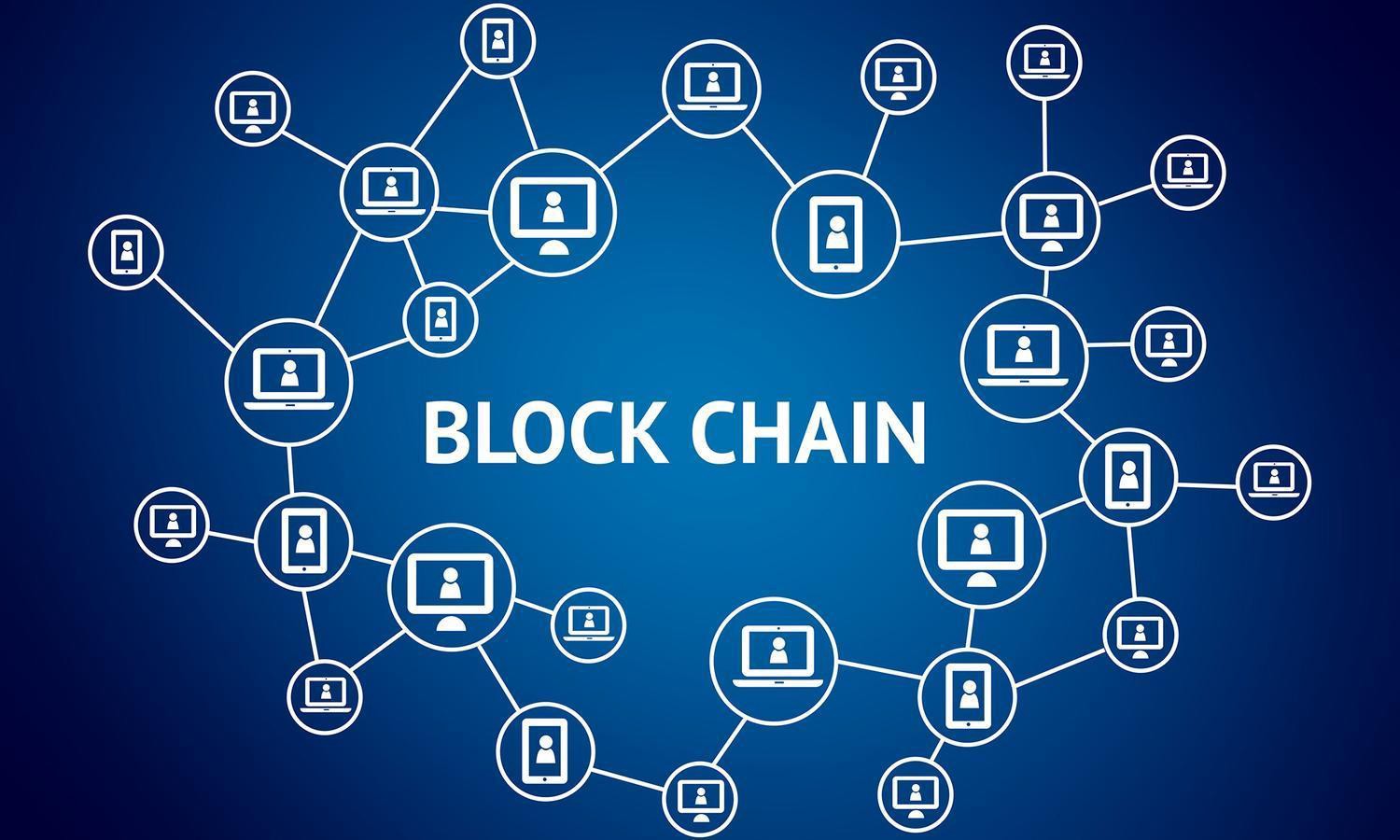
**ლევან იმნაიშვილი, მერაბ ფხოველიშვილი**

**ბლოკჩეინი და მისი გამოყენებები**



**საქართველოს ტექნიკური უნივერსიტეტის საგამომცემლო სახლი**

**თბილისი 2019**

**სარჩევი**

**თავი 1. ისტორია**. **რა არის ბლოკჩეინი, რა არის ბიტკოინი .....................3**

**თავი 2. თანამედროვე კრიპტოვალუტების მახასიათებლები..................8**

**თავი 3. როგორ მუშაობს ბლოკჩეინ ტექნოლოგია ...................................10**

თავი 4. **ჰეშირება.**.............................................................................................................13

**თავი 5. ბლოკჩეინი და მისი ძირითადი თვისებები**................................18

**თავი 6. რატომ უნდა ვისარგებლოდ ბლოკჩეინით და ბიტკოინით….21**

**თავი 7. რისი გაკეთება შეუძლია ბლოკჩეინს.......................................... .27**

**თავი 8. როგორ ხდება ბიტკოინ ტრანზაქციები................................. ......30**

**თავი 9. რითი განსხვავდება ბლოკჩეინი მონაცემთა ბაზისაგან..... ......33**

**თავი 10. ბლოკჩეინ ტექნოლოგია.......................................................... .....36**

**თავი 11. რა არის გონიერი კონტრაქტები. გონიერი კონტრაქტების გამოყენება და უპირატესობები............................................................ .......39**

**თავი 12. სხვა კრიპტოვალუტები. ICO და IPO კონცეფციები.**................44

**თავი 13. მოპოვება (Mining)** .........................................................................49

**თავი 14. გამოყენებები** ..................................................................................53

**თავი 15. სხვა გამოყენებები** .........................................................................62

ლიტერატურა……………………………………………………… ………..65

**თავი 1. ისტორია**. **რა არის ბლოკჩეინი, რა არის ბიტკოინი.**

როგორ დაიწყო ყველაფერი - კრიპტო-ვალუტის იდეა. კრიპტოვალუტისა და ბლოკჩეინის განვითარების ძირითადი ეტაპები

სატოში ნაკომოტოს ნაშრომმა „Bitcoin- A peer-to-peer electronic cash system”, საფუძველი ჩაუყარა ბლოკჩეინ ტექნოლოგიასა და კრიპტოვალუტებს იმ სახით, რომლითაც დღეს ჩვენ მას ვიცნობთ.

ბოლო ხანებში ინტერნეტ ფულადი გადარიცხვები მთლიანად დამოკიდებულია უკვე არსებულ ფინანსურ ინსტიტუტებზე. გამოდის, რომ ნდობა მთლიანად ეკისრება მესამე მხარეს, რათა ეს ელექტრონული გადარიცხვები შესრულდეს. ეს მოდელი

უმეტესი ტრანზაქციებისთვის დღემდე კარგად მუშაობს, მაგრამ არსებობს პრობლემები, რომლებიც ჩნდება ნდობაზე დამყარებულ სისტემებში. ასეთ სისტემაში არ არსებობს შეუქცევადი ტრანზაქციები, რადგან ადამიანებს ყოველთვის

შეუძლიათ ჩაერიონ, როგორც მესამე პირი და ტრანზაქციები შექცევადი გახადონ (მაგალითად გააუქმონ ტრანზაქცია) ნებისმიერ დროს. მესამე მხარის (მაგალითად ბანკის) შუამავლობა ზრდის ტრანზაქციის ხარჯებს, ზღუდავს მიკრო ტრანზაქციების შესაძლებლობას და ამცირებს ჩვეულებრივი ტრანზაქციების მოცულობას. ტრანზაქციების შექცევადობა კიდევ უფრო ავრცელებს ნდობის საჭიროებას. ამის

გამო, გამყიდველები ფრთხილად უნდა იყვნენ თავიანთ კლიენტებთან, რადგან მოუწევთ მათი შეწუხება ისეთი ინფორმაციისთვის, რაც მათ არ დასჭირდებოდათ სხვაგვარად. ასეთ სისტემაში, გაყალბების გარკვეული დონე ყოველთვის არ-სებობს. ზემოთ მოცემული ხარჯები და გაურკვევლობები გვარ-დება მხოლოდ პირისპირ ნაღდი ფულის(ქეშის) გაცვლისას, მაგ-რამ დღემდე არ არსებობს მექანიზმი ონლაინ ტრანზაქციები-სთვის, რომელიც მოსპობს ნდობით აღჭურვილი მხარის საჭიროებას. საჭირო არის ელექტრონული გადახდის სისტემა, რომელიც დაფუძნებულია კრიპტოგრაფიულ მტკიცებულებაზე ნდობის ნაცვლად. ის საშუალებას მისცემს ნებისმიერ ორ მხარეს, დაუყოვნებლივ გადაცვალონ, რაც უნდათ, მესამე პირის

ნდობის საჭიროების გარეშე. ტრანზაქციები, რომელთა შექცევადობაც იქნება წამგებიანი და არაპრაქტიკული, დაიცავს გამყიდველებს თაღლითობისგან. ამასთანავე, ადვილად მოხერხდება უწყვეტი ესქროუ მექანიზმების განხორციელება

მყიდველების დასაცავად. ამ დოკუმენტში, ჩვენ ვთავაზობთ გამოსავალს ორმაგი ხარჯვის პრობლემის გადასაჭრელად, რო-მელიც გულისხმობს ტრანზაქციების ჩაწერას უწყვეტ და დრო-ით ქრონოლოგიურ ჯაჭვში. მისი სიზუსტის მტკიცებულება

მოხერხდება მოცემული კომპიუტერული გამოთვლებით. ეს სისტემა უსაფრთხოა მანამ, სანამ ნოდები აკონტროლებენ უფრო მეტ პროცესულ რესურსს, ვიდრე თავდამსხმელი ნოდები.

**ტრანზაქციები**

მოდით ელექტრონული მონეტა (მონეტები) მივიჩნიოთ, როგორც ციფრული ხელმოწერების/კოდების ერთობლიობა. თითოეული მომხმარებელი მონეტის გადარიცხვისას ციფრულად აღწერს წინა ტრანზაქციის ჰეშს და მიმღების საჯარო გასაღებს, რომელიც შემდგომ იწერება ამ მონეტის (კოდების ერთობლიობის) ბოლოს. მიმღებს საშუალება ეძლევა, დაადასტუროს, თუ ვის ეკუთვნის მონეტა ციფრული ხელმოწერების ჯაჭვის შემოწმებით. პრობლემა რა თქმა უნდა, ის არის, რომ მიმღებს არ შეუძლია გადაამოწმოს, გამომგზავნმა მონეტა ორჯერ დახარჯა თუ არა. ამ პრობლემის პრობირებული

გადაჭრის გზა არის ცენტრალური სერვერის, ან ერთეულის, დანერგვა, რომელიც შეამოწმებს ყველა ტრანზაქციას, რათა არავინ დახარჯოს ორჯერ თავისი მონეტები. ყოველი ტრანზაქციის შემდეგ მონეტა უნდა დაუბრუნდეს სერვერს, რათა ახალი მონეტა გამოიცეს. ამ შემთხვევაში მხოლოდ ის გამოცემული მონეტები არის სანდო, რომელიც ცენტრალურმა სერვერმა გამოუშვა და ისინი არ არის დახარჯული ორჯერ

ან მეტჯერ. პრობლემაა ისაა, რომ ამ შემთხვევაშიც მთელი ფულის სისტემის ბედი დამოკიდებულია ცენტრალურ, გარე კომპანიაზე, და ყველა ტრანზაქცია მათი მეშვეობით უნდა იქნას შესრულებული ისევე, როგორიც, მაგალითად, ბანკის მიერ. ჩვენ გვჭირდება, ვიპოვოთ რაიმე მეთოდი, რათა მიმღებს შეეძლოს, იცოდეს, დახარჯა თუ არა წინა მესაკუთრემ თავისი მონეტები, ან გამოიყენა თუ არა ორჯერ თავისი ციფრული ხელმოწერა. ჩვენი მიზნების მისაღწევად უბრალოდ ვთვლით სულ ყველაზე პირველ ტრანზაქციას, როგორც ნამდვილს, ხოლო ამის შემდგომ არ ვაქცევთ ყურადღებას იმას, დაეხარჯა თუ არა ტრანზაქციებს მონეტები ორმაგად. ერთადერთი გზა ტრანზაქციების ნამდვილობის დასადასტურებლად ისაა, ვიცოდეთ ქსელის ყველა ტრანზაქცია. ცენტრალურ სერვერზე დაფუძნებულ მოდელში სერვერმა იცის ყველა ტრანზაქცია და ამის მიხედვით წყვეტს, თუ რომელი გატარდა პირველად. ამ მიზნის მისაღწევად ოპერაციები საჯაროდ უნდა გამოცხადდეს, რათა გამოირიცხოს სანდო მხარის საჭიროება. ჩვენ გვჭირდება, რომ სისტემის მონაწილეები დაეთანხმონ იმ ტრანზაქციების თანმიმდევრობის ერთიან ისტორიას, რომელიც მათ შეასრუ-ლეს. მიმღებს სჭირდება მტკიცებულება, რომ თითოეული

ტრანზაქციის დროს, ნოდების უმრავლესობა თანხმდებოდეს, თუ რომელი ოპერაცია გატარდა პირველი.

**რა არის ბლოკჩეინი**

ბლოკჩეინი, ეჭვგარეშეა, რომ გენიალური გამოგონებაა - სატოში ნაკამოტოს სახელით ცნობილი ადამიანის (ან ადამიანების ჯგუფის) შემოქმედება. მაგრამ ამის შემდეგ, ის საკმაოდ განვითარდა და მთავარი კითხვა, რაც უკვე თითქმის ყველას უჩნდება, შემდეგია: რა არის ბლოკჩეინი?

ბლოკჩეინის ტექნოლოგია ახალი ინტერნეტის მთავარი ღერძია, რომელიც ციფრულ ინფორმაციას საშუალებას აძლევს გავრცელდეს, მაგრამ არ იყოს კოპირებული. ის თავდაპირველად ციფრული ვალუტის, ბიტკოინისთვის, შეიქმნა, მაგრამ ამჟამად ბლოკჩეინი  სხვა გამოყენების გზებსაც ეძებს.

ბიტკოინს ციფრულ ოქროსაც უწოდებენ და საკმაოდ საფუძვლიანადაც. დღევანდელი მონაცემებით, ვალუტის ჯამური ღირებულება 180 მილიარდ ამერიკულ დოლარს აღემატება, ბლოკჩეინს კი შეუძლია, სხვა ტიპის ელექტრონული ვალუტის შექმნაც. ინტერნეტის (ან თუნდაც მანქანის) მსგავსად, შენ არ გჭირდება იცოდე, თუ როგორ მუშაობს ბლოკჩეინი იმისათვის, რომ მისით ისარგებლო. მიუხედავად ამისა, ამ ახალი ტექნოლოგიის შესახებ მცირე ინფორმაციაც კი გვაჩვენებს, თუ რატომაა ის რევოლუციური. იმედი გვაქვს, ისიამოვნებ ამ სტატიით, სადაც ბლოკჩეინის შესახებ უფრო დეტალურად შეიტყობ.

**ფართოდ გავრცელებული მონაცემთა ბაზა**

​

წარმოიდგინეთ ცხრილი, რომლის ათასობით ეგზემპლიარიც მთელს კომპიუტერების ქსელსაა მოდებული. ახლა კი წარმოიდგინეთ, რომ ეს ქსელი მუდმივად ანახლებს ჩვენს ცხრილს და შენ ბლოკჩეინის შესახებ ზოგადი წარმოდგენა უკვე გექნება.

ბლოკჩეინზე ჩაწერილი ინფორმაცია არსებობს, როგორც გაზიარებული და ერთმანეთთან შეთანხმებული მონაცემთა ბაზა.

ბლოკჩეინის მონაცემთა ბაზა არ არის ერთ ადგილას შენახული, რაც ნიშნავს, რომ ყველა მასში შემავალი მონაცემი ნამდვილად საჯაროა და ადვილად შემოწმებადი. არ არსებობს ამ ინფორმაციის ცენტრალიზებული ვერსია, რომელშიც ჰაკერს შეუძლია შეაღწიოს. ის ერთბაშად მილიონობით კომპიუტერს მასპინძლობს და მისი მონაცემები ხელმისაწვდომია ყველასთვის, ვისაც ინტერნეტი აქვს.

იმისათვის, რომ საკითხს უფრო ჩავუღრმავდეთ გუგლის ცხრილის ანალოგიის მოშველიებით, გთავაზობთ შემდეგ მონაკვეთს ბლოკჩეინის სპეციალისტისაგან:

​

**ბლოკჩეინი როგორც "Google Docs"**

**​**

„დოკუმენტების გაზიარების ტრადიციული მეთოდია ვორდის ფაილის მეორე პირისთვის გაგზავნა და თხოვნა, რომ ფაილს გადახედოს და კომენტარები დაურთოს. მთავარი პრობლემა ისაა, რომ შენ უნდა დაელოდო, სანამ დოკუმენტის ასლს გადმოგიგზავნიან, რადგან არ შეგიძლია მისი ნახვა ან შესწორება, სანამ მეორე ადამიანი თავის საქმეს არ მორჩება. დღეს, მონაცემთა ბაზები ასე მუშაობს. ორ მფლობელს არ შეუძლია ერთდროულად ერთ ფაილზე მუშაობა. ასე ინარჩუნებენ ბანკები ფულისა და გადარიცხვების ბალანსს; ისინი ბლოკავენ წვდომას, სანამ გადარიცხვას აწარმოებენ, შემდეგ  ანახლებენ მონაცემებს და კვლავ ხსნიას წვდომას.

ბლოკჩეინის იდეის გასაგებად მოვიშველიოთ Google Docs-ი, რომელიც ზემოთ ხსენებულ ორივე ადამიანს (მასზე წვდომა აქვს) საშუალებას აძლევს დოკუმენტი დაამუშაონ ერთდროულად - პარალელურ რეჟიმში, ორივე მათგანს შეუძლია მონაცემები შეცვალოს და ორივე მათგანისთვის ხილულია ეს დოკუმენტი.

ახლა წარმოიდგინე ის იურიდიული დოკუმენტები. იმის მაგივრად, რომ ერთმანეთს გადააწოდონ მონაცემები, თავგზა აერიოთ ამდენ ვერსიებში და განახლებული საბუთი გამოეპაროთ ან დაკარგონ, რატომ არ შეიძლება ყველა ბიზნეს დოკუმენტი იყოს განაწილებული და არა ხელიდან ხელში გადაცემული? რამდენი კონტრაქტი იქნებოდა იდეალური ასეთ შემთხვევაში?!

შენ არ გჭირდება ბლოკჩეინი, რათა გააზიარო დოკუმენტები, მაგრამ გაზიარებული დოკუმენტების ანალოგი საკმაოდ ახლოსაა ბლოკჩეინის იდეასთან.“ -                        *ვილიამ მოუგაირი, რისკების მრჩეველი, ოთხგზის ინტერპრენუერი, მარკეტინგის სპეციალისტი, სტრატეგი და ბლოკჩეინის სპეციალისტი.*

***​***

ვინ გამოიყენებს ბლოკჩეინს?

​

შენ არ გჭირდება ბლოკჩეინის შესახებ ყველა დეტალის ცოდნა, რათა ის შენს ცხოვრებაში გამოსადეგი იყოს.

ამჟამად, ფინანსური ოპერაციები, ბლოკჩეინ ტექნოლოგიას საკმაოდ კარგ გამოყენების შესაძლებლობებს სთავაზობს.  მაგალითად, საერთაშორისო ფულადი გადარიცხვები. მსოფლიო ბანკი აცხადებს, რომ 2015 წელს დაახლოებით 430 მილიარდი ამერიკული დოლარის ოდენობის ტრანზაქცია შესრულდა და ყველა მათგანი ფინანსური შუამავლის დახმარებით. ბლოკჩეინს აქვს იმის პოტენციალი, რომ ამ ტრანზაქციებში ფინანსური შუამავალი ამოაგდოს.

​

ბლოკჩეინი და გაზრდილი უსაფრთხოება

​

მთელს ქსელში მონაცემების შენახვით ბლოკჩეინი ამცირებს ისეთ რისკებს, რომელსაც მონაცემების ერთ ცენტრალურ ადგილას შენახვა იწვევს.

მისი ქსელი გამოირჩევა ცენტრალიზაციის არ არსებობით, რაც ჰაკერებისგან თავდაცვის გარანტიას იძლევა. დღევანდელ ინტერნეტს უსაფრთხოების პრობლემები აქვს და ეს ყველასთვისაა ცნობილი. ჩვენ ყველანი ვეყრდნობით „მომხმარებლის სახელი/პაროლი“ სისტემას ჩვენი პირადი ინფორმაციის დაცვისთვის. ბლოკჩეინი კი შიფრის ტექნოლოგიას იყენებს.

მისი საფუძველი ე.წ. საჯარო და პირადი „გასაღებებია“. „საჯარო გასაღები“ (გრძელი, შემთხვევით შერჩეული რიცხვებისა და ლათინური ასოების რიგი) მომხმარებლის მისამართია ბლოკჩეინზე. ბიტკოინები, რომლებიც ქსელში იგზავნება, ამ მისამართებზეა მიმაგრებული. „პირადი გასაღები“ პაროლივითაა, რომლითაც მფლობელი საკუთარ ანგარიშში შედის. განათავსე შენი მონაცემები ბლოკჩეინზე და ის გაყალბებისგან დაცული იქნება. მიუხედავად ამისა, შენი ციფრული აქტივების დაცვა პირადი გასაღების დაცვასაც მოითხოვს, რადგან თუ ვთქვათ ბიტკოინი მოგპარეს ვერც ვერსად იჩივლებ და ვერც ვერაფრით ვერ დაიბრუნებ მას.

**თავი 2. თანამედროვე კრიპტოვალუტების მახასიათებლები.**

არაინფლაციურობა.ხელმისაწვდომობა. გლობალურობა. ანონიმურობა. ღია საწყისი კოდი. ერთრანგიანობა. დეცენტრალიზაცია

**რა არის ბიტკოინი**

საინტერესოა, რომ ბიტკოინი პირველად 2008 წელს გამოჩნდა, მაშინ, როდესაც „Occupy Wall Street“ - მა დიდ ბანკებს ბრალი დასდო კლიენტების ფულის არასწორად გამოყენებაში, მათ გასულელებაში, სისტემის გაბზარვაში და უზარმაზარი

გადასახადების დაწესებაში. ბიტკოინის შემქმნელებს სურდათ, გამყიდველი პირველ ადგილას დაეყენებინათ, შუამავალის ფუნქცია შეემცირებინათ, საპროცენტო ხარჯები გაეუქმებინათ და სავაჭრო ოპერაციები გამჭირვალე გაეხადათ, რათა კორუფცია ადვილად მოესპოთ და გადასახადები შეემცირებინათ. მათ შექმნეს დეცენტრალიზებული სისტემა, სადაც შეგიძლია, თავად აკონტროლო საკუთარი კაპიტალი და იცოდე, რა ხდება მის შიგნით.

რა არის ბიტკოინი**?** მარტივად რომ ვთქვათ, ბიტკოინი არის ელექტრონული ვალუტა. შენ შეგიძლია ჩაატარო ტრანზაქციები ჩეკით, საბანკო ბარათით, ან ნაღდი ფულით. ბიტკოინის (ან

BTC) გამოყენება შესაძლებელია ხელმოწერით, რაც 16 სიმბოლოსაგან შედგენილი გრძელი კოდია. გამყიდველი კოდს თავისი სმარტფონით შიფრავს, რათა შენი კრიპტოვალუტა მიიღოს. სხვა კუთხით რომ შეხედო, კრიპტოვალუტა არის ციფრული ინფორმაციის გაცვლა, რაც საშუალებას გაძლევს, იყიდო ან გაყიდო სხვადასხვა საქონელი და მომსახურება. ტრანზაქცია უსაფრთხოებასა და ნდობას ისეთი კომპიუტერული ქსელით მოიპოვებს, რომელიც ძალიან ჰგავს სკაიპს, ან ბიტ-ტორენტს, ფაილების გაზიარების სისტემას.

**ბიტკოინის ტრანზაქციების მახასიათებლები:**

1. შეუქცევადი: დადასტურების შემდეგ, სავაჭრო ოპერაციის შებრუნება არავის შეუძლია. და არავინ ნიშნავს არავის! ვერც შენ, ვერც შენი ბანკი, ვერც ამერიკის პრეზიდენტი, ვერც სატოში და ვერც შენი მაინერი ოპერაციას ვერ შეაბრუნებს. თუ

ფულს გააგზავნი, შენ მას აგზავნი. არავის შეუძლია დაგეხმაროს, თუ ქოინებს მატყუარას გადაურიცხავ, ან თუ ჰაკერი მოიპარავს მას შენი კომპიუტერიდან.

2. ფსევდონიმური: არც ერთი ოპერაცია, ან ანგარიში ნამდვილი სამყაროს იდენტობებს არ უკავშირდება. შენ იღებ/გზავნი ბიტკოინებს, ე.წ. მისამართზე, რომელიც შემთხვევითად ამორჩეული 30 სიმბოლოსაგან შედგება. აქედან გამომდინარე, თუ ტრანზაქციების მოცულობის და სიხშირის ანალიზი

ძირითადად შესაძლებელია, ეს არ ნიშნავს, რომ აუცილებლად არსებობს მათი რეალურ სამყაროს იდენტობებთან დაკავშირების საჭიროება ან შესაძლებლობა.

3. სწრაფი და გლობალური: ტრანზაქცია ქსელში თითქმის იმწამსვე ვრცელდება და რამდენიმე წუთში დასტურდება. ვინაიდან პროცესი გლობალურ ქსელში მიმდინარეობს, შენი ფიზიკური ადგილმდებარეობა არაფერს წყვეტს.

მნიშვნელობა არ აქვს მე ბიტკოინს მეზობელს გავუგზავნი, თუ ვიღაცას დედამიწის მეორე ბოლოში.

4. უსაფრთხო: ბიტკოინის ფულადი სახსრები ჩაკეტილია საზოგადო გასაღებით - „ cryptography system“. მხოლოდ პირადი გასაღების მქონე პირს შეუძლია კრიპტოვალუტის გადაგზავნა. ძლიერი კრიპტოგრაფი და დიდი რიცხვების მაგიური შესაძლებლობები პროგრამის გატეხვას შეუძლებელს ხდის. ბიტკოინის მისამართი უფრო დაცულია, ვიდრე „Fort Knox“.

5. ნებართვის გარეშე: შენ არ გჭირდება ვინმეს ნებართვა, რათა კრიპტოვალუტა გამოიყენო. ეს უბრალო პროგრამაა, რომლის გადმოწერაც ყველას შეუძლია უფასოდ. დაინსტალირების შემდეგ, შენ შეგიძლია, მიიღო და გააგზავნო ბიტკოინები, ან ნებისმიერი სხვა კრიპტოვალუტა. არავის შეუძლია შენი

შეჩერება. აქ მეკარე არ არსებობს.

**როგორ მუშაობს ბიტკოინი?**

ტექნიკურ დეტალებში ჩაძიების გარეშე რომ ავხსნათ, ბიტკოინი მუშაობს გადანაწილებულ საზოგადეობრივ დავთარზე, რომელსაც ბლოკჩეინი ეწოდება. ბლოკჩეინში ყველა დადასტურებული სავაჭრო ოპერაცია ე.წ. „ბლოკის“ სახითაა

წარმოდგენილი. როგორც კი თითოეული ბლოკი სისტემას დაემატება, ის გადაეცემა ქსელში ჩართულ ყველა კომპიუტერს დამტკიცებისთვის. ამ გზით, ყველა მომხმარებელი ინფორმირებულია თითოეული გადარიცხვის შესახებ, რაც

ქურდობისა და ორმაგი დახარჯვისაგან (როდესაც ვიღაც ორჯერ ხარჯავს ერთი და იგივე ვალუტას) თავის დაცვაში გვეხმარება. პროცესი ასევე ხელს უწყობს ბლოკჩეინს ნდობის მოპოვებაში.

**თავი 3. როგორ მუშაობს ბლოკჩეინ ტექნოლოგია**

რის გაკეთება შეუძლია ბლოკჩეინს. ტრანზაქცია, ბლოკი და ბლოკების ჯაჭვი.

არსებობს სამი ძირითადი ტექნოლოგია, რომლებზეც ბლოკჩეინია დაფუძნებული.

არც ერთი ამ ტექნოლოგიათაგან არ წარმოადგენს სიახლეს. ახალი არის მხოლოდ მიდგომა მათი გამოყენებისადმი.

ეს ტექნოლოგიებია: 1) კრიპტოგრაფიული ჰეშები, 2) გადანაწილებული ქსელი საერთო საბუღალტრო წიგნაკით (დავთარით) და 3) სტიმული ქსელის ტრანზაქციების, ჩანაწერებისა და უსაფრთხოებისათვის (იგივე პროტოკოლი).

ქვევით განხილულია ამ ტექნოლოგიების ერთობლივი მოქმედება, რათა უზრუნველყოფილი იყოს ციფრული ურთიერთობების უსაფრთხოება.

​

**კრიპტოგრაფიული გასაღები**

​

ორ ადამიანს სურს, ინტერნეტით განახორციელოს ტრანზაქცია. თითოეულ მათგანს აქვს პირადი და საჯარო გასაღები.

**პირადობა**

**​**

საკუთრების მყარი კონტროლი არაა საკმარისი ციფრული ურთიერთობების უსაფრთხოებისათვის. მართალია, იდენტიფიკაციის საკითხი მოგვარებულია, მაგრამ საჭიროა ამის კომბინაცია  ტრანზაქციების დადასტურებასა და ნებართვებთან (ავტორიზაციასთან).

ბლოკჩეინის შემთხვევაში ეს იწყება გადანაწილებული ქსელით.

​

**გადანაწილებული ქსელი**

**​**

გადანაწილებული ქსელის სარგებელი და საჭიროება შეიძლება აღვიქვათ შემდეგი მაგალითით: „თუ ტყეში ხე წაიქცა“.

როცა ტყეში ხე წაიქცევა და ამას კამერა დააფიქსირებს, შეგვიძლია დარწმუნებულები ვიყოთ ფაქტის სინამდვილეში. დამატებითი, გარემო ფაქტორების გაურკვევლობის შემთხვევაშიც კი გვაქვს ვიზუალური მტკიცებულება.

ბიტკოინ ბლოკჩეინის მთავარი თვისება ისაა, რომ არის ფართო ქსელი საკონტროლო მოწყობილობებით (კამერის მსგავსად), რომლებიც თანხმდება ერთსა და იმავე დროს გარკვეული ფაქტის არსებობის შესახებ. კამერების ნაცვლად გამოიყენება მათემატიკური ვერიფიკაციები.

მოკლედ რომ ვთქვათ, ქსელის სიდიდე მნიშვნელოვანია მისი საიმედოობისათვის.

ბიტკოინ ბლოკჩეინი არის საკმაოდ ვრცელი და აერთიანებს უამრავი კომპიუტერის ენერგიას - სწორედ ესაა მისი ძირითადი და ყველაზე მნიშვნელოვანი ღირსება. დღეისათვის, ბიტკოინის ბლოკჩეინის სიმძლავრე შეადგენს 12 მილიონ ტერაჰაშს წამში (TH/s), რაც უფრო მეტია ვიდრე, ერთად აღებული მსოფლიოს უდიდესი 10,000-მდე ბანკის კომპიუტერული სიმძლავრე.

**​**

**ჩანაწერების სისტემა**

კრიპტოგრაფიული გასაღების ამ ქსელთან კომბინირებისას აღმოცენდება ციფრული ურთიერთქმედების ძალზე სასარგებლო ფორმები. პროცესი იწყება A-ს მიერ პირადი გასაღების მიღებით, კეთდება გარკვეული ფორმის განაცხადი - ბიტკოინის შემთხვევაში იგზავნება კრიპტოვალუტის ჯამი - და ემაგრება B-ს საჯარო გასაღებს.

​

**პროტოკოლი**

ხელმოწერების, დროითი შტამპისა  და შესაბამისი ინფორმაციის მომცველი ბლოკი გადაეცემა ქსელში ჩართულ ყველა პირს.

**ქსელის სერვისის პროტოკოლი**

**​**

ინფორმაციის ქსელში განთავსების უკეთ გასააზრებლად, დავუბრუნდეთ მანამდე მოყვანილ, ტყეში ხის წაქცევის მაგალითს: რეალურად, ტყეში ხის წაქცევის ფაქტმა შეიძლება შემდეგი კითხვა გააჩინოს: რატომ უნდა იყოს მილიონობით კომპიუტერი კამერებით ხის შესაძლო დაცემის მოლოდინში? სხვა სიტყვებით რომ ვთქვათ, როგორ უნდა მოიზიდოს ამ ქსელის უსაფრთხოებისათვის და გასამართად საჭირო კომპიუტერული ენერგია?

ღია, საზოგადო ბლოკჩეინებისთვის ეს გულისხმობს მაინინგს (მოპოვებას).

ბლოკჩეინის შემთხვევაში, ქსელის სერვისის უზრუნველყოფისასთვის არსებობს ჯილდო ერთ-ერთი კომპიუტერისთვის. საზოგადოების სერვისის გასა-უმჯობესებლად ადამიანის პირადი ინტერესია გამოყენებული.

ბიტკოინის შემთხვევაში, პროტოკოლის მიზანია, აღმოფხვრას ერთი ბიტკოინით ერთსა და იმავე დროს სხვადასხვა ტრანზაქციის შესრულების შესაძლებლობა.

აქვე არის განხილული ბიტკოინის მოქმედება, როგორც ოქროსი, საკუთრების. ბიტკოინები და მათი ძირითადი ერთეულები (satoshis) უნდა იყოს უნიკალური და უნდა ჰქონდეს ფასი. ამის მისაღწევად, ქსელში ფიქსირდება და ინახება თითოეული ბიტკოინის გამოყენების ისტორია, რომელიც ეფუძნება სამუშაოს შესრულების მტკიცებულების (Proof-of-work) მათემატიკური ალგორითმის ამოხსნას.ვინც პირველი ამოხსნის ჰაშს, ქსელს ხმას აწვდენს CPU-ს ენერგიით, ქსელში ჩართული პირები კი ეთანხმებიან ახალ ბლოკებს ან უარყოფენ მიუღებელ ბლოკებს. როდესაც მაინერების უმეტესობა მიაღწევს შეთანხმებას, ჯაჭვს ემატება ახალი ბლოკი და ბლოკიჩეინში ბლოკის დამმატებელი იღებს 12,5 ბიტკოინს ჯილდოდ. ეს ბლოკი  შეიცავს დროით შტამპს და შეიძლება შეიცავდეს მონაცემებს და შეტყობინებებს. .ქვევით განხილულია ბლოკჩეინი:

ტიპი, რაოდენობა და დადასტურება შეიძლება განსხვავდებოდეს ბლოკჩეინების მიხედვით. ეს დამოკიდებულია ბლოკჩეინის პროტოკოლზე, ანუ რა არის მიჩნეული სწორ და რა - არასწორ ტრანზაქციად, ან მართებულად შეიქმნა თუ არა ახალი ბლოკი. დადასტურების პროცესი შეიძლება სპეციფიკური იყოს თითოეული ბლოკჩეინი-სთვის. ნებისმიერი საჭირო წესი და სტიმული შეიძლება შეიქმნას მაშინ, როცა საკმა-რისი რაოდენობის ქსელში ჩართული პირები მიაღწევენ შეთანხმებას იმასთან დაკავ-შირებით, თუ როგორ უნდა დადასტურდეს ტრანზაქციები.ეს არის მომხარებლის არჩევანი და ხალხი მხოლოდ ახლა იწყებს სტრუქტურის გამოცდას.

ჩვენ ამჟამად ვიმყოფებით ბლოკჩეინის განვითარების პერიოდში, რომლის დროსაც ბევრი ექსპერიმენტი ტარდება. დღეისათვის არსებული დასკვნებით ბლოკჩეინის პროტოკოლების სრულყოფილად გააზრება და გამოყენება ჯერ კიდევ წინ გველის.

**თავი 4. ჰეშირება**.

ჰეშ-ფუნქცია. მერკლის ხე. ჰეშ-კრიპტოგრაფია. განსხვავება შიფრაცია და ჰეშირებას შორის

ტრადიციულ მონეტარულ სისტემაში, სახელმწიფო (ან ცენტრალური ბანკი) ბეჭდავს ახალ კუპიურებს, როდესაც ეს მას სჭირდება. ბიტკოინის შემთხვევაში კი, ფული საერთოდ არ იბეჭდება - ხდება მისი აღმოჩენა. მთელი მსოფლიოს მასშტაბით, ქსელში ჩართული კომპიუტერები „მოიპოვებენ“ მონეტებს ერთმანეთთან შეჯიბრის პრინციპით.ადამიანები განუწყვეტლივ უგზავნიან ბიტკოინს ერთმანეთს ქსელის მეშვეობით. მაგრამ, თუ ვინმე ამ ყველაფერს არ აღრიცხავს, ვერავინ შეძლებს გაიგოს, რეალურად ვინ რამდენი გადაიხადა  და ვის რამდენი ბიტკოინი აქვს. ამ ყველაფრის აღრიცხვისათვის, ბიტკოინი აწარმოებს ტრანზაქციების სიას, რომელიც დაგროვდა გარკვეული დროის განმავლობაში და თავს უყრის მათ ერთ ბლოკში. მომპოვებლის, ანუ მაინერის, ფუნქციაა, დაადასტუროს ეს ტრანზაქციები და ჩაწეროს ისინი საერთო დავთარში, რომლის ასლიც ყველა ქსელში ჩართულ კომპიუტერში ინახება.

​

**რაში გამოიყენება ჰეში**

**​**

ზემოთხსენებული საერთო დავთარი არის ბლოკების გრძელი სია, რომელსაც ბლოკჩეინს უწოდებენ. მისი გამოყენება შესაძლებელია იმისათვის, რომ ვნახოთ თითოეულ მისამართზე ბიტკოინების შემოსავლებისა და ხარჯების ისტორია. ყოველი ახალი ტრანზაქციის შექმნით, ინფორმაცია ამ დავთარს ემატება. ამგვარად იქმნება ძალიან გრძელი და მზარდი სია, სადაც ყველა ტრანზაქციის შესახებ ინფორმაცია არის მოცემული, რომელიც ბიტკოინის ბლოკჩეინზე ოდესმე განხორციელებულა. ქსელში ჩართულ ყველა მონაწილეს ეგზავნება ყოველი ტრანზაქციის შესახებ ინფორმაცია და მათ ხელთ არსებული დავთრის ასლი ავტომატურად განახლებადია.

ცხადია, ეს დავთარი ძალიან სანდო უნდა იყოს. ვინაიდან იგი ციფრულად ინახება, ის დაცული უნდა იყოს ჰაკერული თუ სხვა ტიპის შემოტევებისგან და არ უნდა არსებობდეს მასში წარსული მონაცემების შეცვლის შესაძლებლობა. სწორედ ამ მიზანს ემსახურებიან მომპოვებლები.

როდესაც ხორციელდება ბიტკოინ ტრანზაქცია, მაინერები იღებენ ამ ტრანზაქციის შესახებ ინფორმაციას, უსადაგებენ მას მათემატიკურ ფორმულას და გარდაქმნიან ამ მათემატიკური ფუნქციის ამონახსნად.  ეს ამონახსნი შემთხვევითი თანმიმდევრობით დალაგებული ასოებისა და ციფრების კომბინაციაა, რომელსაც ჰეში ეწოდება. ეს ჰეში დროის ნებისმიერ მომენტში ინახება ბლოკთან ერთად ბლოკჩეინის ბოლო ჩანაწერში.

ჰეშებს საკმაოდ საინტერესო თვისება აქვთ. ნებისმიერი ინფორმაციისთვის ჰეშის პოვნა შედარებით მარტივია, მაგრამ შეუძლებელია ამონახსნიდან ვიპოვოთ, რა იყო თავდაპირველი ინფორმაცია.  ამასთან, ყოველი ჰეში (ამონახსნი) უნიკალურია: თუ ბლოკში შეიცვლება ძალიან უმნიშვნელო ინფორმაციაც კი, მისი ჰეში აბსოლუტურად განსხვავებული გახდება.

მაინერები ჰეშის გამოსათვლელად არა მხოლოდ კონკრეტულ ბლოკში მოცემულ ინფორმაციას ითვალისწინებენ, არამედ წინა ბლოკის ჰეშსაც - სწორედ აქედან მოდის სახელი ბლოკჩეინი - ანუ ბლოკების ჯაჭვი. იმის გამო, რომ ყოველი ახალი ჰეში მოიცავს წინა ბლოკის ჰეშსაც, შეგვიძლია შევხედოთ მას, როგორც პლომბს და თუ ერთი პლომბი მაინც გაიხსნება, ეს აისახება ყოველ მის შემდგომ ბლოკზე, რადგან თითოეული მათგანის ჰეში განახლებული ინფორმაციის საფუძველზე იქნება დასათვლელი. თუ ვინმე გადაწყვეტს, რომ შეცვალოს ან გააყალბოს ტრანზაქცია, რომელიც უკვე ბლოკჩეინში არის ჩაბეჭდილი, მისი ჰეში შეიცვლება. ასევე შეიცვლება ყველა მისი შემდეგი ბლოკის ჰეში. შესაბამისად, უახლესი ტრანზაქციის / ბლოკის ჰეში განსხვავებული იქნება ქსელში ჩართული ყველა მონაწილის დავთარში მოცემული მაჩვენებლისგან და მთელი ქსელი მიხვდება, რომ ეს ბლოკი გაყალბებულია.

​

**ფულადი სარგებელი**

**​**

ჩვენ უკვე განვიხილეთ, როგორ ილუქება ბლოკები. ყველა ქსელში ჩართული კომპიუტერი ეჯიბრება ერთმანეთს ამის გაკეთებაში და ამისათვის ისინი იყენებენ სპეციალურად ბიტკოინის ბლოკჩეინისათვის დაწერილ პროგრამას. როდესაც ვინმე წარმატებით ამოხსნის ჰეშს, ჯილდოდ იღებს 12,5 ბიტკოინს. ყველა ქსელში ჩართული კომპიუტერი ხედავს და ადასტურებს ამას. სწორედ ასე ხდება ნოდების წახალისება, რათა მათ გააგრძელონ მოპოვება და ტრანზაქციების დადასტურება.

ამ ყველაფრის პრობლემა იმაში მდგომარეობს, რომ ჰეშის ამოხსნა ძალიან რთულია, შესაბამისად, კომპიუტერული ენერგია, რომელიც გამოიყენება ბიტკოინების მოსაპოვებლად, მუდმივად იზრდება. ალგორითმის ამოხსნა მარტივი, რომ ყოფილიყო ეს გამოიწვევდა ბიტკოინების მარაგის სწრაფად ამოწურვას, რადგან ნოდები შეძლებდნენ წამში ათასობით ჰეშის ამოხსნას და ამისათვის მიიღებდნენ ბიტკოინებს. ამიტომაც ბიტკოინის პროტოკოლი (პროგრამა)„სამუშაოს შესრულების მტკიცებულების“ (Proof of Work) შემოტანით მიზანმიმართულად ართულებს მოპოვების პროცესს.

ბიტკოინის პროტოკოლში ჰეშს კონკრეტული მახასიათებლები უნდა ჰქონდეს, მაგალითად იგი რამოდენიმე 0-იანით უნდა იწყებოდეს, მაგრამ მის ამოხსნამდე იმის განსაზღვრა, თუ როგორი იქნება ჰეში, შეუძლებელია. ყოველი ახალი, თუნდაც მიზერული ინფორმაციის ცვლილებით განახლებული ჰეში აბსოლუტურად იცვლება.

ამ ყველაფრის გარდა, ბიტკოინის პროგრამაში გაჩნდა შემთხვევითი სიდიდე, „ნონსი“, რომელიც ასევე მონაწილეობს ბლოკის შექმნაში. თუ ტრანზაქციის ჰეში არ აკმაყოფილებს გარკვეულ მოთხოვნებს (მაგალითად იმას, რომ არ იწყება რამოდენიმე 0-იანით), ჩნდება ისეთი „ნონსის“ პოვნის საჭიროება, რომელიც ამონახსნს მოარგებს აღნიშნულ ფორმატს. ვინაიდან ნონსი შემთხვევითი სიდიდეა და არ ექვემდებარება ლოგიკურ ახსნას, მაინერები ცდილობენ, იპოვონ საჭირო ნონსი უამრავი ვარიანტის ცდით.

აი, ასე ხდება ბიტკოინის მოპოვება!

დღესდღეობით პოპულარული ციფრული ხელმოწერის

სქმებია: RSA,DSA,ECDSA ისინი ძირითადად ეყრდნობიან რთული რიცხვების ფაქტორიზაციასა და დისკრეტული ალგორითმის გამოთვლის სირთულეს , მეცნიერთა ვარაუდით კი უახლოეს მომავალში კომპიუტერის სისწრაფე საგრძნობლად გაიზრდება და კვანტური კომპიუტერი შიფრის გასაღებთა სიმრავლეს ძალისმიერი მეთოდით გადაარჩევს.კვანტურ კომპიუტერებს შეეძლებათ მარტივად გამო- იანგარიშონ მარტივ რიცხვებზე ფაქტორიზაციის ოპერაციები , სწორედ ამ პრობლემაზე არის დაფუძნებული RSA კრიპტო სისტემა , ეს კრიპტო სისტემა არის დღესდღეობით ყველაზე მეტად გავრცელებული მსოფლიოში, აქედან გამომდინარე მისი გატეხვა გამოიწვევს თითქმის ყველა პროდუქტის გატეხვას.სწორე ამიტომ ჩვენ მოგვიწევს შევქმნათ და შემდგომში დავხვეწოთ ალგორითმი,რომელიც შემდგომში

საშუალებას მოგვცემს განვავითაროთ კვანტური კომპიუტერის შეტე-ვებისადმი მედეგი კრიპტოსისტემა[1]. კვანტური კომპიუტერის შეტევების მიმართ ერთ-ერთი ყველაზე კრიპტომედეგი

ხელმოწერის სქემაა **მერკლის ხელმოწერის** სქემა, რომელიც თავის მხრივ მოიცავს secure hash function და one time signature შესაბამისად დაცული და უსაფრთხო კრიპტოსისტემის შესაქმნელად მნიშ-ვნელოვანია ისეთი ხელმოწერის სქემისა და ალგორითმების გამოყე-ნება, რომლებიც უზრუნველყოფენ ოპტიმიზირებული ციფრული ხელმოწერის შექმნას .იმისთვის რომ შევქმნათ კრიპტომედეგი ციფრული ხელმოწერა მნიშვნელოვანია გავითვალისწონოთ: ერთჯერადი ხელმოწერის(one time signature) გასაღებების დაგენერირებისთვის საჭირო დრო და ხელმოწერისა და

ვერიფიკაციისთვის საჭირო დრო.ლამპორტის ხელმოწერის სქემის გამოყენებისას მნიშვნელოვანია შევარჩიოთ ისეთი ცალმხრივი ჰეშ-ფუნქცია, რომელიც უზრუნველყოფს ერთჯერადი ციფრული ხელმო- წერის უსაფრთხოებასა და საიმედოობას.

ლამპორტის ხელმოწერის სქემის გამოყენებისას მნიშვნელოვანი გავითვალისწინოთ , რომ შეტყობინებაზე ხელმოსაწერად გვიწევს დავაგენერიროთ 2k სიგრძის მქონე ჰეშ-მნიშვნელობა როცა, ასე რომ თუ გვინდა ჩვენი ხელომოწერა დაცული და საიმედო იყოს მოგვიწევს დავაგენერიროთ საკმაოდ გრძელი გასაღები და შესაბამისი დოკუმენ-ტის ჰეშ-მნიშვნელობაც საკმაოდ გრძელი და კომპლექსური იქნება. ლამპორტის სქემით დაგენერირებული ღია გასაღები 50-ჯერ დიდია შესაბამისი 1024 ბიტიანი RSA-ას ღია გასაღებზე, ბუნებრივია ასეთი გრძელი და კომპლექსური ხელმოწერის გამოყენება გავლენას იქონიებს თავად პროცესის წარმადობასა და სისწრაფეზე, სწორედ ამიტომ უნდა მოვნახოთ საშუალებას მოგვცემს შევამციროთ გასაღებების სიგრძე და ამავდროულად შევინარჩუნოთ ხელმოწერის დაცულობა და საიმედოობა, სწორედ ამის საშუალებას გვაძლევს ვინტერცის ხელმოწერის სქემა ,რომლის მიხედვითაც ავარჩევთ ერთ რომელიმე შემთხვევით არჩეული სტრიქონს და მისი საშუალებით სიმულაციურად ხელს მოვაწერთ ( one time signature) რამდენიმე ბიტს (n რაოდენობის ბიტს) შეტყობინების ჰეშ-მნიშვნელობიდან.

ერთჯერადი ხელმოწერის სქემის (one-time signature scheme) ერთ-ერთ მთავარ პრობლემას წარმოადგენს ხელმოწერის გასაღებების შენახვა და მართვა. ამიტომ ციფრული ხელმო-წერის გასაღებების შენახვა- გამოყენებისთვის გამოიყენება **მერკლის ხე.** ერთჯერადი ხელმოწერის დროს (One-time signature) ყოველ ჯერზე გვიწევს ახალი ღია გასაღების გამოიყენება და მისი სიგრძეც არის საკმაოდ დიდი , იმისთვის რომ გავხადოთ ერთჯე-რადი ხელმოწერის სქემა (one-time signature) უფრო მოქნილი,სწრაფი და ეფექტური ,საჭიროა გამოვიყენოთ მერკლის ხელმოწერის სქემა,

რომელიც საშუალებას გვაძლევს ხელმოსაწერად გამოვიყენოთ ერთი ღია გასაღები მრავალ დოკუმენტზე ხელისმოსაწერად.რაიმე M შეტყობინებაზე ხელის მოწერისას ვმოქმედებთ შემდეგი თანმიმდევრობით:ჯერ ხელს ვაწერთ M შეტყობინებას

ერთჯერადი ხელმოწერის სქემით და შედეგად მივიღებთ გარკვეულ ხეს, ამის შემდეგ დავამატებთ კიდევ ერთ კვანძს(ფოთოლს) ბინარულ ხის შესაბამის ღია გასაღებს რომელსაც შესაბამისი ადგილი ექნება მერკლის ხეში. იმისათვის რომ

განვსაზღვროთ გზა ჩვენ მიერ დამატებული კვანძიდან მთავარ კვანძამდე უნდა დავადგინოთ იმ კვანძების შვილები(children) , რომელიც მოქცეულია ამ დიაპაზონში, თუ ჩვენ ვიცით რომ Xარის Y-ის შვილი მისი მნიშვნელობის გამოსათვლელად ჩვენ უნდა დავადგინოთ მისი მეზობელი კვანძი იგივე

რომელიც თავის მხრივ მომცემს კვანძის დადგენის საშუალებას მერკლის ხეში ყოველი კვანძის დადგენა შეიძლება მისი შვილი კვანძების (leaf) კონკატენაციის ჰეშ-მნიშვნელობის გამოთვლით. ხოლო ვერსიფიკაციის დროს ხელმომწერმა იცის გასაღები რომლის საშუალებითაც ხელი უნდა მოაწეროს M შეტყობინებას .

მერკლის ხელმოწერის სქემა ისევე როგორც ლამპორტის სქემა 30-ზე მეტი წელია რაც არსებობს ,მაგრამ მისი ოპტიმიზაციისა და კვლევის მცდელობები ბოლო ხუთი წელია რაც აქტიურად გამოჩნდა სამეცნიერო საზოგადოებებში. მერკლის ხელმოწერის სქემის მთავარ უპირატესობას წარმოადგენს ის რომ განსხვავებით სხვა

ხელმოწერის სქემებისგან მისი უსაფრთხეოება და დაცულობა დამოკიდებული არ არის რაიმე მათემატიკური პრობლემის გადაწყვეტაზე , ის დამოკიდებულია ჰეშ-ფუნქციის გაანგარიშებასა და ერთჯერადი ხელმოწერის ოპტიმიზაციაზე, იმ შემთხვევაშიც კი თუ ერთჯერადი ხელმოწერა ან ჰეშ- ფუნქცია კოლიზიამედეგი

არ არის მარტივად შეიძლება მისი შეცვლა. ამ კვლევის ფარგლებში მე დავხვეწე და გავაუმჯობესე ციფრული ხელმოწერის ალგორითმი, რომელიც სტაბილურად იმუშავებს კვანტური კომპიუტერების პლატფორმაზე ,მისი საშუალებით ლამპორტის სქემის საშუალებით ხდება ღია და დახურული გასაღებების გენერირება ხოლო

შემდგომ უშუალოდ მერკლის ხელმოწერის სქემის საშუალებით ხდება ხელის მოწერა და ხელმოწერის ვერიფიცირება, მერკლის სქემის ოპტიმიზაციისას გამოიყენეba tree hash ალგორითმი , რომელიც საშუალებას იძლევა მარტივად და შედარებით ნაკლებ დროში ციფრულად ხელი მოეწეროს დოკუმენტზე.

გენერირებისთვის საჭირო დრო ლამპორტის ალგორითმი ვინტერნიცის

ალგორითმი მერკლის ალგორითმი ხელმოწერის გასაღებების გენერირებისთვის საჭირო დრო 0.0320000648499 0.0250000953674

ამ ეტაპზე არ გამოიყენება მერკლის ხე ხელმოწერისთვის საჭირო დრო

0.0520000648499

0.0350000953684

0.0450000953674

ვერიფიცირებისთვის

საჭირო დრო

0.0620000648499

0.0450000953074

0.0250000953333

**თავი 5. ბლოკჩეინი და მისი ძირითადი თვისებები**.

ბლოკჩეინის განსაზღვრა. დეცენტრალიზაცია. საჯაროობა. ყველა მონაწილის თანხმობა. შუამავლების არ არსებობა

განსხვავება ტრადიციულ მონაცემთა ბაზას და ბლოკჩეინს შორის, პირველ რიგში, სტრუქტურაშია, ანუ ბლოკჩეინი სხვა ტექნოლოგიით არის მოწყობილი. - მსოფლიო ქსელში ჩართული მონაცემთა ბაზა, უმეტესად, სამომხმარებლო სერვერის მოდელზეა დამყარებული. უფლებამოსილ მომხმარებელს თავისი ანგარიშით შეუძლია შეცვალოს მონაცემები, რომლებიც ინახება ცენტრალიზებულ სერვერზე. თუ დედანი შეიცვალა, მომხმარებელი თავისი კომპიუტერით ქსელში შესვლისას, მიიღებს უკვე განახლებულ მონაცემებს. მონაცემთა ბაზის კონტროლი ადმინისტრატორის ხელშია, რაც საშუალებას აძლევს ცენტრალურ ძალაუფლებას, შეინარჩუნოს წვდომა გარკვეულ ინფორმაციაზე.ბლოკჩეინის სტრუქტურა სრულიად განსხვავებულია.

ბლოკჩეინის მონაცემთა სისტემაში თითოეული მომხმარებელი თავად იღებს, გადაამუშავებს და ანახლებს ბაზაში შესულ ცვლილებებს. ქსელში ჩართული ყველა პირი ერთობლივად მუშაობს ერთი შეთანხმების მისაღებად, რათა ქსელის უსაფრთხოება უზრუნველყონ.

ამ განსხვავების გამო ბლოკჩეინი გარკვეული ფუნქციებისთვის უფრო შესაფერი ჩანაწერთა სისტემაა, ხოლო ცენტრალიზებული მონაცემთა ბაზა კი გამოსადეგია სხვა მახასიათებლების გამო.

​

**დეცენტრალიზებული კონტროლი**

​

ბლოკჩეინი საშუალებას აძლევს სხვადასხვა პირებს, რომლებიც ერთმანეთს არ ენდობიან, გააზიარონ ინფორმაცია ცენტრალური ადმინისტრატორის გარეშეც. ტრანზაქციები გადამუშავდება ქსელში ჩართული მომხმარებლების მიერ კონსესუსის მიღწევით, ისე, რომ ყველა წევრი ერთდროულად ქმნის გაზიარებულ ჩანაწერთა სისტემას.

დეცენტრალიზებული სისტემის ღირსება ისაა, რომ თავიდან გვაცილებს ცენტრალიზებული კონტროლის რისკს. ცენტრალიზებულ მონაცემთა ბაზაში საკმარისი წვდომის მქონე ნებისმიერ ადამიანს შეუძლია, გაანადგუროს ან შეცვალოს ინფორმაცია. ამის გამო, მომხმარებლები დამოკიდებულები არიან ადმინისტრატორზე. უმეტესად, ადმინისტრატორს თქვენი ნდობა დამსახურებულიც აქვს. მაგალითად, ბანკებში ხალხის მიერ შეტანილ ფულს არ იპარავენ, უბრალოდ ინახავენ მას პირად მონაცემთა ბაზაში. არსებობს ლოგიკური მიზეზებიც, თუ რატომ უნდა გინდოდეთ ცენტრალიზებული კონტროლი. ცენტრალიზებული კონტროლის სისტემა ქმნის სპეციალობას, ის შეიძლება ადამიანის საქმნიანობა გახდეს.

თუმცა, ცენტრალიზებული ძალაუფლება, როგორიცაა ბანკი, ხარჯავს მილიარდობით დოლარს მონაცემთა ბაზის უსაფრთხოების უზრუნველსაყოფად, რათა ჰაკერებმა ვერ მოახერხონ ბანკის კლიენტების დაზარალება. თუ ცენტრალური ადმინისტრატორები, რომლებსაც ვანდობთ ჩვენს პირად ინფორმაციას, ვერ შეძლებენ მის დაცვას, დავკარგავთ ქონებას.

​

**ბლოკჩეინის მონაცემთა ბაზის ისტორია**

​

ცენტრალიზებული ბაზების უმეტესობაში, ინფორმაცია გარკვეულ მომენტში განახლდება ხოლმე და ინახება. ანუ, ისინი, მეტნაკლებად, დროის რაღაც მონაკვეთში დაფიქსირებული  ფაქტებია.

ბლოკჩეინის ბაზები კი საშუალებას გვაძლევს, ინფორმაცია მუდამ ახლდებოდეს და თან განახლებამდე არსებული მთელი ინფორმაციაც ინახებოდეს. ბლოკჩეინ  ტექნოლოგიით შეიძლება მონაცემთა ისეთი სისტემის შექმნა, რომელსაც საკუთარი ისტორიის შენახვაც შეუძლია. ისინი წარმოდგენილია, როგორც საკუთარი ისტორიის ზრდადი არქივი, რომელიც, პარალელურად, გვიჩვენებს მდგომარებას მიმდინარე დროში.

ამ მონაცემთა ბაზების შესაცვლელად საკმაოდ დიდი ხარჯები იქნებოდა საჭირო, ამიტომაც, ხალხი ბლოკჩეინის სისტემის დანერგვას უკვე გარდაუვლად თვლის. ეს შეგვიძლია მივიჩნიოთ მონაცემთა ბაზის ჩანაწერთა სისტემის გარდაქმნის დასაწყისად.

შესრულება

მართალია, ბლოკჩეინების გამოყენება შეიძლება ჩანაწერთა სისტემად და იდეალურია ტრანზაქციების პლატფორმისთვის, მაგრამ ტრანზაქციების ისეთ ციფრულ ტექნოლოგიებთან შედარებით, როგორებიცაა Visa და PayPal, ბლოკჩეინი ნელია.

მიუხედავად იმისა, რომ ამ თვალსაზრისით ბლოკჩეინის დახვეწა შესაძლებელია, მისი ტექნოლოგია მოითხოვს, გარკვეულწილად, სისწრაფის დათმობას. ბლოკჩეინ ტექნოლოგიის გადანაწილებული ქსელები არ გულისხმობს გადამუშავების ენერგიის გაზიარებას და გაერთიანებას.  მასში ჩართული ყოველი პირი დამოუკიდებლად მუშაობს ქსელში, შემდეგ ჯამდება თითოეულის მიერ შესრულებული სამუშაოს შედეგები და მიიღწევა შეთანხმება, რომ გარკვეული ფაქტი ნამდვილად მოხდა.

მეორეს მხრივ, ცენტრალიზებული მონაცემთა ბაზები უკვე ათწლეულების მანძილზე არსებობს. ისინი უფრო და უფრო ვითარდებოდა ციფრული სამყაროს იმ ინოვაციურ ფორმულასთან ერთად, რომელსაც „მურის კანონი“ ჰქვია.

**კონფიდენციალობა**

​

ბიტკოინის შემთხვევაში, ინფორმაციის წაკითხვა და შეტანა არ კონტროლდება. ყველას შეუძლია ჯაჭვში ბლოკის დამატება და ყველას შეუძლია მისი წაკითხვა.

შეიძლება ისეთი ბლოკჩეინიც შეიქმნას, რომლის შემთხვევაშიც ბლოკების დამატება და მათი ნახვა გაკონტროლდება მონაცემთა ცენტრალიზებული ბაზის მსგავსად. ანუ, ქსელი, ან პროტოკოლი, შეიძლება ისე აეწყოს, რომ მხოლოდ უფლებამოსილ მომხმარებლებს მიუწვდებოდეთ ხელი ინფორმაციაზე.

თუ კონფიდენციალობა ერთადერთი მიზანია და ნდობის ფაქტორი პრობლემას არ წარმოადგენს, მაშინ ბლოკჩეინის სისტემას არანაირი უპირატესობა არ ექნება ცენტრალიზებული ბაზის მიმართ.

ბლოკჩეინზე ინფორმაციის დამალვა დაკავშირებულია კრიპტოგრაგიულ სირთულეებთან და ქსელში ჩართული პირებისთვის დამატებით შრომას გულისხმობს. ამის გასაკეთებლად საუკეთესო გზა მონაცემების მთლიანად პირად ბაზაში შენახვაა, რასაც ქსელთან დაკავშირებაც კი არ სჭირდება.

გაიხსენეთ ყველა მონაცემთა ბაზა, რომლებიც ეთან ჰანტმა ფილმში, „შეუსრულებელი მისია“, გატეხა და შეგექმნებათ წარმოდგენა პირადი ბაზების კონფიდენციალობაზე.

**თავი 6. რატომ უნდა ვისარგებლოდ ბლოკჩეინით და ბიტკოინით.**

ბლოკები. ბლოკის სტრუქტურა. ბლოკის სათაური. ბლოკის იდენტიფიკატორები: ბლოკის სათაურის და ბლოკის სიმაღლის ჰეშირება. საწყისი ბლოკი. ბლოკების გადაბმა ბლოკჩეინის ჯაჭვში. ბლოკების შემოწმება და დადასტურება

როდესაც ხალხმა ამ გამოგონების მნიშვნელობა, მეტნაკლებად, გააცნობიერა, ბლოკჩეინის ტექნოლოგიის ირგვლივ დიდი მღელვარება წარმოიშვა.

ეს, ალბათ, იმიტომ, რომ ძალზე მარტივია ზედაპირულად წარმოვიდგინოთ, თუ როგორ და რაში შეიძლება მისი გამოყენება. უამრავმა ადამიანმა და ორგანიზაციამ გადაწყვიტა, ღრმად შეესწავლა ეს ტექნოლოგია. შესაბამისად, მილიონობით დოლარია დახარჯული ბლოკჩეინის საკვლევად ბოლო რამდენიმე წლის მანძილზე. უამრავი კვლევაა ჩატარებული სხვდასხვა სიტუაციაში ბლოკჩეინის ტექნოლოგიის გამოყენების მართებულობასთან დაკავშირებით.

ბლოკჩეინ ტექნოლოგია გვთავაზობს ისეთ ახალ საშუალებებს ციფრულ სამყაროში იდენტიფიკაციისა და ავტორიზაციისთვის, რომლებიც თავიდან გვარიდებს ცენტრალიზებულ კონტროლს. შედეგად, ყალიბდება ახალი ციფრული ურთიერთობები.

ახალი ციფრული ურთიერთობების ჩამოყალიბებითა და უსაფრთხოების უზრუნველყოფით ბლოკჩეინ რევოლუცია წარმოგვიდგება, როგორც ხერხემალი ინტერნეტ ტრანზაქციებისა და ფასების ურთიერთკავშირისთვის.

ბევრს ვსაუბრობთ იმის შესახებ, თუ როგორ არის ბლოკჩეინი ინტერნეტ ტრანზაქციების ხერხემალი. თუმცა, ამის მიუხედავად, ბლოკჩეინი, პირადი კრიპტოგრაფიული გასაღები და კრიპტოვალუტები ყოველთვის არ არის გამოსავალი არსებული პრობლემების მოსაგვარებლად.

სხვადასხვა ჯგუფებმა შექმნეს არა ერთი ცხრილი, რომლებიც ეხმარება პიროვნებას ან ორგანიზაციას არჩევანის გაკეთებაში ბლოკჩეინსა და სტანდარტულ, ტრადიციულ სისტემას (მონაცემთა ბაზას) შორის. ქვემოთ მოკლედაა განხილული რამდენიმე ფაქტორი, რომელიც მნიშვნელოვანია ძველი და ახალი მეთოდების შედარებისას:

​

**არის თუ არა მონაცემები დინამიური შემოწმებად ისტორიასთან მიმართებით?**

**​**

ქაღალდი, თავისი ბეჭდით ან სხვა ვიზუალური თავისებურებით, რთული გასაყალბებელია. ქაღალდის დოკუმენტები, გარკვეულწილად, მუდმივია ქვაზე გრავიურის მსგავსად.

თუ მონაცემები მუდმივად იცვლება, ტრანზაქციები კი რეგულარულად და ხშირად ხორციელდება, მაშინ ქაღალდი ჩანაწერთა სისტემისათვის ნაკლებად გამოგვადგება. მონაცემების მექანიკურად, ადამიანის მიერ შეყვანასაც აქვს ლიმიტი.

ვინაიდან, მონაცემები და მათი ისტორია მნიშვნელოვანია ციფრული ურთიერთობების დასამყარებლად, ბლოკჩეინი გვთავაზობს მოსახერხებელ ტევადობას მათ შესანახად. იგი საშუალებას იძლევა, მრავალმა სხვადასხვა მონაწილემ შეიტანოს ახალი მონაცემი ჩანაწერთა სისტემაში, რომელსაც მართავს ბევრი სხვა მფლობელიც.

​

**შესაძლებელია მონაცემების ცენტრალური ხელისუფლების მიერ გაკონტროლება? უნდა ხდებოდეს თუ არა ასე?**

**​**

მაინც რჩება ბევრი მიზეზი, თუ რატომ უნდა არეგულირებდეს მესამე პირი გარკვეულ იდენტიფიკაციებსა და ავტორიზაციებს. არსებობს შემთხვევები, როდესაც მესამე პირის მიერ კონტროლი სავსებით მისაღები და ხელსაყრელია. თუ მონაცემთა კონფიდენციალობა ყველაზე მნიშვნელოვანი ასპექტია, არის ინფორმაციის საიდუმლოდ შენახვის გზები ქსელთან დაკავშირების გარეშე.

თუ ანგარიშებისა და სისტემაში შესასვლელი IT ინფრასტრუქტურა არაა საკმარისი ციფრული იდენტურობის უსაფრთხოებისთვის, მაშინ პრობლემა შეიძლება ბლოკჩეინ ტექნოლოგიამ გადაჭრას.

როგორც სატოში ნაკამოტომ თავის პირველად ნაშრომში (["Bitcoin: A Peer-to-Peer Electronic Cash System"](https://bitcoin.org/bitcoin.pdf) ნაშრომის თარგმანი შეგიძლიათ იხილოთ [ბმულზე](https://www.cryptoz.ge/bitcoin-whitepaper)) დაწერა: „გამყიდველები ფრთხილად უნდა იყვნენ მომხმარებელთან, უნდა შეაწუხონ ისინი და მიიღონ მეტი ინფორმაცია, ვიდრე რეალურად სჭირდებათ, რადგან თაღლითობის გარკვეული ალბათობა გარდაუვლადაა მიჩნეული.“

პირადი გასაღების კრიპტოგრაფიით შესაძლებელია ე.წ. „push“ ტრანზაქციების განხორციელება. ეს არ მოითხოვს ცენტრალიზებულ სისტემებს და დამუშავებულ ანგარიშებს, რომლებიც გამოიყენება ციფრული ურთერთობების დასამყარებლად. ვინაიდან მცირე ზომის ფინანსური ტრანზაქციების უსაფრთხოებისთვის ასეთი მონაცემთა ბაზა მილიონობით დოლარს საჭიროებს, გამოსავალი სწორედ ბლოკჩეინი შეიძლება იყოს.

​

**არის თუ არა ტრანზაქციის სიჩქარე ყველაზე მნიშვნელოვანი ფაქტორი?**

**​**

მოითხოვს თუ არა ეს მონაცემთა ბაზა მილიწამებში მაღალეფექტურად შესრულებულ ტრანზაქციებს?).თუ  მაღალ დონეზე მილიწამებში შესრულებული ტრანზაქცია გჭირდებათ, ტრადიციულ ცენტრალიზებულ სისტემას მიმართეთ. ბლოკჩეინი, როგორც მონაცემთა ბაზა, ნელია და ინფორმაციის შენახვისთვის გარკვეული საფასური არსებობს - ჯაჭვის თითოეული ბლოკის გადამუშავება (მაინინგი). სამომხმარებლო სერვერის მოდელზე დამყარებული ცენტრალიზებული მონაცემთა სისტემები უფრო სწრაფი და იაფია... ჯერჯერობით.

მოკლედ, ჯერ კიდევ არ ვიცით სრულყოფილად ბლოკჩეინის შესაძლებლობები და ლიმიტები. დანამდვილებით შეგვიძლია ვთქვათ, რომ ბლოკჩეინ ტექნოლოგიის გამოყენების გზები, რომლებმაც გაიარა შემოწმება, ეხებოდა ციფრული ურთიერთობების, როგორც ჩანაწერთა სისტემის ნაწილის, მართვასა და უსაფრთხოებას.

ბიტკოინი ვალუტის შედარებით ახალი ფორმაა, რომელიც ახლა იწყებს თავის დამკვიდრებას ძირითად ვალუტებს შორის. ხალხი ჯერ ვერ ხვდება, რატომ უნდა შეეცადონ მის გამოყენებას.

რატომ უნდა ვისარგებლოთ ბიტკოინით? ქვემოთ ჩამოთვლილია 10 მიზეზი, თუ რატომ ღირს ამ ვირტუალური ვალუტის გასაცნობად დროის დახარჯვა.

​

**ის სწრაფია**

**​**

როდესაც ერთ ბანკში სხვა ბანკის ჩეკით იხდი, ფული რამდენიმე დღე კავდება, რადგან საჭიროა თანხის ხელმისაწვდომობის დადასტურება. ასევე, დიდი დრო სჭირდება საერთაშორისო გადარიცხვებსაც. ბიტკოინ ტრანზაქციები კი, ზოგადად, ბევრად სწრაფია.

ტრანზაქციები შეიძლება მომენტალურადაც შესრულდეს, თუ მათი დამტკიცებისათვის ლოდინი არ დაგჭირდათ, ანუ თუ  გამყიდველმა მიიღო ტრანზაქცია ბიტკოინ ბლოკჩეინზე მის დადასტურებამდე (იხილეთ ჩვენი გზამკვლევი: [როგორ ხდება ბიტკოინ ტრანზაქციები](https://www.cryptoz.ge/how-bitcoin-transactions-are-made)). ან ტრანზაქციის დასრულებამ შეიძლება 10 წუთს გასტანოს, თუ გამყიდველმა მოითხოვა ჯერ ტრანზაქციის დადასტურება, თქვენთვის მომსახურების ან პროდუქტის მოწოდებამდე. ორივე შემთხვევაში, ტრანზაქცია უფრო სწრაფად ხორციელდება, ვიდრე ბანკებს შორის გადარიცხვები.

​

**ის იაფია**

**​**

შეიძლება გაგიკვირდეთ და თქვათ, რომ საკრედიტო ბარათის ტრანზაქციებიც მომენტალურია. ეს მართალია. მაგრამ გამყიდველი (და, სავარაუდოდ, თქვენც) იხდით ამ პრივილეგიისთვის. ზოგიერთი გამყიდველი აწესებს საფასურს სადებეტო ბარათით ტრანზაქციებზეც, რადგან მათ განსახორციელებლად უწევთ ‘swipe fee’-ს გადახდა. ბიტკოინ ტრანზაქციების საფასური კი მინიმალურია, ზოგიერთ შემთხვევაში საერთოდ არ არსებობს.

**ცენტრალური ხელისუფლებისთვის მიუწვდომელია**

**​**

ალბათ გახსოვთ 2013 წლის კვიპროსის მოვლენები. ცენტრალურ ბანკს სურდა 100 000 დოლარზე მეტი დაუზღვეველი დეპოზიტის უკან წაღება კომპანიის რეკაპიტალიზაციისთვის, რამაც დიდი მღელვარება გამოიწვია მოსახლეობაში. თავიდან, ზემოთხსენებულ რაოდენობაზე მცირე ზომის დეპოზიტებიდან გარკვეული პროცენტის მიღება უნდოდათ, რაც პირდაპირ ოჯახურ დანაზოგებს შეეხებოდა. ეს ბიტკოინების შემთხვევაში გამორიცხულია, რადგან ვალუტა დეცენტრალიზებულია და მას თავად ფლობთ. არც ერთ ცენტრალურ ხელისუფლებას აქვს კონტროლი, შესაბამისად, ბანკი ვერ ჩამოგართმევთ მას. ეს დიდი პლიუსია მისთვის, ვისთვისაც ტრადიციული საბანკო მომსახურება ბოლომდე სანდო არ არის.

**ტანზაქციები შეუქცევადია**

თუ ბიტკოინი გაგზავნილია, მისი უკან დაბრუნება მიმღების თანხმობის გარეშე შეუძლებელია. ეს ართულებს ბიტკოინ ტრანზაქციით ისეთ თაღლითობას, როგორსაც ხშირად ვხვდებით საკრედიტო ბარათების გამოყენების შემთხვევაში: ხალხი გარკვეული შენაძენის შემდეგ უკავშირდება საკრედიტო კომპანიას და ითხოვს თანხის უკან დაბრუნებას, განხორციელებული ტრანზაქციის „შექცევას".

**ვერავინ მოიპარავს თქვენი გადახდის ინფორმაციას გამყიდველისგან**

ეს უდიდესი პლიუსია. დღეისათვის, ონლაინ შენაძენების უმეტესობა ხორციელდება საკრედიტო ბარათებით, მაგრამ მათი წინამორბედების გამოჩენისას 1920-1930 წლებში ინტერტი საერთოდ არ არსებობდა. საკრედიტო ბარათები არ იყო გათვლილი ონლაინ გამოყენებისთვის და ამიტომ არაა საიმედო. ონლაინ ფორმების შესავსებად იყენებ საიდუმლო ინფორმაციას (საკრედიტო ბარათის ნომერს, ვადას და CSV ნომერს). ეს ყველაზე ნაკლებ საიმედო გზაა ონლაინ ვაჭრობისათვის. ამიტომაც, საკრედიტო ბარათების ნომრებს ხშირად იპარავენ.

ბიტკოინ ტრანზაქციისთვის არ მოგეთხოვებათ არანაირი საიდუმლო ინფორმაცია. ამ დროს გამოიყენება ორი გასაღები: საჯარო და პირადი. ყველას შეუძლია საჯარო გასაღების ნახვა (რაც რეალურად თქვენი ბიტკოინის მისამართია), ხოლო პირადი გასაღები საიდუმლოდ რჩება. ბიტკოინის გაგზავნისას ტრანზაქციას „ხელს აწერ“ საჯარო და პირადი გასაღებების კომბინაციით და მათი მათემატიკური ფუნქციის დამუშავებით. ეს მოწმობს, რომ ტრანზაქცია თქვენგან განხორციელდა. თქვენ დაცული ხართ, თუ, რა თქმა უნდა, პირად გასაღებს არ გაასაჯაროებთ.

**ის არ არის ინფლაციური**

**​**

ჩვეულებრივი ქაღალდის ფულის პრობლემა ისაა, რომ ხელისუფლებას შეუძლია სასურველი რაოდენობით და სიხშირით დაბეჭდოს. თუ სახელმწიფოს ვალის გადასახდელად საკმარისი აშშ დოლარი არ გააჩნია, ფედერალური სარეზერვო ფონდი უბრალოდ დაბეჭდავს მათ. თუ ეკონომიკა არასტაბილურია, ახლად შექმნილი ფული ჩაიდება. ეს კი  ვალუტის მსყიდველობით უნარს ამცირებს.

თუ მიმოქცევაში არსებულ დოლარების რაოდენობას გააორმაგებ, ერთი დოლარის ადგილას ორი დოლარი გაჩნდება. თუ ადამიანი შოკოლადს ერთ დოლარად ყიდდა, ახლა მოუწევს ფასის გაორმაგება, რათა მისი რეალური ღირებულება იგივე გახადოს რაც მანამდე იყო, რადგან დოლარი უცებ თავისი ფასის მხოლოდ ნახევარს შეადგენს. ამას ეწოდება ინფლაცია და ეს განაპირობებს საქონლის და მომსახურების ფასების ზრდას. ინფლაციის გაკონტროლება რთულია და მას შეუძლია ხალხის მსყიდველუნარიანობის შემცირება. ბიტკოინისთვის არსებობს მონეტების რაოდენობის ლიმიტი. თავდაპირველი პირობით, უნდა შეიქმნას მხოლოდ 21 მილიონი ბიტკოინი. ანუ, ამ რაოდენობის მიღწევის შემდეგ, ბიტკოინების რიცხვი აღარ გაიზრდება, შესაბამისად, ინფლაციაც პრობლემა არ იქნება. სხვათა შორის, ბიტკოინების სამყაროში უფრო მოსალოდნელი დეფლაციაა, რაც გულისხმობს საქონლისა და მომსახურების ფასების შემცირებას.

**ის იმდენად საიდუმლოა, რამდენადაც გსურთ, რომ იყოს**

**​**

ზოგჯერ საერთოდ არ გვინდა, ხალხმა გაიგოს, თუ რა შევიძინეთ. ბიტკოინი შედარებით საიდუმლო ვალუტაა. ერთი მხრივ, ის გამჭირვალეა. ბლოკჩეინის დამსახურებით, ყველასთვის ცნობილია გარკვეული ბიტკოინის მისამართზე რამდენი ტრანზაქციაა, საიდან განხორციელდა ისინი და საით გაიგზავნა. მეორე მხრივ კი, სტანდარტული საბანკო ანგარიშებისგან განსხვავებით, არავინ იცის, ვინ არის კონკრეტული ბიტკოინ მისამართის მფლობელი. ეს შეგვიძლია შევადაროთ ისეთი გამჭირვალე საფულის ქონას, რომლის პატრონიც არ ჩანს. ყველას შეუძლია, შიგნით ჩაიხედოს, მაგრამ არავინ იცის, ვის ეკუთვნის ის. თუმცა, აღსანიშნავია, რომ ხალხისთვის, რომელიც სარგებლობს ბიტკოინებით არაგონივრულად (მაგალითად, ყოველთვის ერთსა და იმავე მისამართს იყენებს, ან აერთიანებს მონეტებს ბევრი სხვადასხვა მისამართიდან ერთ რომელიმე მისამართზე), ქსელში იდენტიფიცირების რისკი უფრო დიდია.

**არავის ნდობაზე ხართ დამოკიდებული**

**​**

სტანდარტულ საბანკო სისტემაში თქვენი ფულის სწორად მართვა სხვადასხვა ეტაპზე დამოკიდებულია ხალხზე. თქვენ უნდა ენდობოდეთ, მაგალითად, ბანკს. შეიძლება საჭირო გახდეს მესამე მხარეც, როგორც გადახდების გადამამუშავებელი (მაგალითად Visa). ასევე, ხშირად გიწევთ, ენდოთ გამყიდველს. ყველა ეს ორგანიზაცია/რგოლი თქვენგან მოითხოვს მნიშვნელოვან პირად ინფორმაციას. ბიტკოინი კი სრულიად დეცენტრალიზებულია, ამიტომაც, ამ შემთხვევაში, არავის ნდობაზე არ ხართ დამოკიდებული. ტრანზაქციის შესრულებისას ის მტკიცდება ციფრული ხელმოწერით და დაცულია. უცნობი მაინერი ადასტურებს მას და ტრანზაქციაც სრულდება. რაიმე ნივთის ან მომსახურების შეძენისას, არ არის საჭირო გამყიდველმა იცოდეს თქვენი ვინაობა, თუ თავად არ მოისურვებთ ამის გამხელას.

**ის თქვენ გეკუთვნით**

**​**

არ არსებობს სხვა ელექტრონული ფულის სისტემა, რომელშიც თქვენი ანგარიში მხოლოდ თავად გეკუთვნით. განვიხილოთ PayPal-ის მაგალითზე. თუ კომპანია გადაწყვეტს, რომ რაიმე მიზეზით ანგარიში არასწორად მოიხმარება, შეუძლია ამ ანგარიშზე არსებული ყველანაირი აქტივი გაყინოს მფლობელთან კონსულტაციის გარეშე. შემდეგ კი, მესაკუთრეს თავად მოუწევს იმ ყველა საფეხურის გავლა, რომელიც საჭიროა სიტუაციის გასარკვევად და ანაგარიშისადმი წვდომის აღსადგენად. ბიტკოინების შემთხვევაში, თქვენ ფლობთ პირად გასაღებს და მის შესაბამის საჯარო გასაღებს, რომლებიც ქმნის ბიტკოინის მისამართს. ამის ჩამორთმევა არავის შეუძლია (თუ, რა თქმა უნდა, თავად არ დაკარგავთ, ან რომელიმე ინტერნეტ საფულეში არ შეინახავთ, საიდანაც შეიძლება დაიკარგოს).

**შეგიძლიათ შექმნათ საკუთარი ფული**

**​**

სახლის პირობებში, ბეჭდვის ფერად ტექნოლოგიებში საოცარი მიღწევების მიუხედავად, ხელისუფლების მიდგომა ხალხის მიერ საკუთარი ფულის ბეჭდვასთან დაკავშირებით მკაცრია. ბიტკოინების შემთხვევაში კი პირიქით - ეს წახალისებულია. ბიტკოინის შეძენა, რა თქმა უნდა, შეგიძლიათ ღია ბაზარზე, მაგრამ ასევე შეგიძლიათ მოიპოვოთ საკუთარი, თუ გაქვთ საკმარისი კომპიუტერული ენერგია. აღჭურვილობისა და ელექტრობის თავდაპირველი ხარჯების დაფარვის შემდეგ, ბიტკოინების მაინინგისთვის უბრალოდ საჭიროა აპარატისა და პროგრამული უზრუნველყოფის ჩართულ მდგომარეობაში დატოვება. ვინ უნდა იყოს წინააღმდეგი, რომ შენი ძილის დროს კომპიუტერი ფულს გამოიმუშავებდეს?

**თავი 7. რისი გაკეთება შეუძლია ბლოკჩეინს.**

ციფრული იდენტურობის შექმნა. შეასრულოს ჩანაწერთა სისტემის როლი. დაამტკიცოს მონაცემთა უცვლელობა. ბლოკჩეინი, როგორც პლატფორმა

ბოლო 30 წლის განმავლობაში, ფინანსური ინსტიტუტების თაოსნობით, უამრავი ინდუსტრია დაინგრა; მათ აქვთ გარკვეული წარმოდგენა იმის შესახებ, თუ რა გავლენა შეიძლება იქონიოს რევოლუციურმა ტექნოლოგიებმა მათზე, თუ ისინი იქნებიან უმოძრაონი.

ცვლილებებთან ადაპტაციისთვის, ბანკებმა ძალზე აქტიურად დაიწყეს R&D ლაბორატორიებისა და კვლევითი ცენტრების განვითარება და ბლოკჩეინის დეველოპერ ორგანიზაციებთან თანამშრომლობა, რათა სრულად გათვიცნობიერებულიყვნენ ტექნოლოგიის რევოლუციურ პოტენციალში.

ფინანსური ინსტიტუტები იყვნენ პირველები, ვინც ამ საქმის შესწავლა დაიწყო, მაგრამ ასევე იქცევიან საგანმანათლებლო დაწესებულებები, მთავრობები და საკონსულტაციო კომპანიები.

მთელი მათ მიერ გაწეული შრომა ემატება თავად მეწარმეებისა და დეველოპერების მიერ შესრულებულ სამუშაოს, რაც გულისხმობს ბიტკოინის ან ეთერიუმ ბლოკჩეინების გამოყენების ახალი გზების აღმოჩენას, ან სრულიად ახალი ბლოკჩეინების შექმნას.

ეს გრძელდება ბოლო სამი წლის განმავლობაში და შედეგები ნელ-ნელა თვალსაჩინო ხდება.

მიუხედავად იმისა, რომ მრავალი საკითხი ბურუსითაა მოცული, შემდეგი ფაქტები დანამდვილებით ვიცით ბლოკჩეინის შესაძლებლობების შესახებ:

​

**მას შეუძლია ციფრული იდენტურობის შექმნა**

**​**

ბლოკჩეინის ტექნოლოგიის პიროვნების იდენტიფიცირების ნაწილი განხორციელებულია კრიპტოგრაფიული გასაღებებით. პირადი და საჯარო გასაღებების კომბინაცია ქმნის ძლიერ ციფრულ იდენტურობას, რომელიც დაფუძნებულია საკუთრებაზე. საჯარო გასაღების მეშვეობით ხდება პიროვნების იდენტიფიცირება ხალხის ნაკადში (ელექტრონული ფოსტის მისამართის მსგავსად), პირადი გასაღებით კი ისინი თანხმობას აცხადებენ ციფრულ ურთიერთქმედებებზე. კრიპტოგრაფია მნიშვნელოვანი კომპონენტია ბლოკჩეინ რევოლუციაში.

**შეუძლია შეასრულოს ჩანაწერთა სისტემის როლი**

**​**

ბლოკჩეინი არის ინოვაცია ინფორმაციის რეგისტრაციასა და გადანაწილებაში. ის არის მოსახერხებელი, როგორც სტატიკური (რეგისტრაცია), ასევე დინამიკური (ტრანზაქცია) მონაცემების დასაფიქსირებლად და წარმოადგენს ჩანაწერთა სისტემის ევოლუციას.

რეგისტრაციის დროს, მონაცემები ბლოკჩეინზე შეიძლება შეინახოს შემდეგი სამი გზის ნებისმიერი კომბინაციით:

​

**არაკოდირებული მონაცემები** - არის სრულიად გამჭირვალე და ბლოკჩეინის ნებისმიერი მონაწილისათვის ხელმისაწვდომი.

**კოდირებული მონაცემები** - წაკითხვა შეუძლიათ მხოლოდ გასაშიფრი გასაღებით. გასაღები უზრუნველყოფს წვდომას ბლოკჩეინის მონაცემებზე და შეუძლია გამოავლინოს ვინ და როდის დაამატა ეს ინფორმაცია.

**ჰაშ მონაცემები**- შეიძლება წარმოდგენილი იყოს ჰაშ ფუნქციასთან ერთად, რომლის შედეგადაც იგი მიიღეს, რათა დადასტურდეს ინფორმაციის სინამდვილე და უტყუარობა.

ბლოკჩეინ ჰაშები, როგორც წესი, ხორციელდება საწყის მონაცემებთან კომბინაციით. მაგალითად, ციფრული „თითის ანაბეჭდები“ ბლოკჩეინში მოცემულია, როგორც მისი ჰაშები მაშინ, როცა ძირითადი ინფორმაცია შენახულია ქსელგარეშე (Offline).

მსგავსი გზით, გაზიარებულმა ჩანაწერთა სისტემამ შეიძლება შეცვალოს სხვადასხვა ორგანიზაციის ერთად მუშაობის პრინციპი.

ბოლო დროს, როცა ინფორმაციის შენახვა კერძო სერვერებზე დაიწყო, კომპანიებს შორის ტრანზაქციები ძალიან გაძვირდა, რადგან ეს ტრანზაქციები მოიცავს ჩანაწერების დამუშავებას, პროცედურებსა და შემოწმებებს.

**შეუძლია დაამტკიცოს მონაცემთა უცვლელობა (ორიგინალურობა)**

ბლოკჩეინის საინფორმაციო ბაზის მნიშვნელოვანი თვისებაა, რომ ის ინახავს მთელს თავის ისტორიას. ამიტომ, ხშირად, მას უცვლელს უწოდებენ. სხვაგვარად რომ ვთქვათ, ბაზაში ინფორმაციის შეცვლას ძალიან დიდი ძალისხმევა დასჭირდებოდა, რადგან ეს მოითხოვს იმ კონკრეტული ჩანაწერის შემდგომ ყველა მონაცემის შეცვლას ქსელში ჩართული თითოეული პირისთვის. შესაბამისად, ის უფრო ჩანაწერთა სისტემაა, ვიდრე საინფორმაციო ბაზა. მონაცემთა გაყალბების შესაძლებლობის აღმოფხვრასთან დაკავშირებით უფრო დეტალურად შეგიძლიათ იხილოთ ჩვენს გამკვლევში - „რა არის განსხვავება ბლოკეჩინსა და მონაცემთა ბაზას შორის“

**შეუძლია მოგვევლინოს როგორც პლატფორმა**

**​**

კრიპტოვალუტები იყო პირველი პლატფორმა, რომელიც ბლოკჩეინ ტექნოლოგიის გამოყენებით განვითარდა. ახლა ხალხი ამ პლატფორმას იყენებს არა მხოლოდ კრიპტოვალუტის გასაცვლელად, არამედ სხვადასხვა „გონიერი კონტრაქტისთვის“ (Smart Contracts).

ბოლო დროს, ტერმინი „გონიერი კონტრაქტი“ საკმაოდ ხშირად გვესმის. მისი იდეა შეიძლება რამდენიმე კატეგორიად დაიყოს:

არსებობს 1990 წელს ნიკ ზაბოს მიერ შექმნილი 'vending machine' გონიერი კონტრაქტები. ამ შემთხვევაში, კომპიუტერები იწყებენ მუშაობას მაშინ, როდესაც იღებენ ინფორმაციას გარე წყაროდან, ან აგზავნიან ბლოკჩეინის გამააქტივირებელ სიგნალს.

ასევე არსებობს სამართლებრივი გონიერი კონტრაქტები(იგივე Ricardian). მათი უმეტესობა ემყარება ფაქტს, რომ კონტრაქტი არის აზრების თანხვედრა და ყველა მხარის შეთანხმების შედეგი გარკვეული საკითხის შესახებ. ასე რომ, კონტრაქტი შეიძლება იყოს ვერბალური და წერილობითი შეთანხმების ერთობლიობა და დღეისათვის, ამას შეიძლება დაემატოს ბლოკჩეინის ისეთი სასარგებლო ასპექტები, როგორებიცაა დროითი შტამპი (ბლოკში მოცემული ტრანზაქციის ფიქსირებული დრო ე.წ. timestamps) კრიპტოვალუტები, აუდიტი, დოკუმენტების კოორდინაცია ან ბიზნესის ლოგიკა.

უკანასკნელია ეთერიუმის გონიერი კონტრაქტები. ესენია პროგრამები, რომლებიც ეთერიუმის ბლოკჩეინში განხორციელებული ტრანზაქციების შედეგად წარმოშობილ აქტივებს აკონტროლებს. თავად ეთერიუმი არის პლატფორმა გონიერი კონტრაქტის კოდისათვის.

ბლოკჩეინები არ იქმნება ახალი ტექნოლოგიით, ის ყალიბდება სამი არსებული ტექნოლოგიის ურთიერთქმედებით. ესენია პირადი გასაღების კრიპტოგრაფია, პირისპირა ქსელი და პროგრამა (პროტოკოლი, რომლითაც მუშაობს ბლოკჩეინი).

**თავი 8. როგორ ხდება ბიტკოინ ტრანზაქციები.**

როგორ გამოიყურება ტრანზაქცია. როგორ იგზავნება ბიტკოინები. ლოდინი. კონსენსუსის პრობლემა და კონსენსუსის მართვა.. განაწილებული კონსენსუსი. ჩაწერა ბლოკჩეინში. სამუშაოების შესრულების მტკიცებულობა.

ბიტკოინ ტრანზაქციები ხდება ბიტკოინ საფულეების მეშვეობით. უსაფრთხოებისთვის ციფრული ხელმოწერა გამოიყენება. ქსელში ჩართულმა ყველა პირმა იცის ტრანზაქციის შესახებ და ყველა ტრანზაქციის ისტორიის ნახვა შესაძლებელია ბიტკოინის შექმნის მომენტიდან.

ბიტკოინების შენახვა ხელსაყრელია გადამყიდველებისთვის, რომლებიც ელოდებიან მათი ფასის გაზრდას. მაგრამ ამ ვალუტის მთელი აზრი ხომ მისი დახარჯვაა? განვიხილოთ, თუ როგორ მიმდინარეობს ტრანზაქციები ბიტკოინების დახარჯვის დროს.​

**არ არსებობს ბიტკოინები, არის, მხოლოდ, ჩანაწერები ბიტკოინ ტრანზაქციების შესახებ.**

სახალისო ფაქტი ბიტკოინების შესახებ ის არის, რომ ისინი არსად არსებობენ, მყარ დისკზეც კი. ჩვენ, ხშირად, ვსაუბრობთ ბიტკოინების ფლობაზე. მაგრამ კონკრეტული ბიტკოინის მისამართს თუ შევამოწმებთ, ვნახავთ რომ ციფრული ბიტკოინები იქაც არ ინახება, როგორც ფუნტი ან დოლარი ბანკის ანგარიშზე. ვერც ერთ ციფრულ ფაილზე ან ფიზიკურ საგანზე ვიტყვით, რომ ეს არის ბიტკოინი.

სამაგიეროდ, არსებობს ჩანაწერები სხვადასხვა მისამართს შორის მიმდინარე ტრანზაქციებზე, რომელთა შედეგადაც ბალანსი იზრდება ან მცირდება. თითოეული ტრანზაქცია ინახება ვრცელ საჯარო დავთარში, რომელსაც ბლოკჩეინი ეწოდება. გარკვეული ბიტკოინის მისამართზე ბალანსის ამსახველი ინფორმაცია არ ინახება. ბალანსის დასადგენად უნდა შეამოწმოთ ბლოკჩეინი.

​

**როგორ გამოიყურება ტრანზაქცია?**

**​**

თუ ალისა ბიტკოინებს გაუგზავნის ბობს, ტრანზაქციაში იქნება სამი სახის ინფორმაცია:

​

* Input. ეს არის ინფორმაცია იმის შესახებ, თუ რომელი მისამართიდან მიიღო ალისამ ბიტკოინები (მას ბიტკოინები მეგობარმა, ევამ გამოუგზავნა)
* რაოდენობა. ეს არის ალისას მიერ ბობთან გაგზავნილი ბიტკოინების რიცხვი.
* Output. ეს არის ბობის ბიტკოინ მისამართი.

**როგორ იგზავნება ბიტკოინები?**

**​**

ბიტკოინების გასაგზავნად ორი რამ არის საჭირო: საჯარო მისამართი და პირადი გასაღები. მისამართი ყველა პირს შერჩევითად ენიჭება და არის ასოებისა და ციფრების უბრალო, შემთხვევითი თანმიმდევრობა. პირადი გასაღები, ასევე, ასოებისა და ციფრების კომბინაციაა, მაგრამ, მისამართისგან განსხვავებით, ის საიდუმლოდ ინახება.

ბიტკოინის მისამართი შეგიძლიათ წარმოიდგინოთ, როგორც გამჭირვალე დაცული სადეპოზიტო ყუთი.  ყველასთვის ცნობილია, თუ რა დევს შიგნით, მაგრამ მხოლოდ პირადი გასაღებით არის შესაძლებელი მისი გახსნა და შიგთავსის გამოღება ან მასში რამის შენახვა.

როდესაც ალისას სურს ბიტკოინების ბობისთვის გაგზავნა, იყენებს პირად გასაღებს  შეტყობინების დასადასტურებლად. ეს შეტყობინება მოიცავს პირველად ინფრომაციას- input-ს (გასაგზავნი მონეტების შესახებ ინფომრაციას), რაოდენობას და output-ს (ბობის მისამართს). ის გზავნის მათ საფულიდან ბიტკოინის უფრო ფართო ქსელში. ამის შემდეგ უკვე მაინერები ადასტურებენ ტრანზაქციას, ამატებენ მას ტრანზაქციების ბლოკში და, საბოლოოდ, ამოხსნიან კრიპტოგრაფიულ ჰაშ ფუნქციას, რითაც ადასტურებენ ტრანზაქციას.

**რატომ გიწევს, ზოგჯერ, ლოდინი ტრანზაქციის დასადასტურებლად?**

**​**

ტრანზქციები უნდა დადასტურდეს მაინერების მიერ, ამიტომაც, ზოგჯერ, გიხდება ლოდინი მაინინგის დასრულებამდე. ბიტკოინის პროტოკოლის (პროგრამის) მიხედვით, თითოეული ბლოკის მაინინგს, უხეშად, 10 წუთი სჭირდება.

ზოგიერთმა გამყიდველმა, ვისთანაც ბიტკოინით ვიხდით საფასურს, შეიძლება გალოდინოს, სანამ ბლოკი დადასტურდება. ამ დროის განმავლობაში შეიძლება დაისხათ ყავა, გახვიდეთ და დაბრუნდეთ ცოტა ხანში, რათა, საბოლოოდ, შეძლოთ შეძენილი საქონლის ან მომსახურების მიღება.

თუმცა, ზოგიერთმა გამყიდველმა შეიძლება არც გალოდინოთ ტრანზაქციის დადასტურებამდე. ისინი გენდობიან და თვლიან, რომ იგივე ბიტკოინებით არ შეეცდებით სხვა ტრანზაქციების დადასტურებასაც. ასე, უმეტესად, დაბალი ფასის ტრანზაქციების დროს იქცევიან, როცა თაღლითობის რისკი ნაკლებია.

​

**რა მოხდება, თუ input და output რაოდენობები არ დაემთხვევა?**

**​**

რომელიმე კონკრეტულ მისამართთან შეიძლება ბევრი სხვადასხვა ტრანზაქცია იყოს დაკავშირებული, რადგან ბიტკოინების არსებობა მხოლოდ ტრანზაქციების ჩანაწერებითაა წარმოდგენილი. ვთქვათ, ალისას ჯეინმა გაუგზავნა 2 ბიტკოინი, ფილიპმა - სამი და ევამ - ერთი, ყველა ეს ტრანზაქცია დაფიქსირდება ცალ-ცალკე განსხვავებულ დროს. ისინი ალისას საფულეში ავტომატურად არ დაჯამდება ექვს ბიტკოინად, არამედ იქნება სხვადასხვა ტრანზაქციის ჩანაწერების სახით.

ალისასგან ბობისთვის ბიტკოინების გაგზავნისას, საფულე შეეცდება გასაგზავნი  ბიტკოინების არსებობა შეამოწმოს სხვადასხვა ტრანზაქციების დაჯამებით.

ბიტკოინების ბობისთვის გაგზავნის დროს შეიძლება ალისას არ აღმოაჩნდეს სხვა ტრანზაქციებით შემოსული ბიტკოინების ზუსტი რაოდენობა. ვთქვათ, სურს მხოლოდ 1.5 ბიტკოინის გადაცემა ბობისთვის. მის მისამართზე განხორციელებული ტრანზაქციებიდან არც ერთი ეთმხვევა ამ რაოდენობას და არც მათი კომბინაციით ვიღებთ სასურველ შედეგს. ალისას ტრანზაქციების უბრალოდ დაყოფა არ შეუძლია. მომხარებელს შეუძლია მთლიანი output-ის დახარჯვა და არა მისი გაყოფა პატარა ნაწილებად.

სამაგიეროდ, ალისას შეუძლია გადარიცხოს თანხა ერთ-ერთი მიღებული ტრანზაქციის ოდენობით და მას დაუბრუნდება ხურდა.

ალისა ბობს გადაურიცხავს ჯეინის მიერ გამოგზავნილ 2 ბიტკოინს. ამ შემთხვევაში, ჯეინი არის input და ბობი არის output. მაგრამ, ალისასთვის სასურველი გადარიცხვის რაოდენობა არის 1.5 BTC. ამიტომ, ალისას საფულე ავტომატურად ქმნის ორ output-ს ამ ტრანზაქციისთვის: 1.5 BTC ბობს გაეგზავნება, ხოლო 0.5 BTC ახალ მისამართზე გადაირიცხება, რომელიც შეიქნმა ალისასთვის ხურდის დასაბრუნებლად.

​

**არის თუ არა ტრანზაქციის რაიმე სახის საკომისიო?**

​

არის, მაგრამ არა ყოველთვის.

ტრანზაქციის საკომისიო გამოითვლება სხვადასხვა ფაქტორის გათვალისწინებით. ზოგიერთი საფულე საშუალებას გაძლევს, თავად დააწესო ტრანზაქციის საკომისიო. ტრანზაქციის ნებისმიერი ნაწილი, რომელიც მიმღებამდე არ  მიაღწევს და არც ხურდის სახით ბრუნდება, ითვლება საკომისიოდ. ის დამატებითი ჯილდოს სახით ერიცხება იღბლიან მაინერს, რომელმაც დაადასტურა ეს ტრანზაქცია.

ამ ეტაპზე, უამრავი მაინერი საკომისიოს გარეშე გადაამუშავებს ტრანზაქციებს. ამის ასე გაგრძელება ნაკლებად სავარაუდოა, რადგან ბიტკოინის თითოეულ ბლოკზე ჯილდო ნელ-ნელა მცირდება. ერთ-ერთი ყველაზე მოუხერხებელი ფაქტი ტრანზაქციების საკომისიოებთან დაკავშირებით იყო მათი გამოთვლის სირთულე და ფარულობა. ის არის პროტოკოლის რამდენჯერმე განახლების შედეგი.

ბიტკოინ ტრანზაქციების პროგრამული უზრუნველყოფის განახლება შეცვლის ტრანზაქციის საკომისიოსთან  დაკავშირებულ მიდგომებს და დადგინდება ყველაზე დაბალი გადასახადი, რომლისთვისაც ტრანზაქცია შეიძლება დამტკიცდეს.

​

**რა ხდება მაშინ, თუ მსურს ბიტკოინის მხოლოდ ნაწილის გაგზავნა?**

**​**

ბიტკოინ ტრანზაქციები შეიძლება დაიყოს კიდეც. არსებობს ერთეული - სატოში, რომელიც შეადგენს ბიტკოინის ას მემილიონედს (100,000,000 სატოში = 1 ბიტკოინს). ბიტკოინის ქსელში შესაძლებელია მინიმუმ 5430 სატოშის (0.00005430 ბიტკოინის) ოდენობის ტრანზაქციის განხორციელება.

**თავი 9. რითი განსხვავდება ბლოკჩეინი მონაცემთა ბაზისაგან.**

დეცენტრალიზაცია, უსაფრთხოება, სისწრაფე

განსხვავება ტრადიციულ მონაცემთა ბაზას და ბლოკჩეინს შორის, პირველ რიგში, სტრუქტურაშია, ანუ ბლოკჩეინი სხვა ტექნოლოგიით არის მოწყობილი. ეს განხილულია ჩვენს გზამკვლევში - „[რა არის ბლოკჩეინი](https://www.cryptoz.ge/what-is-blockchain)“.

მსოფლიო ქსელში ჩართული მონაცემთა ბაზა, უმეტესად, სამომხმარებლო სერვერის მოდელზეა დამყარებული.

უფლებამოსილ მომხმარებელს თავისი ანგარიშით შეუძლია შეცვალოს მონაცემები, რომლებიც ინახება ცენტრალიზებულ სერვერზე. თუ დედანი შეიცვალა, მომხმარებელი თავისი კომპიუტერით ქსელში შესვლისას, მიიღებს უკვე განახლებულ მონაცემებს. მონაცემთა ბაზის კონტროლი ადმინისტრატორის ხელშია, რაც საშუალებას აძლევს ცენტრალურ ძალაუფლებას, შეინარჩუნოს წვდომა გარკვეულ ინფორმაციაზე.

ბლოკჩეინის სტრუქტურა სრულიად განსხვავებულია.

ბლოკჩეინის მონაცემთა სისტემაში თითოეული მომხმარებელი თავად იღებს, გადაამუშავებს და ანახლებს ბაზაში შესულ ცვლილებებს. ქსელში ჩართული ყველა პირი ერთობლივად მუშაობს ერთი შეთანხმების მისაღებად, რათა ქსელის უსაფრთხოება უზრუნველყონ.

ამ განსხვავების გამო ბლოკჩეინი გარკვეული ფუნქციებისთვის უფრო შესაფერი ჩანაწერთა სისტემაა, ხოლო ცენტრალიზებული მონაცემთა ბაზა კი გამოსადეგია სხვა მახასიათებლების გამო.

​

**დეცენტრალიზებული კონტროლი**

​

ბლოკჩეინი საშუალებას აძლევს სხვადასხვა პირებს, რომლებიც ერთმანეთს არ ენდობიან, გააზიარონ ინფორმაცია ცენტრალური ადმინისტრატორის გარეშეც. ტრანზაქციები გადამუშავდება ქსელში ჩართული მომხმარებლების მიერ კონსესუსის მიღწევით, ისე, რომ ყველა წევრი ერთდროულად ქმნის გაზიარებულ ჩანაწერთა სისტემას.

დეცენტრალიზებული სისტემის ღირსება ისაა, რომ თავიდან გვაცილებს ცენტრალიზებული კონტროლის რისკს. ცენტრალიზებულ მონაცემთა ბაზაში საკმარისი წვდომის მქონე ნებისმიერ ადამიანს შეუძლია, გაანადგუროს ან შეცვალოს ინფორმაცია. ამის გამო, მომხმარებლები დამოკიდებულები არიან ადმინისტრატორზე. უმეტესად, ადმინისტრატორს თქვენი ნდობა დამსახურებულიც აქვს. მაგალითად, ბანკებში ხალხის მიერ შეტანილ ფულს არ იპარავენ, უბრალოდ ინახავენ მას პირად მონაცემთა ბაზაში. არსებობს ლოგიკური მიზეზებიც, თუ რატომ უნდა გინდოდეთ ცენტრალიზებული კონტროლი. ცენტრალიზებული კონტროლის სისტემა ქმნის სპეციალობას, ის შეიძლება ადამიანის საქმნიანობა გახდეს.

თუმცა, ცენტრალიზებული ძალაუფლება, როგორიცაა ბანკი, ხარჯავს მილიარდობით დოლარს მონაცემთა ბაზის უსაფრთხოების უზრუნველსაყოფად, რათა ჰაკერებმა ვერ მოახერხონ ბანკის კლიენტების დაზარალება. თუ ცენტრალური ადმინისტრატორები, რომლებსაც ვანდობთ ჩვენს პირად ინფორმაციას, ვერ შეძლებენ მის დაცვას, დავკარგავთ ქონებას.

​

**ბლოკჩეინის მონაცემთა ბაზის ისტორია**

​

ცენტრალიზებული ბაზების უმეტესობაში, ინფორმაცია გარკვეულ მომენტში განახლდება ხოლმე და ინახება. ანუ, ისინი, მეტნაკლებად, დროის რაღაც მონაკვეთში დაფიქსირებული  ფაქტებია.

ბლოკჩეინის ბაზები კი საშუალებას გვაძლევს, ინფორმაცია მუდამ ახლდებოდეს და თან განახლებამდე არსებული მთელი ინფორმაციაც ინახებოდეს. ბლოკჩეინ  ტექნოლოგიით შეიძლება მონაცემთა ისეთი სისტემის შექმნა, რომელსაც საკუთარი ისტორიის შენახვაც შეუძლია. ისინი წარმოდგენილია, როგორც საკუთარი ისტორიის ზრდადი არქივი, რომელიც, პარალელურად, გვიჩვენებს მდგომარებას მიმდინარე დროში.

ამ მონაცემთა ბაზების შესაცვლელად საკმაოდ დიდი ხარჯები იქნებოდა საჭირო, ამიტომაც, ხალხი ბლოკჩეინის სისტემის დანერგვას უკვე გარდაუვლად თვლის. ეს შეგვიძლია მივიჩნიოთ მონაცემთა ბაზის ჩანაწერთა სისტემის გარდაქმნის დასაწყისად.

შესრულება

მართალია, ბლოკჩეინების გამოყენება შეიძლება ჩანაწერთა სისტემად და იდეალურია ტრანზაქციების პლატფორმისთვის, მაგრამ ტრანზაქციების ისეთ ციფრულ ტექნოლოგიებთან შედარებით, როგორებიცაა Visa და PayPal, ბლოკჩეინი ნელია.

მიუხედავად იმისა, რომ ამ თვალსაზრისით ბლოკჩეინის დახვეწა შესაძლებელია, მისი ტექნოლოგია მოითხოვს, გარკვეულწილად, სისწრაფის დათმობას. ბლოკჩეინ ტექნოლოგიის გადანაწილებული ქსელები არ გულისხმობს გადამუშავების ენერგიის გაზიარებას და გაერთიანებას.  მასში ჩართული ყოველი პირი დამოუკიდებლად მუშაობს ქსელში, შემდეგ ჯამდება თითოეულის მიერ შესრულებული სამუშაოს შედეგები და მიიღწევა შეთანხმება, რომ გარკვეული ფაქტი ნამდვილად მოხდა.

მეორეს მხრივ, ცენტრალიზებული მონაცემთა ბაზები უკვე ათწლეულების მანძილზე არსებობს. ისინი უფრო და უფრო ვითარდებოდა ციფრული სამყაროს იმ ინოვაციურ ფორმულასთან ერთად, რომელსაც „მურის კანონი“ ჰქვია.

**კონფიდენციალობა**

​

ბიტკოინის შემთხვევაში, ინფორმაციის წაკითხვა და შეტანა არ კონტროლდება. ყველას შეუძლია ჯაჭვში ბლოკის დამატება და ყველას შეუძლია მისი წაკითხვა.

შეიძლება ისეთი ბლოკჩეინიც შეიქმნას, რომლის შემთხვევაშიც ბლოკების დამატება და მათი ნახვა გაკონტროლდება მონაცემთა ცენტრალიზებული ბაზის მსგავსად. ანუ, ქსელი, ან პროტოკოლი, შეიძლება ისე აეწყოს, რომ მხოლოდ უფლებამოსილ მომხმარებლებს მიუწვდებოდეთ ხელი ინფორმაციაზე.

თუ კონფიდენციალობა ერთადერთი მიზანია და ნდობის ფაქტორი პრობლემას არ წარმოადგენს, მაშინ ბლოკჩეინის სისტემას არანაირი უპირატესობა არ ექნება ცენტრალიზებული ბაზის მიმართ.

ბლოკჩეინზე ინფორმაციის დამალვა დაკავშირებულია კრიპტოგრაგიულ სირთულეებთან და ქსელში ჩართული პირებისთვის დამატებით შრომას გულისხმობს. ამის გასაკეთებლად საუკეთესო გზა მონაცემების მთლიანად პირად ბაზაში შენახვაა, რასაც ქსელთან დაკავშირებაც კი არ სჭირდება.

გაიხსენეთ ყველა მონაცემთა ბაზა, რომლებიც ეთან ჰანტმა ფილმში, „შეუსრულებელი მისია“, გატეხა და შეგექმნებათ წარმოდგენა პირადი ბაზების კონფიდენციალობაზე.

**თავი 10. ბლოკჩეინ ტექნოლოგია.**

გადანაწილებული ქსელი საერთო საბუღალტრო წიგნაკით. სტიმული ქსელის ტრანზაქციების, ჩანაწერებისა და უსაფრთხოებისათვის (იგივე პროტოკოლი).

არსებობს სამი ძირითადი ტექნოლოგია, რომლებზეც ბლოკჩეინია დაფუძნებული.

არც ერთი ამ ტექნოლოგიათაგან არ წარმოადგენს სიახლეს. ახალი არის მხოლოდ მიდგომა მათი გამოყენებისადმი.

ეს ტექნოლოგიებია: 1) კრიპტოგრაფიული ჰაშები, 2) გადანაწილებული ქსელი საერთო საბუღალტრო წიგნაკით (დავთარით) და 3) სტიმული ქსელის ტრანზაქციების, ჩანაწერებისა და უსაფრთხოებისათვის (იგივე პროტოკოლი).

ქვევით განხილულია ამ ტექნოლოგიების ერთობლივი მოქმედება, რათა უზრუნველყოფილი იყოს ციფრული ურთიერთობების უსაფრთხოება.

​

**კრიპტოგრაფიული გასაღები**

​

ორ ადამიანს სურს, ინტერნეტით განახორციელოს ტრანზაქცია. თითოეულ მათგანს აქვს პირადი და საჯარო გასაღები.

**პირადობა**

**​**

საკუთრების მყარი კონტროლი არაა საკმარისი ციფრული ურთიერთობების უსაფრთხოებისათვის. მართალია, იდენტიფიკაციის საკითხი მოგვარებულია, მაგრამ საჭიროა ამის კომბინაცია  ტრანზაქციების დადასტურებასა და ნებართვებთან (ავტორიზაციასთან).

ბლოკჩეინის შემთხვევაში ეს იწყება გადანაწილებული ქსელით.

​

**გადანაწილებული ქსელი**

**​**

გადანაწილებული ქსელის სარგებელი და საჭიროება შეიძლება აღვიქვათ შემდეგი მაგალითით: „თუ ტყეში ხე წაიქცა“.

როცა ტყეში ხე წაიქცევა და ამას კამერა დააფიქსირებს, შეგვიძლია დარწმუნებულები ვიყოთ ფაქტის სინამდვილეში. დამატებითი, გარემო ფაქტორების გაურკვევლობის შემთხვევაშიც კი გვაქვს ვიზუალური მტკიცებულება.

ბიტკოინ ბლოკჩეინის მთავარი თვისება ისაა, რომ არის ფართო ქსელი საკონტროლო მოწყობილობებით (კამერის მსგავსად), რომლებიც თანხმდება ერთსა და იმავე დროს გარკვეული ფაქტის არსებობის შესახებ. კამერების ნაცვლად გამოიყენება მათემატიკური ვერიფიკაციები.

მოკლედ რომ ვთქვათ, ქსელის სიდიდე მნიშვნელოვანია მისი საიმედოობისათვის.

ბიტკოინ ბლოკჩეინი არის საკმაოდ ვრცელი და აერთიანებს უამრავი კომპიუტერის ენერგიას - სწორედ ესაა მისი ძირითადი და ყველაზე მნიშვნელოვანი ღირსება. დღეისათვის, ბიტკოინის ბლოკჩეინის სიმძლავრე შეადგენს 12 მილიონ ტერაჰაშს წამში (TH/s), რაც უფრო მეტია ვიდრე, ერთად აღებული მსოფლიოს უდიდესი 10,000-მდე ბანკის კომპიუტერული სიმძლავრე.

**​**

**ჩანაწერების სისტემა**

კრიპტოგრაფიული გასაღების ამ ქსელთან კომბინირებისას აღმოცენდება ციფრული ურთიერთქმედების ძალზე სასარგებლო ფორმები. პროცესი იწყება A-ს მიერ პირადი გასაღების მიღებით, კეთდება გარკვეული ფორმის განაცხადი - ბიტკოინის შემთხვევაში იგზავნება კრიპტოვალუტის ჯამი - და ემაგრება B-ს საჯარო გასაღებს.

​

**პროტოკოლი**

ხელმოწერების, დროითი შტამპისა  და შესაბამისი ინფორმაციის მომცველი ბლოკი გადაეცემა ქსელში ჩართულ ყველა პირს.

**ქსელის სერვისის პროტოკოლი**

**​**

ინფორმაციის ქსელში განთავსების უკეთ გასააზრებლად, დავუბრუნდეთ მანამდე მოყვანილ, ტყეში ხის წაქცევის მაგალითს: რეალურად, ტყეში ხის წაქცევის ფაქტმა შეიძლება შემდეგი კითხვა გააჩინოს: რატომ უნდა იყოს მილიონობით კომპიუტერი კამერებით ხის შესაძლო დაცემის მოლოდინში? სხვა სიტყვებით რომ ვთქვათ, როგორ უნდა მოიზიდოს ამ ქსელის უსაფრთხოებისათვის და გასამართად საჭირო კომპიუტერული ენერგია?

ღია, საზოგადო ბლოკჩეინებისთვის ეს გულისხმობს მაინინგს (მოპოვებას).

ბლოკჩეინის შემთხვევაში, ქსელის სერვისის უზრუნველყოფისასთვის არსებობს ჯილდო ერთ-ერთი კომპიუტერისთვის. საზოგადოების სერვისის გასაუმჯობესებლად ადამიანის პირადი ინტერესია გამოყენებული.

ბიტკოინის შემთხვევაში, პროტოკოლის მიზანია, აღმოფხვრას ერთი ბიტკოინით ერთსა და იმავე დროს სხვადასხვა ტრანზაქციის შესრულების შესაძლებლობა.

აქვე არის განხილული ბიტკოინის მოქმედება, როგორც ოქროსი, საკუთრების. ბიტკოინები და მათი ძირითადი ერთეულები (satoshis) უნდა იყოს უნიკალური და უნდა ჰქონდეს ფასი. ამის მისაღწევად, ქსელში ფიქსირდება და ინახება თითოეული ბიტკოინის გამოყენების ისტორია, რომელიც ეფუძნება სამუშაოს შესრულების მტკიცებულების (Proof-of-work) მათემატიკური ალგორითმის ამოხსნას.

ვინც პირველი ამოხსნის ჰაშს, ქსელს ხმას აწვდენს CPU-ს ენერგიით, ქსელში ჩართული პირები კი ეთანხმებიან ახალ ბლოკებს ან უარყოფენ მიუღებელ ბლოკებს. როდესაც მაინერების უმეტესობა მიაღწევს შეთანხმებას, ჯაჭვს ემატება ახალი ბლოკი და ბლოკიჩეინში ბლოკის დამმატებელი იღებს 12,5 ბიტკოინს ჯილდოდ. ეს ბლოკი  შეიცავს დროით შტამპს და შეიძლება შეიცავდეს მონაცემებს და შეტყობინებებს.

ქვევით განხილულია ბლოკჩეინი:

### ტიპი, რაოდენობა და დადასტურება შეიძლება განსხვავდებოდეს ბლოკჩეინების მიხედვით. ეს დამოკიდებულია ბლოკჩეინის პროტოკოლზე, ანუ რა არის მიჩნეული სწორ და რა - არასწორ ტრანზაქციად, ან მართებულად შეიქმნა თუ არა ახალი ბლოკი. დადასტურების პროცესი შეიძლება სპეციფიკური იყოს თითოეული ბლოკჩეინისთვის. ნებისმიერი საჭირო წესი და სტიმული შეიძლება შეიქმნას მაშინ, როცა საკმარისი რაოდენობის ქსელში ჩართული პირები მიაღწევენ შეთანხმებას იმასთან დაკავშირებით, თუ როგორ უნდა დადასტურდეს ტრანზაქციები.

ეს არის მომხარებლის არჩევანი და ხალხი მხოლოდ ახლა იწყებს სტრუქტურის გამოცდას.

ჩვენ ამჟამად ვიმყოფებით ბლოკჩეინის განვითარების პერიოდში, რომლის დროსაც ბევრი ექსპერიმენტი ტარდება. დღეისათვის არსებული დასკვნებით ბლოკჩეინის პროტოკოლების სრულყოფილად გააზრება და გამოყენება ჯერ კიდევ წინ გველის

**თავი 11. რა არის გონიერი კონტრაქტები. გონიერი კონტრაქტების გამოყენება და უპირატესობები.**

კოდი, რომელიც უზრუნველყოფს ხელშეკრულების პირობების შესრულებას. ბიურო-კრატიული შუამავლის სრული ჩანაცვლება. სანდოობა, სისწრაფე, მართვა და ა.შ.

ბლოკჩეინის ერთ-ერთი საუკეთესო თვისება ისაა, რომ ვინაიდან ის დეცენტრალიზებული სისტემაა, რომელიც ყველა მონაწილეს შორის არსებობს, ის აღარ საჭიროებს შუამავლისთვის ანაზღაურების გადახდას, ზოგავს თქვენს დროს და თავიდან გაცილებთ კონფლიქტს. ბლოკჩეინებს გააჩნიათ თავისი პრობლემები, მაგრამ ისინი ეჭვსგარეშე  უფრო სწრაფი, უფრო იაფი და უფრო დაცულია, ვიდრე სხვა ტრადიციული სისტემები, რის გამოც ბანკები და ხელისუფლებები უპირისპირდებიან მას.

1994 წელს, ნიკ სზაბომ, მეცნიერმა და კრიპტოგრაფმა, გააცნობიერა, რომ დეცენტრალიზებული საბუღალტრო წიგნაკი შეიძლება გამოყენებულ იქნას გონიერი კონტრაქტებისთვის, რომელსაც მეორენაირად თვით-განსჯად, ბლოკჩეინ და ციფრულ კონტრაქტებსაც უწოდებენ. ამ ფორმატში კონტრაქტები შეიძლება გადაკეთდეს კომპიუტერულ კოდად, იქნას შენახული, გამრავლდეს სისტემაში და გაკონტროლდეს კომპიუტერული ქსელების მიერ, რომლებიც ბლოკჩეინს მართავენ. ყველაფერი ამის შემდეგი განვითარების ნაბიჯი იქნება, რომ დავთარი თავად მოაწესრიგებს ფულის გადარიცხვასა და სერვისის თუ პროდუქტის მიღებას.

რა არის გონიერი კონტრაქტი?

გონიერი კონტრაქტები გთავაზობთ ფულის, ქონების, წილის თუ ნებისმიერი სხვა რამის გადაცვლის უკონფლიქტო გზას შუამავლის სერვისების თავიდან არიდებით.

გონიერი კონტრაქტების განმარტებისთვის საუკეთესო გზა იქნება ტექნოლოგიის სავაჭრო აპარატთან (vending machine-თან) შედარება. როგორც ჩვეულებრივად ხდება, თქვენ მიდიხართ იურისტთან, ან ნოტარიუსთან, უხდით მათ ფულს და იცდით, სანამ საჭირო დოკუმენტს მიიღებთ. გონიერი კონტრაქტებით კი თქვენ უბრალოდ აგდებთ ბიტკოინს სავაჭრო აპარატში (ანუ იგივე დავთარში) და თქვენი თანხის დეპონირება, მართვის მოწმობა თუ სხვა თქვენს ანგარიშზე გაჩნდება. ამასთან, გონიერი კონტრაქტები არა მხოლოდ ადგენენ წესებსა და ჯარიმებს შეთანხმების მიხედვით, როგორც ამას ტრადიციული კონტრაქტი აკეთებს, არამედ ავტომატურად აძალებს ორივე პირს მოვალეობების შესრულებას.

როგორც ვიტალიკ ბუტერინი, ეთერიუმის შემქმნელი, განმარტავს გონიერ კონტრაქტს ახლანდელ DC ბლოკჩეინის შეხვედრაზე, აქტივი თუ ვალუტა პროგრამაში გადადის „*და პროგრამა მართავს ამ კოდს, ხოლო რაღაც მომენტში ავტომატურად ამტკიცებს რაიმე მდგომარეობას და ის ავტომატურად წყვეტს, აქტივი უნდა გადავიდეს სხვაზე, თუ უნდა დარჩეს იმავე პირს.*“ ამასობაში, დეცენტრალიზებული დავთარი ინახავს და ამრავლებს დოკუმენტს, რაც მის უსაფრთხოებასა და გარდაუვალობას უზრუნველყოფს.

​

**მაგალითი**

​

ჩავთვალოთ, რომ ჩემგან ბინა იქირავე. ამისათვის, შენ კრიპტოვალუტით იხდი საჭირო თანხას. შენ იღებ ჩეკს, რომელიც შენს ციფრულ კონტრაქტზეა მიბმული; მეორეს მხრივ, მე შენ ციფრულ გასაღებს გაძლევ, რომელიც შენთან სპეციფიურ თარიღში მოდის. თუ გასაღები დროულად არ მოვა, ბლოკჩეინი გინაზღაურებს თანხას. თუ მე გასაღებს ვადაზე ადრე გამოგიგზავნი, პროგრამა ინახავს გასაღებსაც და თანხასაც, სანამ დათქმული თარიღი არ მოვა. სისტემა მუშაობს „თუ..., მაშინ...“ პრინციპით და ხილულია ათასობით ადამიანისთვის, ასე რომ, შეგიძლია ხელშეკრშეკრულების უნაკლო შესრულების იმედი გქონდეს. თუ მე გასაღებს მოგცემ, დარწმუნებული ვარ, რომ ანაზღაურებას მივიღებ. თუ შენ ბიტკოინების განსაზღვრულ რაოდენობას გამოაგზავნი, შენ მიიღებ გასაღებს. დოკუმენტი დროის გასვლის შემდეგ ავტომატურად ჩერდება და შეუძლებელია ნებისმიერი ჩვენგანის მიერ გაწერილ კოდში ჩარევა ისე, რომ მეორე პირმა ეს არ იცოდეს, რადგან პროგრამა ორივე მხარეს ერთდროულად აფრთხილებს ყველა ცვლილების შესახებ.

შენ შეგიძლია, გამოიყენო გონიერი კონტრაქტები უამრავ სხვადასხვა სიტუაციაში, როგორიცაა ფინანსური დერივატივები, სადაზღვევო პრემიები, კონტრაქტები სამართლის დარღვევაზე, საკუთრების კანონი, კრედიტები, ფინანსური სერვისები, ლეგალური პროცესები და crowdfunding შეთანხმებები.

გთავაზობთ, გონიერი კონტრაქტეის გამოყენების რამდენიმე მაგალითს:

​

**ხელისუფლება**

​

სავარაუდოდ, ძალიან რთული იქნება არჩევნების სისტემის გარდაქმნა, მაგრამ მიუხედვად ამისა, გონიერი კონტრაქტები შეასუსტებენ ნებისმიერ თავის ტკივილს ბევრად უფრო დაცული სისტემის შექმნით. დავთრის მიერ დაცული ხმები დეკოდირდება და ძალიან ძლიერი კომპიუტერული ენერგია დასჭირდება მასში შეღწევას. არავის აქვს ამდენი კომპიუტერული ენერგია, ასე რომ საჭირო იქნება ღმერთი ამ სისტემის გასატეხად! მეორეს მხრივ, გონიერი კონტრაქტები შეძლებენ, ამომრჩეველთა დაბალი აქტივობით გამოწვეული პრობლემების მოგვარებას. საარჩევნო პროცესში, ამომრჩეველთა დაბალი აქტივობა, ძირითადად გამოწვეულია  იმ დისკომფორტით თუ ძალისხმევით, რომელიც თან ახლავს არჩევნებში ხმის მიცემას, მაგალითად  რიგში დგომა, პირადობის შემოწმება და საჭირო ფორმების შევსება. გონიერი კონტრაქტებით კი მსურველები საკუთარ ხმას გადააგზავნიან ელექტრონულად, შესაბამისად თავიდან აირიდებენ ამ ყველა უსიამოვნებას.

**​**

**მენეჯმენტი**

​

ბლოკჩეინი არა მხოლოდ გამოყოფს ერთ დავთარს, როგორც ნდობის წყაროს, არამედ წმენდს მას მოსალოდნელი პრობლემებისგან კომუნიკაციასა და საქმის მიმდინარეობაში თავისი აკურატიულობის, გამჭირვალობისა და ავტომატიზირებული სისტემის მეშვეობით. ჩვეულებრივ, ბიზნეს ოპერაციები წინ და უკან მოძრაობენ, უცდიან დამტკიცებებს და აგვარებენ შიდა და გარე პრობლემებს, რათა საქმეში გაერკვნენ. ბლოკჩეინის საბუღალტრო წიგნაკი მთელს პროცესს სწორხაზოვნად წარმართავს. ის ასევე თავიდან იშორებს შეუსაბამობებს, რაც ძირითადად წარმოიშვება ხოლმე დამოუკიდებელი პროცესის დროს და რომელსაც ხანდახან დამატებით გადასახადებთან მივყავართ დაგვიანებებისა და სხვა საკითხების გამო.

**საინტერესო ფაქტი**

**​**

2015 წელს, Depository Trust & Clearing Corp. (DTCC)-მა გამოიყენა ბლოკჩეინის დავთარი 1.5 კვადრილიონ დოლარზე მეტის ღირებულების  ფასიანი ქაღალდების დამუშავებისთვის, რასაც 345 მილიონი ტრანზაქცია დასჭირდა.

**​**

**უძრავი ქონება**

**​**

შენ შეგიძლია, გონიერი კონტრაქტებით მეტი ფული გააკეთო. ჩვეულებრივ, თუ შენ შენი ბინის გაქირავება გენდომებოდა, მოგიწევდა შუამავლისთვის გადახდა, როგორიცაა Craigslist, ან გაზეთი რეკლამირებისთვის და ასევე მისთვის, ვინც დაადასტურებდა, რომ მეორე პირმა ბინის ქირა გადაიხადა (ბანკი) და სახლიც მიიღო (იურისტი). ბლოკჩეინი შენს ხარჯებს ამცირებს. ერთადერთი, რაც უნდა გააკეთო არის ის, რომ ბიტკოინებით გადაიხადო და მიაბა შენი კონტრაქტი დავთარს. ყველა ხედავს მას და შენ ავტომატურ დასტურს იღებ. ბროკერები, უძრავი ქონების აგენტები, ფულის გამსესხებლები და ყველა, ვინც ქონების გაცემასთან დაკავშირებულია, სარგებელს მიიღებს, თუმცა მომავალში მათ პროფესიებს დიდი საფრთხე ემუქრება.

​

**საინტერესო ფაქტი**

ბარკლის კორპორაციული ბანკი იყენებს გონიერ კონტრაქტებს მფლობელობის შეცვლის მისათითებლად და გადასახადების ავტომატურად გადასარიცხად სხვა ფინანსურ ინსტიტუციებთან.

​

**ჯანდაცვა**

​

პირადი ჯანმრთელობის ჩანაწერები შეიძლება მიბმული და შენახული იყოს ბლოკჩეინზე,ხოლო პირადი გასაღები ჩანაწერების ნახვის უფლებას მხოლოდ სპეციფიურ ინდივიდებს მისცემს. იგივე სტრატეგია შეიძლება გამოვიყენოთ იმის უზრუნველსაყოფად, რომ კვლევა ჩატარებული იქნება HIPAA კანონის მიხედვით (უსაფრთხოდ და კონფიდენციალურად). ოპერაციების ფულადი შემოსავლები შეიძლება შევინახოთ ბლოკჩეინზე და ავტომატურად გავუგზავნოთ სადაზღვევო კომპანიებს, როგორც მომსახურების მიღების დამამტკიცებელი საბუთი. დავთარიც შეგვიძლია გამოვიყენოთ, როგორც ზოგადი ჯანმრთელობაზე ზრუნვის მენეჯერი, მაგალითად წამლებზე დასაკვირვებლად, შედეგების დასატესტად და მარაგის სამართავად.

​

**გონიერი კონტრაქტების სამომავლო განვითარება**

​

გონიერი კონტრაქტების მომავალი დამომკიდებულია მასთან დაკავშირებული პრობლემების მოგვარებაზე. მაგალითად, კორნელ თექის ([Cornell Tech](http://tech.cornell.edu/news/smart-contracts-the-next-big-blockchain-application)) ირუსიტებმა, რომლებიც ირწმუნებიან, რომ გონიერი კონტრაქტები ჩვენი ცხოვრების ყოველდღიური ნაწილი გახდება, საკუთარი თავი ამ პრობლემების მოგვარებას მიუძღვნეს.

სიმართლე რომ ითქვას, როცა საქმე გონიერ კონტრაქტებს ეხება, ჩვენ  სამეცნიერო ფანტასტიკის ეკრანებზე გადავდივართ. IT რესურს-ცენტრი ვარაუდობს, რომ გონიერმა კონტრაქტებმა შეიძლება გავლენა იქონიოს კონკრეტული ინდუსტრიების შეცვლაში, როგორიცაა, მაგალითად, იურისპრუდენცია. ამ შემთხვევაში, იურისტები გადავლენ ტრადიციული კონტრაქტების შედგენიდან სტანდარტიზირებული გონიერი კონტრაქტების ნიმუშების შექმნაზე, რომელიც წააგავს სტანდარტულ ტრადიციულ კონტრაქტებს  LegalZoom-ზე. სხვა ინდუსტრიებმა, როგორებიცაა ბითუმად მოვაჭრეები, საკრედიტო კომპანიები და ბუღალტრები, შეიძლება გამოიყენონ გონიერი კონტრაქტები ოპერაციების ნამდვილ დროში რევიზიისა და რისკის აღმოფხვრისათვის. სინამდვილეში, ბლოკჩეინის ტექნოლოგიის ვებსაიტი „ხედავს“, როგორ აერთიანებს გონიერი კონტრაქტი ქაღალდსა და ციფრულ მასალას, სადაც კონტრაქტები გადამოწმებულია ბლოკჩეინის მეშვეობით და დამტკიცებულია ფიზიკური ასლით.

​

**სად შევქმნათ გონიერი კონტრაქტები**

**​**

ბიტკოინი: ბიტკოინი ბიტკოინის სავაჭრო ოპერაციებისთვის ძალიან გამოსადეგია, მაგრამ დოკუმენტების დამუშავებისთვის შეზღუდული შესაძლებლობები აქვს.

NXT: NXT საჯარო ბლოკჩეინის პლატფორმაა, რომელიც მოიცავს გონიერი კონტრაქტების ნიმუშების შეზღუდულ არჩევანს. თქვენ უნდა გამოიყენოთ მხოლოდ ის, რაც მოცემულია; თქვენ არ შეგიძლიათ, საკუთარი კოდის შექმნა.

ეთერიუმი: ეთერიუმი საჯარო ბლოკჩეინის პლატფორმაა და ყველაზე მეტად განვითარებულია გონიერი კონტრაქტების კოდირებისა და დამუშავების სფეროში. თქვენ შეგიძლიათ, შექმნათ რაც გნებავთ, მაგრამ ასევე მოგიწევთ, დაფაროთ კომპიუტერული ენერგიის ხარჯები ეთერიუმის ჟეტონებით.

რაც შეეხება თავად გონიერი კონტრაქტების პოტენციალს, არ არსებობს იმ ინდუსტრიათა სიის დასასრული, რომელზეც მას ზეგავლენის მოხდენა შეუძლია ჯანმრთელობაზე ზრუნვიდან დაწყებული ავტომანქანებით დამთავრებული. სია გრძელდება და გრძელდება, როგორც ამას ეთერიუმის CTO, გავინ ვუდი, ამბობს:

„გონიერი კონტრაქტების პოტენციალი, შეცვალონ სოციუმის ასპექტები, საკმაოდ მაღალმნიშვნელოვანია. ეს არის რაღაც ისეთი, რაც აწარმოებს ტექნიკურ ბაზას ყველა სახის სოციალური ცვლილებისთვის და მე ეს აღმაფრთოვანებს“

აი, რისი მოცემა შეუძლია გონერ კონტრაქტს:

​

**ავტონომიურობა**- თქვენ აწარმოებთ გარიგებას; არ არსებობს დადასტურებისთვის ბროკერის, იურისტის ან სხვა შუამავალის დაქირავების აუცილებლობა. ეს ასევე თავიდან გვარიდებს მანიპულაციის საფრთხეს მესამე პირის მიერ, ვინაიდან განაჩენის გამოტანა ავტომატურად მიმდინარეობს ქსელის მეშვეობით.

​

**ნდობა -** შენი დოკუმენტები დაშიფრულია გაზიარებულ დავთარზე. არ არსებობს იმის შესაძლებლობა, რომ ვინმემ საბუთების დაკარგვა მოიმიზეზოს.

​

**რეზერვი -** წარმოიდგინე, რა მოხდებოდა, შენს ბანკს შენი დამზოგველი ანგარიში რომ დაეკარგა. ბლოკჩეინზე თითოეულ შენს მეგობარს აქვს რეზერვი. შენი დოკუმენტები მრავალჯერ დუბლირებულია.

​

**უსაფრთხოება**- კრიპტოგრაფია, ვებსაიტების შიფრირება, ინახავს შენს დოკუმენტებს უსაფრთხოდ. შეუძლებელია ანგარიშის გატეხვა. საჭიროა არარეალურად მძლავრი კომპიუტერი და გენიალური ჰაკერი, რათა კოდი გატეხოს და მონაცემები გააყალბოს.

​

**სიჩქარე**- ჩვეულებრივ, თქვენ დაგჭირდებოდათ ძალიან ბევრი დროის დაკარგვა და საბუთების შედგენა, რათა ხელით დაგემუშავებინათ დოკუმენტები. გონიერი კონტრაქტი იყენებს პროგრამულ კოდს დავალებების ავტომატურად სამართავად, რისი მეშვეობითაც, ბიზნესის პროცესის უმეტეს დროს ზოგავს

​

**დანაზოგი**- გონიერი კონტრაქტები ზოგავს შენს ფულს, ვინაიდან ის შუამავალს აშორებს საქმეს. მაგალითად, შენ მოგიწევდა ნოტარიუსისთვის ანაზღაურების მიცემა, რათა სავაჭრო ოპერაციას დასწრებოდა და იურიდიულად დაედასტურებინა იგი.

​

**აკურატულობა -** ავტომატური კონტრაქტები არ არის მხოლოდ სწრაფი და იაფი, არამედ ის თავს არიდებს უნებლიე შეცდომებს, რომლებსაც უამრავი ფორმების ხელით შევსებისას უშვებენ ხოლმე.

აი, როგორ აღწერს გონიერ კონტრაქტებს ჯეფ გარზიკი, ბლოკჩეინის სერვისის, ბლოქის, მფლობელი:

„გონიერი კონტრაქტები... გპირდებიან ძალიან, ძალიან სპეციფიურ შედეგებს. არ არსებობს დაბნეულობა და კამათის საჭიროება“

​

**გონიერ კონტრაქტებთან დაკავშირებული პრობლემები**

**​**

გონიერი კონტრაქტები ძალიან შორსაა იდალურისგან. რა მოხდება მაშინ, თუ კოდში ხარვეზი  გამოჩნდება? ან როგორ უნდა დაარეგულიროს ხელისუფლებამ ასეთი კონტრაქტები? როგორ უნდა დააწესოს ხელისუფლებამ გადასახადები გონიერი კონტრაქტებით ჩატარებულ სავაჭრო ოპერაციებზე?

რა მოხდება, თუ მე არასწორ კოდს გადავაგზავნი, ან, როგორც იურისტი ბილ მარინო აღნიშნავს, სწორ კოდს გადავაგზავნი, მაგრამ ჩემი ბინა უკვე გაქირავებული აღმოჩნდება, სანამ გაქირავების თარიღი დადგება? ეს რომ ტრადიციული კონტრაქტი ყოფილიყო, მე შევძლებდი მის გაუქმებას სასამართლოში, მაგრამ ბლოკჩეინი სხვა შემთხვევაა. კონტრაქტი ყოველთვის ხორციელდება ყველაფრისდა მიუხედავად.

გამოწვევების სია გრძელდება და გრძელდება. ექსპერტები ცდილობენ პრობლემების გამოსწორებას, მაგრამ ეს კრიტიკული შემთხვევები პოტენციურ მომხმარებლებს, ამ ტექნოლოგიის გამოყენებაზე უარის თქმას აიძულებენ. გონიერი კონტრაქტები, ისევე როგორც ბლოკეინი, ჯერ კიდევ განვითრების ადრეულ სტადიაზეა და უდავოა, რომ არსებული პრობლემები მომავალში აუცილებლად მოგვარდება!

​

**თავი 12. სხვა კრიპტოვალუტები. ICO და IPO კონცეფციები.**

წინასწარი ICO. ICO და crowdfunding. კავშირი კრიპტოვალუტებთან და ბლოკჩეინის ტექნოლოგიებთან.Litecoin,Altcoin , Ethereum, Ripple, Dash და სხვა

მარტივად რომ ავხსნათ, ეთერიუმი ბლოკჩეინზე დაფუძნებული ღია ქსელის პლატფორმაა, რომელიც დეველოპერებს საშუალებას აძლევს, ააგონ დეცენტრალიზებული აპლიკაციები.

**​**

**არის ეთერიუმი ბიტკოინის მსგავსი? - დაახლოებით, მაგრამ არა ბოლომდე.**

​

ბიტკოინის მსგავსად, ეთერიუმი საჯარო განაწილებული ბლოკჩეინის ქსელია. მიუხედავად იმისა, რომ მათ შორის ყურადსაღები ტექნიკური განსხვავებები არსებობს, ყველაზე მნიშვნელოვანი სხვაობაა ის, რომ ბიტკოინი და ეთერიუმი ერთმანეთისგან არსებითად განსხვავდებიან არსსა და შესაძლებლობებში. ბიტკოინი გვთავაზობს ბლოკჩეინ ტექნოლოგიის ერთ კონკრეტულ გამოყენებას - პირისპირა ელექტრონულ სისტემას, რომელიც შესაძლებელს ხდის ონლაინ (ბიტკოინით) გადახდებს. თუ ბლოკჩეინი გამოყენებულია ციფრული ვალუტის (ბიტკოინის) მფლობელობის დასადგენად, ეთერიუმის ბლოკჩეინი კონცენტრირდება ნებისმიერი დეცენტრალიზებული აპლიკაციის პროგრამული კოდის ამუშავებაზე.

ეთერიუმის ბლოკჩეინში, ბიტკოინისთვის მოპოვების ნაცვლად, მომპოვებლები მუშაობენ ეთერისთვის, კრიპტო მონეტისთვის, რომელიც ქსელს ამუშავებს (იხილეთ ჩვენი გზამკვლევი - რა არის ეთერი?) . სავაჭრო კრიპტოვალუტასთან ერთად, ეთერი ეთერიუმის ქსელში ასევე გამოიყენება ტრანზაქციების საკომისიოებისა და სერვისების გადასახდელად აპლიკაციების დეველოპერების მიერ.

​

*„ბიტკოინი პირველი კრიპტოვალუტაა; ეს ერთი კონკრეტული ბლოკჩეინის გამოყნებაა. თუმცა, ტექნოლოგიას სხვა ძალიან ბევრი შესაძლებლობა აქვს. მსგავსი სიტუაციის წარსული მაგალითი რომ ავიღოთ, იმეილი ინტერნეტის ერთი კონკრეტული გამოყენებაა და ნამდვილად დაეხმარა მის პოპულარიზებას, მაგრამ მის გარდა სხვა ბევრი გამოყენების საშუალება არსებობს.“* - გევინ ვუდი, ეთერიუმის ერთ-ერთი დამფუძნებელი.

ეთერიუმი საშუალებას აძლევს დეველოპერებს, ააგონ დეცენტრალიზებული აპლიკაციები. დეცენტრალიზებული აპლიკაცია, ანუ დაპლი (Dapp), რაღაც კონკრეტულ სამსახურს უწევს მის მომხმარებლებს. მაგალითად, ბიტკოინი არის დაპლი, რომელიც მომხმარებლებს სთავაზობს პირისპირა ელექტრონული ფულის სისტემას, რომელიც შესაძლებელს ხდის ონლაინ გადახდებს. იმის გამო, რომ დეცენტრალიზებული აპლიკაციები იქმნება კოდისგან, რომელიც ბლოკჩეინის ქსელზე მუშაობს, მათ ვერ აკონტროლებს ერთი ინდივიდი ან ცენტრალური პირი.

ნებისმიერი სერვისი, რომელიც ცენტრალიზებულია, შეიძლება გახდეს დეცენტრალიზებული ეთერიუმის გამოყენებით. დაფიქრდი ყველა შუამავალ სერვისზე, რომელიც არსებობს ასობით სხვადასხვა ინდუსტრიაში: აშკარა სერვისებიდან, როგორიცაა ბანკის მიერ გაცემული სესხები, ისეთ შუამავალ სერვსებამდე, რომელზეც უფრო ნაკლებად ვფიქრობთ, მაგალითად, სახელების რეგისტრაციამდე, ხმის მიცემის სისტემამდე და სხვა.

ეთერიუმი ასევე შეიძლება გამოვიყენოთ დეცენტრალიზებული ავტონომიური ორგანიზაციების (DAO) შესაქმნელად. დაო სრულად ავტონომიური, დეცენტრალიზებული ორგანიზაციაა, რომელსაც ერთი ლიდერიც კი არ ჰყავს. დაო მუშაობს პროგრამულ კოდზე და გონიერი კონტრაქტების ერთობლიობაზე, რომლებიც ეთერიუმის ბლოკჩეინზეა ჩაწერილი (იხილეთ ჩვენი გზამკვლევები გონიერ კონტრაქებზე). კოდი შეიქმნა, რათა ჩაენაცვლებინა ტრადიციული ორგანიზაციების წესები და სტრუქტურა, გაექრო ადამიანის ყოფნისა და ცენტრალიზებული კონტროლის საჭიროება. დაოს ფლობს ყველა, ვინც იძენს მონეტებს, მაგრამ იმის მაგივრად, რომ თითოეული მონეტა ათანასწორებდეს თანასწორ წილსა და მფლობელობას, მონეტები მოქმედებენ, როგორც კონტრიბუცია, რომელიც ხალხს ხმის მიცემის უფლებას აძლევს.

*„დაო შედგება ერთი ან მრავალი კონტრაქტისგან და შეიძლება დაფინანსდეს ერთ აზრზე მყოფი ადამიანების ჯგუფის მიერ. დაო მუშაობს სრულიად გამჭირვალედ და ადამიანების ჩარევისგან დამოუკიდებლად (დამფუძნებლებისაც კი). დაო ქსელში დარჩება იმდენ ხანს, რამდენ ხანსაც შეძლებს, საკუთარი თავის უზრუნველყოფის ხარჯების დაფარვას და გამოყენებადი სერვისების შემოთავაზებას კლიენტებისთვის.“* - სტეფან ტუალი, Slock.it-ის დამფუძნებელი, ეთერიუმის ყოფილი CCO.

**​**

**დეცენტრალიზებული აპლიკაციების უპირატესობები**

**​**

ვინაიდან დეცენტრალიზებული აპლიკაციები მუშაობენ ბლოკჩეინზე, ისინი სარგებელს იღებენ ყველა მისი თავისებურებებით:

​

* **გარდაუვალობა** - მესამე პირს მონაცემებში არანაირი ცვლილების შეტანა არ შეუძლია.
* **კორუფციისა და ჩარევის მტკიცებულება**- აპლიკაციები ეფუძნება ქსელს, რომელიც კონსენსუსის პრიციპის გარშემო ტრიალებს, რის გამოც ცენზორის არსებობა შეუძლებელია.
* **უსაფრთხო** - დამარცხების ცენტრალური წერტილის არარსებობის გამო და იმის გამო, რომ ბლოკჩეინი დაცულია კრიპტოგარიფიულად, აპლიკაციები კარგადაა დაცული ჰაკერების შემოტევებისა და თაღლითური ქმედებებისგან.
* **გათიშვის არარსებობა (Zero downtime)** - აპლიკაციები არასდროს ითიშება.

**რა არის დეცენტრალიზებული აპლიკაციების უარყოფითი მხარე?**

**​**

უპირატესობების სიმრავლის მიუხედავად, დეცენტრალიზებული აპლიკაციები უნაკლო არ არის. იმის გამო, რომ გონიერ კონტრაქტებს ადამიანები წერენ, ისინი მხოლოდ იმდენად კარგია, რამდენადაც ეს ადამიანები. კოდის ხარვეზებმა ან წინდაუხედაობამ შეიძლება მოულოდნელ უკუჩვენებამდე მიგვიყვანოს. თუ კოდში შეცდომა გაიპარა, არ არსებობს შეტევის, ან ექსპლუატაციის თავიდან აცილების ეფექტური გზა, გარდა ქსელის კონსენსუსის შენარჩუნებისა და ძირითადი კოდის თავიდან დაწერისა. ეს ბლოკჩეინის მთავარ იდეას ეწინააღმდეგება: მის შეუცვლელობას. ამასთან, ნებისმიერი ქმედება, რომელსაც ცენტრალური პირი სჩადის, სერიოზულ კითხვებს ბადებს აპლიკაციის დეცენტრალიზებულ ბუნებასთან დაკავშირებით.

​

**DAO-ს ჰაკი, რომელმაც ამ ყველაფერს საფრთე შეუქმნა**

**​**

2016 წელს, რაღაც ძალიან ცუდი მოხდა. „the DAO”-დ წოდებული სტარტაპი, რომელიც ერთ კონკრეტულ დაოს პროექტზე მუშაობდა, დაიჰაკა.

დაო იყო პროექტი, რომელიც შეიმუშავა და დააპროგრამირა კიდევ ერთი სტარტაპის, Slock.it-ის, უკან მდგომმა გუნდმა. მათი მიზანი იყო ისეთი რისკიანი კაპიტალის ფირმის (Venture Capital) შექმნა, რომელსაც ადამიანი არ სჭირდებოდა და რომელიც საშუალებას მისცემდა ინვესტორებს, გონიერი კონტრაქტების მეშვეობით მიეღოთ გადაწყვეტილება. დაო ფინანსდებოდა მონეტების გაყიდვით და 150 მილიონ დოლარამდე იშოვა სხვადასხვა ადამიანებისგან.

დაფინანსებიდან ცოტა ხანში, დაო დაჰაკა უცნობმა თავდამსხმელმა, რომელმაც დაახლოებით იმდროინდელი 50 მილიონი დოლარის ოდენობის ეთერი მოიპარა. მიუხედავად იმისა, რომ  შეტევა შესაძლებელი გახდა დაოს პროგრამაში გაპარული ხარვეზის და არა ეთერიუმის პლატფორმის გამო. პრობლემის მოგვარება ეთერიუმის დეველოპერებსა და დამფუძნებლებს მოუწიათ.

​

**ეთერიუმი - დეცენტრალიზებული მომავალი**

**​**

დაოს ჰაკის მიუხედავად, ეთერიუმი წინ მიიწევს და მას ნათელი მომავალი ელის. მომხმარებელზე მორგებული პლატფორმის შექმნით, რომელიც საშუალებას აძლევს ადამიანებს, გამოიყენონ ბლოკჩეინ ტექნოლოგიის შესაძლებლობები, ეთერიუმი მსოფლიო ეკონომიკის დეცენტრალიზაციას აჩქარებს. დეცენტრალიზებულ აპლიკაციებს გააჩნიათ პოტენციალი, ძირფესვიანად აღმოფხვრან ასობით ინდუსტრია ფინანსების, უძრავი ქონების, აკადემიის, დაზღვევის, ჯანდაცვისა და საჯარო სექტორის ჩათვლით სხვა მრავალთან ერთად.

​

„*თუ შენ თვლი, რომ ინტერნეტმა შენს ცხოვრებაზე გავლენა იქონია, ეთერიუმს იგივე ზეგავლენა ექნება ჩვენს კომუნიკაციებზე, ჩვენს მთლიან ინფორმაციის ინფრასტრუქტურაზე. ის ჩვენი არსებობის ყოველ ასპექტს შეეხება.*

*მისი გამოყენება უკვე შეიძლება Crowdfunding პლატფორმების (Weifund), ჯგუფური ხელისუფლების ინსტრუმენტების (Boardroom), მუსიკის/ფილმის/ხელოვნების მასალის რეგისტრაციის და სარგებლიანი პლატფორმების (ujo), ბრძენი ბაზრების (Gnosis) და სათამაშო აპლიკაციების (Virtue Poker) მიზნებისათვის*.“

.

​

**თავი 13. მოპოვება (Mining)**.

რას აკეთებენ მაინერები. როგორ მუშაობს ბიტკოინის მოპოვება. როგორ გამოვთვალოთ მოპოვების მომგებიანობა. რა არის სამომპოვებლო ბრიგადა.

ტრადიციულ მონეტარულ სისტემაში, სახელმწიფო (ან ცენტრალური ბანკი) ბეჭდავს ახალ კუპიურებს, როდესაც ეს მას სჭირდება. ბიტკოინის შემთხვევაში კი, ფული საერთოდ არ იბეჭდება - ხდება მისი აღმოჩენა. მთელი მსოფლიოს მასშტაბით, ქსელში ჩართული კომპიუტერები „მოიპოვებენ“ მონეტებს ერთმანეთთან შეჯიბრის პრინციპით.

ადამიანები განუწყვეტლივ უგზავნიან ბიტკოინს ერთმანეთს ქსელის მეშვეობით. მაგრამ, თუ ვინმე ამ ყველაფერს არ აღრიცხავს, ვერავინ შეძლებს გაიგოს, რეალურად ვინ რამდენი გადაიხადა  და ვის რამდენი ბიტკოინი აქვს. ამ ყველაფრის აღრიცხვისათვის, ბიტკოინი აწარმოებს ტრანზაქციების სიას, რომელიც დაგროვდა გარკვეული დროის განმავლობაში და თავს უყრის მათ ერთ ბლოკში. მომპოვებლის, ანუ მაინერის, ფუნქციაა, დაადასტუროს ეს ტრანზაქციები და ჩაწეროს ისინი საერთო დავთარში, რომლის ასლიც ყველა ქსელში ჩართულ კომპიუტერში ინახება.

​

**რაში გამოიყენება ჰაში**

**​**

ზემოთხსენებული საერთო დავთარი არის ბლოკების გრძელი სია, რომელსაც ბლოკჩეინს უწოდებენ. მისი გამოყენება შესაძლებელია იმისათვის, რომ ვნახოთ თითოეულ მისამართზე ბიტკოინების შემოსავლებისა და ხარჯების ისტორია. ყოველი ახალი ტრანზაქციის შექმნით, ინფორმაცია ამ დავთარს ემატება. ამგვარად იქმნება ძალიან გრძელი და მზარდი სია, სადაც ყველა ტრანზაქციის შესახებ ინფორმაცია არის მოცემული, რომელიც ბიტკოინის ბლოკჩეინზე ოდესმე განხორციელებულა. ქსელში ჩართულ ყველა მონაწილეს ეგზავნება ყოველი ტრანზაქციის შესახებ ინფორმაცია და მათ ხელთ არსებული დავთრის ასლი ავტომატურად განახლებადია.

ცხადია, ეს დავთარი ძალიან სანდო უნდა იყოს. ვინაიდან იგი ციფრულად ინახება, ის დაცული უნდა იყოს ჰაკერული თუ სხვა ტიპის შემოტევებისგან და არ უნდა არსებობდეს მასში წარსული მონაცემების შეცვლის შესაძლებლობა. სწორედ ამ მიზანს ემსახურებიან მომპოვებლები.

როდესაც ხორციელდება ბიტკოინ ტრანზაქცია, მაინერები იღებენ ამ ტრანზაქციის შესახებ ინფორმაციას, უსადაგებენ მას მათემატიკურ ფორმულას და გარდაქმნიან ამ მათემატიკური ფუნქციის ამონახსნად.  ეს ამონახსნი შემთხვევითი თანმიმდევრობით დალაგებული ასოებისა და ციფრების კომბინაციაა, რომელსაც ჰაში ეწოდება. ეს ჰაში დროის ნებისმიერ მომენტში ინახება ბლოკთან ერთად ბლოკჩეინის ბოლო ჩანაწერში.

ჰაშებს საკმაოდ საინტერესო თვისება აქვთ. ნებისმიერი ინფორმაციისთვის ჰაშის პოვნა შედარებით მარტივია, მაგრამ შეუძლებელია ამონახსნიდან ვიპოვოთ, რა იყო თავდაპირველი ინფორმცია.  ამასთან, ყოველი ჰაში (ამონახსნი) უნიკალურია: თუ ბლოკში შეიცვლება ძალიან უმნიშვნელო ინფორმაციაც კი, მისი ჰაში აბსოლუტურად განსხვავებული გახდება.

მაინერები ჰაშის გამოსათვლელად არა მხლოდ კონკრეტულ ბლოკში მოცემულ ინფორმაციას ითვალისწინებენ, არამედ წინა ბლოკის ჰაშსაც - სწორედ აქედან მოდის სახელი ბლოკჩეინი - ანუ ბლოკების ჯაჭვი.

იმის გამო, რომ ყოველი ახალი ჰაში მოიცავს წინა ბლოკის ჰაშსაც, შეგვიძლია შევხედოთ მას, როგორც პლომბს და თუ ერთი პლომბი მაინც გაიხსნება, ეს აისახება ყოველ მის შემდგომ ბლოკზე, რადგან თთოეული მათგანის ჰაში განახლებული ინფორმაციის საფუძველზე იქნება დასათვლელი.

თუ ვინმე გადაწყვეტს, რომ შეცვალოს ან გააყალბოს ტრანზაქცია, რომელიც უკვე ბლოკჩეინში არის ჩაბეჭდილი, მისი ჰაში შეიცვლება. ასევე შეიცვლება ყველა მისი შემდეგი ბლოკის ჰაში. შესაბამისად, უახლესი ტრანზაქციის / ბლოკის ჰაში განსხვავებული იქნება ქსელში ჩართული ყველა მონაწილის დავთარში მოცემული მაჩვენებლისგან და მთელი ქსელი მიხვდება, რომ ეს ბლოკი გაყალბებულია.

​

**ფულადი სარგებელი**

**​**

ჩვენ უკვე განვიხილეთ, როგორ ილუქება ბლოკები. ყველა ქსელში ჩართული კომპიუტერი ეჯიბრება ერთმანეთს ამის გაკეთებაში და ამისათვის ისინი იყენებენ სპეციალურად ბიტკოინის ბლოკჩეინისათვის დაწერილ პროგრამას. როდესაც ვინმე წარმატებით ამოხსნის ჰაშს, ჯილდოდ იღებს 12,5 ბიტკოინს. ყველა ქსელში ჩართული კომპიუტერი ხედავს და ადასტურებს ამას. სწორედ ასე ხდება ნოდების წახალისება, რათა მათ გააგრძელონ მოპოვება და ტრანზაქციების დადასტურება.

ამ ყველაფრის პრობლემა იმაში მდგომარეობს, რომ ჰაშის ამოხსნა ძალიან რთულია, შესაბამისად, კომპიუტერული ენერგია, რომელიც გამოიყენება ბიტკოინების მოსაპოვებლად, მუდმივად იზრდება. ალგორითმის ამოხსნა მარტივი, რომ ყოფილიყო ეს გამოიწვევდა ბიტკოინების მარაგის სწრაფად ამოწურვას, რადგან ნოდები შეძლებდნენ წამში ათასობით ჰაშის ამოხსნას და ამისათვის მიიღებდნენ ბიტკოინებს. ამიტომაც ბიტკოინის პროტოკოლი (პროგრამა)„სამუშაოს შესრულების მტკიცებულების“ (Proof of Work) შემოტანით მიზანმიმართულად ართულებს მოპოვების პროცესს.

ბიტკოინის პროტოკოლში ჰაშს კონკრეტული მახასიათებლები უნდა ჰქონდეს, მაგალითად იგი რამოდენიმე 0-იანით უნდა იწყებოდეს, მაგრამ მის ამოხსნამდე იმის განსაზღვრა, თუ როგორი იქნება ჰაში, შეუძლებელია. ყოველი ახალი, თუნდაც მიზერული ინფორმაციის ცვლილებით განახლებული ჰაში აბსოლუტურად იცვლება.

ამ ყველაფრის გარდა, ბიტკოინის პროგრამაში გაჩნდა შემთხვევითი სიდიდე, „ნონსი“, რომელიც ასევე მონაწილეობს ბლოკის შექმნაში. თუ ტრანზაქციის ჰაში არ აკმაყოფილებს გარკვეულ მოთხოვნებს (მაგალითად იმას, რომ არ იწყება რამოდენიმე 0-იანით), ჩნდება ისეთი „ნონსის“ პოვნის საჭიროება, რომელიც ამონახსნს მოარგებს აღნიშნულ ფორმატს. ვინაიდან ნონსი შემთხვევითი სიდიდეა და არ ექვემდებარება ლოგიკურ ახსნას, მაინერები ცდილობენ, იპოვონ საჭირო ნონსი უამრავი ვარიანტის ცდით.

აი, ასე ხდება ბიტკოინის მოპოვება!

თუ სერიოზულად ფიქრობ კრიპტოვალუტის მაინინგს, აუცილებელია იცოდე, როგორ გამოიყენო ოპტიმალურად საკუთარი სახსრები და კომპიუტერული ტექნიკა. ამ სტატიის მიზანია, დაგეხმაროს ოპტიმალური გადაწყვეტილების მიღებაში.

ცხადია, საკმაოდ დიდი თანხები იხარჯება ბიტკოინის ასიკ მაინერებში (ASICs). თუ შენ გაქვს ასეთი მოწყობილობა, უკვე იცი, როგორ მუშაობს ეს დანადგარები და აპირებ, ან უკვე მოიპოვებ, ბიტკოინს. ეს სტატია მათთვისაა, ვისაც უფრო ნაკლები თანხა აქვს და ფიქრობს GPU მაინერის შეძენას Scrypt-ზე მომუშავე ვალუტების მოსაპოვებლად, ან მცირე სიმძლავრის ასიკის შეძენას ბიტკოინის ან სხვა SHA-256 ალგორითმზე მომუშავე ვალუტების მოსაპოვებლად.

​

**საიდან დავიწყოთ?**

​

კრიპტოვალუტების მოპოვების პროცესი მოიცავს რთული კრიპტოგრაფიული ფუნქციების ამოხსნას. ამ ფუნქციების ამოხსნით, მაინერები ქსელს აწვდიან „სამუშაოს შესრულების მტკუცებულებას“ (Proof of Work) და ამისათვის საჩუქრდებიან კრიპტოვალუტით. სამუშაოს შესრულების მტკიცებულებაზე მომუშავე ალგორითმები, რომლებიც დღეს გამოიყენება, არის: SHA-256 და Scrypt. გარდა ამისა, არსებობს უფრო ნაკლებად გამოყენებადი ალგორითმებიც, რომლებსაც ამ სტატიაში არ შევეხებით (მაგალითად PrimeCoin)

* SHA-256 - ეს არის ალგრითმი, რომელიც უპირატესობას ანიჭებს გადამუშავების სისწრაფეს. ბიტკოინის ადრეულ სტადიებზე მოპოვება შესაძლებელი იყო როგორც CPU, ასევე GPU-ს (graphics processing units) მეშევეობით, რომელიც ხელმისაწვდომი იყო ჩვეულებრივ სახლის კომპიუტერზე. სამწუხაროდ, ამ დრომ კარგა ხანია ჩაიარა და ბიტკოინის მოპოვების სირთულიდან გამომდინარე, დღეს დღეობით აუცილებელია ე.წ. ასიკ მაინერები (ASICs). ასეთი მძლავრი პროცესორების გამოყენებამ გამოიწვია ბიტკოინის მოპოვების სირთულის მკვეთრი ზრდა, რაც თავის მხრივ გადაიზარდა ტექნოლოგიურ კონკურენციაში და დღეისათვის ყველაზე მძლავრი ტექნიკაც კი შეიძლება ხვალ უსარგებლო გახდეს იმის გამო, რომ გამოვიდეს ახალი, გაუმჯობესებული მაინერი.
* Scrypt - ალგორითმი უპრირატესობას ანიჭებს RAM-ს და პარალელურ გამოთვლის შესაძლებლობას. ამის გამო, ასიკები ჯერ-ჯერობით არ არიან გამოსადეგნი ამ ალგორითმზე მომუშავე ვალუტების მოსაპოვებლად. ამიტომაც, ასეთი ვალუტების  ბლოკჩეინის ქსელის მთლიანი სიმძლავრე გაცილებით ნაკლებია.

შენი ბიუჯეტისა და სასურველი ვალუტის განსაზღვრის შემდეგ საჭიროა, მომპოვებელი სისტემის შერჩევა. აქ არსებობს ორი ძირითადი არჩევანი:

* DIY სამომპოვებლო ტექნიკა - შესაძლებელია აეწყოს სახლის პირობებში აწყობა, როგორც წესი მაინერებს სპეციალურ პლატფორმაზე ამონტაჟებენ. მისი უპირატესობა იმაში მდგომარეობს, რომ შესაძლებელია როგორც GPU, ასევე CPU სიმძლავრის გამოყენება მოპოვებისათვის;
* ASIC-ები არის ცალკე მოწყობილობა, რომელიც მონტაჟდება სპეციალური ადაპტერების მეშვეობით და მათ, როგორც წესი, მოყვება ეთერნეტის ან USB პორტები. როგორც წესი, მათი ღირებულება უფრო მეტია, ვიდრე DIY-სა.

​

**ენეგიის მოხმარება**

​

მაინინგი საკმაოდ დიდ ელექტროენრგიის დანახარჯთანაა დაკავშირებული. როდესაც აწყობ მაინერს, საჭიროა მხედველობაში მიიღო მისი ელექტროენერგიის მოთხოვნები, განსაკუთრებით იმ შემთხვევაში, როდესაც მოიპოვებ ვიდეო კარტების მეშვეობით, რადგან მათმა დიდმა რაოდენობამ შესაძლოა გადატვირთოს ელექტროენერგიის ქსელი და პრობლემები შეგექმნას მის მოწოდებასთან დაკავშირებით.

მეორეს მხრივ, ასიკები გაცილებით მეტს კალკულირებენ გაცილებით ნაკლები ენერგიის სანაცვლოდ, ვინაიდან ეს არის სპეციალიზებული ტექნიკა კონკრეტულად მოპოვებისათვის და ამასთან, როგორც წესი, მოჰყვება ადაპტორი.

მოპოვების ეფექტურობა სხვადასხვა სისტემაზე მომუშავე მაინერებისათვის შეგვიძლია გავზომოთ მისი სისწრაფის (წამში ამოხსნილი ჰაშების რაოდენობა) შეფარდებით მის მიერ მოპოვებულ ენერგიაზე: (ჰაშ სისწრაფე / ენერგიის მოხმარება = მოპოვების ეფექტურობას)

​

**შეამოწმე გადასახადი!**

**​**

მაინერის ღირებულების გადახდის შემდეგ, მთავარი ხარჯი სწორედ ელექტროენერგიის ხარჯია. ამიტომ, მომგებიანობის დასათვლელად აუცილებელია, გავითვალისწინოთ ეს ხარჯიც. თუ ელექტროენერგიის ხარჯი აჭარბებს, ან ძალიან უახლოვდება, მიღებულ შემოსავალს, ცხადია, მოპოვება არ არის მომგებიანი.

​

**გაერთიანდი ბრიგადაში**

​

ჩვენს გზამკვლევში, რა არის სამომპოვებლო ბრიგადა, ვრცლადაა აღწერილი მოპოვების ეს მეთოდი. თუცა, მოკლედ რომ ვთქვათ, თითქმის ყოველთვის უმჯობესია, გაერთიანდეთ ასეთ ბრიგადაში, რადგან ერთობლივად ბევრ მაინერს აქვს მეტი შანსი, მიიღოს ბლოკის ჯილდო. როგორც წესი, ეს ჯილდო თითოეულ მაინერზე ნაწილდება მათი სიმძლავრის მიხედვით.

**თავი 14. გამოყენებები**.

ფულადი გზავნილები და ფულის გაცვლა. ვებ-საფულეები. ბანკომატები. სმარტ-კონტრაქტები. რეესტრები. ნოტარიუსი.

დღევანდელ სტატიაში ვაგრძელებთ საუბარს “განაწილებული დავთარის ტექნოლოგია”-ზე (“distributed ledger technology” – DLT), ე.წ.  ბლოკჩეინის ტექნოლოგიაზე. მიუხედავად იმისა, რომ DLT-ი სწრაფი, იაფი და დეცენტრალიზებული გადახდის სისტემის შექმნის იდეამ გააჩინა, ის გადატრიალებას ახდენს თანამედროვე სამყაროში. კრიპტოვალუტები, რის გამოც ამ ტექნოლოგიას მეტწილად იცნობს ხალხი, არ არის დღევანდელი სტატიის მთავარი ფოკუსი. ამ ციკლის პირველ სტატიაში – *“*[*ბლოკჩეინი და მისი მომავალი – ჩინეთი*](https://mybitcoin.ge/2018/08/20/%E1%83%91%E1%83%9A%E1%83%9D%E1%83%99%E1%83%A9%E1%83%94%E1%83%98%E1%83%9C%E1%83%98-%E1%83%93%E1%83%90-%E1%83%9B%E1%83%98%E1%83%A1%E1%83%98-%E1%83%9B%E1%83%9D%E1%83%9B%E1%83%90%E1%83%95%E1%83%90/)*”*, ჩვენი მკითხველი უკვე გაეცნო ჩინეთის მიღწევებს ბლოკჩეინის გავითარების საქმეში. თუმცა, არც სხვა განვითარებულ ქვეყნებს გამორჩენიათ თვალთახედვიდან ეს ტექნოლოგია და დღეს სწორედ მათზე გიამბობთ.



მსოფლიოს ერთერთმა წამყვანმა აუდიტორულმა კომპანიამ “დელიოტი” გამოაქვეყნა “[*გლობალური ბლოკჩეინის კვლევა 2018*](https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-2018-global-blockchain-survey-report.pdf)”.

მას შემდეგ, რაც მსოფლიოს სხვადასხვა ქვეყანაში ბაზრებმა აქტიურად დანერგა DLT-ი ისეთ სფეროებში, როგორიცაა ინფორმაციის შენახვა/აღრიცხვა, ლოჯისტიკა, ჯანდაცვა და ფინანსური ტექნოლოგიები, ინოვაციები და სახელმწიფოების მხარდაჭერა ამ სფეროში საგრძნობლად იზრდება.

კვლევის თანახმად, ბიზნესები აქტიურად ნერგავენ ბლოკჩეინს საკუთარ საქმიანობაში. DLT-ს აქვს შესაძლებლობა მოაწესრიგოს მოკლევადიანი და გრძელვადიანი ბიზნეს პროცესები. ყველა ბიზნესი დაფუძნებულია ქსელში აქტივების გაცვლაზე და ბლოკჩეინის ტექნოლოგია იძლევა ამ პროცესების დაუყოვნებლივ აუდიტისა და დამოწმების შესაძლებლობას. ეს კი მისწრებაა ყველა ბიზნესისთვის, რადგან იზრდება ეფექტურობა და მცირდება ხარჯები. ამიბიციურმა ბიზნეს ლიდერებმა უკვე დაიწყეს მისი ყოველდღიურ ოპერაციებში გამოყენება, მაგალითად ისეთი პროგრამის როგორიცაა “Microsoft Power Ledger”.

მაშინ, როდესაც უკვე უამრავი ბიზნესი იყენებს ბლოკჩეინის ტექნოლოგიას ყოველდღიურ საქმიანობაში, სხვა ბლოკჩეინზე დაფუძნებული აპლიკაციები ქმნიან სრულიად ახალ შესაძლებლობებს. კვლევამ დაამტკიცა, რომ ტრადიციული ბიზნესების 74%-ს შეუძლია ბლოკჩეინის გამოყენება თავიანთ ბიზნეს პროცესებში. DLT-ის ერთერთი ძირითადი უპირატესობაა ადამიანებისა და ინფორმაციის უსაფრთხოების მაღალი დონე, რაც არის ამ ახლად აღმოცენებული ინდუსტრიის ქვაკუთხედი.



ჰონგკონგის მთავრობა უკანასკნელ პერიოდში შეწუხებულია ფინტექის მიმართულებით ინოვაციების ნაკლებობით. სწორედ ამიტომ მათი ყურადღება მიიპყრო DLT-იმ და ამ მიზნით “ჰონგკონგის მეცნიერებისა და ტექნოლოგიის უნივერსიტეტს” (HKUST) გამოეყო 20 მილიონი აშშ დოლარის გრანტი არსებული გადახდის სისტემების უსაფრთხოების გაუმჯობესების მიზნით. ეს უკანასკნელი პროექტის განსახორციელებლად იმუშავებს “ჰონგკონგის ჩინურ უნივერსიტეტთან” (CUHK), “ჰონგკონგის უნივერსიტეტთან” (HKU) და “ჰონგკონგის ქალაქის უნივერსიტეტთან” (CityU).

პროექტის მთავარი მიზანია სტრატეგიული დოკუმენტის შექმნა, თუ როგორ უნდა იქცეს ჰონგკონგი ფინანსურ-ტექნოლოგიურ ჰაბად, რომლის ძირითადი საფუძველი იქნება ბლოკჩეინის ტექნოლოგია. პროექტის ხელმძღვანელი არის პროფესორი ტან ჯიაინი, რომელიც ცნობილია მისი ერთერთი ყველაზე მნიშვნელოვანი პროექტით – “ჰონგკონგის, როგორც რეგიონული და საერთაშორისო ბიზნეს ცენტრის, სტრატეგიული პოზიციის გაძლიერება” და რომლის მიზანი იყო ბლოკჩეინის ტექნოლოგიის, ქსელის უსაფრთხოებისა ხელოვნური ინტელექტის შესაძლებლობების შესწავლა ჰონგკონგის ეკონომიკის გასაძლიერებლად. ჯიაინმა ახალ პროექტში მონაწილეობისთვის კომერციული ბანკებიც მიიწვია, რადგან გრანტის ნაწილი დაიხარჯება ვირტუალური ვალუტის შექმნის მიზანშეწონილობის კვლევაზე.

ეს არ არის ჰონგკონგის პირველი ნაბიჯი, შეისწავლოს DLT-ის ტექნოლოგია. 2017 წელს მთავრობამ შეისწავლა ბლოკჩეინზე დაფუძნებული სავაჭრო ფინანსირების სისტემის შექმნის შესაძლებლობა, რაც მინიმუმამდე დაიყვანს “ადამიანის ჩარევისა და თაღლითობის” ფაქტორებს და გააუმჯობესებს გამჭირვალობას.



მიმდინარე წლის აგვისტოში ფილიპინების ჩრდილოეთში საფუძველი ჩაეყარა “კაგაიანის სპეციალურ ეკონომიკურ ზონასა და თავისუფალ პორტს”. პროექტის დაფინანსება 100 მილიონ აშშ დოლარს შეადგენს და მისი მიზანია ზონაში “აზიის კრიპტო ველის” დაარსება. ფილიპინების მთავრობა იმედოვნებს ამ მოცულობის ინვესტიციით შვეიცარიის ქალაქ ცუგის ([*ქვეყნის “კირპო ველი”*](https://mybitcoin.ge/2018/05/02/%E1%83%A8%E1%83%95%E1%83%94%E1%83%98%E1%83%AA%E1%83%90%E1%83%A0%E1%83%98%E1%83%90-%E1%83%9E%E1%83%9D%E1%83%96%E1%83%98%E1%83%AA%E1%83%98%E1%83%9D%E1%83%9C%E1%83%98%E1%83%A0%E1%83%94%E1%83%91%E1%83%A1/)) მსგავსი გარემოს შექმნას.

ამ ეტაპისთვის “კაგაიანის სპეციალური ეკონომიკური ზონისა და თავისუფალი პორტის” ადმინისტრაციას ურთიერთობა აქვს 25 დიდ კომპანიასთან, რომლებიც მიიღებენ მონაწილეობას პროექტის განვითარებაში. ერთად ისინი გეგმავენ ძლიერი ინფრასტრუქტურის, ინტერნეტ დატა ცენტრების და საგანმანათლებლო/ტრენინგ პროგრამების შექმნას, სადაც მომავლის ბლოკჩეინ ლიდერები შეისწავლიან ამ სფეროს. ფინანსურ ტექნოლოგიებში წამყვან ცენტრად გადაქცევის გარდა, ფილიპინების მთავრობა იმედოვნებს მინიმუმ 10 000 სამუშაო ადგილის შექმნას. მიმდინარე წლის აგვისტოს დასაწყისში ქვეყნის ფასიანი ქაღალდების კომისიამ დაუშვა ICO-ები (მონეტის პირველადი შეთავაზება) და მათი რეგულირება ფასიანი ქაღალდების მსგავსად ხდება. ეს კი უზრუნველყოფს რეგულირებისა და საკანონმდებლო ჩარჩოს არსებობას, სადაც ფინანსურ ტექნოლოგიებში მოქმედი კომპანიები გრძელვადიანად დაცულები იქნებიან სახელმწიფოს მიერ. ეს არის სასიცოცხლოდ მნიშვნელოვანი ნაბიჯი ბლოკჩეინისა და კრიპტო ბიზნესით დაკავებული კომპანიებისთვის აზიაში. თუმცა ეს არის სამხრეთ აზიური ფინტექის მზარდი კულტურის  მხოლოდ ერთი მაგალითი, რადგან ქვეყნებს ამ რეგიონში ბლოკჩეინის ტექნოლოგიის განვითარებასა და ხელშეწყობაში დიდი შეჯიბრი აქვთ.



სამხრეთ კორეამ მსგავსი პროექტი დაიწყო ჯეჯუს კუნძულზე. გუბერნატორმა ვონ ჰეერიონგმა მოიპოვა სეულის თანხმობა კუნძულისთვის ბლოკჩეინისა და კრიპტოვალუტის ბიზნესებისთვის თავისუფალი ინდისტრიულ ზონის სტატუსის მინიჭებაზე. სამხრეთ კორეის მთავრობა მომავალ წელს გეგმავს ჯეჯუზე 4 მილიარდი აშშ დოლარის ინვესტირებას. ეს დაფინანსება მიმართულია საპილოტე პროექტებზე და ციფრული ეკონომიკის განვითარებაზე.



მიმდინარე წლის 13 აგვისტოს სამხრეთ კორეის ეკონომიკისა და ფინანსთა სამინისტრომ გამოაქვეყნა ოფიციალური [*განცხადება*](http://english.moef.go.kr/pc/selectTbPressCenterDtl.do?boardCd=N0001&seq=4532#_ftn1), რომლის მიხედვითაც ქვეყანა გეგმავს 5 მილიარდი აშშ დოლარის ინვესტირებას სახელმწიფო პროექტში – “ზრდა ინოვაციების გზით”. სტრატეგიის მიხედვით 8 საპილოტე პროექტი დაფინანსდება, რომელმაც უნდა განავითაროს “პლატფორმის ეკონომიკა” და ის მოიცავს დიდი მოცულობის ინფორმაციის ანალიზისა და ტრანზაქციების ციფრული პლატფორმის შექმნას, ასევე ჰიდროგენის უჯრედული მიწოდების ქსელის შექმნას, და სხვ.

მთლიანად ამ ინიციატივებზე იგეგემება 10 მილიარდი აშშ დოლარის დახარჯვა, რაც პოზიტიურ გავლენას მოახდენს ქვეყნის სხვა ინდუსტრიებზეც. განცხადებაში აქცენტი გაკეთებულია ბლოკჩეინის ტექნოლოგიაზე, როგორც ზიარი ეკონომიკის გაძლიერების ძირითად სტიმულზე. აღსანიშნავია, რომ მიმდინარე წელს მხოლოდ ერთი მილიარდი აშშ დოლარი დაიხარჯა ამ მიმართულებით, ხოლო მომავალ წელს ასეთი ზრდა მხოლოდ იმაზე მიუთითებს, რომ სამხრეთ კორეა ძალიან დიდ პოტენციალს ხედავს DLT-ის განვითარებაში.  გარდა ამ დაფინანსებისა გაიხსნა ბლოკჩეინის კვლევის რამდენიმე დიდი ცენტრი. ასევე, შეიქმნა სახელწიფო ორგანო – “ფინანსური ინოვაციების ბიურო”, რომელიც პოლიტიკის ძირითადი განმსაზღვრელი იქნება DLT-ის, კრიპტოვალუტებისა და ფინტექის სფეროში.

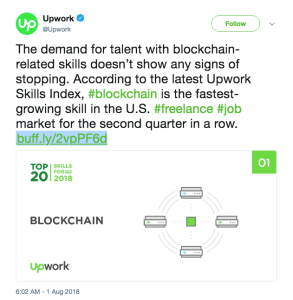


აშშ-ს ციფრული კომერციის პალატამ ასევე გამოაქვეყნა გზამკვლევი – “[*ციფრული ტოკენები: ბაზრის მიმოხილვა და გზამკვლევი პოლიტიკის განმახოციელებლებისა და პრაქტიკოსებისთვის*](https://digitalchamber.org/download/7153/)”. ეს ორგანიზაცია ვაშინგტონში მოღვაწეობს და რამდენიმე ინიციატივას აერთიანებს, როგორიცაა “ბლოკჩეინის ინტელექტუალური საკუთრების საბჭო”, “სმარტ კონტრაქტების ალიანსი”, “ტოკენების ალიანსი”, და სხვ. ამ უკანასკნელმა ასევე გამოაქვეყნა დოკუმენტი, რომელიც იძლევა რეკომენდაციებს ციფრული ტოკენებისა და ICO-ების “პასუხიმგებლობიანი ზრდის” ხელშეწყობაზე. ინიციატივა 350-ზე მეტ პროფესიონალს აერთიანებს, რომელშიც შედიან ეკონომისტები, ყოფილი მარეგულირებლები, სამართლის პრაქტიკოსები, ბლოკჩეინისა და ტოკენების ექსპერტები.



ამერიკის სავაჭრო პალატა, კიდევ ერთი პოლიტიკურად ძალიან გავლენიანი ორგანიზაცია, რომელიც აერთიანებს ამერიკის უმთავრეს და უდიდეს კორპორაციებსა და საშუალო/მცირე ბიზნესს, [*მხარს უჭერს ბლოკჩეინის ტექნოლოგიის განვითარებას*](https://mybitcoin.ge/2018/07/30/%E1%83%90%E1%83%9B%E1%83%94%E1%83%A0%E1%83%98%E1%83%99%E1%83%98%E1%83%A1-%E1%83%A1%E1%83%90%E1%83%95%E1%83%90%E1%83%AD%E1%83%A0%E1%83%9D-%E1%83%9E%E1%83%90%E1%83%9A%E1%83%90%E1%83%A2%E1%83%90/). ორგანიზაციის ანგარიში პალატის ახალი “ფინტექის საინოვაციო ინიციატივის” ნაწილია, რომელიც მან მიმდინარე წლის ივლისის დასაწყისში გამოაქვეყნა. დოკუმენტში თავმოყრილია ამ სფეროში გასატარებელი პოლიტიკისა და რეკომენდაციების დიდი სია და მისი ოფიციალური განხილვები მალე დაიწყება კანონმდებლებთან და მარეგულირებლებთან. “უახლოეს მომავალში ინოვაციების განვითარების სიჩქარე არ შენელდება, პირიქით, მომდევნო წლებში გაიზრდება. აუცილებელია აშშ-ს მთავრობამ და შტატებმა ხელი შეუწყონ ამ ინოვაციებს, რომელიც უკვე ცვლის და მალე მნიშვნელოვნად შეცვლის ყველა ადამიანის ყოველდღიურ ცხოვრებას. ასევე, აუცილებელია აშშ ამ პროცესში მსოფლიო ბაზარზე კონკურენტულ უპირატესობას ფლობდეს; მეტიც, ქვეყანამ წამყვანი როლი უნდა ითამაშოს გლობალური ფინანსური სისტემის განვითარებაში” – ნათქვამია ანგარიშში.

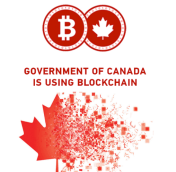
აშშ-ს სულ უფრო მეტი შტატი იყენებს ბლოკჩეინის ტექნოლოგიას და ხელს უწყობს მათ განვითარებას. არიზონას შტატმა მიიღო კანონი, რომელიც აძლევს საშუალებას კორპორაციებს შეინახონ და გაავრცელონ ინფორმაცია ბლოკჩეინის საშუალებით. ტენესის შტატმაც მიიღო კანონი, რომელიც ლეგალურად ცნობს DLT-ის და სმარტ კონტრაქტებს ელექტრონული ტრანზაქციებისთვის. ნებრასკა, ფლორიდა, ნევადა, ვერმონტი, ჰავაი, ილინოისი, ჩრდილოეთ დაკოტა, ეს მხოლოდ ნაწილია იმ შტატებისა, სადაც აქტიურად მიმდინარეობს ამ სფეროს დამკვიდრება და ხელშეწყობა.



კომპანია Upwork-ის უკანასკნელი კვარტალური “[*უნარების ინდექსის*](https://www.upwork.com/blog/2018/07/fastest-growing-skills-upwork-q2-2018/?utm_content=buffer44da0&utm_medium=social&utm_source=twitter&utm_campaign=buffer)” თანახმად, ბლოკჩეინი აშშ-ში 2018 წლის მეორე კვარტალში ყველაზე მზარდი უნარია. ანგარიში აშუქებს ახალ აღმოცენებად უნარებსა და არსებულ ტრენდებს რეალურ დროში. დოკუმენტის თანახმად, ბლოკჩეინმა პირველი ადგილი დაიკავა 5000 უნარს შორის და ის უკვე მეორე კვარტალშიც უცვლელი ლიდერია. “უნარების ინდექსის” მიხედვით “ბლოკჩეინი არის ახალი და უკვე ძალიან ცნობადი ტექნოლოგია, როგორიც 2000-იან წლებში “ღრუბელის” ტექნოლოგია იყო”.

ბლოკჩეინის დეველოპერებზე მოთხოვნა ძირითადად სტარტაპებიდან მოდიოდა. დღეს კი ეს სურათი სრულიად შეცვლილია. დიდმა კომპანიებმა დაინახეს ამ ინოვაციის პოტენციალი. ისეთმა გიგანტებმა, როგორიცაა Microsoft, IBM და Google, დაასრულეს ტესტირების რეჟიმი და საკუთარ ბლოკჩეინზე დაფუძნებულ ქსელებს ქმნიან. IBM არის ბლოკჩეინ ტალანტების უდიდესი შემსყიდველი. კომპანიას 400-ზე მეტი მიმდინარე ბლოკჩეინის პროექტი აქვს, დაქირავებული ჰყავს 1600-ზე მეტი ბლოკჩეინის სპეციალისტი და დამატებით კიდევ 150-ს ეძებს.

ბლოკჩეინის დეველოპერების საშუალო წლიური შემოსავალი აშშ-ში 130 ათასი აშშ დოლარია. ჩვეულებრივი პროგრამული უზრუნველყოფის დეველოპერების წლიური საშუალო ხელფასი 105 ათასი აშშ დოლარია. მაღალი კონცენტრაციის ციფრულ ჰაბებში, როგორიცაა სილიკონის ველი, ბოსტონი, ნიუ ოირკი, ბლოკჩეინის დეველოპერების საშუალო წლიური ხელფასი 158 ათას აშშ დოლარს აღწევს. უცხოეთში, მაგალითად შვეიცარიაში ეს ციფრი 120-180 ათას აშშ დოლარს შორის მერყეობს. ხელფასების ასეთი ზრდა ბლოკჩეინის სპეციალისტებზე მოთხოვნის მნიშვნელოვანი ზრდის პირდაპირი შედეგია.



კანადა პროაქტიულად ავითარებს ბლოკჩეინის აპლიკაციებს სხვადასხვა სფეროში: სახელმწიფო მმართველობა, ფინანსები, სამართალი, ჯანდაცვა, განათლება, ენერგეტიკა, ეროვნული და მულტინაციონალიური კრიპტოვალუტები, ICO-ები, და სხვ. ქვეყნის წამყვანი პოზიცია ბლოკჩეინის ინოვაციებში ნაწილობრივ გამომდინარეობს იმ ფაქტიდან, რომ ეთერიუმის ბლოკჩეინის დამაარსებელი ვიტალიკ ბუტერინი ცხოვრობს და მოღვაწეობს ტორონტოში.



მიმდინარე წლის იანვარში “კანადის ეროვნულმა კვლევითმა საბჭომ” (NRC) და “ინდუსტრიული კვლევების ხელშეწყობის პროგრამამ” (IRAP) წარმატებით დაიწყეს კანადის მთავრობის სახელმწიფო კონტრაქტების გამჭვირვალე ადმინისტრირების ბლოკჩეინ [*პროექტი*](https://www.nrc-cnrc.gc.ca/eng/stories/2018/blockchains.html) (ეთერიუმის ქსელის ბაზაზე).



მიმდინარე წლის 25 ივნისს კანადის ინვესტიციების ინდუსტრიის მარეგულირებელმა ორგანიზაციამ (IIROC) გამოაქვეყნა [*2019 წლის პრიორიტეტები*](http://www.iiroc.ca/Documents/2018/84e09271-5a9a-4761-b0b6-5876d7dbfcbd_en.pdf). ერთერთი ძირითადი პრიორიტეტია სამუშაო ჯგუფის შექმნა, რომელიც შეიმუშავებს კაპიტალის ბაზარზე ბლოკჩეინის აპლიკაციებისთვის რეგულირების რეკომენდაციებს. რეკომენდაციების მიზანია ეფექტური მარეგულირებელი ჩარჩოს შექმნა, რომელიც დაიცავს ინვესტორებს და ხელს შეუწყობს ჯანმრთელი შიდა კაპიტალის ბაზრის განვითარებას.

“ბლოკჩეინის ტექნოლოგიის გამოყენება დრამატულად შეცვლის კაპიტალის ბაზრის მთელ ეკოსისტემას. ციფრული აქტივები, როგორიცაა კრიპტოვალუტები უკვე მნიშვნელოვან ზემოქმედებას ახდენს კაპიტალის ბაზრებზე” – ნათქვამია პრიორიტეტების დოკუმენტში.



კანადის ეროვნული ბანკი 2016 წლიდან იყენებს ბლოკჩეინის ე.წ. Proof-of-Concept ტექნოლოგიას ფასიანი ქაღალდების სფეროში, რომლის მიზანია ნაღდი ფულისა და აქტივების ტოკენიზაცია მათი სწრაფი გაცვლისთვის. გარდა ამისა, ბანკი განიხილავს სახელმწიფო კრიპტოვალუტის შექმნის შესაძლებლობასაც.



შვეიცარია დიდი ხანია ე.წ. “ბლოკჩეინისა და კრიპტო სამოთხის” სახელს იმკვიდრებს მსოფლიოში და [*პოზიციონირებს, როგორც მსოფლიოს ბლოკჩეინ დედაქალაქი*](https://mybitcoin.ge/2018/05/02/%E1%83%A8%E1%83%95%E1%83%94%E1%83%98%E1%83%AA%E1%83%90%E1%83%A0%E1%83%98%E1%83%90-%E1%83%9E%E1%83%9D%E1%83%96%E1%83%98%E1%83%AA%E1%83%98%E1%83%9D%E1%83%9C%E1%83%98%E1%83%A0%E1%83%94%E1%83%91%E1%83%A1/). მიმდინარე წელს შვეიცარიის ეკონომიკის მინისტრმა წარმოადგინა ქვეყნის ბლოკჩეინ დედაქალაქად გადაქცევის გეგმა, სადაც ამ სფეროს სტარტაპებისთვის საუკეთესო პირობები შეიქმნება.



კიდევ ერთი ქვეყანა, რომელმაც წარმატებით განახორციელა ელექტრონული მმართველობის პროექტი – ესტონეთია. მილიონზე ოდნავ მეტი მოსახლეობის მქონე სახელმწიფომ ბლოკჩეინისა და კრიპტოვალუტების ეკონომიკაში ინტეგრაციით შეძლო ახალი იმპულსის მიცემა ციფრული ეკონომიკისთვის და ახლა იქ ამ სფეროში უამრავი სტარტაპია.



ესტონეთის პრეზიდენტმა კერსტი კალიულაიდმა განცხადა: “..ჩვენ შეგვიძლია ათი მილიონი გადახდის შესრულება, ათი მილიონი მოთხოვნის შესრულება და ათი მილიონი კონტრაქტის ხელმოწერა სულ რაღაც 10 წუთში. ჩვენზე 10-ჯერ დიდ სახელმწიფოებს არ შეუძლიათ ამის გაკეთება”.

ესტონეთი აქტიურად იყენებს ბლოკჩეინის ტექნოლოგიას ჯანდაცვის, სასამართლო, საკანონმდებლო, უსაფრთხოებისა და კომერციულ სფეროებში. ესტონელებს DLT-ის საშუალებით შეუძლიათ საჯაროდ ნახონ, ვინ გამოიყენა მათი პერსონალური მონაცემები, ეხება ეს მათ სამედიცინო მონაცემებს, მართვის მოწმობას, თუ სადაზღვევო ინფორმაციას. მათ ასევე შეუძლიათ ლეგალურად შეზღუდონ ამ ინფორმაციის გამოყენება.



შოტლანდიაში გამოქვეყნდა კვლევა – “[*DLT-ისაჯარო მომსახურების სფეროში*](https://www.wallet.services/blog/2018/6/27/scottish-government-dlt-future)”, რომელიც მოუწოდებს შოტლანდიის მთავრობასა და ინდუსტრიას გაერთიანდნენ ტექნოლოგიის გარშემო და ხელი შეუწყონ ამ სფეროში ინოვაციებს. დოკუმენტი შოტლანდიის მთავრობის ციფრულმა დირექტორატმა შეუკვეთა. მასში ნათქვამია: “არსებობს საერთაშორისო კონსესუსი, რომ DLT-ი ითამაშებს გადამწყვეტ როლს მომავალ ციფრულ მმართველობაში. ის პოზიტიურ გავლენას მოახდენს ინფორმაციის მართვაზე, საჯარო სერვისების მიწოდების მექანიზმებზე, ეკონომიკურ მოდელებზე და ზოგადად ეკონომიკის ეკოსისტემებზე”. მთავარი რეკომენდაციაა, რომ შოტლანდია უნდა ჩაერთოს ბლოკჩეინის საერთაშორისო ეკოსისტემაში. საჯარო სექტორში პროექტების განხორციელებისთვის საჭიროა პროცესში უნივერსიტეტებისა და ბიზნესის ჩართვა. მიზანია შოტლანდიის DLT-ის ერთიანი ხედვის ჩამოყალიბება, რომელიც უნდა გაზიარებულ იქნას საერთაშორისო თანამეგობრობასთან და პროაქტიულად დამყარდეს კონტაქტები სხვა სახელმწიფოებთან.



მიუხედავად იმისა, რომ საქართველოშიც არის ამ მიმართულებით ძვრები, ბევრად მეტია გასაკეთებელი იმისთვის, რომ ბლოკჩინის  განვითარებისთვის ხელსაყრელი გარემო შეიქმნას. საქართველოს მთავრობამ შექმნა მიწის საკადასტრო ჩანაწერების საჯარო რეესტრის ბლოკჩეინ ბაზა. მაგრამ ძირითადი განვითარება ამ მიმართულებით მაინც [მაინინგის სფეროში მოღვაწე კომპანიების ხარჯზეა](https://mybitcoin.ge/2018/04/25/%E1%83%A1%E1%83%90%E1%83%A5%E1%83%90%E1%83%A0%E1%83%97%E1%83%95%E1%83%94%E1%83%9A%E1%83%9D-%E1%83%99%E1%83%A0%E1%83%98%E1%83%9E%E1%83%A2%E1%83%9D%E1%83%95%E1%83%90%E1%83%9A%E1%83%A3%E1%83%A2/). ეს საქმიანობა დიდი რაოდენობით ენერგორესურსს მოითხოვს და ენერგიის მოხმარების ასეთ ზრდას ჩვენი ქვეყანა მარტივად ვერ დააკმაყოფილებს. აქცენტი უნდა გაკეთდეს ინოვაციურ პროექტებზე, სტარტაპების დაფინანსებაზე და რაც ყველაზე მთავარია საკანონმდებლო უზრუნველყოფაზე, რამაც საქართველოს, სხვა ქვეყნებთან შედარებით, მნიშნვნელოვანი კონკურენტული უპირატესობა უნდა მიანიჭოს, რომ ამ სფეროს წამყვან კომპანიებს ინტერესი გაუჩნდეთ აქ საქმიანობის. ბლოკჩეინის ტექნოლოგია ხვალინდელი დღეა და ამაზე დაფიქრება სწორედ დღეს არის საჭირო.

**თავი 15. სხვა გამოყენებები**.

ბლოკჩეინის გამოყენება ბიზნესში. ბლოკჩეინის გამოყენება არჩევნებში, იუსტიციის სახლში და ეროვნულ ბანკში. უძრავი ქონების სახელმწიფო რეგისტრაცია. ბლოკჩეინის შესაძლო გამოყენება განათლების სფეროში

**ბლოკჩეინის გამოყენება სხვადასვა სფერო**

* პიროვნების იდენტიფიკაცია.
* ბლოკჩეინის ტექნოლოგიის საფუძველზე მუშაობენ სერვისები იდენტიფიკაციისა და წვდომის უფლების დამტკიცების სფეროში..ისინი ქმნიან პირადობის მოწმობის ციფრულ ანალოგს. ასეთ სტარტაპებს მიეკუთვნება HYRP, BlockVerify, OneName და სხვები.
* **საავტორო უფლებები.** პლატფორმა Ascribe გამოიყენებს დამატებით რეესტრს, რომელშიც მხატვრებს, მუსიკოსებს, გამომგონებლებს შეუძლიათ საავტორო უფლებების შენახვა დაშიფრული იდენტიფიკატორების დახმარებით.
* **ხმის მიცემა.** ჯერ-ჯერობით ღია რეესტრი გამოიყენება მხოლოდ კერძო ხმის მიცემისას. თუმცა ვირჯინიის შტატის უნივერსიტეტი სურთ ტექნოლოგიის დანერგვა, რომელიც ბლოკჩეინზეა ბაზირებული. ეს დაიყვანს ფალსიფიცირების ალბათობას ნულამდე.
* **მართვა და იურისპუდენცია.**  Blocckhain-ის პოტენციალი ამ სფეროში შემოუსაზღვრელია იდეალში შეიძლება შექმნილ იქნას ადგილობრივი და სახელმწიფო ხელისუფლების ანგარიშგების სისტემა, მონაცემების შენახვა ბიუჯეტზე და ა.შ. უკვე არსებობენ Borderless-ის ტიპის პროექტები, რომლიბიც აერთიანებენ იურიდიულ და ეკონომიურ მომსახურებებს.
* **მუსიკა.**  Bittunes პროექტი კომპოზიციის შემსრულებლებს საშუალებას აძლევს შეინახონ გამოყენების უფლება და დაკავდნენ საკუთარი ქმნილებების გაყიდვით
* **ქველმოქმედება.**  ასე პლატფორმა GiveTrack პლატფორმაში წარმოდგენილია ღია ინფორმაცია ფონდებში შეწირულებებზე და მათ ხარჯებზე.
* **უძრავი ქონება.**  ბლოკჩეინის დანერგვა ამ სფეროში მისი გაუმჯობესების შესაძლობლობას იძლევა . დაჩქარდება ყიდვა-გაყიდვის პროცესი, გამოჩნდება საკუთრების უფლებებზე მონაცემების საიმედო შენახვის ინსტრუმენტი. ბლოკჩეინის ტექნოლოგიები გამოიყენება საბირჟო და ჩვეულებრივი ვაჭრობის მომსახურების სფეროში.
* **პოტენციალურად მისი გამოყენება შეიძლება ყველგან სადაც აუცილებელია ანგარიშგება, რაიმეს ნამდვილობის შემოწმება, მონაცემთა შნახვა და ა.**შ.

ბლოკჩეინის დეველოპერებზე მოთხოვნა ძირითადად სტარტაპებიდან მოდიოდა. დღეს კი ეს სურათი სრულიად შეცვლილია. დიდმა კომპანიებმა დაინახეს ამ ინოვაციის პოტენციალი. ისეთმა გიგანტებმა, როგორიცაა Microsoft, IBM და Google, დაასრულეს ტესტირების რეჟიმი და საკუთარ ბლოკჩეინზე დაფუძნებულ ქსელებს ქმნიან. IBM არის ბლოკჩეინ ტალანტების უდიდესი შემსყიდველი. კომპანიას 400-ზე მეტი მიმდინარე ბლოკჩეინის პროექტი აქვს, დაქირავებული ჰყავს 1600-ზე მეტი ბლოკჩეინის სპეციალისტი და დამატებით კიდევ 150-ს ეძებს.

მიმდინარე წლის იანვარში “კანადის ეროვნულმა კვლევითმა საბჭომ” (NRC) და “ინდუსტრიული კვლევების ხელშეწყობის პროგრამამ” (IRAP) წარმატებით დაიწყეს კანადის მთავრობის სახელმწიფო კონტრაქტების გამჭვირვალეადმინისტრირების ბლოკჩეინ პროექტი (ეთერიუმის ქსელის ბაზაზე).

**ბლოკჩეინის გამოყენება განათლების სისტემაში**

* 1. **სერტიფიკატების მუდმივი დაცვისთვის Blockchain-ის გამოყენება**

  ამ სცენარით საგამანათლებო ორგანიზაციები, რომლებიც გასცემენ ციფრულ სერტიფიკატებს გამოიყენებენ საჯარო  Blockchain-ს ციფრულ სერტიფიკაციებთან დაკავშირებული ციფრული ხელმოწერების შესანახად. უნიკალურად ხელმოწერილი ციფრული ატესტატები(დიპლომები) გაიცემა მომხმარებელზე მყისიერად.სერტიფიკატის ნამდვილობის შემოწმება მოითხოვს მხოლოდ Blockchain.-ში შენახულ ციფრულ ხელმოწერასთან შედარებას.

**2. Blockchain-ის გამოყენება მრავალსაფეხურიანი აკრედიტაციის შესამოწმებლად.**

ამ სცენარში არა მარტო საგანმანათლებო ორგანიზაციები გამოიყენებენ ციფრულ სერტიფიკატებს(როგორც პირველ სცენარში), ასევე თვითონ ორგანიზაციები, რომლებიც ღებულობენ აკრედიტაციას, მოათავსებენ თავიანთ ციფრულ ხელმოწერებს    Blockchain-ში .  ასეთი სისტემა შეიძლება გამოყენებულ იქნას სახელმწიფო აკრედიტაციის უზრუნველსაყოფად, ან საგანმანათლებო ორგანიზაციისთვის ხარისხის კონკრეტული სერტიფიკატების  არსებობის შემოწმებისათვის.

 3.  **Blockchain გამოყენება კრედიტების აღრიცხვისა და გადაცემისათვის.**

ამ სცენარის შესაბამისად, საგანმანათლებო ორგანიზაციები, რომლებიც სწავლების პროცესის კონტროლისათვის გამოიყენებენ კრედიტების სისტემას - მიანიჭებენ და გადაცემენ კრედიტებს სპეციალურად შექმნილი Blockchain-ით

**4. Blockchain-ის გამოყენება უწყვეტი სწავლების პასპორტის სახით**

ამ სცენარის მიხედვით მოსწავლეები ნებისმიერი წყაროდან მიღებულ საკუთარ სწავლების მოწმობებს (ეს იქნება ფორმალური თუ არაფორმალური) შეინახავენ და შემდგომ  გამოიყენებენ  Blockchain-ით ამ დოკუმენტების ნამდვილობის მყისიერი შემოწმებისათვის

**5.**  **Blockchain ინტელექტუალური საკუთრების სათვალთვალოდ და მისი განმეორებითი გამოყენების წახალისებისათვის**

ამ სცენარის შესაბამისად მასწავლებლები გამოიყენებენ ბლოკ-ჯაჭვს ღია საგანმანათლებლო რესურსების პუბლიკაციების გამოცხადებისათვის და მათ მიერ გამოყენებული ბმულების ჩასაწერად. ეს პუბლიკაციის და საავტორო უფლების დროის განსაზღვრის საშუალებას იძლევა.  ასევე შესაძლებელი იქნება ნებისმიერი კონკრეტული რესურსის განმეორებით გამოყენებისათვის თვალის მიდევნება.

**6. სტუდენტებისგან გადასახადების მიღება  Blockchain-ით.**

 ამ სცენარის მიხედვით სტუდენტები სწავლის საფასურს გადაიხდიან კრიპტოვალიუტით.

**7. ვაუჩერების სახით სტუდენტების დაფინანსება Blockchain-ს დახმარებით.**

 ამ სცენარის შესაბამისად სწავლების სახელმწიფო(ან სპონსორული) დაფინანსება სტუდენტებზე გაიცემა „ვაუჩერების“ სახით Blockchain-ს დახმარებით. ვაუჩერები შეიძლება დაპროგრამებული იყოს მოსწავლეებისათვის ან საგანმანათლებო ორგანიზაციებისათვის  ფინანსირების ტრანშების გამოყოფაზე ეფექტურობის გარკვეული კრიტერიუმების საფუძველზე, როგორიცაა შეფასებები ან ტესტების შედეგები.

8. **შემოწმებული სუვერენული პირადობის მოწმობების გამოყენება საგანმანათლებლო ორგანიზაციებში მოსწავლეთა იდენტიფიკაციისათვის.**

 მას შემდეგ, როდესაც სტუდენტები თავის პირად მონაცემებს გაუზიარებენ საგანმანათლებლო ორგანიზაციებს, ისინი მიიღებენ ამ ორგანიზაციებისგან  პირადობის მოწმობებს. ბიომეტრიული იდენტიფიკაციის გამოყენება ამ მოწმობებთან ერთად მოსწავლის იდენტიფიკაციის საშუალებას იძლევა ორგანიზაციის შიგნით ნებისმიერ ადგილას: ბიბლიოთეკა, სპორტული დარბაზი, ბუფეტი, სტუდენტური საერთო საცხოვრებელიდა ა.შ. ამ სამსახურებიდან თვითეულს შეეძლება მოსწავლის პიროვნების დადგენა ისე, რომ არ მოითხოვოს და არ შეინახოს არა საჭირო პერსონალური მონაცემები.

**ლიტერატურა**

* 1. Blockgeeks.com
  2. Coindesk.com
  3. <https://bitcoin.org/bitcoin.pdf>
  4. <https://www.futureblockchainsummit.com/speakers?page=1&categories=5019714C-5056-B733-838CE13194ABF2E1&sortby=Community_Featured%20desc,Community_Sponsored%20desc>
  5. Antonopoulos, A. Mastering Bitcoin. Programming the Open Blockchain (2017)
  6. [Paul Vigna](https://www.amazon.com/Paul-Vigna/e/B00CE2WLL8/ref=dp_byline_cont_book_1)   [Michael J. Casey](https://www.amazon.com/Michael-J.-Casey/e/B001JRYOHI/ref=dp_byline_cont_book_2). The Truth Machine: The Blockchain and the Future of Everything Hardcover – February 27, 2018. <https://www.amazon.com/Truth-Machine-Blockchain-Future-Everything/dp/1250114578> .
  7. Franco, P. Understanding Bitcoin. Cryptography, Engineering and Economics. Wiley (2014)

