისტემის სხვა წევრები კი არ დაზარალდნენ, დარჩათ საკუთარი აქტივები, რომლებსაც ზიანის მომტანი კვანძი ვერ მისწვდა. მაგრამ ეს მხოლოდ ზედაპირული დასკვნებია. ქსელზე თავდასხმით ბოროტმოქმედმა სინამდვილეში, გამოუსწორებელი შეცდომა ჩაიდინა, დააზარალა ქსელისადმი დამოკიდებულება მთლიანობაში, დამოკიდებულება მისი უსაფრთხოების კონცეფციის, კრიპტოგრაფიული მოუწყვლადობის, ასევე, კონსენსუსის ჩამოყალიბების პროტოკოლის მიმართ. ეს კი ნიშნავს, რომ ამ ქსელის ყველა ღირებული აქტივი, რომლებსაც ჰქონდა მონეტარული ან საბირჟო შეფასებაც კი, მეყსეულად დაკარგავს ღირებულებას. ეს ეხება თავად ბოროტმოქმედის მიერ არაკეთილსინდისიერად მიღებულ აქტივებსაც, რაც ფაქტობრივად, მის ქმედებებს პირადად, საზოგადოებრივად უსარგებლოდ აქცევს. ქსელი ინგრევა და წყვეტს არსებობას. ამ სიტუაციაში გამარჯვებულები არ არიან, არიან მხოლოდ დამარცხებულები.

- ეს მაგალითი კარგად გვიჩვენებს, რამდენად მნიშვნელოვანია საერთო თანხმობის პროტოკოლი დეცენტრალიზებულ სისტემებში. ის არანაკლებ მნიშვნელოვან როლს თამაშობს,

ვიდრე სისტემაში გამოყენებული მონაცემთა დაშიფვრის ალგორითმების კრიპტომედეგობა. რა სახის მეთოდები შეიძლება გამოვიყენოთ ბლოკჩეინ-პროექტებში კონსენსუსის მისაღწევად? ერთ-ერთი ყველაზე პოპულარულია კონსენსუსი „ბიზანტიელ გენერალთა პრობლემის“ საფუძვლეზე. გადავიდეთ შუა საუკუნეების ბოლო პერიოდში, როდესაც ბიზანტიის იმპერია უკვე დაცემის გზას ადგა. წარმოვიდგინოთ, რომ ბიზანტია ომის მდგომარეობაშია და იმპერატორმა მტრის ერთ-ერთი ქალაქის დასაპყრობად გაგზავნა რაღაც რაოდენობის ჯარები, რომელთაც გენერლები სარდლობენ. გენერლები სამხედროები არიან, რომელთათვისაც თითქოს უცხო არ არის ერთგულება და ღირსება, მაგრამ იმ პერიოდის ბიზანტიაში მხედართმთავრებისათვის ასეთი პირადი თვისებები საკმაოდ უცხო იყო. ამ გარემოების გამო, ყოველი გენერალი გარკვეული ალბათობით, შეიძლება მოსყიდული ყოფილიყო მოწინააღმდეგის მიერ, სხვაგვარად რომ ვთქვათ – მოღალატე გამხდარიყო. თავისი ერთგულების ხარისხიდან გამომდინარე, თითოეულ გენერალს შეეძლო პირდაპირ მიჰყოლოდა ზევიდან წამოსულ ბრძანებას, მაგრამ შეეძლო მოქცეულიყო სრულიად საწინააღმდეგოდაც, რითაც ხელს შეუწყობდა ომში იმპერიის დამარცხებას. დავუბრუნდეთ მათემატიკას და განვიხილოთ შესაძლო დასასრულის ვარიანტები. ერთგულ გენერლებს, ბრძანების შესაბამისად, ერთად მიჰყავთ საკუთარი არმიები ქალაქზე შესატევად, ქალაქი აღებულია, ომი – მოგებული. აშკარაა, რომ ეს ბიზანტიისათვის საუკეთესო შედეგია.

- ერთგული გენერლები, ბრძანების შესაბამისად, ერთდროულად იხევენ უკან, ქალაქი ვერ აიღეს, მაგრამ მთელი ჯარები შენარჩუნებულია შემდგომი ბრძოლებისათვის. ეს შედეგი შეიძლება შუალედურად ჩაითვალოს.
- ერთგული გენერლები, როგორც ნაბრძანები აქვთ, უტევენ, მაგრამ მოღალატე გენერლები შეტევის მაგივრად უკან იხევენ, შედეგად მთელი ჯარები განადგურებულია, ხოლო თვით ომი ბიზანტიის მიერ წაგებულია. ეს არის ყველაზე უარესი შესაძლო ვარიანტებიდან.

ზოგჯერ ამოცანას ართულებენ მთავრსარდლის მონაწილეობით, რომელსაც უფლება აქვს, ბრძანებები ქვემდგომ გენერლებზე გასცეს. გართულების არსი იმაშია, რომ თვითონ მთავარსარდალიც შეიძლება მოღალატე იყოს. მაშინ სხვადასხვა გენერალს ის აზრობრივად სხვადასხვა ბრძანებას მისცემს, რათა გარანტირებულად მიიღოს ბიზანტიისათვის ყველაზე უარესი შედეგი. ამ შემთხვევაში, ყველა გენერლისათვის საუკეთესო სტრატეგია იქნებოდა მთავარსარდლის ბრძანებების სრული იგნორირება. გვერდზე გადავდოთ სამხედრო დისციპლინის საკითხები და ყურადღება გავამახვილოთ იმაზე, თუ როგორ შეიძლება მიღწეულიყო საუკეთესო შედეგი ამგვარ სიტუაციაში. აშკარაა, რომ თუ ყველა გენერალი იმოქმედებს საკუთარი მოსაზრებებით (ვთქვათ, თანაბარი ალბათობით, შეტევისა და უკან დახევის გადაწყვეტილების მიმართ), ხელსაყრელი და საშუალო შედეგის მიღწევის შესაძლებლობა ბიზანტიისათვის ძალზე მცირეა. ამ სიტუაციაში ერთადერთი ოპტიმალური გადაწყვეტილებაა გენერლებს შორის ინფორმაციის პირდაპირი გაცვლა.

ინფორმაციას, რომელსაც გენერლები ერთმანეთში ცვლიან, შეიძლება ჰქონდეს სხვადასხვა ხასიათი. ეს შეიძლება იყოს ცნობები თითოეული არმიის რაოდენობაზე ან საკუთარი განზრახვის დაფიქსირება, შეტევის ან უკან დახევის შესახებ. მნიშვნელოვანია, რომ თითოეული გენერალი (დავუშვათ, მათი რაოდენობაა n) ყველა დანარჩენ გენერალს გადასცემს საკუთარ ინფორმაციას და უკან იღებს n-1-ის მსგავსს. მაგრამ ეს ჯერ კიდევ არ არის ყველაფერი. გამოდის, რომ თითოეული გენერალი ფლობს ინფორმაციის გარკვეულ მოცულობას, რომელიც მიღებულია ყველა დანარჩენი გენერლისაგან პირდაპირი ურთიერთობით, და მას შეუძლია, მიღებული ინფორმაციის რეტრანსლირება მოახდინოს სხვა გენერლებისთვის, ასევე, სხვებისაგან მიიღოს ინფორმაციის მსგავსი ნაკრებები. ამგვარად, თითოეული გენერალი ფლობს არა მარტო იმ ინფორმაციას, რომელიც პირდაპირი გზით მიიღო ყველა სხვა გენერლისაგან, არამედ მის განკარგულებაშია აგრეთვე, მთელი საკომუნიკაციო სურათი ფორმატში „რომელმა გენერალმა რომელ გენერალს რა აცნობა“. ამასთანავე, უნდა გავითვალისწინოთ ის ფაქტი, რომ ერთი ან რამდენიმე გენერალი შეიძლება მოღალატე იყოს და ამიტომ წინასწარი განზრახვით გააყალბოს გადაცემული ინფორმაცია. მიუხედავად ამისა, ყოველთვის

შესაძლებელია შევამოწმოთ, რა გადასცა კონკრეტულმა გენერალმა სხვა გენერლებს, და ინფორმაციაში ვიპოვოთ ან დამთხვევები, ან განსხვავებები. მიღებული მონაცემების საფუძველზე შეგვიძლია გამოვავლინოთ ორპირი გენერლები და შევაფასოთ მათი წილი საერთო მასაში. მათემატიკურად დამტკიცებულია, რომ ერთგული კვანძების 2/3-ის შემთხვევაში, სისტემა მდგრადად ითვლება და კონსენსუსის მიღწევა შესაძლებელია, წინააღმდეგ შემთხვევაში, სისტემა კარგავს ქმედითობას და შედეგად – წევრების ნდობასაც.

„ბიზანტიური პრობლემისადმი“ მდგრადობის პრინციპი არის კლასიკური ამოცანა „თამაშის თეორიიდან“, რომელიც ბლოკჩეინ-პროექტებში კონსენსუსის ჩამოყალიბებისას უსაფრთხოების მნიშვნელოვან ელემენტს წარმოადგენს. სისტემის თითოეული კვანძი მკაცრად უნდა იცავდეს მის წესებს, რომლებიც მოცემულია კვანძის პროგრამული უზრუნველყოფის ალგორითმული ლოგიკის სახით. მაგრამ ბლოკჩეინ-პროექტებში თითქმის ყველა პროგრამული უზრუნველყოფა მოგვეწოდება ღია კოდის სახით, რომელსაც სურვილისამებრ, შეუძლია ყოველი კვანძის მოდიფიცირება იმგვარად, რომ ეცადოს მიიღოს პრეფერენციები, რომლებიც ჩვეულებრივ სიტუაციაში არ ეკუთვნოდა. მაგრამ მაშინაც კი, თუ ქსელის მიერ არასანქცირებული კვანძები შემოვა ცალკეული კვანძების (ან კვანძების ჯგუფის) სახით, შეტევის წარმატებისათვის აუცილებელია, რომ ასეთი კვანძი საკმაოდ ბევრი იყოს. სხვაგვარად, დანარჩენი ქსელი უარყოფს ინფორმაციას დამრღვევებისაგან, რადგანაც ის არ შეესაბამება საერთო წესებს, რომლითაც უმრავლესობა ხელმძღვანელობს. სწორედ ამაში მდგომარეობს კონსენსუსის არსი, რომელიც დეცენტრალიზებული სისტემების სამართავად გამოიყენება. სისტემის მთლიანობა ირღვევა, თუ „სხვაგვარად მოაზროვნე“ კვანძების რაოდენობა იწყებს კრიტიკული მასის გადაჭარბებას, რის შემდეგაც ხდება ქსელის გაყოფა, რასაც ეწოდება „ფორკი“. კვანძები, რომლებიც კონსენსუსის სხვადასხვა წესს ქადაგებს, აყალიბებს სხვადასხვაგვარ ქსელს, რომლებიც გაყოფის მომენტიდან იწყებს საკუთარი ცხოვრებით არსებობას, რადგან არსებითად, განსხვავებულ პროექტებად იქცევა, თუმცა მსგავსი ტექნოლოგიებითაა შექმნილი, უკიდურეს შემთხვევაში, საწყის მომენტებში მაინც. ცნება „ფორკს“ როგორც ბლოკჩეინ-ინდუსტრიის მნიშვნელოვან მოვლენას, ჩვენ კიდევ დავუბრუნდებით.

იმისათვის, რომ კონკრეტული მაგალითებით ავხსნათ კონსენსუსის მუშაობა ბლოკჩეინ-გარემოში, აუცილებელია გადავიდეთ ბლოკებისა და ტრანზაქციების სტრუქტურების შესწავლაზე, აგრეთვე – ბლოკებისა და მათი ჯაჭვების ჩამოყალიბების პრინციპების განხილვაზე. წინა თავებში ვსაუბრობდით ბლოკჩეინ-ტექნოლოგიების ყველა მნიშვნელოვან შემადგენელ ელემენტზე ცალ-ცალკე და ახლა შეგვიძლია ეს ცოდნა გავაერთიანოთ, როგორც ჰამბურგერი, რომლის ინგრედიენტებიც წინასწარ იყო მომზადებული და მაგიდაზე დალაგებული, რათა გარკვეულ მომენტში ერთობლივ კულინარიულ კონსტრუქციად გაერთიანებულიყო. სწორედ მას შევთავაზებთ წვეულებაზე მოწვეულ სტუმრებს, რომლის პრელუდიაც რამდენადმე გაჭიანურდა ზედმიწევნით ტექნიკური პრობლემების გამო.

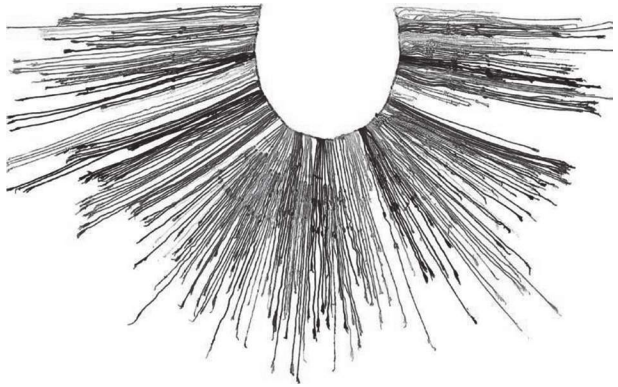
ბლოკები და მათი სტრუქტურა

ბლოკჩეინის სტრუქტურის აგების ზოგადი პრინციპების აღწერაში დეცენტრალიზებული ბაზის არქიტექტურა შედარებული იქნა საბუღალტრო წიგნთან, რომლის გვერდებიც იყო ბლოკები, სადაც იწერებოდა ფინანსური ტრანზაქციები. ცალკე იყო მითითებული, რომ ეს „გვერდები“ დალაგებულია მკაცრი თანმიმდევრობით, რომლის შეცვლაც არ შეიძლება, რადგან ისინი მათემატიკურად მკვიდრად არის შეკრული ერთმანეთთან სპეციალური „კრიპტოგრაფიული ბოქლომებით“. ახლა, როდესაც გავეცანით ბლოკჩეინ-ქსელების ძირითად ტექნოლოგიურ ელემენტებს, კრიპტოგრაფიის ჩათვლით, უფრო დაწვრილებით შეგვიძლია განვმარტოთ, როგორ ნარჩუნდება ბლოკთა სტრუქტურის მთლიანობა და როგორ მოქმედებს ეს განაწილებულ სისტემებში ინფორმაციის შენახვის საერთო უსაფრთხოებაზე. აშკარაა, რომ ყოველ ბლოკჩეინ-სისტემას ცალ-ცალკე აქვს სტრუქტურული თავისებურებები და როდესაც ჩვენ შევისწავლით სხვადასხვა პროექტის ყველაზე პოპულარულ რეალიზაციებს, ამ თავისებურებებს გამოვყოფთ და ყურადღებით განვიხილავთ. ამასთან, ბლოკჩეინ-ტექნოლოგიების ბაზაზე შექმნილ თითქმის ყველა სისტემას სტრუქტურისა და მისი ელემენტების ჩამოყალიბების საერთო პრინციპები აქვს. ამიტომ მიზანშეწონილია მათი განხილვა საერთო აღწერის ფარგლებში, რადგან უმრავლეს პრაქტიკულ შემთხვევაში ისინი მონაწილეობს სტრუქტურებში ძალზე მსგავსი ტექნოლოგიური ფორმებით, არსებითი განსხვავებების გარეშე.

შეკრული სიების საშუალებით ინფორმაციის შენახვის იდეა გაჩნდა საკმაოდ დიდი ხნის წინ, ბევრად ადრე, ვიდრე თვით კომპიუტერული ტექნოლოგიები წარმოიშვა, სახელდობრ – 4000 წელზე მეტი ხნის წინ, ინდიელ ინკთა და მათ წინამორბედთა ცივილიზაციაში, დაახლოებით III ათასწლეულში ჩვენს წელთაღრიცხვამდე. საუბარია ინფორმაციის შენახვაზე ე.წ. „კიპუს“ სახით, რომელიც წარმოადგენდა დახლართულ ძაფებს, შებმულს ერთ თოკზე და ერთმანეთთან დაკავშირებულს ჩასაწერი კონტექსტიდან გამომდინარე.

ყოველ ძაფს შეიძლებოდა ჰქონოდა საკუთარი ფერთა კოდი, ასევე – სპეციალური კვანძები, რომელთა ფორმა და რაოდენობა წარმოადგენდა მნიშვნელოვან მარკერებს, რომლებიც განსაზღვრავდა შენახული ინფორმაციის მნიშვნელობასა და სახეობას. ყოველი ძაფის დასაწყისისა და დაბოლოების დათვალიერებისას შეიძლებოდა, თვალყური მიგვედევნებინა მონაცემთა ჯაჭვის ჩამოყალიბების მთელ გზაზე, ფუძე თოკიდან – განშტოებების დაბოლოებამდე. ერთ კიპუში ძაფების რაოდენობა შეიძლება 2500-მდე ყოფილიყო. კიპუს დახმარებით ინკებს, როგორც ცენტრალური ანდების ინდიელთა კავშირის მმართველ კლასს, შეეძლოთ აღერიცხათ მათთვის დაქვემდებარებული ყველა აუცილებელი რესურსი, ჯარების, სურსათის მარაგების, მოსახლეობის რაოდენობა და ამოსაღები გადასახადების მოცულობა.

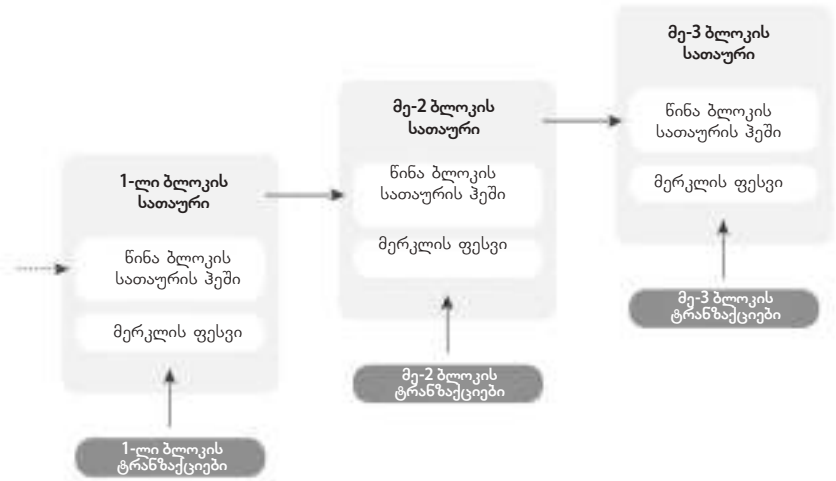
XVI საუკუნის პირველ ნახევარში იმ ადგილებში მოხვედრილი ესპანელი კონკისტადორები კარგა ხანს ვერ მიხვდნენ ამ უცნაური თოკ-კვანძოვანი კონსტრუქციების უტილიტარულ აზრს, რომლის საშუალებითაც ინკები ფაქტობრივად მართავდნენ საკუთარ იმპერიას. იმისათვის, რომ დაემსხვრიათ მართვის ჩვეული წესები, ესპანელებს მოუწიათ, დაპყრობილი ტერიტორიებისათვის თავს მოეხვიათ დამწერლობისა და მონაცემთა აღრიცხვის ევროპული პრინციპები. კიპუ მთლიანად განიდევნა ხმარებიდან და დავიწყებას მიეცა და მხოლოდ XIX საუკუნის დასაწყისში მეცნიერებმა დაიწყეს შედარებით სისტემურად მისი შესწავლა. მათ შეძლეს საკმაოდ დიდი ინფორმაციის გაშიფვრა, რომელსაც გადარჩენილი ეგზემპლარები შეიცავდა. აღრიცხვის ამგვარი სისტემის აგების ლოგიკის ძირითადი პრინციპების გაგების შემდეგ, მეცნიერები გაოცდნენ, რომ ასეთმა ძველმა ცივილიზაციამ, რომელიც იზოლირებული იყო უფრო პროგრესული სამყაროსაგან, შეძლო ეპოვა მონაცემთა კომპაქტური ჩაწერისა და შენახვის ესოდენ ეფექტიანი მეთოდი, რომელიც შეერთებული საინფორმაციო ბლოკების ლოგიკას ექვემდებარება.



XX საუკუნის მეორე ნახევარში, როდესაც ინფორმაციულმა ტექნოლოგიებმა, მართალია, ნელა, მაგრამ მტკიცედ დაიწყო მსოფლიოს დაპყრობა, გაჩნდა აუცილებლობა, ინფორმაციის აღწერისა და შენახვის სხვადასხვა ფორმა შექმნილიყო. ერთ-ერთ ასეთ ფორმად იქცა შეკრული (დაკავშირებული) სიები, მონაცემთა სპეციალური სტრუქტურები, რომელთაგან თითოეული შეიცავდა არა მხოლოდ თვით მონაცემებს, არამედ სპეციალურ განმარტებებს მსგავს სტრუქტურებზე, როგორც წინაზე, ასევე შემდგომზე. ამან საშუალება მოგვცა, უგულებელგვეყო ბუნებრივი შენახვის წესი სხვადასხვა მატარებელზე და ამასთან, გვეხელმძღვანელა მხოლოდ იმ ინფორმაციული ლოჯისტიკით, რომლის პრინციპიც ჩადებული იქნა ბლოკებს შორის შიდა კავშირების ერთობლიობაში. დასახული ამოცანების გადაჭრის ლოგიკიდან გამომდინარე, მონაცემთა სიების ფორმები უმეტეს შემთხვევაში შეიძლება იყოს ცალბმულიანი (ცალმხრივად მიმართული) ან ორბმულიანი (ორმიმართულებიანი). ასევე, ორივე ფორმა შეიძლება ჰქონდეს რგოლურ სტრუქტურას, როდესაც უკანასკნელი ელემენტი მიუთითებს პირველზე ან – პირიქით. მარტივი ცალბმულიანი სიის მაგალითი ნაჩვენებია ნახატზე:

საკუთრივ ბლოკჩეინი თავისი კლასიკური სახით წარმოადგენს ცალად ბმულ სიას სისტემაში, სადაც ყოველი შემდეგი ბლოკი მიუთითებს

წინამორბედზე. საკითხავი ისაა, თუ რას ნიშნავს „მიუთითებს“: როგორაა ეს ტექნოლოგიურად რეალიზებული და, რაც მთავარია, საერთოდ რატომ აკეთებს ამას? პასუხი მარტივია: მონაცემთა ბაზის მთლიანობის შესანარჩუნებლად. ბლოკი შედგება ორი ძირითადი ნაწილისგან – სათაურისაგან, რომელიც შეიცავს სამსახურებრივ ინფორმაციას, და ტრანზაქციების სიისაგან სისტემის წევრთა შორის ციფრული აქტივების გადასაცემად ანდა უბრალოდ, ფაქტების ჩასაწერად. ყველაფერი ეს მონაცემთა ერთობლიობაა, რომელიც შეიძლება ავსახოთ სტანდარტული სიგრძის ჰეშში. სათაურის მონაცემთა ჰეშის გამოთვლის შემდეგ, ვაფიქსირებთ მთელი ბლოკის მდგომარეობას და ნებისმიერი ჩარევა მის მთლიანობაში დაუყოვნებლივ გამოიწვევს საერთო ჰეშის ტოტალურ ცვლილებას. რა მოხდება, თუ ყოველი ახალი ბლოკი შეიცავს წინა ბლოკის მონაცემთა ჰეშს როგორც თავისი სათაურის ერთ-ერთ ელემენტს? მაშინ გამოვა, რომ ერთი სათაურის მონაცემთა ჰეშირებისას, ჩვენ ავტომატურად ვრთავთ მასში წინა ბლოკის სათაურის ჰეშს და ამგვარად მიიღება ბლოკების ჯაჭვის ფორმა. ჩვენთვის ცნობილია, რომ ნებისმიერი უმცირესი ცვლილება პირველსახეში მის ჰეშს უკიდურესად ცვლის. ეს ნიშნავს, რომ თუ ჩავერევით ჯაჭვის შუაში მდებარე ნებისმიერი ბლოკის მომაცემთა ნებისმიერ ბიტში, ეს მომდევნო ბლოკების ყველა ჰეშის გადაანგარიშებას გამოიწვევს. სხვა სიტყვებით რომ ვთქვათ, მთელი ჯაჭვის მონაცემები შეიცვლება.



პირველ რიგში, რაზე მეტყველებს ბლოკების შეერთებული სტრუქტურა? იმაზე, რომ ბლოკჩეინი არის სისტემა, რომელშიც შეიძლება ინფორმაციის მხოლოდ დამატება, მაგრამ არ შეიძლება შეცვლა ან წაშლა. ამასთან, ინფორმაციის დამატება შესაძლებელია მხოლოდ ახალი ბლოკების სახით და მხოლოდ ჯაჭვის ბოლოში. ეს, რა თქმა უნდა, ქმნის გარკვეულ უხერხულობას ბლოკჩეინში ჩასამატებელი ინფორმაციის მართვისას, მაგრამ მეორე მხრივ, განაპირობებს განაწილებული სახის მონაცემთა შენახვის განსაკუთრებულ უსაფრთხოებას. აკი ბლოკების მთელი ბაზა კოპირდება სისტემის ყველა წევრთან და თითოეულ მათგანს შეუძლია მასში ჩაწეროს, რაც მოეხასიათება. სხვა საქმეა, რომ ის ცვლილებები, რომლებიც გაკეთებულია სისტემის წესების დარღვევით, არ იქნება მიღებული სისტემის სხვა წევრთა მიერ, ხოლო წესებთან შესაბამისობის შემოწმება სისტემის წევრების მიერ ხორციელდება მხოლოდ მათემატიკურად, ამიტომ მათთვის დამახინჯებული ინფორმაციის შეპარება შეუძლებელია. ბლოკებში არსებული ინფორმაციის შემოწმების ალგორითმები მაშინვე იძლევა სიგნალს მონაცემთა მთლიანობის დარღვევის შესახებ და ეს ბლოკი მთელი ქსელისათვის მიუღებლად ჩაითვლება.

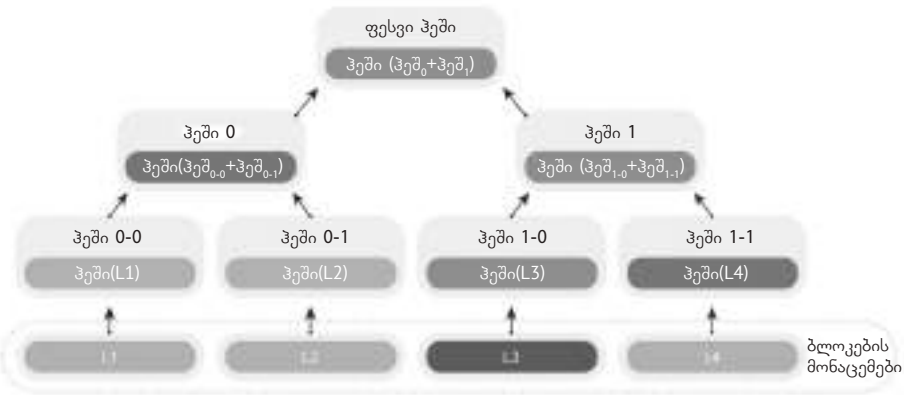
არსებობს კიდევ ერთი უხერხულობა: რადგან შეიძლება მხოლოდ მონაცემთა დამატება და არ შეიძლება მათი წაშლა, თუნდაც მათ დროის გარკვეულ მომენტში დაკარგოს აქტუალობა, საერთო ბაზა პირველი ბლოკის წარმოქმნის მომენტიდან მუდმივად იზრდება. მისი ზომა დამოკიდებულია სხვადასხვა პარამეტრზე, ახალი ბლოკების შექმნის სიჩქარეზე, მათში შემავალი ტრანზაქციების რაოდენობაზე, თვით ტრანზაქციების ზომებზე. ამ პარამეტრებიდან და აგრეთვე, მონაცემთა ბაზის „ასაკიდან“ გამომდინარე, მისი ზომა რამდენიმე წლის აქტიური მუშაობის შემდეგ იანგარიშება ინფორმაციის ასეულობით გიგაბაიტით, რომელიც მუდმივად კოპირდება და სინქრონიზდება სისტემის წევრებს შორის. ბლოკჩეინში მონაცემთა ბაზის ზომის ოპტიმიზაციის ამოცანის ამოხსნა უნდა გახდეს პრიორიტეტი პოპულარული სისტემების შემმუშავებლებისათვის, წინააღმდეგ შემთხვევაში, ამას შეუძლია შეუქმნას დამატებითი დაბრკოლებები პერსპექტიული ტექნოლოგიის განვითარებას. თუმცა, ამ პრობლემის გადაჭრის წინადადებები უკვე არსებობს და მათ ბლოკჩეინ-ტექნოლოგიების მასშტაბირების საკითხებისადმი მიძღვნილ თავში შევეხებით.

მოდი, უფრო დაწვრილებით განვიხილოთ ბლოკის სათაურის სტრუქტურა, რათა გავიგოთ, რა სახის სამსახურებრივ ინფორმაციას შეიცავს იგი. გასაგებია, რომ ბლოკთა სტრუქტურა სხვადასხვა სახის პრაქტიკულ რეალიზაციებში განსხვავებულია, მაგრამ მათ აქვს რიგი საერთო ელემენტებისა, რომლებიც ამა თუ იმ სახით გვხვდება თითქმის ყველა პროექტში. როგორც წესი, პირველი, რითაც ნებისმიერი ბლოკი იწყება, რიგითი ნომერია. პირველ ბლოკს ეწოდება „გენეზისური“, ის სხვებისაგან იმით განსხვავდება, რომ არ შეიცავს წინა ბლოკზე მითითებას, მისი არარსებობის გამო. ჩვეულებრივ, ბლოკში არის ინფორმაცია მისი ვერსიის ნომერზე, ეს აუცილებელია, თუ შემდგომში ბლოკის სტრუქტურა შეიცვლება, და ვერსიის ნომრიდან გამომდინარე, პროგრამული უზრუნველყოფის ალგორითმებმა ისინი სხვადასხვაგვარად უნდა დაამუშაოს. შემდეგ, როგორც ზემოთ იქნა აღნიშნული, სათაური შეიცავს წინა ბლოკის სათაურის ჰეშს, მონაცემთა მთელი ჯაჭვის მთლიანობის შესანარჩუნებლად.

სათაურის მნიშვნელოვანი ელემენტია ასევე ბლოკის შექმნის დრო. ის ჩაწერილია რიცხვის სახით, რომელიც უდრის წამების რაოდენობას, გასულს 1970 წლის 1-ლი იანვრიდან, ეს არის ფორმატი, რომელიც მიღებულია მრავალმომხმარებლიან და მრავალამოცანიან ოპერაციულ სისტემებში, მაგალითად, ისეთებში, როგორიცაა Unix და მასთან თავსებადი სისტემები. ცალკე შევნიშნავთ, რომ ეს საკმაოდ დიდი რიცხვია და ორი ათეული წლის შემდეგ მეხსიერების 32-ბიტიანი უჯრედი, რომელიც ჩვეულებრივ გამოიყოფა ცვლადებისათვის, რომლებიც ამ მნიშვნელობას ინახავს სხვადასხვა პროგრამულ უზრუნველყოფაში, უნდა გადაივსოს. იმ შემთხვევაში, თუ ამ პროგრამების შემმუშავებლები არ შეიტანენ აუცილებელ ცვლილებებს, დროის მნიშვნელობის შემნახავი ცვლადის ზომის 64 ბიტამდე გასაზრდელად, 2038 წლის 19 იანვარს მთელ მსოფლიოში შეიძლება მოხდეს მასობრივი პროგრამული ჩავარდნები. ეს იმიტომ მოხდება, რომ ამ რიცხვის მნიშვნელობა კომპიუტერული არქიტექტურის აგების სპეციფიკის ძალით პროგრამების შესრულებისას ინტერპრეტირდება როგორც უარყოფითი მნიშვნელობის მქონე, აქედან გამომდინარე ყველა ალგორითმული შედეგით.

დაბოლოს, გადავდივართ სათაურის ტრანზაქციიანი ბლოკებისადმი მიძღვნილ ნაწილზე. სათაურში ერთ-ერთი მნიშვნელობაა

ბლოკში ტრანზაქციების რაოდენობა, ხოლო მეორე მნიშვნელობას აქვს იდუმალი სახელი „მერკლის ფესვი“. ეს სხვა არაფერია, თუ არა ამ ბლოკში მდებარე ყველა ტრანზაქციის ჰეშების ერთობლიობა, გამოთვლილი გარკვეული წესით. 1979 წელს ამერიკელმა კრიპტოგრაფმა რალფ მერკლმა დააპატენტა მონაცემთა ასაკრები შემაჯამებელი ჰეშის გამოსათვლელი ალგორითმი, აგებული ორობითი ხის სახით:



მერკლის ალგორითმის ლოგიკის თანახმად, ბლოკში ყველა ტრანზაქცია იყოფა წყვილებად, ჰეშირდება, და მათი ჰეშები ჯამდება ერთმანეთთან. თუ ტრანზაქციების რაოდენობა თავიდანვე კენტი იყო და უკანასკნელ ტრანზაქციას არ აქვს წყვილი, მაშინ მისი საკუთარი ჰეში უბრალოდ ორმაგდება. „ხის“ შემდეგ დონეზე ჰეშების რაოდენობა უკვე ორჯერ ნაკლებია და მათი რაოდენობა გარანტირებულად წყვილია. ჰეშები კვლავ იყოფა წყვილებად, ეს წყვილები ჯამდება და ასე შემდეგ მანამ, სანამ მათგან მხოლოდ ერთი საბოლოო რიცხვი დარჩება. საბოლოოდ, ხის კენწეროზე წარმოიქმნება შემაჯამებელი ანუ ფესვი ჰეში, რომელსაც „მერკლის ფესვი“ ეწოდება და ფაქტობრივად წარმოადგენს ბლოკის ყველა ტრანზაქციის ერთიან ერთობლივ ანაბეჭდს. გასაგებია, რომ ბლოკში ნებისმიერი ტრანზაქციის შეცვლისას მერკლის ხის ყველა ჰეში მაშინვე ახლიდან იანგარიშება და შემაჯამებელი ჰეში ასევე შეიცვლება, რაც იქნება იმის მანიშნებელი, რომ ბლოკების მონაცემებში ჩარევის მცდელობა მოხდა. ამგვარად, მერკლის ფესვის მნიშვნელობა არის ბლოკის ტრანზა-

ქციული ნაწილის „წარმომადგენელი“ საკუთარ სათაურში. სათაურის ზოგად მონაცემებთან „მიჰეშირებული“ და ამგვარად გაშუალებულად ჩართული შემდეგი ბლოკის სათაურში, მერკლის ფესვი ბლოკჩეინში ადრე ჩაწერილი ტრანზაქციების უცვლელობის დამატებითი გარანტიის როლს თამაშობს.

გარდა ბლოკის სტრუქტურის ზემოთ აღწერილი პარამეტრებისა, მასში შეიძლება იყოს ელემენტები, რომლებიც დაკავშირებულია ბლოკის შექმნის უფლების უშუალოდ მიღებასთან და მის დაცვასთან შესაძლო შემდგომი ცვლილებებისგან. საუბარია ახალი ბლოკების შექმნაზე მუშაობის მტკიცებულების მქონე სისტემებში. მაგრამ ამჟამად ამაზე მსჯელობა რამდენამდე ნაადრევია, ამიტომ თავდაპირველად, ბლოკჩეინ-სისტემებში ტრანზაქციის სტრუქტურებს და ბალანსების წარმოების პრინციპებს გავეცნოთ.

ტრანზაქციები და ბალანსები

ყველანი მივეჩვიეთ, რომ საქმე გვაქვს კლასიკურ ბანკებთან: გავხსნათ ანგარიშები, განვახორციელოთ გადახდები ერთი მიმდინარე ანგარიშიდან მეორეზე, მივიღოთ საკუთარ ანგარიშზე თანხები. უკანასკნელი ორი ათეული წლის განმავლობაში ფართოდ გავრცელდა სისტემები „ბანკი-კლიენტი“, რომლებიც საშუალებას იძლევა საკუთარი ანგარიში ვმართოთ ინტერნეტის საშუალებით. მიუხედავად გარეგნული სხვაობისა, პირველ რიგში, ასეთი სისტემების ინტერფეისის დიზაინის ნაწილში, მათი ფუნქციურობა მეტ-ნაკლებად მსგავსია ასეთი მომსახურების შემომთავაზებელი ყველა ფინანსური ინსტიტუტისთვის. ინტერნეტის საშუალებით საკუთარ თანხებთან წვდომის მიღების პირველი ნაბიჯი უმრავლეს შემთხვევაში არის ორფაქტორიანი იდენტიფიკაციის პროცედურის გავლა. მომხმარებელს თავიდან შეჰყავს მრავალჯერადი სარგებლობის ჩვეულებრივი პაროლი და შემდეგ სისტემა ითხოვს სპეციალური ერთჯერადი კოდის შეყვანას, რომელიც გენერირდება ან სპეციალური მოწყობილობის საშუალებით, ან შეიძლება მიღებული იქნას SMS-ითა თუ ელექტრონული ფოსტით. ასე გამოირიცხება კლიენტის ანგარიშზე არასანქცირებული წვდომა, რომლის მონაცემებიც ინახება ბანკის სერვერებზე, ანუ – ცენტრალიზებულად. თუ ბანკის სერვერები რაღაც მიზეზის გამო არ მუშაობს, მაგალითად, ტექნიკურ მომსახურებას გადის, მაშინ ანგარიშთან წვდომა შეუძლებელი იქნება იმ მომენტამდე, სანამ სისტემა თავის ჩვეულ საქმიანობას დაუბრუნდება.

საკუთარ ანგარიშზე წვდომის მიღების შემდეგ, კლიენტს შეუძლია საკუთარი ბალანსის შემოწმება, შემდეგ კი ამ ანგარიშიდან თანხების გადარიცხვის განხორციელება, რა დროსაც ასევე სარგებლობს ერთჯერადი კოდების გენერაციის სისტემით, რადგან ამას მონაცემებთან წვდომის უსაფრთხოების წესები მოითხოვს. ყველა ანგარიშს აქვს თავისი ნომერი, გენერირებული გარკვეული წესებისა და სტანდარტების მიხედვით, დადგენილი ან საკუთრივ ბანკის, ან იმ სახელმწიფოს მიერ, რომელშიც ბანკი მდებარეობს. სხვა ანგარიშებზე გადახდების გაგზავნისას ბანკი, როგორც წესი, მომსახურები-

სათვის იღებს საკომისიოს, რომლის ოდენობასაც ადგენს დამოუკიდებლად, თავისი ბიზნესხარჯების, მოგების ჩადებული ნორმისა და ბაზარზე კონკურენტული სიტუაციის მიხედვით. ცხადია, იმისათვის, რომ კლიენტმა შეძლოს განახორციელოს ან მიიღოს გადახდები, ბანკმა თავიდან უნდა გაუხსნას მას მიმდინარე ანგარიში და გასცეს ინტერნეტბანკთან წვდომის რეკვიზიტები, სხვაგვარად, ყოველგვარი შემავალი და გამომავალი გადარიცხვები შეუძლებელია.

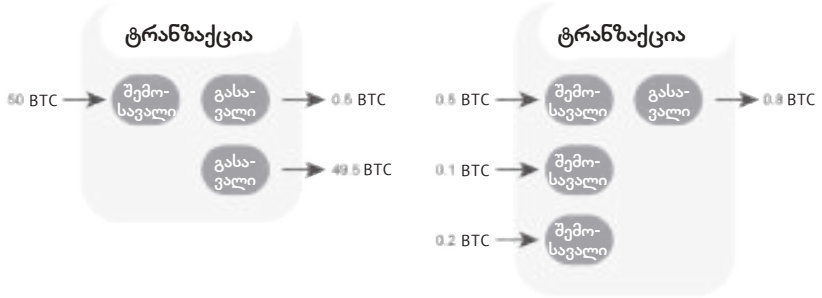
ბლოკჩეინ-სისტემებში ყველაფერი სხვაგვარად არის ორგანიზებული. პირველ რიგში, იქ არ არსებობს არავითარი ბანკი ან სხვა ცენტრალიზებული სისტემა, რომელიც აკონტროლებს ანგარიშებსა და მათი საშუალებით გადახდებს. მეორე რიგში, არანაირი ანგარიში არ იქმნება წინასწარ და მათ ბალანსებს სპეციალურად არავინ აწარმოებს. ერთი შეხედვით, ეს ცოტა უცნაურად გვეჩვენება, მაგრამ სწორედ ამით განსხვავდება გადახდების სისტემები, რომლებიც რეალიზებულია ბლოკჩეინ-ტექნოლოგიების ბაზაზე. იმისათვის, რომ სისტემის წევრი გახდეს, მომხმარებელმა, კონკრეტულ ბლოკჩეინ-სისტემებში დამკვიდრებული ასიმეტრიული კრიპტოგრაფიის გამოყენებით, აუცილებლად უნდა შეიქმნას ორი გასაღები – ღია და დახურული. წყვილის შემადგენელი გასაღებები ყოველთვის მტკიცედ არის შეკავშირებული ერთმანეთთან, საიდუმლო შეიძლება გენერირებული იქნას შემთხვევითად, ხოლო ღია მისგან გამოითვლება მათემატიკურად. ისე, რომ ვთქვათ, ყველაფერი ეს ავტომატურად კეთდება, თვით სისტემის პროგრამული უზრუნველყოფის საშუალებით, მომხმარებლის მოთხოვნით ანუ – პროგრამა-კლიენტის ინტერფეისში შესაბამის ღილაკზე დაჭერით. ამგვარად, კლიენტს უჩნდება საკუთარი ანგარიში სისტემაში, თუმცა უფრო სწორი იქნება, თუ ვიტყვით – მისამართი. და ეს მისამართი ფაქტობრივად, ღია გასაღების მოდიფიკაციას წარმოადგენს, რომელიც შექმნისას ჰეშირებისა და სპეციალური სიმბოლური კოდირების რამდენიმე პროცედურით დამუშავდა. ეს კეთდება არა მარტო მისამართის უფრო მოსახერხებელი ვიზუალური აღქმისათვის, არამედ მასთან დაკავშირებული დახურული გასაღების აღდგენის ამოცანის უფრო გასართულებლად, რადგან ჰეშ-ფუნქციები, და თანაც მიყოლებით რამდენჯერმე გამოყენებული, განსაკუთრებულად ართულებს ბლოკჩეინ-სისტემის გატეხის ნებისმიერ მცდელობას.

შეგახსენებთ, რომ მსგავსი ქსელები დეცენტრალიზებულია, ამიტომ მომხმარებელი ყველა ქმედებას აწარმოებს არა რომელიმე დაშორებული სერვერის მეშვეობით, არამედ უშუალოდ თავისი კომპიუტერის ან მობილურის საშუალებით. იქვე ინახება ყველა აუცილებელი გასაღები, მათ შორის – დახურულიც. კლასიკური ბანკისაგან განსხვავებით, საიდუმლო პერსონალური ინფორმაციის შენახვის ამოცანები თავად კლიენტს ეკისრება. თუ ის დაკარგავს საიდუმლო გასაღებს, მაშინ ავტომატურად დაკარგავს წვდომას აქტივებზე, რომლებიც დაკავშირებულია იმ მისამართთან, რომელიც გენერირებულია ამ საიდუმლო გასაღების საშუალებით. ინტერნეტში შეიძლება ვიპოვოთ კრიპტოვალუტის შეუმდგარ მილიონერთა უამრავი ისტორია, რომლებმაც საკუთარი მისამართების დახურულ გასაღებებთან ერთად, თავიანთი ციფრული მილიონები დაკარგეს. ეს საკმაოდ სერიოზული პრობლემაა, ამიტომ კრიპტოაქტივების შენახვის უსაფრთხოების პრობლემას ცალკე თავი მიეძღვნება.

ახლა, როდესაც კლიენტს აქვს საკუთარი მისამართი პირობით ბლოკჩეინ-სისტემაში, გავერკვეთ, როგორ შეუძლია მას მიიღოს მასზე და შემდეგ მისგან სხვა მისამართებზე გადარიცხოს ციფრული აქტივები. აქ არ შეიძლება, კიდევ ერთხელ არ გავიხსენოთ ანალოგია საბუღალტრო წიგნთან, რომელიც შედგება ფინანსური ტრანზაქციების შემცველი გვერდებისაგან: ვისგან ვისთვის არის გადარიცხული, რამდენი და რატომ. წარმოვიდგინოთ, რომ გვყავს რამდენიმე წარმომადგენელი რომელიღაც ბიზნესგარემოში, რომლებიც მუდმივად ცვლიან საქონელს, მომსახურებასა და თანხებს, ხოლო გაცვლის ყველა ფაქტი იწერება სპეციალურ წიგნში. როდესაც ერთ წევრს მოუნდება გარკვეული თანხის გადარიცხვა მეორისათვის, მისთვის აუცილებელია, ჯერ დაამტკიცოს, რომ ის ფლობს ამ თანხას. ამის გაკეთება შეიძლება მხოლოდ ამ წევრისათვის შემომავალი წინა ტრანზაქციების მითითებით, ანუ გარკვეული აქტივების ფლობის დადასტურების დამოწმებით. ამასთან, შეიძლება არა მარტო ერთი რომელიღაც კონკრეტული ტრანზაქციის მითითება, არამედ ერთბაშად რამდენიმესი, თუკი ერთი საკმარისი არ იქნება გამომავალი გადახდისათვის აუცილებელი თანხის შესაგროვებლად.

როდესაც ბანკი თანხას ერთი ანგარიშიდან მეორეზე რიცხავს, ის აწარმოებს სამ ოპერაციას: გამოაკლებს გადარიცხვის თანხასა და

გადარიცხვისათვის საჭირო საკომისიო თანხას გამგზავნის ანგარიშიდან და ამატებს გადარიცხულ თანხას მიმღების ანგარიშზე. საკომისიოს კი ბანკი იტოვებს თავისთვის როგორც გაწეული საშუამავლო მომსახურების ანაზღაურებას. ბლოკჩეინ-სისტემებში არავითარი შუამავლები არ არსებობენ, ისევე, როგორც თანხები ფიზიკურად არსაიდან აკლდება და არსად ემატება. აქტივების მფლობელი უბრალოდ მიუთითებს ტრანზაქციებს ერთი ან რამდენიმე მიმღების მისამართზე, ანუ კვლავ აკეთებს მითითებებს. საბოლოოდ, ტრანზაქცია წარმოადგენს მითითებების ერთობლიობას გადამხდელის მისამართზე შემომავალ თანხებზე, აგრეთვე, მითითებების ერთობლიობას მისი გადახდების მიმღებების გასავალ მისამართებზე. ასეთი ტრანზაქციებისათვის ბლოკჩეინ-გარემოში ოპერირებენ ცნებებით „შემოსავლები“ და „გასავლები“. არსებობს წესი, რომ ყველა თანხის ჯამი „გასავლებზე“ ტოლი უნდა იყოს თანხების ჯამისა „შემოსავლებზე“. თუ მისამართის მფლობელისათვის აუცილებელი არ არის „შემოსავლების“ ტრანზაქციაში ჩართული თანხების მთლიანად დახარჯვა, ის ქმნის დამატებით „გასავალს“ თავისთვის ხურდის დაბრუნების სახით, რათა დაიცვას თანაბარი ბალანსი „შემოსავლებსა“ და „გასავლებს“ შორის. აშკარაა, რომ „გასავლები“ გამგზავნისათვის იქნება „შემოსავალი“ მიმღებისათვის და მიმღებს შემდგომში, თავის მხრივ, შეუძლია მასზე მითითება, როდესაც განახორციელებს საკუთარ გასავალ გადახდებს.



რა დასკვნები შეგვიძლია გავაკეთოთ ამ სქემის აღწერიდან? პირველ რიგში, როცა გავაანალიზებთ მონაცემთა პირველი (იმავე საგენეზისო) ბლოკიდან ყველა „შემოსავალს“ კონკრეტულ მისამართზე და ყველა „გასავალს“ მისგან, ადვილად შეგვიძლია გამოვავლინოთ,

ამ მისამართის მფლობელს რამდენი დაუხარჯავი „გასავალი“ დარჩა. სწორედ ეს არის მისი ანგარიშის ბალანსი. ანუ თავისთავად ბალანსი სადმე კი არ ინახება, არამედ უბრალოდ გამოითვლება როგორც ყველა დაუხარჯავი „გასავლის“ ჯამი. მეორე რიგში, კონკრეტული მისამართის „შემოსავლის“ მითითებით, გამგზავნი გულისხმობს, რომ სისტემაში არსებობს ისეთი წევრი, რომელსაც აქვს დახურული გასაღები ამ მისამართისათვის. სხვაგვარად რომ ვთქვათ, თუ, მაგალითად, მიმღების მისამართს შევიყვანთ შეცდომით, მაშინ მასზე მიმთითებელი ტრანზაქცია მაინც იქნება მიღებული სისტემის მიერ, მაგრამ ამ გასავალი ტრანზაქციის თანხები სამუდამოდ დაიკარგება და ამოღებული იქნება ბრუნვიდან. ეს დაკავშირებულია იმასთან, რომ ბლოკში მოთავსებული ტრანზაქცია, რომელმაც გაიარა კონსენსუსის პროცედურა და ჩართულია ბლოკთა საერთო ჯაჭვში, მომავალში ვერ შეიცვლება. ზოგიერთი პროექტი, მაგალითად, ბიტკოინი, ქმნის გარკვეულ დაცვას შეცდომისაგან, რადგან გარდაქმნის მისამართს თექვსმეტობრივი რიცხვის ფორმატად ალფაბეტურ-ციფრულ ფორმატში და მიღებული მისამართის ბოლოს ამატებს მის საკონტროლო თანხას. მიმღების მისამართის შეყვანისას გადარიცხვის ფორმის ველში ანგარიშისას შეცდომისა და საკონტროლო თანხის შედარების შემთხვევაში, სისტემა იძლევა გაფრთხილებას. ასევე საკმაოდ ხშირად გამოიყენება მისამართის წარმოდგენა QR კოდის სახით, რათა გამგზავნმა შეძლოს დაასკანეროს ის საკუთარი მობილური ტელეფონით და ავტომატურად გარდაქმნას ასოებისა და ციფრების სწორ ერთობლიობად, რომლებიც მიმღების მისამართს შეადგენს.

წარმოიშვება კითხვა: შეუძლია კი სისტემის წევრს თანხების გადარიცხვისას მიუთითოს „შემოსავლებზე“, რომლებიც მას არ ეკუთვნის, და როგორ შეიძლება ამის შემოწმება? სინამდვილეში, იმისათვის, რომ ლეგიტიმურად მივუთითოთ „შემოსავლებზე“, აუცი-

ლებელია, მითითებაში იყოს საკუთარი ღია გასაღები და საკუთარი ციფრული ელექტრონული ხელმოწერა, რომელიც შექმნილია დახურული, მფლობელის მისამართთან დაკავშირებული, გასაღების საფუძველზე. ციფრული ხელმოწერის შემოწმების ალგორითმების საშუალებით სისტემის ყოველი წევრი შეიძლება დარწმუნდეს, რომ „შემოსავლებზე“ მითითება ნამდვილად ლეგიტიმურია, ხოლო შემოწმების შეცდომის შემთხვევაში, ეს ტრანზაქცია უბრალოდ იგნორირებული იქნება და არ ჩაერთვება ბლოკში იმ კვანძად, რომელიც მას ქსელისათვის აყალიბებს.

ტრანზაქციების ფორმირებისა და ბალანსების წარმოების ასეთ სისტემას ეწოდება UTXO (Unspent Transaction Output — „დაუხარჯავი ტრანზაქციური გასავლები“). როგორც ზემოთ იყო მითითებული, სისტემაში კონკრეტულ მისამართთან დაკავშირებული ბალანსების გათვლისათვის აუცილებელია მასთან დაკავშირებული ყველა „შემოსავლისა“ და „გასავლის“ პოვნა და შემოწმება ბლოკთა ბაზის დასაწყისიდანვე. ამ მეთოდის პლუსია, რომ არ არის საჭირო ბალანსების მდგომარეობის ცალკე შენახვა და მათი მუდმივი აქტუალიზება, რითაც ვიღებთ თავისუფალი ადგილების ეკონომიას მატარებლებში. მინუსი კი არის დრო, რომელიც მუდმივად იხარჯება ბალანსის გათვლაზე, განსაკუთრებით, თუ ბლოკთა ბაზა საკმაოდ გაიზარდა ზომაში. ამიტომ რიგი პროექტებისა ინახავს „აქტუალური მდგომარეობის“ სპეციალურ ბაზებს, სადაც კერძოდ, მდებარეობს მონაცემების მისამართთა ბალანსები, რომელთა მიღებაც სწრაფად შეიძლება.

ახლა განვიხილოთ, კიდევ რომელი დამატებითი სამსახურებრივი ინფორმაცია შეიძლება მოთავსდეს ტრანზაქციაში. პირველ რიგში, ეს არის ტრანზაქციის უნიკალური ნომრის მქონე იდენტიფიკატორი, რომელიც არ შეიძლება განმეორდეს. მას იღებენ თავად ტრანზაქციის ჰეშიდან, რადგანაც ვიცით, რომ კრიპტომედეგი ჰეშ-ფუნქციების კოლიზიის მიღების ალბათობა (ანუ სხვადასხვა წინა სახისთვის ერთნაირი ჰეშების) ძალზე მცირეა. მეორე რიგში, ტრანზაქციის სხეულში ჩვეულებრივ, ათავსებენ ამ ბლოკის წინა ტრანზაქციის ჰეშს, იმის ანალოგიურად, როგორც ეს კეთდება თვით ბლოკების სათაურებში. ყოველ ტრანზაქციაში ამ ინფორმაციის არსებობა ისახავს იმავე მიზანს – მონაცემთა შენახვის მთლიანობის შენარჩუნებას და მის დაცვას არასანქცირებული შეცვლისაგან. გარდა ამისა, „შემოსავლებზე“

მითითებების აღწერისას უთითებენ მისამართის ღია გასაღებსა და ელექტრონულ ხელმოწერას, რომელიც ადასტურებს, რომ ტრანზაქციის ავტორს აქვს ამ წყვილის დახურული გასაღები.

დაბოლოს, რისი თქმაც მსურს ტრანზაქციების ზოგად აღწერაზე, ეს არის საკომისიო. სხვადასხვა ბლოკჩეინ-პროექტი იღებს საკომისიოს ტრანზაქციებისათვის, თუმცა არის ისეთებიც, რომლებშიც ყველა ტრანზაქცია უფასოა. საკომისიო არსებობს ბლოკების შესაქმნელი კვანძების მონეტარული მოტივაციისათვის, ისინი იღებენ საკომისიოს ძირითად ანაზღაურებასთან ერთად, თვით ბლოკის შესაქმნელად. ამ პროცესზე დაწვრილებით ვისაუბრებთ თავში ე.წ. „მაინინგის“ შესახებ, ხოლო აქ ვიტყვით მხოლოდ, რომ ბლოკჩეინ-სისტემებში საკომისიო, როგორც წესი, არ არის ფიქსირებული და ტრანზაქციის ყოველი შემქმნელი თავად წყვეტს, როგორი საკომისიო უნდა გადაუხადონ. მაგრამ თუ ეს საკომისიო აღმოჩნდა ზედმეტად მცირე ან სულაც ნულოვანი, მაშინ ტრანზაქციამ შეიძლება მიიღოს დაბალი პრიორიტეტი ახალი ბლოკების შექმნისას და ჩართული იქნას რომელიმე მათგანში დიდი ხნის დაგვიანებით. რაც შეეხება ტრანზაქციის სხეულში საკომისიოს სიდიდის უშუალო ვიზუალიზაციას, აქაც კვლავ გამოყენებულია მონაცემთა შენახვაში მაქსიმალური სიმტკიცის მიდგომა, ტრანზაქციებში არავითარი საკომისიო პირდაპირ მითითებული არ არის, ის გამოითვლება როგორც სხვაობა ყველა „შემოსავლის“ ჯამსა და „გასავლის“ ჯამს შორის, „ხურდის“ ჩათვლით, რომელიც ნაკლებია სწორედ საკომისიოსხელა სიდიდით.

თავი ტრანზაქციებსა და ბალანსებზე ასრულებს წიგნის პირველ ნაწილს, რომელიც შეიცავს ბლოკჩეინ-ტექნოლოგიის ბაზაზე არსებული პროექტების უდიდესი უმრავლესობის ზოგადი პრინციპების აღწერას. შემდეგი ნაწილი ეძღვნება ამჟამად ყველაზე პოპულარულ პრაქტიკულ რეალიზაციებს განაწილებული რეესტრის ტექნოლოგიის ბაზაზე.

ნაწილი II

პრაქტიკული რეალიზაციები

ბიტკოინის პროექტის წინაისტორია

ნებისმიერი მასშტაბური მოვლენის აღწერა ჩვეულებრივ იწყება მისი წარმოშობის ისტორიიდან და გრძელდება მისი შემდგომი განვითარებით. მაგრამ მანამ, სანამ შევუდგებით ბლოკჩეინ-ტექნოლოგიის ისტორიის თხრობას, უნდა გაგვეცნო მეცნიერებისა და ტექნოლოგიის რიგი ნაწილები. წინააღმდეგ შემთხვევაში გაუცნობიერებელ მკითხველს აუცილებლად შეექმნებოდა სირთულეები იმის გასაგებად, კერძოდ თუ რა იყო გამოგონებული და რატომ აქვს ამ ტექნოლოგიურ სიახლეს ასეთი მნიშვნელობა.

უკანასკნელი რამდენიმე ათეული წლის განმავლობაში აღინიშნა მრავალი მცდელობა, გამოეგონებინათ ტექნოლოგიურად დაცული ციფრული ფული. ამ სფეროში წარმოქმნილი პროექტი ეფუძნებოდა ერთ ან რამდენიმე ტექნოლოგიას, რომლებიც შემდგომში გახდა ბლოკჩეინ კონცეფციის განუყოფელი ნაწილი. მაგრამ ვერც ერთმა მათგანმა ბიტკოინ-ქსელის წარმოქმნის მომენტამდე ვერ შეძლო საკუთარ თავში გაეერთიანებინა ყველა აუცილებელი მდგენელი, რათა მიეღო დამთავრებული, დაცული და, ბოლოს და ბოლოს, დეცენტრალიზებული ციფრული საგადახდო საშუალების შექმნის ამოცანის უბრალოდ ელეგანტური ამოხსნა. ახლა გადავიდეთ უშუალოდ ელექტრონული ფულის ადრეული გადაწყვეტების განვითარების ისტორიაზე.

1976 წელს, ჯერ კიდევ ინტერნეტამდელ ეპოქაში, ცნობილმა ავსტრიელმა ეკონომისტმა ფრიდრიხ ავგუსტ ფონ ჰაიეკმა წარმოადგინა წიგნი სათაურით „კერძო ფული“. ის შეიცავდა ფულადი ემისიების მართვაში სახელმწიფო მონოპოლიის შესაძლო გაუქმების სერიოზულ მსჯელობებს, მათ შორის კონკურენტული ფინანსური სისტემების შექმნის წინადადებებსაც. ფონ ჰაიეკი აგრეთვე წერდა ეროვნული მთავრობების მხრივ საზოგადოებრივი ნდობის ბოროტად გამოყენების ნეგატიური შედეგების შესახებაც. ეს გაფრთხილებები შემდგომში მეტწილად განხორციელდა რეალობაში, როდესაც ფინანსური სამყარო სისტემური კრიზისების გამო მოიცვა რყევებმა, რომლებიც წარმოიქმნა რიგი სახელმწიფოების მსხვილი ბანკებისა და ფინანსური რეგულატორების უპასუხისმგებლო პოლიტიკით.

ფონ ჰაიეკის იდეებმა გამოძახილი პოვა ზოგიერთ კრიპტოგრაფ-ენთუზიასტში, რომლებმაც სერიოზულად დაიწყეს ფიქრი დამოუკიდებელი ელექტრონული ფულადი სისტემების დაპროექტებაზე. პირველ რიგში მათ აინტერესებდათ ფულადი მიმოქცევის დეცენტრალიზაციის და ამავე დროს ანონიმიზაციის შესაძლებლობა, მათი იმ შუამავლებისაგან განთავისუფლება, რომლებიც უმრავლეს შემთხვევაში მკაცრი სახელმწიფო კონტროლის ქვეშ იმყოფებოდნენ.

1982 წელს ამერიკელმა კრიპტოგრაფმა დევიდ ჩაუმმა გამოაქვეყნა სტატია სათაურით „ბრმა ხელმოწერები და გადახდები, რომლებსაც თვალს ვერ მიადევნებ", რომელიც გახდა დაშიფრული კომუნიკაციების სფეროში მისი კვლევების გაგრძელება. ბრმა ხელმოწერის კონცეფცია ადრე უკვე განვიხილეთ, ამიტომ მკითხველს უკვე უნდა ჰქონდეს წარმოდგენა მისი მუშაობის პრინციპებზე. სწორედ ᲩᲔᲛ-ის ამ ფორმის ბაზაზე ჩაუმმა შემდგომში შექმნა ელექტრონული ფულის მიმოქცევის პირველი სისტემა, რომელსაც უწოდა eCash. ეს პროექტი იყენებდა „ბრმა ციფრული ხელმოწერის ტექნოლოგიას" ციფრული ბანკნოტების ავტორიზაციისა და შემოწმებისათვის, რომლებსაც მიმოცვლიდნენ კონტრაგენტები. ამასთან თავად ავტორიზატორი თამაშობდა ბანკის – ცენტრალიზებული სერვისის როლს, რომლის ძირითადი ფუნქციაც იყო სისტემის დაცვის უზრუნველყოფა ციფრული ფულის განმეორებითი დახარჯვის საფრთხისაგან. ამასთან ერთად ამგვარ ცენტრალიზაციას შეიძლება გამოეწვია კლიენტების ბალანსების შესაძლო ფალსიფიკაცია, თუკი სისტემის მფლობელებს ასეთი სურვილი გაუჩნდებოდათ. მიუხედავად ამისა, ეს იყო პირველი პროექტი, რომელშიც გამოყენებული იქნა ასიმეტრიული კრიპტოგრაფიის ალგორითმები ელექტრონული გადამხდელი სისტემის შესაქმნელად.

eCash პროექტის ფუნქციონირების უზრუნველსაყოფად 1990 წელს ნიდერლანდებში დარეგისტრირებული იქნა კომპანია DigiCash, რომელიც 1990-1995 წლების პერიოდში თანამშრომლობდა ბანკებთან და მსხვილ გადამხდელ სისტემებთან, მათ შორის ისეთებთანაც, როგორიცაა VISA. კომპანია Microsoft-იც კი არ დარჩა გვერდზე და სცადა ამ პროექტის ინტეგრირება საკუთარ, იმ დროისათვის უახლეს და მრავალწილად რევოლუციურ ოპერაციულ სისტემაში Windows 95. ითვლებოდა, რომ ინტერესის არსებობა ასეთი სერიოზული პარტნიორების მხრიდან კომპანია DigiCash-ს განვითარების საუკეთესო პერს-

პექტივის გარანტიას აძლევს. მაგრამ ჩაუმის შეცდომებმა ბიზნესის წარმოების სტრატეგიაში 1998 წელს კომპანია გაკოტრებამდე მიიყვანა, რის შემდეგაც მისი აქტივები გაიყიდა, ხოლო პროექტი დაიხურა.

პრაქტიკულად იმავე დროს კომპიუტერების ინჟინერმა და ვაშინგტონის უნივერსიტეტის კურსდამთავრებულმა ვეი დაიმ წარმოდგინა დოკუმენტი B-money პროექტის აღწერით, რომელიც ავტორმა განსაზღვრა როგორც განაწილებული ანონიმური ფულადი სისტემა. ამ პროექტში ასახვა პოვა ციფრული ნაღდი ფულის ტრანზაქციული გადაცემის კონცეფციამ ასიმეტრიული კრიპტოგრაფიის გასაღებების მფლობელთა შორის, დაახლოებით იგივე პრინციპით, როგორიც აღწერილი იყო ბლოკჩეინში ტრანზაქციებისა და ბალანსებისადმი მიძღვნილ თავში. ანუ ტრანზაქცია B-money-ში შეიქმნა მიმღების საჯარო გასაღებზე ციფრული აქტივების გადაცემის საშუალებით, რომელიც მისამართის ან ანგარიშის როლს თამაშობს და მყარდება გამგზავნის დახურული გასაღების დახმარებით შექმნილი ელექტრონული ხელმოწერით. როგორც ბლოკჩეინში, ნავარაუდევი იყო, რომ მიმღებიც და გამგზავნიც ყოველთვის აკონტროლებენ თავიანთ დახურულ გასაღებს და ამგვარად, შეუძლიათ გადასცენ ციფრული ფული ერთმანეთს, იმავდროულად მათემატიკურად დაამტკიცონ მათი ფლობის უფლება. სამწუხაროდ, B-money კონცეფცია როგორც პროექტი ვერ განხორციელდა, თუმცა ციფრული საგადახდო სისტემების შემდგომ ევოლუციაზე საკმაოდ მნიშვნელოვანი გავლენა მოახდინა.

1998 წელი მთლიანობაში მდიდარი იყო მნიშვნელოვანი მოვლენებით მსოფლიო ფინანსურ ინდუსტრიაში. აზიაში ჩასახულმა მსოფლიო ფინანსურმა კრიზისმა ქარიშხალივით გადაუარა მთელ მსოფლიოს და მნიშვნელოვანი ზიანი მიაყენა ზოგიერთი განვითარებადი ქვეყნის ეკონომიკას. ამან აიძულა ბევრი დაფიქრებულიყვნენ იმაზე, რომ უმეტესად მაღალი ხარისხის ცენტრალიზების ბუნების მქონე არსებული მსოფლიო ფინანსური სისტემა საკმაოდ მოწყვლადია ეკონომიკური კრიზისების მიმართ. მათი წარმომშობი მიზეზები კი განპირობებულია ან ეროვნული ეკონომიკების გადაჭარბებული სახელმწიფო „დარეგულირებებით“, ან უმსხვილესი ფინანსური ინსტიტუტების, თანაც როგორც კომერციული, ასევე სახელმწიფო სტრუქტურების სტატუსის მქონე ბანკების, მათ შორის ცენტრალური ბანკებისაც, ხელმძღვანელთა ბანალური არაკომპეტენტურობით.

შესაძლოა, სწორედ მაშინ დაიწყო ჩასახვა დეცენტრალიზებული ფულადი მიმოცვლის იდეებმა, რომლებიც საშუალებას იძლეოდა თავიდან აგვეცილებინა განსაკუთრებული დამოკიდებულება კონკრეტული პერსონალიების კონიუნქტურულ გადაწყვეტილებებზე, რომლებსაც ბედის წყალობით ხელში ეჭირათ პოლიტიკური და ეკონომიკური ძალაუფლება თავიანთ სახელმწიფოებში. როგორც შედეგი, გადახდის დეცენტრალიზებულ პროცესებთან დაკავშირებული ყოველი ახალშექმნილი პროექტი, ისრუტავდა ინდუსტრიის ამ სექტორში ადრე შემუშავებულ ყველა ეფექტურ მეთოდს, და ამგვარად აახლოებდა იმ გადაწყვეტას, რომელიც ფულადი ურთიერთდამოკიდებულების სისტემაში ნამდვილ რევოლუციას მოახდენდა.

გამონაკლისი არ იყო არც პროექტი BitGold, რომელიც შემუშავებული იქნა იმავე წელს (თუმცა საჯაროდ წარმოდგენილი იქნა მხოლოდ 2005 წელს) უნგრული წარმოშობის ამერიკელი მეცნიერის ნიკო საბოს მიერ, რომელიც სპეციალისტი იყო კრიპტოგრაფიის, ინფორმატიკისა და სამართლის დარგში. მის მიერ შექმნილი სისტემა, გარდა ასიმეტრიული კრიპტოგრაფიისა, შეიცავდა საინტერესო ელემენტს, რომელიც შემდგომში უმნიშვნელოვანეს როლს ითამაშებს ბლოკჩეინ-ტექნოლოგიებში, სახელდობრ, სისტემის მომხმარებელთა მიერ ელექტრონული ფულის ემისიის ჩამოყალიბების მიზნით რთულად გამოსათვლელი ამოცანების ამოხსნის აუცილებლობას. ამოცანა დადიოდა სპეციალურ მოცემული სახის ჰეშების ძებნამდე, სადაც საბოლოო შედეგი იყო მონაცემთა სტრიქონის პოვნა, რომლებიც იწყებოდა ნულოვანი მნიშვნელობის მქონე ბიტების გარკვეული რაოდენობით. რადგანაც ჰეშირების ფუნქცია გვაძლევს ალგორითმულად დამოკიდებულ, მაგრამ ვიზუალურად არაწინასწარმეტყველებად შედეგს, აუცილებელია გადავარჩიოთ დიდი რაოდენობის სხვადასხვა საწყისი წინასახეები, რათა საბოლოოდ აბსოლუტურად შემთხვევით მივიღოთ ისეთი ჰეში, რომლის სახეც დააკმაყოფილებს ამოცანის პირობებს. ამ შემთხვევაში ის უნდა შეიცავდეს ნულოვანი სიმბოლოების აუცილებელ რაოდენობას მონაცემთა სტრიქონის დასაწყისში.

რთულად გამოსათვლელი ამოცანის შექმნის ეს წესი ნიკ საბომ გადმოიღო Hashcash პროექტის ავტორ ადამ ბეკისაგან, რომელმაც ჯერ კიდევ 1997 წელს იხმარა მსგავსი ალგორითმი ელექტრონული ფოსტის მასობრივი დაგზავნის საწინააღმდეგო ქმედების სისტემაში.

ბეკის პროექტში ყოველი წერილის გაგზავნისას აუცილებელი იყო ჰეშის გამოთვლა, სადაც შედეგის პირველი 20 ბიტი უნდა ყოფილიყო ნული. თავისთავად ამოცანა გამოთვლითი თვალსაზრისისთ ძნელი არ იყო და გულისხმობდა მაქსიმუმ 220 ვარიანტის გადარჩევას (ანუ დაახლოებით 1 მილიონის), რისთვისაც ჩვეულებრივ კომპიუტერს სჭირდებოდა მხოლოდ რამდენიმე წამი. მაგრამ ასეთი ამოცანა აუცილებელი იყო ამოხსნილიყო ყოველი გასაგზავნი წერილისათვის, და იმ შემთხვევაში, თუ ადრესატთა რაოდენობა საფოსტო დაგზავნის სიაში მნიშვნელოვანი იყო, მაშინ გაანგარიშებაზე დახარჯული დროის მოცულობა პროპორციულად იზრდებოდა. გამოთვლების შედეგი ემატებოდა ყოველი ელექტრონული წერილის თანმდევ მოსამსახურებრივ ინფორმაციას, რის შემდეგაც ადვილად შემოწმებადი იყო „ვალიდურობაზე“ მიმღების კომპიუტერისათვის საწყისი ნულების აუცილებელი რაოდენობის ნაწილში. ასე სპამ-ფილტრებისათვის ბევრად მარტივი იყო მიღებული საფოსტო შეტყობინების კლასიფიკაცია.

უნდა აღინიშნოს, რომ სიტყვა Gold საბოს პროექტის სათაურში შემთხვევით არაა არჩეული, ავტორს სურს, ძნელად გამოსათვლელი ციფრული ფული შეადაროს ოქროს, რომელიც ძნელი საპოვნი, მოსაპოვებელი და გასაყალბებელია. ოქროს ზოდი ან მისგან დამზადებული ნაკეთობა შეიძლება მივიღოთ მხოლოდ სერიოზული ძალისხმევით – თავიდან გეოლოგებისა და მეშახტეების, შემდეგ ჩამომსხმელების და ბოლოს იუველირების შრომით. ოქროს ფასეულობა განისაზღვრება მისი იშვიათობის, უნიკალური ქიმიური თვისებების და მის მოპოვებაზე და დამუშავებაზე დახარჯული შრომის კომბინაციით. მის ფასეულობაში ასევე არცთუ ბოლო ფაქტორია მოთხოვნისა და შეთავაზების ბალანსი მსოფლიო ბაზარზე. მაგრამ ძირითად როლს მაინც ის ფაქტი თამაშობს, რომ ოქრო მფლობელის ხელში ამტკიცებს, რომ მის მისაღებად გაწეული იქნა რთული სამუშაო.

1999 წელს სტატიაში მარკუს იაკობსონისა და არი ჯუელსის ავტორობით პირველად იქნა შემოღებული ცნება Proof-of-Work ანუ „მუშაობის დადასტურება“. ეს ტერმინი ეხებოდა თავდაპირველი პირველსახის პოვნის კრიპტოგრაფიული ამოცანის ამოხსნას, რომლის ჰეშიც სირთულით გარკვეულ მოთხოვნებს დააკმაყოფილებდა. ამასთან, ქსელის ნებისმიერ სხვა წყაროს, რომელიც მიიღებს გამოთვლილ პირველსახეს, შეეძლოს ადვილად შეამოწმოს მისი ვალიდურობა, მისი ჰეშირების პროცედურაში გაშვებით. ეს საშუალებას იძლეოდა,

მიგვეღო იმის ცალსახა დამტკიცება, რომ რთული გამოსათვლელი სამუშაო მართლაც იქნა ჩატარებული კვანძის მიერ, რომელიც პრეტენზიას აცხადებს ამ ფაქტის მისთვის მიწერაზე.

ნიკ საბო თავის პროექტში BitGold, გამოიყენა რა უმრავლესობა ადრე შემუშავებული მეთოდებისა, მართლაც ახლოს მივიდა დაცული ციფრული ფულის შექმნის ამოცანის ამოხსნასთან. თუმცა მის სისტემაში არსებობდა სისუსტე, რომელსაც „სიბილას შეტევას“ უწოდებენ, როდესაც განაწილებულ ქსელში ყოფნის პირობებში რომელიღაც კონკრეტული კვანძი შეიძლება მოხვდეს რიგი სხვა ისეთი კვანძების გარემოცვაში, რომლებსაც ბოროტმოქმედები აკონტროლებენ. მაშინ შეტევის ობიექტი კვანძი შეიძლება გახდეს მსხვერპლი, რომელიც იღებს მხოლოდ მცდარ ინფორმაციას ქსელური ტრანზაქციების შესახებ, ხოლო ქსელში გასაგზავნი მისი საკუთარი ტრანზაქციები შეიძლება მოდიფიცირებული იქნას შემტევი კვანძების მიერ. ამის გარდა, არსებობდა სხვა პრობლემებიც, რომლებმაც საბოლოოდ საშუალება არ მისცა საბოს პრაქტიკაში განეხორციელებინა თავისი პროექტი. მაგალითად, მან ვერ შეძლო გადაეჭრა ციფრული ფულის ინფლაციის პრობლემა, რომელიც აუცილებლად წარმოიქმნებოდა ქსელში შემავალი კვანძების გამომთვლელი სიმძლავრეების თანდათანობით ზრდასთან ერთად.

მიუხედავად ამისა, ზემოთ აღწერილი სისტემების შემქმნელების შრომას ფუჭად არ ჩაუვლია. მცირე დროის გასვლის შემდეგ ეს პრინციპები ასახვას პოვებს დოკუმენტში, რომელიც მსოფლიოს წარუდგინა ავტორმა, რომლის სახელიც მაშინ არავისთვის იყო ცნობილი, ახლა კი ცნობილია ძალზე ცოტასათვის. საუბარია ადამიანზე, რომლის არსებობის საიდუმლო დღემდე არ არის გახსნილი, ბლოკჩეინ-ტექნოლოგიის და მასზე აგებული საკუთრივ ბიტკოინის როგორც პირველი პროექტის იდუმალ შემქმნელზე. ამ შემქმნელის სახელია სატოში ნაკამოტო, რომელმაც 2008 წელს კრიპტოგრაფიულ საზოგადოებას წარუდგინა სტატია, რომელშიც აღწერდა მისი რევოლუციური პროექტის პრინციპებს, რომელმაც რაღაც დროის შემდეგ მსოფლიო აღიარება მოიპოვა. ვინ არის ეს სატოში ნაკამოტო და რაში მდგომარეობს მისი ციფრული ფულის პროექტის მთავარი განსხვავებები სხვა მსგავსებისაგან, რომლებიც ადრე იყო შემოთავაზებული ასიმეტრიული კრიპტოგრაფიის სფეროს სხვა სპეციალისტების მიერ?

ვინ მოიგონა ბიტკოინი

ბიტკოინის პროექტის ფართოდ აღიარების კვალობაზე, ბევრს გაუჩნდა კითხვა: ვინ არის სატოში ნაკამოტო? არსებობს კი რეალობაში ადამიანი ასეთივე სახელით, თუ საქმე გვაქვს მხოლოდ ეგზოტიკურ ფსევდონიმთან? თუ ვცდით იაპონურ ენაზე „სატოში ნაკამოტოს“ დაწერას, დაგვჭირდება სამი იეროგლიფი. „სატოში“ ნიშნავს „საზრიანს“, „ბრძენს“, „ნათელ აზროვნებას“, გვარის ნაწილი „ნაკა“ – ესაა „ურთიერთკავშირები“, ხოლო „მოტო“ „ფუძეა“ ან „წარმოშობა“. რადგან რეალურ ნაკამოტოს არ დაუტოვებია არც ერთი ტექნიკური აღწერა იაპონურ ენაზე, ხოლო ყველა კომუნიკაციას აწარმოებდა უზადო ინგლისურით, გამოტანილი იქნა ცალსახა დასკვნა, რომ საიდუმლო გამომგონებელი წარმოშობით არის ინგლისურენოვანი გარემოდან.

ასეთ მომენტში კირკიტა ჟურნალისტებმა შეძლეს აღმოეჩინათ აშშ-ში მცხოვრები ადამიანი, სახელად სატოში ნაკამოტო, მაგრამ ის დაჟინებით უარყოფდა თავის მონაწილეობას ბიტკოინის შექმნაში. თუმცა დაჟინებით ამას არც არავინ ამტკიცებდა. საქმე ისაა, რომ ნაპოვნი კანდიდატი საკმაოდ არაცალსახად ეფარდებოდა იმ ადამიანის სახეს, რომელსაც მართლაც შეეძლო შეექმნა მსგავსი პროექტი. ამასთან, ის უნდა ყოფილიყო კრიპტოვალუტის მნიშვნელოვანი მარაგის მფლობელი, რომელიც მას მილიარდერად და მსოფლიოში ერთერთ ყველაზე მდიდარ ადამიანად აქცევდა. სახელის მფლობელი აღმოჩნდა იაპონური წარმოშობის ხანში შესული ამერიკელი, რომელიც ცხოვრობდა კალიფორნიის შტატის ქალაქ ტემპლ-სიტიში.

კალიფორნიის პოლიტექნიკური უნივერსიტეტის კურსდამთავრებული და რკინიგზის მოდელებით გატაცებული დორიან სატოში ნაკამოტო ცალსახად ფლობს მათემატიკის სერიოზულ და პროგრამირების ცოდნასაც კი. მიუხედავად ამისა, ის ამტკიცებს, რომ კრიპტოგრაფიაზე მეტად საკმაოდ სუსტი წარმოდგენა აქვს, ხოლო თავად ბიტკოინის პროექტზე ჟურნალისტებისაგან გაიგო მხოლოდ იმ დღეს, როდესაც ისინი გამოჩნდნენ მისი სახლის პარმაღზე, რამაც სულაც არ შეუშალა ხელი მაშინვე, ყოველი შემთხვევისათვის, პოლი-

ცია გამოეძახებინა. გარდა ამისა, მან განაცხადა, რომ ხანგრძლივი დროის მანძილზე უმუშევარი იყო და თავს შემთხვევითი საქმიანობით ირჩენდა, რის გამოც მისი შემოსავლები ძალზე შემცირდა. ფინანსური პრობლემები, მისი სიტყვებით, ისეთი სერიოზული იყო, რომ იძულებული გახდა უარი ეთქვა სახლში ინტერნეტის ქსელში ჩართვაზე. საბოლოოდ ნაკამოტომ ითხოვა, „პატივი ეცათ მისი პირადი ცხოვრებისათვის და თავი დაენებებინათ მისთვის“, ხოლო ზოგიერთ მომაბეზრებელ ჟურნალისტზე სასამართლოში საქმის აღძვრასაც კი ეცადა. თუმცა მან იმავე დროს მადლობა გადაუხადა კრიპტოსაზოგადოების წარმომადგენლებს მორალური და მატერიალურიი მხარდაჭერისათვის, რომელიც მას გარკვეულად გაეწია. ბევრმა გააკეთა დასკვნა, რომ ან ბატონი ნაკამოტო ოსტატურად გვაჩვენებს თავს, რომ არაფერ შუაშია, ან სიმართლეს ამბობს, და მაშინ საჭირო იქნება უფრო დიდი ძალისხმევა ბიტკოინის ნამდვილი შემქმნელის საპოვნელად, ან „შემქმნელებისა“, თუ ეს ერთი ადამიანი არ არის, არამედ ადამიანთა ჯგუფია, რაც სრულიად დასაშვებია.

თუ დავუშვებთ, რომ საქმე გვაქვს კონკრეტული ადამიანის ფსევდონიმთან, მაშინ ბლოკჩეინ-ტექნოლოგიის საიდუმლო შემქმნელის როლზე ერთ-ერთი ყველაზე საუკეთესო კანდიდატი, BitGold-ის ავტორი, თავად ნიკ საბო იყო. როგორც ცნობილია, ორივე პროექტის შექმნის პრინციპები საკმაოდ მსგავსია, ამასთან, საბო გაჩერდა წარმატებიდან ლამის ერთ ნაბიჯზე, რომლის დემონსტრირებაც ბიტკოინმა მოახდინა. გარდა ამისა, ძალზე საეჭვოდ ითვლებოდა ფაქტი, რომ სატოში ნაკამოტოს პროექტ ბიტკოინის აღწერისას, ციფრული ფულის შემქმნელი მრავალი წინამორბედის ციტირებისას, არც ერთხელ არ უხსენებია ნიკ საბო, მიუხედავად იმისა, რომ სწორედ მისი პროექტი იყო ყველაზე ახლოს სატოშის ქმნილებასთან. რაც შეეხება თავად ნიკ საბოს, მან მაშინვე გადაჭრით უარყო ავტორობა და შემდგომში არც ერთი ნაბიჯი არ გადაუდგამს იმისათვის, რათა ამ საკითხში საქმის ვითარება შეეცვალა. საბომ კმაყოფილება გამოთქვა, რომ კრიპტოგრაფიისა და ციფრული ფულის დარგში მისმა კვლევებმა ასეთი წარმატებული განვითარება პოვა პრაქტიკულ გამოყენებაში. მართალია, როდესაც პროექტი ბიტკოინი მხოლოდ გამოჩნდა, საბომ ის „ვითომდა“ ვერ შენიშნა და მასზე არავითარი კომენტარი არ გაუკეთებია, თუმცა დეცენტრალიზებული ციფრული ფულის

შექმნა, გადაჭარბების გარეშე, მისთვის სასიცოცხლო საქმე იყო. სამართლიანობისათვის უნდა აღვნიშნოთ, რომ ნიკ საბომ მნიშვნელოვანი წვლილი შეიტანა ბლოკჩეინ-ტექნოლოგიის შექმნაში, და ასევე ყოფაში შემოიტანა „ჭკვიანი კონტრაქტების“ ცნება, რომლებმაც გამოყენება პოვა თავიდან სისტემაში Ethereum (ეთერიუმი), ხოლო შემდეგ სხვა ბლოკჩეინ-პლატფორმებში.

თუ დავუბრუნდებით ბიტკოინის ავტორობის კანდიდატების ძიების საკითხს, უნდა ითქვას, რომ ყველამ, ვისზეც ეჭვი ჰქონდათ ჟურნალისტებსა და კრიპტოსაზოგადოების წარმომადგენლებს, უარყო ეს ვარაუდები. კერძოდ, 2016 წელს ავსტრალიელმა მეცნიერმა, პროგრამისტმა და მეწარმემ კრეიგ სტივენმა განაცხადა, რომ სწორედ ის არის პროექტ ბიტკოინის ავტორი. მაგრამ მან ვერ შეძლო თავისი ავტორობის დამაჯერებელი მტკიცებულებების წარმოდგენა, როდესაც სთხოვეს დახურული გასაღების საფუძველზე შეექმნა ციფრული ელექტრონული ხელმოწერა, რომელიც გამოიყენებოდა ბიტკოინის პირველი ტრანზაქციების ხელმოსაწერად (რომელიც ეჭვგარეშე ეკუთვნოდა სატოში ნაკამოტოს), რაიტმა ამაზე უარი განაცხადა, რაზეც, როგორც მოსალოდნელი იყო, საჯაროდ გაიკიცხა ბლოკჩეინ-საზოგადოების მიერ, რომელმაც მას ბრალი დასდო ბანალურ სიყალბესა და ტყუილში. დავამატებთ ასევე, რომ რაიტის ავტორობაზე დეკლარაციამდე ცოტა ხნით ადრე მის სახლს სიდნეიში ეწვია პოლიცია, რადგან მის მიერ ფულის გათეთრებაზე ჰქონდათ ეჭვი, რის შემდეგაც, ალბათ, მან გადაწყვიტა ამგვარად მიეპყრო ყურადღება, თუმცა საკმაოდ საეჭვოდ. კიდევ ერთი ფაქტორია რიგ მეცნიერთა აზრი იმის შესახებ, რომ რაიტის ნაცნობობა პროექტ ბიტკოინის ტექნიკურ მხარესთან საკმაოდ ზედაპირულია, რაც ასევე არ მეტყველებს მისი ავტორობის აღიარების სასარგებლოდ.

თუ დავიწყებთ ბიტკოინის შემქმნელისადმი მიძღვნილი სტატიების შესწავლას, უნებურად გაგვიკვირდება, ვისზე არ ჰქონიათ ეჭვი ამ პროექტის ავტორობასთან დაკავშირებით. IT-ინდუსტრიის ძალზე ბევრ ადამიანი გახდა ღირსი ასეთი ვარაუდებისა. სახელდებოდნენ Microsoft-ის დამფუძნებელი ბილ გეიტსი, Apple-ის დამფუძნებელი სტივენ ჯობსი და კომპანიების PayPal, Tesla და Space X-ის ერთ-ერთი დამფუძნებელი ილონ მასკიც კი. რა თქმა უნდა, ყოველმა მათგანმა

საკმაოდ სწრაფად უარყო ბიტკოინის შექმნაში თავისი მონაწილეობის ყოველგვარი ფორმა. კრიპტოსაზოგადოების ავტორიტეტულ წარმომადგენელთაგან ბიტკოინის სავარაუდო ავტორებად სხვადასხვა დროს თვლიდნენ Bitcoin Foundation-ის (არაკომერციული ორგანიზაციები, რომლებიც დაკავებულნი იყვნენ სტანდარტიზაციით, ბიტკოინის დაცვით და მისი გამოყენების წახალისებით მთელ მსოფლიოში) დამფუძნებელს გევინ ანდერსენს და ასევე პროექტ Litecoin-ის, რომელიც ბიტკოინის ალტერნატივად შეიქმნა და რომელიც იყენებდა მის კოდს როგორც საბაზო საფუძველს, ავტორს ჩარლი ლის.

სინამდვილეში ბიტკოინის შემქმნელის როლზე პოტენციური კანდიდატების სია იმდენად დიდია, რომ ჩვენ არ დავიწყებთ მის მთლიანად მოყვანას და თითოეულის ცალ-ცალკე განხილვას. რაც შეეხება კონკრეტულად გევინ ანდერსენს, მას მიმოწერა ჰქონდა ნამდვილ სატოში ნაკამოტოსთან დაახლოებით ორი წლის განმავლობაში, ამ უკანასკნელის უეცარ გაქრობამდე კომუნიკაციის ყველა სახეობიდან 2011 წლის გაზაფხულზე. როგორც თავად ნაკამოტომ განაცხადა, „ის მიდის, რათა დაკავდეს უფრო მნიშვნელოვანი საქმეებით“. მათი ურთიერთობის პროცესში ანდერსენი თვლიდა, რომ საქმე აქვს იაპონური წარმოშობის ნიჭიერ ადამიანთან, რომელიც კარგად ლაპარაკობს ინგლისურად. თუმცა, ნაკამოტოსაგან ქსელის კლიენტის პროგრამული უზრუნველყოფის მიღების შემდეგ, ანდერსენსა და მის კოლეგებს მოუხდათ კოდის დაახლოებით 70%-ის გადაწერა, რადგან მათ ის ჩათვალეს საკმაოდ „დაუდევრად“. სხვათა შორის, სწორედ ამ ფაქტორმა აიძულა ისინი ევარაუდათ, რომ ნაკამოტომ შექმნა ბიტკოინი, ალბათ, მარტომ, წინააღმდეგ შემთხვევაში კოდში არ იქნებოდა ამდენი შეცდომა და ის იქნებოდა უფრო „წაკითხვადი“. შემდგომში ანდერსენი გარკვეული დროის განმავლობაში კრეიგ რაიტს თვლიდა იმ ადამიანად, რომელთანაც ის ურთიერთობდა როგორც ბიტკოინის ავტორთან, მაგრამ შემდეგ მან აღიარა თავისი შეცდომა და ავტორობის საკითხი კვლავ აქტუალური გახდა.

და ბოლოს, რეალური შემქმნელის ძებნით დაკავდა სერიოზული ორგანიზაცია, აშშ-ის ეროვნული უსაფრთხოების სააგენტო. ამ უწყების სპეციალისტემა ჩაატარეს ნაკამოტოს ყველა იმ ტექსტის ლინგვისტური ანალიზი, რომელსაც იგი ათავსებდა კრიპტოგრაფიასა და ციფრული გადახდის საშუალებების შექმნისადმი მიძღვნილ სხ-

ვადასხვა ფორუმზე. ანალიზის პროცესში გამოყენებული იქნა ე.წ. „სტილომეტრიის“ მეთოდი, რომელიც საშუალებას იძლევა, გამოვიკვლიოთ ტექსტების დაწერის სტილისტიკა სხვადასხვა სიტყვის გამეორების სტატისტიკური ანალიზის საფუძველზე. ამ მეთოდს ასევე ეწოდება „საავტორო ინვარიანტი“, რომელიც ასახავს ლიტერატურული ტექსტების რაღაც რაოდენობრივ მახასიათებელს. ნაკამოტოს ტექსტები შეადარეს სხვა ავტორების ტექსტებს, ამასთან, ამ ნიმუშების რაოდენობა ლამის ტრილიონებისაგან შედგებოდა. შედეგად მიიღეს ნაკამოტოს ტექსტების უნიკალური „ციფრული ანაბეჭდი“, რომელიც ცალსახად ახდენდა მის ავტორობას. ჰქონდათ რა წვდომა ისეთი კორპორაციების ელექტრონული შეტყობინებების, ჩატების ლოგების უზარმაზარ საცავთან და მთლიანად მონაცემთა დამუშავებისა და შენახვის ცენტრების არქივების ტრაფიკთან, როგორიცაა Google, Amazon და Facebook, ეუს-ს სპეციალისტებს გაუჩნდათ საშუალება შეედარებინათ ნაკამოტოს „ანაბეჭდი“ მონაცემებთან, რომლებიც ეკუთვნოდა სულ მცირე მილიარდ ადამიანს. ცნობილია, რომ მონაცემთა დამუშავებას დასჭირდა დაახლოებით ერთი თვე, ჭორების მიხედვით, მიიღეს ძიების დადებითი შედეგები, რომელსაც ეუს-ს საიდუმლოდ ინახავს.

რატომ გადაწყვიტა ამ იდუმალებით მოცულმა სატოში ნაკამოტომ ყოფილიყო ინკოგნიტო? ამ კითხვაზე ცალსახა პასუხი არ არსებობს, და ჩვენ შეგვიძლია მხოლოდ ვივარაუდოთ მიზეზები, რომლებმაც მას ამისაკენ უბიძგა. გააკეთა მან ეს მხოლოდ ბუნებრივი მოკრძალებულობის გამო, თუ ხელმძღვანელობდა პირადი უსაფრთხოების მოსაზრებებით, რადგან ესმოდა, რომ მისმა გამოგონებამ რევოლუცია შეიძლება გამოიწვიოს ბიზნესის სამყაროსა და სოციალურ ურთიერთდამოკიდებულებებში? ვარაუდობდა კი ის, რომ მრავალი სახელმწიფოს მთავრობები შეშფოთებულნი იქნებიან ფულადი ემისიების დეცენტრალიზაციის, ფინანსური ნაკადების ანონიმიზაციის და, როგორც შედეგი, მათზე კონტროლის შესაძლო დაკარგვის პრობლემატიკით? ასეა თუ ისე, სატოში ნაკამოტო გაქრა და შემდგომში არასოდეს გაუმჟღავნებია თავი არც ინტერნეტში და არც რომელიმე მედიასაშუალებაში. უკანასკნელ შეტყობინებაში ანდერსენის საპასუხოდ, მიეღო CIA-ს მიწვევა სასაუბროდ შესახვედრად, ნაკამოტომ დაწერა სიტყვასიტყვით შემდეგი:

„იმედი მაქვს, რომ მათთან პირისპირ საუბრისას, შევძლებ პასუხი გავცე ყველა მათ კითხვას და გავაქარწყლო მათი ეჭვები. მე მინდა დავარწმუნო ისინი იმაში, რომ ბიტკოინი არის მხოლოდ უფრო ეფექტური და პოლიტიკოსების ქმედებებზე არადამოკიდებული გადახდის საშუალება და არა შავი ბაზრის ყოვლისშემძლე, როგორც ისინი თვლიან, ინსტრუმენტი, რომელსაც ანარქისტები გამოიყენებენ სისტემის წინააღმდეგ საბრძოლველად“.

ისინი, ვისაც პატივი ხვდა წილად ინტერნეტის საშუალებით ესაუბრათ ნაკამოტოსთან, აღნიშნავენ მის ფართოდ განათლებულობას, და ასევე სერიოზულ კვალიფიკაციას კრიპტოგრაფიასა და პროგრამირებაში. გარდა ამისა, აშკარად გვხვდებოდა თვალში ნაკამოტოს ლიბერტარიანული შეხედულებები და ასევე მისი სიფრთხილე მთავრობების, გადასახადების, ბანკებისა და მათთან დაკავშირებული პერსონების მიმართ. შესაძლოა, საკუთარი სახელის საიდუმლოდ შენახვით, ნაკამოტოს იმედი ჰქონდა, რომ ამით დაიცავდა ბიტკოინს სახელმწიფოს ჩარევისაგან, რისი შედეგიც შეიძლება გამხდარიყო ის, რომ პროექტი საბოლოოდ ვერ იხილავდა დღის სინათლეს. თავად ნაკამოტო ახსენებდა, რომ ბიტკოინის კონცეფციის შექმნაზე მუშაობამ მას წაართვა არანაკლებ შვიდი წლისა და ის დარწმუნებული იყო, რომ ბოლოს და ბოლოს გადაჭრა ამოცანა, რომელსაც თავი ვერ გაართვეს მისმა წინამორბედებმა. ნებისმიერ შემთხვევაში დადგა დრო, დეტალებში განვიხილოთ, თუ რას წარმოადგენს პროექტი ბიტკოინი და როგორია მისი ტექნოლოგიური მოწყობა?

როგორ არის მოწყობილი ბიტკოინი

უნდა ვაღიაროთ, რომ წინა თავებში სხვადასხვა მეთოდიკის, მიდგომისა და ტექნოლოგიის აღწერისას, რომლებიც გამოიყენება ბლოკჩეინზე პროექტების ასაგებად, საფუძვლად სწორედ პროექტ „ბიტკოინის“ პრინციპები გამოიყენებოდა. რასაკვირველია, წარმოშობის მომენტიდან ათი წლის შემდეგ ბიტკოინი რაღაც ხარისხით არქაულად გამოიყურება უფრო თანამედროვე ბლოკჩეინ-პროექტებთან შედარებით. თუმცა, სწორედ ბიტკოინმა ჩაუყარა საფუძველი ბლოკჩეინის ტექნოლოგიის შემდგომ ევოლუციას. არ დავიწყებთ ბიტკოინ-ქსელში გამოყენებული ძირითადი მეთოდების ტექნოლოგიური აღწერის დეტალურ გამეორებას, რადგან ისინი ადრე განვიხილეთ. მაგრამ ამასთან ერთად, ბიტკოინს აქვს რიგი დამატებითი თავისებურებებისა, რომლებიც წინასწარ იყო აღწერილი. ჰოდა, ახლა მათზე უფრო დაწვრილებით შევჩერდებით.

დასაწყისისთვის შევეცადოთ გავერკვეთ, როგორ ყალიბდება ბიტკოინის ქსელში ადრესაციის სისტემა. იმისათვის, რომ ბიტკოინის ქსელში მივიღოთ ადრესაცია, პირველ რიგში აუცილებელია, ასიმეტრიული კრიპტოგრაფიის ერთ-ერთი ალგორითმის საშუალებით გასაღებების წყვილის გენერირება. ბიტკოინი, როგორც სხვა უმრავლესი ბლოკჩეინ-პროექტი, იყენებს დისკრეტული გალოგარითმების ალგორითმს ელიფსური მრუდის წერტილთა ჯგუფში. როგორც ცნობილია, ელიფსური მრუდი (ECDSA) გადმოიცემა შემდეგი განტოლებით:

$$y^2 = x^3 + ax + b$$

ბიტკოინი იყენებს ამ განტოლების ფორმას $y^2 = x^3 + 7$ სახით. აშკარა გამარტივებამ მკითხველი შეცდომაში არ უნდა შეიყვანოს, მითითებული კოეფიციენტები სავსებით საკმარისია იმისათვის, რომ შეიქმნას მნიშვნელოვანი გამოთვლითი სირთულე საჯარო გასაღებიდან საიდუმლოს უკუამოცანის ამოხსნის ნაწილში. საერთოდ, ელიფსური მრუდების პარამეტრებისათვის მონაცემები აღებულია კონსორციუმ SECG-ის რეკომენდაციებიდან, რომელმაც შეიმუშავა

„ეფექტიანი კრიპტოგრაფიის სტანდარტები“, რომლებიც გამოიყენება მათ შორის ბიტკოინ-პროექტში. პარამეტრები გათვლილია იმგვარად, რომ სისტემას შესძინოს მინიმალური მოწყვლადობა შიფრებზე თავდასხმის მცდელობისას, რომლებიც შექმნილია ასიმეტრიული კრიპტოგრაფიული მეთოდების ბაზაზე. მიმდინარე მომენტში არ არის ცნობილი ელიფსური მრუდის იმ ალგორითმის გატეხის წარმატებული მცდელობის არც ერთი შემთხვევა, რომლებიც იყენებს SECG-ის რეკომენდებულ პარამეტრებს. შესაძლოა, ამ ამოცანებს წარმატებით ამოხსნის კვანტური კომპიუტერები, მაგრამ ამისათვის აუცილებელია, მათ ჰქონდეთ საკმარისი რაოდენობის კუბიტები, ხოლო ამას დასჭირდება დრო, თანაც – საკმაოდ დიდი.

დავუბრუნდეთ გასაღებების გენერაციას. თავიდან, შემთხვევითი სახით იქმნება 256-ბიტიანი დახურული გასაღები, ხოლო შემდეგ მათემატიკურად გამოითვლება ზუსტად იმავე ზომის საჯარო გასაღები. მაგრამ საჯარო გასაღები ჯერ სულაც არ არის ბიტკოინის მისამართი. იმისათვის, რომ მისამართი გახდეს, მას გარკვეული პროცედურები უნდა ჩაუტარდეს. თავიდან ღია გასაღებს თანმიმდევრულად ატარებენ ჰეშირების ორ სხვადასხვა ალგორითმში (SHA-256 и MD5). ბოლო შემთხვევაში მისი მისამართი მოკლდება 256 ბიტიდან 160 ბიტამდე. შემდეგ მიღებულ შედეგს დასაწყისში უმატებენ ქსელის (ძირითადი ან სატესტო ქსელი) იდენტიფიკატორის ერთ ბაიტს, ხოლო ბოლოში მისამართის საკონტროლო ჯამის ოთხ ბაიტს, რომელიც ასევე შეადგენს უკანასკნელი შედეგის ჰეშის ნაწილს. საკონტროლო ჯამი აუცილებელია შესამოწმებლად, თუ მისამართის შეყვანა ხელით ხდება: მცდარი შეყვანისას სისტემა გვაფრთხილებს. ბლოკჩეინში ტრანზაქციების უკან გამოწვევა შეუძლებელია, ამიტომ კრიპტოსახსრების გამგზავნს არ აქვს შეცდომის უფლება. თუ შეყვანილი იქნება არაკორექტული მისამართი, გამგზავნის სახსრები გაიგზავნება „არსად“, უფრო სწორად – მისამართზე, რომლისთვისაც ქსელის არც ერთ პოტენციურ მომხმარებელს არ ექნება „საღებელა“ საიდუმლო გასაღების სახით. შედეგად ვერავინ წარადგენს უფლებამოსილებას ამ სახსრებზე, რომლებიც ამის გამო, უკან მოუბრუნებლად იქნება დაკარგული სისტემისათვის.

ბიტკოინ-მისამართის მიღების პროცედურაში დამამთავრებელი ნაბიჯია გარდაქმნა უფრო „წაკითხვად“ სახედ. ამისათვის მონაცემთა ბლოკი თექვსმეტობითი კოდის (რომელიც იყენებს ციფრებს

0-დან 9-მდე და ასოებს A-დან F-მდე) ფორმატით ციფრებისა და ასევე, მცირე და დიდი ლათინური ასოების შემცველ სტრიქონად გარდაიქმნება Base58 ალგორითმით. ეს პროცედურა აუცილებელია, რათა მისამართიდან გამოვრიცხოთ სიმბოლოები, რომლებიც ორგვარად შეიძლება იქნას გაგებული ხელით აკრეფისას: მაგალითად, მცირე ლათინური l და დიდი ლათინური I ან დიდი ასო O და ციფრი 0. ყველა ეს ზომა მიმართულია ტრანზაქციების შესრულებისას მისამართის შეცდომით შეყვანისაგან დამატებით დასაცავად. ყველა აუცილებელი პროცედურის დასრულების შემდეგ ბიტკოინ-მისამართმა შეიძლება მიიღოს, მაგალითად, შემდეგი სახე:

1A1zP1eP5QGefi 2DMPTfTL5SLmv7DivfNa

ახლა მომხმარებელს აქვს საკუთარი მისამართი ბიტკოინ-ქსელში, თუმცა ამის შესახებ თვითონ არაფერი იცის, რადგან მომხმარებელი მისამართის გენერაციას თავის ლოკალურ მოწყობილობაზე ახორციელებდა. მაგრამ, როცა მას აქვს გასაღებების წყვილი და მისგან შექმნილი მისამართი, მომხმარებელს მასზე შეუძლია კრიპტოსახსრების მიღება და შემდეგ მისი გაგზავნა ნებისმიერ სხვა მისამართზე, რომელსაც მოისურვებს. ჰოდა, მაშინ, პირველ ტრანზაქციასთან ერთად, მისი ქსელში გავრცელებისდაგვარად, ამ მისამართის შესახებ გაიგებენ როგორც სისტემის ახალ წევრზე. ჩნდება კითხვა: მაინც სად ხვდება ტრანზაქცია? ლოგიკური იქნებოდა გვევარაუდა, რომ ის ჩართული იქნება ბლოკში, რომელიც ახლა ქსელის მიერ ფორმირდება. მაგრამ მთლად ასე არ არის. თავდაპირველად ტრანზაქცია იგზავნება მთელ ქსელში სხვადასხვა კვანძს შორის პირდაპირი შეერთებების საშუალებით. ამასთან, ყოველი კვანძი, მიიღებს თუ არა ახალ ტრანზაქციას, „ვალიდობაზე“ მის შემოწმებას ახორციელებეს. კვანძები ამოწმებს, მართლაც ფლობს თუ არა გამგზავნი იმ თანხას, რომლის გაგზავნაც სურს. ასეთი შემოწმების განხორციელება შესაძლებელია, ამ გამგზავნის სასარგებლოდ წინა ტრანზაქციების ყველა „დაუხარჯავი გასავლის“ გამოთვლით, ასევე, მათემატიკურად მოწმდება გამგზავნის ციფრული ელექტრონული ხელმოწერის შესაბამისობა მისგან მითითებულ ღია გასაღებთან. ეს იმისათვის არის საჭირო, რომ დავრწმუნდეთ – ტრანზაქციის გამ-

გზავნი ფლობს დახურულ გასაღებს იმ მისამართისა, რომლიდანაც ფულის დახარჯვას აპირებს. თუ ტრანზაქციამ წარმატებით გაიარა ყველა აუცილებელი შემოწმება, მაშინ ის ხვდება დროებით საცავში, რომელსაც „მემპული“ (mempool) ეწოდება.

მემპული არის რაღაც, ტრანზაქციების რიგის მსგავსი, რომლებიც ელოდებიან თავიანთ ჩართვას ბლოკში. ყველა კვანძი დამოუკიდებლად განსაზღვრავს მემპულის ზომას, რომელსაც იგი შეინახავს. სხვაობა მემპულსა და ჩვეულებრივ რიგს შორის მდგომარეობს დასამუშავებლად შემოსული ტრანზაქციების პრიორიტეტიზაციის სხვადასხვა ფორმაში. თუ ჩვეულებრივ რიგში მონაცემები მუშავდება მათი შემოსვლის დროის მიხედვით, მემპულში მათ რანჟირებას უკეთებენ საკომისიოს სიდიდის მიხედვით, რომელიც გამგზავნებმა თავიანთი ტრანზაქციებისათვის განსაზღვრეს. როგორც უკვე ითქვა, ტრანზაქციის საკომისიოს სიდიდე დგინდება დამოუკიდებლად გამგზავნის მიერ, გამომდინარე მისივე სურვილიდან ამ ტრანზაქციის უახლოეს შესაქმნელ ბლოკში ჩართვის სისწრაფიდან. რადგან ბლოკის შემქმნელი ბლოკში ჩართული ყველა ტრანზაქციის მთელ საკომისიოს თვითონ იღებს, ლოგიკური იქნებოდა გვევარაუდა, რომ ის პირველ რიგში, ბლოკში ჩართავს ყველაზე მაღალი საკომისიოს მქონე ტრანზაქციებს.

თუ გავითვალისწინებთ იმ ფაქტს, რომ ბლოკის ზომა ბიტკოინ-ქსელში შეზღუდულია ერთი მეგაბაიტით, ხოლო ტრანზაქციის საშუალო ზომა შეადგენს 300 ბაიტს, მაშინ ერთ ბლოკში შეიძლება ჩავატიოთ დაახლოებით 4000 ტრანზაქცია, რაც თავისთავად, საკმაოდ ცოტაა. ბიტკოინის ქსელი იმგვარადაა აწყობილი, რომ ყოველი ახალი ბლოკი იქმნება დაახლოებით ათ წუთში ერთხელ, ამიტომ მთელი ქსელის გამტარუნარიანობა შეადგენს დაახლოებით შვიდ ტრანზაქციას წამში. ქსელში მაღალი დატვირთვებისას, როდესაც ტრანზაქციების რაოდენობა მნიშვნელოვნად შეიძლება გაიზარდოს, მემპული იწყებს სწრაფად ზრდას ზომებში, იმ დროს, როდესაც ტრანზაქციების ბლოკში ჩართვის სიჩქარე მცირდება. ამიტომ, იმისათვის, რომ ტრანზაქცია რაც შეიძლება სწრაფად მოხვდეს ახალ ბლოკში, გამგზავნები ზრდიან საკომისიოს. 2017 წლის დეკემბერში აღნიშნული იქნა მემპულის რეკორდული ზომა – დაახლოებით 140 მეგაბაიტი; ამასთან, დამუშავების მომლოდინე ტრანზაქციების რიცხვმა 200 000-ს გადააჭარბა. უკვე ნახევარი წლის შემდეგ დაძაბულობა

ბიტკოინ-ქსელში შესუსტდა, მემპულის ზომა ერთეულ მეგაბაიტამდე შემცირდა, ხოლო ტრანზაქციის დამუშავების საკომისიო ჩვეულებრივ მნიშვნელობებს დაუბრუნდა.

როგორც უკვე აღინიშნა, ქსელის ყოველი წევრი, რომელიც კვანძების სხვა წევრთა თანაბარუფლებიანია, თავის ლოკალურ მოწყობილობაზე (როგორც წესი, ეს ჩვეულებრივი კომპიუტერია) იღებს მთელ ინფორმაციას ბიტკოინ-ქსელის ყველა ბლოკისა და ტრანზაქციის შესახებ. რადგან ბლოკთა ბაზა დროთა განმავლობაში იზრდება, სინქრონიზაციისათვის გადაცემული ინფორმაციის მოცულობაც მუდმივად იზრდება ზომაში. აშკარაა, რომ, თუ კვანძმა ადრე მიიღო ინფორმაცია შექმნილ ბლოკებზე, მას უკვე აღარ სჭირდება მისი განახლება, რადგან დროში ის არ იცვლება. მიუხედავად ამისა, მან უნდა გააგრძელოს ინფორმაციის მიღება ახალშექმნილ ბლოკებზე და ასევე, შეინახოს მემპულები, სადაც მუდმივად ხორციელდება ახალი ტრანზაქციები, რომლებიც ჯერ კიდევ არ არის ჩართული ბლოკში.

ყველა ეს მონაცემი მნიშვნელოვანი ზომისაა: 2019 წლის გაზაფხულის მდგომარეობით, ბიტკოინის მონაცემთა ბაზის მოცულობა შეადგენდა დაახლოებით 570 000 ბლოკს და ეკავა დაახლოებით 250 გიგაბაიტი დისკის სივრცეზე. მათთვის, ვისაც არ სურს გამოყოს ადგილი მონაცემთა ასეთი გვარიანი მოცულობისათვის, აზრი აქვს ისარგებლოს „მსუბუქი კლიენტის“ სტატუსის მიღების შესაძლებლობით, როდესაც ინფორმაციის მთელი მოცულობის მაგივრად ის გადმოტვირთავს მხოლოდ ბლოკების სათაურებს ტრანზაქციათა სიის გარეშე. ამ შემთხვევაში, მისთვის აუცილებელია, თავის მოწყობილობაზე მიიღოს მხოლოდ ინფორმაციის რამდენიმე ასეული მეგაბაიტი, რაც შეუდარებლად მარტივად და სწრაფად ხდება, ვიდრე მთელი ბაზის სინქრონიზება. ოღონდ ამ შემთხვევაში, ამ „მსუბუქ“ კვანძს არ შეუძლია მონაწილეობა მიიღოს ახალი ბლოკების შექმნაში. თუმცა, ამით ქსელის ყველა წევრი როდია დაკავებული. 2019 წელს ბიტკოინ-ქსელში იყო დაახლოებით 10 000 სრული კვანძი, ხოლო აქტიურად გამოყენებადი უნიკალური მისამართების რაოდენობა დაახლოებით 640 000-ს შედგენდა.

საერთოდ, ბლოკჩეინის მუშაობის პრინციპებისა და კერძოდ, ბიტკოინ-ქსელის კვლევისას აუცილებელია წარმოვიდგინოთ ახალი ბლოკების შექმნის მექანიკა განაწილებულ ქსელში. გასაგებია, რომ

ჯაჭვის ბოლოს ყოველთვის ემატება მხოლოდ ერთი ბლოკი, რომელიც იმ მომენტში იქმნება ქსელის მხოლოდ ერთი მონაწილის მიერ. ამასთან, მთელი დანარჩენი ქსელი უნდა დაეთანხმოს ამას კონსენსუსის მიღწევის მექნიზმის საშუალებით და თავისთან უნდა მოახდინოს ბლოკების ბაზის სინქრონიზება ახალ, უკანასკნელად შექმნილ ბლოკთან ერთად. თუმცა, როგორც დავრწმუნდით, ქსელში სავსე კვანძების რაოდენობა აღწევს ათასებს და ყოველ მათგანს პოტენციურად შეუძლია სხვა კვანძებისაგან დამოუკიდებლად შექმნას საკუთარი ბლოკი და შესთავაზოს ის მთელ დანარჩენ ქსელს ბლოკების საერთო ჯაჭვში ჩასართველად. ამ ფაქტიდან აუცილებლად გამომდინარეობს, რომ წუთებით განსაზღვულ დროის მცირე მონაკვეთში, ქსელში შეიძლება გაჩნდეს ერთმანეთში კონფლიქტის მქონე ბლოკები, რომლებსაც საერთო ჯაჭვში ჩაბმის პრეტენზია აქვს. ამასთანავე, კვანძების ნაწილი შეიძლება შეიცავდეს ერთგვარ ბლოკს, ხოლო ნაწილი – სრულიად სხვაგვარს. ამ მომენტიდან ქსელში ხდება განტოტება, ბლოკების ბაზის განსინქრონიზება, სხვა სიტყვებით რომ ვთქვათ, წარმოიშობა პრობლემა მთელი ქსელისათვის, რომლის გადაწყვეტაც აუცილებელია.

თუ გვსურს, გადავჭრათ ეს პრობლემა, უნდა განვიხილოთ ბლოკის შექმნის პროცესი როგორც ასეთი. ბლოკის შესაქმნელად აუცილებელია ამოვიღოთ მემპულიდან ტრანზაქციები, სანამ ბლოკში ადგილი გვრჩება, მათ საფუძველზე გამოვთვალოთ მერკლის ხის ძირითადი ფესვის მნიშვნელობა, რომლის ბაზაზეც დანარჩენ სამსახურებრივ ინფორმაციასთან ერთად შეიქმნება ბლოკის სათაური. შემდეგ, შესაქმნელი ბლოკის სათაურში უნდა მოვათავსოთ წინა ბლოკის სათაურის ჰეში, რათა გავაგრძელოთ ბლოკების ჯაჭვის უწყვეტობა, რის შემდეგაც ახალი ბლოკი მზადაა და შეიძლება გაიგზავნოს ქსელში, რათა დანარჩენმა კვანძებმა ის საკუთარ ჯაჭვებში ჩასვან. ახლა დავსვათ კითხვა: რა მოხდება, თუ კვანძების საკმაოდ დიდი რაოდენობა ერთდროულად დაიწყებს საკუთარი ბლოკების შეთავაზებას ქსელის დანარჩენი წევრებისათის? ეჭვგარეშეა, დაიწყება სრული ქაოსი. კავშირის არხები გადატვირთული იქნება სინქრონიზაციისათვის გადაგზავნილი ინფორმაციით, აუცილებლად წარმოიშობა ჯაჭვების განშტოებების სხვადასხვა ვარიანტის უზარმაზარი რაოდენობა, ანუ ქსელი ფაქტობრივად დაკარგავს მთლიანობას და შედეგად, შრომისუნარიანობას.

იმისათვის, რომ თავიდან ავიცილოთ მოვლენათა განვითარების ნეგატიური სცენარი, აუცილებელია, რომ ჯაჭვში ჩასართავი ქსელისათვის შეთავაზებული ბლოკების რაოდენობა ძალზე მცირე იყოს. იდეალურ შემთხვევაში – ბლოკების შექმნას შორის ინტერვალის საშუალო დროის განმავლობაში (ბიტკოინ-ქსელში – დაახლოებით ათი წუთი) ქსელში კონკურენტული ბლოკები საერთოდ არ უნდა არსებობდეს. მაგრამ როგორ მივაღწიოთ ამას? პასუხი მარტივია: აუცილებელია, ბლოკების შექმნის პროცესი გავხადოთ ისეთი რთული, რომ ახალი ბლოკის შესაქმნელად გამოყოფილ დროის კვანტში ქსელს შესთავაზონ ახალი ბლოკების მინიმალური რაოდენობა. ამ შემთხვევაში, მათ შესაქმნელად აუცილებელ პირობად უნდა იქცეს რთული გამოთვლითი ამოცანის გადაჭრა, დაახლოებით ისეთის, რომელიც აღწერილი იყო ცნებაში „მუშაობის დადასტურება“ ანუ Proof-of-Work. ბიტკოინ-ქსელში ბლოკის შექმნის ამგვარ პროცესს ეწოდება „მაინინგი“, სასარგებლო წიაღისეულის მოპოვების ანალოგიურად, სადაც საჭიროა სერიოზული ძალისხმევა მანამ, სანამ შესაძლებელი გახდება შახტიდან ძვირფასი რესურსის ამოღება და მისი რეალიზება, მატერიალური სარგებლის მისაღებად. მაინც როგორ ხორციელდება ციფრული მაინინგი ბიტკოინ-ქსელში?

მაინინგი ბიტკოინ-ქსელში

Proof-of-Work-ის ცნების ინტეგრაციაზე მუშაობისას თავის პროექტ BitGold-თან, რომელსაც ბევრი ბიტკოინის „წინამორბედად“ თვლის, ნიკ საბო გადაეყარა პრობლემას, როდესაც გამოსათვლელი ამოცანის ფიქსირებული სირთულე იწვევდა პოტენციურ მოწყვლადობას, რომელიც დიდი ალბათობით, თავს იჩენდა მომავალში. საქმე ისაა, რომ ქსელის ერთობლივი სიმძლავრე დროთა განმავლობაში ბუნებრივად გაიზრდება. ეს ხდება ორი მიზეზის გამო: პირველ რიგში, გაიზრდება ბლოკების საერთო რაოდენობა, ხოლო მეორე რიგში, მურის კანონის შესაბამისად, სისტემის ცალკე აღებული კვანძის გასაშუალებული გამომთვლელი სიმძლავრე ასევე, თანდათანობით გაიზრდება. ამგვარად, გარკვეული დროის შემდეგ პროექტის ლოგიკაში ჩადებული გამოსათვლელი ამოცანის ფიქსირებული სირთულე ქსელისათვის პრობლემა აღარ იქნება. საბოლოოდ, ქსელის კვანძები გადაიქცევა ელექტრონული ფულის „საბეჭდ დაზგებად“, რაც სისტემაში აუცილებლად გამოიწვევს ჰიპერინფლაციის პროვოცირებას. ღირს კი დავეჭვდეთ, რომ ამის შემდეგ სისტემის ყველა კვანძი მატერიალურად დემონტირდება და ძნელად თუ მოისურვებს შემდგომში მსგავს პროექტში მონაწილეობას?

შეგახსენებთ, რომ რთულად გამოსათვლელი ამოცანის არსი პროექტ BitGold-ში მდგომარეობდა სხვადასხვა წინასახის ჰეშების გადარჩევაში, ხოლო საბოლოო მიზანი იყო ისეთი ჰეშის პოვნა, რომელიც მთელი ქსელისთვის ვალიდურად ჩაითვლებოდა, ანუ ამ შემთხვევაში, შეიცავდა გარკვეული რაოდენობის ნულებს მონაცემთა სტრიქონის დასაწყისში. გამოსათვლელი ამოცანის სტატისტიკური სირთულე საბოსთვის გახდა ერთ-ერთი გადაულახავი წინააღმდეგობა, რომელმაც საშუალება არ მისცა BitGold-ს, დღის სინათლე ეხილა. სამაგიეროდ, სატოში ნაკამოტომ თავის პროექტში ეს ამოცანა გადაჭრა და, როგორც დავრწმუნდებით, საკმაოდ მოხდენილადაც.

სინამდვილეში, ამ პრობლემის გადასაჭრელად, აშკარა გადაწყვეტა თავისთავად მოდის: თუ სტატისტიკური სირთულე სისტემის ეკონომიკური სტაბილურობისათვის ბარიერს წარმოადგენს, მაშინ

ის აუცილებელია, დინამიკური გავხადოთ. როგორც უკვე ცნობილია, იმისათვის, რომ ჰეშის სტრიქონის დასაწყისში მივიღოთ n ნულოვანი ბიტი, ჰეშირებისთვის უნდა გადავარჩიოთ მაქსიმუმ 2n წინასახე. აშკარაა, რომ რაც უფრო დიდია რიცხვი n, ამოცანის სირთულე ამით თვალსაჩინოდ იზრდება. ნაკამოტომ შემოგვთავაზა შესაქმნელი ბლოკის სათაურის ჰეშირება, დაწყებული ყველაზე მცირე სირთულიდან. ამ შემთხვევაში უნდა მიგვეღო მხოლოდ რვა ნულოვანი სიმბოლო სათაურის ჰეშის სტრიქონის დასაწყისში. რადგან ერთი სიმბოლო იჭერს ოთხ ბიტს, საჭიროა 2^{32} ვარიანტზე მეტის ანუ დაახლოებით 4,3 მილიარდის გადარჩევა. შემდეგ, ქსელში კვანძების რაოდენობის ზრდის კვალობაზე, რომლებიც ცდილობს იპოვოს ვალიდური ჰეში, პროპორციულად უნდა გავზარდოთ სირთულე, სასტარტო ნულების რაოდენობაზე მოთხოვნის ზრდით.

როდესაც 2009 წლის დასაწყისში ნაკამოტომ თავისი ბიტკოინების ქსელი გაუშვა, მასში, შემქმნელის გარდა, სხვა წევრი არ იყო. ამიტომ პირველი ბლოკების „მაინირება“ თვითონ ნაკამოტომ გააკეთა. როდესაც ბიტკოინ-ქსელში გაჩნდა სხვა კვანძები, ქსელის სირთულე თანდათანობით გაიზარდა. ქსელის სირთულის მართვაში ამგვარი ლოგიკა იქნა ჩადებული: ქსელის სირთულე ისეთი უნდა იყოს, რომ იმ კვანძების რაოდენობის, რომლებიც ბლოკებს ეძებს, და ასევე, მათი გამომთვლელი სიმძლავრისაგან დამოუკიდებლად ახალი ბლოკის პოვნა საშუალოდ შესაძლებელი იყოს არანაკლებ და არა უმეტეს ათ წუთში. სირთულე ხელახლა ითვლებოდა ყოველი 2016 ბლოკის შემდეგ ანუ დაახლოებით ორ კვირაში ერთხელ. საერთოდ, ყველა 2016 ბლოკის პოვნაზე რეალურად დახარჯული დრო იყოფოდა მათ რაოდენობაზე და მიღებულ შედეგს ადარებდნენ ათწუთიან ეტალონს. თუ ბლოკები საშუალოდ, უფრო სწრაფად იძებნებოდა, სირთულეს ზრდიდნენ, ანუ იზრდებოდა მოთხოვნები ბლოკის სათაურის ჰეშში ნულების რაოდენობაზე. თუ უფრო ნელა, მაშინ მოთხოვნებიც მცირდებოდა.

ახლა მცირედი გადახვევა გავაკეთოთ, რათა გავერკვეთ, როგორ გადაირჩევა ჰეშები მაინინგის პროცესში. რადგან ჰეშირდება ბლოკის სათაური, ეს ნიშნავს, რომ ჰეშირებადი ინფორმაცია საკმაოდ სტატიკურია, რაც, თავის მხრივ, მეტყველებს იმაზე, რომ უცვლელი წინასახისას ყოველთვის ერთსა და იმავე ჰეშს მივიღებთ. ეს წინააღმდეგობაში მოდის ჩვენს მიზანთან, ვიპოვოთ „ოქროს“ ჰეში, რათა ის

იწყებოდეს დიდი რაოდენობის ნულებით. მოდი, კიდევ ერთხელ შევხედოთ ბლოკის სათაურის სტრუქტურას, რათა გავიგოთ: არის თუ არა იქ რომელიმე დინამიკური სიდიდე, რომელიც იმდენად სწრაფად შეიცვლება, რომ მაინერს საშუალება ჰქონდეს, წამში დააჰეშიროს მილიონობით, მილიარდობით და ტრილიონობით წინასახეც კი?

ბლოკის რიგითი ნომერი უაღრესად სტატიკური ინფორმაციაა, რომელიც არ შეიცვლება. ბლოკის ვერსიის ნომერიც ფიქსირებული სიდიდეა. ახლა რაც შეეხება ბლოკის შექმნის დროს, რომელიც გამოიხატება 1970 წლის 1-ლი იანვრიდან გასული წამებით. ლოგიკური იქნებოდა გვევარაუდა, რომ ის შეიცვლება არა უფრო ხშირად, ვიდრე წამში ერთხელ, რაც ჩვენი ამოცანისათვის უკიდურესად დაბალი დინამიკაა. ბლოკში ტრანზაქციების რაოდენობა და მისგან გამოთვლილი მერკლის ხის ფუძის მნიშვნელობა შედარებით მუდმივი სიდიდეა. მაგრამ არსებობს შემთხვევები, როცა ვალიდური ჰეშის ძიებისას მაინერთან მოდის ახალი ტრანზაქციები უფრო მაღალი საკომისიოთი, ვიდრე მან ადრე ჩართო ბლოკში, მაშინ აზრი აქვს ბლოკის ხელახალ აწყობას. ოღონდ ამ პროცედურასაც აქვს საკმაოდ დაბალი დინამიკა და ჰეშების აუცილებელი მრავალფეროვნების პრობლემას არ წყვეტს.

გამოდის, რომ ვინაიდან ბლოკის სათაურში მაღალდინამიკური ინფორმაცია ბუნებრივად არ არსებობს, ამოცანის გადასაჭრელად აუცილებელია, მაინინგის პროცედურაში შევიტანოთ რაღაც ხელოვნური ელემენტი. მას არ ექნება არავითარი სასარგებლო დატვირთვა, გარდა იმისა, რომ ითამაშებს ბლოკის სათაურის დამატებითი შემადგენლის როლს, როგორც ჰეშირების წინასახე. ასეთი ელემენტი მართლაც არსებობს ყოველი ბლოკის სათაურში და ეწოდება „ნონსი“ (nonce). მაინერი გადარჩევისას სწორედ ნონსის მნიშვნელობას შეცვლის განსაკუთრებულად სწრაფად, რითაც შექმნის შესაძლებლობას სხვადასხვა ჰეშის უზარმაზარი რაოდენობის მიღებისა, რომელთა შორის შეიძლება აღმოჩნდეს სანუკვარი „ოქროს“ ჰეში საჭირო როდენობის ნულებით.

არსებითად, მაინინგის პროცედურა დაიყვანება ამ ნონსის შესაბამისი მნიშვნელობის პოვნამდე, რომელიც, ბლოკის სათაურს რომ დაემატება, საშუალებას მისცემს მაინერს, გამოთვალოს ვალიდური ჰეში, რომელიც მთელი ქსელის მიერ უპირობოდ იქნება მისაღები და ახალი ბლოკის შექმნის უფლებას მისცემს. მაგრამ ნონსის აუცილებელი მნიშვნელობის საძიებელი პროცედურა საკმაოდ რთულია.

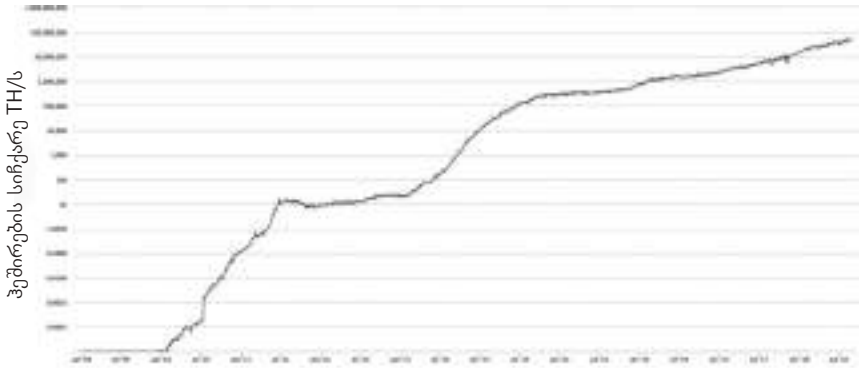
ბიტკოინ-ქსელში გამოიყენება ჰეშირების ალგორითმი SHA-256, რომელიც გულისხმობს ორ ციკლს, თითოეულს ჰეშირების 64 იტერაციით. 2019 წლის გაზაფხულის მდგომარეობით, ბიტკოინ-ქსელის სირთულე ვალიდური ჰეშის მოსაძებნად მოითხოვს 18 პირველი ნულოვანი სიმბოლოს არსებობას, რომელიც შეესაბამება 72 ნულოვან ბიტურ მნიშვნელობას. ეს მოითხოვს დაახლოებით ჰეშების 2^{72} ან $5{\cdot}10^{21}$ გადარჩევას. ბევრია ეს თუ ცოტა? მოდი, შევადაროთ ეს რიცხვი, ვთქვათ, ქვიშის მარცვლების რაოდენობას ჩვენი პლანეტის ყველა პლაჟზე. მეცნიერები ამ რაოდენობას დაახლოებით 10^{18} აფასებენ. ამგვარად, ასეთი მოთხოვნების მქონე ჩვენთვის საჭირო ვალიდური ჰეშის მოძებნის სირთულე ედარება დაახლოებით 5000 დედამიწის მსგავს პლანეტაზე არსებული ქვიშის ყველა მარცვლის გადარჩევის პროცედურას. აი, ასეთი ვალიდური ჰეშის მაგალითი, რომელიც 18 საწყისი ნულის სირთულეს მოითხოვს:

000000000000000000001621af297d27d54b501f6a3d329399c29cf316932973ef

როგორც აღვნიშნეთ, ბიტკოინ-ქსელის პირველ ბლოკებს სატოში ნაკამოტო დამოუკიდებლად პოულობდა და ამისათვის იყენებდა ჩვეულებრივ კომპიუტერს. ისევე, როგორც ქსელის სხვა წევრები, რომლებიც თანდათანობით ჩნდებოდნენ. სწორედ სირთულის იმ საწყის დონეზე კომპიუტერის ჩვეულებრივი პროცესორი სავსებით საკმარისი იყო, რათა ეპოვა ბლოკი საშუალოდ დაწესებულ ათ წუთში. მაგრამ ქსელის წევრთა რაოდენობის ზრდასთან ერთად, სირთულეც იზრდებოდა და რაღაც მომენტში კომპიუტერის ჩვეულებრივი პროცესორისათვის გამოსათვლელი ამოცანა „შეუსრულებადი“ გახდა. მიუხედავად ამისა, მაინერებმა სწრაფად იპოვეს გამოსავალი – მათ ბლოკების საძიებლად გამოიყენეს არა ცენტრალური პროცესორი, არამედ ის, რომელიც დაყენებული იყო მათ ვიდეობარათებზე. თავისი გამომთვლელი არქიტექტურის სპეციფიკის ძალით, გრაფიკული პროცესორი ბევრად უფრო სწრაფად ითვლიდა ჰეშებს, ვიდრე ცენტრალური. მაგრამ გარკვეული დროის გასვლის შემდეგ სირთულე ისე გაიზარდა, რომ გრაფიკულმა პროცესორმაც ვეღარ შეძლო ბლოკების მაინინგის განხორციელება. და მაინც, გამოსავალი საკმაოდ სწრაფად მოიძებნა: 2012 წლის ივნისში კომპანიამ Butterfly Labs დაიწყო სპეციალური პროგრამულ-აპარატული უზრუნველყოფის

მოწოდება სახელწოდებით ASIC (Application-Specific Integrated Circuit ანუ „სპეციალური დანიშნულების ინტეგრალური სქემა“). ფაქტობრივად, ეს იყო პატარა სპეციალიზებული კომპიუტერი, სრულად ოპტიმიზებული მხოლოდ ერთი ამოცანისთვის – გადაერჩია ჰეშები SHA-256 ალგორითმით და ეს განსაკუთრებით სწრაფად გაეკეთებინა. დაიწყო ერა ბიტკოინის თავიდან კერძო, ხოლო შემდგომ – სამრეწველო მაინინგისა, ერთმანეთში აქტიური კონკურენციის მქონე, სხვადასხვა კომპანიის მიერ წარმოებული, ყველაზე თანამედროვე აპარატული საშუალებების გამოყენებით.

იმისათვის, რომ გავიგოთ, რამდენად გაიზარდა ქსელის სირთულე პირველი ათი წლის განმავლობაში, განვიხილოთ ჰეშების გადარჩევის სიჩქარის ცნება ანუ – „ჰეშრეიტი“ (hashrate). ასხვავებენ როგორც ცალკეული მოწყობილობის, ასევე მთელი ქსელის ერთობლივ ჰეშრეიტს. აშკარაა, რომ რაც უფრო მაღალია ბიტკოინ-ქსელის მთლიანი ჰეშრეიტი, მით უფრო რთულია ბლოკის შესაქმნელი ვალიდური ჰეშის პოვნა. სხვა შემთხვევაში, მაინერები ბლოკებს ძალზე სწრაფად იპოვიდნენ, რაც ბლოკჩეინ-სისტემაში ჩადებულ ლოგიკას ეწინააღმდეგება. აი, როგორ იცვლებოდა ჰეშრეიტი ბიტკოინ-ქსელის არსებობის ათი წლის მანძილზე (ლოგარითმული გრაფიკის მაგალითზე):



პირველი ASIC მოწყობილობები მუშაობდა 4,5 გიგაჰეშ წამში ჰეშრეიტით ანუ რომ გამოეყენებინათ ბიტკოინ-ქსელის მუშაობის დასაწყისშივე მინიმალურ სირთულეზე, ისინი იპოვიდნენ ვალიდურ ჰეშს დაახლოებით ერთ წამში. ეს სიჩქარე 600-ჯერ მეტი იყო, ვიდრე თვით სატოში ნაკამოტო ითვლიდა პირველ ბლოკებს თავისი კომპიუტერის პროცესორის საშუალებით. 2019 წლის გაზაფხულის დროინდელი ASIC მოწყობილობები, რომლებსაც აწარმოებს კომპანია Bitmain, ახორციელებს ჰეშების გადარჩევას წამში 53 ტერაჰეშამდე. ეს 10 000-ჯერ და მეტჯერ სწრაფია პირველ მოწყობილობებთან შედარებით, რომლებიც თითქმის შვიდი წლით ადრე იყო წარმოდგენილი. თუმცა, ბიტკოინ-ქსელის ერთობლივი ჰეშრეიტი პიკურ მაჩვენებლებზე აღწევდა სრულიად კოსმოსურ მნიშვნელობებს – დაახლოებით 60 ექსაჰეშს წამში, რაც მთელი ქსელისათვის შეადგენს გადარჩევის სიჩქარეს 6×10^{19} ჰეშს წამში. მიუხედავად ამისა, ვალიდური ჰეშის ძიების ამოცანის სირთულე ისეთია, რომ მთელი ქსელის ასეთი უზარმაზარი ერთობლივი გამოთვლითი სიმძლავრეც კი ახერხებს ერთი ბლოკის მაინირებას საშუალოდ, იმავე 10 წუთში. რას მიუთითებს ეს?

იმას, რომ პრაქტიკულად არც ერთ კონკრეტულ ინდივიდუუმს, თუნდაც ფლობდეს უახლესი მაღალსიჩქარიანი ASIC მოწყობილობების მნიშვნელოვან, ასობით ან თუნდაც ათასობით რაოდენობას, არ შეუძლია თავის მაინინგურ ფერმაში დამოუკიდებლად განახორციელოს ბიტკოინ-ქსელის თუნდაც ერთი ბლოკის მაინინგი. თუ, რა თქმა უნდა, არ დავუშვებთ რაღაც განსაკუთრებულ იღბლიანობას, რომელიც მუდმივად მაინც ვერ მოხდება. ამიტომ მაინერები ერთიანდე-

ბიან უზარმაზარ გამომთვლელ პულებში და ამგვარად ინაწილებენ როგორც ამოცანის სირთულეს, ასევე, მისი გადაჭრისთვის ანაზღაურების პროპორციულად მისაღებად, პულის წევრთა შორის, ყოველი მათგანის მიერ შეტანილი გამომთვლელი სიმძლავრის წვლილის მიხედვით. პირველი ასეთი პული გაიხსნა 2010 წლის 18 სექტემბერს, ჯერ კიდევ ASIC მოწყობილობის გამოჩენამდე, როდესაც მაინინგს პროცესორებითა და ვიდეობარათებით ახორციელებდნენ. შემდგომში ასეთი პულების რაოდენობა გაიზარდა და მათ მთელი მსოფლიოს მაინერების გაერთიანებებში კონსოლიდირება დაიწყეს.

გამომთვლელ პულებში გაერთიანებული მაინინგური ფერმების განხილვისას, ნელ-ნელა ვუახლოვდებით მაინინგის ძირითად პრობლემას Proof-of-Work-ის კონსენსუსის საფუძველზე ანუ – განსაკუთრებულად დიდი რაოდენობის ელექტროენერგიის გამოყენებას მაინინგური მოწყობილობის მუშაობისას. თანამედროვე მაღალსიჩქარიანი Bitmain S17 Pro ტიპის ASIC იყენებს 2250 ვატ სიმძლავრეს, რაც მნიშვნელოვან სიდიდეს შეადგენს, განსაკუთრებით თუ გავითვალისწინებთ, რომ ასეთი მოწყობილობებით აკომპლექტებენ მთელ მაინინგურ ფერმებს. ამასთან, ეს მოწყობილობები მუშაობისას ძალზე ხურდება და საჭიროა მათი მუდმივი გაგრილება, რაზეც ასევე იხარჯება ელექტროენერგია. თავისი მაინინგური ფერმის შექმნისას მეწარმე პირველ რიგში სწევს ხარჯებს მაინინგური მოწყობილობის საყიდლად და ადგილზე მისატანად, ასევე, იმ სპეციალური ნაგებობის დასაქირავებლად და აღსაჭურვად, რომელშიც ფერმა იმუშავებს.

მაგრამ „ფერმერისათვის“ ძირითადი ხარჯი მაინც იქნება მაინინგისათვის საჭირო ელექტროენერგიის გადასახადი. სწორედ ამის საფასური წარმოადგენს ყველაზე კრიტიკულ პარამეტრს სხვადასხვა კრიპტოვალუტის, პირველ რიგში ბიტკოინის, მაინინგზე მუშაობის შემოსავლიანობის გამოთვლისას. მთელი ბიტკოინ-ქსელის მიერ ელექტროენერგიის ერთობლივი წლიური მოხმარება შედარებადია იმ მსხვილი სახელმწიფოს მიერ მოხმარებულ ელექტროენერგიასთან, რომელიც ამ პარამეტრის მიხედვით პირველი 30 ქვეყნის სიაში შედის. საუბარია 30-35 ტერავატ-საათზე წელიწადში, რაც შეადგენს მთელ მსოფლიოში ჯამურად მოხმარებული ელექტროენერგიის დაახლოებით 0,5-0,6%-ს. ანალიტიკოსები პროგნოზირებენ, რომ თუ ბიტკოინ-ქსელის მიერ ელექტროენერგიის მოხმარების ზრდის დინამიკა მიმდინარე

დონეზე დარჩება, მაშინ სამი-ოთხი წლის შემდეგ ბიტკოინ-მაინერები მთელ მსოფლიოში გამომუშავებული მთლიანი ელექტროენერგიის მოხმარებას დაიწყებენ. გასაგებია, რომ მსგავს სცენარს თითქმის არ აქვს განვითარების შანსი: სახელმწიფო რეგულატორები მაინერებს ამის განხორციელების უფლებას უბრალოდ არ მისცემენ.

ზემოთ ჩამოყალიბებული ფაქტორების გათვალისწინებით, უნდა ვაღიაროთ, რომ მაინინგის მომავალი Proof-of-Work კონსენსუსის ბაზაზე საკმაოდ ბუნდოვანია. მოსალოდნელია, რომ მრავალი ქვეყნის მთავრობები დაიწყებენ მაინერების შეზღუდვას ელექტროენერგიის მოხმარების თვალსაზრისით, მაგალითად – ნორმატიული კვოტების დამყარებით, რომელთა ყიდვაც სპეციალურ აუქციონებზე მოუწევთ. არც ის არის გამორიცხული, რომ ელექტროენერგიის განსაკუთრებული დეფიციტის მქონე ზოგიერთ ქვეყანაში მაინინგი კანონით საერთოდ აიკრძალოს. განსაკუთრებით პრობლემატური ჩანს ის, რომ მთელი მოხმარებული ელექტროენერგია მიდის მათემატიკური ამოცანის ამოხსნაზე, რომლის ფასეულობაც ყოველ ათ წუთში საერთოდ ქრება. სხვაგვარად რომ ვთქვათ, როგორც კი ახალი ბლოკი შეიქმნება, ამოცანის ამოხსნა ახლიდან ხდება. აშკარაა, რომ ეს არის ისეთი ღირებული რესურსის განსაკუთრებულად არაეფექტიანი გამოყენება, როგორიცაა ელექტროენერგია, – ის ფაქტობრივად, ტყუილად იხარჯება და ადამიანთა მოდგმისთვის (გარდა ენერგეტიკული კომპანიების მფლობელებისა და თანამშრომლებისა) მნიშვნელოვანი სარგებელი არ მოაქვს.

ბევრად უფრო გონივრული იქნებოდა, ასეთი დიდი გამომთვლელი სიმძლავრე მართლაც საჭირბოროტო ამოცანების გადასაჭრელად გამოგვეყენებინა, მაგალითად, ახალი სამედიცინო პრეპარატების ძიებასთან დაკავშირებული გათვლებისათვის ანდა სხვა სამეცნიერო პრობლემების გადასაჭრელად, რომლებიც სერიოზულ გაანგარიშებებს მოითხოვს. შესაძლოა კრიპტოვალუტების მაინინგი მომავალში ევოლუციონირდეს მსოფლიო საზოგადოებისათვის უფრო ეფექტიან ფორმად, როდესაც ბლოკების საძიებელი მუშაობა სასარგებლო სამეცნიერო ამოცანების გადაჭრაზე იქნება მიმართული. ასეთი პროექტები უკვე არსებობს, თუმცა პოპულარობა ჯერჯერობით არ მოუპოვებია. წინააღმდეგ შემთხვევაში, ბლოკების შექმნისას კონსენსუსის მისაღწევად კრიპტოსაზოგადოებას მოუწევს ბევრად ნაკლები ენერ-

გოტევადობის ფორმებზე გადასვლა, ვიდრე Proof-of-Work-ია. ასეთი პროტოკოლები ასევე აქტიურად მუშავდება და მოწმდება, რათა შედეგად, ახალი ბლოკების შესაქმნელ ტექნოლოგიურ პროცესში დომინანტი პოზიციის დაკავება შეძლონ.

ბიტკოინ-ქსელში მაინინგის პრობლემასთან მიბრუნებისას მივდივართ დასკვნამდე, რომ ეს საკმაოდ ძვირად ღირებული პროცედურაა მათთვის, ვინც მასში თავისი მატერიალური აქტივების დაბანდებას ახდენს. ამდენად, მათთვის უნდა არსებობდეს პირდაპირი მონეტარული მოტივაცია, რათა ამის კეთება მომავალშიც შეძლონ. როგორც ადრე ვახსენეთ, ბლოკის შექმნისას მაინერები თავის სასარგებლოდ რიცხავენ მთელ საკომისიოს იმ ტრანზაქციებისაგან, რომლებიც თავიანთი შექმნილი ბლოკის სხეულში მოათავსეს. თუმცა, ამ საკომისიოების ერთობლივი ოდენობა არც ისე დიდია, რომ გაამართლოს იმათი დანახარჯები, ვინც მაინინგის ძვირადღირებულ ინფრასტრუქტურებს ინახავს. აქამდე ასევე არ გაგვიმახვილებია ყურადღება საკმაოდ მნიშვნელოვან ასპექტზე: იმისათვის, რომ ბიტკოინ-ქსელში ფულადი ტრანზაქციების განხორციელება დავიწყოთ, ეს თანხები ქსელში საიდანღაც უნდა გაჩნდეს. ამიტომ მთავარი ანაზღაურება მათთვის, ვისაც ბლოკის შექმნის განხორციელება ხვდა წილად, არის ე.წ. „მაინინგური ანაზღაურება“. საუბარია ბიტკოინის ციფრულად გამოხატულ თანხაზე, რომელსაც მაინერი ყოველი ახალი ბლოკის შექმნისას იღებს. ახლა უკვე მჭიდროდ მივუახლოვდით ცნება „კრიპტოვალუტას“ ბიტკოინ-ქსელის ციფრული მონეტების მაგალითზე. ეს რა მონეტებია, როგორ და რა რაოდენობით ჩნდება ისინი ბიტკოინ-ქსელში და როგორი შეიძლება იყოს მათი მატერიალური ფასეულობა?

ბიტკოინი როგორც კრიპტოვალუტა

თითქოს რა უნდა იყოს იმაზე ადვილი, ვიდრე ელექტრონული ფულის ემისიის პროცესი? ამისათვის უნდა გაიხარჯოს რესურსები, რომლებიც ლითონის მონეტების ჭედვის ან ქაღალდის ბანკნოტების ბეჭდვის პროცესში გამოყენებულის მსგავსია. თუ ელექტრონული ფულის მიმოქცევის სისტემა უკვე შექმნილია და წარმატებით ფუნქციონირებს, მაშინ ახალი ციფრული მონეტების გამოშვების ამოცანა დაიყვანება სასურველი საემისიო თანხის შეტანამდე სისტემის საწყობებში ამის გამაკონტროლებელი სუბიექტის მიერ. თუმცა, ფულადი ემისიების ასეთი ცენტრალიზებული მართვისას არ არსებობს გარანტია, რომ სისტემის მფლობელებს არ გაიტაცებს არაუზრუნველყოფილი ელექტრონული ფულის გადაჭარბებული „ბეჭდვა“, რადგანაც ეს აუცილებლად გამოიწვევს არაკონტროლირებად ჰიპერინფლაციას და ამასთან ერთად, მათ მიერ რაღაც ფასეულობის როგორც გადახდის საშუალებისა და იმავდროულად სისტემის მომხმარებლის ნდობის დაკარგვას.

ბიტკოინ-სისტემის შექმნისას სატოში ნაკამოტო ალბათ აცნობიერებდა, რომ შეიძლება ჭარბი ელექტრონული ფულის პრობლემა წარმოქმნილიყო და წინასწარ იზრუნა თავისი სისტემის მდგრადობაზე ამგვარი პრობლემებისადმი. პირველ რიგში, მან შეიმუშავა მაინინგის მექანიზმი, რთულად გამოსათვლელი ამოცანის სახით, რომელიც იხსნება დეცენტრალიზებულად, კონკურენტულ საფუძველზე. იმისათვის, რომ მაინერებს მივცეთ მნიშვნელოვანი მონეტარული მოტივაცია, გადაწყდა, რომ ყოველი ახალშექმნილი ბლოკი სისტემაში შეიტანს დამატებით, მცირე ფულადი ემისიის ულუფას. ციფრული მონეტის ღირებულების ზრდასთან ერთად, ამ ემისიის სიდიდე დროთა განმავლობაში უნდა შემცირდეს. ეს პროცესი იქნება მანამ, სანამ სისტემის მიერ გამოშვებული მონეტების ერთობლივი რაოდენობა საბოლოო, სისტემის პროექტირებისას წინასწარ ჩადებულ მნიშვნელობას მიაღწევს.

ნაკამოტომ საწყის პირობად დაადგინა, რომ სისტემის გაშვების მომენტში ბლოკის შექმნისათვის ანაზღაურება 50 ბიტკოინი იქნება, ხოლო შემდეგ, ყოველ ოთხ წელიწადში, შემცირდება ორჯერ მანამ, სანამ სისტემაში ბიტკოინების საერთო რაოდენობა 21 მილიონ მო-

ნეტას მიაღწევს. გათვლების თანახმად, უკანასკნელი ბიტკოინი სისტემაში შეიქმნება დაახლოებით 2140 წლისათვის, თუმცა, უკვე 2036 წელს იარსებებს მონეტების 99%. მას შემდეგ, რაც ყველა მონეტა იქნება გამოშვებული და ბლოკის შექმნისათვის ანაზღაურება ნულს გაუტოლდება, მაინერებს მოუწევთ მხოლოდ ტრანზაქციების საკომისიოთი დაკმაყოფილება, რომელსაც ჩაირიცხავენ ბლოკების შექმნისათვის. ვარაუდობენ, რომ მაინინგური ანაზღაურების არარსებობაც კი არანაირად არ აისახება მაინერების მოტივაციაზე, რადგან მათ მიერ აღებული სატრანზაქციო საკომისიო გადაჭარბებითაც კი აანაზღაურებს მათ მიერ მაინინგის პროცედურებზე გაწეულ ხარჯებს.

უკვე 2018 წლის შუა პერიოდში მაინინგური ანაზღაურება ორჯერ შემცირდა ნაკამოტოს მიერ დადგენილ საწყისთან შედარებით: ჯერ 2012 წელს – 25 ბიტკოინამდე, ხოლო შემდეგ, 2016-ში – 12,5 მონეტამდე. ანაზღაურების მორიგ შემცირებას 2020 წლის მაისში ელიან და მისი სიდიდე 6,25 ბიტკოინი იქნება. ამასთან, ერთობლივი სატრანზაქციო საკომისიო შეიძლება ავიდეს ერთ ბიტკოინამდე ან უფრო მაღლაც. მაგრამ ეს ხდება მხოლოდ ქსელის გაზრდილი დატვირთვისას, როდესაც ტრანზაქციების რაოდენობა ძალზე დიდია და საკომისო მათი ბლოკში ჩართვისათვის იზრდება. ჩვეულებრივ დროს, სერიოზული დატვირთვების არარსებობისას, ბლოკებში ყველა ტრანზაქციის ერთობლივი საკომისიო ბევრად მცირე თანხას შეადგენს.

ბიტკოინების საბოლოო ემისიის მაქსიმალური შესაძლო მოცულობის 21 მილიონი მონეტით შემოფარგვლით, ნაკამოტოს მიზანი, პირველ რიგში, ინფლაციისაგან დაცვა იყო. პროექტის შემქმნელს იმედი ჰქონდა, რომ ბიტკოინის ღირებულება მომავალში მხოლოდ გაიზრდება და შეიძლება საბოლოოდ საკმაოდ სერიოზულ ნიშნულს მიაღწიოს. ამიტომ განსაზღვრული იქნა, რომ ყოველი ბიტკოინი შეიძლება დაიყოს 100 მილიონ ნაწილად ანუ, სხვაგვარად რომ ვთქვათ, ჰქონდეს რვა ნიშანი მძიმის შემდეგ. ბიტკოინის ყველაზე მცირე ნაწილაკს 0,00000001 ბიტკოინს შემდგომში უწოდეს „სატოში“, ბიტკოინ-სისტემის შემქმნელის პატივსაცემად. აშკარაა, რომ თუ ემისიის ზღვარი მკაცრად განსაზღვრულია, მაშინ სისტემას ინფლაციის მაგივრად საქმე ექნება მის სრულიად საწინააღმდეგო მოვლენასთან – დეფლაციასთან, როდესაც ბიტკოინში ნომინირებული ყველა საქონელი და მომსახურება დროთა განმავლობაში შემცირდება თავი-

სი ღირებულების აბსოლუტურ მნიშვნელობებში. მაგრამ მაშინაც კი, თუ ერთი სატოშის ღირებულება ერთი ამერიკული ცენტის ღირებულებას გაუტოლდება, ბიტკოინის ყველა მონეტის საერთო ღირებულება შეადგენს დაახლოებით 21 ტრილიონს, რაც ამ კრიპტოვალუტას საშუალებას მისცემს გახდეს მასობრივი საგადამხდელო საშუალება მთელი მსოფლიოს მასშტაბით.

ფულის ტრადიციულ ფორმებთან შედარებით, ბიტკოინ-ფული სერიოზულად არის დაცული არასანქცირებული გამოშვებისაგან – ამ პროცესის სადარაჯოზე დგას კრიპტომედეგი მატემატიკური ალგორითმები. მაგრამ ბიტკოინ-სისტემასაც კი აქვს ერთი სისუსტე, რომლის გამოყენებაც თეორიულადაც კი ძალზე ძნელია. ამ სისუსტეს უწოდებენ „51%-იან შეტევას“ და მისი არსი იმაშია, რომ ქსელში შეიძლება გაჩნდეს განსაკუთრებული გამომთვლელი სიმძლავრის მქონე კვანძი (ან კვანძების ჯგუფი), რომელიც ქსელის ერთობლივი ჰეშრეიტის 50%-ს შეადგენს. სხვა სიტყვებით რომ ვთქვათ, ეს კვანძები უფრო სწრაფად ახდენს ახალი ბლოკების მაინინგს, ვიდრე დანარჩენი ქსელი. ბიტკოინ-ქსელში არსებობს წესი: იმ შემთხვევაში, თუ სისტემაში წარმოიშობა განშტოებები ბლოკების ჯაჭვში, ქსელი უფრო გრძელ განშტოებას იღებს ჭეშმარიტად. ამგვარად, უფრო მოკლე განშტოება მასში ჩართული ყველა ბლოკით, ქსელის მიერ უბრალოდ არ მიიღება და უქმდება. ავტომატურად უქმდება ის ტრანზაქციები, რომლებიც ჩართული იყო ქსელის მიერ არმიღებული განშტოებების ბლოკებში.

მოვლენების განვითარების ამგვარი სცენარი გულისხმობს, რომ ტრანზაქციის ერთ-ერთ ბლოკში ჩასმის მხოლოდ ფაქტი აშკარად არასაკმარისია. წესების მიხედვით, საჭიროა გარკვეული დრო, რათა დავრწმუნდეთ, რომ ტრანზაქცია არ მოხვდა ბლოკების განშტოებაში, რომელიც, შესაძლოა, უგულებელყოფილი იქნას რომელიღაც უფრო გრძელი ალტერნატიული ჯაჭვის სასარგებლოდ. ჩვეულებრივ თვლიან, რომ ნებისმიერი პარალელური განშტოება არ შეიძლება ექვს ბლოკზე გრძელი იყოს, ანუ ასეთი სიტუაციის წარმოქმნის ალბათობა განსაკუთრებით მცირეა. ამიტომ იგულისხმება, რომ ბიტკოინ-ქსელში ნებისმიერი ტრანზაქციის ექვსი დადასტურება საკმარისია, რომ ის ჩაითვალოს საბოლოოდ შემდგარად. ანუ იმ ბლოკის შემდეგ, რომელშიც მოთავსებული იქნა ტრანზაქცია, ჯაჭვში ჩაერთო კიდევ ზედიზედ ხუთი ბლოკი, – სწორედ ეს არის ის ექვსი დადასტურება, რომლებიც აუცილებელია ტრანზაქციის შესრულების აღიარებისა-

თვის (ერთი ბლოკი ნიშნავს ერთ დადასტურებას). სხვა სიტყვებით რომ ვთქვათ, ტრანზაქციის სრული დადასტურებისათვის აუცილებელი დრო დაახლოებით ტოლია ექვსი ათწუთიანი მონაკვეთისა ანუ ერთი საათისა. დავუბრუნდეთ „51%-იანი შეტევის“ პრობლემას. წარმოვიდგინოთ, რომ რომელიღაც კვანძმა გამოთვლითი თვალსაზრისით პრევალირება დაიწყო ქსელში და სწორედ მისი ბლოკები დალაგდა იმ ჯაჭვად, რომლის ჭეშმარიტებასაც იძულებით ცნობს დანარჩენი ქსელი. რითია ეს ცუდი მთლიანად ქსელისათვის?

პირველ რიგში, ერთი კვანძის ან საერთო მიზნით გაერთიანებული კვანძების ჯგუფის დომინირებამ შეიძლება გამოიწვიოს ის, რომ ბოროტმოქმედთა ამ კონსორციუმმა კონტროლის ქვეშ აიყვანოს ბლოკების ყველა მაინინგი და შედეგად, ქსელის ყველა ტრანზაქცია. გარდა იმისა, რომ ისინი მაინინგისათვის ანაზღაურების ფაქტობრივ მონოპოლიზაციას მოახდენენ, მათ ბლოკებში შეუძლიათ ჩართონ მხოლოდ მათთვის სასურველი ტრანზაქციები. თან, პირველ რიგში ჩაერთვება ტრანზაქციები, რომლებიც უშვებს ერთი და იმავე მონეტების მეორეჯერ გამოყენებას, ანუ ახორციელებს „ორმაგ ხარჯვას“. ერთადერთი, რასაც ისინი ვერ შეძლებენ, არის ადრე შექმნილი ბლოკების მონაცემებში ჩარევა, ამისათვის გამომთვლელი სიმძლავრეების 51%-იც კი არ იქნება საკმარისი. საქმე ისაა, რომ ამ შემთხვევაში აუცილებელი გახდება ბლოკების ყველა ჰეშის გადათვლა, დაწყებული ცვალებადით და დამთავრებული ჯაჭვში უკანასკნელით შეტანილი მოდიფიკაციების გათვალისწინებით. შედეგად საპოვნი იქნება ახალი ნონსები ყველა ახლიდან აწყობილი ბლოკისათვის და ქსელისათვის საჭირო იქნება საკმაოდ რიგიანი სიღრმის ჯაჭვის შეთავაზება. ამავდროულად, მთელი დანარჩენი ქსელი გააგრძელებს ბლოკების გადათვლასა და შექმნას, ადრე მთელი ქსელისაგან მიღებული, საბოლოოდან დაწყებული (ანუ ბევრად უფრო გვიანი ბლოკიდან, ვიდრე ბოროტმოქმედების მიერაა გათვლილი). რაც შეეხება ორმაგი ხარჯვის საკითხს, ის ნამდვილად შეიძლება გახდეს სერიოზული პრობლემა. შეიძლება ითქვას, რომ სწორედ ამან, თავის დროზე, არ მოგვცა საშუალება შეგვექმნა დეცენტრალიზებული ციფრული ფული „ბლოკჩეინებამდელ პერიოდში“. იმისათვის, რომ გავიგოთ, რატომ მოგვცემს „51%-იანი შეტევა“ ორმაგი ხარჯვის შესაძლებლობას, განვიხილოთ შემდეგი მაგალითი.

დავუშვათ, ქსელში არსებობს დიდი, უფრო მეტი სიმძლავრის მქონე გამომთვლელი კვანძი, ვიდრე ერთად აღებულს, ყველა დანარ-

ჩენ კვანძს აქვს. ეს კვანძი ირჩევს რომელიღაც ბლოკს „ათვლის წერტილის“ სახით და იწყებს მისგან ახალი ბლოკების მაინინგის განხორციელებას ისე, რომ რაღაც დროის განმავლობაში არ ახდენს მათ დემონსტრირებას მთელი დანარჩენი ქსელისათვის. ამავდროულად ის დაიწყებს კრიპტოსახსრების ხარჯვას ძირითად ჯაჭვში, სანამ არ მიიღებს ქსელისაგან ყველა მათგანის ცალსახა დადასტურებას. ამგვარად, ძირითად ჯაჭვში გაჩნდება მინიმუმ ხუთი ბლოკი იმის შემდეგ, რომელშიც განთავსებული იყო ზიანის მომტანი კვანძის ხარჯვის ტრანზაქციები. შემდეგ კვანძი მთელ ქსელს გაუხსნის მისგან შექმნილ ალტერნატიულ ჯაჭვს, უფრო გრძელს, რადგან ამ კვანძის გამომმთვლელი სიმძლავრე ერთობლივად მეტია, ვიდრე ყველა დანარჩენისა, და ქსელი იძულებული იქნება, ჭეშმარიტად აღიაროს ეს განშტოება. ამასთან, მოგვიწევს ძველი ბლოკების, ქსელისაგან ადრე გათვლილისა და დადასტურებულის, გადაყრა, ანუ მათთვის ე.წ. „დაობლებული ბლოკების“ (orphaned blocks) სტატუსის მინიჭება, რომლებმაც კავშირი დაკარგა მთავარ ჯაჭვთან. გასაგებია, რომ მათთან ერთად ავტომატურად გადაგდებული იქნება ზიანის მომტანი კვანძის ყველა ხარჯვითი ტრანზაქცია, თითქოს ისინი არასდროს არსებულა.

ძნელი არ არის იმის მიხვედრა, რომ თვით თაღლითი-კვანძის მიერ ქსელისათვის შეთავაზებული ალტერნატიული ბლოკები მისთვის განკუთვნილ არავითარ ხარჯვით ტრანზაქციას არ შეიცავს. ამგვარად, მიუხედავად იმისა, რომ ბოროტმოქმედმა თავისი სახსრები დახარჯა ადრე, „წინა რეალობაში“, და მიიღო რაღაც საქონელი, მომსახურება ან თუნდაც სხვა კრიპტოვალუტა, გარკვეული დროის შემდეგ ის ყველა თავის აქტივს უკან დაიბრუნებს და ქსელი იძულებული იქნება, ამას დათანხმდეს. თითქოს Proof-of-Work პრინციპით ბლოკების შემქმნელი ნებისმიერი ბლოკჩეინ-სისტემისათვის ეს მომაკვდინებელი პრობლემაა. თუმცა პრაქტიკაში ასეთი სცენარის რეალიზება განსაკუთრებულად რთულია როგორც ორგანიზაციულად, ასევე მონეტარულადაც, ხოლო რიგ შემთხვევებში ამას პრაქტიკული აზრიც კი შეიძლება არ ჰქონდეს. შევეცდებით ავხსნათ, რატომ.

დავიწყოთ იმით, რომ ასეთი შეტევის განხორციელება ადვილია მხოლოდ თეორიულად. წარმოვიდგინოთ, გამომთვლელი სიმძლავრეების რა მოცულობა უნდა გამოვიყენოთ, რომ ხელში ჩავიგდოთ რომელიმე ქსელის ჰეშრეიტების ნახევარზე მეტი, განსაკუთრებით, თუ ეს ბიტკოინ-ქსელია, რომლის ჰეშების გადარჩევის ერთობლივი სიჩქა-

რე ასტრონომიული სიდიდეებით განისაზღვრება. ამგვარი შეტევების ეფექტიანობის შესაფასებლად, ბოროტმოქმედთათვის აუცილებელია „შეტევის ღირებულების“ ცნებით ოპერირება. სერიოზული გამომთვლელი სიმძლავრეების მოზიდვა – ზოგადად მონეტარულად უკიდურესად ძვირია, ხოლო როდესაც საუბარია ისეთ მძლავრ ქსელზე შეტევისათვის საჭირო წესებზე, როგორიც ბიტკოინია, მაშინ აშკარად ვაწყდებით მინიმუმ პრაქტიკულად გადაუჭრელ რამდენიმე პრობლემას.

პირველი, ეს არის ასეთი ოპერაციისათვის საჭირო რაოდენობის კომპიუტერების ან ASIC მოწყობილობების მოზიდვის ფიზიკური შეუძლებლობა, რადგან რეალურად, შეუძლებელია ამ მოცულობით მათი კონსოლიდირება ერთიანი მართვის ქვეშ. ისეთი სახელმწიფოს მთავრობამაც კი, როგორიც აშშ-ია, რომ მოინდომოს აწარმოოს ასეთი შეტევა ბიტკოინ-ქსელზე კონტროლის დამყარების მიზნით, ნაკლებსავარაუდოა, რომ თუნდაც ასეთი დონის სახელმწიფო ინსტიტუტებსაც კი შესწევდეთ ამის ძალა. მეორე ფაქტორი, რომლის მხედველობაში მიღებაც აუცილებელია, არის ამ მოცულობის გამომთვლელი რესურსების მოზიდვის ღირებულება. დიდი ალბათობით, ის მრავალჯერ გადააჭარბებს იმ ეკონომიკურ ეფექტს, რომლისთვისაც ბოროტმოქმედებს შეიძლებოდა თეორიულად მიეღწიათ ამ შეტევით.

დაბოლოს, მიმდევრობით, მაგრამ არა მნიშვნელობით, უკანასკნელი ფაქტორია მთლიანობაში კრიპტოვალუტისადმი ნდობის დაკარგვა მასზე წარმატებით განხორციელებული შეტევის შემდეგ. ეჭვგარეშეა, მასზე საბაზრო ფასი თითქმის ნულამდე დაეცემა, რაც გააკოტრებს სისტემის ყველა წევრს, თვითონ შემტევის ჩათვლით. აშკარაა, რომ ასეთი შეტევებისათვის უფრო მოწყვლადი დაბალი ჰეშრეიტის და, შესაბამისად, მათზე შეტევის დაბალი ღირებულების მქონე „ახალგაზრდა“ ქსელებია. ასეთ შემთხვევებში შეტევის აზრი ორმაგი ხარჯვის რეალიზაციაც კი არ არის, არამედ უფრო – ქსელებისათვის ზიანის მიყენება, მათი დანგრევის ან მინიმუმ, რაღაც დროით შრომისუნარიანობის ბლოკირების მიზნით. კვანძი, რომელმაც ქსელზე კონტროლი განახორციელა, ხომ თავად წყვეტს, რომელი ტრანზაქციები ჩართოს ბლოკში და რომელი – არა. და მას შეუძლია შექმნას, მაგალითად, მხოლოდ ცარიელი ბლოკები ტრანზაქციების გარეშე, რითაც შესატევი ქსელის ფარგლებში კრიპტოვალუტის ნებისმიერი გადარიცხვის პარალიზებას მოახდენს.

ბიტკოინ-ქსელის ისტორიაში იყო შემთხვევა, როდესაც 2014 წლის 13 ივნისს მაინინგურმა პულმა Ghash რამდენიმე საათით მოიპოვა კონტროლი მთელი ქსელის გამომთვლელი სიმძლავრის 51%-ზე. ეს ბუნებრივად მოხდა პულის წევრთა რაოდენობის მნიშვნელოვანი ზრდის გამო. თუმცა მაშინვე, როგორც კი დაფიქსირდა ჰეშრეიტის გადაჭარბება, პულის ბევრმა წევრმა შეაჩერა მაინინგის პროცესი, ხოლო თავად პულმა შეწყვიტა ახალი მომხმარებლების რეგისტრაცია და ჩართვა. ეს განგებ მოხდა, მთლიანობაში ქსელისათვის შესაძლო დესტრუქციული შედეგების თავიდან ასაცილებლად. გარკვეული დროის გასვლის შემდეგ, როდესაც ბიტკოინ-ქსელის ჯამური ჰეშრეიტი მნიშვნელოვნად გაიზარდა, მსგავსი სიტუაციები ვერც ერთი მსგავსი პულისათვის ვერ წარმოიშვებოდა.

ყველა შემთხვევაში, როგორც უკვე აღინიშნა, ქსელზე გამომთვლელი კონტროლის დამყარების მთავარი ნეგატიური შედეგი იქნება მთლიანად ქსელისადმი წევრების ნდობის კატასტროფული დაცემა. შედეგად, დიდი ალბათობით შეგვიძლია ველოდოთ კლასიკურ ფულად ეკვივალენტში, რომელსაც „ფიატურს“ უწოდებენ, გამოსახული ქსელური კრიპტოვალუტის ღირებულების სერიოზულ დაცემას. დასახელება „ფიატური ფული“ ეხება ჩვენთვის ცნობილ მსოფლიო ვალუტებს, რომლებიც ემიტირებულია ეროვნული სახელმწიფოების მთავრობათა ან კონსორციუმთა მიერ, – მაგალითად, ისეთებს, როგორიცაა ევროკავშირი. ფიატური ფულით ჩვენ ყველანი ყოველდღიურად ვსარგებლობთ, ხოლო ამ ტერმინს შემდგომში გამოვიყენებთ როგორც კრიპტოვალუტის გადახდის საშუალების საწინააღმდეგოს.

რადგან რეალური საქონლის ან მომსახურების შეძენა უშუალოდ კრიპტოვალუტით ამჟამად ნაკლებად განვითარებულია, მაინერების უმრავლესობისთვის, გამომუშავებული კრიპტოვალუტის ფიატურ ვალუტაზე გადაცვლის პროცესი ყოველდღიური აუცილებლობაა. ეს კი ნიშნავს, რომ ქსელის ყველა წევრისათის (და პირველ რიგში, ყველაზე აქტიური მაინერებისათვის) კრიპტოვალუტის ფიატურ ფულზე გადაცვლის კურსი ძალზე მნიშვნელოვანი პარამეტრია. გასაგებია, რომ კრიპტოვალუტის ფიატური ეკვივალენტი ასახავს მის ფასეულობას, მაგრამ მაშინ როგორ შეიძლება შევაფასოთ, რაზეა დამოკიდებული საერთოდ კრიპტოვალუტებისა და კერძოდ ბიტკოინის კურსი?

ბიტკოინი როგორც ფასეულობა

ბლოკჩეინის გაშვებიდან ცხრა დღის შემდეგ, სახელდობრ, 2009 წლის 12 იანვარს, სატოში ნაკამოტომ მისი მეშვეობით პირველი ისტორიული ტრანზაქცია განახორციელა. მან ტესტის სახით ათიოდე ბიტკოინი გაუგზავნა ქსელის სხვა წევრს, რომელიც მასში ნაკამოტოს შემდეგ თითქმის მაშინვე გაჩნდა. ის აღმოჩნდა ამერიკელი პროგრამისტი და კრიპტოენთუზიასტი ჰელ ფინი, რომელმაც ჯერ კიდევ 2004 წელს დაწერა Proof-of-Work-ის პირველი ალგორითმი PGP ოქმის პროგრამული უზრუნველყოფისათვის, რომელიც ღია გასაღებით დაშიფვრის ფუნქციონალს უზრუნველყოფდა. ბლოკში ტრანზაქცია 170-ე ნომრით იყო ჩართული და ქსელის ორ მონაწილეს შორის ფიზიკურად განხორციელებული ბლოკჩეინ-ტრანზაქციის ისტორიაში პირველი გახდა. შეეძლო კი სატოში ნაკამოტოს ევარაუდა, რომ ტესტირების მიზნების გულისათვის მან გაასხვისა ციფრული მონეტები, რომელთა საერთო ღირებულება ათ წელზე ნაკლებ დროში იქნებოდა ათეული და ასეული ათასი დოლარიც კი? პირველი ტრანზაქციის განხორციელებისას ბიტკოინს არ გააჩნდა არავითარი მონეტარული ღირებულება. როგორ მოხდა, რომ მალე მასში კრიპტოვალუტის ბაზრებზე სერიოზული ფიატური თანხების გადახდა დაიწყეს?

ამ კითხვაზე პასუხის გასაცემად აუცილებელია გავიგოთ, რისგან შედგება ბიტკოინის ღირებულება. ჩვეულებრივი ფულის ისტორია ყველასათვის კარგადაა ცნობილი: თავიდან ბრუნვაში იყო მხოლოდ ძვირფასი ლითონებისაგან, ოქროსა და ვერცხლისაგან, დამზადებული მონეტები. ამ დროს ღირებულებას ისინი თავად წარმოადგენდა. შემდეგ კაცობრიობა გადავიდა ქაღალდის ბანკნოტებზე, რომლებიც თავიდან გარანტიას იღებდა სახელმწიფო ბანკების ოქროს მარაგით, ხოლო ოქროს სტანდარტის გაუქმების შემდეგ უზრუნველყოფილი იყო მთლიანი შიდა პროდუქტით. უკიდურეს შემთხვევაში, ეს ფაქტი ფორმალურად დეკლარირდება ეროვნული მთავრობების მიერ. სინამდვილეში, სიტუაცია ბევრად უფრო რთულია – ყოველი სახელმწიფოს ეკონომიკა მუდმივად ეჯახება ისეთ მოვლენებს, როგორებიცაა ინფლაცია, უმუშევრობა, საგარეო ვალის მოცულობა, ასევე სხვა

მაკროეკონომიკური პრობლემები. ყოველი მათგანი გავლენას ახდენს ეროვნული ვალუტის ღირებულებაზე და მათ შორის, მისი კურსის მერყეობაზე სხვა ქვეყნების ვალუტების მიმართ.

თავიანთი სახელმწიფოების ავლადიდებით ფორმალურად უზრუნველყოფილი ეროვნული ვალუტები, რამდენადაც ეს ტექნოლოგიურად შესაძლებელია, დაცულია ფალსიფიკაციისაგან. ამისათვის ბანკნოტების დასამზადებლად საჭირო ქაღალდის დამზადების სპეციალური მეთოდები გამოიყენება, სარგებლობენ განსაკუთრებული საბეჭდი საღებავით, ხოლო კუპიურებზე დაცვის სპეციალური ელემენტები დააქვთ – წყლის ნიშნები, რიგითი ნუმერაცია და ჰოლოგრაფიული გამოსახულებები. რა თქმა უნდა, ეს ყველაფერი ყალბი ფულის გამოჩენისაგან ასპროცენტიან გარანტიას არ იძლევა, მაგრამ შემთხვევათა უდიდეს უმრავლესობაში ქაღალდის ბანკნოტებისადმი ადამიანებს ნდობის პრობლემა არ აღეძვრებათ. ადამიანთა ნდობის საფუძველს ფიატური ფულისადმი შემდეგი ფაქტორები განაპირობებს:

- მთავრობის მიერ ქაღალდის ბანკნოტების გადახდის კანონიერ საშუალებად აღიარება;
- ეროვნული ვალუტის მთლიანი შიდა პროდუქტით და ასევე, სახელმწიფოს ოქროსა და უცხოური ვალუტის მარაგით უზრუნველყოფა;
- ფულადი ემისიების შეზღუდვა, შესაძლო ინფლაციაზე კონტროლის მიზნით;
- ბანკნოტების გაყალბებისაგან ფიზიკური დაცვა;
- ნდობა სხვა ადამიანების მხრიდან, რომლებიც მზად არიან მიიღონ ბანკნოტები გადახდისათვის;
- ეროვნული ვალუტის სხვა სახელმწიფოების ვალუტებთან შედარებით სტაბილური კურსი.

ზემოთ ჩამოთვლილი ფაქტორებიდან თუნდაც ერთის არარსებობა, როგორც წესი, მნიშვნელოვნად უკარგავს ნდობას ეროვნულ ვალუტას, ყოველდღიურ სარგებლობაში მის გამოყენებაზე სრული უარის ჩათვლითაც კი. ასეთი სიტუაცია არც ისე დიდი ხნის წინ იყო ზიმბაბვეში, როდესაც განსაკუთრებულმა ჰიპერინფლაციამ ამ ქვეყნის მოქალაქეები აიძულა, მთლიანად აშშ დოლარით ანგარიშგებაზე

გადასულიყვნენ. მსგავსი სურათია ამჟამად ვენესუელაშიც, სადაც ეროვნული ვალუტა ბოლივარი მასშტაბურად გაუფასურდა. ამან გამოიწვია ის, რომ კვების პროდუქტების შესაძენადაც კი ბანკნოტების მთელი მთები გახდა საჭირო, რომლებსაც კარგა ხანია, იმ ქაღალდის ფასიც კი აღარ ჰქონდა, რომელზეც ისინი ოდესღაც დაბეჭდეს.

ახლა კი დავუბრუნდეთ ბიტკოინს და შევეცადოთ მოვარგოთ მას ნდობის იგივე ფაქტორები, რომლებიც ჩამოთვლილი იყო ფიატური ფულისათვის. რადგანაც ბიტკოინი წარმოადგენს დეცენტრალიზებულ ციფრულ ფულს, რომელსაც რომელიმე სახელმწიფოს მიერ კონტროლირებადი ერთიანი ემისიური ცენტრი არ გააჩნია, მისი გადახდის ოფიციალურ საშუალებად ცნობაზე არ ვსაუბრობთ. უფრო სწორად, ეს შეიძლება მოხდეს მომავალში, მაგრამ ყოველმა ცალკეულმა სახელმწიფომ ნებაყოფლობით უნდა გამოხატოს თავისი დამოკიდებულება ამ საკითხისადმი და სავსებით შესაძლებელია მოხდეს ისე, რომ აზრები გაიყოს: რიგი ქვეყნებისა აღიარებს ბიტკოინსა და სხვა კრიპტოვალუტებს გადახდის საშუალებებად, ხოლო სხვანი – არა.

ახლა რაც შეეხება ემისიის შეზღუდულობას. როგორც ვიცით, ბიტკოინის ემისია მოცულობით სასრულია და შემოფარგლულია 21 მილიონი მონეტით. ამგვარად, შესაძლო ინფლაციის საკითხი არ დგება, ამასთან, დაცვის გარანტია იქნება არა რომელიმე სახელმწიფოს დაპირება, გააკონტროლოს ინფლაციური პროცესები, არამედ მკაცრი შესაბამისობა პროექტში ჩადებული მათემატიკური ლოგიკისადმი. იგივე ეხება გაყალბებისაგან დაცვას – ბიტკოინების ემისია წმინდა მათემატიკური პროცესია, რომელიც ეფუძნება ძნელად გამოსათვლელი კრიპტოგრაფიული ამოცანების დეცენტრალიზებულ ამოხსნას, ამიტომ, ჩვეულებრივი ბანკნოტებისაგან განსხვავებით, ამ შემთხვევაში გვაქვს მათემატიკურად დამტკიცებული გარანტია იმისა, რომ „ჭარბი“ ციფრული მონეტები სისტემაში არ გაჩნდება.

ბიტკოინის კრიტიკის ერთ-ერთი მთავარი მიზეზია რაიმე სახის ფასეული უზრუნველყოფის არარსებობა. ამაზე ოდნავ დაწვრილებით შევჩერდეთ. ერთ-ერთ წინა თავში Proof-of-Work-ის ცნების აღწერისას, მაგალითის სახით ვაანალიზებდით, რაზე შეიძლება ყოფილიყო დაფუძნებული ოქროს ფასეულობა. სხვა არგუმენტებს შორის გამოყოფილი იქნა, რომ ოქროს ფლობა არის გეოლოგიური ძიების, მეშახტეთა შრომის, ჩამოსხმით დამუშავების, სატვირთო გადაზიდ-

ვის, მისგან საწარმოო ნაკეთობების დამამზადებელი და ბოლოს, მისი მომხმარებლისათვის მიყიდვის სპეციალისტების გულმოდგინე მუშაობის შედეგი. აშკარაა, რომ ჩვეულებრივ საბაზრო სიტუაციაში ოქროს ნაკეთობის ღირებულება – გინდ ზოდი ან მონეტა იყოს და გინდ იუველირული სამშვენისი – არ შეიძლება ნაკლები იყოს, ვიდრე შრომითი და მისი შექმნისათვის დახარჯული მატერიალური რესურსების ერთობლივი ღირებულება. დავამატოთ მომგებიანობის ჩადებული ნორმა „ფასეულობათა ამ ჯაჭვის“ თითოეული რგოლისათვის და ჯამში მივიღებთ საბოლოო პროდუქტის რაღაც ლოგიკურად დასაბუთებულ ღირებულებას, რომლის დონის ქვემოთაც მის წარმოებას არავითარი კომერციული აზრი არ ექნება.

ახლა ამ სიტუაციის პროეცირება მოვახდინოთ კრიპტოვალუტების, კერძოდ ბიტკოინის, მაინინგის პროცესზე. ამ შემთხვევაშიც დავინახავთ ღირებულებათა წარმოქმნის ჯაჭვს, რომელიც ძალიან ჰგავს ნებისმიერ სხვას, რაიმე პროდუქტის წარმოებისას, ოქროს ჩათვლით. კომპიუტერებისა და მაინინგისათვის საჭირო მოწყობილობების ყიდვა, კრიპტოფერმისათვის საჭირო სათავსების ქირაობა და მოწყობა, ASIC-მაინერების მუშაობისათვის აუცილებელი ელექტროენერგიის გადასახადი, ფერმის მომსახურე IT-სპეციალისტებისათვის ხელფასების გადახდა, საგადასახადო მოსაკრებლები – აი, მეწარმე-მაინერის დანახარჯების არცთუ სრული სია, რაც, თავის მხრივ, ნიშნავს, რომ მაინინგით მიღებულ ყოველ ბიტკოინზე მოდის მონეტარული დანახარჯების გარკვეული თანხა, რომელიც იქნება საბოლოო წარმოებული პროდუქტის – კრიპტოვალუტის მონეტის ღირებულების ქვედა „ზღვრული“ მნიშვნელობა. როდესაც სატოში ნაკამოტო თავის პირველ ბიტკოინებს იღებდა, ქსელის მინიმალური სირთულის გამო დანახარჯები ნულთან ახლოს იყო, როგორც თვით ბიტკოინის ფასეულობა იმ მომენტში. მაგრამ დროთა განმავლობაში მაინინგის პროცესი ძალზე ხარჯიანი ღონისძიება გახდა.

ბევრი ვარაუდობს, რომ ბიტკოინი (ისევე, როგორც ნებისმიერი კრიპტოვალუტა, რომელიც მიღებულია Proof-of-Work-ის კონსენსუსის მიღწევის მექანიზმის საფუძველზე) უზრუნველყოფილია მხოლოდ მის მოპოვებაზე დახარჯული ელექტროენერგიით. შესაძლოა ასეც ითქვას, მაგრამ, როგორც უკვე დავრწმუნდით, ბიტკოინის მაინინგისათვის მხოლოდ ელექტროენერგია არ არის საკმარისი, თუმცა

მასზე დანახარჯები აშკარად აღემატება ყველა დანარჩენს. ცვლადი დანახარჯების სწორედ ეს სახეობა აიძულებს მაინერებს ეცადონ, როგორც თვითონ ამბობენ, „არ დაეშვან როზეტზე დაბლა“, ანუ ბიტკოინის ფასის ფიატური ეკვივალენტი არ უნდა იყოს უფრო დაბალი, ვიდრე მის მიღებაზე დახარჯული ელექტროენერგიის ღირებულება. და იმის გათვალისწინებით, რომ ელექტროენერგიის საბაზრო ღირებულება დროთა განმავლობაში მხოლოდ იზრდება, ისევე, როგორც იზრდება ერთი მონეტის მოსაპოვებლად აუცილებელი ენერგოდანახარჯების მოცულობა, ბირჟებზე ბიტკოინის კურსის განსაკუთრებით მნიშვნელოვანი ნეგატიური რყევების დროს მაინინგი შეიძლება წამგებიანიც გახდეს.

რამდენად უცნაურიც უნდა იყოს, მოვლენათა განვითარების ასეთი სცენარი გათვალისწინებული იყო ბიტკოინის პროექტის ნიჭიერი შემქმნელის მიერ – მონეტების მოპოვების სირთულეს ხომ ქსელი ავტომატურად მართავს ორივე მიმართულებით, და თუ მაინერებისათვის სირთულის რომელიღაც დონეზე არამომგებიანი ხდება ფერმების შენახვა, მათ შეუძლიათ, უარი თქვან ამ საქმიანობაზე და გამორთონ მოწყობილობები, სამუდამოდ ან თუნდაც დროებით. მაშინ ქსელის საერთო ჰეშრეიტი დაიწყებს ვარდნას, ხოლო მისი სირთულე პროპორციულად შემცირდება. ამავდროულად შემცირდება ერთი კრიპტომონეტის მოსაპოვებლად საჭირო მოხმარებული ელექტროენერგიის მოცულობა. თუმცა პრაქტიკაში, ბიტკოინის კურსის არსებითი კორექციისას ფასთა მაქსიმუმიდან მნიშვნელოვანი დაცემისაკენ ქსელის ერთობლივი გამომთვლელი სიმძლავრე მაინც აქტიურად იზრდება.

მხოლოდ 2018 წლის განმავლობაში ბიტკოინ-ქსელში ჰეშრეიტი გასამმაგდა, მიუხედავად იმისა, რომ ამავე პერიოდში ბიტკოინი თითქმის ოთხჯერ გაიაფდა. აშკარაა, რომ მაინერების ამოუწურავი ოპტიმიზმი და მათი რწმენა ბიტკოინის აღდგენისა და ღირებულების შემდგომი ზრდისა პრევალირებს საბაზრო სიტუაციის რეალისტურ ანალიზზე. ამგვარად, ყოველგვარი საფუძველი გვაქვს ვიფიქროთ, რომ მაინერთა უდიდესი უმრავლესობა მიდრეკილია განიხილოს ფასთა კორექციის პერიოდები როგორც მოვლენები, რომლებსაც მხოლოდ დროებითი ხასიათი აქვს, იმ დროს, როცა აღმავალ ღირებულებით ტრენდებს შედარებით პერმანენტული ფაქტორის როლი ენიჭება.

დაბოლოს, კონკრეტული ადამიანის მხრიდან კრიპტოვალუტისადმი ნდობის უმნიშვნელოვანესი ფაქტორია პირადად მისი აღქმა იმისა, თუ რამდენად მასობრივია იმავე აქტივის მიმართ ბაზრის სხვა მონაწილეთა ნდობა. სწორედ საზოგადოების ეს ერთობლივი ნდობა ასევე წარმოადგენს მნიშვნელოვან დანამატს ნებისმიერი ფინანსური აქტივის ფასეულობაზე, მათ შორის კრიპტოვალუტაზეც. როდესაც XVIII საუკუნეში ევროპაში ქაღალდის ფული გამოჩნდა, მას ძალზე ნაკლებად ენდობოდნენ. რამდენიმე ათასწლეულის მანძილზე ყველა სავაჭრო ურთიერთობა იგებოდა ძვირფასი ლითონებისაგან, პირველ რიგში – ოქროსა და ვერცხლისაგან დამზადებული მონეტების ცირკულაციაზე, და მგონი, მხოლოდ კოლუმბამდელი ინდიელები დარჩნენ ამ პროცესის მიღმა. ისინი ოქროსაგან აკეთებდნენ ყველაფერს, ფულის გარდა, ყოველ შემთხვევაში მანამ, სანამ კონკისტადორებმა არ „ჩართეს“ მსოფლიო ფინანსურ სისტემაში. რაც შეეხება ქაღალდის ასიგნაციებს, მათ მიმართ ნდობის გაჩენის ევოლუციას ასწლეულები დასჭირდა, თან მაშინ, როცა სახელმწიფო ბანკები ხანგრძლივი დროის განმავლობაში, საკუთარი მარაგებიდან ბანკნოტების ოქროზე გადაცვლის გარანტიას იძლეოდნენ, პრაქტიკულად, ოქროს სტანდარტის გაუქმებამდე, გასული საუკუნის 70-იან წლებში.

თავისთავად ყალიბდება დასკვნა, რომ გადახდის სხვადასხვა საშუალების მიმართ ნდობის ჩამოყალიბება მხოლოდ საყოფაცხოვრებო ჩვევის საკითხია, რომელიც ადამიანებს ასეული და ათასეული წლის მანძილზე უყალიბდებათ და საბოლოოდ აღმოჩნდება, რომ საქმე გვაქვს მხოლოდ საუკუნეების განმავლობაში ჩამოყალიბებულ, ფულის დასამზადებელი მასალების „რეპუტაციასთან“ და თვით ემიტენტებთან, რომლებიც მათ ბრუნვაში უშვებენ. არსებობს ელექტრონული კრიპტოვალუტები ანუ არსებობს ახალი ტიპის ფიზიკურად აღუქმელი და ამის გამო ბევრისთვის მიუჩვეველი ფული. მაგრამ მას აქვს, როგორც დავრწმუნდით, რიგი სერიოზული უპირატესობისა ფიატურ ფულთან შედარებით. ხოლო ამ შემთხვევაში ემიტენტის როლს საკუთარ თავზე იღებს მათემატიკური ალგორითმები, რომელთა რეპუტაციაც ზედმიწევნით მეცნიერულია და ამიტომ უდავოა.

ძნელია საუბარი ახალი ფორმის ფულის მიმართ მსოფლიო მასშტაბით ჩვევისა და მასობრივი ნდობის ჩამოყალიბებაზე ბიტკოინ-ტექნოლოგიის არსებობის ათი წლის განმავლობაში. თუმცა, ყველა

საფუძველი არსებობს ვივარაუდოთ, რომ გადახდის საშუალების ეს სახეობა მსოფლიოს დაიპყრობს უფრო სწრაფად, ვიდრე მისი ისტორიული წინამორბედები. განსაკუთრებით, თუ გავითვალისწინებთ, როგორ ხდებოდა პირველი კრიპტოვალუტის საბაზრო კურსის ჩამოყალიბება მისი არსებობის საწყის წლებში. რომელიღაც მომენტში კრიპტოსაზოგადოებამ ბიტკოინის განხილვა დაიწყო არა მარტო როგორც სწრაფი, ანონიმური და იაფი უტილიტარული საშუალებისა, არამედ ასევე, როგორც ფინანსური ინვესტიციის ფორმისა. ბევრი ინვესტორი არცთუ უსაფუძვლოდ ვარაუდობდა, რომ მსგავსმა დაბანდებებმა მათ მფლობელებს შესაძლოა მოუტანოს მნიშვნელოვანი შემოსავლები დროის შედარებით მოკლე პერიოდში. რამდენად ახდა მათი მოლოდინები არსებული მომენტისათვის?

ბიტკოინი როგორც ინვესტიცია

ბიტკოინ-ქსელის მუშაობის ადრეულ ეტაპებზე ბევრი მაინერი, რომლებიც აწარმოებდა კრიპტომონეტების მოპოვებას სირთულის დაბალ დონეებზე, ამას არც ისე სერიოზულად აღიქვამდა. ისინი ამაში უფრო თამაშის ელემენტებს ხედავდნენ და ახალი ტიპის ფინანსური სისტემის ნაწილებად თავს ნაკლებად მიიჩნევდნენ. შედეგად, პირველ მიღებულ ბიტკოინებს საკუთარი აღქმის შესაბამისად ექცეოდნენ: ერთმანეთისთვის ტესტურ გადარიცხვებს ახორციელებდნენ, ჩუქნიდნენ, ყრიდნენ უსარგებლობის გამო ან უბრალოდ კარგავდნენ, თავიანთი ციფრული საფულეების საიდუმლო გასაღებებთან ერთად. მიუხედავად ამისა, 2009 წლის 5 ოქტომბერს ბიტკოინმა მიიღო ისტორიაში თავისი პირველი საბაზრო მონეტარული შეფასება, რომელიც რეალურად ჩატარებულ გარიგებებს ეფუძნებოდა. ერთ დოლარში იძლეოდნენ 1309 ბიტკოინს ანუ ერთი მონეტა ღირდა დაახლოებით 0,08 ამერიკული ცენტი.

მაგრამ კურსმა საკმაოდ სწრაფი ზრდა დაიწყო. ამასთან დაკავშირებით გვინდა გავიხსენოთ ერთი ისტორია, რომელიც 2009 წლის ბოლოს მოხდა ნორვეგიაში, სადაც ადგილობრივი სტუდენტი კრისტოფერ კოხი წერდა ნაშრომს კრიპტოგრაფიაში. თავისი სადიპლომი ნაშრომის ერთ-ერთი თავი მან მიუძღვნა კრიპტოგრაფიაში შედარებით ახალგაჩენილ მოვლენას – ბიტკოინს. კვლევისას მან სასინჯად შეიძინა ბიტკოინის 5000 მონეტა და მასზე დაახლოებით 27 ამერიკული დოლარი დახარჯა. ეს შეესაბამებოდა ნახევარ ცენტზე ოდნავ მეტს ერთი მონეტისთვის. იმის შემდეგ, რაც დიპლომი დაწერილი და დაცული იქნა, შეძენილი ბიტკოინები კოხმა საერთოდ დაივიწყა. მაგრამ მათი გახსენება მოუხდა ოთხი წლის შემდეგ, როდესაც კრიპტოვალუტამ სულ უფრო მეტად გაითქვა სახელი და მასზე ინფორმაცია აქტიურად ვრცელდებოდა მთელ მსოფლიოში. როცა მიხვდა, რომ მნიშვნელოვანი რაოდენობის ციფრული მონეტების მფლობელი იყო, კოხმა სასწრაფოდ დაიწყო თავისი დიდი ხნით მიგდებული ვირტუალური აქტივის ძებნა. ბიტკოინ-საფულისათვის პაროლის პოვნა ყოფილმა სტუდენტმა ძლივს შეძლო, თუმცა ძალისხმევა ამად ღირდა: გაირკვა, რომ მისი

ნახევრად მივიწყებული 27-დოლარიანი შემთხვევითი ინვესტიცია რამდენიმე წელიწადში ძვირფას განძად გადაიქცა და დაახლოებით 1 მილიონი დოლარი ღირდა, ანუ ამ ხნის განმავლობაში, ერთი ბიტკოინის ღირებულება რამდენიმე ასეულით გაზრდილიყო. სადიპლომო ნამუშევარმა კოხი მოულოდნელად მდიდარ ადამიანად აქცია. ციდან ჩამოვარდნილი სიმდიდრის დიდი ნაწილის უძრავი ქონების შეძენაზე დახარჯვის შემდეგ, კრიპტომონეტების ნაწილის შენახვა კოხმა მაინც გადაწყვიტა საფულეში, ბიტკოინის შემდგომი ზრდის იმედად, რამაც არ დააყოვნა შემდგომი რამდენიმე წლის განმავლობაში.

მაგრამ ყველა ისტორიას ასეთი ბედნიერი დასასრული როდი ჰქონდა. ბევრად ცნობილი გახდა ამბავი, რომელიც ბიტკოინის ისტორიაში კრიპტოვალუტით ფიზიკური საქონლის პირველად ყიდვასთანაა დაკავშირებული. ეს მოხდა 2010 წლის მაისის ბოლოს, როდესაც ამერიკელმა პროგრამისტმა ლასლო ჰანეჩმა (Laszlo Hanyecz) ბიტკოინ-ფორუმზე გაავრცელა ხმა, რომ მზადაა გადაიხადოს 10 000 ბიტკოინი, თუკი ფლორიდის ქალაქ ჯექსონვილში მიუტანენ დაახლოებით 25 დოლარად ღირებულ ორ პიცას. გავიდა მთელი ოთხი დღე, სანამ კონტრაგენტს იპოვიდნენ, რის შემდეგაც პიცა მიტანილი იქნა მისამართზე, ხოლო შესაბამისი თანხა ბიტკოინებში ამის საფასურად გადაირიცხა. ეს მოხდა 22 მაისს, და ამის შემდეგ ეს გაზაფხულის დღე მთელი ბიტკოინ-ინდუსტრიის პირველი და ჯერჯერობით უკანასკნელი დარგობრივი სამახსოვრო დღე გახდა, რომელსაც Bitcoin Pizza Day ეწოდა. ამ დღეს კრიპტოენთუზიასტები მთელ მსოფლიოში ჭამენ პიცას და არცთუ სახარბიელოდ ლაპარაკობენ უიღბლო მაინერის წინასწარმეტყველურ ნიჭზე, რომელმაც ორ პიცაში რამდენიმე ათეული მილიონი დოლარის ეკვივალენტი გადაიხადა. სწორედ ასეთი დონის თანხად იქცა ის 10 000 ბიტკოინი შვიდი წლის შემდეგ. მიუხედავად ამისა, არ შეიძლება ითქვას, რომ ბიტკოინის კურსი არსებობის პირველი ათი წლის განმვლობაში მხოლოდ იზრდებოდა. ბიტკოინის ღირებულება, როგორც ნებისმიერი სხვა ფინანსური ინსტრუმენტისა, განიცდიდა სხვადასხვაგვარ რყევას და კორექციებს სხვადასხვა, როგორც ტექნიკური, ასევე ფუნდამენტური ფაქტორის გამო.

ბიტკოინების ფიატურ ვალუტაზე გადაცვლის პირველი მოედანი ბიტკოინ-პროექტის გაშვებიდან დაახლოებით ერთ წელიწადში გაჩნდა, 2010 წლის 6 თებერვალს დაიწყო მუშაობა ბირჟამ Bitcoin Market.

თუმცა ბიტკოინებით ორგანიზებული ვაჭრობის ადრეულ პერიოდში ყველაზე ცნობილი გახდა სხვა საბირჟო მოედანი – Mt. Gox. ის გაიხსნა 2010 წლის 17 ივლისს და საკმაოდ სწრაფად მოიპოვა პოპულარობა ბიტკოინ-ტრეიდერებს შორის, რადგან არსებითად, გახდა „პირველი ნომერი ბირჟა“ კრიპტოვალუტური გარიგებების რეალიზებისათვის. დაზუსტებით რომ ვთქვათ, პროექტ Mt. Gox.-ის საიტი გაშვებული იქნა 2006 წელს, პოპულარული სამაგიდო თამაშის Magic The Gathering სათამაშო ბარათებით ელექტრონული საბირჟო ვაჭრობის ორგანიზაციისათვის. სწორედ თამაშის შემოკლებული სახელიდან წარმოიშვა ბირჟის დასახელება. მისმა შემქმნელმა, შემმუშავებელმა ჯედ მაკკალებმა 2011 წლის გაზაფხულზე პროექტი მიჰყიდა ფრანგ პროგრამისტ მარკ კარპელესს, რომელიც იმჟამად იაპონიაში ცხოვრობდა.

დაახლოებით იმ დროს დაემთხვა კრიპტოვალუტებით ვაჭრობის „ბუმი“ და ბიტკოინის ღირებულებამ ზრდა დაიწყო. თუმცა, უკვე იმავე წლის ივნისში ბირჟას თავს დაესხნენ ჰაკერები, რის შედეგადაც, ბირჟის ანგარიშებიდან მოპარული იქნა რამდენიმე ათეული ათასი ბიტკოინი, რომლებიც დაახლოებით 32 დოლარად იყო შეფასებული. მიუხედავად იმისა, რომ სისტემის უსაფრთხოებაში „ხვრელი“ საკმაოდ სწრაფად იქნა ლიკვიდირებული, ბიტკოინისადმი საინვესტიციო ნდობა სერიოზულად დაეცა. ბირჟის მფლობელსა და მის თანამშრომლებს დიდი ძალისხმევა დასჭირდათ ტრეიდერებს შორის პანიკის შესაჩერებლად, რის შემდეგაც ბიტკოინის კურსმა ნელ-ნელა ზრდა დაიწყო და თანდათანობით „უკან დააბრუნა“ ღირებულების მასშტაბური დაცემა. შეტევით მიღებული გამოცდილების ყოველმხრივ გათვალისწინების შედეგად, კარპელესმა სერიოზული ძალისხმევა მოახმარა ბირჟის მუშაობის უსაფრთხოების ამაღლებას. სხვა ზომებს შორის შემოღებული იქნა ორფაქტორიანი იდენტიფიკაცია ერთჯერადი პაროლების გენერატორების ბაზაზე, რომელსაც ტრეიდერები ბირჟაზე შესვლისას იყენებდნენ.

Mt. Gox.-ის აყვავებისა და კეთილდღეობის ეპოქა შემდგომ სამ წელზე მოდის, თუმცა ამ პერიოდში ბირჟაზე ხანდახან ხდებოდა სხვადასხვა სახის უსიამოვნებები. რომელიღაც მომენტში სავაჭრო მოედნის საქმიანობას ყურადღება მიაქციეს აშშ-ის ფინანსურმა რეგულატორებმა. შედეგად, დაბლოკილი იქნა ბირჟის ამერიკული ქვეგანყოფილების საბანკო ანგარიშები, სადაც განთავსებული იყო დაახლოებით

4,5 მილიონი დოლარი. თანხების დაბრუნება საბოლოოდ შესაძლებელი გახდა, მაგრამ ამან ვერ გადაჭრა მთლიანობაში ამერიკულ საბანკო სისტემასთან არსებული ყველა პრობლემა. ამერიკული ფინანსური ინდუსტრიის წარმომადგენლები ძალზე სკეპტიკურად უყურებდნენ ბირჟის მუშაობას, ეჭვობდნენ მის თანამონაწილეობას ფულის მასობრივ გათეთრებაში კრიპტოვალუტით ვაჭრობის საშუალებით.

მიუხედავად ამისა, ბიტკოინის კურსი იზრდებოდა და 2013 წლის ნოემბრისათვის ერთ ბიტკოინზე 1200 დოლარს მიაღწია. ამასთან, Mt. Gox.-ის ბირჟაზე ამ დროს ბიტკოინ-ქსელის ტრანზაქციების დაახლოებით ნახევარი მოდიოდა. მაგრამ იმავდროულად, ბირჟის მუშაობაში ბზარები გაჩნდა, რაც განსაკუთრებულად გამოიხატა Mt. Gox.-ის როგორც კრიპტოვალუტური, ისე ფიატური ანგარიშებიდან კლიენტების სახსრების გამოტანაში. ტრეიდერებმა დაიწყეს უკმაყოფილების გამოხატვა, ხოლო ბევრი მათგანი საერთოდ გადავიდა კონკურენტულ სავაჭრო მოედნებზე. ბლოკჩეინ-გარემოში ვრცელდებოდა ჭორები Mt. Gox-ის შიდა პრობლემებზე, სანამ, ბოლოს და ბოლოს, 2014 წლის თებერვალში მოხდა ამ ინტრიგის ტრაგიკული გახსნა. თებერვლის დასაწყისიდან ბირჟამ შეწყვიტა ანგარიშებიდან სახსრების გატანის ყველანაირი ოპერაციის განხორციელება, ხოლო 23 თებერვალს კარპელესმა გამოაქვეყნა მოკლე შეტყობინება ბირჟის სრული კრახის შესახებ, რის შემდეგაც პროექტის საიტი ინტერნეტიდან გაქრა.

ბირჟის კლიენტებში, როგორც მოსალოდნელი იყო, პანიკა ატყდა. ზოგიერთ ბლოკჩეინ-ფორუმზე გაჩნდა ინფორმაცია ბირჟის შიდა დოკუმენტის „გაჟონვის“ ფორმით, სადაც ლაპარაკი იყო ჰაკერების მიერ საბირჟო ანგარიშებიდან 744 000 ბიტკოინის მოპარვის შესახებ. კიდევ რამდენიმე დღის შემდეგ, 28 თებერვალს, ბირჟის ხელმძღვანელობამ ოფიციალურად განაცხადა გაკოტრების შესახებ. ეს მაშინვე მაქსიმალურად სწრაფად აისახა ბიტკოინის კურსზე, ის 550 დოლარამდე დაეცა. ოფიციალურად იქნა აღიარებული 650 000 ბიტკოინის დაკარგვა, თუმცა ბოლომდე მაინც ვერ გაირკვა, მართლა განხორციელდა ჰაკერული თვდასხმა თუ კრახი ინსპირირებული იყო მფლობელის მიერ. არსებობდა ეჭვი, რომ კარპელესმა საბირჟო ტრეიდერების კუთვნილი ბიტკოინების უზარმაზარი რაოდენობა რომელიღაც საიდუმლო მისამართზე გადაიტანა, შემდგომში საკუთარი მიზნით მათი გამოყენების იმედით. მიუხედავად კარპელესის მხრი-

დან გამოხატული ფორმალური მზაობისა, ყველანაირად დახმარებოდა გამოძიებას, 2019 წლის გაზაფხულზე მას 2,5 წლით პატიმრობა მაინც მიუსაჯეს. სანამ გამოძიება და სასამართლო განხილვა მიმდინარეობდა, პროექტის საბანკროტო მმართველებმა შეძლეს ბირჟის კლიენტებისათვის სახსრების გარკვეული რაოდენობის დაბრუნება, რომლებიც აღმოაჩინეს და მოაგროვეს შემდგომი გადახდებისათვის. Mt. Gox.-ის კრახის შემდეგ ბიტკოინს დაახლოებით სამი წელი დასჭირდა, რათა აღედგინა ადრე მოპოვებული ღირებულებითი პოზიციები. ამასთან, ამ პერიოდში კრიპტოვალუტების ბირჟების რაოდენობა მნიშვნელოვნად გაიზარდა. ამჟამად ინტერნეტში არის ასეული სავაჭრო მოედანი, რომლებიც აქტიურად გვთავაზობს სხვადასხვა ციფრული მონეტის როგორც ერთმანეთზე, ასევე ფიატურ გადახდის საშუალებებზე გაცვლის მომსახურებას.

2017 წლის ბოლოსათვის ბლოკჩეინ-ინდუსტრიის გარშემო შეიქმნა სიტუაცია, რომელსაც კრიპტოსაზოგადოებაში „ჰაიპი“ უწოდეს, ინგლისური სიტყვა hype-ის მიხედვით, რაც მნიშვნელობით ახლოსაა ცნებებთან „ხმაური“, „აჟიოტაჟი“ ან „მომაბეზრებელი რეკლამა“. ეს პერიოდი თითქმის ყველა კრიპტოვალუტის და პირველ რიგში, ბიტკოინის მკვეთრი ზრდით აღინიშნა. ძირითადი კრიპტოვალუტის კურსი მუდმივად ამყარებდა ფასობრივ რეკორდებს მანამ, სანამ, ბოლოს და ბოლოს, შობის წინ, 20 000 დოლარზე მაღალ ნიშნულს მიაღწია. ამ დროისათვის, მსოფლიოში ბიტკოინზე გაგონილი არ ჰქონდათ მხოლოდ ზარმაცებს, იმათი ჩათვლით, ვისაც არასდროს ჰქონდა კავშირი არც საინფორმაციო და არც საფინანსო ტექნოლოგიებთან. მართლაც, 2018 წლის იანვრიდან დაწყებული, ბიტკოინმა განიცადა სერიოზული ფასობრივი კორექცია და წლის განმავლობაში თავისი ღირებულების 75% დაკარგა. შედეგად ბევრმა ინვესტორმა, რომლებმაც გაუფრთხილებლობით, ბიტკოინი ფასობრივი პიკის დროს შეიძინეს, მნიშვნელოვანი ფინანსური ზარალი განიცადა. მაგრამ ისინი, ვინც ინვესტიციები ჯერ კიდევ 2017 წლის პირველ ნახევარში ან უფრო ადრე განახორციელეს, დღემდე მოგების ზონაში იმყოფებიან, იმდენად მკვეთრად გაიზარდა ბიტკოინის კურსი წლის მეორე ნახევარში. მნიშვნელოვანი ფასობრივი ვარდნის დროსაც კი ბიტკოინის მომავლისადმი რწმენა ჯერ კიდევ შენარჩუნებულია უმრავლეს როგორც პირდაპირ, ასევე ირიბ ინვესტორებში –

მაინერებში. მეწარმეთა ეს კატეგორია აგრძელებს ჰეშრეიტის ზრდას ბიტკოინ-ქსელში განსაკუთრებულად მაღალი ტემპებით. ეს ხდება მიუხედავად იმისა, რომ ამჟამად მაინინგი არამომგებიანად, ზოგჯერ კი წამგებიანადაც ითვლება. აუცილებელია გვესმოდეს, თუ რომელ ფაქტორებზეა დამოკიდებული ბიტკოინისა და სხვა მსგავსი კრიპტოვალუტების მაინინგის ეფექტურობა, რომლებიც მოიპოვება მუშაობის დამადასტურებელი პრინციპის (Proof-of-work) საფუძველზე.

ჩვენ უკვე ვმსჯელობდით იმაზე, რომ ამ საქმიანობის მსურველ მეწარმეებს უწევთ მნიშვნელოვანი ფულადი სახსრების ინვესტირება მაინინგურ მოწყობილობებსა და იმ სათავსების აღჭურვაში, სადაც ეს მოწყობილობები მონტაჟდება. გარდა ამისა, მაინერებს აქვთ ხარჯები, რომლებიც დაკავშირებულია ელექტროენერგიის მნიშვნელოვან მოხმარებასთან, სისტემური ინჟინრების ხელფასების გადახდასთან, საგადასახადო თანხების დაფარვასთან და სხვა. ლოგიკურია ვივარაუდოთ, რომ მსოფლიოში ყველა ადგილი როდი გამოდგება კრიპტოვალუტათა მაინინგისათვის. აუცილებელია ისეთი გეოგრაფიული ადგილმდებარეობის შერჩევა, სადაც შესაძლებელი იქნება ზემოთ ჩამოთვლილი ფინანსური დანახარჯების მინიმიზება, რამდენადაც მეწარმე ამას შეძლებს. როგორც აღმოჩნდა, მსოფლიოში არც ისე ბევრია ადგილი, სადაც მაინინგი იმდენად ეფექტიანი იქნება, რომ „მაინინგური ფერმების“ ხარჯები არ გადააჭარბებს მოპოვებული კრიპტოვალუტების რეალიზაციით მიღებულ შემოსავალს, განსაკუთრებით მათი საბაზრო ღირებულების მნიშვნელოვანი კორექციის პირობებში.

მიმდინარე მომენტისათვის, კრიპტომოპოვების დარგში შეიქმნა სიტუაცია, როდესაც მაინინგური სიმძლავრეების დაახლოებით 80%-მა თავი მოიყარა მსოფლიოს სამრეწველო „სამჭედლოში“ – ჩინეთში. სწორედ ამ ქვეყანაში ბუნებრივად შეიქმნა პირობები, რომლებიც ხელს უწყობს ასეთ საქმიანობას, თუ, რა თქმა უნდა, ყურადღებას არ მივაქცევთ ჩინეთის მთავრობის რამდენადმე არამეგობრულ და ღიად ეჭვიან პოზიციას მთლიანად კრიპტოვალუტების მიმართ. მიუხედავად ამისა, მაინინგისათვის საჭირო ძირითადი მოწყობილობები იქმნება სწორედ ჩინეთში, ამიტომ ადგილობრივ მაინერებს არ სჭირდებათ ძვირად ღირებული მოწყობილობის ნახევარ მსოფლიოზე გადაზიდვა და ასევე, დამატებითი საბაჟო მოსაკრებლების გადახდა. ელექტროსადგურები ქვეყნის მთიან რეგიონებში ელექტროენერგიაზე მისა-

ღები ფასების დაწესების საშუალებას იძლევა და ამავე რაიონების საკმაოდ ცივი კლიმატი მოწყობილობის გადახურების პრობლემის ხელსაყრელ საბიუჯეტო გადაჭრას უზრუნველყოფს. თუკი მიღებულია ტექნოლოგიური გადაწყვეტილება წყლით გაგრილების სასარგებლოდ, მაშინ ამავე რაიონებში, როგორც წესი, მაინერების მომსახურებისათვის მთის ცივი მდინარეები მოედინება. მუშახელის ღირებულებაც ჩინეთის პერიფერიულ რეგიონებში ასევე საკმაოდ დაბალია, რაც კიდევ ერთ მნიშვნელოვან ფაქტორს წარმოადგენს სწორედ ამ ქვეყნის ასარჩევად კრიპტოვალუტების მაინინგის საქმიანობაში ინვესტირებისათის.

ითვლება, რომ ბიტკოინ-ქსელის გამომთვლელი სიმძლავრის უდიდეს წილს ოთხი მაინინგური პული აკონტროლებს და ყველა მათგანი ჩინეთში იმყოფება. ერთი პოლიტიკური იურისდიქციის ფარგლებსა და მხოლოდ ოთხი მმართველი სუბიექტის კონტროლის ქვეშ მყოფი ერთობლივი ჰეშრეიტის ასეთი მაღალი კონცენტრაცია, რასაკვირველია, არ არის პოზიტიური ფაქტორი ტექნოლოგიისათვის, რომელიც მოწოდებულია იყოს ჭეშმარიტად დეცენტრალიზებული. მაგრამ კრიპტოსაზოგადოება ამ სიტუაციას როგორც დროებითს განიხილავს და სჯერა, რომ ბიტკოინ-ქსელის მაინინგის ევოლუციონირება თანდათან გადანაწილების ფორმას მიიღებს. ყველა შემთხვევაში, ჯერჯერობით სწორედ ბიტკოინი რჩება ყველაზე მოთხოვნად და პოპულარულ კრიპტოინსტრუმენტად, რომლის ჯამური ემისიის ერთობლივი ღირებულება მთელი კრიპტოვალუტის ბაზრის კაპიტალიზაციის დაახლოებით ნახევარს შეადგენს. პროექტი „ბიტკოინი“ სატოში ნაკამოტოს მიერ შექმნილია როგორც დეცენტრალიზებული გადახდის ციფრული სისტემა, ხოლო თვით ბიტკოინის მონეტები უნდა გამხდარიყო გადახდის პოპულარული ფორმა, რომელიც თანდათანობით გამოაძევებდა ნაჩვევ ფიატურ ფულს ყოველდღიური ბრუნვიდან. შევეცადოთ შევაფასოთ, რამდენად შეძლო პროექტმა „ბიტკოინმა“ ჩანაფიქრის განხორციელება მისი არსებობის პირველი ათწლეულის განმავლობაში.

ბიტკოინი როგორც გადახდის საშუალება

იმის შემდეგ, რაც ბიტკოინ-ქსელის ციფრულმა მონეტებმა ფინანსურ ბაზარზე სერიოზული მონეტარული შეფასება მიიღო, ამ ციფრული აქტივების დიდი რაოდენობის მფლობელები ყველასთვის (და შეიძლება თავად მათთვისაც) მოულოდნელად, შეძლებულ ადამიანებად იქცნენ. ბევრი მათგანის კრიპტოვალუტური კაპიტალი ასეული მილიონით, ხანდახან კი მილიარდობით დოლარითაც კი ფასდება. რა თქმა უნდა, პირველი, ვისზეც ყურადღება გაამახვილეს, ბიტკოინ-პროექტის შემქმნელი სატოში ნაკამოტო გახდა. როგორც მისივე შექმნილ ქსელში პირველმა მაინერმა, მან შეძლო დიდი რაოდენობით მონეტების მოპოვება, რადგანაც სისტემის სირთულის საწყისი დონე ამას ხელს უწყობდა. ერთი პირობა ითვლებოდა, რომ ნაკამოტომ შეძლო დაახლოებით ერთი მილიონი მონეტის გამომუშავება, მაგრამ უკანასკნელი კვლევებით, ეს რიცხი 700 000-ს არ აჭარბებს. მაგრამ თუნდაც ამ შემთხვევაში, მისი ქონების კაპიტალიზაცია ამჟამად, დაახლოებით 3,5 მილიარდ დოლარად ფასდება. ასე მოხვდა იდუმალი გამომგონებელი ჟურნალ Forbes-ის მილიარდერთა მსოფლიო რეიტინგში, ხოლო ბიტკოინის რეკორდული ფასების პერიოდში ნაკამოტოს ადგილი ეკავა პირველ ორმოცდაათ მილიარდერს შორის.

ამასთან დაკავშირებით, არ შეიძლება არ გავიხსენოთ არცთუ უცნობი ტყუპი ძმა – კემერონ და ტაილერ უინკლვოსები. ჰარვარდის ყოფილმა სტუდენტებმა და ოლიმპიელმა სპორტსმენებმა თავის დროზე, Facebook-ის შემქმნელ მარკ ცუკერბერგს სასამართლოს ძალით მოუგეს დაახლოებით 65 მილიონი დოლარი ვითომდა სოციალური ქსელის მათგან მოპარული იდეის საკომპენსაციოდ. მიღებული თანხის ნაწილი ძმებმა მომგებიანად ჩადეს ბიტკოინში, როდესაც ის ერთი მონეტისათვის ჯერ კიდევ 100 დოლარზე ოდნავ მეტი ღირდა. ვარაუდობენ, რომ მათ შეძლეს 100 000-ზე მეტი ბიტკოინის შეძენა, რამაც ნახევარ მილიარდთან (რა თქმა უნდა, ეს დამოკიდებულია ბირჟებზე ბიტკოინის საბაზრო კურსის მერყეობაზე) მიახლოე-

ბული თანხის მფლობელებად აქცია. დადიოდა ხმები, რომ თავიანთი ბიტკოინ-მისამართების საიდუმლო გასაღებები ძმებმა დაბეჭდეს ქაღალდზე, რომელიც შემდეგ რამდენიმე ნაწილად დაჭრეს და ეს ნაჭრები ცალ-ცალკე შეინახეს აშშ-ის სხვადახვა ქალაქის ბანკების სეიფებში. ასეთი რთული ოპერაცია იმისათვის ჩაატარეს, რომ დაეცვათ თავიანთი ციფრული აქტივები ქსელური ბოროტმოქმედების ხელყოფისაგან.

დაბოლოს, ღირს კიდევ ერთხელ ვახსენოთ Mt. Gox-ის ბირჟის ყოფილი მფლობელი მარკ კარპელესი, რომელზეც 650 000 ბიტკოინის დატაცების ეჭვი არსებობდა და რომლებიც, როგორც თავად ამტკიცებს, ჰაკერებმა მოიპარეს. თუკი ის ამ განძის საიდუმლო მფლობელია, მაშინ ამჟამად ეს განძი 3 მილიარდ დოლარზე მეტად ფასდება, რაც თავად ნაკამოტოს კაპიტალის სადარი სიდიდეა. ოღონდ, ბლოკჩეინ-ტექნოლოგიის გამომგონებლის შემთხვევაში, მის მიერ შეძენილი ბიტკოინების ლეგიტიმურობა ეჭვს არ იწვევს, რადგან ისინი მიღებული იქნა აბსოლუტურად ღიად, მაინინგური პროცესების საშუალებით.

არსებობს ბლოკჩეინ-ტექნოლოგიის ბაზაზე აგებული რიგი გადახდის სისტემებისა, რომლებსაც აქტიურ მონაწილეთა მნიშვნელოვანი რაოდენობა ჰყავს, რომლებსაც კრიპტომონეტების გარკვეული რაოდენობის დაგროვება შეუძლიათ. ამასთან დაკავშირებით წარმოიშობა კანონიერი კითხვა: რა საქონელი და მომსახურება შეიძლება შეძენილი იქნას ამ ციფრული ფულით? არსებითად, პასუხი ნათელია: ზუსტად ისეთივე, როგორიც ფიატური გადახდის საშუალებით. პრობლემა მხოლოდ გამყიდველების მზაობაა, მიიღონ კრიპტოვალუტა, პრობლემაა კრიპტოვალუტაში მიღებული შემოსავლების ლეგიტიმაციის საკითხი და ასევე, ფიატურ ვალუტებში მათი კონვერტირების საკითხი, მათი კანონიერი საბუღალტრო და საგადასახადო აღრიცხვის მიზნით. აშკარაა, რომ ეს საკითხები ამა თუ იმ სახელმწიფოში ეროვნული საფინანსო კანონმდებლობის თავისებურებებიდან გამომდინარე წყდება, და, რამდენად სამწუხაროც უნდა იყოს, კრიპტოვალუტებით გადახდებისათვის ყველგან როდია შექმნილი შედარებითი ხელშეწყობის რეჟიმი. ამიტომ საქონლისა და მომსახურების კრიპტოვალუტით შეძენამ ჯერ კიდევ ვერ პოვა მართლაც მასობრივი გავრცელება. თუმცა, ეს პროცესი ნელა, მაგრამ უფრო და

უფრო იპყრობს სხვადასხვა საქმიან სფეროს და იმედია, რომ ადრე თუ გვიან, კრიპტოვალუტები მსოფლიო სასაქონლო-ფინანსურ ბრუნვაში ღირსეულ ადგილს დაიკავებს.

დროდადრო მსოფლიო მედიაში ქვეყნდება სარეკლამო შეტყობინებები იმის შესახებ, რომ ამა თუ იმ აქტივის შეძენა ბიტკოინით ან სხვა კრიპტოვალუტით შეიძლება. როგორც წესი, საუბარია ფუფუნების საგნებზე, მდიდრულ ვილებზე, იახტებზე, ძვირფას ავტომობილებზე ან კერძო თვითმფრინავებზე. მაგრამ უკანასკნელ დროს უფრო და უფრო ხშირად ჩნდება ინფორმაცია, რომ შესაძლებელია ციფრული ფულით სავსებით ჩვეულებრივი, ყოველდღიური მოხმარების საგნების შეძენა. თუმცა, სამწუხაროდ, ასეთი სავაჭრო წერტილები, ჯერჯერობით მხოლოდ ერთეულებია და წარმოდგენილია ღარიბი სასაქონლო ასორტიმენტის მქონე ინტერნეტმაღაზიებით. იმისათვის, რომ ამ სახის გადახდის ფორმა მასობრივი გახდეს, აუცილებელია გადახდათა სისტემების განშტოებული სტრუქტურები, რომლებიც უზრუნველყოფს ფულადი ნაკადების ერთი ფულადი ფორმიდან მეორეში აუცილებელ კონვერტაციას. ასეთი სისტემები უკვე აქტიურად ავითარებს საქმიანობას მსოფლიოს სხვადასხვა რეგიონში, მიუხედავად იმისა, რომ ყველა ქვეყნიდან მხოლოდ იაპონიამ აღიარა კრიპტოვალუტები გადახდის ოფიციალურ საშუალებად.

გადახდის სისტემების გარდა, არსებობს კიდევ ერთი ელემენტი, რომელიც სასიცოცხლოდ აუცილებელია კრიპტოვალუტების მასობრივ ბრუნვაში წარმატებული ჩანერგვისათვის – ბანკომატი, რომელიც გასცემს ნაღდ ფიატურ ფულს ბიტკოინზე ან სხვა პოპულარულ კრიპტომონეტებზე. პროექტები ფულის ამგვარი აპარატების შესაქმნელად და დასამონტაჟებლად უკვე არსებობს და აქტიურად ზრდის საკუთარი ბიზნესის მოცულობის ბრუნვებს მთელ მსოფლიოში. მაგალითად, 2019 წლის დასაწყისისათვის მხოლოდ ბიტკოინ-ავტომატების რაოდენობამ 4000 შეადგინა. მსოფლიოში ყოველდღიურად დგება მინიმუმ შვიდი ახალი აპარატი. ამასთან, ყველა არსებული ავტომატიდან მესამედში მაინცაა შესაძლებელი არა მარტო ნაღდი ფულის მიღება ბიტკოინების სანაცვლოდ, არამედ საწინააღმდეგო ოპერაციის ჩატარებაც – კრიპტოვალუტის შეძენაც. მსოფლიოს ყველა ბიტკოინ-ავტომატის ნახევარზე მეტი აშშ-ის ტერიტორიაზე დგას, მაგრამ სხვა ქვეყნებიც ზრდიან მათ რაოდენობას. განსაკუთრებული

პოზიტიური დინამიკა კანადასა და ავსტრიაში აღინიშნება. სულ, ასეთი ბანკომატების დახლოებით სამი ათეული მწარმოებელი არსებობს, ერთი აპარატის ფასი დაახლოებით 10 000 დოლარია.

კრიპტოვალუტების მასობრივი გავრცელების ერთ-ერთი დაბრკოლებაა ვირტუალობა. ბევრი ადამიანისათვის, რომლებსაც საქმე მუდმივად აქვთ მონეტებთან და ბანკნოტებთან, ფულის ფორმა, რომელზეც ხელის შეხება არ შეიძლება, უჩვეულოა, განსაკუთრებით, თუ გავითვალისწინებთ, რომ მისი საქონლისა და მომსახურების შესაძენად გამოყენება ტექნოლოგიურად შედარებით რთულია. ფიზიკური ფული ხშირად ხდება კოლექციონირების საგანი, რაც კრიპტოვალუტისათვის ნაკლებად შესაძლებელია. 2011 წელს ვინმე მაიკ კალდველმა გადაწყვიტა გამოეშვა საკოლექციო ბიტკოინები ფიზიკური მონეტების სახით. მან შექმნა ბიტკოინებში ნომინირებული ლითონის მონეტების დიზაინი. ყოველ მონეტას შეესაბამებოდა კრიპტოსაფულე, რომელიც ნომინალის ტოლ ბიტკოინების რაოდენობას შეიცავდა. ამასთან, საფულის საიდუმლო გასაღები უშუალოდ მონეტაზე იყო დატანილი კოდის სახით და იფარებოდა სპეციალური ჰოლოგრამით, რომელიც აუცილებლობისას შეიძლებოდა წაგვეშალა და მიგვეღო წვდომა გასაღებსა და საფულის სახსრებთან. ნათელია, რომ ჰოლოგრამის წაშლის შემდეგ მონეტა ფაქტობრივად უსარგებლო ხდებოდა, რადგანაც გასაღები აღარავისთვის იყო საიდუმლო. გამოშვებული იქნა რამდენიმე ათასი ასეთი მონეტა, უმრავლესობა შეიძინეს კოლექციონერებმა და კრიპტოენთუზიასტებმა. შედეგად, სხვა მეწარმეებმაც სცადეს შეექმნათ ბიტკოინებში ნომინირებული მონეტები, მათ შორის – დიდი ნომინალების მქონე, მაგრამ ისინი ფართოდ ვერ გავრცელდა.

ბიტკოინზე როგორც გადახდის საშუალებაზე მსჯელობისას, ობიექტურობისათვის, ყურადღება უნდა გავამახვილოთ იმ შესაძლებლობების ნეგატიურ მხარეზეც, რომელსაც ბლოკჩეინ-ტექნოლოგიის ბაზაზე აგებული კრიპტოვალუტა იძლევა. საუბარია მის ერთ-ერთ ყველაზე მნიშვნელოვან თვისებაზე – ანონიმურობაზე. სწორედ კრიპტოვალუტურ გადახდებზე თვალყურის დევნებისა და ტრანზაქციის უშუალოდ მის ავტორთან, როგორც ფიზიკურ პირთან, დაკავშირების ტექნოლოგიურმა შეუძლებლობამ წარმოშვა მთელი კრიმინალური ინდუსტრია, რომელიც სხვადასხვა სახის უკანონო საქონელსა და მომსახურებას გვთავაზობს მხოლოდ კრიპტოვალუტებში. ამგვარი საქმიანობის წარმოქმნა და არსებობა გახდა ერთ-ერთი მთავარი ფაქტორი, რომლის გამოც კრიპტოვალუტებმა და კერძოდ ბიტკოინმა ვერ მიიღო ოფიციალური გადახდის საშუალების სტატუსი უმრავლეს სახელმწიფოში. მოდი მივმართოთ უშუალოდ საკითხის ისტორიას.

2011 წელს ინტერნეტქსელში საიტი SilkRoad (აბრეშუმის გზა) გამოჩნდა. ამ სავაჭრო პორტალზე შესაძლებელი იყო არალეგალური საქონლისა და მომსახურების ფართო სპექტრის შეძენა – ნარკოტიკების, მოპარული საბანკო ბარათების, ყალბი ფულისა და მკვლელის მომსახურებისაც კი. გამყიდველთა და მყიდველთა ანონიმურობის უზრუნველსაყოფად, მხოლოდ ბიტკოინებით გადახდის მეთოდით სარგებლობდნენ. საიტის მფლობელი იყო აშშ-ში მცხოვრები ვინმე როს ულბრიხტი, რომელსაც ექსტრემალური შეხედულებები ჰქონდა და უარყოფდა სახელმწიფოს ყოველგვარი ფორმით ჩარევას ადამიანთა ცხოვრებაში. საიტის გაყიდვების წლიური მოცულობა 2012-2013 წლებში დახლოებით 12-15 მილიონი აშშ დოლარით ფასდებოდა, ხოლო გარიგებების ჯამური მოცულობა კრიპტოვალუტურ ეკვივალენტში 10 მილიონ ბიტკოინს უახლოვდებოდა. სულ საიტის მომსახურებით დაახლოებით 100 000-მა მყიდველ-გამყიდველმა ისარგე-

ბლა. საბოლოოდ, ულბრიხტი დააკავეს და 2015 წელს სამუდამო პატიმრობა მიუსაჯეს, ხოლო საიტი SilkRoad დახურეს. მიუხედავად ამისა, თვით ასეთი სერვისის წარმოშობა და არსებობა შავ ლაქად დარჩა ბიტკოინის როგორც ინტერნეტში ანონიმური გადახდის საშუალების რეპუტაციაზე. შედეგად რიგ სახელმწიფოთა და რეგულატორთა ოფიციალურ პირებს ეს ისტორია მოჰყავდათ მაგალითად და ახსნად იმისა, თუ რატომ არის კრიპტოვალუტების გადახდის ოფიციალურ საშუალებად ცნობა ნაადრევი ან სულაც დაუშვებელი.

ციფრული ფულის დასაცავად შეიძლება იმ არგუმენტის მოყვანა, რომ ბევრი ჩვეული სასარგებლო ყოფითი ნივთი შეიძლება გამოვიყენოთ არა მარტო პირდაპირი დანიშნულებით, არამედ დაუფარავი კრიმინალური მიზნებისათვის. მაგალითად, სამზარეულოს ჩვეულებრივი დანები უამრავჯერ გამხდარა დანაშაულის იარაღი, მაგრამ მათი გაყიდვა და პროდუქტების დასაჭრელად გამოყენება კანონმდებლობით არასდროს ყოფილა აკრძალული მთელი მსოფლიოს სამზარეულოებში. ფულის ჩვეულებრივი კუპიურებიც მუდმივად გამოიყენება, პირველ რიგში, კორუფციული დანაშაულის ჩასადენად. მიუხედავად ამისა, ეს არ გამხდარა მიზეზი ბრუნვიდან მათი ამოღებისა გადახდის სხვა ფორმების სასარგებლოდ. იბადება ლოგიკური დასკვნა, რომ რიგი საყოფაცხოვრებო საგნების შესაძლო გამოყენება კრიმინალური მიზნებით არის ბუნებრივი შედეგი მათი არსებობისა, მაგრამ მათი აკრძალვა ადამიანებს უფრო მეტ ზიანს მოუტანდა, ვიდრე სარგებელს. ამიტომ სამართლიანი იქნებოდა, კრიპტოვალუტების მიმართაც გამოგვეყენებინა მსგავსი აწონილ-დაწონილი მიდგომა. მასობრივი აკრძალვების მაგივრად უნდა ვებრძოლოთ კრიპტოვალუტების შესაძლო უკანონო გამოყენებას და ამისათვის გამოვიყენოთ პროფესიული სახელმწიფო სამსახურები.

ბიტკოინისადმი მიძღვნილი ნაწილის დასრულებისას, კიდევ ერთხელ გვსურს აღვნიშნოთ, რომ ეს პროექტი გახდა ისეთი უახლესი მაღალტექნოლოგიური დარგის პიონერი, როგორსაც ბლოკჩეინი წარმოადგენს. მისი გამოჩენიდან თითქმის ათი წელი გავიდა და სავსებით ლოგიკურია, რომ ბევრს კრიპტოვალუტის ინდუსტრიაში ბიტკოინი მიაჩნია რამდენადმე მოძველებულ და თანამედროვე მოთხოვნებისთვის ნაკლებდამაკმაყოფილებელ პროექტად. მაგრამ სწორედ ასეთი კრიტიკოსების გამო გაუჩნდა ბიტკოინს კონკურენტები.

2019 წლის დასაწყისში ბლოკჩეინ-ინდუსტრიაში უკვე არსებობდა 2000-ზე მეტი სხვადასხვა კრიპტოვალუტა, რომლებსაც ერთი აქციის საბირჟო შეფასება მაინც ჰქონდა. ამ წიგნის ფარგლებში, რა თქმა უნდა, ვერ შევძლებთ ამ პროექტების უმრავლესობის განხილვას. მაგრამ შევჩერდებით ყველაზე მნიშვნელოვნებზე ე.წ. „ალტკოინების“ რიგიდან ანუ – ბიტკოინის ალტერნატიულ კრიპტოვალუტებზე. თითოეული ამ პროექტის მიზანი იყო, შეექმნა თავისი „წინაპრისაგან“ მომგებიანად განსხვავებული უნიკალური ფასეული წინადადება. მათ შორის პირველად უნდა განვიხილოთ Ethereum, რომელსაც ხანდახან „ბიტკოინ 2.0“-ს უწოდებენ იმის გამო, რომ ბლოკჩეინ-ტექნოლოგია განვითარების ახალ საფეხურზე აიყვანა.

Ethereum-ის შესავალი

ბიტკოინის ქსელის – ბლოკჩეინის ტექნოლოგიის ბაზაზე შექმნილი პირველი სისტემის გამოჩენიდან დაახლოებით ხუთი წლის შემდეგ ახალგაზრდა კრიპტოინდუსტრიაში საკმაო რაოდენობის პროექტი ბრუნავდა. უმრავლესობა მნიშვნელოვანწილად, „ბიტკოინის მაგვარი“ იყო და თავიანთი გენეზისური პირველსახიდან მხოლოდ წვრილმანი „კოსმეტიკური“ დეტალებით განსხვავდებოდა. თუმცა ბიტკოინიც, როგორც უმრავლესობა მისი შემდგომი კლონებისა, წარმოადგენდა ისეთსავე ჩვეულებრივ გადახდის დეცენტრალიზებულ სისტემას, საკმაოდ პრიმიტიულს თავისი შესაძლებლობებით. მიუხედავად ამისა, როცა ბლოკჩეინ-ტექნოლოგიის ყველა უპირატესობა შეაფასა, მის საფუძველზე ჩასახულმა ინდუსტრიამ დაიწყო მოთხოვნების ფორმირება ბლოკჩეინ-ქსელის უფრო რთული ფუნქციონირებისთვის. კრიპტოსაზოგადოებამ გაიაზრა უფრო პროგრესული ტექნოლოგიური საშუალებების მიღების აუცილებლობა, რომლებიც შესაძლებლობას მოგვცემდა, დაგვეწყო დეცენტრალიზებული პროექტების აგება ახალ ხარისხობრივ დონეზე.

ასეთი ინსტრუმენტი მართლაც, შემოთავაზებული იქნა 2013 წლის ბოლოს ერთ-ერთი კრიპტოენთუზიასტის მიერ, იმჟამად საზოგადოებისათვის ცნობილის როგორც ჟურნალ Bitcoin Magazine-ის რედაქტორი. ეს იყო ვიტალიკ ბუტერინი, რუსული ფესვების მქონე 19 წლის კანადელი პროგრამისტი, რომელმაც წარმოადგინა პროექტ Ethereum-ის აღწერა, რომლის შესაძლებლობებმაც მომეტებული ყურადღება მიიპყრო. Ethereum-ში წარმოდგენილი იყო სრულიად ახალი კონცეფციები, რომლებიც საკმაოდ აღემატებოდა ჩვეული ბლოკჩეინ-პროექტების პოტენციალის ფარგლებს. უფრო მეტიც, ეს პროექტი საერთოდ არ პოზიციონირდებოდა როგორც გადახდის სისტემა, არამედ წარმოადგენდა ახალი თაობის ბლოკჩეინ-პლატფორმას. მთავარი სიახლე გახდა ე.წ. „ჭკვიანი კონტრაქტების“ სისტემა ან, როგორც მიღებულია კრიპტოინდუსტრიაში, სმარტ-კონტრაქტების სისტემა. სმარტ-კონტრაქტების სტუქტურასა და მუშაობის პრინ-

ციპებს მოგვიანებით განვიხილავთ, ახლა კი აღვნიშნოთ ზოგიერთი თვისება, რომელიც პროექტ Ethereum-ს ბიტკოინისა და მსგავსი სისტემებისაგან განასხვავებს.

დავიწყოთ მისამართების ფორმირებით. ისევე, როგორც პროექტი „ბიტკოინი“, Ethereum-იც იყენებს მათი შექმნის მსგავს ალგორითმს, მაგრამ არ გარდაქმნის მათ წაკითხვად სახედ და საჯარო გასაღების ჰეშს პრაქტიკულად უცვლელად ტოვებს. ეს, ერთი მხრივ, იმიტომ გაკეთდა, რომ Ethereum-ი, როგორც ზემოთ აღინიშნა, თავიდანვე არ იყო ჩაფიქრებული გადახდის სისტემად. ამიტომ მისამართების ფორმირება უფრო მოსახერხებელი ვიზუალიზაციით, რაც ხელით აკრეფას ეხმარებოდა, ამ სისტემაში არ განხორციელდა. ადრესაციის ფორმირებაში განსხვავებების გარდა, პროექტის შემქმნელებმა მიიღეს გადაწყვეტილება, სისტემაში ბლოკები უფრო სწრაფად შეექმნათ, ვიდრე ბიტკოინ-ქსელში. თანაც მათი ზომა შეზღუდულია არა ბაიტების რაოდენობით, არამედ ბლოკის მონაცემთა დასამუშავებლად საჭირო გამომთვლელი სიმლავრეებით. ასეთი ზომები მართლაც გამართლებული იყო, რადგან სმარტ-კონტრაქტების არსებობა, როგორც მათი უფრო დაწვრილებით განხილვისას დავრწმუნდებით, შემმუშავებლებს ფაქტობრივად ავალდებულებს მსგავსი ლიმიტების შემოღებას.

მაინინგი Ethereum-ქსელში არსებითად განსხვავდება პრინციპებისაგან, რომლებითაც მუშაობს ბიტკოინი, თუმცა იგი ბლოკების მოსაძებნად ბიტკოინის მსგავსად მუშაობის დამტკიცების პრინციპს (Proof-of-Work) იყენებს. გამომთვლელი ამოცანის სირთულის მართვა, ისევე, როგორც ბიტკოინში, დამოკიდებულია ქსელის ერთობლივ ჰეშრეიტზე. ამასთანავე, სირთულის ხარისხი მნიშვნელოვნად შემცირებულია, ამიტომ Ethereum-ს ბლოკის შესაქმნელად ბევრად მცირე დრო სჭირდება. ამჟამად ქსელ Ethereum-ში ბლოკის შესაქმნელად საჭირო საშუალო დრო დაახლოებით ცამეტი წამია, ბიტკოინის 10 წუთის საპირისპიროდ, ანუ სანამ ბიტკოინ-ქსელში ერთი ბლოკი იქმნება, Ethereum-ში დაახლოებით ორმოცდაათი იქმნება. ამგვარად, Ethereum-ის ქსელის ბლოკებისა და ტრანზაქციების ბაზა უკვე შეგვიძლია შევადაროთ ბიტკოინისას, მიუხედავად იმისა, რომ Ethereum შეიქმნა ექვს-ნახევარი წლით გვიან, ვიდრე ბლოკჩეინ-ინდუსტრიის ფუძის ჩამყრელი პროექტი – ბიტკოინი. ქსელის შიგნით ანგარიშსწორებისათვის, მათ შორის ტრანზაქციის საკომისიოების გადასახდე-

ლად და მაინინგისათვის ანაზღაურების შესაქმნელად, გამოიყენება კრიპტოვალუტა „ეთერი“ (Ether). იმ შემთხვევაში, როცა მაინინგისას ვალიდური ჰეშის ძიების სირთულე შედარებით დაბალია, ქსელში ბლოკები საკმაოდ სწრაფად იქმნება. ეს ნიშნავს, რომ მაინინგისათვის ანაზღაურება პროპორციულად მცირეა და ღირებულების თვალსაზრისით, ვერაფრით შეედრება ბიტკოინის ქსელის ბლოკების შემქმნელთა პრემიას.

ბიტკოინ-ქსელში მაინინგის დეცენტრალიზებული პროცესის აღწერისას, განვიხილავდით კოლიზიის სიტუაციას იმ შემთხვევაში, თუ სხვადასხვა კვანძი ბლოკებს პოულობს დროის ათწუთიან ინტერვალში. ბლოკების ჯაჭვში ამ დროს წარმოქმნილი განშტოებები ქსელის მიერ საბოლოოდ გადაყრილი უნდა იქნას უფრო გრძელი ჯაჭვის სასარგებლოდ. მსგავსი მეთოდი Ethereum-ის ქსელშიც გამოიყენება. თუმცა, იმის გამო, რომ მასში ბლოკები იქმნება თითქმის ორმოცდაათჯერ უფრო სწრაფად, კონკურენტი ნაპოვნი ბლოკების სიტუაციის წარმოქმნა ამდენჯერვე ხშირად გვხვდება. ამიტომ Ethereum-ის ქსელს თითქმის ყოველთვის აქვს ალტერნატიული ჯაჭვები, რომლებიც საფრთხეს უქმნის ქსელის მთლიანობას, ასე რომ, გამუდმებით უნდა ვაკეთოთ არჩევანი სისტემისათვის უფრო ფასეული განშტოების სასარგებლოდ. ამისათვის Ethereum-ში გამოიყენება ოქმი GHOST (Greedy Heaviest Observed Sub Tree — „ხარბი და ყველაზე წონადი ცნობილი განშტოებებიდან“). ის უპირატესობას ანიჭებს იმ ბლოკებიან განშტოებებს, რომელთა მოპოვებაზეც მეტი გამოთვლები ჩატარდა.

იქიდან გამომდინარე, რომ კონკურენტი ბლოკები ძალძე ხშირად, თითქმის ერთდროულად იქმნება, დგება საკითხი, როგორ დავაჯილდოოთ მაინერები. თუ დავაჯილდოებთ მხოლოდ ერთ გამარჯვებულ მაინერს, მაშინ სხვებისათვის, რომლებმაც ასევე იპოვეს ბლოკი, ეს მნიშვნელოვანი დემოტივაცია იქნება. რადგან კონკურენტი მაინერები ისეთსავე რთულ გამოთვლით სამუშაოს ასრულებენ, სისტემის შემქმნელებმა გადაწყვიტეს, გასამრჯელოს ნაწილი მაქსიმუმ კიდევ ორ პარალელურად ნაპოვნ, მაგრამ ქსელისაგან უარყოფილი ბლოკის მპოვნელს მისცენ. ასეთ ბლოკებს უწოდეს uncles (ინგლისურად uncle — „ძია“), რადგან მათ საერთო „წინაპარი ბლოკი“ აქვთ. მათი შემქმნელი მაინერებიც იღებენ გარკვეულ პრემიას, ოღონდ ნაკლებს, ვიდრე ქსელისაგან როგორც ჭეშმარიტი, ისე მიღებული ბლოკების

შემქმნელები; ამისათვის, გასამრჯელოს განაწილების სპეციალური ფორმულა არსებობს.

ეთერების მაინინგის საკუთრივ პროცედურა ასევე განსხვავდება ბიტკოინ-პროექტისაგან. Ethereum-ის ქსელში გამოიყენება ვალიდური ჰეშების ძიების სრულიად განსხვავებული ალგორითმი, რომელსაც შემმუშავებლებმა Ethash უწოდეს. ბიტკოინების მოსაპოვებლად ელექტროენერგიის განსაკუთრებული ხარჯვის პრობლემა ყოველთვის იწვევდა პროექტ Ethereum-ის შემქმნელი ვიტალიკ ბუტერინის შეშფოთებას. ამიტომ მან თავის პროექტში გადაწყვიტა, შებრძოლებოდა ერთობლივი ჰეშრეიტის ჭარბ ზრდასა და პირველ რიგში, მაინინგისათვის ASIC მოწყობილობათა გამოყენებას. ამის გამო გადაწყდა ჰეშების გადარჩევის ალგორითმის გართულება იმ დონემდე, რომლის დროსაც საჭირო იქნებოდა მნიშვნელოვნად დიდი ოპერატიული მეხსიერება, ვიდრე ბიტკოინ-ქსელში გამოყენებულ SHA-256 ალგორითმს სჭირდება.

როგორც ცნობილია, მსხვილი მაინერები სერიოზულ გამომთვლელ სიმძლავრეებს იღებენ ASIC მოწყობილობებისაგან შედგენილი ფერმების კონსტრუირებისას. ფერმების არსებობა ნებისმიერი ბლოკჩეინ-ქსელისათვის ნეგატიურ ფაქტორად ითვლება, რადგანაც ისინი აძლიერებს მაინინგის ცენტრალიზების ხარისხს, ხოლო ეს, თავის მხრივ, ეწინააღმდეგება თავდაპირველად ჩაფიქრებულ გეგმას – ქსელის მართვისას მაქსიმალურად მოეშორებინათ გამომთვლელი სიმძლავრის ზედმეტი კონსოლიდაციის ყველა შესაძლო წერტილი. ვიტალიკ ბუტერინმა თავისი მრავალიდან ერთ-ერთ ინტერვიუში გვიამბო ისტორია იმის შესახებ, რომ ახალგაზრდობისას ბევრ დროს უთმობდა კომპიუტერულ თამაშს World of Warcraft. დროდადრო მისი ვირტუალური პერსონაჟი კარგავდა უნარ-ჩვევებს სათამაშო ბალანსის კორექციის გამო, რომელსაც, მოთამაშე საზოგადოების აზრის დაუკითხავად, პერიოდულად ატარებდნენ კომპანია Blizzard-ის შემმუშავებლები. თამაშის წესების ყოველი ასეთი ცვლილების შემდეგ ახალგაზრდა კაცი განიცდიდა ძლიერ ემოციურ დარტყმას იმის გამო, რომ მისი ძალისხმევა თავისი პერსონაჟის განსავითარებლად პრაქტიკულად ნულამდე დადიოდა. ეს ხდებოდა ცენტრალიზებულად მიღებული რომელიღაც გადაწყვეტილების გამო, რომელზეც მას პირადად ზემოქმედება ვერაფრით შეეძლო. ახალგაზრდობის დროინდელ-

მა ფსიქოლოგიურმა ტრავმამ მნიშვნელოვანი გავლენა მოახდინა ბუტერინის მსოფლმხედველობაზე, რის შედეგადაც მივიდა დასკვნამდე, რომ მართვის ცენტრალიზაცია აბსოლუტური ბოროტებაა.

მიუხედავად ბუტერინის მიერ მაინინგისათვის საჭირო მეხსიერების მოცულობისადმი მოთხოვნების გასაძლიერებლად მიღებული ზომებისა, Ethereum-ის ქსელის ASIC მოწყობილობების გაჩენისაგან სრულად დაცვა, სამწუხაროდ, მაინც ვერ მოხერხდა. სამაგიეროდ, მოხერხდა ჰეშრეიტის მნიშვნელოვანი შემცირება ამ სახის მოწყობილობებით კრიპტომონეტების მოსაპოვებლად, შედეგად, მაინინგის დეცენტრალიზაციის ხარისხის ამაღლება და ამის წყალობით, მისი კონკურენტუნარიანობის გაზრდა. თუ შევადარებთ მაინინგისათვის საჭირო ორ მოწყობილობას ბიტკოინისა და Ethereum-ის ქსელებისათვის, დავინახავთ, რომ მაინერი ეთერების მოსაპოვებლად ჰეშებს იძენს ათიათასჯერ უფრო ნელა, ვიდრე ბიტკოინური ანალოგი. ეს ხდება იმიტომ, რომ ეთერების მაინინგისას ალგორითმი Ethash ითვალისწინებს ოპერატიული მეხსიერებისადმი მუდმივ მიმართვას, სადაც მაინინგის პროცედურის კორექტული მუშაობისათვის აუცილებელი დამატებითი მონაცემებია განლაგებული. ეს ხშირი მიმართვა იმდენად ანელებს ალგორითმის მუშაობას, რომ ჰეშების გადარჩევის სიჩქარეების სხვაობა შეადგენს არანაკლებ ოთხი ხარისხისა.

ამ მიდგომამ შესაძლებლობა მოგვცა შეგვენარჩუნებინა ეთერის მონეტების მაინინგი ვიდეობარათების ჩვეულებრივი გრაფიკული პროცესორებით, რაც სერიოზულად ამაღლებს Ethereum-ის ახალი ბლოკების პოვნის პროცესის დეცენტრალიზაციის ხარისხს. მთლიანობაში კი ქსელი Ethereum ლამის სამჯერ ნაკლებ ელექტროენერგიას მოიხმარს, ვიდრე ბიტკოინ-ქსელი, თუმცა ეს სიდიდეც საკმაოდ მნიშვნელოვანია, ამიტომ Ethereum-ის პროექტის შემმუშავებლებს კვლავ სერიოზულად აღელვებთ მათი პროექტის ენერგოტევადობის პრობლემა და უახლოეს დროში გეგმავენ, რომ ძირეულად გადახედონ ქსელში ბლოკების შექმნის პრინციპს. ამჟამად ქსელი Ethereum, Proof-of-Work კონსენსუსის ოქმის საფუძველზე აგებულ მაინინგზე თანდათანობით უარის თქმისა და „ფლობის დამტკიცების“ (Proof-of-Stake) პრინციპზე გადასვლის პროცესშია, რაზეც ცალკე შევჩერდებით.

რაც შეეხება Ethereum-ის ქსელში ანგარიშგების მთავარ კრიპტოვალუტას – ეთერს, ბიტკოინისაგან განსხვავებით, რომლის გაყოფაც

100 მილიონ ნაწილადაა შესაძლებელი ან რომელსაც შეუძლია მიიღოს მინიმალური მნიშვნელობა მძიმის შემდეგ განთავსებულ მერვე ნიშანზე, ეთერი იყოფა კვინტილიონ ნაწილად ანუ მთელ 18 ათობით ნიშნად. ეთერის უმცირეს ნაწილაკს Wei ეწოდება – B-money პროექტის შემქმნელ ვეი დაის პატივსაცემად, ეთერის მემილიონედ ნაწილს – Szabo – ნიკ საბოს პატივსაცემად, რომელმაც გამოიგონა სმარტ-კონტრაქტები და შექმნა პროექტი BitGold, ბიტკოინის პროექტთან ყველაზე ახლო მდგომად რომ ითვლება. დაბოლოს, ეთერის მეათასედმა მიიღო სახელი Finney – ჰელ ფინის პატივსაცემად, რომელმაც სხვებთან ერთად შეიმუშავა კრიპტოგრაფიული PGP ოქმი და იყო სატოში ნაკამოტოს კონტრაგენტი ბიტკოინ-ქსელში პირველი გარიგების დროს, 2009 წლის იანვარში.

ბიტკოინისაგან კიდევ ერთ მნიშნელოვან განსხვავებას ის წარმოადგენს, რომ ამ დროისათვის ეთერების ემისია არანაირად არ არის შეზღუდული და ამგვარად, შეიძლება მომავალში ინფლაციას დაექვემდებაროს. როდესაც ვიტალიკ ბუტერინმა თავისი პროექტი წარმოადგინა, მან ერთდროულად შექმნა და ინვესტორებს ეთერის დაახლოებით 60 მილიონი მონეტა მიჰყიდა, რაშიც ბიტკოინებში დაახლოებით 18 მილიონი დოლარის ეკვივალენტი მიიღო. ეთერის კიდევ დაახლოებით 12 მილიონი მონეტა ბუტერინმა რეზერვში შეინახა პროექტის სამომავლო დაფინანსებისათვის. მონეტების ასეთ ერთდროულ გამოშვებას ჩვეულებრივ, „პრემაინინგს“ უწოდებენ.

თვით პლატფორმა გაშვებული იქნა 2015 წლის 30 ივლისს. მას შემდეგ გასული ოთხი წლის განმავლობაში მაინინგის უკვე ჩვეული პროცედურების საშუალებით განხორციელდა 30 მილიონ მონეტაზე ოდნავ მეტის ემისია. ამგვარად, მათმა საერთო რაოდენობამ 100 მილიონს გადააჭარბა, 20 მილიარდ აშშ დოლარზე ოდნავ ნაკლები მიმდინარე ერთობლივი კაპიტალიზაციით. ეთერი კრიპტოვალუტურ ინდუსტრიაში პოპულარობით მტკიცედ ინარჩუნებს მეორე ადგილს ბიტკოინების შემდეგ და მიმოქცევაშია თითქმის ყველა ბირჟაზე, რომლებიც კრიპტოვალუტით ვაჭრობის მომსახურებას გვთავაზობენ. თუ ბიტკოინს „კრიპტოვალუტურ ოქროს“ უწოდებენ, ეთერს „ვერცხლის“ ტიტული ხვდა წილად.

Ethereum-ის ქსელში ყოველდღიურად, მსოფლიოს მასშტაბით ნახევარ მილიონზე მეტი ტრანზაქცია ხორციელდება. თუ მივმარ-

თავთ მონეტების ბალანსის აღრიცხვის პრინციპს სისტემის მისამართებზე, მაშინ იკვეთება კიდევ ერთი მნიშვნელოვანი განსხვავება ბიტკოინ-ქსელისაგან. როგორც ცნობილია, ტრანზაქციები ბლოკჩეინში ელექტრონული ხელმოწერების ჯაჭვს წარმოადგენს, რომლებზე თვალყურის დევნებაც ბლოკების მთელ ბაზაშია შესაძლებელი. ამგვარად, ყოველთვის არსებობს ნებისმიერი მისამართის ბალანსის ავტომატურად გაანგარიშების შესაძლებლობა, თუ შესავლებს როგორც შემოსავალს და გასავლებს როგორც დანახარჯს, ისე შევადარებთ. სწორედაც დაუხარჯავი გასავლები იქნება მისამართის მიმდინარე ბალანსი. ამ პრინციპს ეწოდება UTXO ანუ „დაუხარჯავი ტრანზაქციური გამოსავლების აღრიცხვა“, რასაც გარკვეული დრო უკვე დავუთმეთ. Ethereum-ის ქსელში გადაწყვიტეს, რომ მიზანშეწონილი იქნებოდა, ქსელის ყოველი მისამართისათვის შემოღებული ყოფილიყო მიმდინარე მდგომარეობის ბაზა. აღრიცხვის ეს მეთოდი, მართალია, დამატებით გარკვეული მონაცემების შენახვას მოითხოვს, მაგრამ მაინც შეუდარებლად უფრო მოსახერხებელია UTXO პრინციპთან შედარებით, რომლის დროსაც მუდმივად საჭიროა გაანგარიშების საშუალებით მისამართების აქტუალური მდგომარეობის მიღება.

ამავდროულად, აქტუალური მდგომარეობის შენახვის პრინციპმა შემმუშავებლებს შესაძლებლობა მისცა, Ethereum-ის პლატფორმაში შეეტანათ მისი წარმოქმნის მომენტისათვის უნიკალური სმარტ-კონტრაქტების ფუნქციონალი, სახელდობრ ის, რომელიც პროექტის მთავარ ფასეულ შეთავაზებად იქცა. რა არის სმარტ-კონტრაქტები და Ethereum-ის ქსელში მათმა რეალიზაციამ როგორი გავლენა მოახდინა მთლიანად ბლოკჩეინ-ტექნოლოგიის განვითარებაზე?

სმარტ-კონტრაქტები

ახალი ტექნოლოგიების დანერგვის პროცესში შემმუშავებლები, რომლებიც გადახდის საშუალებად ბიტკოინს იყენებდნენ, გამუდმებით ეჯახებოდნენ ტრანზაქციების ჩატარების უფრო რთული მოდელების შექმნის პრობლემას, განსაკუთრებით ისეთ სისტემებში, რომლებშიც სტანდარტულისაგან განსხვავებული პირობების არსებობა იყო შესაძლებელი. სატოში ნაკამოტო ცდილობდა ასეთი სიტუაციის გათვალისწინებას და ბიტკოინ-ქსელის კლიენტის პროგრამული რეალიზაციის პირველსავე ვერსიიდან დაწყებული, მასში მოათავსა ე.წ. სკრიპტების სისტემა ტრანზაქციების დასამუშავებლად. ფაქტობრივად ეს იყო სტეკის ტიპის პროგრამირების ენის გამარტივებული ფორმა, როდესაც მისი ყველა ბრძანება მუშავდება რიგის მიხედვით მარცხნიდან მარჯვნივ იმის მიხედვით, როგორც იყო ისინი თვით სკრიპტში მითითებული.

ბიტკოინის სკრიპტ-ენა შეიცავს დაახლოებით ოთხმოც ათეულ სხვადასხვა ბრძანებას, რომელთაგან თითოეული გარკვეულ ალგორითმულ ოპერაციას ასრულებს – ელემენტარულიდან, ორი რიცხვის შედარების მსგავსით დაწყებული, უფრო რთული მონაცემთა ჰეშირებით და ციფრული ელექტრონული ხელმოწერების შემოწმების ალგორითმით დამთავრებული. შემთხვევათა დიდ უმრავლესობაში ყოველი ტრანზაქციის გამოსავლის პარამეტრებში თავსდება სდანდარტული სკრიპტი სახელად P2PKH, ან Pay to Public Key Hash. ეს სკრიპტი ახორციელებს საჯარო გასაღების გადახდის პროცედურას ჰეშზე, რომელიც, სახელდობრ, წარმოადგენს ტრანზაქციის მიმღების ბიტკოინ-მისამართს.

გადახდების არასტანდარტული სიტუაციების დამუშავებისათვის გამგზავნმა შეიძლება შეადგინოს თავისი სკრიპტი, რომელიც ტრანზაქციის დასამუშავებელ დამატებით პირობებს შეიცავს. თუმცა, უნდა ითქვას, რომ მას დიდი არჩევანი არ აქვს. მაგალითად, არსებობს შესაძლებლობა მულტიხელმოწერის ფუნქციონალის რეალიზებისა ან იმგვარად გაკეთებისა, რომ გაგზავნილი სახსრების დახარჯვა სკრიპტში მითითებულ განსაზღვრულ დრომდე არ შეიძლებოდეს.

მაგრამ ამგვარი საშუალებებით, ტრანზაქციების დასამუშავებელი, პარამეტრების დამატებითი ნაკრებით აღჭურვილი მართლაც რთული ალგორითმული კონსტრუქციების შექმნა პრაქტიკულად შეუძლებელია. თან, აქ პრობლემა მარტო ბიტკოინ-სკრიპტში ბრძანებების შეზღუდული ნაკრები კი არა, არამედ უფრო ისაა, რომ ეს ენა არის „არასრული, ტიურინგის მიხედვით“. რას ნიშნავს ეს?

1936 წელს, გერმანულ დასაშიფრ მოწყობილობა „ენიგმასთან“ კრიპტოგრაფიული ბრძოლის მომავალმა გმირმა ალან ტიურინგმა შემოგვთავაზა გამომთვლელი მანქანის მოდელი მათემატიკური აბსტრაქციის ფორმით. მიღებულ მოდელს შემდგომში „ტიურინგის მანქანა“ უწოდეს. ეს ლოგიკური გამომთვლელი კონსტრუქცია გახდა ინსტრუმენტი სხვადასხვა ამოცანის ალგორითმული ამოხსნის არსებობის ან არარსებობის დასამტკიცებლად. რაც შეეხება „სისრულეს ტიურინგის მიხედვით“, მისი ერთ-ერთი კრიტერიუმია პროგრამირების ენაში ბრძანებების არსებობა, რომელთა ბაზაზეც შეიძლება ალგორითმული ციკლების აგება. ბიტკოინ-ქსელის სკრიპტ-ენას არა აქვს ციკლების დამმუშავებელი ოპერატორები ანუ მასზე რთული გამომთვლელი ალგორითმების რეალიზების შესაძლებლობა ძალზე შეზღუდულია. ბიტკოინისაგან განსხვავებით, პროექტ Ethereum-ში ამგვარი შესაძლებლობა გათვალისწინებულია, ხოლო ის განხორციელებულია სწორედ სმარტ-კონტრაქტების ფუნქციონალის გამოყენებით. ვცადოთ გავერკვეთ, რას წარმოადგენს ისინი?

როგორც უკვე არაერთხელ აღინიშნა, კონცეფციის ავტორი გახლდათ ნიკ საბო, რომელმაც ჯერ კიდევ 1994 წელს პირველად წარმოადგინა შესრულებადი ელექტრონული კონტრაქტების ფორმა დეცენტრალიზებულ სისტემაში. საბომ ვირტუალური შეთანხმების ეს ფორმა განსაზღვრა როგორც „ინფორმაციის გადაცემის ოქმი, რომელიც უზრუნველყოფს მხარეების მიერ გარიგების პირობების ავტომატურ შესრულებას“. კონტრაქტების დადების ასეთი ფორმის უპირატესობებად ავტორი თვლიდა კონფიდენციალურობას, ოპერაციის ჩატარების დაბალ დანახარჯებსა და გარიგებებში მხარეთა ნდობის უზრუნველსაყოფად შუამავლების მოწვევის აუცილებლობის არარსებობას. თუ ელექტრონულ კონტრაქტებს ჩვეულებრივებს შევადარებთ, მაშინ დავინახავთ, რომ აშკარა განსხვავებას წარმოადგენს სმარტ-კონტრაქტის შესაძლებლობა, გააკონტროლოს გარიგების

მხოლოდ მათემატიკურად დამტკიცებადი პირობები, იმ დროს, როდესაც ჩვეულებრივ კონტრაქტში გადმოცემული პირობები შეიძლება იყოს არამკაფიო, ანუ – აღწერითი ხასიათი ჰქონდეს. საბოლოოდ, ნიკ საბო შემოიფარგლა თავისი მოდელის მხოლოდ თეორიული წარდგენით, ხოლო ამ კონცეფციის უშუალო რეალიზაციამ დღის სინათლე მხოლოდ ორი ათეული წლის შემდეგ, პროექტ Ethereum-ში იხილა.

სმარტ-კონტრაქტის ფორმირების პროცესი მთლიანობაში ჩვეულებრივ ტრანზაქციას ჰგავს, რომელიც დამატებითი ელემენტების რიგს შეიცავს და რომლებიც მას უნიკალურ თვისებებს ანიჭებს. პირველ რიგში საუბარია პროგრამულ კოდზე, რომელიც დეცენტრალიზებულ შესრულებას ექვემდებარება ე.წ. Ethereum-ის ვირტუალური მანქანის (EVM) საშუალებით, უშუალოდ ქსელის ბლოკების შემქმნელ კვანძებზე. სმარტ-კონტრაქტის კოდში აღწერილია ქსელის მომხმარებელსა და სმარტ-კონტრაქტის მფლობელს შორის, რომელმაც იგი ბლოკჩეინში მოათავსა და ამგვარად აამოქმედა, გარიგებების დასამუშავებელი არითმეტიკული ლოგიკა. ამ მომენტიდან სმარტ-კონტრაქტი არსებობს ჯაჭვის ერთ-ერთ ბლოკში და ქსელის ნებისმიერ მსურველ წევრს შეუძლია მისი მუშაობის გააქტიურება სისტემაში კონტრაქტის მისამართზე ტრანზაქციის გაგზავნის გზით. ამგვარად, სმარტ-კონტრაქტი სისტემის სრულუფლებიანი სუბიექტია, რომელსაც ტრანზაქციების მიღება და ფორმირება შეუძლია. მაგრამ ის ამას დამოუკიდებლად კი არ აკეთებს, არამედ მხოლოდ მაშინ, როცა კოდის კონტრაქტი შესასრულებლად გაიშვება ვირტუალური მანქანა Ethereum-ის საშუალებით მაინერის კვანძზე ბლოკების ნაკრების შექმნისას. როგორ მიმდინარეობს ეს პროცესი?

სიმარტივისთვის სმარტ-კონტრაქტი შეიძლება შევადაროთ სავაჭრო ავტომატს, რომელიც ყიდის, მაგალითად, სასმელებს. მყიდველი ავტომატში ათავსებს გარკვეულ თანხას ნაღდი ფულის სახით ან საბანკო ბარათის საშუალებით, ხოლო აპარატი იძლევა არჩეულ საქონელს შეტანილი სახსრების შესაბამისად. თუ ამ სიტუაციას დავაპროეცირებთ ბლოკჩეინ-ქსელზე, მაშინ სმარტ-კონტრაქტის აქტივაცია ხდება იმ მომენტში, როდესაც ბლოკში თავსდება ტრანზაქცია, რომელიც კონტრაქტის მისამართით რაღაც კრიპტოვალუტურ აქტივებს გზავნის. ასეთი ტრანზაქციის დამუშავებისას მაინერი პოულობს ბლოკს, სადაც მოთავსებულია სმარტ-კონტრაქტი, და ვირტუალური

მანქანის დახმარებით უშვებს მის კოდს დასამუშავებლად, დასვამს რა მას ამ ტრანზაქციის შესავალზე. სმარტ-კონტრაქტის ქმედების შედეგი შეიძლება სხვადასხვაგვარი იყოს, რაც თვით კონტრაქტის კოდში ჩადებული ალგორითმის ლოგიკითაა განპირობებული. ეს შეიძლება იყოს უბრალო ცვლილებები სისტემის მდგომარეობაში ანდა კონტრაქტის მიერ საპასუხო ტრანზაქციების ჩამოყალიბება – ერთის ან რამდენიმესიც კი. ასევე არ უნდა დავივიწყოთ, რომ სმარტ-კონტრაქტები გაიშვება არა მხოლოდ მაინერების მიერ, არამედ ჩვეულებრივი კვანძების მიერაც. ეს ხდება მომენტებში, როდესაც ისინი ამუშავებენ სმარტ-კონტრაქტებთან დაკავშირებულ ტრანზაქციებს, მათ შორის – მაინერებისაგან მიღებული ბლოკების ვალიდურობაზე შემოწმების დროსაც. ასეთი ოქმი, ერთი მხრივ, გვთავაზობს გარკვეულ გამოთვლით სიჭარბეს, ხოლო მეორე მხრივ, უზრუნველყოფს მთლიანობაში სისტემის სტაბილური მუშაობის დამატებით გარანტიებს.

ბიტკოინის სკრიპტ-ენისაგან განსხვავებით, სმარტ-კონტრაქტების კოდი იწერება პროგრამირების ენებზე, რომლებიც ტიურინგის სისრულის კრიტერიუმებს აკმაყოფილებს. Ethereum-ის სმარტ-კონტრაქტების ყველაზე გავრცელებული ობიექტურად ორიენტირებული ენაა Solidity, რომელიც სემანტიკურად ჰგავს პროგრამირების პოპულარულ ენას JavaScript. თუმცა, სმარტ-კონტრაქტის სხეულში ათავსებენ არა უშუალოდ საწყის კოდს, რომელიც, მაგალითად, დაწერილია იმავე Solidity-ით, არამედ კომპილაციის პროცედურაგავლილ ე.წ. „ბაიტ-კოდს“. ეს კოდი წარმოადგენს დაბალი დონის ბრძანებების ნაკრებს, რომელიც ვირტუალური მანქანა Ethereum-სათვისაა განკუთვნილი.

იმის ძალით, რომ ნებისმიერი ბლოკჩეინ-სისტემა წარმოადგენს დეცენტრალიზებულ გარემოს, სადაც ყოველი ბლოკი და ყოველი ტრანზაქცია ხელმისაწვდომია შესასწავლად ქსელის ნებისმიერი მონაწილისათვის, Ethereum-ის სმარტ-კონტრაქტებიც გამონაკლისს არ წარმოადგენს. მაგრამ რადგან კონტრაქტი ინახება ბლოკჩეინ-ბაზაში ბაიტ-კოდის ფორმატში, იმისათვის, რომ გავერკვეთ მისი მუშაობის პრინციპში, გამოიყენება სპეციალური დეკომპილატორები. ეს არის პროგრამები, რომლებსაც კოდი შედარებით „წაკითხვად“ სახემდე მიჰყავს, თუმცა – საწყისიდან დაშორებულ, იმისაგან დაშორებულ სახემდე, რომელზეც ის თავიდანვე იყო შექმნილი სმარტ-კონტრაქ-

ტის პროგრამისტის მიერ. დეკომპილატორს არ შეუძლია აღადგინოს ცვლადების საწყისი დასახელებები, ასევე, პროგრამისტისაგან თავისი კოდისათვის გაკეთებული ყველა კომენტარი. ამგვარად, ალგორითმის საწყისი ლოგიკის აღდგენა სმარტ-კოდის დეკომპილაციის პროცესის შემდეგ რთული ხდება. თუმცა, არის საწინააღმდეგო შემთხვევებიც, როდესაც სმარტ-კონტრაქტების შემქმნელები აქვეყნებენ საკუთარი კოდის საწყის ტექსტს, რათა უზრუნველყონ მეტი გამჭვირვალობა და ნდობა თავისი ალგორითმებისადმი. პუბლიკაციისათვის გამოიყენება გარე ინტერნეტრესურსები, სადაც შესაძლებელია კოდების ტექსტების გაცნობა ადვილად წაკითხვადი ფორმით, რომელიც აუცილებელ კომენტარებს შეიცავს.

როგორც ნებისმიერ ჩვეულებრივ კომპიუტერულ პროგრამას, სმარტ-კონტრაქტსაც აქვს სხვადასხვა სახის ფუნქციური შესაძლებლობები ანუ ზოგიერთი სმარტ-კონტრაქტისათვის საკმარისია კოდის რამდენიმე სტრიქონი, სხვებს შეიძლება ჰქონდეს რთული ალგორითმები, რომლებიც ასეული და ათასეული სტრიქონისგანაც კი შედგება. ეს პირველ რიგში გვიჩვენებს, რომ გამომთვლელი ძალისხმევით სმარტ-კონტრაქტები თანაბარუფლებიანები სულაც არ არის, თითოეულის დასამუშავებლად საჭიროა სხვადასხვა პროცესორული დრო. აქედან ჩნდება ლოგიკური კითხვა: როგორ შევქმნათ მაინერის მოტივაცია მსგავსი კონტრაქტების დამუშავებისას? რა იქნება, თუ სმარტ-კონტრაქტის კოდი შეიცავს, მაგალითად, უსასრულო ციკლს, რომელიც დამმუშავებლის კომპიუტერს „დაკიდებს“, როდესაც ის უსასრულოდ ეცდება წრეზე შეასრულოს ოპერაციათა ერთი და იგივე ერთობლიობა? ასეთი სიტუაციებისაგან დასაცავად Ethereum-ში გათვალისწინებულია გამომთვლელი სიმძლავრის ანაზღაურება სმარტ-კონტრაქტების დასამუშავებელი სპეციალური „საწვავის“ საშუალებით. Ethereum-ში ასეთ „საწვავს“ ჩვეულებრივ, „გაზს“ უწოდებენ, რადგან ეს ტერმინი შეესატყვისება მის ინგლისურ დამწერლობას (gas), თუმცა ამ სიტყვის სხვა თარგმანებიც არსებობს.

რამდენად უცნაურიც არ უნდა იყოს, Ethereum-ის ქსელის მთავარი საანგარიშგებო კრიპტოვალუტა – ეთერი შექმნილია პირველ რიგში, უმნიშვნელოვანესი უტილიტარული მიზნისათვის – აანაზღაუროს გაზის ფასი სმარტ-კონტრაქტების დასამუშავებლად. თვით გაზი თვლადი სიდიდეა, მაგრამ – არამონეტარული, და პირდაპირ

ასახავს მაინერის მიერ სმარტ-კონტრაქტის კოდის გასაშვებად დახარჯული გამომთვლელი რესურსების მოცულობას. Ethereum-ის ქსელის ბაიტ-კოდის ყოველი ოპერატორისათვის არსებობს გაზის ერთეულებში ნომინირებული ფიქსირებული „ღირებულება“. არითმეტიკული მოქმედებების მსგავსი მარტივი ოპერატორები „ღირს“ უფრო იაფი, მაშინ, როდესაც რთული, – მაგალითად, ჰეშირების პროცედურებისა – უფრო ძვირი. ამგვარად, სისტემაში თავიდანვე იყო ჩადებული რაღაც „პრაისლისტის“ მსგავსი, რომლის საფუძველზეც ყოველთვის შეიძლება გამოითვალოს, რამდენი გაზი დაიხარჯება კონკრეტული სმარტ-კონტრაქტის დამუშავებაზე. რადგან ჩვეულებრივი ტრანზაქციები კრიპტოვალუტის ერთი ადრესატიდან მეორისათვის გადასარიცხად ასევე მოითხოვს გამოთვლით დამუშავებას, ამიტომ მათაც აქვს საკუთარი „გაზობრივი ღირებულების“ ეკვივალენტი. ჩვეულებრივ, სტანდარტული ტრანზაქცია ღირს 21 000 გაზი, საკითხი მხოლოდ ისაა, რა ღირს თვით გაზი.

ფასწარმოქმნა გაზზე ყოველთვის დამოკიდებულია Ethereum-ის ქსელის მიმდინარე დატვირთვაზე. თუ დამუშავებისა და ბლოკში ჩართვის რიგში ბევრი ტრანზაქცია დგას, მაშინ მაინერები პრიორიტეტს ანიჭებენ იმათ, რომელთა გამგზავნებმა გაზის უფრო მაღალი ფასი მიუთითეს. Ethereum-ის ქსელის კლიენტის პირველი ვერსიის სტარტის წინ დადგინდა, რომ გაზის ერთეული ეღირება 10 000 Gwei ანუ ეთერის ერთი მეასიათასედი. ამჟამად ეს ფასი მეტისმეტად დიდად ჩაითვლებოდა, რადგან ეთერის მონეტების ფასი პროექტის გაშვების მომენტიდან ძალზე მნიშვნელოვნად გაიზარდა, თუმცა შორს არის საკუთარი ისტორიული მაქსიმუმისაგან. მიუხედავად ამისა, თუ გაზს ამ ფასად ვიყიდით, მაშინ ჩვეულებრივი ტრანზაქციის გაგზავნა ამჟამად დაახლოებით 30 აშშ დოლარი დაგვიჯდება.

გასაგებია, რომ ეთერის მონეტის ღირებულების ზრდასთან ერთად, გაზის ფასი პროპორციულად ეცემოდა, გარდა იმ ხანმოკლე პერიოდებისა, როდესაც ქსელზე დატვირთვა მნიშვნელოვნად იზრდებოდა. ამ შემთხვევაში, ტრანზაქციის გამგზავნები იბრძოდნენ უახლოეს შესაქმნელ ბლოკში მათი პრიორიტეტული ჩართვისათვის გაზზე ფასის გაზრდის გზით. 2019 წლის გაზაფხულისათვის გაზის საშუალო ღირებულება 2-4 Gwei-ის ფარგლებში მერყეობდა, რაც ჩვეულებრივი ტრანზაქციის საკომისიოს ერთ-ორ ამერიკულ ცენტს

უთანაბრებს. ტრანზაქციის გაგზავნისას შეიძლება მიეთითოს გაზის უფრო მცირე ფასი, ვიდრე მიმდინარე საბაზროა. ამ შემთხვევაში ტრანზაქცია დამუშავდება უფრო ხანგრძლივად, ვიდრე ჩვეულებრივ, ხოლო თუ წარდგენილი ფასი საბაზროზე ბევრად მცირეა, მაშინ ის შეიძლება საერთოდაც ვერ მოხვდეს დასამუშავებელთა შორის.

ქსელში ტრანზაქციის გაგზავნისას სმარტ-კონტრაქტთან საურთიერთობოდ, გამგზავნმა მხოლოდ დაახლოებით შეიძლება ივარაუდოს, რა მოცულობის გაზი დასჭირდება მის დამუშავებას. ამიტომ ის უთითებს არა გაზის ზუსტ მნიშვნელობას, არამედ სიდიდეს ჭარბად ანუ გაზის მაქსიმუმს ტრანზაქციისათვის, რომლის „დაწვის“ უფლებასაც ის თავს მისცემს. ზუსტ მნიშვნელობას უთითებს მაინერი ტრანზაქციისა და სმარტ-კონტრაქტების უშუალო დამუშავებისას, თანაც გამომგზავნს გადაახდევინებენ ზუსტად რეალურად დახარჯულ მოცულობას, ხოლო გამოუყენებელი ნაშთი უკან დაუბრუნდება. იმ შემთხვევაში კი, თუ გაზის ლიმიტი სმარტ-კონტრაქტის დასამუშავებლად საკმარისი არ აღმოჩნდება, მისი შესრულება ვადამდე შეჩერდება და „გარიგება“ არ შედგება. ამასთან, უკვე გამოყენებული გაზი უკან არ დაუბრუნდება, ხოლო მისი ღირებულება მაინერის შემოსავალში წავა.

თუ ბლოკის ყველა, მათ შორის სმარტ-კონტრაქტებთან დაკავშირებულ ტრანზაქციას გავაანალიზებთ, შეგვიძლია ვიანგარიშოთ გაზის ერთობლივი მოცულობა, რომელიც საჭიროა მთელი ბლოკის დასამუშავებლად. ამიტომ Ethereum-ის ქსელში ბლოკის ზომა შეზღუდულია არა მოცულობითი ბაიტებით, როგორც ბიტკოინში, არამედ ერთი ბლოკისათვის დასაშვები გაზის მაქსიმალური რაოდენობით. გამოდის, რომ ბლოკში შეიძლება იყოს ტრანზაქციების მცირე რაოდენობაც, მაგრამ ბევრი მათგანი ძალზე „გაზხარჯიანი“ შეიძლება იყოს, ამიტომ ლიმიტს შეიძლება ძალზე სწრაფად მივაღწიოთ. მიმდინარე მომენტისათვის ლიმიტი ერთ ბლოკზე შეადგენს დაახლოებით გაზის 8 მილიონ ერთეულს, რაც საშუალებას იძლევა, Ethereum-ის ერთ ბლოკში მოვათავსოთ მაქსიმუმ ოთხ ასეულზე ოდნავ ნაკლები სტანდარტული ტრანზაქცია. ვარაუდობენ, რომ ბლოკზე გაზის ლიმიტი გაიზრდება ქსელის კვანძების გამომთვლელი შესაძლებლობების ბუნებრივ ზრდასთან ერთად.

ახლა გასაგები ხდება, რატომ აქვს სმარტ-კონტრაქტების კონცეფციას აშკარა უპირატესობა ჩვეულებრივ კონტრაქტებთან შედარებით. თუმცა, არ შეიძლება გამოგვრჩეს, რომ აქაც არსებობს თავისი სისუსტეები. რადგან სმარტ-კონტრაქტები იქმნება თვით ქსელის წევრების მიერ, ამ პროცესში მონაწილეობს ე.წ. „ადამიანური ფაქტორი“, მაგალითად, ისეთი, როგორიცაა ალგორითმებისა და პროგრამული კოდების შემქმნელი პროგრამისტების პროფესიული კვალიფიკაცია. პროექტ Ethereum-ის არსებობის რამდენიმე წლის მანძილზე აღნიშნული იქნა ბევრი შემთხვევა, როდესაც შეცდომები, დაშვებული პროგრამისტების მიერ სმარტ-კონტრაქტების კოდების დაწერისას, სერიოზულ ფინანსურ დანაკარგებს იწვევდა.

ეს ფაქტი ხშირად გამოიყენება ამგვარი სისტემების კრიტიკული შეფასებისას, რადგან მისი თავიდან აცილება ძნელია ქსელის სრული ღიაობისა და დეცენტრალიზაციის გამო. 2018 წლის თებერვალში ექსპერტთა გაერთიანებულმა ჯგუფმა განაცხადა, რომ Ethereum-ის ქსელის დაახლოებით 34 000 სმარტ-კონტრაქტს აქვს პრობლემები და სისუსტეები, რომლებსაც მათი მფლობელები ჯერჯერობით ვერ ხვდებიან. იყო შემთხვევები, როცა სმარტ-კონტრაქტების კოდებში შეცდომების გამო ბოროტმოქმედები ათეულობით მილიონ დოლარს იპარავდნენ. იმისათვის, რომ რისკების მინიმიზება მოახდინონ, სმარტ-კონტრაქტების ავტორებს ურჩევენ, მეტი დრო დაუთმონ მათ ტესტირებას, ასევე, დარგის აღიარებულ პროფესიონალებს კოდის აუდიტი შეუკვეთონ.

დაბოლოს, დადგა დრო, განვიხილოთ, როგორი ფუნქციები ახდენს ძირითად გავლენას Ethereum-ის ქსელში სმარტ-კონტრაქტებზე ამჟამად. სტატისტიკის თანახმად, ქსელში სულ განთავსებული იქნა 2 მილიონ სმარტ-კონტრაქტზე ოდნავ ნაკლები, რომელთაგან დაახლოებით ნახევარი მილიონი „აქტიურ“ მდგომარეობაში იმყოფება. სმარტ-კონტრაქტებთან დაკავშირებული ტრანზაქციების საერთო რაოდენობა 100 მილიონზე მეტად ფასდება. დეცენტრალიზებული კრიპტოვალუტური ბირჟების საქმიანობისთვის შექმნილი სმარტ-კონტრაქტების გარკვეული რაოდენობა უზრუნველყოფდა კონტრაგენტებს შორის ბირჟების გარე გარიგებების მხარდაჭერას, ასევე კრიპტოთამაშების ორგანიზაციას, რომელთაგან ზოგიერთმა ფართო პოპულარობა მოიპოვა. და მაინც, სმარტ-კონტრაქტების

უმრავლესობა გამოყენებული იქნა ციფრული კრიპტოჟეტონების ანუ ე.წ. ტოკენების გამოშვებისა და მიმოქცევის უზრუნველსაყოფად. სწორედ პროექტმა Ethereum მისცა სტარტი ძალზე საინტერესო და მასშტაბურ მოვლენას ციფრულ დეცენტრალიზებულ სამყაროში, რომელსაც „ტოკენიზაცია“ ეწოდება და რომლის აღწერაც დაწვრილებით თხრობას მოითხოვს.

ტოკენიზაცია

ყოველ ბლოკჩეინ-პლატფორმას აქვს საკუთარი ძირითადი კრიპტოვალუტა მონეტების ან, როგორც მათ ასევე უწოდებენ, კოინების სახით – ინგლისურიდან coin („მონეტა“). საკუთარი კრიპტოვალუტის ემისია ჩვეულებრივ ნაკარნახევია იმ კვანძებისათვის მონეტარული მოტივაციის შესაქმნელად, რომლებიც ქსელის სტაბილურ მუშაობას განაპირობებს. კერძოდ, ბიტკოინის ან Ethereum-ის პროექტებში არსებობს საკუთარი საბაზო კრიპტოვალუტები, რომლებსაც იყენებენ როგორც მაინინგური ანაზღაურების გასაცემად, ასევე ტრანზაქციური საკომისიოების გადასახდელად. დამატებით ეს კრიპტოვალუტები გამოიყენება კიდევ გადახდის საშუალებად და როგორც ინვესტიციის ინსტრუმენტიც კი. თუმცა, მაგალითად, Ethereum-ის პროექტის თავდაპირველი იდეა მონეტების ამგვარ გამოყენებას არ ითვალისწინებდა, მაგრამ ეს გახდა პროექტის შესაძლებლობების ექსპლუატაციის ერთ-ერთი ბუნებრივი შედეგი. იმ დეცენტრალიზებული პროექტების მხარდასაჭერად, რომლებსაც სურდათ საკუთარი ციფრული აქტივების ქონა, Ethereum-ის პროექტმა მათი შექმნის შესაძლებლობა წამოაყენა. აქტივების ასეთ ტიპს უწოდეს ციფრული კრიპტოჟეტონები ან უბრალოდ ტოკენები (ინგლისურიდან token — „ჟეტონი“). ძირითადი განსხვავება ტოკენებსა და კოინებს შორის არის საკუთარი ბლოკჩეინ-ინფრასტრუქტურის არარსებობა; ისინი გახდა ტექნოლოგიური ზედნაშენი უკვე არსებული ქსელისა, რომელიც უზრუნველყოფს მათ ემისიას და დეცენტრალიზებულ მიმოქცევას.

რისთვის შეიძლება დასჭირვებოდათ Ethereum-ის ქსელის ბაზაზე პროექტების შემქმნელებს საკუთარი ტოკენები და რატომ არ მოისურვეს მათ საკუთარი საჭიროებისათვის ქსელის უკვე არსებული კრიპტოვალუტა ეთერის გამოყენება? პირველ რიგში, მათ არ სურდათ, დამოკიდებულნი გამხდარიყვნენ მონეტა ეთერის ფასობრივ საბაზრო კონიუნქტურაზე. პროექტის საბაზო კრიპტოვალუტის ფასების რყევა საკმაოდ მნიშვნელოვანი შეიძლება ყოფილიყო და, როგორც შემდგომმა მოვლენებმა გვიჩვენა, ეს ვარაუდი სწორი

აღმოჩნდა. მაგრამ მთავარი მიზეზი ის ფაქტი იყო, რომ ეთერი ყველა პროექტს არ ერგებოდა, რადგან მათი მოთხოვნები ჩვეულებრივი კრიპტომონეტების თვისებების ფარგლებს სცდებოდა. ზოგ პროექტს დაუდგა აუცილებლობა, შეექმნა ციფრული აქტივების ახალი ტიპი, რომლებიც ძირფესვიანად განსხვავდებოდა გადახდის საშუალებად გამოყენებული, ჩვეული საბაზო კრიპტოვალუტებისაგან. ახლა სწორედ ამ განსხვავებებზე უფრო დაწვრილებით ვისაუბრებთ.

ზოგადი დახასიათებით, ნებისმიერი ტოკენი უნდა განვიხილოთ როგორც თვლის ერთეული, რომელიც სავალდებულო არაა წარმოადგენდეს ციფრულ ფულს, თუმცა კრიპტოტოკენებმა ყველაზე მეტად, სწორედ ამ სახით მოიპოვა დიდი სახელი. პროექტების საკმარისად დიდმა რაოდენობამ საკუთარ სისტემებში ინტეგრირება გაუკეთა სპეციალურ საგადახდო ტოკენებს, რომლებსაც მონეტა ეთერის ღირებულების რყევისგან განურჩევლად, საკუთარი შიდა ფასეულობა ჰქონდა. ასეთმა ტოკენებმა მიიღო „უტილიტარულის“ (utility) ან „სასარგებლო“ ტოკენების სახელი და განასახიერებდა ან საკუთარი პროექტებისათვის საჭირო შიდა ფულს, ან აღრიცხვის ერთეულების სხვა ფორმებს, მაგალითად – ამა თუ იმ კომპანიის ლოიალობის პროგრამის ქულებს ან რაღაც მსგავსს. უტილიტარული ტოკენები განკუთვნილია ერთი ძირითადი მიზნისათვის, იყოს პროექტის მიერ შემოთავაზებული საქონლის ან მომსახურების საანგარიშო ეკვივალენტი. ისინი არ არის აქტივები, რომლებსაც რაღაც ფასობრივი უზრუნველყოფა აქვს, ხოლო მათი საბაზრო ღირებულების ფორმირება, თეორიული თვალსაზრისით, არ უნდა იყოს დამოკიდებული პროექტის წარმატებებსა და დამარცხებებზე. მიუხედავად ამისა, რეალობა ისაა, რომ უტილიტარულ ტოკენებზე მოთხოვნების მოცულობა გავლენას ახდენს მათ საბაზრო ფასზე, ხოლო თვით მოთხოვნილება ყალიბდება ამა თუ იმ კრიპტოპროექტის პოპულარობის ხარისხის მიხედვით, რომლებიც გვთავაზობს საკუთარ ტოკენებს რეალიზაციისათვის.

პროექტების შემმუშავებლებს, როგორც წესი, ძალზე სჭირდებათ ინვესტიციები. იშვიათად ხდება, რომ მათ პროექტის დამოუკიდებლად შექმნისათვის საჭირო ყველა ხარჯის დაფარვის შესაძლებლობა ჰქონდეთ, ეს უფრო ახასიათებთ მსხვილ კორპორაციებს, რომლებსაც საკუთარი ფინანსური რეზერვები აქვთ, ხოლო პროგრამისტი-ენთუზიასტების ჯგუფი, რომელმაც თავისი პროექტისა-

თვის საინტერესო იდეა შეიმუშავა, ალბათ ეცდება, პროექტის შექმნის ადრეული ეტაპები გარედან სახსრების მოზიდვით დააფინანსოს. კრიპტოგარემოში ბლოკჩეინ-ტექნოლოგიების ბაზაზე შესაქმნელი პროექტებისათვის, საკუთარი ტოკენების გამოშვება გახდა საუკეთესო საშუალება, შეაგროვონ მნიშვნელოვანი სახსრები მათ შესამუშავებლად. ასეთმა პროექტებმა მიიღო „მონეტების პირველადი განთავსების“ სახელი ანუ ICO (Initial Coin Offering), ცნობილი ტერმინის IPO (Initial Public Offering) ანალოგიით, როდესაც კომპანია უშვებს საკუთარ აქციებს საფონდო ბირჟაზე გასასვლელად და ამგვარად იზიდავს ფულად სახსრებს შემდგომი განვითარებისათის.

თუ რომელიმე პროექტი პოზიციონირებს გამოშვებული მონეტებით, არა როგორც შესაქმნელ სისტემაში ანგარიშებისათვის საჭირო უტილიტარული საშუალებით, არამედ როგორც საკუთარი კომპანიის ვირტუალური აქციებით, მაშინ საუბარია ტოკენის როგორც ციფრული აქტივის საერთოდ სხვა ტიპზე. აუცილებელია გავითვალისწინოთ ის ფაქტი, რომ როდესაც ინვესტორი იძენს ამგვარ ტოკენებს, ის, იდეაში, კომპანია-ემიტენტის თანამფლობელი უნდა გახდეს, ანუ მიიღოს ყველა თანმდევი პრივილეგია, მისი საქმიანობის დივიდენდებისა და მნიშვნელოვანი გადაწყვეტილებების მიღებისას ხმის უფლების ჩათვლით. ახლა არ შევეხებით ამგვარი ტოკენების შეძენის იურიდიულ ასპექტებს, მხოლოდ შევნიშნავთ, რომ ამ შემთხვევაში საქმე გვაქვს ე.წ. „საინვესტიციო“ (security) ტოკენებთან, რომლებიც მოწოდებულია, ასახოს შემძენის მიერ პროექტის პროპორციული ნაწილის ფლობის იურიდიული უფლება.

ქსელ Ethereum-ში ტოკენების განლაგების ჩვეული პროცედურების ჩატარებისას პროექტების მფლობელები სმარტ-კონტრაქტებს იყენებენ. ისინი კონტრაქტის კოდს იმგვარად ადგენენ, რომ ნებისმიერი ინვესტორისაგან ეთერის მონეტებში ნომინირებული ნებისმიერი თანხის შემოსვლისას, მას სამაგიეროდ გადაეცემა პროექტის ტოკენების შესაბამისი რაოდენობა, განლაგების პირობებიდან გამომდინარე. ამ შემთხვევაში, სმარტ-კონტრაქტი ემისიასა და ტოკენების გავრცელებაზე კონტროლს ახორციელებს. თუ პროექტის მფლობელები მოისურვებენ, მაგალითად, წაახალისონ საკუთარი ტოკენების ადრეული შესყიდვა, მათ შეიძლება შემოგვთავაზონ უფრო დაბალი ფასები ინვესტიციის თარიღის მიხედვით. ამ შემთხ-

ვევაში, სმარტ-კონტრაქტმა უნდა დაამუშაოს მიმდინარე თარიღი, შეადაროს ის პირობებში ჩადებულ დისკონტების ცხრილს და ამგვარად განსაზღვროს ტოკენის აქტუალური ღირებულება დროის მიმდინარე პერიოდისათვის. სმარტ-კონტრაქტს ამგვარადვე შეუძლია ინვესტორებისაგან ტოკენების გამოსყიდვაც, მფლობელების მიერ დეკლარირებული ფასის მიხედვით, ასევე, მიიღოს ტოკენები და სამაგიეროდ გასცეს ეთერის მონეტები შესაბამისი ეკვივალენტით. არსებობს შემთხვევები, როდესაც საჭიროა ზედმეტი ტოკენების თავიდან მოშორება მათი „დაწვის“ გზით, მაგალითად – გადაგზავნით ქსელში არარსებულ მისამართზე, რომლისთვისაც არც ერთ წევრს საიდუმლო გასაღები არ გააჩნია.

სამწუხაროდ, გვიწევს იმის აღნიშვნა, რომ მრავალი კრიპტო-პროექტის მფლობელები ხშირად არ აკეთებენ აქცენტებს ტოკენების სახეობათა შორის პრინციპულ სხვაობაზე, რომლებსაც ისინი გასაყიდად სთავაზობენ ინვესტორებს. კრიპტოვალუტურ ინდუსტრიაში ხშირი გახდა შემთხვევა, როდესაც ICO-ის ეგიდით ვრცელდებოდა არა საინვესტიციო, არამედ წმინდად უტილიტარული ტოკენები, რომლებიც ფლობის არავითარ უფლებას არ იძლეოდა. ამგვარმა პრეცედენტებმა სწრაფად მიიპყრო სხვადასხვა ქვეყნის ფინანსური რეგულატორების ყურადღება, რომლებმაც აქტიური მოქმედება დაიწყეს ტოკენის ტიპების სამართლებრივად დასაყოფად, იმავდროულად, ინვესტორებს უხსნიდნენ მათ შორის სხვაობას. გასაგებია, რომ თითოეულმა სახელმწიფომ სხვადასხვაგვარად ჩამოაყალიბა დამოკიდებულება კაპიტალის მოზიდვის ახალ ფორმასთან. რომელიღაც ქვეყნებმა იჩქარეს შეექმნათ ICO-ის გამტარებელი პროექტებისათვის უმაღლესი ხელშეწყობის რეჟიმი და თავიანთ კანონმდებლობაში საკმაოდ სწრაფად შეიტანეს შესაბამისი ცვლილებები და დამატებები; სხვებმა მოცდის პოზიცია დაიკავეს, რადგან ვერ გადაწყვიტეს, რა მიმართულებით გაეტარებინათ რადიკალური ზომები, ხოლო ცალკეულმა იურისდიქციებმა მაშინვე გამოთქვეს ნეგატიური დამოკიდებულება ასეთი პროცესების მიმართ და ლოკალური კრიპტოინდუსტრიის წინააღმდეგ განსაზღვრული რეპრესიული ქმედებებიც ჩაატარეს და ვალდებულება დააკისრეს პროექტების მფლობელებს, ინვესტორებისათვის დაებრუნებინათ ICO-ის საშუალებით ადრე მოზიდული სახსრები.

მიუხედავად იმისა, რომ უტილიტარული და საინვესტიციო ტოკენები მთელ კრიპტოინდუსტრიაში დომინირებს, ციფრული ტოკენების სახეობები მხოლოდ მათი ორი სახეობით როდი შემოიფარგლება. არსებობს ყველა საფუძველი ვივარაუდოთ, რომ ტოკენიზაციის ყველაზე პერსპექტიული ფორმა იქნება „დიგიტალიზაცია“ ანუ ჩვეულებრივი ფინანსური აქტივების გარდაქმნა ციფრულ ფორმად. საუბარია ფიატურ ვალუტებზე, კორპორაციათა აქციებზე, ნედლეულ საქონელზე ანდა წარმოებულ ინსტრუმენტებზე, როგორებიცაა ფიუჩერსები, ოპციონები ან კონტრაქტები ფასთა სხვაობაზე. ყოველი ასეთი ფინანსური აქტივისათვის არსებობს შესაძლებლობა გამოუშვას ტოკენები, რომლებიც მიმოქცევაში იქნება დეცენტრალიზებულ ბლოკჩეინ-გარემოებში, აქედან გამომდინარე ყველა უპირატესობით. თუმცა, ასეთ ტოკენებს ექნება გარკვეული თავისებურებები. პირველ რიგში, მათი ფასი მთლიანად და სრულად იქნება დამოკიდებული კლასიკურ ფინანსურ ბაზრებზე „შესაბამისი აქტივის“ საბაზრო ღირებულების რყევაზე. სხვა სიტყვებით რომ ვთქვათ, მათი ფასი ყოველთვის სტაბილური უნდა იყოს თავიანთ საბაზო აქტივებთან მიმართებაში. სწორედ ამიტომ ტოკენების ასეთ ტიპს დაარქვეს „სტეიბლკოინები“ ანუ „სტაბილური მონეტები“, თუკი სიტყვასიტყვით ვთარგმნით ინგლისურიდან.

მეორე მნიშვნელოვანი განსხვავება უტილიტარული ტოკენებისაგან არის სტეიბლკოინების შესაბამისი საბაზო აქტივებით სრული უზრუნველყოფის მექანიზმების ორგანიზების აუცილებლობა. აშკარაა, რომ ამგვარი მოდელები შეიძლება განვახორციელოთ მხოლოდ დეცენტრალიზებული მეთოდით ანუ სპეციალური დეპოზიტარიების საშუალებით, რომლებიც შეინახავს საბაზო უზრუნველყოფის აუცილებელ მოცულობებს. ამ ტიპის დეპოზიტარიებმა შესანახად უნდა მიიღოს საბაზო აქტივი, ხოლო სამაგიეროდ, მომხმარებელზე გასცეს შესაბამისი სტეიბლკოინები. იგივე ეხება უკუოპერაციასაც, როდესაც დეპოზიტარიები უკან მიიღებენ სტეიბლკოინებს და ვალდებულნი იქნებიან, გაცვალონ ისინი საბაზო აქტივის უზრუნველყოფაში შენახულ ტოლ მოცულობაში. მაგალითის სახით შეიძლება განვიხილოთ პროექტი Tether, რომელიც უზრუნველყოფს ამერიკული დოლარის სტეიბლკოინების ემისიას Ethereum-ისა და ბიტკოინ-ქსელებში (ზექსელური ინფარსტრუქტურა Omni Layer-ის საშუალებით).

სტეიბლკოინი Tether 2015 წელს გამოუშვა ჰონკონგურმა კომპანიამ Tether Limited, რომელმაც მისი ემიტირება და უზრუნველყოფა ივალდებულა. დოლარის ტოკენიზაციის აუცილებლობა ნაკარნახევი იყო კრიპტოვალუტური ბირჟების ტრეიდერების მხრიდან მნიშვნელოვანი მოთხოვნებით, რომლებსაც სურდათ განეხორციელებინათ კრიპტოვალუტების არა მარტო ერთმანეთზე, არამედ ციფრული ფორმით წარმოდგენილი ფიატური ვალუტების ანალოგებზე გაცვლაც. ამგვარად მათ სურდათ, თავი დაეცვათ კრიპტოვალუტების ფასების რყევებისაგან, ფიატური ვალუტის ეკვივალენტებში საკუთარი კაპიტალის გადატანით, ხოლო ბევრ მათგანს უბრალოდ სურდა, განეხორციელებინათ კრიპტოვალუტის კონვერტაცია დოლარის ტოკენებში, რათა შემდგომ პირდაპირ გაეცვალათ ემიტენტთან ჩვეულებრივ დოლარებზე, საბანკო გადახდის საშუალებით საცავიდან მათი მიღებით.

ლოგიკური იქნებოდა გვევარაუდა, რომ თუკი რომელიღაც კომპანია უშვებს, ვთქვათ, 1 მილიონი აშშ დოლარის სტეიბლკოინს, მაშინ მის საბანკო ანგარიშზე უნდა იყოს არანაკლებ 1 მილიონი ფიზიკური დოლარისა, რომლებითაც ეს ტოკენებია უზრუნველყოფილი. არადა, სტეიბლკოინების საბაზო აქტივებით უზრუნველყოფის მექანიზმები თავისთავად ბლოკჩეინ-ქსელის კონტროლის ფარგლებს გარეთ მდებარეობს და ნდობაზე დამყარებულ დეცენტრალიზებულ სერვისს წარმოადგენს. ამგვარად, საქმიანობის „გამჭვირვალობის“ უზრუნველყოფა თვით ემიტენტზეა დამოკიდებული. Tether-ის შემთხვევაში, დეპოზიტარიის საქმიანობის გამჭვირვალობა აშკარად არასაკმარისად იყო უზრუნველყოფილი. გარე აუდიტებზე კომპანია ყოველთვის უარს ამბობდა, არადა, USDT (Tether) ტოკენების საერთო ემისიამ 2019 წლის გაზაფხულისათის 2,5 მილიარდ დოლარს გადააჭარბა. გასაკვირი არ არის, რომ კომპანია მუდმივად საფინანსო რეგულატორების დაჟინებული დაკვირვების ობიექტია როგორც ჰონკონგში, ასევე დოლარის ემიტენტ ქვეყანაში, აშშ-ში, სადაც 2018 წელს რეგულატორებმა კომპანიას აუკრძალეს ოპერაციები ქვეყნის რეზიდენტებთან. მიუხედავად ამისა, Tether-ის სტეიბლკოინები სარგებლობს განსაკუთრებული პოპულარობით კრიპტოტრეიდერებში და ნდობის პრობლემები, ამ მომენტისთვის მაინც, არ წარმოექმნება.

მიუხედავად კლასიკური ფინანსური აქტივების ტრანზაქციის ორგანიზაციული და რეგულაციური სირთულისა, ეს პროცესი

თანდათანობით უფრო პოპულარული ხდება. ჩნდება პროექტები, რომლებიც გვთავაზობს ძვირფასი ლითონების ტრანზაქციას ან საბირჟო კომპანიების აქციებს. Ethereum-ის ქსელის გარდა, ბაზარზე ჩნდება სხვა მატოკენიზებელი პლატფორმები, თუმცა მათთვის ადვილი არ არის დარგის ლიდერთან ბრძოლა, რომელიც გამოშვებული ტოკენების უდიდეს უმრავლესობას აერთიანებს. იმისათვის, რათა დარგობრივ ტოკენიზაციას სისტემური ფორმა მისცეს, Ethereum-ის პროექტმა შეიმუშავა სპეციალური სტანდარტები სხვადასხვა ტიპის ტოკენებისათვის. ამჟამად ყველაზე პოპულარული სტანდარტია ERC-20, სწორედ ამ ფორმატშია გამოშვებული სხვადასხვა პროექტის ტოკენების უმეტესობა. ეს სტანდარტი აღწერს ტექნიკური სპეციფიკაციების ერთობლიობას გამოსაშვები ტოკენებისათვის, რათა ისინი მიიღოს მთელმა ქსელმა და შესაძლებელი გახდეს მათი ურთიერთქმედება სისტემის სხვა ტოკენებთან, რომლებიც თავსებადია ფორმატის მიხედვით.

საკმაოდ ხშირად ტოკენების მფლობელებს უჩნდებათ ტოკენების ერთიმეორეზე გადაცვლის აუცილებლობა. Ethereum-ის ქსელის საბაზო ფუნქციონალი არ იძლევა საშუალებას, ერთი ტრანზაქციის ფარგლებში პირდაპირ გაიცვალოს სხვადასხვა ტოკენი. იმისათვის, რომ ქსელის წევრებმა შეძლონ ერთმანეთში სხვადასხვა აქტივის გაცვლა, საჭიროა არანაკლებ ორი ტრანზაქციისა, რომლებსაც შემხვედრი გარიგების ფორმა აქვს. რადგან ბლოკჩეინ-ქსელებში ყველა ტრანზაქცია არის „უკან გამოუთხოვადი“, ასეთ შემთხვევებში, მხარეებს შორის ნდობის უზრუნველყოფის საკითხი საკმაოდ აქტუალური ხდება. გაცვლის რეალიზაციის ყველაზე პოპულარული მეთოდია კრიპტოვალუტის ბირჟები, რომელთა შუამავლობითაც ტარდება უმეტესობა გარიგებებისა ტოკენებში, მათ შორის – ERC-20 სტანდარტისა. ასევე არსებობს რიგი დეცენტრალიზებული ბირჟებისა, რომლებიც მხოლოდ Ethereum-ის ქსელის ტოკენების ერთმანეთში მიმოცვლაში სპეციალიზდება.

Ethereum-ის ქსელის არასრული ოთხი წლის არსებობის განმავლობაში მასში ემიტირებული იქნა სხვადასხვა ტიპის 200 000 ტოკენზე ოდნავ ნაკლები, უტილიტარული, საინვესტიციო და რიგი სხვა. ტოკენიზაციის ამგვარი მასშტაბები იმაზე მეტყველებს, რომ კრიპტოტოკენების დარგი აქტიურად ვითარდება და უახლოეს დრო-

ში შეგვიძლია ვიხილოთ უფრო მეტი პროექტი, რომელიც ამ ტიპის ციფრულ აქტივებს დაეფუძნება. ზოგიერთი შეფასებით, Ethereum-ის პლატფორმის ბაზაზე დეცენტრალიზებული დანართების შექმნის ინდუსტრიაში ჩართულია ასეულათასობით IT სპეციალისტი მთელ მსოფლიოში და მათი რიცხვი იზრდება. ვითარდება თვით Ethereum-ის ქსელის შესაძლებლობები: მისი შემმუშავებლები და, პირველ რიგში, თვითონ ვიტალიკ ბუტერინი, მუდმივად ეძებენ შესაძლებლობებს ქსელის მუშაობის გასაუმჯობესებლად და იმ პრობლემების გადასაჭრელად, რომლებიც აუცილებლად წარმოიქმნება პროექტის ექსპლუატაციის პროცესში. ეს არის ბლოკების ბაზის გადაჭარბებული ზრდა და, რა თქმა უნდა, მაინინგზე დახარჯული ელექტროენერგია. ამჟამად Ethereum-ის ქსელი იმყოფება გარდამავალ პერიოდში ენერგოტევადი Proof-of-Work კონსენსუსიდან უფრო პროგრესულ ალგორითმამდე, რომელიც საშუალებას მოგვცემს, თავიდან ავიცილოთ გადაჭარბებული ენერგოდანახარჯები, რადგან სულ სხვა პრინციპს ეფუძნება. მას ეწოდება „მფლობელობის დამტკიცება“ ან Proof-of-Stake, და უკვე აქტიურად გამოიყენება ზოგიერთ კრიპტოინდუსტრიულ პროექტში. იმის წყალობით, რომ არსებითად, მუშაობის დამტკიცების ალგორითმის ძირითად ალტერნატივას წარმოადგენს, ეს პრინციპი ენერგეტიკულად არაეფექტიან თავის კონკურენტს თანდათან აძევებს.

მფლობელობის დამტკიცება

სამუშაოს დადასტურების ალგორითმის საშუალებით ბლოკჩეინ-ქსელის დაცვის პრინციპების ანალიზისას აშკარად ისახება როგორც მისი უპირატესობები, ასევე ნაკლოვანებები. კონცეფციის აშკარა უპირატესობაა მათემატიკური სიზუსტე, რომელიც გამოსათვლელი ამოცანის განსაზღვრას უზრუნველყოფს; უდავოა, რომ აღნიშნული ამოცანის გადაწყვეტა ბლოკის შექმნისთვის ანაზღაურების უფლებას ადასტურებს. ამასთან ერთად, ადგილი აქვს ნეგატიურ ასპექტებსაც, სახელდობრ – დიდ ენერგოდანახარჯებს, რომლებიც საკმაოდ არარაციონალურად გამოიყენება, რადგან სარგებელი გამოთვლებით მიღებული შედეგებიდან მთავრდება უშუალოდ ყოველი ახალი ბლოკის შექმნის მომენტში. გასაგებია, რომ დეცენტრალიზებულ გარემოებში კონსენსუსის მიღწევის მსგავსი მეთოდი იღებს კრიტიკული გამოხმაურებების მასას, რომლებიც დაკავშირებულია ენერგორესურსების არაეფექტიან გამოყენებასთან. ამ პრობლემით კრიპტოენთუზიასტები შეფიქრიანებულნი იყვნენ ჯერ კიდევ ბიტკოინ-ქსელის მუშაობის ადრეულ პერიოდში, წინასწარ გათვლიდნენ სიტუაციას, როდესაც მთელი ქსელის ერთობლივი ენერგოდანახარჯები კრიპტოპროექტის პოპულარობის ზრდასთან ერთად გაიზრდებოდა. ეს პრობლემატიკა სერიოზულად განიხილებოდა კრიპტოსაზოგადოების მიერ, როდესაც 2011 წლის ივლისში ერთ-ერთ ყველაზე პოპულარულ ბიტკოინ-ფორუმზე გაიჟღერა რევოლუციურმა იდეამ იმის შესახებ, რომ ენერგოდამოკიდებულ მაინინგზე უარის თქმა მაინც შეიძლება. მუშაობის დამადასტურებელი კონცეფციის შემცვლელად შემოთავაზებული იქნა მოდელი „მფლობელობის წილის დადასტურება“, რომელსაც კრიპტოსაზოგადოებაში იმ დროიდან მოყოლებული Proof-of-Stake (PoS) უწოდებენ.

ფორუმულ ფსევდონიმ Quantum Mechanic-ს ამოფარებული იდეის ავტორი იტყობინებოდა გამომთვლელი სიმძლავრის ქსელის კვანძების მიერ კონტრიბუციის მაგივრად კრიპტოვალუტის მფლობელობის პოტენციალის გამოყენების შესაძლებლობის შესახებ, როგორც ეს ჩვეულებრივი მაინინგისას კეთდება. სხვაგვარად რომ ვთქვათ, შე-

მოთავაზებული იქნა იდეა, გაცემულიყო ბლოკების შექმნის უფლება იმ კვანძებისათვის, რომელთა ბალანსზეც განთავსებული იყო კრიპტომონეტების მნიშვნელოვანი რაოდენობა შედარებით ხანგრძლივი დროის განმავლობაში. იდეა სრულად იქნა მხარდაჭერილი და განვითარებული კრიპტოსაზოგადოების მიერ. დაახლოებით ერთი წლის შემდეგ, 2012 წლის აგვისტოში, შემმუშავებლების – სკოტ ნედალისა და სანი კინგის მიერ წარმოდგენილი იქნა გადახდის სისტემა Peercoin. ეს იყო პირველი ბლოკჩეინ-ქსელი, რომელმაც მფლობელობის მტკიცებულების ელემენტები დაუმატა მუშაობის ჩვეულ მტკიცებულების პრინციპს და ამგვარად შექმნა კონსენსუსის ჰიბრიდული მექანიზმი. ახალი ფულადი ემისიების ფორმირებისათვის ბლოკების შემქმნელი მაინერების გასამრჯელოს სახით, სატრანზაქციო საკომისიოებთან ერთად, ქსელში გამოიყენებოდა Peercoin ოქმი Proof-of-Work (PoW), – ბიტკოინ-ქსელის ანალოგიურად, ამასთანავე, PoW ბლოკებთან ერთად, ქსელში შეიძლებოდა წარმოქმნილიყო ბლოკებიც, რომლებიც მფლობელობის მტკიცებულების პრინციპის (PoS) საფუძველზე იქმნებოდა. ბლოკის შესაქმნელად აუცილებელია ჩატარდეს ქმედებები, რომლებიც ცალკეულად მაინინგს გვაგონებს, ოღონდ მფლობელობის მტკიცებულების საფუძველზე ბლოკების შემქმნელებს უწოდეს არა მაინერები, არამედ ვალიდატორები, ანუ ბლოკების დამადასტურებელი კვანძები, ხოლო თვით ბლოკების შექმნის პროცესს – ფორჟინგი ან მინტინგი, ინგლისური სიტყვებიდან forging და minting, რაც ნიშნავს „გამოჭედვას“, „მონეტების მოჭრას“. სანამ ბლოკის შექმნას შეუდგებოდა, ვალიდატორს აუცილებლად უნდა ეჩვენებინა, თუ რა რაოდენობის კრიპტომონეტებს ფლობდა. ისევე, როგორც მაინინგისას, საჭირო იყო ზოგიერთი პარამეტრის ჰეშირება, როგორიცაა წინა ბლოკის მონაცემები, მიმდინარე დრო და მისამართი, რომელზეც განთავსებული იყო ვალიდატორის სახსრები. მიღებული ჰეში დარდებოდა ორი მნიშვნელობის ნამრავლს, რომლებიც წარმოადგენდა ვალიდატორის მონეტების რაოდენობასა და მათი ფლობის ხანგრძლივობას. როგორც კი შეძლებდნენ ჰეშის მიღებას, რომლის მნიშვნელობაც ნაკლები იყო ნამრავლზე, ბლოკი შექმნილად ითვლებოდა. აშკარაა, რომ რაც უფრო მეტი მონეტა აქვს ვალიდატორს და რაც უფრო ხანგრძლივად ფლობს მათ, მით მეტია შანსი, რომ ამ რიცხვების ნამრავლი ძალზე დიდია და გადააჭარბებს შემთხვევით

მიღებულ ჰეშს, რომელიც ყოველთვის შეგვიძლია განვიხილოთ ჩვეულებრივ რიცხვად. რადგან ჰეშირების პროცესში არის მხოლოდ ერთი მუდმივად ცვლადი პარამეტრი – დრო სრულ წამებში, ამიტომ ჰეში შეიძლება შეიცვალოს მხოლოდ ერთხელ წამში. ბლოკის შემქმნელი ვალიდატორი უშუალოდ ამისათვის გასამრჯელოს არ იღებს, გამოიმუშავებს მხოლოდ ბლოკში მოთავსებული ტრანზაქციის საკომისიოს.

როგორც ბლოკების შესაქმნელი ალგორითმიდან Proof-of-Stake გამომდინარეობს, ამისათვის მნიშვნელოვანი ენერგოდანახარჯები არ გვჭირდება. მაგრამ ეს არ ნიშნავს, რომ კონსენსუსის ამ ტიპს არ გააჩნია ნაკლოვანებები და უხერხულობები. Proof-of-Stake პრინციპით ბლოკების შემქმნელი ვალიდატორი ფაქტობრივად ყინავს სახსრებს საკუთარ ანგარიშზე და იძულებულია არ გამოიყენოს ისინი საკმაოდ ხანგრძლივი დროის განმავლობაში, რათა არ დაკარგოს ბლოკების შესაძლო შექმნისათვის საჭირო დაგროვილი პოტენციალი. თვით ქსელისათვის ეს კარგი არ არის, რადგან ფულის მიმოქცევის სიჩქარე მის შიგნით შეიძლება მნიშვნელოვნად შემცირდეს, რაც ნეგატიურად აისახება მისი გამოყენებისა და განვითარების შესაძლებლობებზე. ბლოკების შექმნის ასეთი მეთოდი მოტივირებას უკეთებს კვანძებს პირველ რიგში სახსრების დაგროვებაზე და არა დახარჯვაზე. ამგვარად, მათმა ზედმეტმა კონსოლიდაციამ ერთი ან რამდენიმე კვანძის კონტროლქვეშ შეიძლება გამოიწვიოს ქსელის მართვის პროცესების ცენტრალიზაციის ხარისხის მომატება, წინასწარი ჩანაფიქრის საწინააღმდეგოდ. ასევე, ბლოკების შექმნაზე პრაქტიკულად არავითარ გავლენას არ ახდენს კრიპტომონეტების მცირე რაოდენობის მფლობელი კვანძები, რადგან მათ პრაქტიკულად არ აქვთ შანსი, გახდნენ ვალიდატორები თავიანთი უმნიშვნელო ფინანსური პოტენციალის გამო.

ამ ნაკლოვანებების გამოსასწორებლად შემუშავებული იქნა Proof-of-Stake ოქმების მოდიფიკაცია, სადაც წარმოდგენილი იყო ქსელის რიგითი წევრებისაგან მათ მიერ არჩეული კვანძებისადმი ვალიდატორობის უფლებამოსილების მინიჭების მექანიზმები. ყოველ კვანძს სპეციალური ტრანზაქციის საშუალებით შეუძლია ხმა მისცეს ვალიდატორობის ერთ ან რამდენიმე პოტენციურ კანდიდატს. ხმათა უმრავლესობის მიმღები კვანძი-დელეგატები შეიძლება არც ფლობდნენ მონეტების მნიშვნელოვან რაოდენობას, მაგრამ სამაგიეროდ ისინი მზად არიან

აამოქმედონ თავიანთი გამოთვლითი შესაძლებლობები ქსელის სტაბილური მუშაობის ხელშესაწყობად და ამისაგან მიიღონ შედარებით მოკრძალებული სატრანზაქციო საკომისიო. მსგავს პრინციპს უწოდეს „მფლობელობის დელეგირებული მტკიცებულება“ (DPoS), Proof-of-Stake ოქმის სწორედ ეს ფორმა შემდგომში ყველაზე ფართოდ გავრცელდა პროექტებში, რომლებმაც გადაწყვიტეს, უარი ეთქვათ ენერგოდანახარჯებიანი მუშაობის დამამტკიცებელ ალგორითმზე.

DpoS-ის განსხვავება მფლობელობის მტკიცებულების კლასიკური ფორმისაგან იმაში მდგომარეობს, რომ ვალიდატორები, რომლებმაც დელეგირების უფლება მიიღეს, შესაბამისი მნიშვნელობის საპოვნელად უკვე აღარ არჩევენ ჰეშებს. ამის მაგივრად ისინი ადგენენ მათი მსგავსი დელეგატების რიგს, რათა შეთანხმდნენ ბლოკების ფორმირების მკაცრ თანმიმდევრობაზე. ყოველ ვალიდატორს გამოეყოფა გარკვეული დროის პერიოდი, რომლის განმავლობაშიც მას აქვს მთელი ქსელისათვის მისაღები ბლოკის შექმნის უფლება. თვით პერიოდი საკმაოდ მოკლე შეიძლება იყოს და წამის ერთეულებით აითვალოს, ეს დამოკიდებულია ქსელის ოქმსა და იმაზე, თუ რამდენად დიდი გამტარუნარიანობის მიღება სურთ ქსელის წევრებს თავიანთი ტრანზაქციებისათვის. იმ შემთხვევაში, თუ რაიმე მიზეზის გამო ვალიდატორმა გამოტოვა თავისი რიგი, ბლოკის შექმნის უფლება გადადის რიგით შემდეგ ვალიდატორზე. თვით თანმიმდევრობას აქვს ყველასათვის საერთო ფორმირების წესი, ამასთან, ყოველი ვალიდატორი მას დამოუკიდებლად ითვლის. გასაგებია, რომ ყველა ვალიდატორისათვის ეს გათვლილი თანმიმდევრობა ზუსტად უნდა ემთხვეოდეს ერთმანეთს, სხვაგვარად ქსელის მუშაობა შეიძლება დაირღვეს.

Proof-of-Stake ფორმის უპირატესობა უფლებამოსილებების დელეგირებასთან შედარებით აშკარაა. პირველ რიგში, უმნიშვნელო ბალანსების მქონე კვანძებს აქვთ მართალია, ირიბი, მაგრამ თავიანთი ფინანსური ბალანსების პროპორციული გავლენა ვალიდატორ-კვანძების არჩევანზე. თავიანთი ერთობლივი მასით ეს კვანძები მსხვილ მოთამაშეებს დიდი ალბათობით, საშუალებას არ მისცემენ დაიპყრონ და ცენტრალიზებულად აქციონ ქსელის მართვის პროცესები. უშუალოდ ბლოკების შექმნით დაკავებულნი იქნებიან კვანძები, რომლებიც საუკეთესოდ არიან ამისათვის მზად და აქვთ ქსელის კვანძთა უმეტესობის ნდობა. დაბოლოს, რაც ასევე მნიშვნელოვანია, არ არ-

სებობს ანგარიშებზე კრიპტოსახსრების დიდი მოცულობების ბლოკირების აუცილებლობა, რათა ვალიდატორს შესაძლებლობა ჰქონდეს, მუდმივად ამტკიცოს საკუთარი ფინანსური შეძლება და ამგვარად მიიღოს ქსელში ახალი ბლოკების შექმნის უფლება.

ეს არ ნიშნავს, რომ მფლობელობის დამადასტურებელ კონცეფციას არ გააჩნია პოტენციური პრობლემები. ამ პროტოკოლზეც შეიძლება განხორციელდეს სხვადასხვა სახის შეტევა, რომელთაგან ერთ-ერთი შეიძლება გახდეს ჩვენთვის ცნობილი „51%-იანი შეტევა“. მართალია, მუშაობის მტკიცებულების მქონე სისტემებისაგან განსხვავებით, რომლებშიც მოითხოვება ქსელის მთელი გამოთვლითი სიმძლავრის არანაკლებ ნახევრის ხელში ჩაგდება, Proof-of-Stake-ის შემთხვევაში აუცილებელია პროექტის კრიპტომონეტების ნახევრის ან უფრო მეტის გაკონტროლება, თუმცა ასეთი შეტევის შედეგებს მსგავსი ნეგატიური ბუნება აქვს ორივე კონცეფციაში, რადგანაც ავტომატურად იწვევს მთელი ქსელისადმი ნდობის დაკარგვას და ლოკალური კრიპტოვალუტის გაუფასურებას, რითაც კოტრდება თვით თავდამსხმელიც.

ერთ-ერთი შესაძლო სიძნელე ასეთი ფორმის კონსენსუსის გზაზე შეიძლება გახდეს შეტევა Nothing at Stake ანუ „არაფერი ფსონზე“. მსგავსი სიტუაცია წარმოიშობა, როდესაც არაკეთილსინდისიერი ვალიდატორი ცდილობს შექმნას და ხელი მოაწეროს ბლოკებს ჯაჭვის სხვადასხვა განშტოებაში, რომლებიც წარმოიქმნა შემთხვევით ან წინასწარი განზრახვით. მუშაობის დამადასტურებელ შემთხვევაში, მაინერის ასეთი ქცევა არარაციონალურია, რადგან ამგვარად ის ანაწილებს საკუთარ გამოთვლით სიმძლავრეს განშტოებებს შორის და ამით ამცირებს რომელიმე მათგანში ბლოკის შექმნის საკუთარ შანსებს. მფლობელობის დამადასტურებელ მოდელში ის, პირიქით, არაფერს რისკავს, რადგან ბლოკების შექმნაზე კონკურენტ განშტოებებში არ ხარჯავს არც სახსრებს, არც გამოთვლით რესურსებს. თუმცა, ასეთი საქმიანობა აუცილებლად გამოიწვევს კონსენსუსის დარღვევას, რომელსაც ქსელი ჯამში ვერასდროს მიაღწევს. Proof-of-Stake-ით მოსარგებლე ყოველი პროექტი განსხვავებული ეფექტიანობით ცდილობს, წინ აღუდგეს ამ პრობლემას.

Proof-of-Stake-ის კლასიკური ფორმის კიდევ ერთი მნიშვნელოვანი თვისებაა მაინინგის ანაზღაურების ანალოგი. რადგან მაინინგი

და მისი ხელშესაწყობი ინფრასტრუქტურული დანახარჯები, თავისთავად, არ არსებობს, ამიტომ ითვლება, რომ ვალიდატორის წამახალისებელი შეიძლება იყოს მხოლოდ ტრანზაქციების საკომისიო. მაგრამ ამ შემთხვევაში წარმოიშობა „ქათმისა და კვერცხის“ ცნობილი დილემა: თუ არ არსებობს მაინინგური ემისიები, მაშინ საიდან გაჩნდება ფული სისტემაში? ამ საკითხს მფლობელობის დამადასტურებელი პრინციპის გამოყენების სურვილის მქონე სხვადასხვა პროექტი სხვადასხვაგვარად აგვარებს. ზოგი ირჩევს Proof-of-Stake-ის პიონერული პროექტის Peercoin-ის გაკვალულ გზას. მასში, როგორც ვიცით, რეალიზებული იქნა კონსენსუსის ჰიბრიდული მოდელი, როდესაც ადრეული ბლოკები იქმნებოდა მუშაობის დამადასტურებელი მაინინგის საშუალებით. შემდეგ მათ „შეურიეს“ მფლობელობის დამადასტურებელი ოქმის საშუალებით ვალიდატორების მიერ შექმნილი ბლოკები, რის შემდეგაც ბლოკები PoS დომინირებდა ქსელში, ხოლო PoW გამოიყენებოდა მხოლოდ დამატებითი ემისიის განსახორციელებლად, რომლის მოცულობაც მუდმივად მცირდებოდა სისტემაში მონეტათა საერთო რაოდენობის ზრდასთან ერთად. ასევე ცნობილია პროექტები, რომლებმაც გადაწყვიტეს, საერთოდ არ ჩაერთოთ მუშაობის დამადასტურებელი ოქმი და მთელი ემისია შექმნეს პირველ გენეზისურ ბლოკში, როცა ისინი შემმუშავებლების კონტროლირებად მისამართებზე განათავსეს. შემდგომში ეს მონეტები გაიყიდა ქსელის ახალ წევრებზე და ამგვარად ჩამოყალიბდა ქსელის შიდა ფულადი მიმოქცევა. ამ შემთხვევებში, როგორც წესი, სარგებლობდნენ DPoS მოდელით, რომელიც საშუალებას იძლეოდა, სწრაფად და ეფექტიანად შექმნილიყო ტრანზაქციიანი ბლოკები.

თუ პროექტ Ethereum-ს მივუბრუნდებით, მნიშვნელოვანია გავითვალისწინოთ, რომ ის კონსენსუსის ერთი ტიპიდან მეორეში გადასვლის პროცესში იმყოფება. ჯერ კიდევ 2017 წელს პროექტის შემმუშავებლებმა მომავალი მაინინგიდან Proof-of-Stake-ზე გადასვლასთან დაკავშირებული ცვლილებები დააანონსეს. 2018 წლის პირველ ნახევარში გამოჩნდა გარდამავალი პერიოდით განპირობებული განცხადება. დაანონსებული იყო მაინინგისათვის ანაზღაურების თანდათანობითი შემცირება. ამ პროცესს Ethereum-ის ქსელისათვის „გამყინვარების პერიოდი“ უწოდეს. მოარული ხმებით, იგეგმება ვალიდატორებისათვის საკმაოდ მკაცრი წესების შემოღება „ქონებრივი ცენზის“ მიხედ-

ვით. გვთავაზობენ, რომ ვალიდატორების მიერ სახსრების დაბლოკვის მინიმალური ზღვარი იყოს არანაკლებ ეთერის 1500 მონეტისა, რაც მიმდინარე კურსითაც კი, რომელმაც თავისი მაქსიმუმიდან მნიშვნელოვანი კორექცია განიცადა, შეესაბამება 200 000 დოლარზე მეტ ფიატურ თანხას. უფრო მეტიც, ვალიდატორი თეორიულად რისკავს ამ თანხის დაკარგვას, რადგან ის შეიძლება განადგურდეს, თუკი კვანძი მხილებული იქნება Nothing at Stake შეტევაში, ანუ ჯაჭვის სხვადასხვა განშტოებაში კონკურენტი ბლოკების ერთდროულ ხელმოწერაში. საბოლოო წესები შემმუშავებლების მიერ განცხადებული იქნება განახლებების გამოშვების შემდეგ, რომლებიც კონსენსუსის ოქმს შეცვლის მფლობელობის მტკიცებულებით Ethereum-ის ქსელში.

ყველა ამ ზომას კრიპტოინდუსტრიაში აქვს როგორც დადებითი, ასევე უარყოფითი გამოხმაურებები. ეჭვგარეშეა, რომ უკმაყოფილო რჩება ის, ვინც ადრე მოახდინა მნიშვნელოვანი სახსრების ჩადება ეთერის მონეტების მაინინგში. Proof-of-Stake-ზე გადასვლამ ისინი საქმეს ჩამოაშორა, თუ, რა თქმა უნდა, ისინი მაინინგისათვის ვიდეობარათებით არ სარგებლობდნენ. საქმე ისაა, რომ გრაფიკული პროცესორები წარმოადგენს უნივერსალურ ინსტრუმენტს ამ საქმიანობისათვის და საჭიროების შემთხვევაში შეიძლება გადაინტეგრირდეს სხვა კრიპტოვალუტების მაინინგზე. ასევე გაისმის საგანგაშო ხმები, რომლებიც გვაფრთხილებს უსაფრთხოების შესაძლო პრობლემებთან დაკავშირებით, PoS ოქმზე გადასვლისას. შემმუშავებლების მიერ გადადგმულ ნაბიჯებს დადებითად კი აფასებენ კრიპტოსაზოგადოების ის წარმომადგენლები, რომლებიც თვლიან, რომ ენერგეტიკულად არაეფექტიანი მაინინგი ბლოკჩეინ-ტექნოლოგიის განვითარებისათვის სერიოზულ წინააღმდეგობას წარმოადგენს. ისინი საკუთარ პოზიციას იმით ხსნიან, რომ მაინინგი არის განსაკუთრებულად რესურსდანახარჯიანი პროცესი, რომელიც ნეგატიურ გავლენას ახდენს ეკოლოგიურ მდგომარეობაზე მსოფლიოში და მას აკრიტიკებენ, თვით სახელმწიფოების დონეზეც კი.

ალტკოინები

ადამიანის კრიტიკული ანალიზის უნარი ცივილიზაციის განვითარების ერთ-ერთ ძირითად მამოძრავებელ ძალას წარმოადგენს. სკეპტიციზმის ფილოსოფია ეფუძნება ეჭვის ცნებას, რომლის ჭეშმარიტებაც დადგენილია დოგმატიკოსების საზოგადოებაში როგორც აზროვნების პრინციპი. სწორედ სკეპტიციზმი, რომელიც ეჭვქვეშ აყენებს ჩვენ გარშემო არსებული სამყაროს იდეალურობას, მოტივაციას სძენს ადამიანების მიერ მოპოვებული სამეცნიერო, კულტურული და სოციალური მიღწევების ცვლილებებსა და განვითარებას. ეჭვგარეშეა, რომ ეს ერთ-ერთი მიზეზი იყო იმისა, რომ კრიპტოინდუსტრიის ცალკეულმა წარმომადგენლებმა ადრეული ბლოკჩეინ-ქსელები საკმარისად სრულყოფილად არ მიიჩნიეს და ახალი, საკუთარი შესაძლებლობებით უფრო პროგრესული პროექტების შექმნა დაიწყეს. რაღაც მომენტში ამ პროცესმა ზვავის მსგავსი სახე მიიღო, როდესაც კრიპტოპროექტების რაოდენობა ათასებამდე გაიზარდა და მათთან დაკავშირებული ინფორმაციის მთელი მოცულობის ათვისება და გაანალიზება შეუძლებელი გახდა.

ბიტკოინის კაპიტალიზაცია, ანუ მთელი მისი ემისიის ერთობლივი ფასეულობა, ყველა დანარჩენი არსებული კრიპტომონეტების ერთად აღებულ ფასეულობას შეესატყვისება. მისი ავტორიტეტი ბლოკჩეინ-ინდუსტრიაში იმდენად მაღალი და შეუვალია, რომ უფრო გვიან გაჩენილ ყველა კრიპტოვალუტას „ალტკოინებს“ უწოდებენ, ანუ სწორედ ბიტკოინის ალტერნატივებად თვლიან. პირველი ალტკოინები ბიტკოინ-ქსელის გაშვებიდან სულ რამდენიმე წელიწადში, სახელდობრ, 2011 წელს გაჩნდა. ეს პროექტები ცდილობდა გადაელახა ის, მათი აზრით, უხერხულობები, რომლებიც ბუნებრივად შეიქმნა თვით ბიტკოინში. ამასთან, ერთ-ერთმა ახალწარმოქმნილმა ალტკოინმა პრაქტიკულად სრულად გაიმეორა თავისი წინამორბედის ფუნქციონირების ლოგიკა და უბრალოდ, მასში მიმდინარე პროცესების პარამეტრები შეცვალა. ამ პროექტმა მიიღო სახელი Litecoin, რაც თავისთავად იმაზე მეტყველებს, რომ ის ბიტკოინის შემსუბუქებულ ვერსიას წარმოადგენს.

პროექტი Litecoin შეიმუშავა ამერიკელმა პროგრამისტმა ჩარლი ლიმ, რომელსაც გარკვეული დროის განმავლობაში, ბიტკოინის ავტორად თვლიდნენ. თუმცა ძნელია ლოგიკური კავშირის პოვნა ერთ პროექტში ინკოგნიტოდ ყოფნისა და მეორეში თავის გამოაშკარავებას შორის. მიუხედავად ამისა, მსგავსი იდეა კრიპტოსაზოგადოებაში განიხილებოდა მანამდე მაინც, სანამ ყურადღება სხვა, უფრო ოდიოზურ კანდიდატებზე გადაირთო. ასეა თუ ისე, Litecoin-მა შეძლო ბაზრისათვის გამოეგლიჯა საკუთარი ნიშა და დღემდე, კაპიტალიზაციის მიხედვით, ათ ყველაზე დიდ ალტკოინს შორისაა. რა განასხვავებს ამ პროექტს თავისი უფრო „მასობრივი“ წინამორბედისაგან?

ძირითადი განსხვავებები შეიძლება გადმოიცეს ციფრი „4“-ით. პროექტის ავტორის მიერ სწორედ ეს თანამამრავლი იქნა არჩეული ბიტკოინ-ქსელის პარამეტრების მასშტაბირებისათვის. ბლოკები Litecoin-ში იქმნება 4-ჯერ უფრო სწრაფად, ანუ საშუალოდ 150 წამში, ხოლო საბოლოო ემისიის ზღვრად დადგენილია 84 მილიონ მონეტაზე ოთხჯერ მეტი. მისამართების შესაქმნელად, ისევე, როგორც ბიტკოინში, გამოიყენება ჰეშირების ალგორითმი SHA-256, სამაგიეროდ, მაინინგის მექანიზმი მნიშვნელოვნად შეცვლილია. Litecoin-ის ქსელში ახალი ბლოკების მოსაძებნად გამოიყენება სპეციალური ალგორითმი Scrypt, რომელიც ოპერატიული მეხსიერების დიდ მოცულობებს მოიხმარს. ეს საშუალებას იძლევა, წინააღმდეგობა გაეწიოს მაინინგს ASIC-ის გამოყენებით, თუმცა საბოლოოდ, ეს მოწყობილობები მაინც იქნა წარმოდგენილი ბაზარზე.

რაც შეეხება Litecoin-ის მონეტებზე საბაზრო მოთხოვნილებას, ის საშუალო დონეზეა. საკმაოდ დიდხანს ფასი 2-სა და 4 დოლარს შორის დიაპაზონში მერყეობდა, მაგრამ დიდი „ჰაიპის“ დროს თავის ისტორიულ მაქსიმუმს – 358 დოლარს მიაღწია. შემდეგ ის შემცირდა 80 დოლარამდე, რომელზეც დღესდღეობითაც დგას, ხოლო Litecoin-ის საერთო კაპიტალიზაცია 5 მილიარდ დოლარზე ოდნავ ნაკლებს შეადგენს (ბიტკოინის კაპიტალიზაციის დაახლოებით 5%). Litecoin-ის მონეტები საკმაოდ პოპულარული ფინანსური ინსტრუმენტია სპეკულაციური ვაჭრობისათვის და მათ ხშირად შეიძლება შევხვდეთ მრავალი კრიპტოვალუტური ბირჟისა და საბროკერო კომპანიის ლისტინგებში.

კიდევ ერთი ალტერნატიული ალტკოინი, რომელიც მეორე ადგილს მუდმივად ედავება Ethereum-ს, არის Ripple, შემუშავებული

ფინანსურ ინსტიტუტებსა და პირველ რიგში ბანკებს შორის, ვალუტათა გაცვლის პროცესების მაორგანიზებელი იმავე სახელის მქონე კომპანიის მიერ. Ripple თავიდანვე ჩაფიქრებული და შექმნილი იყო B2B ინდუსტრიისათვის, ანუ – საქმიანი გარემოსათვის, სადაც ყველა ურთიერთქმედება მხოლოდ იურიდიულ პირებს შორის ხდება. ამას ხელი არ შეუშლია ბევრი კერძო კრიპტოტრეიდერისათვის, კრიპტოვალუტა Ripple განეხილათ როგორც საინვესტიციო ინსტრუმენტი და მასში კურსების სხვაობის მეშვეობით მოგების მისაღებად საკმაოდ მნიშვნელოვანი კაპიტალი ჩაედოთ. პროექტს Ripple აქვს საკმაოდ ბევრი განსხვავება ჩვეულ ბლოკჩეინ-ქსელებისაგან, რომელთა ნაწილის განხილვა ჩვენთვის მიზანშეწონილი იქნება.

საინტერესოა, რომ Ripple-ის გამოჩენის საქმეში ერთ-ერთი მნიშვნელოვანი პერსონა ფაილების გაცვლა-გამოცვლის ქსელ eDonkey-სა და ბირჟა Mr. Gox-ის შემქმნელი ჯედ მაკკალები გახდა. სწორედ მან, ინვესტორ კრის ლარსენთან ერთად, შესთავაზა 2012 წელს საგადახდო ოქმის Ripplepay-ის შემმუშავებელ რაიან ფუგერს, შეექმნა სპეციალური კრიპტოვალუტა, რომლის გამოყენებაც შესაძლებელი იქნებოდა ბანკთაშორისო სავალუტო ოპერაციების საწარმოებლად. თუმცა, უკვე ერთი წლის შემდეგ მაკკალებმა დატოვა კომპანია Ripple და დააარსა მისი პირდაპირი კონკურენტი, პროექტი Stellar, რომელიც კაპიტალიზაციის მიხედვით ასევე შედის კრიპტოვალუტათა პირველ ათეულში. რა იყო ამ პროექტების შექმნის მთავარი აზრი?

საზღვართშორისი საბანკო გადახდების განხორციელებისას, რომლებიც ერთი ეროვნული ვალუტის მეორეში კონვერტაციას გულისხმობს, ტრადიციულად, ძვირად ღირებულ ბანკთაშორის საშუამავლო ინფრასტრუქტურას იყენებდნენ. სწორედ მისი ექსპლუატაცია გახდა მაღალი საკომისიოების არსებობის მიზეზი, რომლებიც ბანკის კლიენტებს იძულებულს ხდიდა, გადარიცხვების საწარმოებლად გადაეხადათ. ხანდახან, როდესაც გადარიცხვისას საჭირო იყო „მესამე სამყაროს“ ქვეყნების ვალუტების ერთმანეთზე კონვერტაცია, საკომისიოებს შეიძლება შეედგინა ათეულობით დოლარის საკურსო ეკვივალენტი, რაც მცირე თანხების გადარიცხვას ეკონომიკურად აზრს უკარგავდა. გარდა ამისა, ამ გადარიცხვებს შეეძლო მნიშვნელოვანი დრო წაეღო, რაც ასევე უკიდურესად მოუხერხებელი იყო ტრადიციული საფინანსო ინსტიტუტების ბევრი კლიენტისათვის.

პროექტი Ripple მოწოდებული იყო ამ სიტუაციის ძირფესვიანად შესაცვლელად და ბანკის კლიენტების გასათავისუფლებლად მსოფლიო ფინანსური ქსელების სასარგებლოდ უზომო საკომისიო გადასახადებისაგან, რომლებიც შუამავლების როლს ასრულებდნენ ფულის გადარიცხვისა და სავალუტო კონვერტაციების პროცესებში. ამასთან ერთად, იგეგმებოდა გადახდის განხორციელების საშუალო დროის მნიშვნელოვანი შემცირება, ერთი ეროვნული ვალუტიდან მეორეში კონვერტაციის საუკეთესო კურსების შეთავაზებით. ამისათვის აუცილებელი იყო მთელი მსოფლიოდან პროექტში ბევრი ბანკის ჩართვა, რომლებისთვისაც საზღვართშორისი გადახდებისას დანახარჯების შემცირებით, აუცილებელი მოტივაცია გაჩნდებოდა. ითვლება, რომ Ripple ამ ამოცანას საკმაოდ წარმატებულად წყვეტს, რადგან პირდაპირ აკავშირებს თავისი განაწილებული ქსელის საშუალებით კონტრაგენტებს და ადასტურებს ტრანზაქციას საშუალოდ ოთხ წამში. სულ უფრო მეტი ბანკი ხდება Ripple-ის ქსელის ახალი წევრი, რაც პროექტის აქტიურ განვითარებაზე მეტყველებს.

რაც შეეხება ტექნოლოგიურ ასპექტებს, Ripple-ს აქვს ერთი მნიშვნელოვანი განსხვავება ტრადიციული ბლოკჩეინ-ქსელებისაგან, სახელდობრ – მაინინგის არარსებობა. კრიპტოვალუტა Ripple-ის ემისიის მთელი მოცულობა გენერირებული იქნა პროექტის სტარტიდანვე, ხოლო მონეტების საერთო რაოდენობამ მთელი 100 მილიარდი ერთეული შეადგინა. სწორედ ემისიის ასეთმა დიდმა მოცულობამ ამ კრიპტოვალუტას შესაძლებლობა მისცა, მოხვედრილიყო ტოპ-სიაში კაპიტალიზაციის მიხედვით. ამასთან, 60 მილიარდი მონეტა ინახება სპეციალურ რეზერვში და მთლიანად ამოღებულია ბრუნვიდან. პროექტის კრიპტოვალუტა გამოიყენება პირდაპირი ბანკთაშორისი ტრანზაქციებისათვის, რომლებიც აისახება საერთო გამანაწილებელ რეესტრში. ქსელში საკომისიო არსებობს როგორც ტრანზაქციური სპამის დაცვა, მაგრამ, რადგან მაინინგი ქსელში არ არსებობს, ის უბრალოდ იწვება, რითაც ამცირებს მონეტების ერთობლივ ცირკულაციას. Ripple-ის ქსელის გამტარუნარიანობა წამში დაახლოებით 1500 ტრანზაქციას შეადგენს, რაც საკმაოდ სერიოზული მაჩვენებელია ასეთი დეცენტრალიზებული ქსელისათვის.

დავუბრუნდეთ პოპულარული ალტკოინების მიმოხილვას. არ შეიძლება არ ვახსენოთ Ethereum-ის სმარტ-კონტრაქტების პლატფორმის ერთ-ერთი კონკურენტი პროექტი EOS. ის 2018 წლის იანვარში

გაუშვა კომპანიამ block.one და ასევე იძლევა საშუალებას შეიქმნას სმარტ-კონტრაქტები განაწილებულ ბლოკჩეინ-ქსელში. ამასთან, მათ დასაწერად იყენებენ პროგრამირების პოპულარულ ენას C++. Ethereum-საგან განსხვავებით, რომელშიც სმარტ-კონტრაქტების შესაქმნელად სპეციალურად საამისოდ შემუშავებული ენა Solidity არსებობს, პლატფორმა EOS-ში შემმუშავებლებმა პროგრამული კოდის დასაწერად შეიძლება გამოიყენონ ჩვეული ინსტრუმენტები. ქსელი კონსენსუსის ოქმის სახით იყენებს „წილის დელეგირებულ მტკიცებულებას“ (DPoS), რომლის საშუალებითაც ტრანზაქციები მასში მტკიცდება სულ რაღაც წამის მეოთხედში. ბლოკის შემქმნელი კვანძები შეირჩევა ხმის მიცემის უწყვეტი პროცედურით EOS-ის ლოკალური კრიპტოვალუტის ყველაზე დიდი ბალანსების მფლობელებიდან. ამასთან, კვანძი-დელეგატი, რომელსაც დღე-ღამის განმავლობაში არც ერთი ბლოკი არ შეუქმნია, შემდგომში ავტომატურად თავისუფლდება ამ საპატიო მოვალეობისაგან.

EOS-ის ქსელში ტრანზაქციების საინტერესო თავისებურებას წარმოადგენს მათში წინა ბლოკების ჰეშების შენახვა. ეს იძლევა საშუალებას, თავიდან ავიცილოთ ტრანზაქციის დუბლირება განშტოებებში (ფორკებში) და ცალსახად ახდენს იმის იდენტიფიცირებას, თუ მოცემულ მომენტში რომელ განშტოებაში იმყოფება ქსელის კონკრეტული მომხმარებელი. ტრანზაქციების საკომისიო EOS-ის ქსელში არ არსებობს, ხოლო კრიპტოვალუტა გამოიყენება სმარტ-კონტრაქტებსა და სისტემაში შექმნილი ტოკენების გაცვლის ხელშესაწყობად. სულ მიმოქცევაში EOS-ის დაახლოებით 900 მილიონი მონეტაა. ემისიის მიმდინარე კაპიტალიზაცია შეადგენს 5 მილიარდ დოლარზე ოდნავ ნაკლებს, რაც პროექტს საშუალებას აძლევს, ამ პარამეტრის მიხედვით პირველ ხუთეულში იყოს. ისევე, როგორც პროექტ Ripple-ში, მაინინგი EOS-ის ქსელშიც არ არსებობს, ხოლო მონეტები შეიძლება მივიღოთ მხოლოდ შემმუშავებლებისაგან პირდაპირი ყიდვით, კრიპტოვალუტური ბირჟების მეშვეობით. EOS-ის კრიპტომონეტების პირველადი განთავსებისას ICO-ის ყველა ერთობლივი რაუნდის განმავლობაში შემმუშავებლებმა შეძლეს შეეგროვებინათ დაახლოებით 185 მილიონი დოლარი პლატფორმის შემდგომი განვითარებისათვის.

დაბოლოს, უკანასკნელი პროექტი ყველაზე პოპულარული ალტკოინების რიგიდან, რომელიც გვსურდა განგვეხილა, არის IOTA. თავდაპირველად ის გამიზნული იყო მონაცემებისა და გადახდების გადა-

საცემად საკომისიოს გარეშე მოწყობილობებს შორის ე.წ. „ნივთების (საგნების) ინტერნეტში“. „ნივთების ინტერნეტის“ (Internet of Things) კონცეფცია შეიმუშავეს სხვადასხვა მოწყობილობას, მაგალითად – საყოფაცხოვრებო ხელსაწყოებს შორის ქსელური ურთიერთობებისათვის. ვიზიონერი ტექნოლოგები წინასწარმეტყველებენ, რომ შორს არ არის დღე, როდესაც ადამიანს შეეძლება გადასცეს ფინანსური ოპერაციების ჩატარების შესაძლებლობა ჩვეულებრივ საოჯახო ხელსაწყოებს, რომლებიც ავტომატურად შეისყიდის მათი შეუფერხებელი ფუნქციონირებისათვის აუცილებელ რესურსებს. სწორედ ქსელი IOTA შეიძლება გახდეს მოსახერხებელი გარემო მსგავსი ტრანზაქციების მოსახდენად.

აღსანიშნავია, რომ პროექტი IOTA არ სარგებლობს ბლოკჩეინ-სტრუქტურით, მისი კლასიკური გაგებით, ანუ ქსელში არ არსებობს ბლოკები როგორც ასეთი, არის მხოლოდ ტრანზაქციების ერთობლიობა, რომლებიც ერთმანეთთანაა დაკავშირებული და ქმნის ე.წ. მიმართულ აციკლურ გრაფებს. გრაფების ამ სახეობაში არ არსებობს ციკლები და მათი წიბოები ყოველთვის ერთი მიმართულებისაა. ამ პრინციპზე დაყრდნობით, IOTA-ს ქსელში ყოველი ახალი ტრანზაქცია ადასტურებს ორ ძველს, ხოლო მსგავსი დადასტურებებიდან ყალიბდება ვერიფიკაციების მთელი „ობობას ქსელი“, რომელიც ქსელს ორმაგი ხარჯვებისაგან იცავს. ქსელის კრიპტოვალუტას „იოტა“ ეწოდება, ხოლო მისი ემისია დასრულებულია და შეადგენს ასტრონომიულ სიდიდეს – 2 779 530 283 277 761 მონეტას. ბლოკების არარსებობის გამო ქსელში არ არსებობს მაინინგიც, ხოლო ყველა ტრანზაქცია განთავისუფლებულია საკომისიოსაგან. მონეტა იოტის მოსახერხებელი გამოყენებისათვის მას ითვლიან მილიონებში ანუ MIOTA-ებში. მიმდინარე მომენტისათვის, პროექტის კაპიტალიზაცია დაახლოებით 900 მილიონ დოლარს შეადგენს.

სხვადასხვა სახის ალტკოინების პროექტების განხილვისას პერიოდულად შეიძლება გადავაწყდეთ რეალიზაციებს, რომელთა სახელებიც პოპულარული ბლოკჩეინ-პროექტების სახელებიდანაა ნაწარმოები. ამასთან, თვით ისინი პოზიციონირებს როგორც პირველსახეების მოდიფიცირებული ასლები, რომლებმაც რაღაც მომენტიდან დამოუკიდებელი ცხოვრება დაიწყო. ასეთ ალტკოინებს პროექტების ფორკები ეწოდება. როგორ ჩნდება ისინი და როგორ იქცევა ბლოკჩეინ-ინდუსტრიის ნაწილად?

ფორკები

ისეც ხდება, რომ თანამოაზრეთა ჯგუფი, რომლებიც ადრე რაღაც შემოქმედებითი, პოლიტიკური, კომერციული ან რაიმე სხვა ეგიდის ქვეშ გაერთიანებული საზოგადოების წევრები იყვნენ, კარგავენ ურთიერთგაგებას.

ჩვეულებრივ, ეს გამოიხატება შეხედულებების სერიოზული დაშორების კონსტატაციით იმაზე, თუ რის შექმნას ან განვითარებას ცდილობენ ისინი ერთობლივი ძალისხმევით. მაშინ გაერთიანება იშლება, რეორგანიზდება სხვადასხვა ჯგუფად, რომლებსაც თავისებურად ესმით მომავალი განვითარების გზების ეფექტიანობა. ასე იქმნება განშტოებები საერთო, მაგრამ სხვადასხვა მომავლის მქონე ისტორიიდან. ეს პროცესი ბუნებრივია, უსასრულო და ჩვეულიც კი, რადგან მუდმივად ვლინდება ადამიანთა ცხოვრების სხვადასხვა სფეროში. ბლოკჩეინ-ინდუსტრია ამ შემთხვევაშიც არ გამხდარა გამონაკლისი, მასში სხვადასხვა სახის პროექტების წარდგენის ღია ფორმა არცთუ მცირედ უწყობდა ხელს მსგავსი პროცესების ბუნებრივად წარმოქმნას.

მართლაც, ბლოკჩეინ-ტექნოლოგიებზე დაფუძნებული პროექტების დიდი უმრავლესობა აქვეყნებს თავიანთი პროგრამების საწყის ტექსტებს ღია სახით, რათა მათი გაცნობა ნებისმიერ მსურველს შეეძლოს. ამისათვის რამდენიმე მიზეზი არსებობს. ჩვეულებრივ, ღია კოდი ლოგიკურია, თუ საუბარია თანაბარუფლებიან წევრთა დეცენტრალიზებული ქსელის ორგანიზაციაზე, რომელშიც შემმუშავებელს არ აქვს რაიმე განსაკუთრებული უპირატესობები. გარდა ამისა, ღია კოდის არსებობა ქსელის წევრებს ქსელში მიმდინარე ყველა პროცესის სრული გამჭვირვალობის, ისევე, როგორც კონსენსუსით მიღებულ ოქმებთან მათი სრული შესაბამისობის გარანტიას აძლევს. დაბოლოს, ეს ნებისმიერ მსურველს საშუალებას აძლევს, შეამოწმოს კოდი ზიანის მომტანი ელემენტების არსებობაზე, რომლებიც თეორიულად შესაძლებელია პროგრამაში ჩადებულიყო შემუშავების დროს. სხვა სიტყვებით რომ ვთქვათ, შემმუშავებლებისათვის ღია კოდის მიწოდება აუცილებელი ზომაა, რომელიც მისი ყველა წევრის მხრიდან პროექტისადმი ნდობას უზრუნველყოფს.

მაგრამ გამჭვირვალობის უზრუნველყოფის ამ ტრადიციას მეორე მხარეც აქვს. ის ქმნის მაქსიმალურად ხელსაყრელ პირობებს საწყისი კოდის მესამე პირების მიერ ნაწილობრივ ან სრულად გადმოღებისათვის. მნიშვნელობა არ აქვს, იყვნენ თუ არა ეს პირები გუნდის წევრები ადრე, თუ საუბარია სრულიად უცხო სუბიექტებზე, რომლებმაც ამგვარად გადაწყვიტეს პროექტის გაუმჯობესება, საკუთარი შეხედულებისამებრ მასში ეფექტიანობისა და სარგებლიანობის მიზნით ცვლილებებისა და დამატებების შეტანით. ასე წარმოიქმნება განშტოება საბაზო პროექტიდან, რომელსაც ბლოკჩეინ-ინდუსტრიაში უწოდებენ „ფორკს“, რაც ინგლისურად „ჩანგალს“ ნიშნავს. ცნება „ფორკს“ უკვე გავეცანით ბლოკების ჯაჭვში იმ მომენტში წარმოქმნილი განშტოებების განხილვისას, როდესაც სხვადასხვა კვანძმა დროის ერთ მომენტში შეიძლება შექმნას კონკურენტი ბლოკები. მაგრამ ამ სახის ფორკები არ იწვევდა ახალი პროექტების გაჩენას, რადგან კონსენსუსის ოქმები ბლოკჩეინ-ქსელების ნებისმიერ კონცეფციაში აუცილებლად გულისხმობდა ჭეშმარიტი ჯაჭვის ამორჩევას და იმავდროულად, ცრუ განშტოებების უკუგდებას.

მაგრამ არსებობს სხვა სახის ფორკებიც, და მათთან საქმე უფრო რთულადაა, რადგან საუბარია კოდის უშუალო ცვლილებაზე ბლოკჩეინ-პროექტის კლიენტის ნაწილში. გამოიყოფა ასეთი ფორკების ორი ვარიანტი – რბილი (სოფტფორკი) და ხისტი (ჰარდფორკი). უმრავლეს შემთხვევაში, ფორკების ინიცირება ხდება თავად პროექტის შემმუშავებლების მიერ, როდესაც მის ლოგიკაში აუცილებელია რაღაც ცვლილებების შეტანა. თუ ცვლილებებმა კვანძის პროგრამული უზრუნველყოფის აუცილებელი შეცვლის მოთხოვნა არ გამოიწვია, მაშინ საუბარია სოფტფორკზე. სოფტფორკის აქტივაციისას ქსელში არ არსებობს ახალი წესების ძველ კვანძებთან შეთანხმების აუცილებლობა. სოფტფორკი შეიძლება საკმაოდ ბევრი იყოს, ისინი ჩნდება კლიენტის კვანძის პროგრამული უზრუნველყოფის ახალი ვერსიების გამოსვლასთან ერთად, რომლებსაც არავითარი შეუქცევადი ცვლილებები არ შემოაქვს არც ქსელის წესებში და არც მონაცემთა შენახვის ფორმატში.

ჰარდფორკებთან საქმე სხვაგვარადაა. იმ შემთხვევაში, თუ კვანძების ნაწილი ახალ ცვლილებებს არ იღებს და თავის პროგრამულ უზრუნველყოფას არ განაახლებს, ისინი ვერანაირად ვერ შეძლებს იმ

კვანძებთან ურთიერთობას, რომლებიც ამ ფუნდამენტურ მოდიფიკაციებს დათანხმდა. თუ გაჯიუტებულთა რიცხვი საკმაოდ დიდია, მათ შეუძლია, ჩამოყალიბდნენ ცალკე ქსელად, რომელიც გაატარებს ძველ პრინციპებს, პროექტის კოდის მასშტაბურ გადამუშავებამდე რომ არსებობდა. ანდა, პირიქით, ქსელის აქტიური კვანძები, რომლებსაც სურს დანერგოს, მათი აზრით, პროგრესული ცვლილებები, ეჯახება შემმუშავებელთა კონსერვატიზმს, რომლებიც უარს ამბობენ კოდში მათ ინტეგრირებაზე და დაჟინებით ამტკიცებენ ცვლილებების მიზანშეუწონლობას. ორივე შემთხვევაში ერთსა და იმავე შედეგს ვიღებთ – წარმოიქმნება ჰარდფორკი, რომელიც წარმოშობს ბლოკთა ორ ბაზას ერთის მაგივრად და თითოეული მათგანი ამ მომენტიდან, ბლოკჩეინ-ინდუსტრიაში დამოუკიდებელ ცხოვრებას იწყებს.

ჰარდფორკის შედეგად წარმოქმნილი ახალი პროექტი იღებს შემმუშავებელთა საკუთარ გუნდს, რომელიც ჩამოყალიბებული ან ადრე შექმნილია საინიციატივო ჯგუფის ბაზაზე, ან რომელიღაც მეწარმის ნებით, რომელმაც რიგ შემთხვევებში წინასწარი განზრახვით გამოიწვია გაყოფა. პროექტი იღებს ახალ სახელს, როგორც წესი, ნაწარმოებს საბაზო დასახელებიდან. ლოკალურ კრიპტოვალუტასაც ეცვლება სახელი და იღებს ცალკე საბაზრო ტიკერს, ანუ შემოკლებულ დასახელებას, შედგენილს რამდენიმე სიმბოლოსაგან. შემდეგ პროექტის კოდი მოდიფიცირდება იმ თავისებურებების გათვალისწინებით, რომლებიც სწორედაც გახდა პროექტის ორ განშტოებად გაყოფის მთავარი მიზეზი. მთლიანობაში, ასეთი პროცესი ანალოგიურია იმისა, რაც ჩვეულებრივ ბიზნესგარემოშიც ხდება, როდესაც რომელიღაც კომპანიიდან გამოიყოფა გუნდი, რომელიც ქმნის საკუთარ კომპანიას, წინა სამუშაო ადგილზე შეძენილი გამოცდილებისა და ზოგჯერ, იქვე მოპოვებული აქტივების ბაზაზე.

გაურკვევლობის თავიდან ასაცილებლად, როდესაც მომავალში ცნება „ფორკით“ ვისარგებლებთ, მხედველობაში გვექნება სწორედ „ჰარდფორკი“. ახლა ვეცადოთ, ვუპასუხოთ კითხვას: ნეგატიური თუ პოზიტიური მოვლენაა საბაზო პროექტებში ფორკების წარმოქმნა? როგორც ხშირად ხდება, სიტუაცია ორი მხრიდან შეგვიძლია განვიხილოთ. რასაკვირველია, კონკურენტი პროექტის გაჩენა, რომელიც ფუნქციონალის მიხედვით ძალზე ახლოსაა საბაზოსთან, იწვევს ორ

ქსელს შორის აუდიტორიის გაყოფას. საბაზო პროექტში, თუმცა როგორც წესი, არცთუ ძლიერად, მაგრამ მაინც, იკლებს მოთხოვნა ადგილობრივ კრიპტოვალუტაზე, ხოლო ბირჟებზე მისით ვაჭრობის მოცულობები მცირდება. მაგრამ ამ პროცესებში არის ერთი დადებითი მომენტიც მფლობელებისთვის, რომლებსაც პროექტების გაყოფამდე საბაზო კრიპტოვალუტის მნიშვნელოვანი მოცულობები ჰქონდათ. საქმე ისაა, რომ ფორკის შექმნის მომენტში ბლოკების მონაცემთა ბაზა ერთი ერთში კოპირდება ახალ განშტოებაში და მხოლოდ შემდეგ ჩნდება ამ ბაზებს შორის დესინქრონიზაცია ტრანზაქციების ძიებაში, რომლებიც ყოველ განშტოებაში ერთმანეთისაგან დამოუკიდებლად წარმოიქმნება. რას ნიშნავს ეს?

ეს ნიშნავს, რომ საბაზო პროექტში კრიპტოვალუტის მფლობელები ავტომატურად მიიღებენ ზუსტად იმავე ბალანსს ახალ ქსელში, ნომინირებულს ფორკის კრიპტოვალუტაში. ეს იმიტომ ხდება, რომ ყველა ძველი ტრანზაქცია გაყოფამდე, ორივე პროექტში აბსოლუტურად იდენტურია. ამიტომ, თუ ახალი კრიპტოვალუტა იღებს რაიმე საბაზრო შეფასებას, მაშინ მისი მფლობელებისათვის ეს შეიძლება შეფასდეს როგორც დამატებითი მონეტარული შემოსავალი, რადგან მათი ბალანსები ძირითად ქსელში უცვლელი რჩება. ფორკის გამო მიღებული კრიპტოვალუტა მათ შეუძლიათ გაყიდონ ბირჟებზე და მიიღონ დამატებითი შემოსავალი, რომელიც გარკვეულად უკომპენსირებს ამ პროექტის გაყოფით შექმნილ უხერხულობას. გასაგებია, რომ დიდი ალბათობით, ფორკის კრიპტოვალუტის საბაზრო ღირებულება საბაზოზე მნიშვნელოვნად ნაკლები იქნება, მაგრამ ნულზე მაღალი ნებისმიერი ღირებულება უკვე სუფთა შემოსავალს წარმოადგენს, რომელიც ციდან ჩამოვარდა.

ფორკების შექმნის ლოგიკა საბაზო წინასახეების ფუნდამენტური შეზღუდვების გადალახვას ეფუძნება. ბიტკოინ-ქსელის გაშვებიდან უკვე რამდენიმე წლის შემდეგ დაიწყო მისი მასშტაბირების შესაძლო საზღვრების გამოსახვა. განიხილებოდა ფაქტორები, რომლებიც დაკავშირებული იყო პირველ რიგში, ტრანზაქციების დამუშავების სიჩქარესა და ბლოკის ზომასთან, რომელიც შემოფარგლული იყო ერთი მეგაბაიტით. ბიტკოინის პირველი ისტორიული ფორკი 2015 წელს წარმოქმნილი BitcoinXT-ის რეალიზაცია გახდა. კლასიკური ბიტკოინისაგან განსხვავებით, ამ ფორკში ბლოკის ზომა რვა მეგაბაიტამდე

გაიზარდა, რის შემდეგაც, ბლოკის ზომის ყოველწლიური გაორმაგება დაიგეგმა. თავიდან ფორკი კეთილგანწყობით მიიღეს ბიტკოინ-საზოგადოებაში, ხოლო BitcoinXT-ის კვანძების რაოდენობა დაახლოებით 4000-ჯერ გაიზარდა. მაგრამ უკვე 2016 წელს მისი პოპულარობა დაეცა, ხოლო კვანძების რაოდენობა ორ ათეულამდე შემცირდა, რაც ფაქტობრივად, ფორკის სიკვდილს მოასწავებდა.

BitcoinXT-ის არასახარბიელო ბედმა ვერ შეაჩერა ბიტკოინის ისეთი ფორკის შექმნის მცდელობები, რომლებიც მოწოდებული იქნებოდა პროექტ-წინაპრისათვის პირველობის ჩამოსართმევად. 2017 წლის 1-ლ აგვისტოს გაშვებული იქნა ალბათ ბიტკოინ-პროექტის ქსელის ფორკებს შორის ყველაზე „სახელიანი" – Bitcoin Cash, რომელსაც მხარი დაუჭირა ბლოკჩეინ-საზოგადოების აქტივისტმა და კრიპტოვალუტის ინვესტორმა როჯერ ვერმა. ამ ფორკმა კრიპტოინდუსტრიაში პოპულარობის მოპოვება დაიწყო. მისი არსი ბევრი რამით გვაგონებდა BitcoinXT-ის, რადგან ისიც ითვალისწინებდა ბლოკის ზომის 8 მეგაბაიტამდე გაზრდას. გარდა ამისა, Bitcoin Cash-ში განხორციელდა კიდევ რამდენიმე ტექნოლოგიური სიახლე, როგორებიცაა ქსელის სირთულის დაჩქარებული ცვლილება და ახალი ტიპის გაძლიერებული კრიპტოდაცვის მქონე ტრანზაქციების შემოღება. Bitcoin Cash-ის გაშვებიდან ერთი წლის შემდეგ, ბლოკის ზომა მის ქსელში კიდევ ოთხჯერ – 32 მეგაბაიტამდე გაიზარდა.

ფორკის მიმართ ყურადღების ერთ-ერთი მთავარი ფაქტორი იყო AISC მოწყობილობების ჩინური მწარმოებლისა და რამდენიმე მსხვილი მაინინგური პულის მხარდაჭერა. აშკარაა, რომ ინტერესი ნაკარნახევი იყო ამ სუბიექტების სურვილით, გაფართოებულიყო მოწყობილობების გასაღების ბაზარი და კიდევ უფრო დიდი რაოდენობის კვანძები მოეზიდათ მაინინგის პროცესში. აქვე უნდა აღინიშნოს, რომ ყველა მაინერი როდი ემხრობოდა ბლოკის ზომის გაზრდას, რადგან ეს პოტენციურად, მათ მიერ გამომუშავებული ტრანზაქციების საკომისიოების შემცირებას იწვევდა. რადგან მოკლევადიანი მონეტარული მიზნები ჰქონდათ, მაინერები განსაკუთრებით არ ზრუნავდნენ ბიტკოინის პროექტის შემდგომ განვითარებაზე, იმიტომ, რომ მათ სავსებით აძლევდათ ხელს შეზღუდული ზომის ბლოკებში ადგილის დეფიციტი. საქმე ისაა, რომ ქსელზე დატვირთვის გაზრდა ავტომატურად იწვევდა გამგზავნების მიერ მითითებული საკომისიოების

ზრდას, რომლებსაც სურდათ, რაც შეიძლება სწრაფად მოეთავსებინათ თავიანთი ტრანზაქციები უახლოეს შესაქმნელ ბლოკებში.

კრიპტოინდუსტრიის სპეციალისტებმა დათვალეს, რომ მხოლოდ ბიტკოინმა განიცადა დაახლოებით შვიდი ათეული შედარებით ცნობილი ფორკი, ამასთან, მათმა უდიდესმა უმრავლესობამ ვერ მოიპოვა რამდენადმე მნიშვნელოვანი პოპულარობა. თავიდან ინფორმაცია ყოველ მოახლოებულ ფორკზე ნეგატიურ გავლენას ახდენდა ბიტკოინ-მონეტების საბაზრო ღირებულებაზე. მაგრამ როდესაც ფორკების, რომ იტყვიან, ბღუჯა-ბღუჯა გამოჩენა დაიწყო, ამ პროცესმა გავლენა დაკარგა საბაზო კრიპტოაქტივის ფასზე, ხოლო ფორკის მონეტების ღირებულება იშვიათად აჭარბებდა 1 დოლარსაც კი. ბიტკოინის ფორკების უმრავლესობის შექმნის მიზეზი იმ პერიოდში იყო მხოლოდ შემქმნელების სურვილი კრიპტოსფეროსადმი საზოგადოებრივი ინტერესის ამაღლების მონეტიზებისა. ამასთან, ისინი მაინცდამაინც არ ზრუნავდნენ იმ ფასეულ შეთავაზებებზე, რომლებიც ფორკებს შეიძლებოდა ინდუსტრიისათვის მიეწოდებინა.

2017 წლის ბოლოს მსოფლიო საზოგადოების კრიპტოვალუტებისადმი ინტერესის უეცარი აფეთქებისა და მისი მომდევნო ფასთა მნიშვნელოვანი კორექციის შემდეგ, ფორკების რაოდენობის შემცირება დაიწყო და მათ თითქმის აღარავინ აქცევდა ყურადღებას. კრიპტოსაზოგადოებამ თავისი ინტერესის ფოკუსი მიაბრუნა საბაზო ბიტკოინ-პროექტის განვითარებისაკენ, რომელიც აქტიურად აგრძელებდა დომინირებას კრიპტოინდუსტრიაში ისეთივე მნიშვნელოვანი მასშტაბით, როგორიც თავისი მრავალი მოდიფიკაციის აქტიური გამოჩენის პერიოდამდე ჰქონდა.

რა თქმა უნდა, ფორკები შეიძლება გაუჩნდეს არა მარტო ბიტკოინს. თუ მთლიანობაში ალტკოინებს შევხედავთ, დავინახავთ, რომ მაშინ ალბათ ყველაზე ცნობილი ფორკი წარმოიშვა Ethereum-ის ქსელში სულ ცოტა ხანში მას შემდეგ, რაც ეს ქსელი გაშვებული იქნა მასობრივი მოხმარებისათვის. 2016 წლის გაზაფხულზე ჩატარდა ინვესტიციათა დეცენტრალიზებული მომსახურების პროექტის – The DAO-ის წარმატებული ICO, რომელიც Ethereum-ის პლატფორმის ბაზაზე აიგო. პროექტის დასახელება იშიფრება როგორც „დეცენტრალიზებული ავტონომიური ორგანიზაცია“. ის ორგანიზაციული მართვის, მის ბლოკჩეინ-გარემოში დეცენტრალიზაციის საშუალებით, ახალი

მიდგომის კარგ მაგალითად იქცა. პროექტს მთლიანად დაუჭირა მხარი თვით Ethereum-ის ავტორმა ვიტალიკ ბუტერინმა და გარკვეულწილად ამის გამო, The DAO-ის ტოკენების განთავსებისას შეგროვდა უზარმაზარი თანხა – ეთერის 12 მილიონი მონეტა. ამ მომენტისათვის მოზიდული ინვესტიციები დაახლოებით 165 მილიონ დოლარად შეფასდა, ამჟამად ის 3 მილიარდ დოლარს მიუახლოვდებოდა.

მაგრამ უკვე 17 ივნისს The DAO-ის ხელმძღვანელებმა განაცხადეს ეთერის ყველა მოზიდული მონეტის 30%-ის გატაცების შესახებ, რაც დაახლოებით 50 მილიონ დოლარს შეადგენდა. ამ ცნობამ წარმოშვა პანიკა ბაზარზე და ეთერის ფასი მნიშვნელოვნად დაეცა. გარკვეული დროის შემდეგ გაირკვა, რა მოხდა. The DAO-ის სმარტ-კონტრაქტის კოდში აღმოჩნდა სისუსტე, დაკავშირებული ე.წ. „რეკურსულ გამოძახებებთან“, როდესაც პროგრამული პროცედურა საშუალებას იძლეოდა, ციკლურად გაეშვა საკუთარი თავი. ამან შექმნა შესაძლებლობა, გადაეტანათ ფული The DAO-ის საფულიდან მის სპეციალურად შექმნილ შვილობილ სტრუქტურებზე უსასრულოდ ბევრჯერ, დედობილი კომპანიის მრავალჯერადი გაყოფის საშუალებით. Ethereum-ის ქსელის მომხმარებელთა საზოგადოებისათვის წარმოიშვა სერიოზული დილემა: ჩაეტარებინათ თუ არა მთელი ქსელის ჰარდფორკი, რითაც გააუქმებდნენ ბოროტმოქმედთა ტრანზაქციებს, თუ ჩაეთვალათ ასეთი სიტუაციები დეცენტრალიზებულ ღია გარემოში ბუნებრივად და ეცადათ, მომავალში მსგავსი სისუსტეების წარმოქმნა არ დაეშვათ.

სისტემის მომხმარებელთა უმრავლესობა, ბუტერინის ჩათვლით, ჰარდფორკის ჩატარების მხარდაჭერით გამოვიდა. მაგრამ ამ გადაწყვეტილებას გამოუჩნდნენ მოწინააღმდეგეებიც, რომლებმაც „ტრანზაქციური უკუთამაშის“ ნებისმიერი ფორმა უპატიოსნო ზომად ჩათვალეს. ისინი ამტკიცებდნენ, რომ ეს პრეცედენტი ფართო საშუალებებს ტოვებს მომავალი ჩარევებისათვის, რაც სერიოზულ საფრთხეს წარმოადგენს თვით სისტემის დამოუკიდებელი არსებობისათვის. თუმცა ჰარდფორკი, მიუხედავად პროტესტებისა, მაინც მოხდა და The DAO-ის ინვესტორებს დაუბრუნეს მოპარული სახსრები, ამის მოწინააღმდეგე მომხმარებლებმა შექმნეს საკუთარი განშტოება, რომელშიც სახსრების ასეთი დაბრუნება შეუძლებელი იყო. ამ ფორკს ეწოდა Ethereum Classic, რაც ხაზს უსვამს მის ორთოდოქსულობას ქსელის თავისუფალ მუშაობაში შესაძლო ჩარევების თვალსაზრისით. მიუ-

ხედავად Ethereum-ის შემქმნელისა და მთელი საზოგადოების მხარდაჭერის არარსებობისა, ქსელი Ethereum Classic მაინც გადარჩა. ის დღესაც არსებობს, თუმცა ფორკის მონეტის ღირებულება იმ დროის შემდეგ პრაქტიკულად არ გაზრდილა და ძირითადი ქსელის მონეტის ფასის დაახლოებით 4%-ს შეადგენს.

ზემოთქმულის შეჯამებისას გვინდა აღვნიშნოთ, რომ, მიუხედავად ფორკების ავტორების მიერ დიდი იმედისა, პროექტების მსგავსმა კლონებმა მნიშვნელოვანი ადგილის დაკავება ბლოკჩეინ-ინდუსტრიაში ვერ შეძლო. დარწმუნებით შეგვიძლია ვთქვათ, რომ ფორკების უდიდესი უმრავლესობა პირდაპირი მნიშვნელობით შეერია სხვა ათასობით პროექტს, აგებულს განაწილებული რეესტრის ტექნოლოგიის ბაზაზე. ბლოკჩეინ-ინდუსტრიაში ახალი პროექტები იქმნება საკმაოდ სწარაფად და დიდი რაოდენობით. ამას, რა თქმა უნდა, ხელს უწყობს უფრო ადრინდელი პროექტების საწყისი კოდის ღიაობა, საიდანაც ახალი ბლოკჩეინ-სტარტაპების შემმუშავებლები მთელი სეგმენტების გადმოღებას მისდევენ, რათა დაზოგონ დრო და რესურსები და უკვე არსებული მოდულებისა და პროცედურების ხელახლა შექმნას დააღწიონ თავი.

საბოლოოდ, ეს საშუალებას აძლევს ბლოკჩეინ-ტექნოლოგიას განვითარდეს ბევრად უფრო სწრაფად, ვიდრე იმ პირობებში, როდესაც პროექტების საწყის ტექსტებს შემმუშავებლები არ აქვეყნებდნენ. შესაძლოა, სწორედ ამ ტექნოლოგიური ღიაობის გამო გაჩნდა კრიპტოინდუსტრიაში ბევრად უფრო მნიშვნელოვანი მოვლენა, ვიდრე ჩვეულებრივი ფორკებია, რომელმაც მისი გარკვეული სექტორიც კი ჩამოაყალიბა. საუბარია პროექტებზე, რომლებიც თავისი მომხმარებლებისათვის მკაცრ ანონიმურობას უზრუნველყოფს. ახლა გავერკვეთ კანონზომიერად წარმოჭრილ საკითხში: რატომ გახდა მსგავსი პროექტები ასეთი მოთხოვნადი გარემოში, სადაც ანონიმურობა ისედაც ტექნოლოგიის განუყოფელი ნაწილია?

ანონიმურობა ბლოკჩეინში

ოდესღაც, ძალზე დიდი ხნის წინ ბანკის ნებისმიერი მეანაბრის სურვილი, საიდუმლოდ შეენახა თავისი სახელი, საპატიოდ და რესპექტაბელურად ითვლებოდა. განსაკუთრებით, თუ საქმე გვქონდა დიდ თანხებთან. მიზეზი, ბანკის კლიენტებს ინკოგნიტოდ დარჩენისკენ რომ უბიძგებდა, მრავალი იყო, მათ არც კი ჩამოვთვლით. თუმცა, თვით ბანკირებს ეს მიზეზები დიდად არ აინტერესებდათ, რადგანაც ისინი საკუთარ ვალდებულებად თვლიდნენ, ზედმიწევნით შეენახათ საბანკო საიდუმლო და თავიანთ საცავებში დაეცვათ კლიენტების სახსრები რამდენ ხანსაც უნდოდათ. ხანგრძლივი დროის განმავლობაში პოპულარული იყო ანგარიშის ნომრები წარმდგენზე, როდესაც ნებისმიერ ბანკში შესულ სუბიექტს მოლარისათვის ანგარიშის პაროლის თქმის შემდეგ შეეძლო წვდომა მიეღო სახსრებთან, ხოლო სურვილის შემთხვევაში მთლიანად გაეტანა ისინი. მაგრამ ის დალოცვილი დრო წარსულს ჩაჰბარდა, რადგან რომელიღაც მომენტში უმრავლესი სახელმწიფოების მთავრობები შეაწუხა საკუთარი მოქალაქეების მიერ კანონიერი დაბეგვრისთვის თავის არიდების პრობლემამ.

ამის შემდეგ ყველა ბანკი და სხვა საფინანსო ორგანიზაცია თავიანთი კლიენტების იდენტიფიკაციის აუცილებელ პროცედურებს ახორციელებს, ხოლო საბანკო საიდუმლოს ცნება უკვე აღარ არის საკრალური და უფრო უარყოფით შინაარსს ატარებს ეროვნული ფინანსური რეგულატორების თვალში. ეს სამთავრობო ორგანიზაციები ახორციელებენ მკაცრ ზედამხედველობას თავიანთი ქვეყნების ფინანსურ ინდუსტრიაზე და ეჭვის გაჩენის შემთხვევაში უფლება აქვთ დაადანაშაულონ მათ კონტროლს დაქვემდებარებული საკრედიტო ინსტიტუტები თანამედროვე საქმიანი სამყაროს ერთ-ერთ მომაკვდინებელ ცოდვაში – ფულის გათეთრებაში. თუმცა, რეალურ ბოროტმოქმედებთან ბრძოლის მაგივრად, მსოფლიო საფინანსო დარგს ესვრიან „წვრილთვალა ბადეს“, რომელშიც ხშირად ებმებიან მცირე ორგანიზაციები და საშუალო შეძლების კერძო პირები, რომელთა ფინანსური ოპერაციები ბანკებსა და მათ რეგულატორებს არცთუ მთლად გამჭვირვალედ ანუ საეჭვოდ ეჩვენებათ.

განსაკუთრებით უჭირთ მათ, ვინც ფინანსურ გარიგებებს დებს თავიანთი საგადასახადო რეზიდენციის ქვეყნის ფარგლებს გარეთ. არსებობს საკმაოდ დიდი ალბათობა იმისა, რომ ბანკებმა მათ ანგარიშები დაუხურონ ან მინიმუმ, სახსრები დაბლოკონ. თანაც ეს გააკეთონ განსაკუთრებული საფუძვლის გარეშე, რადგან ბანკს არ აქვს არავითარი სურვილი, გარისკოს თავისი ლიცენზიით, რომელსაც რეგულატორი სერიოზული პროცედურული დარღვევების გამო გაუუქმებს. რადგან რეგულატორები ბანკებიდან შემოსული ინფორმაციის უზარმაზარ მოცულობებს ვერ უმკლავდებიან, ისინი თანდათანობით, ფულის გათეთრებასთან დაკავშირებულ საკუთარ ფუნქციას თავად საფინანსო ინსტიტუტებს აბარებენ. ისინი კი, თავის მხრივ, იძულებულნი ხდებიან, რეინვესტირება გაუკეთონ თავიანთ შემოსავლებს არა ძირითად საქმიანობაში, არამედ კლიენტებისა და მათი ფინანსური ნაკადების კონტროლის ინფრასტრუქტურის განვითარებაში. ბანკების ქმედებები საკუთარი კლიენტების მიმართ სულ უფრო მკაცრი ხდება, რაც, რა თქმა უნდა, მსოფლიოს ეკონომიკას მთლიანობაში არ ადგება. ამიტომ სულაც არ არის გასაკვირი, რომ ამ ქმედებების საპასუხოდ ცივილიზაციამ ბუნებრივი რეაქცია მოახდინა, ბლოკჩეინ-პროექტების სახით, სადაც ანონიმურობა თვით ტექნოლოგიის ერთ-ერთი მთავარი ფასეულობა გახდა. და ეს ფასეულობა მოთხოვნით სარგებლობს საფინანსო მომსახურების მომხმარებლებში მთელ მსოფლიოში.

მონაცემთა შენახვის მოდელი და მათი მართვა ბლოკჩეინში გულისხმობს, რომ ქსელის მომხმარებლები თავიანთ ოპერაციებს ახორციელებენ გაუპიროვნებელი მისამართების სახელით, რომლებიც ჰეშირებული კრიპტოგრაფიული გასაღებების ფორმით წარმოგვიდგება.

ამგვარად, შეუძლებელია რომელიმე ფიზიკური პირის დაკავშირება მის ბლოკჩეინ-მისამართთან, გარდა ზოგიერთი განსაკუთრებული შემთხვევისა. ერთ-ერთ ვარიანტად შეიძლება გახდეს მფლობელის მიერ თავისი მისამართის ნებაყოფლობითი გამოცხადება და მასზე განთავსებული სახსრების ფლობის ფაქტის აღიარება. კიდევ, მსგავსი დაკავშირება ლოგიკური დასკვნის სახით შეიძლება გამოვიტანოთ, როგორც ეს სატოში ნაკამოტოს შემთხვევაში მოხდა. ეჭვს არ იწვევს, რომ ის იყო პირველი მაინერი ბიტკოინ-ქსელში, ანუ ყველა სამაინინგო ანაზღაურება ქსელში ყველაზე ადრეული ბლოკების შექმნისათვის სწორედ მის კუთვნილ მისამართებზე გროვდებოდა.

მიუხედავად იმისა, რომ ბლოკჩეინ-ქსელის კონკრეტული მისამართის ფიზიკური მფლობელის განსაზღვრა შეუძლებელია, უმრავლეს შემთხვევაში ნებისმიერ მსურველს მაინც შეუძლია თვალყური ადევნოს ამ ანგარიშის ბალანსს და მასთან დაკავშირებულ ყველა კრიპტოვალუტურ გადარიცხვას. რაღაც მომენტში გაირკვა, რომ ასეთი სიტუაცია ბლოკჩეინ-ტექნოლოგიებზე აგებული ქსელის ყველა წევრს როდი აწყობს. ამ მომხმარებლებმა ისურვეს ანონიმურობის მაღალი ანუ ისეთი ხარისხის მიღება, როდესაც შეუძლებელი იქნება როგორც ქსელის კონკრეტული წევრის ანგარიშებზე განთავსებული სახსრების რაოდენობის, ასევე იმ მოცულობების განსაზღვრა, რომელსაც ის ანგარიშებს შორის რიცხავს. დამატებითი საიდუმლოობის მოთხოვნილებამ გამოიწვია რიგი პროექტების გაჩენა, რომლებიც მომხმარებლისთვის ამის უზრუნველსაყოფად მზად იყო, რისთვისაც იყენებენ სხვადასხვა კრიპტოგრაფიულ ალგორითმს, დაკავშირებულს ტრანზაქციების საწყისი ციფრული ხელმოწერების დაფარვასთან.

ჯერ კიდევ 2012 წლის ივლისში კრიპტოსამყაროში გაჩნდა პროექტი Bytecoin, რომელიც ბლოკჩეინში ტრანზაქციების სრულ ანონიმურობას უზრუნველყოფდა. სისტემის შემქმნელი გახდა შვიდი შემმუშავებელი, რომლებმაც თავიანთ პროექტში გამოიყენეს ოქმი CryptoNote, რომელიც მომატებულ საიდუმლოობას უზრუნველყოფდა. მაგრამ ფართო მოხმარებაში ქსელის გაშვების მომენტისთვის გაირკვა, რომ Bytecoin-ის მონეტების 80% გამოშვებული და წინასწარ განაწილებული იყო თვით შემმუშავებლებსა და მათთან დაკავშირებულ პირებს შორის. ამან პროექტისადმი სისტემის ახალი, დამოუკიდებელი მომხმარებლების უნდობლობა გამოიწვია. ამ ვითარების გათვალისწინებით, Bytecoin-ის ორმა შემმუშავებელმა – რიკარდო სპანიმ და ფრანსისკო კაბანიასმა გადაწყვიტეს სისტემის ფორკის შექმნა, მისი ნაკლოვანებების გამოსწორებისა და ფუნქციურობის გაუმჯობესების მიზნით. მიუხედავად იმისა, რომ ისინი ადრე შექმნილი Bytecoin კოდის მნიშვნელოვან ნაწილს იყენებდნენ, სისტემის მუშა მდგომარეობაში მოსაყვანად მაინც გარკვეული დრო გახდა საჭირო. ახალი სისტემა გაუშვეს 2014 წლის აპრილში, სახელწოდებით Monero, რაც ესპერანტოს ენაზე „მონეტას“ ნიშნავს.

პროექტი Monero დამცავი ოქმით Proof-of-Work სარგებლობს, თუმცა თავიდან ქსელი გაშვებული იყო მაინინგის გარეშე, რომელიც მხოლოდ რამდენიმე კვირის შემდეგ გახდა ხელმისაწვდომი.

ქსელში გამოიყენება ოქმი CryptoNote, რომელიც უზრუნველყოფს ე.წ. „ობფუსკაციის“ პროცესს, ანუ იმ ინფორმაციის „აბურდვას“ ან „შერევას“, რომელსაც ქსელის ტრანზაქციები შეიცავს. ამ მიზნის მისაღწევად სარგებლობენ წრიული ხელმოწერის მეთოდით, რომლის გამოც უცხო დამკვირვებელი ვერაფრით გაარკვევს, ვინ არის ტრანზაქციის ჭეშმარიტი გამგზავნი ან მიმღები. რამდენიმე წლის შემდეგ, 2017 წლის ბოლოსათვის, ქსელის პროგრამულ კოდში დამატებით შეიტანეს ალგორითმი RingCT, რომელიც გადასაგზავნი თანხების საიდუმლოებას უზრუნველყოფს. ჩვეულებრივ, ბიტკოინის მსგავს კრიპტოსისტემებში მომხმარებელს აქვს მხოლოდ ერთი საიდუმლო და ერთი საჯარო გასაღები. ქსელში Monero თითოეული მისამართისათვის არსებობს „დანახარჯების გასაღები“, რომელიც საიდუმლო გასაღების ანალოგიურია, და ასევე, დამატებითი „გადასახედი გასაღები“, რომელიც მან შეიძლება აჩვენოს მესამე პირებს, თავისი ტრანზაქციების შესამოწმებლად.

წრიული ელექტრონული ხელმოწერის მექანიზმის გამოყენება ქსელის სხვა წევრებს საშუალებას არ აძლევს, სწორად განსაზღვრონ დაუხარჯავი გამოსავლები კონკრეტული მისამართისათვის და გამოთვალონ მისი ბალანსი, ხოლო ყველა გამოსავალი გზავნილი ყოველთვის კეთდება ერთჯერად მისამართზე, რაც საბოლოოდ შეუძლებელს ხდის ქსელის ერთი ფიზიკური წევრისგან მეორისთვის სახსრების გადაცემაზე თვალყურის დევნებას. თუმცა წრიული ხელმოწერის ფორმირების პროცედურა გვთავაზობს ბლოკჩეინ-ბაზიდან გარკვეული რაოდენობის საჯარო გასაღებების სესხებას, რომლებიც ქსელის სხვა წევრებს ეკუთვნით. ტრანზაქციის სხეულში ამ შემნიღბავი ინფორმაციის განთავსება იწვევს მის მნიშვნელოვან ზრდას და ბიტკოინ-ქსელში ტრანზაქციის საშუალო ზომას დაახლოებით რვაჯერ აჭარბებს. რასაკვირველია, ინფორმაციის ასეთი სიჭარბე სისტემას გამოსაყენებლად მოუქნელს ხდის, რაც აშკარა ნაკლია.

მიუხედავად ამისა, კრიპტოვალუტა Monero-მ პოპულარობის მოპოვება შეძლო, მას ხშირად იყენებენ შენაძენების საფასურის გადასახდელად ონლაინთამაშებსა და ინტერნეტკაზინოებში. Monero შედის ყველაზე პოპულარული კრიპტოვალუტების რიგში, რომელთა კაპიტალიზაცია 1 მილიარდ დოლარზე ოდნავ მეტს შეადგენს. Monero-ს ემისიას ზღვარი არ აქვს, მაგრამ სისტემაში ჩადებულია მაინინგისათვის ანაზღაურების შემცირება 18,4 მილიონი მონეტის

გამოშვების შემდეგ. ბლოკები ქსელ Monero-ში იქმნება ყოველ ორ წუთში, რაც საშუალებას იძლევა, საკმაოდ სწრაფად დადასტურდეს მომხმარებელთა ტრანზაქციები.

პროექტ Monero-ზე ცოტათი ადრე გაჩნდა სისტემა DASH – DigitalCash ანუ „ციფრული ფული“. სისტემა მოიგონა და შეიმუშავა ევან დაფილდმა და გაშვებული იქნა 2014 წლის 18 იანვარს. ისევე როგორც სხვა პროექტებში, რომლებიც ბიტკოინისგან ნასესხებ კოდთან მიდის, მაინინგისათვის აქ მუშაობის დადასტურების ოქმი გამოიყენება. DASH-ის განსხვავება ისაა, რომ მაინერებს ხვდებათ მაინინგისათვის ანაზღაურების მხოლოდ 90%, დარჩენილი 10% კი ქსელის წევრთა მიერ მოწონებული, სისტემასთან დაკავშირებული, პროექტების დაფინანსებას ხმარდება. ამასთან, თვით მაინინგის პროცედურა DASH-ში ბევრად ნაკლებ ენერგოდანახარჯებს მოითხოვს, ვიდრე, მაგალითად, ბიტკოინ-ქსელში.

DASH ქსელის მართვა სრულად დეცენტრალიზებულია. ტრანზაქციების დასამუშავებლად გამოიყენება ინფრასტრუქტურა მასტერ-ნოდი („კვანძების ოსტატი“). ასეთ კვანძად შეიძლება იქცეს ნებისმიერი მსურველი პროექტის მონაწილეთაგან, რომელიც მზად არის, DASH-ის 1000 მონეტა შეიტანოს გირაოს სახით, რაც უზრუნველყოფს მის წესიერ ქსელურ ქცევას. მასტერ-ნოდის ერთ-ერთი ძირითადი ფუნქციაა ტრანზაქციების ობფუსკაცია PrivateSend ალგორითმის მეშვეობით. ამ შემთხვევაში საუბარია რამდენიმე რაუნდად მიმდინარე გადახდების შერევაზე, რომელთა რაოდენობას თავად ფულის გადამგზავნი განსაზღვრავს. ყოველ ჯერზე შესარევად ახალი მასტერ-ნოდი აირჩევა, რომელთა საერთო რიცხვმა მიმდინარე მომენტისათვის 5000-ს გადააჭარბა. გადახდის თანხა იყოფა ანონიმიზებულ ნაწილებად, ხოლო შემდეგ ერთნაირი მოცულობის მქონე ნაწილები ერთმანეთში შეირევა. თავიანთი საქმიანობის მოტივაციისათვის მასტერ-ნოდები იღებენ მაინერული ანაზღაურების 50%-ს, ქსელის მიერ ნაპოვნი ბლოკებისათვის.

ასევე საინტერესოა იმის აღნიშვნაც, რომ ქსელ DASH-ში მაინინგისათვის გამოიყენება ჰეშირების პრინციპი, რომელიც მთელი თერთმეტი ფუნქციისაგან შედგება და რომლებსაც სხვადასხვა სახის ალგორითმული ბუნება აქვს. ეს კვლავაც კეთდება ASIC-ის მაინინგის საწინააღმდეგოდ, თუმცა მოწყობილობათა მწარმოებლებმა მაინც შეძლეს ამ სირთულის გადალახვა და ბაზარზე მოთხოვნით გამორჩეული მოწყო-

ბილობების გატანა. სულ ქსელში გაშვებულია 8 მილიონ მონეტაზე ოდნავ მეტი, დაახლოებით 1 მილიარდი დოლარის საერთო კაპიტალიზაციით. პროექტი საკმაოდ პოპულარულია და მოცულობების მიხედვით, მის პირდაპირ კონკურენტ სისტემა Monero-ს შეგვიძლია შევადაროთ.

დაბოლოს, გვსურს მოგითხროთ პროექტზე, რომელიც კრიპტოინდუსტრიის სპეციალისტების მიერ მიჩნეულია ერთ-ერთ ყველაზე პერსპექტიულად ისეთი ფინანსური ტრანზაქციების სრული ანონიმიზაციის თვალსაზრისით, რომლებიც გადახდების დეცენტრალიზებულ სისტემებში გამოიყენება. პროექტმა Zcash, რომელიც 2016 წლის ოქტომბრის ბოლოს გამოჩნდა, საკმაოდ სწრაფად მოიპოვა სახელი და აღიარება როგორც მართლაც ანონიმურმა გადახდის ქსელმა. პროექტ-ანონიმიზატორის პოპულარობამ ისეთ დონეს მიაღწია, რომ თვით ევროკავშირის საპოლიციო სამსახურმა (ევროპოლმა) შეშფოთება გამოთქვა კრიმინალური მიზნებით სხვადასხვა ქმედებისთვის ამ ქსელის შესაძლო გამოყენების გამო. მაშ, Zcash-სა და გადახდათა გაზრდილი ანონიმიზაციის მქონე მის სხვა „თანამოძმეთა“ შორის არსებულმა რა განსხვავებებმა გამოიწვია ასეთი განგაში ევროპის სამართალდამცავ ორგანოებში?

Zcash-ში ანონიმურობის შესაქმნელად გამოიყენება ნულოვანი გახმაურების მქონე zk-SNARK დადასტურების ოქმი, რომელიც არსებითად, ბრმა ელექტრონული ხელმოწერის ვერსიის ფუნქციურ გაფართოებას წარმოადგენს. თვით ქსელი იყენებს ორი ტიპის მისამართს: დაფარულ „z-მისამართს“ და ღია „t-მისამართს“, ხოლო ტრანზაქციების განხორციელება შესაძლებელია ამ ტიპის მისამართებს შორის ნებისმიერ ოთხ კომბინაციაში. განურჩევლად იმისა, z მისამართის მქონე ტრანზაქციაში მისამართი გამგზავნისაა თუ მიმღების, იშიფრება ინფორმაცია შესავლებზე ან გამოსავლებზე, ანდა იფარება საერთოდ მთელი ინფორმაცია, გადარიცხვის თანხის ჩათვლით. t მისამართის გამოყენებისას ინფორმაცია ღია რჩება. ტრანზაქციების ფორმირების უზრუნველსაყოფად იქმნება ე.წ. გასაღებების „კორტეჟი“, რომელიც შედგება დახარჯვის, გადახედვის გასაღებებისა და ხარჯის მისამართისაგან. ამასთან, გადახედვის გასაღები და გადახდის მისამართი მათემატიკურად გამოითვლება ხარჯვის გასაღებიდან, რომელიც აზრობრივად, ჩვეულებრივი დახურული გასაღების ანალოგიურია.

ამგვარად, ქსელის მომხმარებლები თავად წყვეტენ, ბლოკჩეინში ინფორმაცია თავიანთ ტრანზაქციებში დაფარონ თუ ღიად დატოვონ. მისი დაფარვის შემთხვევაში, ცალკეული Zcash მონეტის წარმოშობაზე

თვალყურის დევნება ტექნოლოგიურად შეუძლებელია. ფაქტობრივად შესრულებული ტრანზაქციების შესახებ იციან მხოლოდ გამგზავნებმა და მიმღებებმა, რომლებიც დაუშიფრავად მხოლოდ გადახდის შექმნის დროის ნიშნულს ტოვებენ. გარდა თანხების გადარიცხვისა, ქსელის წევრებს ერთმანეთისათვის დაშიფრული შეტყობინებების გაგზავნა შეუძლიათ. პროექტი Zcash ასევე უშვებს მულტიხელმოწერებით სარგებლობას იმ შემთხვევებში, როდესაც აუცილებელია რამდენიმე მომხმარებლის მიერ ანგარიშის ერთობლივი მართვა. ამ ფუნქციონალის რეალიზაციისათვის აუცილებელია შემოვიღოთ „წონითი“ წესები ყოველი ხელმოწერისათვის და მათი ერთობლივი „წონის“ მინიმალური სიდიდე, რათა ტრანზაქცია ქსელისათვის ვალიდური გახდეს.

ქსელში კონსენსუსის ოქმი ეფუძნება მუშაობის მტკიცებულებას, ბლოკი იქმნება 150 წამში, ხოლო Zcash-ის ემისია, ისევე როგორც ბიტკოინისა, შემოფარგლულია 21 მილიონი მონეტით. წახალისების სახით შემმუშავებლები გამოყოფენ მთლიანი ემისიის 10%-ს მაინერების დამატებითი ანაზღაურებისათვის, ფართო მოხმარებაში ქსელის გაშვების მომენტიდან პირველი ოთხი წლის განმავლობაში. თუ რომელიმე ტრანზაქცია ვერ მოხვდა მემპულში მისი გაშვების მომენტიდან პირველ 20 ბლოკში, ის ვადაგასულად ითვლება და ქსელი მას აღარ ითვალისწინებს. ტრანზაქციის საკომისიო ფიქსირებულია და შეადგენს უმნიშვნელო სიდიდეს 0,0001 მონეტის ოდენობით. სისტემა Zcash კაპიტალიზაციის მიხედვით, კრიპტოპროექტების რეიტინგში მეორე ათეულის ბოლოს იკავებს ადგილს, გამოშვებული აქვს დაახლოებით 6 მილიონი მონეტა, დაახლოებით 450 მილიონი დოლარის საერთო ღირებულებით.

ამით ყველაზე პოპულარული უნივერსალური კრიპტოპროექტების აღწერა შეგვიძლია დავასრულოთ და გადავიდეთ წიგნის მესამე ნაწილზე, სადაც არანაკლებ საინტერესო თემებს შევეხებით. პირველ რიგში განვიხილავთ ბლოკჩეინ-ტექნოლოგიების პრაქტიკულ გამოყენებას ადამიანთა ცხოვრების სხვადასხვა სფეროში. შევეხებით ისეთ მნიშვნელოვან თემას, როგორიცაა კრიპტოინდუსტრიისა და სახელმწიფოს ურთიერთობა. დასკვნითი ნაწილის მნიშვნელოვანი ადგილი დაეთმობა კრიპტოპროექტებში ინვესტიციებს, ფინანსურ ბაზრებზე კრიპტოაქტივებით ვაჭრობის ჩათვლით. ბოლოს შემოგთავაზებთ გარკვეულ ფილოსოფიურ განსჯას ბლოკჩეინ-ტექნოლოგიების პერსპექტივასა და იმაზე, თუ როგორ შეუძლია მას ჩვენი მსოფლმხედველობის შეცვლა უახლოეს მომავალში.

ნაწილი III

ბლოკჩეინ-ინდუსტრია

ბლოკჩეინის გამოყენება

წინა თავში საკმაოდ დიდი ყურადღება დავუთმეთ ყველაზე პოპულარულ დეცენტრალიზებულ პლატფორმებს, რომლებიც აგებულია ბლოკჩეინ-ტექნოლოგიების ბაზაზე. ეს პროექტები უნივერსალურია თავისი არსით და საქმიანი და სოციალური სამყაროს რომელიმე კონკრეტულ სექტორს ვერ მივაკუთვნებთ. ყველაზე უკეთ ისინი მოირგებდა ფინანსური პლატფორმის სახელს, რადგანაც მათი ფუნქციონალი მორგებულია სწორედ ამ საქმიანობაზე. პირველ რიგში საუბარია ციფრული გადახდის სისტემებზე, რომლებიც განაწილებული ქსელის ბაზაზე სწრაფი და ანონიმური ფულადი გადარიცხვების საშუალებას იძლევა. მაგრამ ეს მხოლოდ ბლოკჩეინ-ტექნოლოგიის გამოყენების მრავალთაგან ერთ-ერთი ფორმაა, რომლის შესაძლებლობებიც შორს ცდება მხოლოდ ფინანსური ოპერაციების ფარგლებს.

იმ თავში, სადაც განვიხილავდით ციფრული ელექტრონული ხელმოწერის კონცეფციას, მაგალითის სახით მოვიყვანეთ ესტონეთში ხელისუფლების სახელმწიფო ორგანოების არჩევნებში ინტერნეტით ხმის მიცემის პროცედურა. სისტემა I-Voting, რომელიც პირველად გამოიყენეს 2007 წლის ადგილობრივ საპარლამენტო არჩევნებში, გახდა პირველი მსგავს მაღალ სახელმწიფოებრივ დონეზე. სტატისტიკის მიხედვით, ესტონეთის რესპუბლიკის მთელი ელექტორატის დაახლოებით მესამედმა გამოიყენა ინტერნეტი და ასიმეტრიული კრიპტოგრაფიის ტექნოლოგიები საკუთარი საარჩევნო ნების გამოსახატად. თუმცა, ესტონეთში ბლოკჩეინ-ტექნოლოგიების გამოყენებით არჩევნების ჩატარება ჯერ მხოლოდ იგეგმება. რამდენად უცნაურიც უნდა იყოს, პირველი ქვეყანა, სადაც არჩევნების ჩასატარებლად ბლოკჩეინი გამოიყენეს, გახდა ტექნოლოგიების განვითარების მხრივ არცთუ ისე მოწინავე ქვეყანა – აფრიკული სახელმწიფო სიერა-ლეონე. 2018 წლის მარტში ჩატარდა საპრეზიდენტო არჩევნები, რომლის დროსაც ბლოკჩეინ-ტექნოლოგიები ამომრჩეველთა ხმების შესამოწმებლად გამოიყენეს. გვინდა გვჯეროდეს, რომ თუ ასეთ ღარიბ და პოლიტიკურად არასტაბილურ ქვეყანაშიც კი იყენებენ მსგავს პროგრესულ ტექნოლოგიებს, მაღალგანვითარე-

ბული ქვეყნები მით უმეტეს არ უნდა ჩამორჩნენ. ხმის მიცემის პროცედურებში ბლოკჩეინის გამოყენება არჩევნების მაქსიმალურ გამჭვირვალობასა და მისდამი ნდობას უზრუნველყოფს, რადგანაც მათემატიკური ალგორითმები გულისხმობს იმ ადამიანური ფაქტორის ტექნოლოგიურ გაქრობას, რომელიც პოტენციურად, ირიბ გავლენას ახდენს არჩევნების შედეგებზე.

ბლოკჩეინი ფართო შესაძლებლობას უხსნის ნედლეულისა და ძვარფასი ლითონების ბაზრებზე ვაჭრობის ორგანიზაციას. ამ ტექნოლოგიის დახმარებით სანედლეულო კონტრაქტებით ვაჭრობის პროცესებს უფრო სტაბილური და გამჭვირვალე ფორმა შეიძლება მიეცეს. საუბარია იმაზე, რომ დავაჩქაროთ საბაზრო ანგარიშსწორებები, გავამარტივოთ ფინანსების მოზიდვა გარიგებებისათვის, ასევე მოვაწესრიგოთ შესაბამისი აქტივების ფლობის უფლების საკითხები. რაც შეეხება ძვირფას ქვებს (მაგალითად, ალმასებს), აქ ბლოკჩეინ-ტექნოლოგიამ შეიძლება სერიოზული გავლენა მოახდინოს მათი ბრუნვის ბაზარზე. სამრეწველო კომპანიები, რომლებიც ალმასის მოპოვებასა და დამუშავებას აწარმოებენ, კერძოდ – სამხრეთაფრიკული კომპანია De Beers, გეგმავს გამოუშვას სპეციალური პასპორტები ყოველი ძვირფასი ქვისათვის და მათზე ინფორმაცია ბლოკჩეინებში შეინახოს. ამგვარად, ბრილიანტების მსოფლიო ბაზარი შესაძლოა პრაქტიკულად მთლიანად დეცენტრალიზებული კონტროლის ქვეშ აღმოჩნდეს, რაც საშუალებას მოგვცემს, მნიშვნელოვნად შევამციროთ ძვირფასი ქვების შესაძლო კრიმინალური ბრუნვა. კიდევ არსებობს რიგი პროექტებისა, რომლებიც სხვადასხვა წონის ოქროს ზოდების ფლობის უფლების ტოკენიზაციით განხორციელდება. საკუთრივ ოქრო ფიზიკურად არსად გადაადგილდება და დაცულ ცენტრალიზებულ დეპოზიტარიებში დევს, იმ დროს, როდესაც შენახულ ოქროზე მყარად მიბმული სპეციალურად ემიტირებული სტეიბლკოინებით ვაჭრობენ სხვადასხვა კრიპტოვალუტურ ბირჟაზე და იყენებენ პირდაპირ არასაბირჟო ვაჭრობისას.

გარდა ამისა, ბლოკჩეინი თითქმის იდეალურად გამოდგება ლოკალური საბაზრო მოედნების ასაგებად მრავალი მცირე კერძო მოთამაშის მონაწილეობით. ასეთი სავაჭრო წერტილების საუკეთესო გამოყენებაა ჭარბი ელექტროენერგიის გაყიდვა, რომელიც განახლებადი წყაროებიდან მიიღება. არსებობს მრავალი მცირე კერძო

მინიელექტროსადგური, რომლებიც როგორც წესი, მზის ან ქარის ენერგიაზე მუშაობს. თუ ელექტროენერგიის გამომუშავებისას წარმოიქმნება გარკვეული სიჭარბე, ის საერთო მოხმარების ენერგოქსელში შეიძლება გასაღდეს. არადა, საბაზრო ინფრასტრუქტურის არარსებობის გამო, ასეთი გარიგებების კონტრაგენტების პოვნა ხშირად ვერ ხერხდება. უფრო მეტიც, ხდება, რომ ელექტროენერგიის ერთადერთ შემსყიდველად გვევლინება თავად ქსელის მფლობელი, ლოკალური ენერგეტიკული მონოპოლისტი. აშკარაა, რომ შესასყიდი ფასი ამ შემთხვევაში ყოველთვის როდი პასუხობს ბაზრის პირობებს, ზოგჯერ კი ენერგეტიკულმა კომპანიამ საერთოდ შეიძლება უარი თქვას ასეთ შეთანხმებაზე. ელექტროენერგიის მწარმოებლებსა და მომხმარებლებს შორის პირდაპირი გარიგებების დასადებად ბლოკჩეინ-პროექტების აგება საკმაოდ სასარგებლო და პერსპექტიულ ამოცანას წარმოადგენს. მსგავსი პროგრესული კონცეფციების რეალიზაციის პირველი მაგალითები უკვე გვაქვს ზოგიერთი ქვეყნის ენერგეტიკულ სექტორში.

ბლოკჩეინი ძალზე სასარგებლო შეიძლება აღმოჩნდეს მედიცინაში. მისი საშუალებით შეიძლება მოხდეს პაციენტთა სამედიცინო მონაცემების შენახვის ორგანიზება. მაგალითად, ეს იქნება სამედიცინო ბარათების ამონაწერები, ავადმყოფობის ისტორიები, დანიშნული წამლები და სხვა ინფორმაცია, რომელიც ჩვეულებრივ, სხვადასხვა სამედიცინო დაწესებულას შორისაა განაწილებული. ამ მონაცემთა გაერთიანება, როგორც წესი, ძალზე რთულია, ზოგჯერ კი – შეუძლებელიც. გასაგებია, რომ ინფორმაცია ბლოკჩეინ-ბაზაში დაშიფრული სახით უნდა ინახებოდეს. ამასთან, მასზე წვდომა, მთლიანად ან ნაწილობრივ, შეუძლია მოგვცეს თავად პაციენტმა საავადმყოფოს ან კლინიკის მოთხოვნით, რომლებსაც ის სამედიცინო დახმარებისათვის მიმართავს. გარდა ამისა, ბლოკჩეინი შეიძლება გამოყენებული იქნას წამლების მიწოდების ჯაჭვზე თვალყურის სადევნებლად, მათი ფალსიფიკაციისთვის არიდების მიზნით. იგივე ეხება იმ წამლების წარმოებასა და მიწოდებასაც, რომლებიც ნარკოტიკულ ნივთიერებებს შეიცავს, რადგან მსგავსი პრეპარატები მკაცრი კონტროლის ქვეშ უნდა იყოს. დაბოლოს, ბლოკჩეინის საშუალებით შესაძლებელია სამედიცინო დაზღვევის მუშაობის მნიშვნელოვანო შემსუბუქება, თუკი განაწილებულ ბაზაში მოთავსებულია სმარტ-კონტრაქტები,

რომლებიც გაწეული სამედიცინი დახმარებისათვის ავტომატურ გადახდებს აწარმოებს. რა თქმა უნდა, ამ სმარტ-კონტრაქტებმა, სანამ გადახდას მოახდენს, დაზღვევის კონკრეტული ხელშეკრულების ყველა აუცილებელი პირობის შესრულება უნდა შეამოწმოს.

გაყალბებასთან ბრძოლა მხოლოდ სამედიცინო პრეპარატების წარმოებით როდი შემოიფარგლება. საქონელთან ან მის ლოჯისტიკასთან დაკავშირებული ყველა დარგი ცდილობს გადაჭრას მსგავსი პრობლემები. ბლოკჩეინ-ინდუსტრიაში უკვე ჩნდება პროექტები, რომლებიც გვთავაზობს საქონლის სპეციალური მარკირების სერვისს, მონაცემთა განაწილებულ რეესტრში წარმოების ადგილისა და სასაქონლო პარტიების მიწოდების ჯაჭვებზე ინფორმაციის შემდგომი განთავსებით. ეს ინფორმაცია შემდგომში შეიძლება მოთხოვნილი და შემოწმებული იქნას ქსელის ყოველი წევრის მიერ, რათა შესაძენი საქონლის ლეგალურ წარმოშობაში დარწმუნდეს. აქვე დავძენთ, რომ საქონლის მარკირების ასეთი ფორმა კარგად არის დაცული არასანქცირებული კვლავწარმოებისაგან, ამიტომ ელიან, რომ სამომხმარებლო ბაზრის მხრიდან ნდობის ხარისხი ფალსიფიკაციასთან ბრძოლის მსგავსი მეთოდების მიმართ საკმაოდ მაღალი იქნება.

ბლოკჩეინ-გადაწყვეტები ტურისტული ინდუსტრიისათვისაც საინტერესო შეიძლება გახდეს. როგორც უმრავლეს დარგებში, ტურისტული საქონლის ფასწარმოქმნაზე მნიშვნელოვან გავლენას ახდენს საშუამავლო ფასნამატი, რომელიც შეიძლება საბოლოო ღირებულების მესამედს ან მეტსაც კი შეადგენდეს. ამ შემთხვევაში ბლოკჩეინ-ტექნოლოგიის გამოყენება, რომელიც ტურისტული მომსახურების მწარმოებლებსა და მომხმარებლებს შორის პირდაპირი გარიგების შესაძლებლობას იძლევა, მთლიანად აგვარიდებს თავიდან ძვირად ღირებულ საშუამავლო მარჟას საბოლოო ფასწარმოქმნიდან. საუბარია სხვადასხვა ტიპის ტრანსპორტზე ბილეთების შეძენის მომსახურებაზე, სასტუმროების დაჯავშნაზე, ასევე, ტურიზმთან დაკავშირებული არაძირითადი პროდუქტების გაყიდვაზე, მაგალითად – ექსკურსიებზე. რა თქმა უნდა, მომსახურების გავრცელების პროცესების დეცენტრალიზაციისას, რომლებიც დაკავშირებულია ვალდებულებების შესრულებასთან ბლოკჩეინის გარეშე, აუცილებლად წარმოიშობა კონფლიქტური სიტუაციები, რომლებიც გადაჭრას საჭიროებს. ეს არის ბიზნესში შუამავლის როლის ერთ-ერთი ძირი-

თადი პრობლემა, როდესაც ის საერთოდ ვარდება საქონლისა და მომსახურების შეძენის პროცედურიდან. თუმცა ამის გადაჭრის ვარიანტები უკვე არსებობს და მათ მოგვიანებით განვიხილავთ.

არც ისე დიდი ხნის წინ სოციალური ქსელები მომხმარებელთა პერსონალური მონაცემების გაჟონვასთან დაკავშირებულმა სკანდალებმა შეარყია. საუბარი იყო მათ შორის Facebook-ის ქსელის რამდენიმე მილიონ მომხმარებელზე, რომელთა მონაცემები აღმოჩნდა მესამე ფირმების განკარგულებაში, რომლებიც მათ როგორც კომერციული, ასევე პოლიტიკური მიზნებით იყენებდნენ. მსგავსი პრობლემები შეეხო სხვა სოციალურ ქსელებსაც. რა თქმა უნდა, ამის ძირითადი მიზეზი იყო კომპანიების, პროექტების მმართველების მხრიდან მათი მომხმარებლების პერსონალური მონაცემების შენახვის საკითხში გამოვლენილი არცთუ საკმარისი ყურადღება, ხოლო რიგ შემთხვევებში საქმე შეიძლება გვქონდეს დაინტერესებული პირებისთვის მონაცემთა განზრახ მიყიდვაზეც კი. მაგრამ თუ ამ სიტუაციას ღრმად გავაანალიზებთ, ნათელი ხდება, რომ პრობლემის ძირი სწორედ მონაცემთა შენახვის ცენტრალიზებული ფორმის სფეროშია. ამასთან, ზემოაღწერილი ინციდენტები უნდა განვიხილოთ როგორც მსგავსი მოდელის გამოყენების ბუნებრივი შედეგი.

ამგვარად, იკვეთება დასკვნა, რომ ამ პრობლემების თავიდან აცილება შესაძლებელია მხოლოდ სოციალური ქსელებისა და მესენჯერების მომხმარებლების მიერ მონაცემთა შენახვის დეცენტრალიზებით. სწორედ ამ შემთხვევაში ბლოკჩეინ-ტექნოლოგია კვლავ შეიძლება დამხმარედ მოგვევლინოს. განაწილებული რეესტრის ტექნოლოგიების გამოყენება მომხმარებელს საშუალებას მისცემს, თავად გააკონტროლოს საკუთარი პირადი ინფორმაცია, მისი პუბლიკაცია, შენახვა და გამოყენება. დეცენტრალიზებულად შენახული და კრიპტომედეგი ალგორითმებით დაშიფრული ინფორმაციის უცხო პირების მიერ არაკანონიერად გამოყენება შეუძლებელი ხდება. რა თქმა უნდა, ამგვარ სისტემებთან მუშაობა წარმოშობს თავის სირთულეებს, პირველ რიგში იმიტომ, რომ მასში ადრე მოთავსებული ინფორმაციის წაშლა შეუძლებელია. მაგრამ უპირატესობები მნიშვნელოვნად გადააჭარბებს დეცენტრალიზებული სისტემების გამოყენებასთან დაკავშირებულ ყველა სხვა ფაქტორს. რა თქმა უნდა, ბლოკჩეინ-ბაზაზე

შექმნილ ტექნოლოგიებს გაუჭირდება პოპულარული ცენტრალიზებული ქსელებისაგან ბაზრის საკუთარი წილის გამოგლეჯა. მიუხედავად ამისა, გვინდა გვჯეროდეს, რომ დროთა განმავლობაში ისინი ამას შეძლებს, რადგან მოთხოვნა პერსონალური მონაცემების შენახვის უსაფრთხოებაზე აშკარა ზრდის ტენდენციით გამოირჩევა.

დაბოლოს, ბლოკჩეინის გამოყენება აქტიურად იწყება გართობის ინდუსტრიაში, კერძოდ კი აზარტული თამაშებისა და ბუკმეკერული ფსონების ორგანიზებაში. როგორც ცნობილია, კაზინოები და ბუკმეკერული კომპანიები თავიანთ შემოსავლებს იღებენ თამაშებისა და მოვლენათა შესახებ სანაძლეოების პირობებში ჩადებული ე.წ. „უარყოფითი მათემატიკური მოლოდინიდან“ კლიენტებისათვის. რა არის ეს? ნებისმიერი თამაში თუ ნაძლევი, როგორც წესი, გულისხმობს საბოლოო შედეგის სამ ვარიანტს: მოგებას, წაგებას და ყაიმს (ფრეს). ჩვეულებრივ, თამაშის ორგანიზატორი მისთვის სასარგებლო გადახდის პირობას აყენებს. სხვაგვარად რომ ვთქვათ, კლიენტი იღებს ოდნავ ნაკლებ ფულს, ვიდრე მას ეკუთვნოდა ანაზღაურების სამართლიანად განაწილებისას, რომელიც პირდაპირაა დამოკიდებული მოგების წარმოქმნის ალბათობაზე. სწორედ ეს დისბალანსი აყალიბებს შედარებით გარანტირებულ მოგებას ორგანიზატორისათვის სათამაშო გარიგებათა მნიშვნელოვანი მოცულობების ერთობლიობის შემთხვევაში, ხანგრძლივი პერიოდის განმავლობაში.

სათამაშო ფსონების მიღების ორგანიზატორი ცენტრალიზაციის კლასიკური ელემენტია, რომელიც თავის სასარგებლოდ ირიცხავს საკომისიო გასამრჯელოს. მან შეიძლება მიიღოს სხვადასხვა ფორმა, მათ შორის შეფარულიც, გადახდის პირობებში ზემოთ აღწერილი დისბალანსის სახით. ბლოკჩეინ-ტექნოლოგია საშუალებას გვაძლევს, ეს ცენტრალიზებული ელემენტი მოვიშოროთ და ამით დავაბალანსოთ სათამაშო გარიგებების პირობები ორივე მხარისათვის. დღეს უკვე ჩნდება აზარტული თამაშების პროექტები, სადაც ერთიანი ორგანიზატორი არ არსებობს. შედეგად აღარ არსებობს პირობების შექმნის აუცილებლობა, რომელიც ერთ-ერთ მხარეს არათანაბარ პირობებში აყენებს. ამასთან ერთად ბლოკჩეინ-ტექნოლოგიის გამოყენება უზრუნველყოფს სრულ გამჭვირვალობას და პატიოსნებას უშუალოდ თამაშისას, რადგან ასეთი პლატფორმების კოდი აუდიტის ჩასატარებლად ღიაა პროექტში მონაწილე ნებისმიერი სუბიექტისათვის.

ბევრია დარგი, სადაც ბლოკჩეინ-ტექნოლოგიის გამოყენება შესაძლებელია ეფექტიანობის სხვადასხვა ხარისხით. კიდევ ერთხელ აღვნიშნავთ, რომ ამ ტექნოლოგიის დანერგვის ძირითადი მიზანია საშუამავლო როლისა და მასთან დაკავშირებული ხარჯების შემცირება ან მთლიანად მოშორება. ასევე არცთუ უმნიშვნელო ფაქტორია ყველა წესისა და პროცედურის გამჭვირვალობის უზრუნველყოფა, ასეთი სისტემების მიმართ მომხმარებლის ნდობის ასამაღლებლად. ამასთანავე, მსგავსი პროექტების შრომისუნარიანობის ხელშესაწყობად აუცილებელი ხდება კრიპტოვალუტურ და ფიატურ სამყაროებს შორის კაპიტალის სასაზღვრო მოძრაობის უზრუნველყოფა, ეს კი, თავის მხრივ, აიძულებს სხვადასხვა ქვეყნის მთავრობებს, ყურადღება მიაპყრონ კრიპტოსფეროში მიმდინარე პროცესებს, რათა არ დაკარგონ კონტროლი მათ დაქვემდებარებაში მყოფი საქმიანი გარემოდან გადასახადების ამოღებაზე.

როგორც უკვე აღინიშნა, სახელმწიფო რეგულატორებში ყველაზე მეტ შეშფოთებას იწვევს პროცესები, რომლებიც უკანონოდ მიღებული ფინანსური საშუალებების ლეგალიზაციას უკავშირდება. ეს ხშირად უბიძგებს სახელმწიფო მოხელეებს ცალსახად ხელის შეშლისაკენ თანამედროვე ფინანსურ სამყაროში ისეთი პროგრესული ტექნოლოგიებისათვის, როგორიცაა ბლოკჩეინი. მართლაც, ბლოკჩეინ-ინდუსტრიასა და სახელმწიფოს შორის საკმაოდ რთული ურთიერთდამოკიდებულება დამყარდა და ამ ურთიერთობის ზოგიერთი მხარე განსაკუთრებულ ყურადღებას იმსახურებს.

ბლოკჩეინი და სახელმწიფო

საქმიანი სამყაროს შემსწავლელი სამეცნიერო დარგები სახელმწიფო მართვას უპირობოდ, მენეჯმენტის ყველაზე ნაკლებეფექტიან სახეობად მიიჩნევს. ამის საფუძველი საკმარისზე მეტია: პოლიტიკური მოსაზრებით დანიშნული პირების დაბალი მმართველობითი კომპეტენცია და ხელმძღვანელი სუბიექტის კონტროლირებადი რესურსების აშკარა ნაკლებობა (ან პირიქით, სიჭარბე). როგორც წესი, მმართველობით პროცესებზე უარყოფით გავლენას ახდენს არამკაფიოდ ჩამოყალიბებული სტრატეგიული მიზნები, საშემსრულებლო დისციპლინის კონტროლის სუსტი სისტემები, პირადი პასუხისმგებლობის არამკაფიო ფორმები და, რაც ასევე მნიშვნელოვანია, მმართველთა დაბალი ფინანსური მოტივაცია. დაბოლოს, პოლიტიკური პოპულიზმის გამოყენება სახელმწიფო ძალაუფლების მოპოვებისა და შენარჩუნების ინსტრუმენტად უმრავლეს შემთხვევაში ვნებს ნებისმიერ ეკონომიკურ მოდელს, თუნდაც ადრე მას წარმატებით ემოქმედა. სახელმწიფოს მართვის ხასიათი ეფუძნება პოლიტიკურ იდეოლოგიებს: მემარჯვენეს, ცენტრისტულს ან მემარცხენეს. სახელმწიფოს პოლიტიკური სტრატეგია ხორციელდება დემოკრატიული ან ავტოკრატიული მეთოდებით, ხოლო მეორე სახეობას ხშირად სისტემური კორუფცია ერწყმის.

ნებისმიერი სახელმწიფოს შემოსავლები, როგორც წესი, შედგება ორი მთავარი წყაროსაგან: მეწარმეებისა და შრომისუნარიანი მოსახლეობის საგადასახადო შემოსავლებისა და ასევე, ბუნებრივი რესურსების მოპოვებისა და რეალიზაციისაგან. ამ კონტექსტში სახელმწიფოს განვსაზღვრავთ როგორც ბიუროკრატიული ინსტიტუტების ერთობლიობას, რომლებიც აუცილებელია მისი ფუნქციონირების უზრუნველსაყოფად. აშკარაა, რომ გადასახადების გადახდაზე კონტროლი წარმოადგენს უმნიშვნელოვანეს ფაქტორს, რომელიც თვით სახელმწიფოს მმართველობითი ინფრასტრუქტურის არსებობას უზრუნველყოფს. ამიტომ სწორედ ამ საკითხს უთმობს დიდ ყურადღებას მოხელეთა უმრავლესობა. კონტროლის როგორ მეთოდებს იყენებს სახელმწიფო? დავიწყოთ იმით, რომ ქვეყნების უმრავლეს-

ობის საქმიანი სფეროს უმნიშვნელოვანესი სისტემური მდგენელია ეროვნული ფინანსური ბაზარი. სწორედ ფულადი ურთიერთობების სისტემა განსაზღვრავს სახელმწიფოს ეკონომიკის მდგომარეობას: აქტიურად თუ პასიურად განვითარდება ის, თუ მას ელის სტაგნაცია, რომელსაც აუცილებლად ეკონომიკური დეპრესია მოჰყვება.

რაკი კარგად აქვს შეგნებული ფინანსური ინდუსტრიის მდგომარეობის მნიშვნელობა, სახელმწიფო ყოველთვის ცდილობს, მასზე მმართველობითი გავლენა მოახდინოს, სხვაგვარად რომ ვთქვათ, დაარეგულიროს. ამისათვის სახელმწიფოს ხელთ აქვს აუცილებელი ინსტრუმენტები – დარგობრივი კანონების კრებული, ასევე – ბიუროკრატიულ და ძალოვან უწყებათა ინფრასტრუქტურა. რა თქმა უნდა, ფინანსურ სფეროში მკაცრი რეგულაციები იმთავითვე არ დადგენილა, არამედ გარკვეული ევოლუციის შედეგად ჩამოყალიბდა. კაცობრიობის ისტორიის საკმაოდ ხანგრძლივი პერიოდის განმავლობაში სხვადასხვა სახელმწიფოს ფინანსური ბაზრები ჩვეულებრივი თვითრეგულაციის საფუძველზე ფუნქციონირებდა, მაგრამ გლობალურმა ფინანსურმა კრიზისებმა ხელისუფლების ორგანოები აიძულა, გადაეხედათ რეგულირებისადმი მიდგომები გამკაცრების მიმართულებით. ზოგმა სახელმწიფომ ტიპური ლიბერტარიანული მოდელებიდან (მათ შორის დემოკრატიულიდან) მათ კონტროლქვეშ მყოფ ფინანსურ ინდუსტრიაზე ზემოქმედების ღიად პროტექციონისტულ და რეპრესიულ ფორმებზე გადასვლაც კი დაიწყო.

ბოლო ათწლეულებში ფართოდ გავრცელდა რეგულაციური სისტემა, რომელშიც დომინანტურ იდეას წარმოადგენს ფულის გათეთრებასთან ბრძოლა საქმიანი სფეროს იმ სუბიექტების მხრიდან, რომლებიც თავს არიდებენ კანონმდებლობით გათვალისწინებულ გადასახადებს. ბლოკჩეინ-ტექნოლოგიების გამოჩენამ მისი დეცენტრალიზებული და დამოუკიდებელი ინფრასტრუქტურით, ასევე, მასში ჩადებული აუცილებელი ანონიმურობით, მაქსიმალურად გაართულა ფინანსური ნაკადების მოძრაობაზე აუცილებელი კონტროლის დამყარების პროცესები. მართლაც, ბლოკჩეინ-ტექნოლოგიების ბაზაზე აგებული პირველი პროექტების შედარებით ფართო გავრცელებამდე ხელისუფლებები მას სერიოზულ ყურადღებას არ აქცევდნენ. ეს უყურადღებობა იმითაც იყო განპირობებული, რომ ბლოკჩეინ-სისტემის საფუძველზე გადახდების სისტემების აგების კონცეფციის ტექ-

ნოლოგიური სირთულე წარმოადგენს მნიშვნელოვან ბარიერს იქ მიმდინარე პროცესების არსისა და იმის გასაგებად, თუ როგორ შეიძლება ამან იმოქმედოს მთლიანად ფინანსურ ინდუსტრიაზე.

სამაგიეროდ, საკმაოდ მალე კრიპტოვალუტის ბაზრის კაპიტალიზაცია უკვე ათეულობით და ასეულობით მილიარდ დოლარსაც კი აღწევდა. ამან ზოგიერთი სახელმწიფოს მთავრობა აიძულა გაეაზრებინა, რომ მოვლენა „ბლოკჩეინის“ შემდგომი იგნორირების სტრატეგიამ შესაძლოა გამოუსწორებელი შედეგები მოუტანოს მისი სახელმწიფოს ბიუჯეტს. მოხელეების წინაშე დადგა რთული ამოცანა: როგორ გამოეხატათ თავიანთი დამოკიდებულება ახალი ფინანსურ-ტექნოლოგიური ფენომენისადმი და შემდეგ როგორ ემართათ ეროვნული ეკონომიკის მასთან დაკავშირებული რისკები? აქ უნდა დავაზუსტოთ, რომ იმ ნაბიჯების რადიკალიზმის გრადუსი, რომლებსაც ეროვნული მთავრობები კრიპტოინდუსტრიის მიმართ დგამენ, პირდაპირაა დაკავშირებული პოლიტიკური კონკურენციის თავისუფლების ხარისხთან კონკრეტულ სამართლებრივ გარემოში.

ჭეშმარიტი საპარლამენტო დემოკრატიის ქვეყნებში სახელმწიფო მოხელეები იძულებულნი არიან, შეაჯერონ საკუთარი საჯარო გამოსვლები ამით მოხდენილ პოლიტიკურ ეფექტთან, რამაც შეიძლება გავლენა მოახდინოს შემდეგი არჩევნების შედეგებზე. აშკარაა, რომ არც ერთ პოლიტიკოსს არ სურს საკუთარი ელექტორატის თვალში გამოჩნდეს გამოუსწორებელ რეტროგრადად, რომელიც გზას უღობავს სამეცნიერო-ტექნიკურ პროგრესს. უფრო მეტიც, ბევრი მათგანი ცდილობს, საკუთარი ამომრჩევლის წინაშე გაითამაშოს „ტექნოლოგიური ბანქო“, რათა ასწიოს თავისი პარტიის იმიჯი და თავი ქვეყნის ტექნოლოგიური განვითარების მომხრედ წარმოადგინოს. თუმცა, რადგან პასუხს აგებენ სახელმწიფო ბიუჯეტის შესრულებაზე, მოხელეები მუდმივად ზრუნავენ ფინანსურ ნაკადებსა და საგადასახადო შემოსავლებზე კონტროლის შენარჩუნებაზე. ამიტომ ზოგიერთ შემთხვევაში მმართველი პარტიების ან კოალიციების წარმომადგენლები ინარჩუნებენ საჯარო ნეიტრალიტეტს და პრაქტიკულად, საკმაოდ იშვიათად უჭერენ მხარს კრიპტოვალუტებთან დაკავშირებულ რომელიმე პროექტს.

სახელმწიფოებში, სადაც განუყოფლად ბატონობს ავტორიტარიზმი, მმართველი პარტიის წარმომდგენლებს არ ადარდებთ კონკურენცია სხვა პოლიტიკურ ძალებთან. ამიტომ მათი პოზიციები ურყე-

ვია და უმრავლეს შემთხვევაში, ამკრძალავი ზომების ერთობლიობით ხასიათდება, რაც მნიშვნელოვნად ზღუდავს კრიპტოვალუტურ სისტემებს იმ სამართლებრივი სივრცის ფარგლებში. მაგალითად, ზოგი ქვეყანა ცდილობს აკრძალოს მაინინგი, კრიპტოვალუტების ყიდვა-გაყიდვა და ზოგ შემთხვევაში – შენახვაც კი. გარდა ამისა, იზღუდება ან სრულად იკრძალება კრიპტოვალუტური ბირჟების საქმიანობა, შესაბამისი გადახდის სისტემების მუშაობასთან ერთად. მაგრამ ეს რეპრესიული ზომები აწყდება ბუნებრივ ტექნოლოგიურ სირთულეებს ანდა მისი განხორციელების სრულ შეუძლებლობას, რადგან ბლოკჩეინ-სისტემებს ახასიათებს ისეთი თვისებები, როგორებიცაა დეცენტრალიზაცია და სარგებლობის ანონიმურობა.

გამოდის, რომ არც ერთ სახელმწიფოს არ შეუძლია ჩაერიოს რომელიმე არსებული დეცენტრალიზებული ბლოკჩეინ-ქსელის საქმიანობაში, მის შიგნით თვალი ადევნოს გადახდებს, ასევე, დაბლოკოს და კონფისკაცია უყოს ქსელურ მისამართებთან დაკავშირებულ სახსრებს. ფიატური ფულის კლასიკურ სამყაროში სახელმწიფოს ყოველთვის შეუძლია განახორციელოს ზომების ეს კომპლექსი ბანკების, როგორც ცენტრალიზებული და ლიცენზირებული ფინანსური ინსტიტუტების, საშუალებით, რომლებიც ყოველთვის მზად არიან ხელისუფლებასთან სათანამშრომლოდ. მაგრამ ბლოკჩეინ-ქსელებში ამ ზომების გატარება შეუძლებელია. კრიპტოგარემოზე თუნდაც უმნიშვნელო გავლენის მოსახდენად რეგულატორებს რჩებათ ერთადერთი გზა – კრიპტოვალუტურ და ფიატურ სამყაროებს შორის „სასაზღვრო კონტროლის“ ერთგვარი პუნქტები განალაგონ. ამისათვის რეგულატორები მობილიზებას უკეთებენ ბანკებსა და ფიატური გადახდის სისტემებს, რომლებიც იღებენ განკარგულებებს, თვალყური ადევნონ კაპიტალისა და მისი კლიენტების მოძრაობას ამ სრულიად განსხვავებულ ფინანსურ გარემოებს შორის.

არ ჩამორჩებიან აღმასრულებელი ხელისუფლების სახელმწიფო ორგანოებიც. ისინი ეროვნულ პარლამენტებთან ერთად აქტიურობენ კრიპტოინდუსტრიის შესახებ ახალი კანონშემოქმედებითი ინიციატივების შექმნასა და წინ წაწევაში. დაწყებული 2017 წლის შემოდგომიდან, კრიპტოვალუტურ ბაზრებზე დაიწყო ნამდვილი ბუმი, რის შემდეგაც ბევრმა ქვეყანამ მიიღო კანონები, რომლებიც ზღუდავს კრიპტოვალუტების ბრუნვას ეროვნული იურისდიქციის ფარგლებ-

ში და აღასრულებს მათ სიმკაცრის სხვადასხვა ხარისხით. ყველაზე რადიკალურნი იყვნენ ბოლივია და ნეპალი, სადაც სრულიად აკრძალეს კრიპტოვალუტებთან დაკავშირებული ნებისმიერი საქმიანობა. მათ არ ჩამორჩნენ ყირგიზეთი და ინდონეზია, ლიბია და ალჟირი. იქ აიკრძალა კრიპტოვალუტის შეძენა და გაყიდვა, თუმცა მაინინგის პროცედურების მიმართ მკაფიო დამოკიდებულება არ გამოუხატავთ. ყველაზე დიდი გავლენა მსოფლიო კრიპტოვალუტურ ბაზარზე მოახდინეს ჩინეთმა, აშშ-მა და სამხრეთ კორეამ.

ითვლება, რომ ჩინეთში თავმოყრილია მსოფლიო კრიპტოვალუტათა მაინინგის 70-80%. აშკარაა, რომ ჩინეთის მთავრობის ქმედებები კრიპტობაზრის მიმართ ყველაზე მნიშვნელოვან გავლენას ახდენს მის კაპიტალიზაციაზე. ანუ, საუბარია ყველაზე პოპულარული კრიპტოვალუტების – ბიტკოინის, ეთერისა და მათი მსგავსების ღირებულების ფიატურ ეკვივალენტებზე. 2017 წლის სექტემბერში ჩინეთმა აკრძალა კრიპტოვალუტებით ვაჭრობა და ICO-ის ჩატარება, ხოლო ფიატური და კრიპტოვალუტური სახსრები, უკვე შეგროვილი პროექტების შემმუშავებლების მიერ, გადაწყდა, უკან დაებრუნებინათ ინვესტორებისათვის. გარდა ამისა, ხელისუფლებამ გადაწყვიტა მაინერების შეზღუდვა ელექტროენერგიის შეძენაში და საერთოდ, აშკარად ხელს უშლიდა მათ საქმიანობას. ამან ბევრ კრიპტო-ფერმერს უბიძგა, თავიანთი მონაცემთა ცენტრები ჩინეთს გარეთ, სხვა, ამისათვის უფრო მოსახერხებელ ქვეყნებში გადაეტანათ. სამხრეთ კორეის მთავრობამაც გასცა განკარგულება, შეეწყვიტათ ინვესტიციების მოზიდვა ICO-ის საშუალებით და დამატებით გამოსცა კანონი ანონიმური ქსელური მისამართებიდან კრიპტოვალუტური ტრანზაქციების აკრძალვის შესახებ.

შეერთებულმა შტატებმა ICO-ის საშუალებით გავრცელებული ტოკენები გაუთანაბრა ფასიან ქაღალდებს, აქედან გამომდინარე ყველა რეგულაციური შედეგით, რადგან ამ ღონისძიების ჩატარება ძალზე რთული და ხარჯიანი გახდა. ბიტკოინთან როგორც კრიპტოვალუტასთან მიმართებაში კი შეიქმნა გარკვეული რეგულაციური კოლიზია: ზოგი სასამართლო პრეცედენტი მას განსაზღვრავდა როგორც ჩვეულებრივ ვალუტას, იმ დროს, როდესაც საკომისიოები საბირჟო CFTC ფიუჩერსების მიხედვით ბიტკოინს საბირჟო საქონელს უთანაბრებდა. ზოგიერთმა შტატმა – მაგალითად, ნიუ-იორკმა და ვაშინგტონმა – შე-

მოიღო აუცილებელი ლიცენზირება იმ კომპანიებისათვის, რომლებიც კრიპტოვალუტებთან დაკავშირებულ საქმიანობას ეწეოდნენ. გარდა ამისა, აქტივების ამ კატეგორიის ოპერაციებზე შემოიღეს სპეციალური გადასახადები, რომელთა საბოლოო სიდიდე შტატზეა დამოკიდებული.

თუ კრიპტოვალუტური ბაზრის ლეგალიზაციისაკენ მიმართულ პოზიტიურ ნაბიჯებზე ვისაუბრებთ, აქ ლიდერი აღმოჩნდება იაპონია, რომელიც პირველი და ჯერჯერობით ერთადერთი ქვეყანაა, რომელმაც კრიპტოვალუტა გადახდის ოფიციალურ საშუალებად აღიარა. იქვე არსებობს კრიპტოვალუტური ბირჟების ოფიციალური ლიცენზირება და რეგულაცია. ევროპის ქვეყნებს შორის ICO-ის ჩასატარებლად ყველაზე ხელსაყრელი სამართლებრივი ბაზა შვეიცარიის კანტონ ცუგს აქვს, სადაც ჯერ კიდევ 2017 წელს მიღებული იქნა კრიპტოგარემოს მიმართ კეთილგანწყობილი კანონმდებლობა. ევროკავშირში ბლოკჩეინისათვის რეგულაციური ბაზის შექმნაში ლიდერად ითვლება კუნძულოვანი სახელმწიფო მალტა, სადაც 2018 წლის შუა პერიოდში მიიღეს კანონი ვირტუალური ფინანსური აქტივების შესახებ. მალტის საკანონმდებლო ბაზამ განსაზღვრა სხვადასხვა ტიპის კრიპტოტოკენებთან დაკავშირებული ცნებები, რომელთა გამოყენებაც შესაძლებელია ბლოკჩეინ-ტექნოლოგიით აგებულ პროექტებში. შედეგად მიიღეს ინვესტიციების უზარმაზარი ნაკადები ბლოკჩეინ-პროექტების შემმუშავებელ მალტურ კომპანიებში. არ ჩამორჩა ესტონეთიც, რომელმაც კრიპტოვალუტების ბირჟებისათვის შემოიღო გამარტივებული ლიცენზირება, რომლის ხასიათიც თავიდან „საგანაცხადე“ უფრო იყო, ვიდრე „ნების დამრთავი“ (უფლების მიმცემი). 2018 წლის ბოლოსათვის ესტონეთში 500-ზე მეტი ასეთი ლიცენზია გაიცა, რის შემდეგაც რეგულატორები დაფიქრდნენ ლიცენზირების პროცესიის ერთგვარ გართულებაზე, ბაზრის ზოგიერთი წევრისგან ამით ბოროტად სარგებლობის თავიდან ასაცილებლად.

მიუხედავად სახელმწიფოსა და ბლოკჩეინის ურთიერთობებში დადებითი ძვრებისა, ამ სფეროში კიდევ მრავალი გადაუჭრელი პრობლემაა, რომელიც საშუალებას არ იძლევა გადავიდეთ კრიპტოგარემოსადმი დაბალანსებული სარეგულაციო პოლიტიკის ჩამოყალიბებაზე. ერთ-ერთი მთავარი სირთულე, როგორც უკვე აღინიშნა, ბლოკჩეინში ფინანსური ტრანზაქციების ანონიმურობაა. ჰოდა, სანამ პროექტების შემმუშავებლები ფინანსური ნაკადების დეანო-

ნიმიზაციის რეგულატორებისათვის მისაღებ ფორმებს შემოგვთავაზებენ და ასევე, მსგავსი ქსელების წევრთა იდენტიფიკაციისათვის აუცილებელ ინფრასტრუქტურებს შექმნიან, სახელმწიფოსთან ურთიერთობაზე საუბარი ზედმეტია. იმისაგან დამოუკიდებლად, ბლოკჩეინ-ტექნოლოგია რამდენად ჩაითვლება პროგრესულად, ეროვნული მთავრობები არ იჩქარებენ მისი მასობრივი დანერგვისა და გამოყენების მხარდაჭერას, ყოველ შემთხვევაში – იმ მომენტამდე მაინც, სანამ მასზე აგებული პროექტები არ დააკმაყოფილებს სტანდარტულ საკანონმდებლო მოთხოვნებს, რომლებსაც ჩვეულებრივ, ფინანსური ინდუსტრიის წევრებს უყენებენ.

იმისათვის, რათა დავაჩქაროთ იმ ეპოქის მოახლოება, როდესაც ქვეყნების მთავრობები დადებითად შეხედავენ ბლოკჩეინ-ინდუსტრიას, აუცილებელია უზარმაზარი სამუშაოს ჩატარება კრიპტოპროექტების შემმუშევებლებსა და სახელმწიფო მოხელეებს შორის მსოფლმხედველობრივი პოზიციების დასაახლოებლად. ამ ამოცანის შესასრულებლად მიზანშეწონილი იქნებოდა, ყველა ქვეყანაში შექმნილიყო პროფილური ასოციაციები, ხოლო მათ ფარგლებში – სამუშაო ჯგუფები მთავრობასთან ურთიერთქმედებისათვის. მხოლოდ კონსტრუქციული დიალოგის წარმართვა მოგვცემს საშუალებას, გადავჭრათ სხვადასხვა სახელმწიფოს საქმიან და სოციალურ სფეროებში ახალი ტექნოლოგიების ჩართვის უმნიშვნელოვანესი ამოცანა. ზოგიერთ ქვეყანაში ეს საქმიანობა კრიპტოსაზოგადოების მიერ უკვე აქტიურად ტარდება, ხოლო ზოგში – მხოლოდ პირველი მცდელობებია. გადასახადების გადახდის კონტროლისა და ფულის გათეთრების საწინააღმდეგო ფუნქციების გარდა, სახელმწიფო ფინანსურ რეგულატორებს აქვთ კიდევ ერთი არანაკლებ მნიშვნელოვანი ამოცანა: საუბარია სამომხმარებლო ფინანსური ბაზრის დაცვაზე საეჭვო რეპუტაციის მქონე პირებისა და კომპანიების მხრიდან შესაძლო ბოროტად სარგებლობისა და ღია თაღლითობისაგან. ფინანსური რეგულატორები ცდილობენ გააფრთხილონ საზოგადოება, რომელიც ძირითადად არაპროფესიონალი ინვესტორებისაგან შედგება, თავი აარიდონ დაუფიქრებელი ნაბიჯების გადადგმას, რომლებიც დაკავშირებული იქნება კრიპტოპროექტებში შენატანებთან. მაგრამ რას ფიქრობენ ამის შესახებ თავად საზოგადოების წარმომადგენლები? როგორ აღიქვამენ ისინი შედარებით ახალ ტექნოლოგიას, რომლის ბაზაზეც მთელი დარგი აღმოცენდა?

ბლოკჩეინი და საზოგადოება

დიდი ხნის განმავლობაში კრიპტოგრაფიული ოქმების შესწავლა დეცენტრალიზებული გადახდების სისტემების შესაქმნელად იყო მხოლოდ ენთუზიასტთა ვიწრო ჯგუფის ხვედრი, რომლებიც საკუთარ თავს „შიფროპანკებს“ ეძახდნენ. და მაშინაც კი, როდესაც სატოში ნაკამოტომ შექმნა პირველი ბლოკჩეინ-ქსელი, მის მიმართ კრიპტოტექნოლოგიებში გაუცნობიერებელი ადამიანების ინტერესი გარკვეული დროის განმავლობაში ნულის ტოლი იყო. პოპულარული მედია პრაქტიკულად არ აშუქებდა კრიპტოსამყაროს ახალ ამბებს, ხოლო კრიპტოვალუტებზე რამდენადმე აქტუალური ინფორმაციის წაკითხვა შეიძლებოდა მხოლოდ ვიწრო პროფესიულ ინტერნეტფორუმებზე. ბიტკოინ-ქსელის არსებობიდან ორი წლის თავზე მასში 1000-მდე აქტიურ მისამართს თუ დაითვლიდით, მაგრამ უკვე ნახევარი წლის შემდეგ მათი რიცხვი მკვეთრად – 20-ჯერ და მეტად გაიზარდა. Mt. Gox ბირჟის გაკოტრების მომენტისათვის, რომელიც მნიშვნელოვანი მოვლენა იყო ახალჩასახულ კრიპტოინდუსტრიაში, აქტიურ მომხმარებელთა რაოდენობამ დაახლოებით 150 000 შეადგინა. შემდგომში მათი რიცხვი უფრო და უფრო იზრდებოდა, თუმცა ხანდახან შემცირების მიმართულებით გარკვეულ კორექციასაც განიცდიდა. როგორც წესი, ეს კრიპტოაქტივებზე ფასების აქტიური ზრდის პერიოდების დამთავრების შემდეგ ხდებოდა.

ლოგიკურია ვივარაუდოთ, რომ კრიპტოენთუზიასტების პირველ თაობას საინფორმაციო ტექნოლოგიების ინდუსტრიის წარმომადგენლები, პირველ რიგში, პროგრამისტები წარმოადგენდნენ. პროფესიული კომპეტენციის ძალით მათ სხვებზე ადრე და სწრაფად შეძლეს ახალი ტექნოლოგიის მუშაობის პრინციპებში გარკვევა. სწორედ მათ მიეცათ შესაძლებლობა, მიეღოთ გარკვეული შემოსავალი კრიპტოვალუტებში ინვესტირებისაგან მათი არსებობის ადრეულ ეტაპზე. მართლაც, ზოგიერთმა შორსმჭვრეტელმა IT სპეციალისტმა ხელიდან არ გაუშვა მისთვის მიცემული შანსი და მიიღო ძალზე წონადი საინვესტიციო მოგება, ხოლო ისინი, ვინც უფრო შორს წავიდნენ და მონაწილეობდნენ კრიპტოპროექტების შექმნაში, რომლებმაც ბაზარ-

ზე პოპულარობა მოიპოვა, მულტიმილიონერები გახდნენ. შედეგად, ინფორმაცია პირველი კრიპტოინვესტორების წარმატებების შესახებ გავრცელდა მათ მეგობრებსა და ნაცნობებში, რამაც დიდად შეუწყო ხელი კრიპტოვალუტებისადმი ინტერესის ზრდას ადემიანებში, რომლებსაც საინფორმაციო ტექნოლოგიებთან შეხება არ ჰქონდათ.

იმის შემდეგ, რაც გაიგო, რომ ფინანსურ ბაზარზე ახალი ტიპის რომელიღაც აქტივი გაჩნდა, რომელზეც მილიონებს შოულობდნენ, ბევრი ადამიანი კრიპტოვალუტურ ბირჟას ეცა. ამავე დროს, ადამიანთა უმეტესობას არც კი უცდია, ცოტათი მაინც შეესწავლა იმ მოვლენის ბუნება, რომელშიც თავისი ფულის ჩადებას აპირებდა. შედეგად ბევრმა უიღბლო ინვესტორმა ზარალი განიცადა, რის შემდეგაც სასწრაფოდ სცადა კრიტპოვალუტებზე საინვესტიციო ბუშტისა და ფინანსური პირამიდის იარლიყის მიკერებაც კი. უნდა ითქვას, რომ ეს აზრი ენთუზიაზმით აიტაცა საზოგადოების არაერთმა წარმომადგენელმა, რომლებსაც კიდევ უფრო ნაკლები წარმოდგენა ჰქონდათ კრიპტოვალუტებზე, ვიდრე იმათ, ვინც თავიანთი კაპიტალის უიღბლოდ განთავსების გამო ფინანსური ზარალის სიმწარე იწვნიეს. მოდი გავერკვეთ, კრიპტოვალუტების, როგორც ინვესტირების ობიექტის, კრიტიკული შეფასება რამდენად ახლოა ჭეშმარიტებასთან.

გერმანელმა ფილოსოფოსმა, სოციოლოგმა და ეკონომისტმა კარლ მარქსმა თავის ნაშრომში „კაპიტალი“ აღწერა საზოგადოებრივ-ეკონომიკური ფორმაცია სახელად „კაპიტალიზმი“ და ამტკიცებდა, რომ მისი მნიშვნელოვანი ფაზაა ჭარბწარმოებით წარმოქმნილი პერიოდული კრიზისი. მსგავსი ციკლურობა აქტიური ეკონომიკური ზრდისა და მისი მომდევნო აუცილებელი დეპრესიის პერიოდების ცვლას გულისხმობს. მართლაც, მარქსის ნაშრომების პუბლიკაციის დროიდან გასული ასზე მეტი წლის განმავლობაში მსოფლიო რამდენჯერმე შეაზანზარა სხვადასხვა სიმძიმის ფინანსურმა კრიზისმა, რომლებიც შემდეგ ხანგრძლივმა ეკონომიკურმა სტაგნაციამ შეცვალა. სახელმწიფოებს მრავალი წელი დასჭირდათ, რათა კოლაფსების შედეგები აღმოეფხვრათ, რის შემდეგაც ელოდნენ ბაზრების გარკვეულ გამოცოცხლებას და კვლავ იწყებდნენ მოძრაობას ეკონომიკური აღმავლობისაკენ.

თითქმის ყოველთვის ფინანსურ კრიზისს წინ უსწრებდა ეროვნული ეკონომიკების „გადახურებული“ მდგომარეობა, რაც იმით გა-

მოიხატებოდა, რომ ბაზრის წევრების ხელში თავისუფალი საინვესტიციო სახსრების სიჭარბე მასზე მოვაჭრე ინსტრუმენტების „ჭარბ ყიდვას“ იწვევდა. საფონდო ბირჟებზე აღინიშნებოდა განსაკუთრებული აქტივობა, როდესაც ფულს მასობრივად დებდნენ კომპანიების აქციებში, რომელთა ჭეშმარიტი ფინანსური მდგომარეობა ხშირად სავალალო იყო, თუმცა ინვესტორთაგან ცოტა ვინმე თუ აქცევდა ამას სათანადო ყურადღებას. შედეგად, ბირჟაზე იბერებოდა ე.წ. „საბირჟო ბუშტი“, რომელსაც ჰქონდა სპეკულაციური მდგენელის დამახასიათებელი მაღალი წილი ფასიანი ქაღალდების ღირებულებაში. მარტივად რომ ვთქვათ, სპეკულაციურ ნაწილში იგულისხმება იმ კომპანიის აქტივების რეალურ ღირებულებაზე ფასნამატი, რომლის აქციებითაც საჯაროდ ვაჭრობენ ბირჟებზე. ჰოდა, როდესაც დგება ფინანსური კრიზისის დრო, გადაფასებული აქციები კომპანია-ემიტენტის აქტივების ღირებულების დონემდე, ზოგჯერ კი უფრო დაბლაც ეცემა, რადგანაც ბაზარს საქმე აქვს ე.წ. „პანიკურ გაყიდვებთან“. მსოფლიოსათვის ცნობილი ერთ-ერთი პირველი საინვესტიციო ბუშტი წარმოიშვა 1636-1637 წლებში ნიდერლანდებში ტიტების ბოლქვებით საბირჟო ვაჭრობის დროს. „ტიტომანიით“ უზომოდ გაბერილი ბაზარი საბოლოოდ ჩამოინგრა და მასობრივად გააკოტრა გვიანი ციკლების ინვესტიციის მონაწილეები.

კრიპტოვალუტებით ვაჭრობის ბაზარზეც იგივე ხდება, რაც ჩვეულებრივ საბირჟო მოედნებზე, რომლებზეც გავლენას ახდენს ადამიანის ფსიქოლოგიასთან დაკავშირებული ფაქტორები, ეს კი, თავის მხრივ, ნიშნავს, რომ საინვესტიციო ინსტრუმენტებზე მაღალი მასობრივი მოთხოვნილების პერიოდებში სპეკულაციური მდგენლები მათ ფასში რეალურზე სერიოზულ დომინირებას იწყებს. ამგვარად, ინვესტიციური ბუშტის ცნება შეიძლება დაკავშირებული იყოს ნებისმიერ საბირჟო ინსტრუმენტთან, განურჩევლად მისი ბუნებისა, კრიპტოვალუტების ჩათვლით. ნებისმიერი ტიპის საფინანსო ბაზრებზე მოვაჭრე ინვესტორისათვის მნიშვნელოვანია მისი გადახურების ხარისხის განსაზღვრა და იმის გადაწყვეტა, თუ როგორი რისკების გასაწევად არის მზად. ბევრი ანალიტიკოსი კრიპტოვალუტებზე ფიქრობს, რომ სპეკულაციური მდგენელი მათ ღირებულებაში მთელ 100%-ს შეადგენს, რადგან რეალურ ფასეულობაზე ამ შემთხვევაში საუბარი არ შეიძლება. მაგრამ ოდნავ უფრო ადრე ბიტკოინის მა-

გალითზე გავარკვიეთ, რომ ზოგიერთ კრიპტოვალუტას მაინც აქვს საკუთარი შიდა ფასეულობა, რომელიც მისი მოპოვების დანახარჯებს ეფუძნება.

კრიპტოაქტივებთან დაკავშირებული კიდევ ერთი კრიტიკული მიმართულებაა მათი გათანაბრება ფინანსურ პირამიდებთან. მოდი გავაანალიზოთ ეს პოზიცია. ფინანსური პირამიდა, სამწუხაროდ, საკმაოდ ხშირი მოვლენაა თანამედროვე სამყაროში. ის სათავეს იღებს ვინმე ჩარლზ პონცის მიერ მოგონილი ცნობილი სქემიდან, რომელიც 1919 წელს აშშ-ში გასცემდა თამასუქებს, რომლებისთვისაც ყოველ აღებულ 1000 დოლარზე სამი თვის განმავლობაში 1500-ის გადახდის ვალდებულებას კისრულობდა. ასეთ მაღალ პროცენტს ის ხსნიდა საერთაშორისო საფოსტო კუპონების გაცვლის სისტემაში ინვესტიციებით, რომლებსაც მისთვის დადებითი საკურსო განსხვავება ჰქონდა. სამაგიეროდ, ის არ ახსენებდა, რომ ნაყიდი კუპონების განაღდება კი არ შეიძლებოდა, არამედ შესაძლებელი იყო მხოლოდ საფოსტო მარკებზე მათი გადაცვლა. რა თქმა უნდა, არანაირ კუპონს პონცი არ ყიდულობდა და დაკავებული იყო მხოლოდ კრედიტორებისაგან ფულის საკუთარ სქემაში მოზიდვით. მან შეძლო 4 მილიონი დოლარის შეგროვება და ამასთან, 7 მილიონი დოლარის უკუგადახდის ვალდებულების შექმნა. 1920 წლის აგვისტოში პირამიდა ჩამოინგრა, ხოლო თავად პონცი თაღლითობისათვის ხუთი წლით ამერიკულ ციხეში ჩაჯდა.

შემდგომში ფინანსური პირამიდა არცთუ იშვიათად ჩნდებოდა მსოფლიოს სხვადასხვა ქვეყანაში და ამისათვის სახსრების მოზიდვის სხვადასხვა მოდელს იყენებდნენ. მაგრამ ყველა მათგანს ჰქონდა რამდენიმე საერთო ნიშანი, რომლებიც აშკარად მიუთითებს, რომ ინვესტორებს თაღლითობასთან აქვთ საქმე. პირამიდის ძირითად ატრიბუტებს შორის უნდა დავასახელოთ მონაწილეთათვის ისეთი გადახდების შეპირება, რაც უშუალოდ არ უკავშირდება იმ კომპანიის კომერციულ საქმიანობას, რომელიც სქემის უკან დგას. ამასთან ერთად, ყველა პირამიდა ხასიათდება აგრესიული სარეკლამო კამპანიით, რომელიც თან სდევს სახსრების მოზიდვის პროცესს. მაგრამ ყველაზე მთავარია აშკარა ცენტრალიზაცია და შესაქმნელი პირამიდის მკაცრი იერარქიულობა. კენწეროზე ყოველთვის დგას ორგანიზატორი როგორც სქემის მთავარი საბოლოო ბენეფიციარი. დონით ქვემოთ არიან

სახსრების დაქირავებული ან ნებაყოფლობითი შემგროვებლები, რომლებიც სახსრების მოზიდვისთვის საკომისიოს იღებენ. პირველ ხანებში პირამიდის ორგანიზატორები მართლაც უხდიან ფულს შედარებით ადრეულ შემომტანებს, უფრო გვიანდელების შემოტანილი თანხებიდან. მაგრამ საბოლოოდ, ნებისმიერ შემთხვევაში დგება დრო, როდესაც ყველა გადახდა წყდება, რის შემდეგაც პირამიდა ჩამოიშლება, ხოლო მასში სახსრების შემომტანები ხელცარიელნი რჩებიან.

ახლა კი შევადაროთ ფინანსური პირამიდის სიტუაცია კრიპტოვალუტურისას, ბიტკოინის მაგალითზე. კრიტიკოსებისათვის სავალალოდ, ბიტკოინ-ქსელის აგების დეცენტრალიზებული ხასიათი თავისთავად გამორიცხავს რომელიმე ერთი სარგებლის მიმღების არსებობას, ვინც სხვა შემომტანების ხარჯზე მდიდრდება. ბიტკოინ-ქსელს არ ჰყავს მფლობელი, არ აწარმოებს არანაირ რეკლამას კრიპტომონეტების გაყიდვაზე და არ ჰპირდება გადახდებს, გარდა ანაზღაურებისა, რომელიც თავიდანვე ჩადებულია ქსელის წევრებისათვის კონკურენტული მაინინგის პროტოკოლით. სამართლიანობისათვის უნდა აღვნიშნოთ, რომ ბიტკოინის მაგალითი ამ შემთხვევაში, ძალზე იდეალისტურია. კრიპტოინდუსტრიაში არსებობს არცთუ ისე ცოტა პროექტი, რომელთა სრული დეცენტრალიზაცია მართალია, დეკლარირებულია, მაგრამ ფაქტობრივად, სინამდვილეს არ შეესაბამება. ასეთ შემთხვევებში, კრიპტოვალუტის საწყისი გამოშვება პრემაინინგის ეტაპზე ხორციელდება და ის თავსდება რეზერვებში, რომლებიც კონტროლდება მფლობელების მიერ, შემდგომი რეალიზაციის მიზნით. ამგვარად, მხოლოდ მსგავს შემთხვევაშია შესაძლებელი პროექტის შემმუშავებლების მხრიდან მისი ბოროტად გამოყენება, რადგან მოცემულ კრიპტოტოკენებში სახსრების ჩამდებმა ინვესტორებმა შეიძლება ზარალი განიცადონ. ამის მიზეზი საკმაოდ ბევრია და ჩვენ ICO-ში ინვესტირების პრობლემებს ცალკე თავში განვიხილავთ.

ხდება ხოლმე, რომ ზოგიერთი ადამიანი, რომელმაც ვერ შეძლო რაიმე მოვლენაზე საკუთარი აზრის ჩამოყალიბება, მას ცნობილი ადამიანების გამონათქვამების მიხედვით აყალიბებს. კრიპტოინდუსტრიის არსებობის ათი წლის განმავლობაში, მასზე განსხვავებული ავტორიტეტის მქონე ადამიანთა მხრიდან აზრების მთელი სპექტრი გამოითქვა. აღსანიშნავია, რომ თუკი იშვიათად გამონათქვამები ზომიერებით გამოირჩეოდა, უმრავლესობა ხასიათდებოდა შეფასების ან

უკიდურესად გულწრფელი აღტაცებით, ანდა პირიქით, აგრესიული მიუღებლობით და აპოკალიფსურ წინასწარმეტყველებებსაც შეიცავდა. ბიზნესის, პირველ რიგში მაღალტექნოლოგიური სფეროს წარმომადგენელთა შეფასებები ძირითადად, დადებითი გახლდათ. ცნობილი ეკონომისტები და მილიარდერი ინვესტორები მიდრეკილნი იყვნენ ნეგატიური სცენარებისაკენ იმასთან დაკავშირებით, თუ სადამდე შეიძლება კრიპტოვალუტებმა მიიყვანოს მათ მიმართ ზედმეტად ოპტიმისტურად განწყობილი მყიდველები. კრიპტოვალუტების იდეას ერთმნიშვნელოვნად დაუჭირეს მხარი ბიზნემენებმა – ილონ მასკმა და რიჩარდ ბრენსონმა, ასევე, აშშ-ის ფედერალური სარეზერვო სისტემის ყოფილმა მეთაურმა, ბენ ბერნანკემ. საწინააღმდეგოდ იყვნენ განწყობილი ისეთი ცნობილი ინვესტორები, როგორებიც არიან უორენ ბაფეტი და ჯორჯ სოროსი. კომპანია Microsoft-ის ხელმძღვანელი ბილ გეიტსი თავიდან კრიპტოვალუტების მხარდამჭერად მოგვევლინა, მაგრამ შემდეგ, შეფასებისას უფრო თავშეკავებული იყო.

არ შეიძლება არ აღინიშნოს კრიპტოგარემოზე საზოგადოებრივი აზრის ჩამოყალიბებისთვის კიდევ ერთი მნიშვნელოვანი ფაქტორი. საქმე ისაა, რომ ბევრი ანალიტიკოსი სავსებით სამართლიანად, ერთმანეთისგან მიჯნავს ცნებებს – „ბლოკჩეინი“ და „კრიპტოვალუტა“. ამასთან, პირველი, როგორც წესი, იღებს პოზიტიურ შეფასებას და მას ბრწყინვალე მომავალს უწინასწარმეტყველებენ, ხოლო მეორეს რჩება მხოლოდ ნეგატივი და კრიტიკა, უსწრაფესი დაღუპვის გულწრფელი სურვილით, მათი აზრით – სრული უსარგებლობის გამო. ამ შემთხვევაში საინტერესო ინდიკატორად გვევლინებიან მსხვილი კომერციული ორგანიზაციები და ბანკები, რომლებიც აცხადებენ კრიპტოვალუტების სრულ მიუღებლობას და პარალელურად, მუშაობენ შიდა კორპორაციული და დარგობრივი ბლოკჩეინ-გარემოების მასშტაბურ პროექტებზეც კი. ამ პროექტების მიზანია ინფორმაციის გაცვლისა და დეცენტრალიზებული შენახვის ორგანიზაცია. ამის რეალიზაციისათვის კორპორაციები მსხვილ კონსორციუმებადაც კი ერთიანდებიან, რომლებიც წევრებისაგან მნიშვნელოვან დაფინანსებას იღებენ.

კრიპტოსაზოგადოების წარმომადგენლები საკმაოდ მწვავედ რეაგირებენ სხვადასხვა დონის სპეციალისტების ნეგატიურ გამონათქვამებზე, რომელთა ავტორიტეტსაც თავად კრიპტოენთუზიასტები

ხშირად ეჭვქვეშ აყენებენ. როგორც წესი, ეს გამოიხატება კრიტიკოსების, როგორც ექსპერტების, შესაძლებლობებზე გესლიან თავდასხმებში, რომლებიც ცივილიზაციის ტექნოლოგიური განვითარების მომავლის წინასწარმეტყველებას ჩემულობენ. ახლა ძნელია გამოიცნო, რომელი მხარე აღმოჩნდება მართალი, თუმცა, არ შეიძლება უარვყოთ საზოგადოების დიდი ინტერესი საერთოდ, ბლოკჩეინ-ტექნოლოგიისა და კერძოდ, კრიპტოვალუტების მიმართ. კრიპტოგარემოს გაჩენამ წარმოშვა ფინანსური ინდუსტრიის ისეთი ახალი სექტორები, როგორებიცაა კრიპტოვალუტებით საბირჟო ვაჭრობა და ინვესტიციების მოზიდვა ICO-ის საშუალებით. როგორც ამ პროცესის პირდაპირი შედეგი, წარმოიშვა ფინანსური მომსახურების მომხმარებლებისათვის სრულიად უცნობი რისკები, რომლებსაც რიგ შემთხვევებში მოჰყვა მნიშვნელოვანი ფინანსური დანაკარგები არაპროფესიონალ ინვესტორებს შორის. ამიტომ მომდევნო თავში ვისაუბრებთ კრიპტოვალუტასა და ინვესტიციებზე და კიდევ იმაზე, თუ როგორ უნდა ვმართოთ ამ დროს აუცილებლად წარმოქმნილი რისკები.

ინვესტიციები ICO-ში

2016 წელს – 100 მილიონი დოლარი, ერთი წლის შემდეგ – 6 მილიარდი, ხოლო 2018 წელს 22 მილიარდ დოლარზე მეტი. ეს სხვა არაფერია, თუ არა ინვესტიციები კრიპტოტოკენების პირველად განთავსებაში, ანუ, სხვა სიტყვებით რომ ვთვათ, ICO პროექტებში, რომლებიც უკანასკნელ რამდენიმე წელიწადში ბლოკჩეინ-ტექნოლოგიების ბაზაზე შეიქმნა. ტოკენიზაციისადმი მიძღვნილ თავში გაკვრით შევეხეთ კრიპტოპროექტებში სახსრების მასობრივი მოზიდვის საკითხს, რომელსაც სლენგზე აგრეთვე უწოდებენ „ტოკენების კრაუდსეილებს“ – ინგლისური tokens crowdsale-იდან (სიტყვასიტყვით – „ტოკენების მასობრივი გაყიდვა“). ახლა დადგა დრო, ეს პროცესი დეტალურად განვიხილოთ. ჩვენი მიზანია გავარკვიოთ, სახელდობრ რამ უბიძგა ინვესტორების მასას, ჩაედოთ, გადაუჭარბებლად შეიძლება ითქვას, უზარმაზარი თანხები ვირტუალური კრიპტოაქტივების შეძენაში, მეტიც – აქამდე ყველასთვის უცნობი პროექტების ემიტირებულში, არსაიდან გაჩენილში, რაც მათ ხელს არ უშლის, პრეტენზია ჰქონდეთ სხვადასხვა საქმიან სფეროში და, პირველ რიგში, ფინანსურ ინდუსტრიაში რევოლუციურ ცვლილებებზე.

პროექტების ჩაფიქრება და სარეალიზაციოდ წარდგენა ხდებოდა ძირითადად IT სფეროს ახალგაზრდა სპეციალისტთა ჯგუფების მიერ, სამეცნიერო სამყაროს წარმომადგენლებთან ერთად. როგორც წესი, ესენი იყვნენ მათემატიკისა და ეკონომიკის დოქტორები და მაგისტრები. სწორედ ეს უკანასკნელნი ანიჭებდნენ პროექტებს აუცილებელ აკადემიურ ბრწყინვალებას, ქმნიდნენ მათთვის რთულ მათემატიკურ და ეკონომიკურ აპარატებს, რაც შესაფერის შთაბეჭდილებას ახდენდა ინვესტორებზე. არსებითად, შთაბეჭდილების მოხდენა აუცილებელი იყო, წინააღმდეგ შემთხვევაში, პროექტის სასტარტო ნაწილის რეალიზება ანუ მნიშვნელოვანი ინვესტიციების შეგროვება, ძალზე პრობლემატური იქნებოდა.

უკანასკნელ დრომდე ბლოკჩეინ-პროექტების შემუშავებაში ინვესტიციების მოსაზიდად, მათ მფლობელებს სჭირდებოდათ მხოლოდ

სამი რამ – საკუთარი იდეის ახსნა, საზოგადოებაში კრიპტოვალუტის გარშემო ხმაურის ატეხა და კრიპტოდარგში რეგულაციის არარსებობა. პროექტის კონცეფციის ახსნა მოცემული იყო დოკუმენტის ფორმით, რომელსაც დაარქვეს „თეთრი წიგნი“ – ინგლისურად white paper. მასში, როგორც წესი, თავიდან დგებოდა რაღაც პრობლემა, ხოლო შემდეგ გვთავაზობდნენ ბლოკჩეინ-ტექნოლოგიის გამოყენებით მისი გადაჭრის მეთოდს. უმრავლეს შემთხვევაში, მსგავსი დოკუმენტები შეიცავდა თავებს, რომლებიც ეთმობოდა პროექტის კრიპტოვალუტის გამოშვებას, სადაც მითითებული იყო მისი საწყისი ღირებულება თავდაპირველი ბრუნვის დროს. ბოლოს, კონცეფციების ახსნა სრულდებოდა საგზაო რუკით, რომელიც პროექტის განვითარების, მისი რეალიზაციის დროის კონკრეტულ პერიოდებზე მიბმული ეტაპების განსაზღვრებებს შეიცავდა.

დანიშნულ დროს პროექტის კრიპტომონეტები გასაყიდად გამოჰქონდათ, ხოლო ინვესტორებს ფიატური ფულით ან ფართო მოხმარებაში არსებული სხვა კრიპტოვალუტით – როგორც წესი, ეს ბიტკოინები და ეთერები იყო – მათი შეძენა შეეძლოთ. იყო მომენტები, როცა სავაჭროდ გამოტანილი ტოკენების რაოდენობა ვერ აკმაყოფილებდა მოთხოვნილებას, ძალზე ბევრ ინვესტორს სურდა პროექტში საკუთარი სახსრების ჩადება, მისი კაპიტალიზაციის სწრაფი გაზრდის იმედით. ასეთ შემთხვევებში შესაძლო იყო მოვლენების განვითარების ორი ვარიანტი: ან ტოკენები ხვდებოდათ მათ, ვინც ისინი ადრე იყიდა, ან პროექტის მფლობელები ყველა მსურველის განაცხადებს იღებდნენ, ხოლო შემდეგ ტოკენებს განაცხადების მოცულობის მიხედვით ინვესტორებს შორის ანაწილებდნენ. გასაგებია, რომ ყველა მყიდველს ჯგამში ნაკლები ტოკენი ხვდებოდა, ვიდრე სურდა, მაგრამ მათ შესაძლებლობა ჰქონდათ, რაღაც ნაწილი მაინც შეეძინათ და კრიპტოაქტივების პირველადი განაწილების პროცესს მიღმა არ დარჩენილიყვნენ.

მიუხედავად შემმუშავებლებისათვის ICO პროცედურის მიმზიდველობისა, ყველა მათგანი როდი მიდიოდა ამ ღონისძიებაზე. ზოგიერთმა დეველოპერმა თავისთვის შეუძლებლად ჩათვალა მონეტების პირველადი განთავსება, ამავდროულად ორგანიზება გაუკეთა მათ განაწილებას ან მაინინგის საფუძველზე, ან ჩვეულებრივი საცალო მიყიდვის სახით ქსელის წევრებზე. უკანასკნელ შემთხვევაში, მონეტების შეძენას ფრიად უტილიტარული ხასიათი ჰქონდა, რად-

გან ლოკალური ტოკენები საჭირო იყო ქსელის შიგნით ტრანზაქციების საკომისიოების გადასახდელად. რა თქმა უნდა, ისინი შეიძლება შეეძინათ სპეკულაციური მიზნებითაც, თუმცა შემმუშავებლები ოფიციალურად არ პოზიციონირებდნენ პროექტის კრიპტოვალუტას როგორც საინვესტიციო ფინანსურ ინსტრუმენტს.

სატოში ნაკამოტომ შექმნა ქსელი „ბიტკოინი“, სადაც არავითარი ICO საერთოდ არ იგულისხმებოდა, ამ გარემოში კრიპტომონეტები კონკურენტული მაინინგის საშუალებით მოიპოვება. ამ შემთხვევაში უპირატესობა ჰქონდა იმ კვანძებს, რომლებმაც მონეტების მოპოვება ქსელის სხვა წევრებზე ადრე დაიწყეს, რადგან ისარგებლეს შესაფერისი მომენტით, როდესაც მაინინგის გამოსათვლელი ამოცანის სირთულე ჯერ კიდევ დაბალ მაჩვენებლებზე იყო. ამგვარად, ბიტკოინის პირველმა მაინერებმა, თავად სატოში ნაკამოტოს ჩათვლით, შეძლეს თავი მოეყარათ საკმაო კაპიტალისათვის, როდესაც ამ კრიპტოაქტივის ფასები ცამდე ავარდა. მაგრამ Ethereum-ის შემქმნელმა ვიტალიკ ბუტერინმა თავისი ICO მაინც ჩაატარა და შეკრიბა სახსრები ფონდისათვის, რომელიც მისი პროექტის განვითარების ხანგრძლივვადიანი დაფინანსების გარანტიას იძლეოდა. ოღონდ ის სულაც არ იყო პირველი, რომელმაც მსგავსი პროცედურა განახორციელა.

კრიპტომონეტების პირველადი განთავსების ჩატარების დარგში პიონერად ითვლება პროექტი Mastercoin (შემდგომში Omni ეწოდა), რომელმაც 2013 წელს პროექტის შემუშავებისათვის დაახლოებით 500 000 დოლარი შეაგროვა. ამავე წლის ბოლოსათვის მისმა კაპიტალიზაციამ 100 მილიონ დოლარს გადააჭარბა, ხოლო უკვე 2014 წელს Mastercoin ინდუსტრიაში ყველაზე მსხვილ კრიპტოვალუტათა შვიდეულში შევიდა. პროექტი შეიქმნა როგორც ბიტკოინ-ქსელის ინფრასტრუქტურის ზედნაშენი, რათა მისთვის უფრო მეტი უსაფრთხოება და სტაბილურობა მიენიჭებინათ. პროექტი ასევე ითვალისწინებდა მიმოქცევის უფრო რთული, ვიდრე ბიტკოინის, წესების მქონე კრიპტოვალუტური ინსტრუმენტების შექმნის შესაძლებლობას ისე, რომ საბაზო ქსელის პროტოკოლი არ იცვლებოდა. მიუხედავად პროექტის კრიპტოვალუტის გაშვებიდან სულ ცოტა ხანში მის მიმართ ინვესტორთა საწყისი ინტერესისა, კოტირებებმა ულმობელი ვარდნა დაიწყო და იმ ხმაურმაც კი, რომელიც 2017 წლის ბოლოს ატყდა, ისინი ისტორიულ მაქსიმუმამდე ვერ დააბრუნა. შემდგომშიც

კაპიტალიზაციის გამალებული ვარდნა გრძელდებოდა და თითქმის ასჯერ – დაახლოებით 1,5 მილიონ დოლარამდე შემცირდა.

პროექტ Mastercoin-ის ისტორია ბევრ რამეში საჩვენებელია, რადგან შემმუშავებლების დაპირებები წინააღმდეგობაში მოვიდა რეალობაში დანერგილ ფუნქციონალთან და ფასეულობებთან, რომლებიც პროექტს შეეძლო მომხმარებლებისათვის შეეთავაზებინა. პროექტისადმი საინვესტიციო ინტერესის დაკარგვაში არცთუ უმნიშვნელო როლი, რა თქმა უნდა, მისმა მომდევნო კონკურენტებმაც შეასრულეს. აქ პირველ რიგში, კვლავ უნდა გავიხსენოთ პროექტი Ethereum, რომლის ICO-ც ჩატარდა Mastercoin-ის კვალდაკვალ უკვე 2014 წლის ზაფხულში. როგორც ადრე აღვნიშნეთ, სულ რაღაც 42 დღეში პროექტმა შეაგროვა შთამბეჭდავი თანხა – 18 მილიონი დოლარი, ამასთან, ეთერის ერთი მონეტის ფასმა დაახლოებით 30 ამერიკული ცენტი შეადგინა, თავისი ფასის პიკში კი, 2018 წლის იანვარში, მონეტა 1400 დოლარზე ოდნავ ნაკლებად ღირდა. თუმცა, მისი უმრავლესი „თანამოძმე“ კრიპტოვალუტის მსგავსად, ეთერმა ღირებულებით პიკზე ყოფნისას ასრებული ფასის 90% უკვე იმავე 2018 წლის ბოლოსათვის დაკარგა.

პროექტ Ethereum-ის ICO-ის შემდეგ განთავსება იშვიათობას აღარ წარმოადგენდა, ხოლო კრიპტომონეტების საჯარო განთავსებების „ოქროს ხანა“ 2017 წელს დადგა, როდესაც ამ პროცესმა ზვავისებრი სახე მიიღო. სწორედ ამ წლის განმავლობაში პოვა ყველაზე ფართო გავრცელება მოვლენამ, რომელსაც შემდგომში „კრიპტოვალუტური ჰაიპი“ („ხმაური“, „ხმაურიანი რეკლამა“) უწოდეს. არაპროფესიონალ ინვესტორთა ბრბოები, რომელთა უმრავლესობასაც ბუნდოვანი წარმოდგენა ჰქონდა ბლოკჩეინ-ტექნოლოგიებზე, უყოყმანოდ დებდნენ თავიანთ ფულს სხვადასხვა კრიპტოპროექტში. ამასთან, ბევრი პროექტი არსებობდა მხოლოდ იდეის ზოგადი აღწერილობის სახით, რომელიც თანმდევ „თეთრ წიგნში“ იყო გადმოცემული.

ზოგ შემთხვევაში შემმუშავებლები ისეთი ფუნქციების განხორციელების დაპირებას იძლეოდნენ, რომლებსაც იმ მომენტში (და შემდეგშიც) აშკარად არ ჰქონდა ტექნოლოგიური გადაწყვეტა. მაგრამ გულად კრიპტოინვესტორებს ეს საერთოდ არ აწუხებდათ, ისინი აქტიურად ყიდულობდნენ განურჩევლად ყველა ტოკენს, იმის იმედით, რომ უახლოეს მომავალში მათი ღირებულება სულ მცირე 10-ჯერ მაინც გაიზრდებოდა. ასეთმა საინვესტიციო მოლოდინმა

კრიპტოსაზოგადოებაში სლენგური სახელი to the Moon ანუ „მთვარეზე აფრენა“ მიიღო. კრიპტოინვესტორების კიდევ ერთი სამოტივაციო ფაქტორი იყო ე.წ. „სინდრომი FOMO“ ანუ „ვერმოსწრების შიში“ (fear of missing out). საუბარი იყო იმის შიშზე, რომ არ გამოჰპაროდათ აქტიურად მზარდ კრიპტოდარგში საკუთარი სახსრების ინვესტირების დრო და საბოლოოდ, ზემოგებების სწრაფად მიღების შანსის გარეშე არ დარჩენილყვნენ.

მართლაც, ძალზე ბევრი კრიპტოაქტივის ღირებულება საფუარიავით იზრდებოდა. ზრდის დრაივერები გახდა მთავარი კრიპტოვალუტები – ბიტკოინი და ეთერი, ხოლო დანარჩენი ტოკენები ერთ-ერთ მათთაგანთან კოტირდებოდა. ამგვარად, საფლაგმანო კრიპტოვალუტების ფიატური ფულის მიმართ ღირებულების ზრდა სხვა კრიპტოაქტივების მიყოლასაც იწვევდა. მართალია, მათ შორის რომელიმე იშვიათად ძვირდებოდა უშუალოდ ბიტკოინის ან ეთერის მიმართ, მაგრამ ასეთი შემთხვევებიც მომხდარა. „თეთრი წიგნის“ პროექტები პირობას იძლეოდა, რომ პროდუქტების პირველი ვერსიების გამოშვება ერთი წლის ან მეტი დროის შემდეგ მოხდებოდა, ამიტომ ინვესტორები იძულებულნი იყვნენ, უბრალოდ დაეჯერებინათ შემმუშავებლებისათვის. ბიზნესანალიტიკოსები მრავალჯერ ეცადნენ, ინვესტორთა ყურადღება მიეპყროთ კრიპტოპროექტების კაპიტალიზაციის შეფასების აშკარა დისბალანსზე კლასიკურ სტარტაპებთან შედარებით. მაგრამ ამ გაფრთხილებებს მიზნობრივმა აუდიტორიამ ყური არ ათხოვა. ინვესტორები მოგვიანებით გამოფხიზლდნენ.

პირველ რიგში, მასობრივ ICO-ის ყურადღება სხვადასხვა ქვეყნის მთავრობებმა და ფინანსურმა რეგულატორებმა მიაქციეს. ერთ-ერთი თავისი ფუნქციის, ინვესტორთა ინტერესების დაცვით დეკლარირებასთან ერთად, ამ ინსტიტუტებმა სასწრაფოდ დაიწყეს ზომების მიღება კრიპტოშემმუშავებლების მიერ საინვესტიციო სახსრების შეგროვების შესაზღუდად, რაც ფაქტობრივად, ფინანსური „ველური დასავლეთის“ მოდელით ხორციელდებოდა. თავიდან ინვესტიციები ICO-ში აკრძალეს აშშ-ში, სადაც ფინანსური რეგულირებისა და კონტროლის მსოფლიოში ერთ-ერთი ყველაზე მკაცრი სამართლებრივი სისტემაა. შემდეგ მსგავსი ზომები მიიღეს ჩინეთში, თანაც, ბევრად უფრო მკაცრი ფორმით: ხელისუფლებამ არა მარტო აკრძალა ნებისმიერი ICO-ის ჩატარება, არამედ შემმუშავებლებს ადრე მოზიდული

სახსრების მთლიანი მოცულობით დაბრუნება დააკისრა. მიუხედავად იმისა, რომ კიდევ რამდენიმე სახელმწიფო მიჰყვა აშშ-ისა და ჩინეთის კვალს, სწორედ ამ ქვეყნებში შემოღებულმა აკრძალვებმა მოახდინა მაქსიმალურად ნეგატიური გავლენა ფინანსურ ნაკადებზე კრიპტოინდუსტრიაში.

რა თქმა უნდა, არაკორექტული იქნებოდა ჩაგვეთვალა, რომ კრიპტოვალუტების შეუჩერებული ზრდის შემდგომ კრიპტოვალუტების კოტირებების ჩამოშლა გამოწვეული იყო მხოლოდ გარემო ფაქტორებით, კერძოდ, რეგულაციური ზომებით. ფინანსური სამყაროს კანონები ისეთია, რომ აქტივების ღირებულების ერთი მიმართულებით მომხდარი სწრაფი ცვლილება, რომელსაც მხოლოდ ემოციური და არა ფუნდამენტური მიზეზები არ გააჩნია, ძალზე დიდხანს ვერ გაგრძელდება. ადრე თუ გვიან, სავაჭრო ინსტრუმენტზე, თუნდაც უახლესი ტექნოლოგიების პროდუქტზე, მონეტარული შეფასების კლასიკურ პრინციპებს გამოიყენებენ, და იმ შემთხვევაში, როდესაც ამ აქტივების უკან მდგომი პროექტი-ემიტენტები ვერ შეძლებს საკუთარ ინვესტორებს უჩვენოს გონივრული ბიზნესსტრატეგია, სწორი საბაზრო ფოკუსირება და მომხმარებელთა ბაზრის რეალური მოცვა, მაშინ მათი კაპიტალიზაციის ვარდნა მხოლოდ დროის საკითხი იქნება.

რაც შეეხება ICO-ის მომავალს, ეს მოვლენა უეჭველად განვითარდება ინდუსტრიაში დაგროვილი გამოცდილების გათვალისწინებით. ცვლილებები შეეხება რეგულაციურ ასპექტებსაც, პირველ რიგში იმიტომ, რომ ინვესტორებს ნაყიდი კრიპტოაქტივების ფლობის იურიდიული უფლება მიეცეთ. ამჟამად მსოფლიოში ძალზე ცოტაა ქვეყანა, რომლის კანონმდებლობაც ICO-ში ინვესტიციებს ჩვეულებრივ კომპანიებში წილების ან აქციების კლასიკური ყიდვა-გაყიდვის თანაბრად აღიარებს. უმრავლეს შემთხვევაში ICO-ზე ან ბირჟაზე ნაყიდი ტოკენები, თუნდაც მათ საინვესტიციო სტატუსი ჰქონდეს, ინვესტორებს არ აძლევს კომპანია-ემიტენტის პროპორციული წილის ფლობის იურიდიულ უფლებას. ამგვარად, ასეთი ტოკენების მფლობელს, როგორც პროექტის მმართველ იურიდიულ პირს, არ ექნება არავითარი უფლება არც ხმის მიცემისა სტრატეგიულად მნიშვნელოვან საკითხებზე, არც დივიდენდების განაწილებისა და არც ახალ ინვესტორებზე კომპანიის მიყიდვისა. უფრო მეტიც, პროექტების ბევრ შემმუშავებელს ურჩევნია გაავრცელოს უტილიტარული ტოკენები საინვესტიციოს

მაგივრად, რაც პოტენციური მყიდველის აშკარა შეცდომაში შეყვანაა მათი იმ პროექტში წილობრივი საკუთრების უფლების მოპოვების თვალსაზრისით, რომელშიც ისინი სახსრების ჩადებას აპირებდნენ.

არანაკლებ ცხადია, რომ ICO-ის საშუალებით სახსრების შეგროვების მცდელობები მხოლოდ PDF ფორმატში ფაილის სახით „თეთრი წიგნის“ არსებობისას, რომელსაც შემმუშავებელი პროექტის საიტზე დებს, უცილობლად წარსულს ჩაჰბარდება. სანამ ინვესტიციების მოზიდვას დაიწყებენ, პროექტების მფლობელებს მოუწევთ აუცილებელი იურიდიული პროცედურების გავლა: კომპანიის რეგისტრაციით, აუცილებლობისას ლიცენზიის მიღებით, ასევე, ადგილობრივი ფინანსური რეგულატორების მიერ დამტკიცებული ემისიის პროსპექტის მომზადებით. მაგრამ ბევრად უფრო მნიშვნელოვანია, რომ ICO-ის ჩატარების მომენტისათვის უკვე უნდა არსებობდეს ე.წ. MVP (Minimum Viable Product) ანუ „მინიმალურად სიცოცხლისუნარიანი პროდუქტი“, რომელიც პროექტის რეალიზაციის საწყის ეტაპს გულისხმობს. ეს საჭიროა იმისათვის, რომ ინვესტორებს ვაჩვენოთ არა მარტო შემმუშავებლის განზრახვის სერიოზულობა, არამედ პროექტით შემოთავაზებული ტექნოლოგიური კონცეფციის ქმედითობა.

მრავალრიცხვოვანმა ICO-მ, როგორც მოსალოდნელი იყო, უთვალავი, როგორც უტილიტარული, ასევე საინვესტიციო ტოკენების წარმოქმნა გამოიწვია. ლოგიკურია ვივარაუდოთ, რომ პროექტების შემმუშავებლებსაც და ახალგამოჩეკილ ინვესტორებსაც მოუხდათ კრიპტოაქტივების გაცვლა როგორც ერთმანეთში, ასევე – ფიატურ ფულზე. ამისათვის საჭირო გახდა ელექტრონული სავაჭრო მოედნები, რომლებიც საშუალებას იძლეოდა, საკმაოდ სწრაფად და საერთო საბაზროსთან მაქსიმალურად მიახლოებული ფასების საფუძველზე დადებულიყო მსგავსი გარიგებები. ასე გაჩნდა კრიპტოვალუტური ბირჟების ინფრასტრუქტურა, რომლებიც სხვადასხვა ტექნოლოგიური გადაწყვეტის გამოყენებით იყო აგებული და ვაჭრობისათვის შემოთავაზებული მრავალგვარი ინსტრუმენტით გამოირჩეოდა. შემდეგი თავი სწორედ კრიპტოინდუსტრიის ამ მნიშვნელოვანი კომპონენტის განხილვას ეთმობა.

კრიპტოვალუტური ბირჟები

პირველად თავის ისტორიაში კაცობრიობა ცნება „ბირჟას“ შეხვდა 1406 წელს, როდესაც ქალაქ ბრიუგეში, ახლანდელ ბელგიაში, იმ დროს კი ბურგუნდიის საჰერცოგოში, თამასუქებით ვაჭრობის პირველი მოედანი მოეწყო. ის დააფუძნეს ვან დერ ბურსის ფინანსური ოჯახის წარმომადგენლებმა, რომელთა გვარი ლათინურზე „საფულეს“ (beurs, bourse, burse) ნიშნავს. სწორედ მან მისცა სახელი მსგავს სავაჭრო მოედნებს, რომლებსაც შემდგომში „ბირჟები“ (exchanges) უწოდეს. თავიდან ბირჟები უმეტესად სასაქონლო იყო, მაგრამ შემდგომში მათზე სხვადასხვა სახის ფასიანი ქაღალდებით ვაჭრობაც დაიწყეს. 1730 წელს პირველი ბირჟა გაჩნდა იაპონიაშიც, ბრინჯით ვაჭრობისათვის, აშშ-ში კი პირველი სავაჭრო მოედანი მხოლოდ 1792 წელს ნიუ-იორკში შეიქმნა.

XX საუკუნის დასაწყისისათვის ბირჟები ყველგან გავრცელდა, ისინი მოქმედებდა თითქმის ყველა განვითარებულ ქვეყანაში. წარმოშობის მომენტიდან და თითქმის წინა საუკუნის ბოლომდე ბირჟებზე ვაჭრობა მიმდინარეობდა ბირჟის მაკლერთა საშუალებით, რომლებიც კონტრაგენტებთან გარიგებებს დებდნენ საკუთარი ხმის გამოყენებით. სწორედ მაკლერების შეძახილები, რომლებიც შეიცავდა სავაჭროდ გამოტანილი ინსტრუმენტის სახელს, მის ფასსა და გარიგების მიმართულებას (ყიდვა ან გაყიდვა), წარმოადგენდა ე.წ. „საბირჟო ორდერს“ ანუ დავალებას გარიგების დადებაზე მათთვის უფლებამიმნიჭებელი კლიენტების მხრიდან. ვაჭრობის დაწყება და დასრულება აღინიშნებოდა სპეციალური საბირჟო ზარების რეკვით, რომლებსაც ზოგიერთი ბირჟა დღემდე კვლავაც იყენებს, ახლა უკვე წარსულისთვის ხარკის გაღების ნიშნად.

ინტერნეტისა და საინფორმაციო ტექნოლოგიების განვითარებამ ხელი შეუწყო საბირჟო მაკლერების ხმაურიანი ბრბოს სავაჭრო ოთახებიდან თანდათანობით გამოძევებას. გარიგებები თანამედროვე საბირჟო მოედნებზე ხორციელდება სპეციალური კომპიუტერული სისტემების მეშვეობით. ისინი საშუალებას იძლევა, ბევრად უფრო სწრაფად და ეფექტიანად შეახვედროს ერთმანეთს გარიგებების კონტრა-

გენტები და ასევე, ბირჟების მონაწილეთა მიერ ჩატარებული ვაჭრობის მთელი მოცულობის აღრიცხვა აწარმოოს. საბირჟო მოედნების ინტერნეტში ჩართვამ შექმნა საფუძველი, მნიშვნელოვნად გაზრდილიყო ვაჭრობაში მონაწილე ტრეიდერების რაოდენობა – ახლა მასში მონაწილეობენ არა მარტო ბაზრის მსხვილი წარმომადგენლები, არამედ ტრეიდერებიც, რომლებიც ფინანსური ინსტრუმენტების შედარებით მცირე მოცულობებით ოპერირებენ. მიუხედავად ამისა, საბირჟო ვაჭრობაზე აქციების გატანა რთულ და ძვირად ღირებულ პროცესად რჩება, განსაკუთრებით მცირე და საშუალო კომპანიებისათვის, რომლებიც შემოსავლების მაღალი დონით ვერ დაიკვეხნიან.

როგორაა ბირჟის მუშაობა მოწყობილი? გამარტივებულად ეს ასე შეგვიძლია აღვწეროთ: ვაჭრობების მონაწილეები საბირჟო სისტემაში გზავნიან თავიანთ წინადადებებს გარიგებების შესახებ: რომელი ინსტრუმენტი და რა ფასად სურთ იყიდონ ან გაყიდონ. შემდეგ ამ წინადადებების, ან „ორდერების“ მთელი მოცულობა ანალიზდება ბირჟის პროგრამული უზრუნველყოფის მიერ, რომლის ამოცანაცაა შემხვედრი განაცხადების შეპირაპირება, რათა მათგან შედგეს გარიგება. დავუშვათ, ბირჟის რომელიღაც ტრეიდერს სურს ასი უნცია ოქროს გაყიდვა, თითოეული უნცია – 1300 დოლარად, ვიღაცას კი სურს ამ ფასად გარკვეული რაოდენობის ოქროს შეძენა. ასეთი ორდერების არსებობისას ბირჟა ახორციელებს მათ „მატჩინგს“ ანუ არეგისტრირებს ტრეიდერთა სავაჭრო მოთხოვნების დამთხვევას, რის შემდეგაც გარიგება დადებულად ითვლება, ერთი ტრეიდერი აძლევს ოქროს და იღებს ფულს, ხოლო მეორე იღებს ოქროს და გასცემს ორდერში შეთანხმებულ თანხას.

გასაგებია, რომ ორდერი, რომელიც თავის შემხვედრ „წყვილს“ ვერ პოულობს, სისტემაში ბევრად მეტია, ვიდრე გარიგების ფორმირებისას შესრულებული, ამიტომ ბირჟის პლატფორმა მუდმივად ასახავს მოთხოვნისა და მიწოდების ორდერების ერთობლიობას ყოველ ცალკე აღებულ სავაჭრო ინსტრუმენტზე. ორდერები ხარისხდება საუკეთესო ფასიდან ყველაზე ცუდამდე, და ის ორი, რომლებსაც ყველაზე ახლო მნიშვნელობები აქვს მოთხოვნასა და მიწოდებას შორის, სიის სათავეში დგას. მათ შორის ფასობრივი განსხვავება შეადგენს ცნებას „ბირჟის სპრედი“, ე.ი. მატჩინგისათვის ანუ გარიგების შესრულებისათვის, ხელის შემშლელი კოტირების მინიმალური წყვეტის ცნებას. არცთუ

უსაფუძვლოდ ითვლება, რომ საბირჟო აქტივებზე ფასწარმოქმნა, რომელიც ვაჭრობების პროცესში სტიქიურად ფორმირდება, ყველაზე სამართლიანი და მიმდინარე საბაზრო მნიშვნელობებთან მაქსიმალურად მიახლოებულია. რა თქმა უნდა, ეს მტკიცება სწორი იქნება მხოლოდ მაშინ, როცა ბირჟას ჰყავს საკმარისად ბევრი მონაწილე, რომლებიც ამ ინსტრუმენტის მნიშვნელოვანი მოცულობებით ვაჭრობენ, სხვა სიტყვებით რომ ვთქვათ, როდესაც ინსტრუმენტს მაღალი ლიკვიდურობა აქვს.

ბუნებრივია, როცა გაჩნდა ისეთი მოვლენა, როგორიც კრიპტოვალუტაა, მის მფლობელებს ავტომატურად აღეძრათ ელექტრონული სავაჭრო მოედნების მოთხოვნილება, ამ ახალი ტიპის ინსტრუმენტების გასაცვლელად თავიდან ფიატურ ვალუტაზე, ხოლო შემდეგ – სხვა კრიპტოაქტივებზე. ბიტკოინის როგორც ინვესტიციისადმი მიძღვნილ თავში აღწერილი იყო პირველი კრიპტობირჟები, რომლებმაც ამჟამად უკვე შეწყვიტეს არსებობა. ჰაკერული შეტევების ან შიდა დანაშაულების გამო, კრიპტომონეტების მნიშვნელოვანმა დანაკარგებმა გამოიწვია პირველი ყველაზე პოპულარული ბირჟის Mt. Gox-ის გაკოტრება. მიუხედავად ამისა, შემდგომში გაჩნდა ახალი, გარემო ფაქტორებისადმი უფრო მედეგი კრიპტოვალუტური ბირჟები. ბევრმა მათგანმა შეძლო განევითარებინა თავისი საქმიანობა მართლაც მსოფლიო მასშტაბამდე და ვაჭრობის მოცულობით დღე-ღამეში მილიარდობით დოლარის ეკვივალენტის ოპერაციებს ახორციელებდა.

ბუნებრივია, კრიპტოინდუსტრიის ბირჟების ვაჭრობის ერთობლივი მოცულობა ჯერ კიდევ ძალზე შორსაა კლასიკური ბირჟებისაგან. თავისი პოპულარობის პიკზეც კი 2017 წლის დეკემბერში კრიპტობირჟებზე ვაჭრობის საერთო მოცულობა დღე-ღამეში დაახლოებით 50 მილიარდ დოლარს შეადგენდა, იმ დროს, როდესაც ნიუ-იორკის საფონდო ბირჟის (NYSE) საშუალო სადღეღამისო მოცულობა დაახლოებით 1,5 ტრილიონ დოლარს აღწევს. მას ბევრად არ ჩამორჩება ბირჟა NASDAQ, 1,3 ტრილიონი დოლარის საშუალო სადღეღამისო მოცულობით. 2019 წლის გაზაფხულისათვის კრიპტოვალუტებით ვაჭრობის მოცულობა დღე-ღამეში სულაც 30 მილიონ დოლარამდე შემცირდა. მაგრამ ნუ დავივიწყებთ იმას, რომ კრიპტოვალუტური ინდუსტრია ძალზე ახალგაზრდაა, მნიშვნელოვან ფასობრივ რყევებს განიცდის და თავის კლასიკურ „თანამოძმეთაგან“ განსხვავებით, მნიშვნელოვანი რეგულაციური წნეხის ქვეშ იმყოფება.

ათასობით ახალი კრიპტოპროექტის გამოჩენამ სხვადასხვა კრიპტოტოკენის მასობრივი ემისია გამოიწვია, რომელთა მფლობელებს ძალიან სურდათ მათი მონეტარული საბირჟო შეფასების მიღება. ამისათვის პროექტების შემმუშავებლები უნდა შეთანხმებოდნენ პოპულარული ბირჟებიდან ერთ-ერთს მაინც, რათა მათი ტოკენები ვაჭრობაზე დაეშვათ. კრიპტოვალუტური ჰაიპის დროს ეს არცთუ ისე იოლი ამოცანა იყო, უფრო სწორად – არცთუ ისე იაფი. ყოველი ახალი კრიპტოვალუტის ინტეგრაცია იწვევდა აუცილებელი პროცედურების მთელი რიგის წარმოქმნას, რომლებიც საბირჟო სავაჭრო პლატფორმების პროგრამული უზრუნველყოფის შეცვლასთან იყო დაკავშირებული.

უკანასკნელ როლს არც უსაფრთხოების საკითხები თამაშობდა, რადგან, თუ ახალი ტოკენების გამომშვები პროექტის პროგრამულ კოდში სისუსტეები არსებობდა, მათ ავტომატურად, „მემკვიდრეობით“ იღებდა ბირჟაც, რომელსაც სავაჭრო კრიპტოაქტივების მნიშვნელოვანი რაოდენობა უნდა შეენახა საკუთარ დეპოზიტარიუმებზე. წარმატებული ჰაკერული თავდასხმების შემთხვევაში, ბირჟები იდგნენ ამ ტოკენების მნიშვნელოვანი ნაწილის დაკარგვის რისკის წინაშე და იძულებულნი გახდებოდნენ, ტრეიდერებისათვის ზარალი კაპიტალის საკუთარი რეზერვებიდან აენაზღაურებინათ. მხოლოდ 2018 წლის პირველ ნახევარში კრიპტობირჟებიდან მოპარული იქნა 761 მილიონი დოლარი, ხოლო ყველა საბირჟო ქურდობამ კრიპტოინდუსტრიის არსებობის მთელი დროის განმავლობაში ჯამურად უკვე მილიარდობით დოლარს მიაღწია. არა მხოლოდ ამის გამო, განსაკუთრებით პოპულარულ კრიპტობირჟებზე „შესასვლელი ბილეთი“ საკუთარი ტოკენების განთავსების მსურველთათვის მილიონობით დოლარს ითვლიდა. დამატებით არსებობდა ალბათობა, რომ რაღაც დროის შემდეგ ამ ტოკენებს დელისტინგის (ბირჟის სავაჭრო ლისტინგიდან ამოგდება) პროცედურა ელოდა. ეს შეიძლება მომხდარიყო პირველ რიგში ამ ინსტრუმენტებით ვაჭრობის მცირე მოცულობების გამო, რაც საბირჟო სისტემებში მათი შენარჩუნების პროცესს დაბალეფექტიანს ან წამგებიანსაც კი ხდიდა.

კრიპტოვალუტური ბირჟების აგების მოდელების უმეტესობა შექმნილია კლასიკური არქიტექტურის „კლიენტი-სერვერი“ სახით, ცენტრალიზაციის პრინციპების საფუძველზე. სხვა სიტყვებით რომ

ვთქვათ, ტრეიდერი უნდა ჩაერთოს ბირჟის სერვერში, ასევე გადაგზავნოს თავისი აქტივები (როგორც ფიატური, ასევე კრიპტოვალუტური) ბირჟის დეპოზიტარიუმში (საცავში) იმისათვის, რომ მათით ვაჭრობა შეძლოს. ამ მომენტიდან ის საკუთარ სავაჭრო საშუალებებზე კონტროლს კარგავს და მათი შენახვის უსაფრთხოებასთან დაკავშირებულ ყველა საკითხს ბირჟას გადასცემს. მისთვის აუცილებელია, ენდობოდეს ბირჟას, თუნდაც იმ დრომდე, სანამ საკუთარ საშუალებებს თავის კრიპტოსაფულეზე ან საბანკო ანგარიშზე დაიბრუნებს.

ისტორიამ იცის მრავალი შემთხვევა, როდესაც ტრეიდერები ნაწილობრივ ან მთლიანად კარგავდნენ საკუთარ აქტივებს. ეს ხდებოდა სხვადასხვა პრობლემის გამო, რომლებიც დაკავშირებული იყო როგორც ჰაკერულ თავდასხმებთან, ასევე საბირჟო მოედნების თანამშრომელთა ან მფლობელთა ზიანის მომტან ქმედებებთან. ცენტრალიზებული კრიპტობირჟები ასევე ყოველთვის იყო და იქნება მოწყვლადი იმ მართლმსაჯულების სისტემის ძალოვანი ან მარეგულირებელი ორგანოების რეპრესიული ხასიათის მოქმედებების მიმართ, სადაც ისინი არიან რეგისტრირებული. ყველა ამ ფაქტორმა ერთობლიობაში გამოიწვია ის, რომ ინდუსტრიაში გაჩნდა ტექნოლოგიურად აბსოლუტურად განსხვავებულ პრინციპებზე აგებული ბირჟები.

მოდი გავიხსენოთ, რომ თვით კრიპტოვალუტების ბუნება დეცენტრალიზებულ საწყისებს ეფუძნება და თუ ასეა, მაშინ ძალზე ლოგიკური იქნებოდა საბირჟო სისტემების ასევე განაწილებული არქიტექტურის საფუძველზე აგებაც და ტრეიდერს საკუთარი აქტივების საბირჟო ვაჭრობათა ორგანიზატორების ანუ მესამე პირების კონტროლის ქვეშ გადაცემის აუცილებლობა აღარ ექნებოდათ. სხვა საკითხია, თუ რა უპირატესობები და ნაკლოვანებები აქვს საბირჟო მოედნის აგების დეცენტრალიზებულ პრინციპს. უდავოა, რომ ცენტრალიზებული ბირჟა ორდერების მატჩინგის პოვნასა და დადასტურებაზე ბევრად სწრაფად და საიმედოდ იმუშავებს, რადგან ყველა სავაჭრო განაცხადი ერთ ადგილასაა მოთავსებული და საბირჟო პლატფორმების ალგორითმების ანალიზისათვის ხელმისაწვდომია.

რა თქმა უნდა, დეცენტრალიზებულ ბირჟებს სერვერები არ გააჩნია. ყველა ტრეიდერი ოპერირებს კლიენტის პერსონალური პლატფორმით, რომელიც ინფორმაციას ცვლის სხვა იმგვარივე ტერმინალებთან პირდაპირი შეერთების საშუალებით, peer-to-peer („თანაბარი

თანაბართან“) პრინციპით. მაშ, სადღა ინახება ორდერების ბაზა, როგორ ხორციელდება მათი მატჩინგი, ასევე, როგორ სრულდება გარიგებები, კონტრაგენტებს შორის სავაჭრო აქტივების ფიზიკური გადაადგილების ჩათვლით?

თუ დეცენტრალიზებული ბირჟების მუშაობის მექანიზმებს დეტალურად არ განვიხილავთ, ძირითადი ის გახლავთ, რომ სისტემაში გაგზავნილი ყველა ორდერი კოპირდება ყველა მის წევრს შორის. ამასთან, საბირჟო ქსელის კვანძები დამოუკიდებლად ახორციელებს ორდერების მატჩინგს, სთავაზობს დანარჩენ წევრებს გარიგებათა შეპირაპირების ვარიანტებს, რათა ქსელმა ამოარჩიოს მათ შორის საუკეთესო შეფასების შეთანხმებული პარამეტრების მიხედვით, და ამგვარად მივაღწიოთ საერთო კონსენსუსს. ხანდახან ქსელი შეიძლება იყოფოდეს „ფედერაციებად“, როდესაც ყოველი მათგანის სათავეში დგას ან არჩეული, ან სპეციალურად დანიშნული კვანძი. სისტემის ეს წევრები პასუხს აგებენ როგორც საკუთარ სეგმენტში ინფორმაციის გავრცელებაზე, ასევე მის შიგნით ორდერების მატჩინგზე და ამისათვის საკომისიოს იღებენ. მართალია, ამ დროს ინფორმაცია თავისი ფედერაციის ფარგლებს არ ტოვებს, რაც სავაჭრო ინსტრუმენტების ლიკვიდურობას ზღუდავს, მაგრამ სამაგიეროდ მნიშვნელოვნად აჩქარებს ბირჟის მუშაობის საერთო პროცესს.

დეცენტრალიზებული ბირჟების აშკარა უპირატესობაა ცენტრალიზებული ხელმძღვანელი სუბიექტის არარსებობა, რომელსაც შეუძლია ვაჭრობის პროცესების გაკონტროლება, მასში ჩარევა ან ფასობრივი მანიპულაციების ჩატარების ცდა. დეცენტრალიზაცია ჰაკერებისთვის ქმნის გადაულახავ ბარიერს აქტივების საერთო საცავში არასანქცირებული შეღწევის მცდელობისას, რადგან ასეთი საერთოდ არ არსებობს. ყველა აქტივი ინახება ქსელის წევრთა კომპიუტერებში მათივე კონტროლის ქვეშ, ხოლო წევრები ამავდროულად ანონიმურები არიან, რადგან მსგავს გარემოში არ ხდება მათი იდენტიფიკაცია იმის გამო, რომ ამის გამკეთებელი არსად და არავინაა.

და ბოლოს, ასეთი ბირჟები პრაქტიკულად უვნებელია რეგულაციური ზემოქმედებისათვის, მათი მუშაობის შეჩერება რაღაც ადმინისტრაციული მითითებით, ასევე, ტრეიდერთა ანგარიშების გაყინვა ან კონფისკაცია უბრალოდ შეუძლებელია. თეორიულად შესაძლებელია საბირჟო ქსელის ერთი ან რამდენიმე კვანძის მწყობრიდან გა-

მოყვანა, მაგრამ მთელი ქსელის მიმართ ამის გაკეთება განსაკუთრებით რთულია. მიუხედავად ამისა, დეცენტრალიზებულ ბირჟებსაც სჭირდება მინიმალური მართვა, თუნდაც იმისათვის, რომ შევიმუშაოთ და გავააქტიუროთ ვაჭრობების ჩატარების ზოგადი წესები, და ასევე, ჩავატაროთ სავაჭრო ინსტრუმენტების ლისტინგი. როგორც წესი, ეს ამოცანები ხორციელდება არჩევითი კომიტეტების საშუალებით, თუმცა მათი ფორმირების პროცესი ხშირად გაუმჭვირვალეა და ზოგ შემთხვევაში შედეგად ყალიბდება მმართველი ორგანო, რომელიც მთლიანად საბირჟო სისტემის შემმუშავებელთა სტრუქტურასთანაა დაკავშირებული. ძნელი მისახვედრი არ არის, რომ ასეთი მიდგომა ფაქტობრივად ცენტრალიზებულს ხდის ბირჟის მუშაობას, რითაც ზიანს აყენებს სავაჭრო სისტემის განაწილებული არქიტექტურის საფუძველზე შექმნის თვით იდეასაც კი.

სწორედ ამ მიზეზით, დეცენტრალიზებული ბირჟები ჯერჯერობით სათანადოდ ვერ გავრცელდა მათ პროექტირებასთან დაკავშირებული რიგი სირთულეების, პირველ რიგში, ერთმანეთთან არათავსებადი სხვადასხვა ბლოკჩეინ-ქსელის აქტივების გაცვლის ტექნოლოგიური არასრულყოფილების გამო. საქმე ისაა, რომ ბლოკჩეინ-გარემოში ყველა ტრანზაქცია გამოუწვევადია და ძალზე მნიშვნელოვანია, ორივე მხარის ქმედება ისე შევუწყოთ ერთმანეთს, რომ არც ერთ კონტრაგენტს აქტივების მიღების შემდეგ არ გაუჩნდეს სურვილი უარი თქვას ვალდებულებათა თავის ნაწილზე. რადგან მუდმივად კონტრაგენტების კეთილ ნებაზე იმედად ყოფნა განაწილებულ სისტემებში არ ეგების, აუცილებელია, ან საშუამავლო ელემენტები – როგორიცაა პირობითი დეპონირების სერვისები – გამოვიყენოთ, ან ისეთი მეთოდები გამოვიგონოთ, რომლებიც გარიგების ვალდებულებების შესრულების გარანტიას მოგვცემს.

ამ ამოცანის გადასაჭრელად შემუშავებული იქნა ე.წ. „ატომური სვოპების“ კონცეფცია. სიტყვა „ატომი“ ბერძნულად განუყოფელს ნიშნავს, თუმცა მეცნიერებმა თვით ეს ფაქტი დიდი ხანია უარყვეს. მიუხედავად ამისა, ტერმინი, როგორც იტყვიან, დამკვიდრდა და ბლოკჩეინ-ტექნოლოგიაშიც გამოიყენება იმის საჩვენებლად, რომ დეცენტრალიზებულ გარიგებაში ვალდებულებები ორივე მხარის მიერ გარანტირებულად უნდა შესრულდეს განურჩევლად იმისა, არსებობს თუ არა მათ შორის ნდობა. ატომური სვოპის მუშაობის პრინციპი გულისხმობს,

რომ გარიგება ორივე კონტრაგენტის მიერ ან სრული მოცულობით იქნება შესრულებული, ან გაუქმებული იქნება, აქტივების გაცვლა-გამოცვლის პროცესის ყველა მონაწილისათვის ფინანსური ზარალის გარეშე. ატომური სვოპების უშუალო ტექნოლოგიური რეალიზაცია დამოკიდებულია იმ კონკრეტულ ბლოკჩეინ-გარემოთა თავისებურებებზე, რომელთა შიგნით ან რომელთა შორისაც გარიგებები ხდება.

პირველი ატომური სვოპი 2017 წლის 20 სექტემბერს, Decred და Litecoin ბლოკჩეინებს შორის განხორციელდა. დეტალებს განსაკუთრებით ნუ ჩავუღრმავდებით და მხოლოდ აღვნიშნოთ, რომ მსგავსმა გარიგებებმა მოითხოვა ძირითად ქსელებზე დამატებითი ზედნაშენები, რამაც, რა თქმა უნდა, გაცვლის პროცესები გაართულა. ამის შემდეგ ბლოკჩეინ-ტექნოლოგთა ბევრი გუნდი ატომური სვოპების კონცეფციის სრულყოფაზე მუშაობს, რათა უახლოეს მომავალში, განაწილებული არქიტექტურის მქონე ბირჟებმა მაინც მიიღონ მნიშვნელოვანი უპირატესობები თავიანთ ცენტრალიზებულ კონკურენტებთან შედარებით.

დავუბრუნდეთ იმას, თუ კერძოდ რისთვის შეიქმნა კრიპტოვალუტური ბირჟები, და ყურადღება გავამახვილიოთ ამ სერვისის მომხმარებელთა ორ ძირითად კატეგორიაზე: პირველია პოზიციური მომხმარებლები, რომლებიც კრიპტოვალუტებს ყიდულობენ ხანგრძლივი პერიოდით შესანახად, რათა მათი ზრდით მოგება მიიღონ; მეორეა სპეკულანტი ტრეიდერები, რომლებიც ინვესტიციებს ახორციელებენ მოკლევადიან ან საშუალოვადიან საფუძველზე, რათა სცადონ, მოგება მიიღონ გარკვეული კრიპტოვალუტების ღირებულების როგორც ზრდით, ასევე დაცემითაც. სპეკულაციური ვაჭრობის პრინციპებსა და მიდგომებში გასარკვევად, კრიპტოვალუტური ინსტრუმენტების ფასთა მოძრაობის ფინანსურ ანალიზს უნდა მივმართოთ.

კრიპტოვალუტური ბაზრის ანალიზი

მთელი ფინანსური ისტორიის განმავლობაში, პირველი სავაჭრო მოედნების შექმნიდან დღემდე, ბირჟის ტრეიდერები ყოველთვის ცდილობდნენ, როგორღაც ეწინასწარმეტყველათ სავაჭრო აქტივების ფასების მოძრაობა. შუა საუკუნეებიდან მოყოლებული, XX საუკუნის დასაწყისამდე ამ მიზნებისათვის იყენებდნენ ილეთების ფართო სპექტრს, ასტროლოგიური და რელიგიური პრაქტიკებით დაწყებული და იმ მეთოდებით დამთავრებული, რომლებიც მეცნიერულთან მიახლოებულადაც კი შეიძლება ჩაითვალოს. რა თქმა უნდა, ინვესტიციური გადაწყვეტილებების მიღებისას მთავარ როლს თამაშობდა ყველანაირი გზით მოპოვებული ინსაიდერული ინფორმაცია. ღია ინფორმაციის მიღების სიჩქარეც ასევე მნიშვნელოვან როლს ასრულებდა. მაგალითად, ვატერლოოს ბრძოლის შემდეგ, 1815 წლის ივნისში როტშილდების ოჯახმა პირველმა მიიღო ცნობა იმპერატორ ნაპოლეონის არმიაზე ბრიტანული არმიის გამარჯვების შესახებ. ამან როტშილდების ბანკს საშუალება მისცა, თავიდან საფუძვლიანად დაეგდო ფასები დიდი ბრიტანეთის მთავრობის აქციებზე და შემდეგ, იმავე სავაჭრო დღის განმავლობაში უკვე ბევრად დაბალ ფასად შეეძინა ეს აქციები.

თუმცა, მსგავსი შემთხვევები უფრო გამონაკლისი იყო, ვიდრე წესი, ამიტომ ჩვეულებრივ სავაჭრო პრაქტიკაში გაჩნდა მცდელობები, შეეგროვებინათ და დაემუშავებინათ ამა თუ იმ ფასიანი ქაღალდების ემიტენტებთან დაკავშირებული ინფორმაცია, რათა მიეღოთ აწონილ-დაწონილი გადაწყვეტილებები მათ შესაძენად ან გასაყიდად. საბოლოოდ ეს პროცესები ჩამოყალიბდა ფასთა პროგნოზირების სხვადასხვა მოდელად, რომლებმაც ფინანსური ბაზრების ანალიზის ცნება წარმოშვა. თანამედროვე ფინანსურ სამყაროში ფართოდ გამოიყენება საბაზრო ანალიზის ორი ძირითადი სახეობა: ფუნდამენტური და ტექნიკური. პირველი განეკუთვნება ფასიანი ქაღალდების ემიტენტი კომპანიების საწარმოო და სავაჭრო მაჩვენებლების ფინანსური ანალიზის საფუძველზე პროგნოზირების მეთოდებს.

მაგალითად, თუ საუბარია ეროვნულ ვალუტაზე, მაშინ განიხილება ამ ვალუტის გამომშვები ქვეყნის მაკროეკონომიკური მაჩვენებლები. ფუნდამენტური ანალიზის ასევე მნიშვნელოვან მაჩვენებლებს მიეკუთვნება ფინანსური ინსტრუმენტის ემიტენტთან – კომპანიასა თუ ქვეყანასთან დაკავშირებული მნიშვნელოვანი ახალი ამბები. ანალიზის მეორე, ტექნიკურ მეთოდს საფუძვლად აქვს სუფთა ფსიქოლოგიური საფუძველი, ეყრდნობა სავაჭრო ინსტრუმენტების ციფრული გრაფიკების ანალიზს და ასევე, მათზე სხვადასხვა მათემატიკური ალგორითმის გამოყენებას, ფასთა მოძრაობის კანონზომიერების დასადგენად. განვიხილოთ ორივე სახის ანალიზი.

ითვლება, რომ ფუნდამენტური ანალიზის წარმოქმნა დაკავშირებულია თითქმის ასი წლის წინ მომხდარ მოვლენასთან, როდესაც 1934 წელს გამოქვეყნდა წიგნი „ფასიანი ქაღალდების ანალიზი“, რომლის ავტორებიც იყვნენ ამერიკელი ეკონომისტები – ბენჯამინ გრემი და დევიდ დოდი. თავიანთ წიგნში ისინი შეეცადნენ შემოეთავაზებინათ სისტემური მიდგომა ფასიანი ქაღალდების ანალიზისადმი მათი რეალური ღირებულების განსაზღვრის მიზნით მიმდინარე საბაზროსთან მიმართებაში. ასეთი ანალიზის შედეგად შესაძლებელი ხდებოდა გამოგვევლინა განსახილველი საბირჟო ქაღალდების ან შეუფასებლობა, ანდა აშკარა გადაფასება, რათა შემდეგ მათ მიმართ შესაბამისი სავაჭრო გადაწყვეტილება მიგვეღო. შედეგად ფუნდამენტური ანალიზის პრონციპები აქტიურად განვითარდა, რითაც მნიშვნელოვნად გააფართოვა გასაანალიზებელ ფაქტორთა სპექტრი, რომლებიც ამა თუ იმ დოზით ახდენს გავლენას ფასების საბაზრო მოძრაობაზე. რომელიღაც მომენტში ეს ფაქტორები იმდენად მომრავლდა, რომ ამგვარი ანალიტიკური მეთოდების კრიტიკოსებმა საუბარი დაიწყეს ფასებზე მოქმედი აბსოლუტურად ყველა მოვლენის გათვალისწინების შეუძლებლობაზე, რადგან მათ უმრავლესობას ძნელად საწინასწარმეტყველო ანდა საერთოდაც შემთხვევითი ხასიათი ჰქონდა.

ეროვნული ვალუტების მოძრაობის პროგნოზირებისთვის ფუნდამენტური ანალიზის გამოყენების ტიპური მაგალითია ისეთი მაკროეკონომიკური პარამეტრების განხილვა, როგორებიცაა ინფლაცია, უმუშევრობა ან ცენტრალური ბანკების საპროცენტო განაკვეთე-

ბი. როგორც წესი, ერთ-ერთი ამ მაჩვენებლის ცვლილება იწვევს ეროვნული ვალუტის მნიშვნელოვან ფასობრივ ცვლილებებს გამყარების მიმართულებით, თუ ეს პარამეტრები ეკონომიკურად ხელსაყრელია, ანდა შესუსტების მიმართულებით, საწინააღმდეგო შემთხვევებში. ხშირად, ჭორებსა და ვარაუდებზე დაყრდნობით, ბაზრებს ფუნდამენტური სიახლის გამოჩენისას უკვე შეუძლია მისი შესაბამისი მოძრაობის ამოწურვა და უკუკორექციის მოხდენაც, თუკი მოვლენის მოლოდინის ეფექტი რამდენადმე გადაჭარბებული აღმოჩნდება.

თავისი ფუნდამენტური „კოლეგისაგან“ განსხვავებით, ტექნიკური ანალიზი ეყრდნობა უკვე მომხდარ მოვლენებს ანუ – ისტორიულ კოტირებებს, რომელთაგან დგება ფასთა მოძრაობის გრაფიკები დროის სხვადასხვა პერიოდებისათვის. შემდეგ, ამ გრაფიკების კვლევით, ტექნიკურ-ფინანსური ანალიტიკოსები ცდილობენ გამოავლინონ ფასობრივი პატერნები ანუ სავაჭრო აქტივზე ფასის მოძრაობის შედარებით მდგრადი კანონზომიერებები. ამ პროგნოზირებისათვის საჭირო საფუძველს წარმოადგენს ვარაუდი, რომ ტრეიდერების ფსიქოლოგია ბაზრის ყველა მონაწილისათვის ერთნაირად ამუშავდება, რადგან მათი უმრავლესობა ტექნიკური ანალიზის ერთი და იმავე მეთოდებით ხელმძღვანელობს.

მიუხედავად იმისა, რომ ტექნიკური ანალიზის მთავარი ინსტრუმენტი ფასების კოტირების გრაფიკია, რომლის აგებაც კომპიუტერების გარეშე რუტინული ხასიათის სერიოზულ ხელით შრომას საჭიროებს, ანალიზის ეს სახეობა ფუნდამენტურ ანალიზზე ორი ასეული წლით უფროსი მაინცაა. ის ჩაისახა XVIII საუკუნეში იაპონიაში, ტოკიოში ბრინჯით ვაჭრობის სასაქონლო ბირჟის შექმნის შემდეგ. დაახლოებით 1750 წელს ტრეიდერებმა დაიწყეს ფასების მოძრაობის ასახვა სპეციალური ნახატებით, რომლებსაც შემდგომში „იაპონური სანთლები“ უწოდეს. ასეთი სანთელი წარმოადგენს გრაფიკულ კონსტრუქციას, რომელიც ყველაზე მნიშვნელოვან ფასობრივ დონეებს ასახავს დროის გარკვეული ინტერვალის განმავლობაში. საუბარია ფასებზე პერიოდის დასაწყისსა და ბოლოში, ასევე, ფასის ლოკალურ მაქსიმუმსა და მინიმუმზე დროის ამ მონაკვეთის ფარგლებში. ამასთან, თუ სანთელი ასახავს აღმავალ ბაზარს, მაშინ სანთლის სხეული „ღრუა“, ხოლო თუ დაღმავალს – მაშინ შეღებილი.

ხარის სანთელი დათვის სანთელი

იაპონელმა ბრინჯით მოვაჭრეებმა ასეთი სანთლების შექმნას ყოველი სავაჭრო დღის ბოლოს მიჰყვეს ხელი, შემდეგ კი, საკმარისი სტატისტიკის დაგროვებისას, დაიწყეს ფასის მოძრაობის კანონზომიერების შესწავლა, მიღებული სანთლოვანი ფიგურების შეხამებიდან გამომდინარე. კომბინაციებმა მიიღო საკუთარი უნიკალური სახელები, ხოლო შემდეგ მათ გარკვეული სახით ხსნიდნენ და საბაზრო მოძრაობებს წინასწარმეტყველებდნენ. შემდგომში ამ ახსნებმა შეადგინა სქელტანიანი მანუსკრიპტები, რომლებიც აღწერდა სანთლის ფიგურების ყველა შესაძლო კომბინაციასა და მათთან დაკავშირებული ფასობრივი დინამიკის პროგნოზებს.

კომპიუტერული ტექნიკის გამოჩენასა და განვითარებასთან ერთად, ტექნიკური ანალიზი ხელახლა დაიბადა. ახლა გრაფიკების შედგენა გამომთვლელი მანქანებისათვის შეიძლებოდა მიგვენდო და გაგვეზარდა როგორც დროის პერიოდი, ასევე ანალიზისათვის საჭირო შესაძლო გრაფიკული ელემენტების რაოდენობა. თავიდან იყენებდნენ ალფაბეტურ-ციფრულ დისპლეებს, ხოლო შემდეგ – გრაფიკულ დისპლეებსაც. ანალიტიკოსებმა ისტორიული კოტირებების მასივებს მიუყენეს სხვადასხვა ტექნიკური ინდიკატორის მქონე მათემატიკური ალგორითმები.

ფასების ანალიზმა შედარებით ფართო დროით დიაპოზონებში საშუალება მოგვცა გამოგვევლინა ე.წ. „ტრენდები“ ანუ ფასის მოძრაობის აშკარა ტენდენციები. ფასების ცვლის გრაფიკული გამოსახულებების კომბინატორიკამ ძველებურ იაპონურ გრაფიკულ ანალიზს საშუალება მისცა, ხელახლა დაბადებულიყო, ოღონდ – თანა-

მედროვე ინტერპრეტაციით. ტექნიკურ ანალიტიკაში გაიელვა ტერმინებმა – „თავი და მხრები“, „ორმაგი და სამმაგი მწვერვალები“, „სამკუთხედები“ და „რომბები“ – როგორც ტრენდული მოძრაობების გაგრძელების ან ცვლილების გრაფიკულმა ფიგურებმა.

რა თქმა უნდა, ტექნიკურ ანალიზს გამოუჩნდნენ კრიტიკოსები, რომლებიც არცთუ უსაფუძვლოდ თვლიდნენ, რომ ფასების ისტორიის კვლევას ცოტა რამ აქვს საერთო ფასების მომავალთან. ასევე ითქვა, რომ შედარებით მნიშვნელოვანი ყველა ფუნდამენტური სიახლე ისტორიულობის ანუ ფასების გრაფიკზე ასახული პროცესების რეაქციულობის ძალით უეჭველად დაანგრევს ადრე გამოთქმულ ყველა პროგნოზს. მიუხედავად ამისა, როგორც ფუნდამენტურ, ასევე ტექნიკურ ანალიზსაც ჰყავს უამრავი მიმდევარი, რომლებიც უმრავლეს შემთხვევაში, ერთდროულად იყენებენ ორივე ანალიტიკურ მიმართულებას, რადგან თვლიან, რომ ერთი ყოველთვის ავსებს მეორეს. ფინანსურ სამყაროში ყოველდღიურად ჩნდება მრავალი ანალიტიკური სტატია და პროგნოზი ბაზრებზე კოტირებულ ყველა ფინანსურ ინსტრუმენტთან დაკავშირებით.

კრიპტოვალუტებიც არ აღმოჩნდა გამონაკლისი. მაგრამ მოდი ვიმსჯელოთ, ანალიზის რა სახეობები და რატომ შეიძლება მივუყენოთ ფინანსური აქტივების მოცემულ ტიპს. დავიწყოთ იმით, რომ ფუნდამენტური ანალიზის უდიდესი ნაწილი კრიპტოვალუტებს სუსტად ეთანადება ცენტრალიზებული ემიტენტის არარსებობის და, როგორც შედეგი, მისი ეკონომიკური ანალიზის შეუძლებლობის

გამო. პირველ რიგში ეს ეხება დეცენტრალიზებული კონკურენტული მაინინგის საფუძველზე აგებულ კრიპტოვალუტებს, როგორებიცაა ბიტკოინი, ეთერი და მათი მსგავსი სხვა. ეს კი ნიშნავს, რომ სხვადასხვა ქვეყნის ან გაერთიანების (მაგალითად, ევროკავშირის) ვერც ერთი სუვერენული მაკროეკონომიკური მაჩვენებელი პირდაპირ გავლენას ვერ მოახდენს დეცენტრალიზებული კრიპტოაქტივების ღირებულებაზე. სამართლიანობისათვის უნდა ვაღიაროთ, რომ კრიპტოვალუტების ღირებულებაზე ირიბი გავლენა მაინც იქნება, მაგრამ – მხოლოდ მაკროეკონომიკური ინდიკატორის იმ ფიატურ ვალუტაზე ზემოქმედების ნაწილში, რომელზეც უშუალოდ ვაჭრობენ საკუთრივ კრიპტოაქტივით. თუმცა, ამჟამად ეს გავლენა უმნიშვნელოა და კრიპტოვალუტების ფასთა მოძრაობის ანალიზში ის თამამად შეგვიძლია არ გავითვალისწინოთ.

მიუხედავად ამისა, ფუნდამენტური სიახლეები კრიპტოვალუტებისათვის არსებობს და მათ დიდი გავლენა შეუძლია მოახდინოს ვალუტის ღირებულებაზე. სხვა საქმეა, რომ ეს სიახლეები უმრავლეს შემთხვევაში ერთჯერად ეფექტს ახდენს, რადგან ხშირად დაკავშირებულია ეროვნული მთავრობების გადაწყვეტილებასთან კრიპტოვალუტების ან შეზღუდვასთან, ან აკრძალვასთან. უფრო მეტიც, არსებობს ძალზე ცოტა ქვეყანა, საიდანაც სიახლეებს შეუძლია სერიოზული გავლენა მოახდინოს კრიპტოვალუტის კოტირებაზე. პირველ რიგში, ესენია – ჩინეთი, აშშ, სამხრეთ კორეა და იაპონია ანუ ქვეყნები, სადაც თავმოყრილია შესაბამის ბირჟებზე კრიპტოვალუტებით ვაჭრობის ყველაზე დიდი მოცულობა.

იმ შემთხვევაში, თუ კრიპტოაქტივს უშვებენ ცენტრალიზებულად და, რაც ძალზე მნიშვნელოვანია, ის არა უტილიტარული, არამედ საინვესტიციო ტოკენია, ფუნდამენტური ანალიზი გარკვეულწილად გამოყენებადია მმართველი კომპანია-ემიტენტის მაჩვენებლების შესაფასებლადაც. აქ კლასიკური შეფასება ნაკლებად შესაძლებელია იმიტომ, რომ მმართველი კომპანია უმრავლეს შემთხვევაში წარმოადგენს ახლახან შექმნილ სტარტაპს, რომელსაც, როგორც წესი, ჯერ კიდევ არ დაუწყია პროექტიდან მონეტარული მოგების მიღება. ამიტომ ანალიზში ყურადღება უნდა გამახვილდეს სტარტაპებისათვის დამახასიათებელ ისეთ ტიპურ პარამეტრებზე, როგორიცაა: პროექტის შემმუშავებელი გუნდის წევრების გამოცდილება,

რეალიზაციისათვის შემოთავაზებული სტრატეგია, პროდუქტის აქტუალობა და მისი საბაზრო პოზიციონირება, მოზიდული საინვესტიციო სახსრების მოცულობა, MVP-ის არსებობა და ა.შ.

კრიპტოვალუტების მიმართ უფრო ეფექტიანად გამოყურება ტექნიკური ანალიზი, რადგან ის, როგორც უკვე აღვნიშნეთ, ბაზრის წევრების ფსიქოლოგიიდან გამომდინარეობს. ეს კი ნიშნავს, რომ კრიპტოტრეიდერების ქცევითი ნიმუშები დიდად არ განსხვავდება ისეთებისგან, რომლის ხილვასაც კლასიკურ ბაზრებზე შევეჩვიეთ. ბევრი ტექნიკური ანალიტიკოსი არ უარყოფს სხვადასხვა ინდიკატორის ქმედითობას, პირველ რიგში – გრაფიკულისას; საუბარია როგორც ტრენდულ ხაზებზე, ასევე სპეციალურ ფიგურებზეც, რომლებიც ტრენდულ სიგნალებს იძლევა. არცთუ უმნიშვნელო როლს თამაშობს ძლიერი ფასობრივი ფსიქოლოგიური დონეები, რომლებიც „ლამაზი“ მნიშვნელობებით გამოირჩევა – 1, 10, 100, 1000 და ა.შ.

როგორც აღვნიშნეთ, ტექნიკური ანალიზი ისტორიულად წინ უსწრებდა ფუნდამენტურს, რადგანაც მისი პრინციპები ეფუძნება კონკრეტულ მოედნებზე ვაჭრობების შესახებ ადვილად შესაგროვებელ მონაცემებს და დროის თვალსაზრისით „უკანაა“ მიმართული. სახელმწიფოთა ემიტენტებზე ან მაკროეკონომიკურ მაჩვენებლებზე ინფორმაციის შეგროვებისა და მოწესრიგებისდა გვარად, ტექნიკურ ანალიზს მაშველად ფუნდამენტური ევლინება. ამ ასპექტებში კრიპტოფინანსები ბევრი რამით იმეორებს ფიატური სავაჭრო ინსტრუმენტების გზას.

დაბოლოს, გვინდა რამდენიმე სიტყვა ვთქვათ სავაჭრო სტრატეგიებზე, რომლებსაც ტრეიდერები კრიპტოვალუტურ ბაზრებზე იყენებენ. ისევე, როგორც კლასიკურ ფინანსურ ბაზრებზე, გლობალურად შეგვიძლია გამოვყოთ ორი სტრატეგიული მიდგომა: სპეკულაციური და პოზიციური. პირველი არის მოკლევადიანი, დღის განმავლობაში ვაჭრობისათვის განკუთვნილი, როდესაც ტრეიდერის მიერ პოზიციები იხსნება და იხურება ერთი დღის განმავლობაში, პოზიციის შენარჩუნებამდე რამდენიმე დღით ან მაქსიმუმ ერთი კვირით. ასეთი სტრატეგია გულისხმობს, რომ სავაჭრო კრიპტოვალუტას აქვს საკმაოდ კარგი ვოლატილობა ანუ კოტირების შესაძლო რხევის მაღალი ამპლიტუდები და შესაძლებელია მოგების მიღება, საჭირო ფასობრივი ამოტყორცნის სწორად „დაჭერით“.

მეორე, საინვესტიციო მიდგომა, აისხნება buy and hold პრინციპით ანუ – „ვიყიდო და შევინახო“. ასეთი სავაჭრო პოზიციების შენარჩუნება ინვესტორებს შეუძლიათ თვეობით და წლობითაც კი, ფასების მნიშვნელოვანი ზრდის იმედით. თუმცა, ისეც ხდება, რომ პოზიციის შენარჩუნებისას კრიპტოაქტივმა შეიძლება როგორც ისტორიულ პიკებს მიაღწიოს, ასევე თავისი ღირებულების უპრეცედენტო ვარდნაც განიცადოს. კრიპტოვალუტური პორტფელების ხანგრძლივ შემნახველებს სლენგზე „ჰოდლერებს“ უწოდებენ, დამახინჯებული ინგლისური სიტყვიდან hodl (hold – ინგლისურსდ „დაჭერა“, „შენარჩუნება“). კრიპტოგარემოში პოპულარული ეს სიტყვა პოპულარული Bitcointalk-ის ფორუმის ერთ-ერთმა მომხმარებელმა 2013 წლის დეკემბერში შემოიღო. ალკოჰოლური თრობის მდგომარეობაში მყოფმა (რაშიც შემდგომ თავად გამოტყდა), მან შეცდომა დაუშვა და დაწერა I am hodling, ჰოდა, ეს ფრაზა ფორუმის სხვა მონაწილეებმა აიტაცეს. შემდგომში ტერმინი ფართოდ გავრცელდა კონსერვატული საინვესტიციო ქცევის აღსანიშნავად, რომელიც ხანგრძლივი პერიოდის განმავლობაში აღმავალ ფასობრივ ტრენდზეა გათვლილი.

კრიპტოვალუტებში ინვესტიციებისადმი მიძღვნილი თავის დასასრულს გვინდა, თქვენი ყურადღება გავამახვილოთ ერთ მნიშვნელოვან პრობლემაზე, რომელსაც მრავალი ინვესტორი აწყდება, განსაკუთრებით ისეთებზე, რომელთა ახსნაც სიტყვა „ჰოდლერით“ შეიძლება. საუბარია შეძენილი კრიპტოვალუტების ხანგრძლივ შენახვაზე შედარებით არასტაბილური გარემოს შემთხვევაში, რომელშიც კრიპტოაქტივები ბრუნავს. უნდა აღვნიშნოთ მთელი რიგი ფაქტორებისა: კრიპტოსაფულეების კოდში ტექნიკური სისუსტეებიც, ჰაკერული თავდასხმებიც, კრიპტობირჟების გაკოტრებებიც. უსაფრთხოების საკითხებისა და რისკების მართვის საკითხებისადმი არასათანადო ყურადღება ინვესტორისათვის სამწუხარო შედეგებს იწვევს. ამ რისკების მართვის თემას ეთმობა შემდეგი თავი.

კრიპტოაქტივების შენახვა

ბიტკოინის როგორც ინვესტიციისადმი მიძღვნილ თავში გადმოცემული იყო ნორვეგიელი სტუდენტის შემთხვევა, რომელმაც კრიპტოგრაფიის თემაზე დიპლომზე მუშაობისას სიმბოლურ ფასად, გასატესტად იყიდა რამდენიმე ათასი ბიტკოინი. წლობით დავიწყებული შენაძენის შესახებ მაშინ გაახსენდა, როცა მის ხელთ არსებული კრიპტოაქტივების ფასი „ცაში აიჭრა“. მას საკმაო ძალებისა და დროის დახარჯვა დასჭირდა, რათა აღედგინა წვდომა საკუთარ ბიტკოინ-საფულესთან. ისტორია კეთილად დასრულდა, რადგან ყოფილმა სტუდენტმა მაინც შეძლო თავისი ბიტკოინ-საფულის კოდის აღდგენა და სრულად ისარგებლა მოულოდნელად მოპოვებული სიმდიდრით.

თუმცა ყველა ისტორია ასე კარგად როდი მთავრდება. კრიპტომონეტების მფლობელები ხშირად, სხვადასხვაგვარად კარგავდნენ თავიანთი საფულეების საიდუმლო გასაღებს. დაკარგვის ყველაზე გავრცელებული ვარიანტი იყო კომპიუტერული მოწყობილობის მწყობრიდან ბანალური გამოსვლა, პირველ რიგში – მყარი დისკებისა, რომლებზეც ძვირფასი მონაცემები ინახებოდა. ციფრული მონეტების უსაფრთხო შენახვის პრობლემის გადაჭრა ახალგაზრდა კრიპტოსაზოგადოებაში ერთ-ერთი ყველაზე მოთხოვნადი გახდა, ამიტომაც ინდუსტრიამ მასზე რეაგირება არ დააყოვნა. ეს გამოიხატა სხვადასხვა პროექტის გეგმურ შექმნაში, რომლებიც საშუალებას იძლევა, სხვადასხვა ხარისხის წარმატებით გადაიჭრას კრიპტოაქტივების საიმედოდ შენახვის ამოცანა, რომელთა ღირებულებაც ყოველდღიურად იზრდება. ვცადოთ გავერკვეთ კრიპტოვალუტების შენახვის მრავალფეროვან მეთოდებში, რომლებიც მომხმარებლებისათვის ამჟამად ხელმისაწვდომია.

ისევე როგორც ჩვეულებრივი ფიატური ფული, კრიპტოვალუტებიც სპეციალურ საფულეებში ინახება. გლობალურად გვაქვს კრიპტოსაფულეების ორი ტიპი: ე.წ. „ცხელი“ და „ცივი“. ცხელი საფულეები განლაგებულია ინტერნეტში ჩართულ მომხმარებელთა მოწყობილობებზე ან წარმოადგენს ცენტრალიზებულ ინტერნეტსერვისებს, რომლებიც შეიძლება კრიპტობირჟებიც კი იყოს. ცხელ საფულეებში შენახული კრიპტოვალუტური სახსრები ნებისმიერ მომენტში ხელმი-

საწვდომია ტრანზაქციების განსახორციელებლად, სხვა სიტყვებით რომ ვქთვათ – დასახარჯად. ცივს კი უწოდებენ საფულეებს, რომლებიც მუდმივადაა დაკავშირებული სატელეკომუნიკაციო სამყაროსთან და რაღაცით სეიფს გვაგონებს: სანამ მასში შენახულ კრიპტოაქტივებს დავხარჯავთ, მანამდე აუცილებელია რიგი პროცედურების ჩატარება, რათა ისინი საცავიდან ამოვიღოთ.

ცხელი საფულეები იყოფა ისეთებად, რომლებსაც მომხმარებლები დამოუკიდებლად აკონტროლებენ, და ისეთებად, რომელთა მართვისა და კონტროლის ფუნქციებიც დელეგირებულია მესამე მხარეების ანუ ცენტრალიზებული სერვისებისათვის. როგორც ცნობილია, კრიპტოსახსრების ფლობის უფლებას უზრუნველყოფს კონტროლი იმ ანგარიშების შესაბამის პრივატულ გასაღებებზე, რომლებზეც ისინი არის მიბმული. ამიტომ თითოეული მომხმარებელი თავად წყვეტს: საკუთარ თავზე აიღებს თავისი პრივატული გასაღების დამოუკიდებლად შენახვის შრომასა და რისკს და უზრუნველყოფს მისი შენახვის უსაფრთხოებას, თუ ამ ფუნქციებს მიანდობს ერთ-ერთ პოპულარულ ინტერნეტ-სერვისს, რომელიც სხვადასხვა კრიპტოვალუტისათვის საფულეთა ფუნქციონალს გვთავაზობს. პირველი მეთოდი გულისხმობს, რომ მომხმარებელი უნდა გახდეს შესაბამისი ბლოკჩეინ-სისტემის კვანძი. ეს ნიშნავს, რომ მას მოუხდება, საკუთარ მოწყობილობაზე მთლიანად ან ნაწილობრივ ჩატვირთოს ბლოკების მონაცემთა ბაზა, რომლებზეც მიბმულია მისი კრიპტოსახსრები. ჩვეულებრივ, ამისათვის საჭიროა, მონაცემთა შენახვის ლოკალურ მოწყობილობაზე გამოიყოს მნიშვნელოვანი ადგილი და მუდმივად ხდებოდეს ამ ბლოკების გადატვირთვა-განახლება, რაც გარკვეულ დროს შეიძლება მოითხოვდეს.

კრიპტოსახსრების შენახვის მეთოდის სისუსტე ისაა, რომ მომხმარებლის ინტერნეტში ჩართული მოწყობილობა შეიძლება გახდეს ჰაკერული თავდასხმის ობიექტი პრივატული გასაღების მოპარვის მიზნით. გარდა ამისა, არსებობს უამრავი კომპიუტერული ვირუსი, ე.წ. „ტროას ცხენები“, რომლებსაც შეუძლია მომხმარებლის კომპიუტერში ჩატვირთოს სხვადასხვა ბლოკჩეინ-გარემოს პრივატული გასაღებების საძიებელი სპეციალური კოდი და გადაუგზავნოს ის ვირუსის შემმუშავებელს, ბლოკჩეინ-მისამართის პრივატული გასაღების ფლობა კი მასზე არსებულ კრიპტომონეტებზე სრული კონტროლის მიღების ტოლფასია. უსაფრთხოებისათვის საფრთხის შემცველი მთელი თაიგულის არსებობა პრივატული გასაღებების ინფრასტრუქტუ-

რის დამოუკიდებლად მხარდაჭერისას აიძულებს ტექნიკაში ცუდად გარკვეულ ბევრ მომხმარებელს, თავისი კრიპტოდანაზოგები პროფესიონალებს მიანდოს. საუბარია სერვისებზე, რომლებიც სხვადასხვა კრიპტოვალუტის შენახვის ცენტრალიზებულ გადაჭრას გვთავაზობს.

ეჭვგარეშეა, რომ საკუთარი კრიპტოსახსრების სრული კონტროლის არარსებობამ შეიძლება გამოიწვიოს მფლობელთა შფოთვა მათ შენახვასთან დაკავშირებით. თავისთავად გამოდის, რომ კრიპტოვალუტების შენახვის ყველა პოპულარული ცენტრალიზებული პროექტი დიდ ყურადღებას უთმობს გატეხის საწინააღმდეგო დაცვას, ამისათვის შტატში ჰყავს კომპიუტერული უსაფრთხოების კვალიფიციური სპეციალისტები. მიუხედავად ამისა, მსგავსი სერვისები ჰაკერული თავდასხმების მეტი რისკის ქვეშაა, ვიდრე კრიპტოვალუტების კერძო მფლობელები. ტექნოლოგიურ საფრთხეებს ემატება სხვა სახის რისკებიც, რომლებიც დაკავშირებულია კომპანიის პროექტების მფლობელების ან მმართველი თანამშრომლების მხრიდან შესაძლო დანაშაულის ჩადენასთან. ბირჟა Mt. Gox-ის ბიტკოინების გაქრობასთან დაკავშირებული ისტორია ჯერ კიდევ ბევრს ახსოვს, ეს კი სულაც არ არის ერთადერთი შემთხვევა, როდესაც ცენტრალიზებული სერვისების მომხმარებელი ამა თუ იმ მიზეზით, თავის კრიპტოაქტივებს კარგავს.

კრიპტოვალუტების შენახვის ცენტრალიზებული სერვისების მომხმარებლისათვის რისკების მართვა უნდა გამოიხატებოდეს პირველ რიგში, თვით მოედნის არჩევისადმი აწონილ მიდგომაში. აუცილებელია ისეთი ფაქტორების გათვალისწინება, როგორებიცაა: კომპანიის არსებობის ხანგრძლივობა, მისი ისტორია და რეპუტაცია, აგრეთვე, კრიპტოაქტივების მოპარვისა და უსაფრთხოების სისტემის გატეხის პრეცედენტების არარსებობა. რეგისტრაციის იურისდიქცია და ლიცენზიის არსებობა, უკიდურეს შემთხვევაში, ნიშნავს, რომ კომპანიის საქმიანობა რეგულატორული ზედამხედველობის ქვეშაა, რაც ნიშნავს სხვადასხვა – როგორც ფინანსური, ასევე ტექნოლოგიური – აუდიტის მუდმივ გავლას. ყველანაირი რისკის გათვალისწინებით, სავსებით რეალურია ცხელ საფულეებში საკუთარი კრიპტოდანაზოგების შენახვის შესაბამისი ფორმის მოძებნა, მაგრამ თუ მომხმარებელი უსაფრთხოების საკითხებში მაქსიმუმისაკენ ისწრაფვის, მისთვის აზრი აქვს, მხოლოდ „ცივი ტიპის“ საფულეებზე შეჩერდეს. რა უპირატესობები და რა ნაკლოვანებები აქვს კრიპტოვალუტების შენახვის ამ ტიპს?

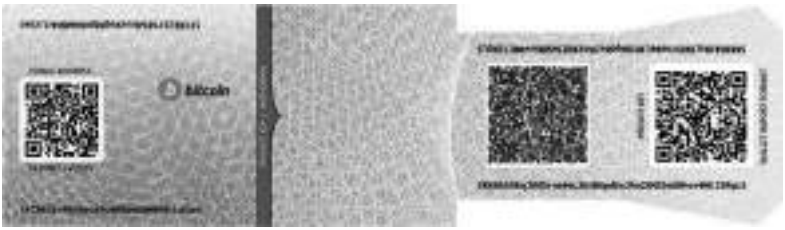
ცივი საცავის როლი შეიძლება შეასრულოს ნებისმიერმა კომპიუტერულმა მოწყობილობამ, რომელიც ინტერნეტში არ არის ჩართული. დიდი პოპულარობა მოიპოვა აპარატულმა გადაწყვეტებმა, რომლებიც ჩვეულებრივი ფლეშ-მეხსიერების მოწყობილობებს ჰგავს. კაცმა რომ თქვას, მსგავსი აპარატული საფულეები პრაქტიკულად ასეთებიცაა, ოღონდ იმ განსხვავებით, რომ ისინი კრიპტოვალუტების შესანახად საჭირო სპეციალურ პროგრამულ უზრუნველყოფას შეიცავს. ხშირად ეს მოწყობილობები აღჭურვილია მცირე ზომის თხევადკრისტალური ეკრანით, რომელზეც მოწყობილობის კომპიუტერთან მიერთებისას აისახება სხვადასხვა სასარგებლო ინფორმაცია, მაგალითად – საფულის კრიპტოვალუტური ბალანსის მდგომარეობა.

მოწყობილობები კომპიუტერს უერთდება მხოლოდ ტრანზაქციების ჩატარების მომენტში, ამიტომ მათგან პრივატული გასაღების მოპარვა ძალზე რთულია. გარდა ამისა, ზოგიერთი მოწყობილობა დამატებით შეიცავს ტრანზაქციის ელექტრონული ხელმოწერის ფორმირების სპეციალურ ღილაკს, რომელზეც გადარიცხვის განსახორციელებლად საჭიროა თითის დაჭერა, რაც საიდუმლო ინფორმაციის მოპარვას პრაქტიკულად შეუძლებელს ხდის. ამჟამად აპარატული კრიპტოსაფულეების ყველაზე პოპულარული მოდელებია Trezor, Ledger Nano S და KeepKey. ყველა ძვირია, სამაგიეროდ, კრიპტოვალუტების შენახვის უსაფრთხოების საკმაოდ მაღალ დონეს უზრუნველყოფს, რაც თავისთავად ძალზე მნიშვნელოვანია, განსაკუთრებით როდესაც საუბარია მნიშვნელოვანი ფიატური ეკვივალენტის მქონე თანხებზე.

კრიპტოვალუტის მარაგების ყველაზე მსხვილ მფლობელებს, კერძოს ან ინსტიტუციურს, სპეციალური მიწისქვეშა ბუნკერებიც კი აქვთ, რომლებიც თითქმის არ განსხვავდება ბანკთა ყველაზე სერიო-

ზული საცავებისაგან. მსოფლიოში არსებობენ კომპანიები, რომლებიც გვთავაზობენ საკმაოდ ძვირ, მაგრამ განსაკუთრებით საიმედო სერვისს ციფრულ ფასეულობათა მნიშვნელოვანი მოცულობების შესანახად. მასიური ფოლადის კარები, ტყვიაგაუმტარი მინები, ელექტრომაგნიტური ზემოქმედების საწინააღმდეგო ბარიერები, მომხმარებელთა იდენტიფიკაციის უმკაცრესი ფორმები – ეს არის იმ ადგილების ატრიბუტების არასრული სია, რომლებშიც ინახება მილიარდობით დოლარის კრიპტოვალუტები, მათი მფლობელების პრივატული გასაღებების სახით. მიუხედავად იმისა, რომ მსგავსი სტრუქტურები კიბერდამნაშავეთა მუდმივი თავდასხმების ობიექტებია, ჯერ ვერავინ შეძლო დაცვის ამ კასკადების დაძლევა, რათა დაუფლებოდა იქ შენახულ ერთ საიდუმლო გასაღებს მაინც.

კრიპტოვალუტების ცივი შენახვის სახეობების აღწერის ბოლოს არ შეგვიძლია არ აღვნიშნოთ კიდევ ერთი ძალზე მარტივი, მაგრამ ამასთან, საკმაოდ დაცული მეთოდი. რამდენად საოცარიც უნდა იყოს, საუბარია ჩვეულებრივი ქაღალდის ფორმით წარმოდგენილ საფულეებზე. ბოლოს და ბოლოს, თუ კრიპტოვალუტური ანგარიშის ფლობა ეფუძნება მხოლოდ მასთან დაკავშირებული პრივატული გასაღების კონტროლს, მაშინ რატომ არ შეიძლება ის დავბეჭდოთ ქაღალდზე და შევინახოთ სეიფში ან საბანკო უჯრაში? ინტერნეტში არსებობს არცთუ ისე ცოტა სერვისი, რომელიც საშუალებას იძლევა, გარდავქმნათ ნებისმიერი ბლოკჩეინ-ანგარიში წყვილი QR-კოდის ამონაბეჭდად, რომელიც საჯარო და პრივატულ გასაღებებსაც ასახავს. არსებობს უსაფრთხოების გაზრდის დამატებითი შესაძლებლობა გასაღებების სპეციალური პაროლით დაშიფვრის გზით. ეს აუცილებელია იმ შემთხვევებისთვის, როდესაც ბოროტმოქმედნი ქაღალდის საფულეს მოიპარავენ ან უბრალოდ გადაიღებენ.



ქაღალდის ასეთი საფულეები ხშირად გამოიყენება კრიპტოვალუტების იმ მესამე პირებისათვის საჩუქრად გადაცემის დროს, რომლებსაც ჯერ არ გააჩნიათ შესაბამისი პროგრამული უზრუნველყოფა და ადრე შექმნილი ანგარიშები ბლოკჩეინ-სისტემებში. თუ ხელთ აქვთ „ქაღალდის სერტიფიკატი“ გასაღებების წყვილითა და მათი კოდებით, ახალ მფლობელებს ნებისმიერ მომენტში შეუძლიათ, მასზე დადებული კრიპტოსახსრები გადაიტანონ ნებისმიერ არჩეულ ცხელ საფულეში და შემდეგ, აუცილებლობისას, მათი საშუალებით განახორციელონ ტრანზაქციები.

კრიპტოვალუტათა შენახვის ამ თავში აღწერილი მეთოდებით მათი სია სრულიადაც არ ამოიწურება. არსებობს კიდევ ნაკლებად გავრცელებული რამდენიმე მეთოდი, მაგალითად – მულტიხელმოწერის მქონე საფულეები ან დანაწევრებული გასაღებები. პირველ შემთხვევაში, ტრანზაქციის გასაგზავნად აუცილებელია რამდენიმე პრივატული გასაღების ქონა ანუ საუბარია საფულიდან სახსრების გადარიცხვის ერთობლივ დადასტურებაზე. მეორე მეთოდი გულისხმობს, რომ პრივატული გასაღები იყოფა რამდენიმე ნაწილად, რომლებიც სხვადასხვა ადგილას ინახება. შესაძლოა, უახლოეს მომავალში „ციფრული ოქროს“ შენახვის სრულიად ახალი მეთოდებიც გამოჩნდეს. თუმცა, კრიპტოვალუტების ყველა მფლობელს უჩნდება ერთი და იგივე კითხვა: მისი შენახვის რომელი სტრატეგიაა ყველაზე ოპტიმალური?

კრიპტოსაზოგადოების ერთობლივი გამოცდილება მეტყველებს, რომ კრიპტოაქტივების შენახვის ყველაზე მისაღებ და მოხერხებულ ფორმად ითვლება ცხელი და ცივი საფულეების კომბინაცია, ანუ ძირითადი კრიპტომარაგები უნდა შევინახოთ ოფლაინ აპარატულ, ზოგჯერ კი – ქაღალდის საფულეებში, ამავე დროს, ცხელ საფულეებში მიზანშეწონილია შევინახოთ მხოლოდ მცირე თანხები იმისათვის, რომ მათი საშუალებით ნებისმიერ მომენტში განვახორციელოთ ტრანზაქციები. კიდევ, თუ მფლობელი აქტიური საბირჟო ტრეიდერია და მისთვის აუცილებელია, მუდმივად აწარმოოს სავაჭრო ოპერაციები, მაშინ მისი აქტივების დიდი ნაწილი იქნება საბირჟო საფულეებში, ოღონდ ეს დამატებით რისკებთანაა დაკავშირებული. ე.წ. „ჰოდლერები“, რომლებმაც კრიპტოვალუტებში სერიოზული გრძელვადიანი შენატანები გააკეთეს, რა თქმა უნდა, მათ უდიდეს ნაწილს ყველაზე უსაფრთხო – ცივ საფულეებში შეინახავენ.

თუ კრიპტოვალუტების მიმართ მსოფლიო საზოგადოების ინტერესის ამსახველ გრაფიკს შევადგენთ, დავინახავთ მრუდს, რომელსაც სხვადასხვა დროს აქვს ზრდა და ვარდნა. ამ გრაფიკის მოძრაობის მიმართულებაზე მრავალი ფაქტორი ახდენს გავლენას – სოციალური, საქმიანი, რეგულაციური, აგრეთვე, სუფთად ტექნოლოგიური. ხშირად ამ უკანასკნელზეა დამოკიდებული, შეძლებს თუ არა კრიპტოვალუტები უახლოეს მომავალში მსოფლიო ეკონომიკაში მნიშვნელოვანი დოზით შეავიწროოს ფიატური ვალუტები. ბლოკჩეინის აქტიური განვითარების გზაზე კიდევ მრავალი რთული პრობლემა დგას, რომლებსაც ამჟამად ოპტიმალური გადაწყვეტა არ გააჩნია და რომლებიც კრიპტოვალუტებს საშუალებას არ აძლევს, თანაბარი კონკურენცია გაუწიოს ფიატურ „კოლეგებს“. რომელი აქტუალური ამოცანები დგას ბლოკჩეინ-ტექნოლოგიების წინაშე და რა მიმართულებით უნდა ვეძებოთ მათი გადაჭრის გზები?

ბლოკჩეინის აქტუალური პრობლემები

განვითარებულ ქვეყნებში ადამიანთა უმრავლესობა ნაღდი ფულის მაგივრად საქონლის შესაძენად მოსახერხებელი საბანკო ბარათებით სარგებლობას მიეჩვია. გადახდის ბარათები დიდი ხანია და მყარად შევიდა ყოველდღიურობაში, მიუხედავად მათი გამოყენების გარკვეული მოუხერხებლობისა: ბარათები შეიძლება ადვილად დავკარგოთ ან საფულესთან ერთად მოგვპარონ; ისინი შეიძლება დააკოპირონ არაკეთილსინდისიერმა გამყიდველებმა გადასახდელად მათთვის ბარათის გადაცემისას, თანაც ხელმოწერა შეიძლება გაყალბდეს, ხოლო პინ-კოდი უცხო პირმა დაინახოს. თაღლითობისათვის კიდევ უფრო ხელსაყრელი გარემოა ინტერნეტი, რომელშიც ბოროტმოქმედთა ბანდები მოქმედებენ. მხოლოდ 2014 წელს საბანკო ბარათებიდან სახსრების მოპარვით ერთობლივმა დანაკარგებმა მსოფლიო მასშტაბით 16 მილიარდ დოლარზე მეტი შეადგინა და ეს ციფრები ყოველწლიურად იზრდება. რატომ არ ჩქარობს მსოფლიო ფინანსური ინდუსტრია საბარათე გადახდების ისეთ ფორმაში გადაყვანას, რომელიც კრიპტოვალუტურ ოპერაციებზე გაცილებით უსაფრთხოდ გამოიყურება?

იმისათვის, რომ ამ კითხვას ვუპასუხოთ, აუცილებელია აღვიქვათ იმ ტრანზაქციების მოცულობების მასშტაბები, რომლებიც თუნდაც ერთი პოპულარული – Visa-ს ან Mastercard-ის საბარათე სისტემაში მიმდინარეობს. ჩვეულებრივ დღეებში ამ სისტემებში ფინანსური ნაკადები წამში ათასობით ტრანზაქციით იზომება, ხოლო გაზრდილი აქტიურობისას – მაგალითად, წინასაახალწლო გაყიდვებისას – პიკურმა დატვირთვებმა შეიძლება წამში 20 000-40 000 ტრანზაქცია შეადგინოს. ახლა დავთვალოთ, ამ კუთხით რა შეუძლია შემოგვთავაზოს გადახდის ყველაზე პოპულარულმა ბლოკჩეინ-სისტემამ – ბიტკოინ-ქსელმა.

როგორც გვახსოვს, ამ სისტემაში ბლოკის ზომა 1 მეგაბაიტს შეადგენს, ხოლო საშუალო ტრანზაქცია მასში დაახლოებით 250-300 ბაიტს იკავებს, ამასთან, ყოველი ახალი ბლოკი ქსელში ყოველ 10 წუთში ფორმირდება. მარტივი გამოთვლები გვიჩვენებს, რომ ბი-

ტკოინ-ქსელის გამტარუნარიანობა შეადგენს წამში დახლოებით შვიდ ტრანზაქციას. ახლა შევადაროთ იგი ოპერაციების დამუშავების სიჩქარეს მსხვილ საბარათე ქსელებში. თან, ეს მხოლოდ ერთი პარამეტრია, რომლის მიხედვითაც ორ პრინციპულად განსხვავებულ ფინანსურ ტექნოლოგიას ვადარებთ. უფრო მეტიც, ეს მაჩვენებელი დიდი პრობლემის მხოლოდ ერთ-ერთი შემადგენელი ნაწილია, რომელიც გზას უღობავს ფიატურ საშუალებებთან შედარებით კრიპტოვალუტების გადახდის კონკურენტულ სტატუსში აყვანას. ეს პრობლემაა მასშტაბირებადობა.

ბლოკჩეინ-ტექნოლოგია თავისთავად, ბევრ უპირატესობას ფლობს, რომლებიც ძალზე დეტალურად განვიხილეთ ამ წიგნში. ახლა დადგა დრო, ვისაუბროთ მის ზოგიერთ ნაკლოვანებაზე, უფრო სწორად კი – იმ ასპექტებზე, რომლებიც ხელს უშლის განაწილებული რეესტრის ტექნოლოგიებზე დაფუძნებული პროდუქტის სწრაფ გავრცელებას. ბლოკჩეინ-პროდუქტებს მასშტაბირების სუსტად გამოხატული უნარი აქვს, პირველ რიგში, ტრანზაქციების დადასტურების სიჩქარის გამო, აგრეთვე, ბლოკების მონაცემთა ბაზის მუდმივი ზრდის გამო, რადგან შეუძლებელია მათში ადრე მოთავსებული ინფორმაციის წაშლა. სხვა სიტყვებით რომ ვთქვათ, თუ ამოცანის პირობა მიკროტრანზაქციების უზარმაზარი რაოდენობის დამუშავებაა, ბლოკჩეინი ამას კარგად სულაც ვერ გაუმკლავდება.

წარმოვიდგინოთ სიტუაცია, როდესაც ბლოკჩეინ-ტექნოლოგიის ბაზაზე აგებული გადახდის სისტემა ითვალისწინებს, ვთქვათ, ფინჯანი ყავის შეძენას ერთ-ერთი ყველაზე მსხვილი ქსელური Starbucks-ის ტიპის ყავახანაში. საუბარია რამდენიმე დოლარის ეკვივალენტის ფასეულობის გადაცემის ტრანზაქციაზე. თავდაპირველად ტრანზაქცია უნდა დადასტურდეს ანუ მოთავსდეს ბლოკში, რომელსაც მთელი დეცენტრალიზებული ქსელი მიიღებს, შემდეგ კი, სისწორისთვის, გარდა ამ ბლოკისა, მის მომდევნო ჯაჭვში უნდა მოთავსდეს მინიმუმ რამდენიმე მომდევნო ბლოკი. ეს პროცესი უეჭველად გარკვეულ დროს მოითხოვს. ჩნდება კითხვა: მოიცდიან კი მყიდველები და გამყიდველები წუთების ან ათეულობით წუთის განმავლობაშიც კი, რათა გადახდის ტრანზაქციამ ყველა აუცილებელი დადასტურება მიიღოს? დიდი ალბათობით, ისინი გადახდის დადასტურების უფრო სწრაფ გზას აირჩევენ.

ახლა გავითვალისწინოთ კიდევ ერთი მნიშვნელოვანი დეტალი: ყავის ფინჯანი შეიძლება ძალიან ბევრი იყოს. ითვლება, რომ მსოფლიოში ყოველდღიურად ისმება 1,5 მილიარდი ფინჯანი ყავა, რომელთა მნიშვნელოვანი ნაწილი რესტორნებსა და ყავახანებში იყიდება. თუ მათთან დაკავშირებულ გადახდის ოპერაციებს ბლოკჩეინში მოვათავსებთ, მაშინ ბლოკთა მონაცემთა ბაზა კოსმოსური სისწრაფით გაიზრდება. არადა, ვსაუბრობთ მონაცემთა შენახვის დეცენტრალიზებულ ფორმაზე, რაც გულისხმობს მონაცემთა მუდმივ კოპირებასა და სინქრონიზაციას ქსელის ყველა სავსე კვანძს შორის. თანამედროვე ბლოკჩეინ-გარემოებს არ ძალუძს ასეთი რაოდენობის მცირე ტრანზაქციების დამუშავება, მით უმეტეს, რომ განვიხილეთ საქონლის მხოლოდ ერთი დასახელება – ფინჯანი ყავა. აქედან ვასკვნით, რომ ბლოკჩეინში ტრანზაქციური ინფორმაციის ჩაწერისა და შენახვის კლასიკური მოდელი არანაირად არ გამოდგება მასობრივი მიკროტრანზაქციებისთვის არც დამუშავების სიჩქარით და არც მონაცემთა შენახვის საჭირო მოცულობებით. როგორ შეიძლება გადავჭრათ ეს პრობლემა?

გადაჭრის ერთ-ერთ ვარინტად შეიძლება იქცეს ე.წ. „შარდინგი“ (ინგლისური სიტყვდან shard — „ნამსხვრევი“). ქსელის მონაწილეთა შორის ბლოკების მონაცემთა მთლიანი ბაზის ჭარბი კოპირებისაგან განსხვავებით, შარდინგის კონცეფცია ბლოკჩეინ-ტექნოლოგიაში გულისხმობს მონაცემთა ბაზის დაყოფას გარკვეული რაოდენობის ნაწილებად, რომლებიც ქსელური კვანძების მხოლოდ გარკვეულ ჯგუფებში კოპირდება. მონაცემთა განაწილებული ინფრასტრუქტურის მთლიანობის შესანარჩუნებლად აუცილებელია სრული ბაზის ნაწილების რაოდენობის ზუსტი მათემატიკური გამოთვლა, ყოველი მათგანის მოცულობისა და მონაცემთა ბაზის თავისი სეგმენტების შემნახავ ყოველ ჯგუფში კვანძების რაოდენობის გამოთვლა. ცნება „მთლიანობა“ ამ შემთხვევაში გულისხმობს 100%-თან მიახლოებულ გარანტიას იმისა, რომ დროის ნებისმიერ მომენტში ქსელის ყოველი კვანძისათვის სასინქრონიზაციოდ ხელმისაწვდომი იქნება ბლოკების მონაცემთა სრული ბაზის ნებისმიერი ნაწილი.

ამჟამად ბლოკჩეინ-პროექტების ბევრი შემმუშავებელი იკვლევს შარდინგის კონცეფციის დანერგვის შესაძლებლობას. ამგვარი სამუშაოს შესახებ ერთ-ერთმა პირველმა განაცხადა პროექტ Ethereum-ის

დეველოპერთა გუნდმა ვიტალიკ ბუტერინის მეთაურობით. მაგრამ საზოგადოების წინაშე დღემდე არ წარდგენილა შარდინგის რამდენადმე ქმედითი მოდელი. არადა, შარდინგი არ არის პანაცეა ბლოკების მონაცემთა „გაბერვის“ თვალსაზრისით, არამედ მხოლოდ იმის საშუალებას გვაძლევს, რომ დროში გადავავადოთ ამ პრობლემის ნეგატიური გავლენა. შარდინგი ნამდვილად გააუმჯობესებს ვითარებას იმ ბლოკჩეინ-გარემოებში, სადაც მიკროტრანზაქციები ან საერთოდ არ არსებობს, ან ტრანზაქციების დომინანტურ ტიპს არ წარმოადგენს. რაც შეეხება გადახდის ბლოკჩეინ-სისტემებს, რომლებსაც პრეტენზია აქვს ყოველდღიურ ცხოვრებაში მასობრივ გამოყენებაზე, მასშტაბირების პრობლემის ბევრად უფრო პერსპექტიული გადაჭრა იქნება Lightning Network — „ელვისებური ქსელის“ ოქმის კონცეფცია.

ბიტკოინ-ქსელის მიკროგადახდებთან ადაპტირების მცდელობისას კიდევ ერთ – საკომისიოების პრობლემას ვაწყდებით. როგორც ცნობილია, ამ ქსელში არსებობს სატრანზაქციო საკომისიოები, რომლებსაც ბლოკების ფორმირებისას მაინერები იღებენ. გარდა მაინერთა მონეტარული მოტივაციისა, საკომისიოები ასრულებს კიდევ ერთ მნიშვნელოვან ფუნქციას – უზრუნველყოფს სატრანზაქციო სპამისაგან თავდაცვას, რომელსაც შეუძლია სერიოზულად შეანელოს ქსელის მუშაობის სიჩქარე. საკომისიოების ფიატურმა ეკვივალენტებმა შეიძლება სერიოზული თანხები შედგინოს, რაც მიკროტრანზაქციების ფორმირებას უაზრობად აქცევს. თუ, მაგალითად, ფინჯანი ყავა 2 დოლარი ღირს, ხოლო მისი გადახდის ტრანზაქციის საკომისიო მასთან მიახლოებულ თანხას შეადგენს, ვის ექნება სურვილი გადაიხადოს ორმაგი ფასი კრიპტოვალუტით გადახდის სიამოვნების გამო? სწორედ ასეთი სიტუაციებისათვის შეიქმნა მოდელი Lightning Network.

Lightning Network ფაქტობრივად, ბლოკჩეინ-სისტემის ინფრასტრუქტურულ ზედნაშენს წარმოადგენს. ამასთან, საუბარია არა მხოლოდ ბიტკოინ-ქსელზე, არამედ მსგავსი კონცეპტები მუშავდება სხვა პოპულარული ბლოკჩეინ-გარემოებისთვისაც. „ელვისებური გადარიცხვების“ ქსელი შედგება კვანძებისაგან, რომლებიც ერთმანეთში წყვილების შექმნისას ე.წ. ორმხრივი „გადახდის არხებს“ აყალიბებს. ამ ორი კვანძიდან თითოეული გარკვეულ სახსრებს ბლოკავს შექმნილი არხისათვის, რომლის თანხაც შეადგენს მის გადახდის გამტარუ-

ნარიანობის უნარს. ამასთან, კვანძებს შეუძლია შექმნას ერთდროულად რამდენიმე კვანძის მქონე არხები, რითაც ქმნის მთელ ქსელს, რომლის შიგნითაც შეიძლება ჩამოყალიბდეს დაბალი საკომისიოს მქონე სწრაფი სატრანზიტო ოპერაციების გზები.

სახსრების გადაცემა ხორციელდება არხების კვანძებზე ურთიერთბალანსების ცვლილების გზით მანამ, სანამ ერთ-ერთ კვანძში სახსრები გამოილევა, ანუ – არხი აღმოჩნდება „გამოფიტული“. კვანძებს ნებისმიერ დროს შეუძლია დახუროს არხები და თავისთვის ჩაირიცხოს სახსრები, რომლებიც აქტუალური ურთიერთშემხვედრი ბალანსის ტოლია. ამგვარად, სწრაფად და განსაკუთრებულად იაფად გვარდება მიკროტრანზაქციების პრობლემა პოპულარული კრიპტოვალუტებით გადახდისათვის. თუმცა, ამ მოდელსაც აქვს ნაკლოვანებები, რომელთა შორისაც მთავარია ქსელის კვანძებისათვის ხანგრძლივვადიანი მოტივაციის არარსებობა, რომ დაიცვან გადახდის არხები, მოკრძალებული შემოსავლის გამო. მიმდინარე შეფასებებით, Lightning Network-ის კვანძის შენახვას მფლობელისთვის სულ, წლიური შემოსავლის მხოლოდ 1% მოაქვს. ამასთან, გადახდის არხების ყოველმა კვანძმა უნდა დაბლოკოს საკუთარი სახსრები ქსელის ფუნქციონირებისათვის, უნდა იყოს მუდმივად ონლაინრეჟიმში და ამით ჰაკერული თავდასხმის საშიშროების ქვეშ აღმოჩნდეს.

მსგავსი ქსელის ფუნქციონირების კიდევ ერთი პრობლემაა შესაძლო ჭარბი ცენტრალიზაცია, როდესაც ყველაზე მთავარ კვანძებში შეიძლება დაგროვდეს მნიშვნელოვანი კრიპტოვალუტური ლიკვიდურობა. კვანძის ქსელიდან გამოთიშვის შემთხვევაში, სხვა მომხმარებლების სახსრები, რომლებმაც ისინი მოცემული ინფრასტრუქტურის საშუალებით გადაიხადეს, შეიძლება ხანგრძლივად დაბლოკილი აღმოჩნდეს. ამ ქსელში არსებობს თაღლითობის საშიშროებაც, განსაკუთრებით, თუ არხის ერთ-ერთი კვანძი ხანგრძლივად გაქრება ქსელიდან. მიუხედავად ამისა, Lightning Network-ის მოდელის კონცეფცია აგრძელებს აქტიურ განვითარებას. მხოლოდ ბიტკოინ-ქსელში 2019 წლის გაზაფხულის მდგომარეობით, გადახდის 40 000 არხი არსებობს და მათი რიცხვი იზრდება.

უნდა დავამატოთ, რომ „ელვისებური ქსელის“ მოდელი ბლოკჩეინის მასშტაბირების ერთადერთი საშუალება არ არის. უფრო დაწვრილებით არ შევჩერდებით სხვა კონცეფციების ტექნოლოგიურ

აღწერაზე, როგორებიცაა, მაგალითად, მიმართული აციკლური გრაფები ან ტრანზაქციის ზომის შემცირების მეთოდიკა მისგან ციფრული ელექტრონული ხელმოწერების ამოღების გზით. აღვნიშნავთ მხოლოდ, რომ ჯერჯერობით ვერც ერთმა არსებულმა მეთოდმა ვერ შეძლო, სრულად გადაეჭრა გამტარუნარიანობის ან მონაცემთა შენახვის ჭარბი მოცულობების პრობლემა.

ტექნოლოგიურის გარდა, ბლოკჩეინს აქვს სოციალური ხასიათის პრობლემებიც. როგორც ბიტკოინის მაინინგისა და Proof-of-work ოქმის აღწერისადმი მიძღვნილ თავში იყო აღნიშნული, კრიპტოვალუტების ემისიის ეს მეთოდი ხასიათდება განსაკუთრებული ენერგოტევადობით და ირიბად აზიანებს გარემოს. მისი კონცეპტუალური სირთულის გამო, ძალზე ბევრ მომხმარებელს ცუდად ესმის განაწილებული რეესტრის ტექნოლოგიის უპირატესობები და ნაკლოვანებები. „კრიპტოვალუტური ჰაიპის“ გავლენა ხშირად იწვევს იმას, რომ საქმიანი საზოგადოების ცალკეული წარმომადგენლები ცდილობენ, თავიანთი არსებული პროექტები ბლოკჩეინად გარდაქმნან. ყოველთვის უნდა გავითვალისწინოთ, რომ ასეთმა ერთობ გაუაზრებელმა სტრატეგიამ, დამატებითი ფასეულობების შექმნის მაგივრად, შეიძლება დაანგრიოს მანამდე საკმაოდ წარმატებული ბიზნესი.

რეგულაციური გარემოც იშვიათად არის როგორც ბლოკჩეინის, ასევე მისი დაფინანსების მეთოდების, კერძოდ, ICO-ის მიმართ მეგობრული. ყველა საფუძველი გვაქვს ვიფიქროთ, რომ ბლოკჩეინ-ინდუსტრიის რეგულირების პროცედურების სიმკაცრე მომავალში მხოლოდ გაიზრდება. ამასთან, არ უნდა დაგვავიწყდეს, რომ კრიპტოვალუტების მფლობელები იმთავითვე ანონიმურები არიან, ამიტომ გადახდისათვის კრიპტოვალუტების მიმღებ გამყიდველებს მოუწევთ შეასრულონ თავიანთი კლიენტების იდენტიფიკაციის რეგულაციური მოთხოვნები. რაც შეეხება მსხვილ ფინანსურ ინსტიტუტებს, პირველ რიგში კი ბანკებს, ისინი არცთუ უსაფუძვლოდ ხედავენ ბლოკჩეინ-ტექნოლოგიაში საფრთხეს თავიანთი არსებობისათვის, რადგან ის დეცენტრალიზაციასა და ფინანსური შუამავლობის ჩამოშორებას გვთავაზობს. სამართლიანობისათვის უნდა აღინიშნოს, რომ ბევრმა ბანკმა დაიწყო ბლოკჩეინ-ტექნოლოგიის გამოყენება თავისი ხარჯების ოპტიმიზაციისათვის და საკუთარი ფინანსური პროდუქტების კონკურენტუნარიანობის ასამაღლებლად.

მიმდინარე მომენტისათვის შეიძლება მხოლოდ რამდენიმე ძირითადი დასკვნის კონსტატირება: ბლოკჩეინი არის ძალზე პერსპექტიული ტექნოლოგია, მას აქვს რამდენიმე საკმაოდ სერიოზული პრობლემა და ამ პრობლემების გადაჭრაზე მუშაობენ როგორც მსოფლიო მათემატიკის, ასევე IT-ინდუსტრიის საუკეთესო თავები. რა თქმა უნდა, ამას გარკვეული დრო დასჭირდება და სწრაფი გარღვევების მოლოდინიც არ გვაქვს. კრიპტოსაზოგადოება ამოცანებს გადაჭრის ნაბიჯ-ნაბიჯ და შემდეგ, როდესაც სასარგებლო იდეების, ინსტრუმენტების, მოდელებისა და კონცეფციების რაღაც კრიტიკული მასის დაგროვება მოხდება, ყველანი ერთობლივად შეძლებენ მიუახლოვდნენ აქტუალური პრობლემების გადაწყვეტას, რომლებიც ბლოკჩეინ-ტექნოლოგიების წინაშე დგას.

სამყაროს ახალი სურათი (დასკვნა)

უკვე ათ წელიწადზე მეტი ხანი გავიდა იმ მომენტიდან, როდესაც ბიტკოინის პროექტის პირველ ბლოკჩეინ-ქსელში საგენეზისო ბლოკი გამოჩნდა. ამ მოვლენამ აღნიშნა მთელი ჰაიტეკ-ინდუსტრიის წარმოქმნა და შემდგომში გავლენა იქონია ბევრი ადამიანის ცხოვრებაზე. იყვნენ ისეთებიც, რომლებმაც შეძლეს კრიპტოვალუტაში ადრეული ინვესტიციებით გამდიდრება, აგრეთვე ისეთებიც, რომლებმაც შეძლეს ინვესტორების ინტერესებისაგან წამოსული იდეების გატანა და ICO-ზე მნიშვნელოვანი თანხების შეგროვება, მაგრამ იყვნენ ისეთებიც, რომლებმაც დაუჯერეს შემმუშავებლებს და ახალ კრიპტომონეტებში ჩადეს საკუთარი სახსრები, რომლებიც უკვე რამდენიმე თვეში გაუფასურდა. ბლოკჩეინ-ინდუსტრიას შეუძლია აღტაცებისა და იმედგაცრუების გამოწვევა, იმედებისა და მათი დამსხვრევის მოტანა, ბიძგის მიცემა ტოტალური ცვლილებებისთვის ბიზნესმოდელების აგების ფილოსოფიაში, ისევე როგორც მკვლევრების შეყვანა ჩიხში, რომლიდან გამოსვლაც, ერთი შეხედვით, შეუძლებელია. ერთი სიტყვით, მიმდინარეობს ნორმალური ევოლუციური პროცესი, რომელიც აუცილებლად თან სდევს ნებისმიერ სიცოცხლისუნარიან ინოვაციურ მოვლენას.

არსებობს აზრი, რომ ბლოკჩეინ-ტექნოლოგიას მეტი კითხვა სდევს, ვიდრე პასუხი, მაგრამ მოდი ვაღიაროთ, რომ ათი წელი ძალზე მცირე ვადაა იმისათვის, რომ ნაჩქარევი დასკვნები გავაკეთოთ. ამერიკელმა ფიზიკოსმა, აშშ-ის ენერგეტიკის ყოფილმა მინისტრმა და ნობელის პრემიის ლაურეატმა, სტივენ ჩუმ ერთხელ თქვა: „ქვის ხანა დამთავრდა არა იმიტომ, რომ ქვები გათავდა“. ეჭვგარეშეა, რომ ბლოკჩეინ-ტექნოლოგია ამჟამად ჯერ კიდევ თავის „ქვის ხანაში“ იმყოფება. მაგრამ ინფორმაციის ღიაობის ის პრინციპები, რომლებიც ბლოკჩეინ-ინდუსტრიაშია მიღებული, ყველა საფუძველს იძლევა ვივარაუდოთ, რომ მისი განვითარება მოხდება საკმაოდ სწრაფი ტემპით. პირველ რიგში, ამას ხელს შეუწყობს მასში ჩართული ყველა

სპეციალისტის, მეწარმეების, ინჟინრებისა და მეცნიერების სინერჯია. ელის თუ არა ბლოკჩეინს შემდგომი ევოლუციური პროგრესი, „ბრინჯაოსა“ და „რკინის“ ხანის სახით, ამას მომავალი გვიჩვენებს. ერთი რამ არის ეჭვგარეშე: საქმე გვაქვს არა მარტო აღრიცხვის, ფასეულობათა შენახვისა და გადაცემის ახალ კონცეფციასთან, არამედ – ახალ ტექნოლოგიურ ფილოსოფიასთანაც, რომელმაც შეიძლება გამოიწვიოს ტექნოლოგიური წანაცვლება ათასწლობით ჩამოყალიბებულ სოციალურ მოდელებსა და საქმიან ურთიერთობებში.

პირველ რიგში, საუბარია შუამავლის ცნების ტრანსფორმაციაზე. თუ ბლოკჩეინი ბოლომდე არ სპობს ამ როლს, შეუძლია მისი დომინირების შემცირება მაინც, კონტრაგენტებს შორის დეცენტრალიზებული ურთიერთობის კონცეფციის შემოთავაზებით. რა შედეგები შეიძლება მოიტანოს ამ ფაქტმა? საშუამავლო მარჟის გამოთავისუფლება უმძლავრესი ფაქტორია, რომელიც საშუალებას იძლევა, გადავანაწილოთ ძვირფასი ადამიანური და ფინანსური რესურსები არამწარმოებლური ფუნქციებიდან შემოქმედებითში. რა თქმა უნდა, შუამავლობის ყველა ფორმა როდია ბალასტი მსოფლიო ეკონომიკისათვის, თუმცა არსებობს ტიპური საშუამავლო ოპერაციები, რომლებისგანაც კაცობრიობას უმტკივნეულოდ გათავისუფლება შეუძლია, და ამისათვის ძირითად ინსტრუმენტად შეგვიძლია გამოვიყენოთ ბლოკჩეინ-ტექნოლოგია, რომლით სარგებლობაც პრინციპულად ახალი პროექტების აგების არქიტექტურული იდეოლოგიის დარგში საშუალებას მოგვცემს განვახორციელოთ მასშტაბური დეზინტერმედიაცია კომერციული და სხვაგვარი მომსახურების სფეროში.

რაც შეეხება სახელმწიფოსა და ფინანსური რეგულაციის როლს, აქ აუცილებლად უნდა გავითვალისწინოთ, რომ ბიუროკრატიული ინსტიტუტების ბუნებრივი კონსერვატიზმი უფრო შეეწინააღმდეგება ბლოკჩეინ-ტექნოლოგიის განვითარებას, ვიდრე ხელს შეუწყობს მას. მხოლოდ იმის იმედიღა გვრჩება, რომ გამოჩნდებიან მთავრობები, რომლებიც დაუშვებენ კრიპტოგარემოს რეგულირების მიმართ აზრიანი რისკების სტრატეგიას, რაც, თავის მხრივ, ხელს შეუწყობს შემდგომ პროგრესს როგორც ფინანსური სექტორის, ასევე მთლიანად სერვისის ინფრასტრუქტურის განვითარებაში. ეს მათ მისცემს უდავო უპირატესობას იმ ქვეყნებთან შედარებით, რომლებიც კლასიკური ფინანსური მოდელების მიმართ დამცავ პრინციპებს ემხრობიან, რაც

მათ მოჩვენებითი სტაბილურობის, მაგრამ ამასთან ერთად, ტექნოლოგიურ განვითარებაში ერთ წერტილში უთუო გაყინვის გარანტიას აძლევს. ნებისმიერ შემთხვევაში, არაგონივრული იქნება უგულებელვყოთ საინფორმაციო ტექნოლოგიებში მსოფლიო ინდუსტრიის სტრატეგიული ტენდენციები, რადგან ეს აუცილებლად გამოიწვევს ტექნოლოგიურ ჩამორჩენასა და ინფრასტრუქტურულ დეგრადაციას.

მივმართოთ სტატისტიკას, რომელიც ჩვეულებრივ, საკმაოდ მეტყველია. მხოლოდ 2019 წლის განმავლობაში მსოფლიოში ბლოკჩეინის შემმუშავებელთა რაოდენობა 33-ჯერ, ხოლო ბლოკჩეინ-გადაწყვეტების სპეციალისტებზე კომერციული კომპანიების მოთხოვნა 517%-ით გაიზარდა. საქმიანმა სპეციალურმა ქსელმა LinkedIn გამოაქვეყნა კვლევის შედეგები, რომელშიც ბლოკჩეინ-შემმუშავებლები ყველაზე მოთხოვნად სპეციალისტებად არიან დასახელებული ამერიკის შრომის ბაზარზე. ბევრი უნივერსიტეტი მთელ მსოფლიოში ხსნის ბლოკჩეინ-ინდუსტრიის სპეციალისტების მოსამზადებელ კათედრებს, მაგრამ ეს პროცესი, სამწუხაროდ, ისე სწრაფად არ ვითარდება, როგორც ამას ინფორმაციულ ტექნოლოგიებთან დაკავშირებული მსოფლიო ბიზნესი ისურვებდა. ყველაფერი ეს გვიჩვენებს თვით ბლოკჩეინ-ტექნოლოგიების მიმართ მასშტაბურ ინტერესს და აგრეთვე იმას, რომ მასთან უფრო მეტად აკავშირებენ საქმიანი და სოციალური გარემოს შემდგომი განვითარების პერსპექტივას.

დავუბრუნდეთ ამერიკელი ადვოკატის, ნიკოლას კლაინის ციტატას, რომლითაც ეს წიგნი დაიწყო, შევეცადოთ ვივარაუდოთ, დაუდგამენ თუ არა ძეგლს ბლოკჩეინს. ტექნოლოგიის არსებობის პირველი ათი წლის განმავლობაში მან საზოგადოების მხრიდან ემოციების მთელი სპექტრი განიცადა: გულგრილობიდან ან თავშეკავებული ოპტიმიზმიდან – აგრესიამდე და ჭეშმარიტად ბიბლიურ ფანატიზმამდე. მას ანათემას გადასცემდნენ სახელმწიფოები და სახელმწიფო რეგულატორები, მაგრამ ადიდებდნენ ლიბერტარიანული და ანარქიული იდეების მქონე ადამიანები. ზოგი ანალიტიკოსი კრიპტოპროექტებს ფინანსური ბუშტებისა და პირამიდების იარლიყს აწებებდა, მაგრამ იყვნენ ისეთებიც, რომლებიც ღაღადებდნენ მსოფლიოს ახალ სურათზე, რომელიც ძველ იერს აღარასდროს დაიბრუნებდა. ზოგიერთი ავტორიტეტული შორსმჭვრეტელი ვარაუდობდა, რომ ბიტკოინი უკვე უახლოეს წლებში მილიონები ეღირებოდა, სხვები კი პირიქით, უსახე-

ლო აღსასრულს უწინასწარმეტყველებდნენ. ზოგმა ისიც კი დათვალა, რომ ბიტკოინის პროექტი – არც მეტი, არც ნაკლები – 334-ჯერ „დამარხეს“ და ეს ალბათ ზღვრული მონაცემი არ არის.

ერთი რამ ჯერჯერობით დაბეჯითებით შეიძლება ითქვას: ბლოკჩეინ-ტექნოლოგია განვითარების გზის დასაწყისშია. უწერია კი მას შეცვალოს ბიზნესის, სახელმწიფოებისა და საზოგადოების მართვის ჩვეული ცენტრალიზებული მეთოდები? მიიღებს კი კრიპტოვალუტები შანსს, ბრუნვაში თუნდაც გარკვეულწილად შეავიწროოს გადახდის კლასიკური საშუალებები? შეუწყობს კი ეს ხელს იმას, რომ ფასეულობათა გადაცემის პროცესი უფრო გამჭვირვალე და საზოგადოებისათვის უფრო სამართლიანი გახდეს? თუ ამ საკითხთა უმეტესობა დადებითად გადაწყდება, მაშინ შეიძლება ვიქონიოთ იმედი, რომ მადლიერი შთამომავლობა მართლაც აუგებს ძეგლს ბლოკჩეინს.

ტალინი, ესტონეთი
2018–2019