საქართველოს ტექნიკური უნივერსიტეტი

ხელნაწერის უფლებით

თეიმურაზ თუთბერიძე

ბიზნეს ინფორმაციის უსაფრთხოების უზრუნველყოფა თანამედროვე ტექნოლოგიების გამოყენებით

დოქტორის აკადემიური ხარისხის მოსაპოვებლად

წარდგენილი დისერტაციის

ა ვ ტ ო რ ე ფ ე რ ა ტ ი

სადოქტორო პროგრამა: „ინოვაციებისა და ოპერაციათა მენეჯმენტი“

შიფრი: 0413

თბილისი

2025 წელი

სამუშაო შესრულებულია საქართველოს ტექნიკურ უნივერსიტეტში

ენერგეტიკის ფაკულტეტი

საწარმოო ინოვაციების და ოპერაციათა მენეჯმენტის დეპარტამენტი

ხელმძღვანელი: პროფესორი მ. მაღრაძე

რეცენზენტები:

დაცვა შედგება 2025 წლის ”---------” ”-------------------------” ”----------” საათზე საქართველოს ტექნიკური უნივერსიტეტის ენერგეტიკის ფაკულტეტის სადისერტაციო ნაშრომის დაცვის კოლეგიის სხდომაზე, კორპუსი VIII, სხდომათა დარბაზი.

მისამართი: 0160, თბილისი, კოსტავას 77.

დისერტაციის გაცნობა შეიძლება სტუ-ის ბიბლიოთეკაში,

ხოლო ავტორეფერატისა - ფაკულტეტის ვებგვერდზე

ფაკულტეტის სწავლული მდივანი, პროფესორი გ. გიგინეიშვილი

ნაშრომის ზოგადი დახასიათება

თემის აქტუალურობა. ციფრული ტექნოლოგიების ეპოქაში კორპორაციული მენეჯმენტი სულ უფრო და უფრო მეტად ეფუძნება ტექნოლოგიების ეფექტურ მოხმარებას. პრაქტიკულად მზარდი ბიზნეს კონკურენციის პირობებში კომპანიის წარმატება მნიშვნელოვანწილად განპირობებულია ეფექტური მენეჯმენტით, რომლის ერთ-ერთი განმსაზღვრელი ფაქტორია მართვის პროცესში ტექნოლოგიური მიღწევების სწორად გამოყენება. ეს არის შეუქცევადი პროცესი, შესაბამისად აუცილებელი ხდება მომზადდეს იმ პრობლემების დროული და ეფექტური გადაწყვეტები, რაც ტექნოლოგიების მოხმარებას ახლავს თან.

მზარდ კონკურენტულ გარემოში წარმატების მისაღწევად დიდ მნიშვნელობას იძენს ბიზნეს პროცესების დაჩქარება და მათი ეფექტიანობის ამაღლება. ამ კუთხით არსებითია ქაღალდზე დაფუძნებული პროცესების ციფრული ტრანსფორმაცია და ამაში თანამედროვე ინფორმაციული ტექნოლოგიების გამოყენება. გლობალურად შეინიშნება ბიზნეს პროცესების კომპიუტერიზაციის ტენდენცია, თუმცა ბიზნეს პროცესებში ახალი ტექნოლოგიების დანერგვა დაკავშირებულია ბევრ ისეთ პრობლემასთან, რომელიც მანამდე არ გვხვდებოდა. იმის გამო, რომ უფრო და უფრო მზარდი ტემპებით ხდება კომპიუტერული ტექნოლოგიების დანერგვა და პრაქტიკულად სრულად ჩანაცვლდა ქაღალდის დოკუმენტაცია ელექტრონულით, მწვავედ დგას ამ ელექტრონული დოკუმენტაციის დაცულობის და სანდოობის საკითხი. ის, რისი გაკეთებაც ვერ დარჩება შეუმჩნეველი ქაღალდზე, ბევრად მარტივად შეიძლება მოხერხდეს ელექტრონულ დოკუმენტაციაში. სწორედ ამის გამო ჩნდება აუცილებლობა იმისა, რომ უწყვეტ რეჟიმში მოწმდებოდეს ელექტრონული დოკუმენტაციის სანდოობა.

ინფორმაციული ტექნოლოგიების ეპოქაში, მონაცემთა სანდოობის, უსაფრთხოებისა და უცვლელობის უზრუნველყოფა მნიშვნელოვან გამოწვევას წარმოადგენს. თანამედროვე ორგანიზაციების ყოველდღიური საქმიანობა მნიშვნელოვნად არის დამოკიდებული ციფრული ინფორმაციის მართვაზე. თუმცა, მონაცემთა ცენტრალიზებული შენახვის მოდელები, რომლებიც დღეს

ფართოდ გამოიყენება, ყოველთვის ვერ უზრუნველყოფენ საკმარის დაცვას ინფორმაციის მოდიფიკაციისგან, რაც ქმნის რისკს, რომ მნიშვნელოვანი მონაცემები — იქნება ეს ფინანსური ოპერაციები, სამედიცინო ჩანაწერები თუ აკადემიური დოკუმენტაცია — შესაძლოა მიზანმიმართულად ან შემთხვევით შეიცვალოს, რაც სერიოზულ ზიანს აყენებს როგორც ორგანიზაციებს, ასევე მათ მომხმარებლებს.

გარდა ამისა, მონაცემთა მოდიფიკაციისა და ინფორმაციის გაყალბების შემთხვევები საგრძნობლად აფერხებს საზოგადოების ნდობას სხვადასხვა დაწესებულების მიმართ.

პრაქტიკა გვიჩვენებს, რომ ორგანიზაციებში ხშირად ხდება ერთხელ უკვე შესრულებული ოპერაციის არსებითად კორექტირება და ხშირად ასეთი კორექტირება ხორციელდება ძველი თარიღითაც, რაც შეიძლება ორგანიზაციის ან მისი კონკრეტული თანამშრომლის მიერ გამოყენებულ იქნას სახელმწიფო მაკონტროლებლისგან ან აუდიტორისგან განსაკუთრებულად მნიშვნელოვანი ინფორმაციის დაფარვისთვის.

მონაცემთა სანდოობის საკითხი ერთ-ერთი ყველაზე მტკივნეული პრობლემაა ორგანიზაციის ფინანსების მოძრაობისას. აღრიცხული ფინანსების საფუძველზე ხდება ორგანიზაციის გადასახადით დაბეგრვა. ბუღალტრული ინფორმაცია ასევე საინტერესოა აუდიტორისთვის, რადგან წარმოდგენილ ინფორმაციაზე დაყრდნობით მან უნდა გააკეთოს დასკვნა ორგანიზაციის ლიკვიდურობის თაობაზე.

ყოველივე ზემოთ აღნიშნული განაპირობებს ინფორმაციის უსაფრთხოების საკითხის აქტუალობას.

კვლევის მიზანი და ამოცანები. წარმოდგენილი ნაშრომის კვლევის მიზანს წარმოადგენს შეიქმნას ინოვაციური ბიზნესმოდელი, რომელიც დაფუძნებული იქნება თანამედროვე ტექნოლოგიებზე და რომელიც უზრუნველყოფს ორგანიზაციისთვის ინფორმაციის საიმედობას და სანდოობას. რამდენად ეფექტური იქნება ახალი შეთავაზებული ბიზნესმოდელი და რა პროცესებისა და გზების დახმარებით გახდება შესაძლებელი ინოვაციური ბიზნესმოდელის

ინტეგრირება ყოველდღიურ საქმიანობაში და როგორ იმოქმედებს იგი ორგანიზაციების საიმედოდ მუშაობაზე.

კვლევის მიზნის განხორციელებისთვის საჭიროა:

- ორგანიზაციაში მიმდინარე ბიზნეს პროცესების შესწავლა ორგანიზაციის სპეციფიკის გათვალისწინებით.
- ძირითადი(მნიშვნელოვანი) პარამეტრების იდენტიფიცირება, რომელიც აუცილებელია ორგანიზაციის მუშაობისათვის.
- მონაცემთა ბაზის ანალიზი და მასში ბლოკჩეინის დამცავი მექანიზმისთვის აუცილებელი სტრუქტურული ცვლილებების განხორციელება;
- ბლოკჩეინის დამცავი მექანიზმის შესაბამისი პროგრამული უზრუნველყოფის შემუშავება და მისი მონაცემთა ბაზაზე მორგება;
- დროითი და ენერგეტიკული დანახარჯების შეფასება სხვადასხვა სირთულის მქონე ბლოკჩეინის დამცავი მექანიზმის აგებისას;
- ბლოკჩეინის დამცავი მექანიზმის გენერაციის სერვისის სახით მიწოდების სიმულაცია ორგანიზაციის საინფორმაციო სისტემისთვის;
- ორგანიზაციაში მიმდინარე ბიზნეს პროცესების გამოკვლევა და მათი მონაცემების სანდოობის ბლოკჩეინით უზრუნველყოფის მოდელების შემუშავება.

დასახული მიზნის მისაღწევად აუცილებელია ჰიბრიდული მოდელის შემუშავება, რომელიც აერთიანებს ბლოკჩეინის ტექნოლოგიას და ცენტრალიზებულ მონაცემთა ბაზებს, რათა უზრუნველყოს მონაცემთა სანდოობა და უცვლელობა. ეს მიზანი ემსახურება როგორც ტექნოლოგიური, ასევე ორგანიზაციული გამოწვევების გადაჭრას, რაც დაკავშირებულია მონაცემთა უსაფრთხოების თანამედროვე მოთხოვნებთან.

ჩატარებული კვლევები. დისერტაციის ფარგლებში განხორციელდა კომპლექსური კვლევითი სამუშაოები, რომლებიც მოიცავდა როგორც თეორიულ ანალიზს, ასევე პრაქტიკულ ექსპერიმენტებს. ლიტერატურის მიმოხილვისას გაანალიზდა ბლოკჩეინის ტექნოლოგიის განვითარება, მისი გამოყენების შემთხვევები და არსებული კვლევების შედეგები. ყურადღება გამახვილდა იმ პრობლემებზე, რომლებიც უკავშირდება ცენტრალიზებული მონაცემთა ბაზების

სანდოობასა და უსაფრთხოებას. ასევე, გაანალიზდა ბიზნეს მოდელების შემუშავების საკითხები, განვიხილეთ ლინ კანვასი და კანვას ბიზნეს მოდელის მეთოდოლოგიები და გავაანალიზეთ მათი დანარგვის საკითხები სხვადასხვა ტიპის ბიზნეს მოდელებისთვის.

გარდა ამისა, ჩატარდა საველე კვლევები სხვადასხვა ორგანიზაციებში. ჩვენ გამოვკითხეთ ჯანდაცვის და განათლების სექტორის წარმომადგენლები, რათა დადგენილიყო მათი მონაცემთა სანდოობის და დაცვის საჭიროებები. კვლევის პროცესში ასევე ჩატარდა ტექნოლოგიური ტესტირებები. ამ ტესტირებებში განხორციელდა ბლოკჩეინის მოდელის ინტეგრაცია სხვადასხვა სცენარებში და შეფასდა მისი ეფექტიანობა რეალურ მონაცემთა ბაზებთან მუშაობისას.

კვლევის ჰიპოთეზა მდგომარეობს შემდეგში: შესაძლოა შეიქმნას ბიზნეს მოდელი, რომელიც ხელმისაწვდომს გახდის ბლოკჩეინის მექანიზმის ელემენტებს მცირე და საშუალო ბიზნესისთვის ცენტრალიზებულ მონაცემთა ბაზებში ბლოკჩეინის ტექნოლოგიის ინტეგრაციის გზით, რაც გაზრდის მონაცემთა სანდოობას და უზრუნველყოფს მათ უცვლელობას. ეს ჰიპოთეზაეფუძნება ბლოკჩეინის უნიკალურ მახასიათებლებს, როგორებიცაა დეცენტრალიზაცია, კრიპტოგრაფიული დაცვა და ტრანზაქციების ჩანაწერებისა უდიტის შესაძლებლობა. წინამდებარე ნაშრომი ჩატარებული კვლევებითა და ლიტერატურილი მიმოხილვის დახმარებით ეცდება მოცემული ჰიპოთეზის დადასტურებას ან/და უარყოფას.

კვლევისთვის გამოყენებული მეთოდები. კვლევაში გამოყენებულია თეორიული და ემპირიული მეთოდების კომპლექსი. თეორიული ანალიზი მოიცავდა ბლოკჩეინის ტექნოლოგიისა და კრიპტოგრაფიული მექანიზმების შესწავლას, არსებული ლიტერატურის განხილვას და კონცეპტუალური ჩარჩოს ჩამოყალიბებას. ემპირიული კვლევები მოიცავდა საველე კვლევებს, გამოკითხვებს და ინტერვიუებს. კომპიუტერული მოდელირების გამოყენებით შეიქმნა ბლოკჩეინის ჰიბრიდული მოდელი, რომელიც ტესტირდა სხვადასხვა სცენარებში.

კვლევის ობიექტი და საგანი. კვლევის **ობიექტს** წარმოადგენს ბიზნეს მოდელი, რომელიც ორიენტირებული იქნება ინფორმაციის საიმედობასა და სანდოობაზე სხვადასხვა სფეროს წარმომადგენელ ორგანიზაციებში. კვლევის

საგანია სხვადასხვა სფეროში(დარგში), როგორიცაა ჯანდაცვა, განათლება, ბუღალტერია და ა.შ. ინფორმაციის საიმედოობის გაზრდის მეთოდების თავისებურებების დადგენა, ბლოკჩეინის სერვისის დანერგვისა და გამოყენების ეფექტურობის საფუძველზე ახალი ბიზნესმოდელის შემუშავება, რომელიც სხვა ანალოგიურ ბიზნესში არ არის.

ნაშრომის მეცნიერული სიახლე. ინფორმაციის სანდოობის ამაღლების მიზნით:

- განისაზღვრა სხვადასხვა სფერო, რომელთათვისაც მნიშვნელოვანია ინფორმაციის საიმედოობა და დაცვა;
- დადგინდა ფუნქციონალური კავშირები ორგანიზაციისთვის ინფორმაციის სანდოობის და დაცულობისთვის საჭირო პარამეტრებს შორის;
- ჩამოყალიბდა ბიზნეს მოდელი, რომელიც უზრუნველყოფს ინფორმაციის სანდოობას და დაცულობას;
- გამორკვეულ იქნა ორგანიზაციებში მიმდინარე ბიზნეს პროცესები და შემუშავდა მონაცემების სანდოობის ბლოკჩეინით უზრუნველყოფის მოდელი;
- შემუშავდა ბლოკჩეინის დამცავი მექანიზმების შესაბამისი პროგრამული უზრუნველყოფა;
- შემუშავებული პგოგრამული უზრუნველყოფა ადაპტირდა სხვადასხვა ორგანიზაციის მონაცემთა ბაზაზე.

ნაშრომის შედეგების **პრაქტიკული გამოყენება** მოიცავს რამდენიმე ძირითად მიმართულებას:

- *ფინანსური, იურიდიული და საჯარო სექტორებისთვის* შემოთავაზებული ბიზნეს მოდელი უზრუნველყოფს მონაცემთა სანდოობასა და უცვლელობის დაცვას. ეს ხელს უწყობს ტრანზაქციების უსაფრთხოებას, აუდიტის გამარტივებას, დოკუმენტების გაყალბების პრევენციას და რეგულაციებთან შესაბამისობის გაუმჯობესებას.
- *ჯანდაცვასა და განათლებაში* მოდელი მნიშვნელოვნად ზრდის პაციენტის ჩანაწერებისა და აკადემიური სერტიფიკატების სანდოობას. ეს ამცირებს მონაცემთა გაყალბების რისკს და აძლიერებს მომხმარებლის ნდობას.

- *მიწოდების ჯაჭვებში და მცირე/საშუალო ბიზნესში* შემოთავაზებული მოდელი ზრდის მონაცემების გამჭვირვალობას და სანდოობას, რაც ხელს უწყობს ოპერაციების მართვის ეფექტურობას და თაღლითობის პრევენციას, ინფრასტრუქტურის ძირეული ცვლილებების გარეშე.

ამრიგად, ნაშრომის პრაქტიკული დანერგვა მონაცემთა უსაფრთხოებისა და სანდოობის გაძლიერებით, სხვადასხვა ინდუსტრიაში გაუმჯობესებულ ეფექტურობას და ნდობას უზრუნველყოფს.

სამუშაოს აპრობაცია. დისერტაციის თემაზე საქართველოს ტექნიკური უნივერსიტეტის ენერგეტიკის ფაკულტეტის საწარმოო ინოვაციებისა და ოპერაციათა მენეჯმენტის დეპარტამენტში ჩატარდა პრეზენტაცია სამ კოლოქვიუმზე და წინასწარ დაცვაზე. ხოლო კვლევის შედეგები, მოხსენებული იქნა 4 საერთაშორისო კონფერენციაზე. ასევე, დისერტაციის თემაზე გამოქვეყნებულია 6 სტატია.

დისერტაციის მოცულობა და სტრუქტურა

სადისერტაციო ნაშრომი მოიცავს 151 ნაბეჭდ გვერდს 3 ცხრილისა და 11 ნახაზის ჩათვლით და შედგება ლიტერატური მიმოხილვის, შესავალის, 5 თავის, 23 ქვეთავის, დასკვნისა და გამოყენებული ლიტერატურის ნუსხისაგან.

ნაშრომის ძირითადი შინაარსი

დისერტაცია შედგება შესავლის, ხუთი თავისა და შეჯამებისგან, საიდანაც შესავალში შეფასებულია თემის აქტუალობა და აღწერილია პრობლემა საქართველოს მაგალითზე, ასევე, გამოყენებული მეთოდებისა და კვლევის მიზნების აღწერის შემდეგ წარმოდგენილია ლიტერატურის მიმოხილვა, სადაც განხილულია საერთაშორისო გამოცდილება ბიზნეს მოდელებისა და ინფორმაციის სანდოობის მიმართულებებით.

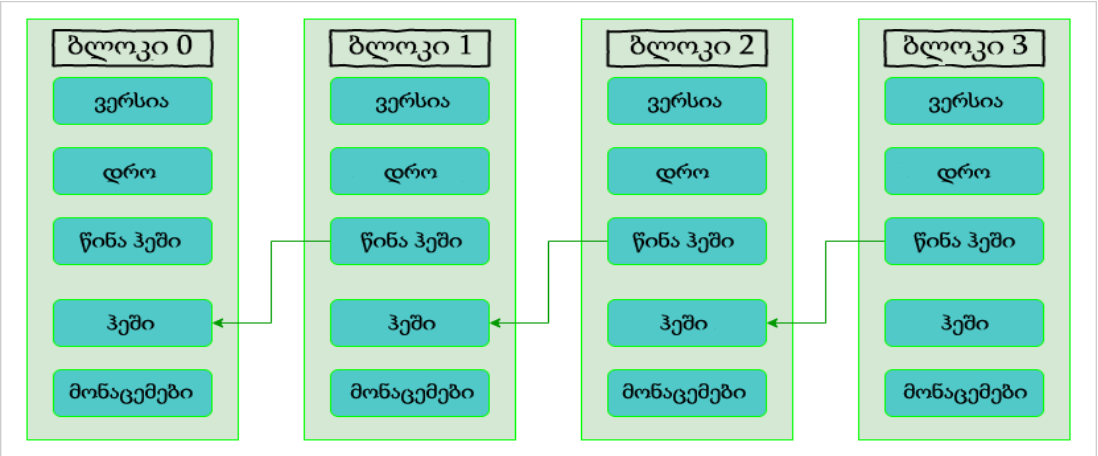
ლიტერატურის მომიხილვის შემდეგ იწყება **პირველი თავი, ბლოკჩეინის ორიგინალი მოდელი,** რომელიც წარმოადგენს ბლოკჩეინის ტექნოლოგიის საფუძვლიან შესწავლას და მისი პრაქტიკული გამოყენების შესაძლებლობების განხილვას. ამ თავში დეტალურად არის განხილული ბლოკჩეინის არქიტექტურა, კრიპტოგრაფიული მექანიზმები, მონაცემთა დაცვის მეთოდები და კომუნიკაციის პროცესები. განსაკუთრებული ყურადღება ეთმობა ბლოკჩეინის ინტეგრაციის შესაძლებლობას არსებული ცენტრალიზებული მონაცემთა ბაზების ინფრასტრუქტურაში, რაც რეალისტური და ეფექტიანი გადაწყვეტაა იმ ორგანიზაციებისთვის, რომლებიც ვერ ახერხებენ სრულად დეცენტრალიზებულ სისტემებზე გადასვლას.

პირველი თავის პირველ ქვეთავში, **მონაცემთა ბაზებში ინფორმაციის შენახვისას თანამედროვე კრიპტოგრაფიული მეთოდების გამოყენების ასპექტები,** დეტალურადაა განხილული, თუ როგორ გამოიყენება ჰეშირების ალგორითმები მონაცემთა დაცვის უზრუნველსაყოფად. ჰეშირების ალგორითმები, როგორიცაა **SHA-256** (Secure Hash Algorithm 256-bit), ქმნიან მონაცემთა უნიკალურ და ფიქსირებული სიგრძის „ანაბეჭდს“. ნებისმიერი უმნიშვნელო ცვლილება მონაცემებში იწვევს სრულიად განსხვავებულ ჰეშს, რაც შეუძლებელს ხდის ცვლილების შეუმჩნევლად განხორციელებას. მაგალითად, ფინანსურ სექტორში, როდესაც ტრანზაქცია ემატება მონაცემთა ბაზას, მისგან წარმოებული ჰეში ინახება ბლოკჩეინში. მომავალში, თუ ვინმე შეეცდება ამ ტრანზაქციის შეცვლას, ბლოკჩეინზე არსებული ჰეში ვერ დაემთხვევა მონაცემთა ბაზის ახალ ვერსიას, რაც

დაუყოვნებლივ გამოავლენს დარღვევას. ეს მექანიზმი უზრუნველყოფს მონაცემთა მთლიანობის დაცვას და სისტემაში ნებისმიერი ცვლილების „გამოჭერას“.

ამ სექციაში ასევე განხილულია **ასიმეტრიული კრიპტოგრაფიის** მნიშვნელობა. ამ მეთოდის გამოყენებით, მონაცემთა დაცვა უზრუნველყოფილია საჯარო და პირადი გასაღებების წყვილით. მაგალითად, ცენტრალიზებულ მონაცემთა ბაზაში შენახული მონაცემების შესამოწმებლად, მომხმარებელს შეუძლია მონაცემის ავთენტურობა დაადასტუროს მხოლოდ საჯარო გასაღებით, მაშინ როცა პირადი გასაღები ინახება მხოლოდ უფლებამოსილი პირის ხელში. ეს პროცესი აძლიერებს მონაცემთა ბაზის დაცულობას და გამორიცხავს მონაცემების არაავტორიზებული მოდიფიკაციის შესაძლებლობას.

პირველი თავის მეორე ქვეთავში, **ბლოკჩეინი როგორც მონაცემთა სტრუქტურა**, აღწერილია ბლოკჩეინის სტრუქტურის კომპლექსური დეტალები. ბლოკჩეინი შედგება ბლოკებისგან, რომლებიც უკავშირდებიან ერთმანეთს და ქმნიან თანმიმდევრულ ჯაჭვს. თითოეული ბლოკი შეიცავს ტრანზაქციების მონაცემებს, წინა ბლოკის ჰეშს და დროის შტამპს. ბლოკებს შორის კავშირის უნიკალურობას განაპირობებს ჰეშირების პროცესი, რაც ქმნის ბლოკის შინაარსის უნიკალურ იდენტიფიკატორს. ამგვარი სტრუქტურა შეუძლებელს ხდის ბლოკის შეცვლას ისე, რომ ამის შესახებ არ შეიტყოს მთელმა ქსელმა.



ბლოკჩეინის სტრუქტურა.

ბლოკჩეინის აგებისას ცდილობენ, რომ ყოველ კვანძისთვის გამოთვალონ ისეთი სიდიდე (ტექსტში შემდგომ - ნონსი), რომელიც დამოკიდებული იქნება

კვანძის შიგთავსზე, რომლის გამოთვლაც გარკვეულ დროით და ენერგეტიკულ დანახარჯთან იქნება დაკავშირებული და რომელსაც შეინახავენ თავად ამ კვანძში. როგორც წესი, კვანძის ნონსი გამოითვლება, როგორც უტოლობის ამონახსნი, რომლის პარამეტრიც არის წინა კვანძის მონაცემები, ხოლო თავად უტოლობაში უცნობი ცვლადი შებმულია ჰეშირების ფუნქციაში. ნონსის გამოთვლა შესაძლებელია შემდეგი უტოლობით:

$$H(X_i, D_i, H(N_{i-1})) < 0000001$$

სადაც:

N_i – i-ური კვანძი

D_i – i-ურ კვანძში შენახული მონაცემები

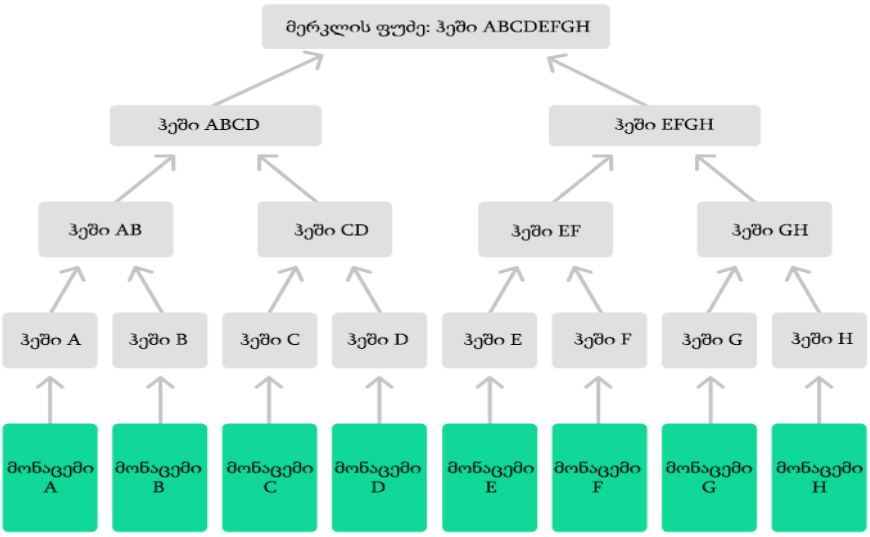
H - ჰეშ ფუნქცია

X_i – i-ური კვანძის ნონსი

აქედან გამომდინარე, ამ უტოლობის ერთი მაინც ამონახსნის საპოვნელად აუცილებელია გადარჩევის მეთოდის გამოყენება, რაც დაკავშირებულია უამრავი ჰეშის გამოთვლასთან და მნიშვნელოვან დროით და ენერგეტიკულ დანახარჯთან.

ამავე სექციაში განსაკუთრებული ყურადღება ეთმობა **მერკლის ხის (Merkle Tree)** ტექნოლოგიას. მერკლის ხე წარმოადგენს ბინარული ხის სტრუქტურას, რომლის ფოთლები შეიცავენ ტრანზაქციების ჰეშებს, ხოლო შიდა კვანძები ინახავენ შვილობილი ჰეშების შეჯამას

.



მერკლის ხის სტრუქტურა.

მერკლის ხის მთავარი უპირატესობა ისაა, რომ იგი იძლევა ტრანზაქციის სწრაფი და ეფექტური ვალიდაციის შესაძლებლობას. მაგალითად, ცენტრალიზებულ მონაცემთა ბაზაში არსებული დიდი მოცულობის ჩანაწერების შემოწმებისას, მერკლის ხე საშუალებას იძლევა მხოლოდ შესაბამისი ფოთლების ვალიდაცია განხორციელდეს, რაც ამცირებს გამოთვლითი რესურსების ხარჯვას. მერკლის ხის ტექნოლოგია ფართოდ გამოიყენება ფინანსურ და სამედიცინო სექტორებში, სადაც დიდი რაოდენობის ჩანაწერების სანდოობა და ვალიდაცია აუცილებელია.

შემდეგ სექციაში, **ბლოკჩეინის მწარმოებელ და მომხმარებელ მხარეს შორის ორმხრივი კომუნიკაციის ანალიზი**, განხილულია ბლოკჩეინის ქსელში ინფორმაციის გადაცემის პროცესები. ბლოკჩეინის ქსელი ფუნქციონირებს პირთა შორის (P2P) კომუნიკაციის პრინციპით, რაც ნიშნავს, რომ ყველა მონაწილე კვანძი პირდაპირ უკავშირდება სხვა კვანძებს და მონაცემებს არეგისტრირებს ცენტრალური სერვერის გარეშე. ეს იწვევს მონაცემთა გადაცემის სისწორისა და მთლიანობის შენარჩუნებას. ცენტრალიზებული მონაცემთა ბაზების შემთხვევაში, ბლოკჩეინის ამ მექანიზმის გამოყენება იძლევა დამატებითი დაცვის შესაძლებლობას, რადგან მონაცემთა ნებისმიერი ცვლილება უნდა დამოწმდეს ქსელის მონაწილეების მიერ.

თავი 1.4, **ბლოკჩეინის მოდელის წარმოება და ჰოსტინგი,** აღწერს ბლოკჩეინის მოდელის შექმნისა და ჰოსტინგის პროცესს, რაც გულისხმობს საჭირო აპარატურისა და ინფრასტრუქტურის სწორად ორგანიზებას. ბლოკჩეინის წარმოება დაკავშირებულია მნიშვნელოვან ფინანსურ და ტექნიკურ ხარჯებთან, მათ შორის ძვირადღირებულ აპარატურასთან და შესაბამისი კვალიფიკაციის მქონე პერსონალის საჭიროებასთან.

ამ პროცესის ეფექტურად განხორციელებისთვის, შესაძლებელია, რომ ბლოკჩეინის წარმოებაზე პასუხისმგებელი იყოს დამოუკიდებელი განყოფილება, რომელიც არ იქნება უშუალოდ დაკავშირებული იმ განყოფილებებთან, რომლებიც ბლოკჩეინს ყოველდღიური საქმიანობისთვის იყენებენ. ეს მიდგომა ხელს უწყობს ფუნქციური განაწილებისა და უსაფრთხოების გაუმჯობესებას, რადგან

ბლოკჩეინის წარმოებისა და გამოყენების პროცესები ერთმანეთისგან დამოუკიდებლად იმართება.

გარდა ამისა, ბლოკჩეინის ჰოსტინგისთვის მნიშვნელოვანია ისეთი პლატფორმის შერჩევა, რომელიც უზრუნველყოფს მაღალი დონის ხელმისაწვდომობას, უსაფრთხოებას და მასშტაბურობას. ჰოსტინგის სტრატეგიის სწორი დაგეგმარება კრიტიკულია იმისთვის, რომ ბლოკჩეინის მოდელი სტაბილურად და ეფექტურად ფუნქციონირებდეს სხვადასხვა სერვისების მხარდასაჭერად

ბოლოს, **ბლოკჩეინის კონფიდენციალობის ასპექტები** ეხება იმ სირთულეებს, რომლებიც დაკავშირებულია ბლოკჩეინის სისტემაში მონაცემთა კონფიდენციალურობის უზრუნველყოფასთან. მიუხედავად იმისა, რომ ბლოკჩეინი უზრუნველყოფს მონაცემთა მაღალი დონის გამჭვირვალობას, არსებობს გარკვეული შემთხვევები, როდესაც აუცილებელია მონაცემთა კონფიდენციალური შენახვა. ბლოკჩეინის ტექნოლოგიაში კონფიდენციალობა მიღწეულია კრიპტოგრაფიული მეთოდების გამოყენებით, რაც საშუალებას იძლევა მომხმარებლის იდენტიფიცირება მოხდეს მხოლოდ ღია გასაღების მეშვეობით. ამ მიდგომით, ბლოკჩეინზე დაფუძნებულ სისტემებში ტრანზაქციები საჯაროა, მაგრამ მონაწილეთა პირადი ინფორმაცია ანონიმურია და არ არსებობს გზა, რომ ღია გასაღებიდან უშუალოდ ამოიცნო მისი მფლობელი. მტკიცებულებები ნულოვანი ინფორმაციით (Zero-Knowledge Proofs) იძლევა საშუალებას, ინფორმაცია ვალიდურად დადასტურდეს მისი შინაარსის გამჟღავნების გარეშე. ასევე, ჰომომორფული დაშიფვრა საშუალებას იძლევა მონაცემთა დაშიფრული სახით დამუშავება, რაც კრიტიკულია ისეთ სექტორებში, როგორიცაა ჯანდაცვა და ფინანსები.

1.6 ქვეთავში განხილულია ბლოკჩეინის მწარმოებელსა და მომხმარებელს შორის წარმოშობადი სადაო საკითხები. ეს საკითხები ძირითადად ეხება ბლოკჩეინის სანდოობას, მონაცემთა დამუშავების სისწორესა და სისტემის გამჭვირვალობას. მომხმარებლებს შეიძლება გაუჩნდეთ ეჭვები ბლოკჩეინის მწარმოებლის მიერ მონაცემთა არასწორად დამუშავების ან ჩანაწერების მანიპულირების შესახებ. ასეთი სადაო სიტუაციების პრევენციისთვის, ნაშრომში

შემოთავაზებულია ტექნიკური გადაწყვეტილებები, რომლებიც მოიცავს ბლოკჩეინის ჩანაწერების ვალიდაციის პროცესებსა და აუდიტის მექანიზმებს.

თავი 1.7 აღწერს იმ მეთოდებსა და მექანიზმებს, რომლებიც საჭიროა მონაცემთა ბაზაში მართლსაწინააღმდეგო ცვლილებების პრევენციისთვის. განსაკუთრებული ყურადღება ეთმობა იმ საფრთხეებს, რომლებიც დაკავშირებულია მონაცემთა ბაზის ადმინისტრატორებისა და ტექნიკური პერსონალის მიერ არალეგიტიმური ცვლილებების განხორციელებასთან. ასეთი ცვლილებები შესაძლოა პირდაპირ მონაცემთა ბაზის ფაილებში განხორციელდეს, რაც მონაცემთა მართვის სისტემის გვერდის ავლით ხდება და მათი აღმოჩენა რთულდება.

პრევენციული მექანიზმები მოიცავს ციფრული ხელმოწერების, ჰეშირების და მონიტორინგის მექანიზმების გამოყენებას, რათა ნებისმიერი ცვლილება გამოვლენილი და დადასტურებული იყოს ავტომატურად. ამ მეთოდების მიზანია მონაცემთა მთლიანობის დაცვა და ბოროტმოქმედების მცდელობების სწრაფი გამოვლენა

პირველი თავის ბოლო ქვეთავი **მონაცემთა ბაზის დაცვის ამოცანები,** ყურადღებას ამახვილებს მონაცემთა ბაზის დაცვის ამოცანებზე, რომლებიც მიზნად ისახავს მონაცემთა სანდოობის, მთლიანობისა და უცვლელობის უზრუნველყოფას. ნაშრომში განხილულია რამდენიმე კონკრეტული გამოწვევა, რაც დაკავშირებულია მონაცემთა ბაზაში ცვლილებების კონტროლთან და მათი არალეგიტიმური მოდიფიკაციების პრევენციასთან. ერთ-ერთი ამოცანა არის ისეთი ცხრილების დაცვა, სადაც დაშვებულია მხოლოდ მონაცემთა დამატება, მაგრამ არა მათი შეცვლა ან წაშლა. ამის უზრუნველყოფა ხდება ბლოკჩეინის ჰეშირების მექანიზმებით, რაც საშუალებას იძლევა ნებისმიერი ცვლილება სწრაფად გამოვლინდეს.

დაცული უნდა იყოს ის ცხრილებიც, სადაც ცვლილებები ლეგიტიმურად შეიძლება განხორციელდეს. ამ შემთხვევაში, ყოველი ცვლილებისას ხდება ახალი ჰეშის გენერირება, რაც მონაცემთა ისტორიის დეტალურ აღრიცხვას უზრუნველყოფს და აუდიტის პროცესს ამარტივებს. მნიშვნელოვანია არალეგიტიმური ცვლილებების პრევენცია, განსაკუთრებით ადმინისტრატორების

მიერ შესაძლო მანიპულაციების თავიდან ასაცილებლად. ამისთვის გამოიყენება ციფრული ხელმოწერები და ჰეშირების რეგულარული შემოწმება, რაც უზრუნველყოფს მონაცემთა ბაზაში ნებისმიერი ცვლილების კონტროლს.

თავში ასევე განხილულია მონაცემთა ბაზის შემოწმების მექანიზმები, რომლებიც მონაცემთა მდგომარეობის პერიოდულ მონიტორინგს და ანალიზს ახორციელებს. ეს მექანიზმები ავტომატურად აფიქსირებს ნებისმიერ არათავსებად ცვლილებას და აფრთხილებს სისტემის ადმინისტრატორებს ან მენეჯმენტს. ამგვარად, ბლოკჩეინის ტექნოლოგიის გამოყენება მონაცემთა ბაზის დაცვის ამოცანების გადაჭრაში აძლიერებს მონაცემთა სანდოობას და სისტემის გამჭვირვალობას, რაც კრიტიკულად მნიშვნელოვანია ინფორმაციის უსაფრთხოებისთვის.

პირველი თავი აჯამებს ბლოკჩეინის ტექნოლოგიის სიღრმისეულ ანალიზს და აჩვენებს, თუ როგორ შეიძლება მისი ინტეგრაცია ცენტრალიზებულ მონაცემთა ბაზებში. ამ ინტეგრაციის საშუალებით, შესაძლებელია მონაცემთა უსაფრთხოებისა და სანდოობის დონის მნიშვნელოვნად ამაღლება არსებული ინფრასტრუქტურის ძირეული ცვლილების გარეშე. ბლოკჩეინის კრიპტოგრაფიული მექანიზმები, მერკლის ხე და ჰოსტინგის ტექნოლოგიები იძლევა კომპლექსურ გადაწყვეტას, რომელიც ადაპტირებადია სხვადასხვა სექტორის საჭიროებებზე.

მეორე თავი. პროგრამული უზრუნველყოფის შემუშავებისა და მენეჯმენტის მექანიზმები

მეორე თავი ფოკუსირებულია ბლოკჩეინის ტექნოლოგიის იმპლემენტაციისთვის აუცილებელი პროგრამული უზრუნველყოფის შემუშავების პროცესზე და პროექტის მართვის მექანიზმებზე. ამ თავში დეტალურად არის აღწერილი პროგრამული განვითარების თანამედროვე მეთოდოლოგიები, პროექტის მართვის სტრატეგიები და ბლოკჩეინის დანერგვის ეტაპები. განსაკუთრებული ყურადღება ეთმობა იმ საკითხებს, რომლებიც დაკავშირებულია ცენტრალიზებულ მონაცემთა ბაზებში ბლოკჩეინის ინტეგრაციის პროცესთან, რაც იძლევა მოქნილ და დაცულ სამუშაო სისტემას.

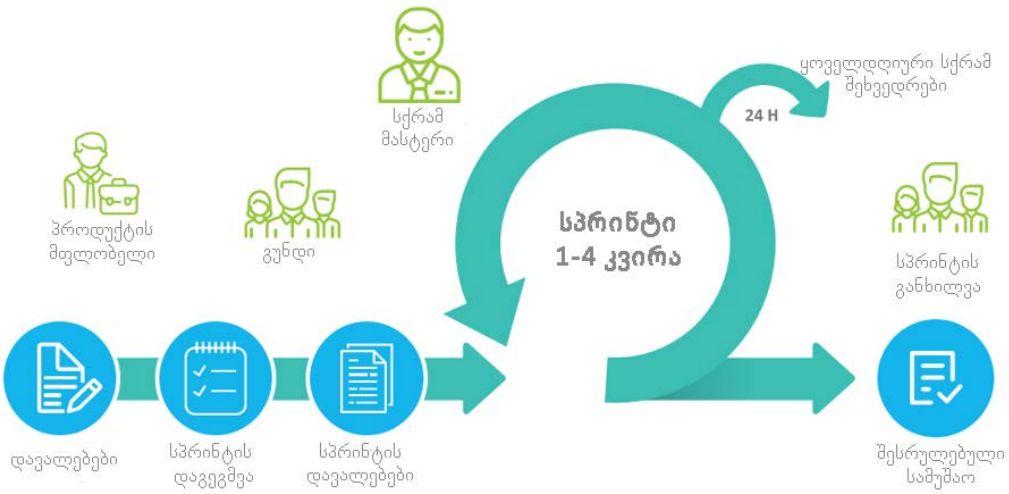
პირველ ქვეთავში მიმოხილულია პროგრამული უზრუნველყოფის ეფექტური შემუშავების მეთოდოლოგიები და მათი მნიშვნელობა თანამედროვე ბიზნესში. აქ ყურადღება გამახვილებულია იმაზე, რომ თანამედროვე ტექნოლოგიური გარემოს კონკურენტულ პირობებში წარმატებას აღწევს ის კომპანია, რომელიც ეფექტურად იყენებს პროგრამული უზრუნველყოფის განვითარებისთვის არსებულ მეთოდებსა და პრაქტიკებს.

განსაკუთრებით აღინიშნება, რომ პროგრამული უზრუნველყოფის შემუშავება მოითხოვს მრავალფეროვანი სპეციალისტების მონაწილეობას, როგორიცაა დარგობრივი ექსპერტები, მენეჯმენტი, უსაფრთხოების სპეციალისტები და იურისტები. თანამშრომლობითი მიდგომის საშუალებით იქმნება **პროგრამული** მოთხოვნების სპეციფიკაციის დოკუმენტი (SRS), სადაც დეტალურადაა გაწერილი პროგრამის ფუნქციონალი და მოთხოვნები.

პროცესის დაგეგმვის ეტაპზე განისაზღვრება შესასრულებელი დავალებები და იმ მოთხოვნების სია, რომლებიც შეიძლება მომდინარეობდეს მომხმარებლებისგან, მარკეტინგის გუნდებისგან ან დეველოპერებისგან. ასევე, ხაზგასმულია, რომ პროექტის მიმდინარეობისას ცვლადი მოთხოვნების გამო აუცილებელია პროცესის მოქნილობა და სწრაფი რეაგირების მექანიზმები.

თავის მეორე ნაწილში განხილულია **პროგრამული უზრუნველყოფის შემუშავების მეთოდოლოგია**. თანამედროვე ბლოკჩეინ პროექტების წარმატებული იმპლემენტაციისთვის კრიტიკულად მნიშვნელოვანია მოქნილი და ადაპტირებადი მეთოდოლოგიების გამოყენება. Agile და Scrum მეთოდოლოგიები უზრუნველყოფენ ეტაპობრივ და სწრაფ განვითარებას, რაც განსაკუთრებით მნიშვნელოვანი ხდება ტექნოლოგიურად კომპლექსური პროექტების შემთხვევაში. Agile მიდგომა გულისხმობს განვითარების ციკლის დაყოფას მცირე ინტერვალებად (სპრინტებად), რაც საშუალებას იძლევა თითოეული ეტაპის ბოლოს მოხდეს კოდის ტესტირება, ვალიდაცია და საჭიროების შემთხვევაში გაუმჯობესება. Scrum მეთოდოლოგია კი უზრუნველყოფს დავალებების ორგანიზებულ მართვას, გუნდის წევრების პასუხისმგებლობის ზუსტ განსაზღვრას და მუდმივ კომუნიკაციას პროექტის მონაწილეებს შორის. ეს

მეთოდოლოგიები საშუალებას იძლევა სწრაფად მოხდეს შეცდომების იდენტიფიცირება და გასწორება, რაც ზრდის პროექტის წარმატების ალბათობას.



„სქრამ“-ის (SCRUM) მუშაობის პრონციპი.

მეორე თავის მესამე ნაწილში განხილულია **პროგრამული უზრუნველყოფის შექმნის პროცესის მართვის მექანიზმები**. ბლოკჩეინის პროექტების წარმატებით განხორციელებისთვის აუცილებელია სწორი მართვის სტრატეგიების დანერგვა. პროექტის მართვის ერთ-ერთი მნიშვნელოვანი ასპექტია რესურსების მართვა, რაც მოიცავს გუნდის წევრების დავალებების სწორად დელეგირებას, სამუშაოს მოცულობის განსაზღვრას და ვადების კონტროლს. გამოიყენება ისეთი ინსტრუმენტები, როგორიცაა Jira, Trello და Asana, რომლებიც ხელს უწყობს პროექტის პროცესების მონიტორინგს და სამუშაოს ეფექტურ ორგანიზებას. ასევე განხილულია რისკების მენეჯმენტის მეთოდები, რომლებიც ითვალისწინებენ პოტენციური პრობლემების იდენტიფიცირებას და მათ პრევენციას პროექტის ყველა ეტაპზე.

მნიშვნელოვანი საკითხია კომუნიკაციის მართვა პროექტის გუნდსა და დაინტერესებულ მხარეებს შორის. ბლოკჩეინის პროექტები ხშირად მოითხოვს ინტერდისციპლინარულ გუნდებთან თანამშრომლობას, რაც გულისხმობს დეველოპერების, სისტემური არქიტექტორების, უსაფრთხოების ექსპერტების და ბიზნეს ანალიტიკოსების კოორდინირებულ მუშაობას. რეგულარული შეხვედრები, ანგარიშგებები და უკუკავშირის სისტემები უზრუნველყოფს

პროექტის გამჭვირვალობას და მისი განვითარების პროცესში მონაწილეთა ჩართულობას.

მეორე თავის ერთ-ერთი საკვანძო ასპექტია ბლოკჩეინის სისტემის დანერგვის ეტაპები. ბლოკჩეინის ინტეგრაციის პროცესში მოცემულია კონკრეტული ნაბიჯები, რომლებიც საჭიროა სისტემის წარმატებით დანერგვისთვის. პროცესის პირველი ეტაპი მოიცავს მოთხოვნების დეტალურ ანალიზს, რომლის მიზანია განისაზღვროს ბლოკჩეინის დანერგვის საჭიროება და მიზნები. ამის შემდეგ ხდება სისტემის დიზაინის შექმნა, სადაც განისაზღვრება ბლოკჩეინის არქიტექტურა, მისი კომპონენტები და ფუნქციონალური მახასიათებლები. იმპლემენტაციის ეტაპზე ხდება ბლოკჩეინის კოდის დაწერა და სისტემის მოდულების ინტეგრაცია. ამ პროცესში განსაკუთრებული ყურადღება ექცევა ცენტრალიზებულ მონაცემთა ბაზასთან ბლოკჩეინის ჰარმონიულ კავშირს, რათა არ დაირღვეს არსებული სისტემის სტაბილურობა.

მნიშვნელოვანია ტესტირების ეტაპი, რომელიც მოიცავს როგორც ერთეულის ტესტირებას, ისე სისტემურ ტესტირებას. ბლოკჩეინის ინტეგრაციისას საჭიროა ტრანზაქციების სისწორის, უსაფრთხოების და სანდოობის დეტალური შემოწმება. ტესტირების შედეგების საფუძველზე ხორციელდება გაუმჯობესებები და კორექტივები, რის შემდეგაც სისტემა მზად არის საბოლოო გაშვებისთვის. დანერგვის ბოლო ეტაპი მოიცავს სისტემის მონიტორინგს და მხარდაჭერას, რათა უზრუნველყოფილი იყოს მისი უწყვეტი და სტაბილური მუშაობა.

მეორე თავში დადგინდა, რომ ბლოკჩეინის ტექნოლოგიის წარმატებული იმპლემენტაცია დიდწილად დამოკიდებულია პროგრამული უზრუნველყოფის შემუშავებისა და პროექტის მართვის ეფექტიან პროცესზე. Agile და Scrum მეთოდოლოგიების გამოყენება, რესურსების მართვის სწორი სტრატეგიები და კომუნიკაციის კარგად ორგანიზებული სისტემა იძლევა იმის შესაძლებლობას, რომ ბლოკჩეინის პროექტი განხორციელდეს დროულად და მაღალი ხარისხით. ბლოკჩეინის სისტემის დანერგვის ეტაპების მკაფიოდ განსაზღვრა უზრუნველყოფს მის სწორ ინტეგრაციას ცენტრალიზებულ მონაცემთა ბაზებთან, რაც საბოლოოდ იძლევა მოქნილ, უსაფრთხო და სანდო სისტემას, რომელიც პასუხობს თანამედროვე ბიზნესის მოთხოვნებს.

მესამე თავი ემსახურება ბლოკჩეინის ტექნოლოგიის საჭიროებისა და გამოყენების შესაძლებლობების შესწავლას სხვადასხვა ინდუსტრიულ სფეროში. აქ განხილულია, როგორ შეუძლია ბლოკჩეინის ინტეგრაციას გააუმჯობესოს მონაცემთა სანდოობა, უსაფრთხოება და პროცესების გამჭვირვალობა ისეთ კრიტიკულ დარგებში, როგორებიცაა განათლება, ჯანდაცვა და ფინანსები. ეს თავი ყურადღებას ამახვილებს კონკრეტულ პრობლემებზე, რომელთა გადაჭრა ბლოკჩეინის მეშვეობით შესაძლებელია, და აღწერს ბლოკჩეინის პრაქტიკული დანერგვის სარგებელს თითოეულ სფეროში.

თავის პირველ ნაწილში მიმოხილულია ბლოკჩეინის საჭიროება საგანმანათლებლო დაწესებულებებში. თანამედროვე სასწავლო დაწესებულებები დიდ გამოწვევებს განიცდიან აკადემიური ჩანაწერების სანდოობისა და მონაცემთა ხელშეუხებლობის უზრუნველყოფის კუთხით. უნივერსიტეტებსა და სკოლებში ხშირად ხდება ისეთი შემთხვევები, როდესაც დიპლომები ან სერტიფიკატები ყალბდება, რაც საფრთხეს უქმნის საგანმანათლებლო სისტემის რეპუტაციას. ბლოკჩეინის ტექნოლოგიის დანერგვა იძლევა შესაძლებლობას, რომ ყველა აკადემიური ჩანაწერი დამუშავდეს და შენახულ იქნას ბლოკჩეინში. ამის შედეგად, ნებისმიერი ჩანაწერი ხდება უნიკალური, უცვლელი და მარტივად ვერიფიცირებადი. მაგალითად, როდესაც სტუდენტი იღებს დიპლომს, მისი ბლოკჩეინში დამატება უზრუნველყოფს დიპლომის ნამდვილობის სწრაფად დადასტურებას მომავალი დამსაქმებლების ან საგანმანათლებლო დაწესებულებების მიერ. ეს ამცირებს ადმინისტრაციულ ხარჯებს და აძლიერებს სასწავლო პროცესის გამჭვირვალობას.

მეორე ნაწილში განხილულია ბლოკჩეინის გამოყენება ჯანდაცვის სისტემაში. ჯანდაცვის სექტორი განსაკუთრებით მგრძნობიარეა მონაცემთა სანდოობისა და უსაფრთხოების საკითხების მიმართ, რადგან პაციენტის ჩანაწერები მოიცავს კონფიდენციალურ ინფორმაციას, რომლის დაკარგვა ან შეცვლა შეიძლება სიცოცხლისთვის საშიში გახდეს. ამ პრობლემების გადასაჭრელად, ბლოკჩეინის ტექნოლოგია საშუალებას იძლევა შეიქმნას ერთიანი, უსაფრთხო და ტრანსპარენტული სისტემა პაციენტის ჩანაწერების შესანახად. ბლოკჩეინში შენახული სამედიცინო ჩანაწერები ხელმისაწვდომია მხოლოდ უფლებამოსილი

პირებისთვის და მათი შეცვლა შეუძლებელია ავტორიზაციის გარეშე. გარდა ამისა, ბლოკჩეინის მეშვეობით შესაძლებელია პაციენტის ისტორიის თვალის დევნება, რაც უზრუნველყოფს მკურნალობის სიზუსტესა და უწყვეტობას. მაგალითად, ექიმს შეუძლია სწრაფად და ზუსტად იხილოს პაციენტის სრული ისტორია სხვადასხვა კლინიკებიდან, რაც მკურნალობის პროცესს მნიშვნელოვნად აჩქარებს.

მესამე ნაწილში დეტალურადაა განხილული ბლოკჩეინის ტექნოლოგიის საჭიროება ფინანსურ სექტორში. საბანკო და საბუღალტრო მონაცემთა სანდოობა კრიტიკულად მნიშვნელოვანია ფინანსური ტრანზაქციებისას. ტრადიციული ფინანსური სისტემები დიდად დამოკიდებულნი არიან ცენტრალიზებულ მონაცემთა ბაზებზე, რაც ზრდის მონაცემთა შეცვლის ან გაყალბების რისკებს. ბლოკჩეინის ინტეგრაცია ამ სისტემებში იძლევა იმის გარანტიას, რომ ყოველი ფინანსური ოპერაცია ჩაიწერება უცვლელ და სანდო ფორმატში. ტრანზაქციების ჰეშირება და მათი შენახვა ბლოკჩეინში გამორიცხავს ნებისმიერი უკანონო ცვლილების შესაძლებლობას. ეს განსაკუთრებით მნიშვნელოვანია აუდიტის პროცესში, რადგან ბლოკჩეინის მეშვეობით შესაძლებელია ყველა ოპერაციის სრული ისტორიის შემოწმება რეალურ დროში. ფინანსურ სექტორში ბლოკჩეინის დანერგვამ შეიძლება მნიშვნელოვნად შეამციროს თაღლითობის შემთხვევები და გაზარდოს მომხმარებელთა ნდობა ფინანსური ინსტიტუტების მიმართ.

გარდა ამისა, მესამე თავი ყურადღებას ამახვილებს ბლოკჩეინის ინტეგრაციის სირთულეებზე და გამოწვევებზე სხვადასხვა დარგში. მიუხედავად იმისა, რომ ბლოკჩეინი უამრავ შესაძლებლობას იძლევა, მისი სრულყოფილი დანერგვა მოითხოვს დიდ რესურსებს, ტექნოლოგიურ ცოდნას და არსებულ სისტემებთან თავსებადობას. საგანმანათლებლო, ჯანდაცვისა და ფინანსურ სფეროში ბლოკჩეინის დანერგვა გულისხმობს მონაცემთა ბაზების მოდიფიკაციასა და ჰიბრიდული მოდელების შექმნას, სადაც ბლოკჩეინი გამოიყენება როგორც დამატებითი სანდოობისა და უსაფრთხოების ფენა. ამ პროცესში მნიშვნელოვანია გაიწეროს დეტალური გეგმები და დაინერგოს ეტაპობრივი ტესტირება, რათა არ დაირღვეს არსებული სისტემების ფუნქციონირება.

მესამე თავის დასკვნაში ნათლად ჩანს, რომ ბლოკჩეინის ტექნოლოგიის გამოყენება მნიშვნელოვნად აუმჯობესებს მონაცემთა სანდოობას, უსაფრთხოებასა

და გამჭვირვალობას ისეთ კრიტიკულ დარგებში, როგორიცაა განათლება, ჯანდაცვა და ფინანსები. ბლოკჩეინის ინტეგრაცია აკადემიურ სისტემებში უზრუნველყოფს დიპლომებისა და სერტიფიკატების ნამდვილობის დაცვის ახალ სტანდარტს. ჯანდაცვის სექტორში ბლოკჩეინი ხელს უწყობს პაციენტის მონაცემთა სიზუსტესა და უწყვეტობას, ხოლო ფინანსურ სისტემებში ის ქმნის უფრო უსაფრთხო და სანდო ტრანზაქციების გარემოს. მიუხედავად არსებული გამოწვევებისა, ბლოკჩეინის ტექნოლოგიის ჰიბრიდული მოდელების დანერგვა ცენტრალიზებულ მონაცემთა ბაზებში წარმოადგენს გრძელვადიან ინვესტიციას, რომელიც უზრუნველყოფს პროცესების ეფექტურობასა და მომხმარებელთა ნდობის გაზრდას.

მეოთხე თავი განიხილავს ბლოკჩეინის ტექნოლოგიის აუთსორსინგის შესაძლებლობებს, სარგებელსა და გამოწვევებს. ბლოკჩეინის დანერგვა და მისი ტექნიკური მხარდაჭერა მრავალი კომპანიასთვის შეიძლება იყოს რთული და რესურსების ჭარბად მოხმარების მიზეზი. ამ პრობლემების გადასაჭრელად აუთსორსინგი წარმოადგენს ერთ-ერთ ოპტიმალურ სტრატეგიას, რომელიც კომპანიებს საშუალებას აძლევს ბლოკჩეინის სერვისების განხორციელება და მართვა გადააბარონ სპეციალიზებულ მესამე მხარეს. ეს თავი მიმოიხილავს, როგორ მუშაობს ბლოკჩეინის აუთსორსინგის პროცესი, რა უპირატესობები და რისკები აქვს ამ მიდგომას, და როგორ შეიძლება სხვადასხვა კომპანიამ მოახდინოს ამ სერვისის ეფექტური გამოყენება.

თავის დასაწყისში განხილულია აუთსორსინგის დადებითი მხარეები. ერთ-ერთი მთავარი სარგებელი არის ხარჯების ოპტიმიზაცია და ტექნიკური კომპეტენციის გარედან მიღება. ბლოკჩეინის დანერგვა მოითხოვს მაღალკვალიფიციურ დეველოპერებს, სისტემურ არქიტექტორებს და უსაფრთხოების სპეციალისტებს. მათი მოძიება და შენარჩუნება შიდა გუნდში დაკავშირებულია დიდ ხარჯებთან და დროის რესურსთან. აუთსორსინგის შემთხვევაში, კომპანიას შეუძლია ბლოკჩეინის სერვისების მიღება სპეციალიზებული სააგენტოებისგან, რომლებიც უკვე ფლობენ საჭირო ცოდნას და გამოცდილებას. ეს ამცირებს დანერგვის დროს და უზრუნველყოფს სისტემის მაღალ ხარისხს.

მეორე მნიშვნელოვანი უპირატესობა არის სისტემის მასშტაბირებადობა. ბლოკჩეინის პროექტების ზრდასთან ერთად, კომპანიას შეიძლება დასჭირდეს ინფრასტრუქტურის გაფართოება და რესურსების ზრდა. აუთსორსინგის კომპანიები ხშირად გვთავაზობენ მოქნილ ინფრასტრუქტურულ გადაწყვეტილებებს, რომლებიც ადვილად მასშტაბირდება მომხმარებლის მოთხოვნების შესაბამისად. ეს განსაკუთრებით მნიშვნელოვანია სწრაფად მზარდი სტარტაპებისთვის და საშუალო ზომის კომპანიებისთვის, რომლებსაც სჭირდებათ სწრაფი ადაპტაცია ბაზრის მოთხოვნებთან.

თუმცა, აუთსორსინგს აქვს გარკვეული რისკები და უარყოფითი მხარეები. ერთ-ერთი მთავარი გამოწვევაა კონფიდენციალურობისა და უსაფრთხოების საკითხები. ბლოკჩეინის სერვისების აუთსორსინგისას კომპანიამ უნდა უზრუნველყოს, რომ მესამე მხარესთან მონაცემთა გადაცემა და შენახვა უსაფრთხოა. ასევე არსებობს რისკი იმისა, რომ აუთსორსინგის კომპანია ვერ დაიცვას საჭირო უსაფრთხოების სტანდარტები, რაც შეიძლება გახდეს მონაცემთა გაჟონვის ან კიბერშეტევის მიზეზი. ამის თავიდან ასაცილებლად აუცილებელია, რომ კომპანიამ შეარჩიოს სანდო და სერტიფიცირებული აუთსორსინგის პარტნიორები და გააფორმოს მკაფიო ხელშეკრულებები მონაცემთა დაცვის შესახებ.

ამავე თავში ყურადღება ეთმობა ბლოკჩეინის გენერაციის პროცესში წარმოშობილ ენერგეტიკულ ხარჯებს და მათ შემცირების შესაძლო სტრატეგიებს. ბლოკჩეინის გენერაცია, რომელიც გულისხმობს უტოლობის გადარჩევის მეთოდით ამოხსნას, მოითხოვს კომპიუტერის პროცესორის მაქსიმალურ ჩართულობას. ეს პროცესი იწვევს პროცესორის 100%-იან დატვირთვას, რაც ხელს უწყობს ენერგიის ინტენსიურ მოხმარებას და სითბოს გამოყოფას. სითბოს დროული არიდება მძლავრი გაგრილების სისტემებსა და გარემოს შესაბამის ტემპერატურას საჭიროებს, რაც კიდევ უფრო ზრდის ენერგეტიკულ ხარჯებს.

აღსანიშნავია ისიც, რომ დედამიწის ჩრდილოეთ და სამხრეთ ნახევარსფეროებში სეზონების ცვალებადობის გამო შესაძლებელია ბლოკჩეინის გენერატორების განთავსების ადგილის პერიოდული ცვლილება, რაც მთელი წლის განმავლობაში იაფი ელექტროენერგიის გამოყენების საშუალებას იძლევა. ამ

მიდგომას ემატება ის ფაქტი, რომ იაფი ელექტროენერგიის ტრანსპორტირება რთულია, მაშინ როცა ბლოკჩეინის ტრანსპორტირება ინტერნეტით მარტივად ხორციელდება.

მეოთხე თავის დასკვნაში ნათლად ჩანს, რომ ბლოკჩეინის აუთსორსინგი წარმოადგენს ეფექტიან სტრატეგიას იმ კომპანიებისთვის, რომლებსაც სურთ ბლოკჩეინის ტექნოლოგიის დანერგვა, მაგრამ არ აქვთ საკმარისი რესურსები ან ექსპერტიზა შიდა განვითარებისთვის. აუთსორსინგი უზრუნველყოფს ხარჯების ოპტიმიზაციას, ტექნიკური ცოდნის მიღებას და სისტემის მასშტაბირებადობას. მიუხედავად იმისა, რომ არსებობს უსაფრთხოების და კონფიდენციალურობის რისკები, სწორი პარტნიორის შერჩევისა და ხარისხის კონტროლის მექანიზმების დანერგვით ეს რისკები მინიმუმამდე დადის. ბლოკჩეინის სერვისების დივერსიფიცირებული მოდელების გამოყენება კომპანიებს საშუალებას აძლევს ეფექტურად მართონ დანახარჯები და მიაღწიონ მაღალი ხარისხის შედეგებს.

მეხუთე თავი განიხილავს ბლოკჩეინზე დაფუძნებული გადაწყვეტილებების დანერგვისთვის შემუშავებულ ბიზნეს მოდელს, რომელიც მიმართულია ორგანიზაციებში მონაცემთა სანდოობისა და უცვლელობის უზრუნველყოფაზე. ნაშრომის ფარგლებში ჩატარდა კვლევა სხვადასხვა სექტორში, მათ შორის **საავადმყოფოებსა და უნივერსიტეტებში**, რათა დადგენილიყო მონაცემთა დაცვის საჭიროებები.

შემოთავაზებული მოდელი ეყრდნობა **ბიზნეს მოდელ კანვასის (BMC)** სტრუქტურას, რომელიც მოიცავს მომხმარებელთა სეგმენტების, ღირებულების შეთავაზების, არხების, პარტნიორებისა და ხარჯების ანალიზს. მოდელი ორიენტირებულია მცირე და საშუალო ზომის კომპანიებზე, რომელთათვისაც ბლოკჩეინის სრული დანერგვა რთული და ძვირადღირებული პროცესია.

ბიზნეს მოდელი სთავაზობს ორ ძირითად სერვისს:

1. **ერთჯერადი ინტეგრაცია**, რომლის მოიცავს ერთჯერად კონფიგურაციას, სადაც ჩვენ ვუზრუნველყოფთ ბლოკჩეინის ტექნოლოგიის ინსტალაციას კლიენტის მონაცემთა სისტემაში, რაც საშუალებას აძლევს ორგანიზაციას დამოუკიდებლად მართოს იგი. ამ მოდელით ორგანიზაცია სრულად ინარჩუნებს მონაცემთა კონტროლს, რაც სასურველია

კონფიდენციალურობის მკაცრი მოთხოვნებისთვის. თუმცა, ორგანიზაციამ უნდა დაასაქმოს კვალიფიციური პერსონალი სისტემის შენარჩუნებისთვის, რაც დამატებით ხარჯებს მოითხოვს.

2. **გრძელვადიანი სერვის მოდელი**, რომელიც მოიცავს საწყის ინტეგრაციას და მუდმივ მართვას გამოწერის ხელშეკრულების საფუძველზე. ამ მოდელში ჩვენი გუნდი იღებს პასუხისმგებლობას სისტემის უსაფრთხოებაზე, განახლებებსა და რეგულატორულ კონტროლზე, რაც კლიენტისთვის უზრუნველყოფს სრულ სერვისს, რომელიც არ მოითხოვს შიდა ბლოკჩეინ ექსპერტიზას. მიუხედავად იმისა, რომ ამ მოდელს აქვს გამოწერის საფასური და მონაცემთა ბაზაზე დაშვების საჭიროება, ის მნიშვნელოვნად ამცირებს კლიენტის ოპერაციულ დატვირთვას.

კანვას ბიზნეს მოდელი შემოთავაზებული ბიზნეს მოდელისთვის.

ბიზნეს მოდელის მისი მიზანია ბლოკჩეინის ტექნოლოგია გახადოს ხელმისაწვდომი და პრაქტიკული ორგანიზაციებისთვის, რომლებიც ეძებენ სანდოობისა და უსაფრთხოების გაუმჯობესების გზებს მათი არსებული ინფრასტრუქტურის სრულად შეცვლის გარეშე.

დასკვნა

ტრადიციულ მონაცემთა ბაზებში სანდოობისა და უსაფრთხოების ნაკლებობა გახდა მთავარი საკითხი, რომელიც გამოიხატება მონაცემთა ბაზების ცენტრალიზებულ ხასიათში. განვიხილეთ, თუ როგორ მოქმედებს ეს პრობლემა სხვადასხვა სექტორში, როგორიცაა ჯანდაცვა, განათლება და ბუღალტერია. ასევე გავითვალისწინეთ, რომ არსებული სისტემები ვერ უზრუნველყოფენ მონაცემთა გამჭვირვალობას და უცვლელობას ისე, როგორც ამას თანამედროვე რეგულაციები და ორგანიზაციების მოთხოვნები ითხოვენ.

ჩატარებული კვლების შედეგად:

1. გამოვლინდა, რომ ჯანდაცვის, საბუღალტრო, საგანმანათლებლო და ბიზნეს სექტორებში განსაკუთრებით მნიშვნელოვანია ინფორმაციის სანდოობის საჭიროება.
2. დეტალურად განისაზღვრა ის პარამეტრები, რომლებიც აუცილებელია ინფორმაციის სანდოობისთვის სხვადასხვა ტიპის ორგანიზაციებში. მათ შორის უნიკალური ჰეშირების გამოყენება, მონაცემთა ცვლილებების ისტორიის და აუდიტის მექანიზმები, ავტორიზებული წვდომის კონტროლი, დროული განახლების უზრუნველყოფა, მონაცემთა კონსისტენტურობის და ხარისხის რეგულარული მონიტორინგი.
3. განისაზღვრა ალგორითმი, რომელიც გვაძლევს ბლოკჩეინის დამცავი მექანიზმის გამოყენების საშუალებას ცენტრალიზებულ მონაცემთა ბაზებში, რაც უზრუნველყოფს მონაცემთა სანდოობას და დაცულობას.
4. ბლოკჩეინის ტექნოლოგიის ინტეგრაციის მეთოდების გამოყენებით შევიმუშავეთ ბიზნეს მოდელი, რომელიც პასუხობს როგორც ტექნოლოგიურ, ასევე ბიზნეს საჭიროებებს. შემუშავებული მოდელი უზრუნველყობს მონაცემთა უცვლელობას და სანდოობას.
5. გამოვლინდა ის კომპონენტები (კანვას ბიზნეს მოდელი (BMC) და ლინ კანვასი (LC)), რომლებიც ეფექტურია ბაზრის შესწავლაში და ორგანიზაციული საჭიროებების სწორად გაანალიზებაში.

6. კვლევის შედეგად გამოიკვეთა სერვისის შეთავაზების სტრატეგია: ერთჯერადი ინტეგრაციის სერვისი და სააბონენტო მომსახურება.

   ერთჯერადი ინტეგრაციის სერვისის უპირატესობა მდგომარეობს იმაში, რომ ორგანიზაცია მხოლოდ საწყის საფასურს იხდის და შემდგომ თავად მართავს სისტემას. დადგინდა, რომ ეს სერვისი უფრო მიზნობრივია ორგანიზაციებისათვის, რომელთაც ჰყავთ კვალიფიციური კადრები და სურთ სისტემის სრული კონტროლი.

   სააბონენტო მომსახურება - მომხმარებლებს საშუალებას აძლევს, არ დაიქირაონ დამატებითი კადრები, რადგან სისტემის მოვლა და ტექნიკური მომსახურება სრულიად გადაეცემა სერვისის მომწოდებელს. კვლევებმა აჩვენა, რომ ამ ვარიანტს განსაკუთრებული უპირატესობა აქვს ისეთ ორგანიზაციებისთვის, რომლებიც ნაკლებად აპირებენ ტექნიკური რესურსების შექმნას.
7. შევქმენით სისტემა, რომლის საშუალებითაც შესაძლებელია ბლოკჩეინის მონაცემთა ბაზებთან ინტეგრაცია. სისტემაში გათვალისწინებულია მომხმარებლის მოთხოვნები და მარეგულირებელი სტანდარტები, რაც კიდევ უფრო ამყარებს ბიზნეს მოდელის სანდოობას და უსაფრთხოებას.
8. ბლოკჩეინის ტექნოლოგიის ინტეგრაციის გამოყენებით შევქმენით გლობალური და სტაბილური პლატფორმა, რომელიც უზრუნველყოფს მონაცემთა კონფიდენციალურობას, გამჭვირვალობას და უცვლელობას.
9. კვლევებმა დაადასტურა, რომ შემუშავებული მოდელი ეფექტურია ინფორმაციის სანდოობის უზრუნველსაყოფად ყველა იმ სფეროში, სადაც მონაცემთა სანდოობა და უცვლელობა პრიორიტეტია. ასეთი მიდგომა საშუალებას აძლევს სხვადასხვა ინდუსტრიას, გააუმჯობესონ მონაცემთა დაცვის ხარისხი და შესაბამისად გააძლიერონ მომხმარებელთა ნდობა.

გამოქვეყნებული ნაშრომების სია:

1. ბებიაშვილი ნ., ბერძენიშვილი თ., მეგრელიშვილი დ., თუთბერიძე თ. ბლოკჩეინ ტექნოლოგიების გავლენა საბანკო სექტორზე. აბრეშუმის გზის მე-17 დისტანციური საერთაშორისო კონფერენციის შრომების კრებული, თბილისი, საქართველო, 21-22 ოქტომბერი, 2022, გვ. 108-114.

2. ბებიაშვილი ნ., ბერძენიშვილი თ., თუთბერიძე თ. ბიზნესპროცესების სტრატეგიული მენეჯმენტის მოდელირებაში იტერაციული მიდგომების გამოყენება. აბრეშუმის გზის მე-16 დისტანციური საერთაშორისო კონფერენციის შრომების კრებული, თბილისი, საქართველო, 14-15 ოქტომბერი, 2021, გვ. 336-341.

3. თუთბერიძე თ., გრიგალაშვილი ა., ილურიძე ქ. „ინდუსტრია 4.0“-ის „ჭკვიან“ ქსელურ სისტემებში, ინოვაციური ტექნოლოგიების დანერგვისა და განვითარების პრობლემების მიმოხილვა. ჟურნალი „განათლება“, სტუ, 2020, N4(31), გვ. 248-252.

4. ბებიაშვილი ნ., ბერძენიშვილი თ., თუთბერიძე თ., ილურიძე ქ. ენერგეტიკული ბლოკჩეინპროექტების ინვესტიციური ლანდშაფტი. აბრეშუმის გზის მე-15 დისტანციური საერთაშორისო კონფერენციის შრომების კრებული, თბილისი, საქართველო, 09-10 ოქტომბერი, 2020, გვ. 148-152.

5. თუთბერიძე თ. პროექტების კომპიუტერული მართვის თანამედროვე მეთოდოლოგია „ეჯაილი“ და ტექნოლოგია „სქრამი“. აბრეშუმის გზის მე-15 დისტანციური საერთაშორისო კონფერენციის შრომების კრებული, თბილისი, საქართველო, 09-10 ოქტომბერი, 2020, გვ. 157-162.

6. სამადაშვილი ა., თუთბერიძე თ. ბლოკჩეინის პოტენციალი ბიზნეს პროცესების მართვაში. I საერთაშორისო სამეცნიერო-ტექნიკური კონფერენციის - „ენერგეტიკის თანამედროვე პრობლემები და მათი გადაწყვეტის გზები“ - შრომების კრებული. თბილისი, საქართველო, ”ენერგია”, 2019, №3(91), გვ. 102-104.

Abstract

In today's world, protecting data from tampering and making sure it's reliable are critical needs, especially in fields like finance, healthcare, and education. Many organizations rely on centralized databases, which are effective but don't offer built-in ways to prevent data changes or verify integrity. Blockchain, on the other hand, is well-known for providing tamper-proof records but is difficult and costly for many organizations to adopt fully. Our research aims to fill this gap by introducing a way to integrate blockchain's immutability features into existing centralized databases, allowing companies to improve data security and reliability without major changes to their current systems.

The core of our approach is a method that adds blockchain hashes to traditional databases. This method captures data in its current form and protects it from unauthorized changes. It works by creating unique cryptographic hashes for data stored in centralized databases, then recording these hashes on a blockchain. These hashes act like secure "fingerprints" for the data, allowing organizations to track and verify any changes. This setup enhances data integrity and helps organizations keep an unchangeable history of data changes while staying within their current systems and workflows.

Alongside our technical approach, we identified a business opportunity to provide this blockchain integration service to small and medium-sized companies. Many of these companies would benefit from the added security of blockchain but find full blockchain adoption too costly or complex. Using the "Business Model Canvas" approach, we created a business model for a company offering blockchain integration. This model includes two main services: a one-time integration service for organizations wanting a simple setup, and an ongoing service that provides continued maintenance and verification. This business model is specifically tailored for smaller companies that want enhanced data security without fully moving to blockchain.

Our analysis focuses on customer groups that depend on secure data, such as financial institutions, healthcare providers, and educational institutions. For example, in finance, this integration supports secure transaction records and helps prevent fraud. In healthcare, it creates an unchangeable history of patient records, supporting compliance and patient trust. Educational institutions could use it to secure student records, making them harder to tamper with and easier to verify.

In this paper, we explain the technical details of our approach, including how blockchain hashing works and the adjustments needed to add this to existing databases. Our model minimizes any extra time for data processing while maximizing security. By bringing blockchain benefits to centralized databases, we offer a hybrid model that combines the strengths of both systems and makes blockchain security accessible without a complete system overhaul.

As keeping data safe and trustworthy becomes more important, this hybrid model could help set new standards for protecting information. By combining the strengths of blockchain with current databases, this method could change how industries keep data secure, especially as laws about data protection get stricter. Beyond finance, healthcare, and education, this approach could be useful in areas like legal records, supply chains, and public records, where data needs to be open and protected from tampering.

This paper presents a practical and scalable solution for improving data integrity in existing centralized databases. By adding blockchain hashes to traditional systems, we offer an approach that combines the security of blockchain with the familiarity of centralized databases. Our business model outlines how this technology can be effectively marketed, especially in areas where secure data is a top priority.