1 ქვიზი

1. აღწერეთ სხვაობა web 2.0 და web3.0-ს შორის
   Web 2.0 ფოკუსირებულია კონტენტის შექმნაზე (დაწერაზე, და წაკითხვაზე) ამის მაგალითი კი სოციალური ქსელებია. რაც შეეხება web3.0 ფოკუსირებულაი დეცენტრალიზირებულ ქსელზე და არის სემანტიკური ქსელი, ის ასევე შეეხება წაკითხვას, დაწერას და ფლობას.

2. რომელი ნდობის მოდელს მიესადაგება ყველაზე მეტად სერთიფიკატებით გამყარებული არქიტექტურა? აღწერეთ მუშაობის პრინციპი.

   სერთიფიკატზე დაფუძნებული არქიტექტურა ყველაზე მეტად შეეფერება იერარქიულ ნდობის მოდელს. ნდობის ამ მოდელში ნდობა ორგანიზებულია იერარქიული წესით, ხის სტრუქტურის მსგავსი.

3. ჩამოთვალეთ და აღწერეთ ნდობის მოდელის შემდაგენელი ელემენტები

   აუთენტიფიკაცია - უნიკალური ვინაობის დადასტურება
   ავტორიზაცია - რაღაც კონკრეტული უფლებების მინიჭება
   კონფიდენციალურობა - ინფორმაცია არ იქნება გაზიარებული არაავტორიზებული მხარეებისადმი
   მონაცემების მთლიანობა - მონაცემები არ შეიცვლება არაავტორიზებული მხარის მიერ
   ხელმისაწვდომობა - ინფორმაცია ხელმისაწვდომია დროის ნებისმიერ მონაკვეთში

4. რა და რა პრინციპების მართვაში გვეხმარება სწორად დაგეგმილი სისტემები და აპლიკაციები.

   სწორად დაგეგმილი სისტემები და აპლიკაციები გვეხმარება ინფორმაციის ეფექტურად მართვაში. პრინციპები, რომლებიც ხელმძღვანელობს ამას, მოიცავს მასშტაბურობას, საიმედოობას, უსაფრთხოებას, გამოყენებადობას და შენარჩუნებას.

5. აღწერეთ როგორ მუშოაბს და რა სხვაობაა ასიმეტრიულ და სიმეტრიულ კრიპტოგრაფიას შორის.

   სიმეტრიული კრიპტოგრაფია იყენებს ერთ გასაღებს როგორც დაშიფვრისთვის, ასევე გაშიფვრისთვის. ხოლო ასიმეტრიული იყენებს ორი გასაღების public და private key. public გამოიყენება დასაშიფრად ხოლო private გასაშიფრად.

6. რა არის და რომელ ინდუსტრიულ რევოლუციას მიეკუთვენბა დიდი ზომის მონაცმეების დამუშავება? კიდევ რა პროცები შეიძლება ჩამოთვალოთ აღნიშნულ ინდუსტრიულ რევოლუციიდან?

   დიდი ზომის მონაცემების დამუშავება მიეკუთვენაბეა მეოთხე ხინდუსტრიულ რევოლუციას. ის მოიცავს დიდი და რთული მონაცემების შეგროვებას, შენახვას, ანალიზს და ინტერპრეტაციას. ასევე მეოთხე ინდუსტიურლი რევოლუციას ეკუთვნის

აუგმენტური რელობა, კიბერუსაფრთხოება, რობოტიკა, სიმულაციები, cloud computing და სხვა.

7. სად და რაში გამოიყენება დიფ-ჰელმანის მეთოდი?
   დიფ-ჰელმანის მეთოდი გამოყენება კრიპტოგრაფიაში კონკრეტულად იმისთვის რომ შეიქმანს საერთო საიდუმლო გასაღები ორ მხარეს შორის საკომუნიკაციოს რათა უზრუნველყოს უსადრთო კომუნიკაცია. ის გამოიყენაბ პროტოკოლებში მაგალიტად https და vpn

8. რა შეიძლება განვიხილო მეორე ინდუსტრიული რევოლუციის დაწყების ინდიკატორად?
   ელექტროობის გამოგონება და მისის გამოყენება სხვა და სხვა საწარმო პროცესებში თუ პროდუქტებში

9. ეთანხმები თუ არა რომ ბოლო ინდუსტრიული რევოლუცია წარმოიშვა თავისთავად და მასზე ზეგვალენა არ მოუხდენია წინა ინდუსტრიულ რევოლუციას? პასუხი დაასაბუთე.
   არ ვეთანხმები, ბოლო ინდუსტრიულ რევოლუციაზე გავლენა მოახდინა და დაფუძნებული იყო წინა ინდუსტრიული რევოლუციების წინსვლაზე. თითოეულმა ფაზამ საფუძველი ჩაუყარა ტექნოლოგიურ და ეკონომიკურ ცვლილებებს, რაც ხელს უწყობს ინდუსტრიალიზაციის საერთო პროგრესს.

10. რით განსხვავდება გაზიარებული მონაცემთა ბაზა სხვა ტიპის მონაცემთა ბაზებისგან და რა უპირატესობა აქვს ასეთ სისტემას?

    გაზიარებული მონაცემთა ბაზა, რომელიც ამოცანის იმპლემენტაციის გათვალისწინებით ხელმისაწვდომია ამ ქსელის ყველა მონაწილისათვის და აღნიშნული ბაზის ასლი ინახება თითოეულ მათგანთან.

    უპირატესობებში შედის რეალურ დროში განახლებები, მონაცემთა თანმიმდევრულობა და გამარტივებული კომუნიკაცია.

11. ეთანხმებით თუ არა ნდობის პირდაპირი მოდელი (Direct Trust) და ნდობის გარდამავალი მოდელი (Transitive Trust) მხარეების ვალიდაციას ერთნაირად ახორციელებს? პასუხი დაასაბუთეთ.
    რათქმაუნდა ეს ორი მოდელი ერთმანეთისგან განსხვავდება რადგან Direct Trust გულისცმოსბ პირდაპირ ნდობას მხარეებს შორის და მესამე მხარე ამ ნდობის პროესში ჩართული არ არის, ხოლო transitive trust მოდელის დროს ნდობა დამოკიდებულია რამდენიმე მხარეზე მაგალითად A ენდობა B-ს და B-ენდობა C-ს , მაშინ A ენდობა C-ს ანუ A-ს ნდობას C-ს მიმართ განსაზღვრავს B.

12. აღწერეთ რას წარმოადგენს web of trust ?
    Web of trust არის დეცენტარლიზებული კონცეფია რომელის დროსაც ერთი მხარე ირწმუნება სხვების დანდოობას და ავთენტურობას რომელიც საბოლოო ჯამში ქმნის სანდრო ურთიერთობის ქსელს.

13. რა უპირატესობები აქვს დისტანციურ სერვისებსა და რა მიმართულებით შეიძლება მათი დანრგვა?

    დისტანციური მომსახურების უპირატესობები:

    - **მოხერხებულობა და მოქნილობა:** კლიენტებს და თანამშრომლებს შეუძლიათ სერვისებზე წვდომა ნებისმიერი ადგილიდან, ნებისმიერ დროს.
    - **ხარჯების დაზოგვა:** ბიზნესს შეუძლია დაზოგოს ფული საოფისე ფართზე, მოგზაურობის ხარჯებზე და IT პერსონალზე.
    - **გაუმჯობესებული პროდუქტიულობა:** თანამშრომლები შეიძლება იყვნენ უფრო პროდუქტიულები, როდესაც მუშაობენ კომფორტულ და ნაცნობ გარემოში.
    - **ხელმისაწვდომობა ნიჭიერების ფართო აუზზე:** ბიზნესს შეუძლია თანამშრომლების დაქირავება მსოფლიოს ნებისმიერი ადგილიდან, ადგილმდებარეობის მიუხედავად.
    - **მომხმარებელთა კმაყოფილების გაზრდა:** მომხმარებლები აფასებენ სერვისებზე წვდომის მოხერხებულობას მოგზაურობის გარეშე.

    განხორციელების მიმართულებები:

    - დისტანციურად მუშაობა: მიეცით თანამშრომლებს დისტანციურად მუშაობის უფლება.
    - ვირტუალური თანამშრომლობის ინსტრუმენტები: გამოიყენეთ ინსტრუმენტები უწყვეტი კომუნიკაციისთვის.
    - ღრუბლოვანი სერვისები: ხელმისაწვდომობისთვის გადადით ღრუბელზე დაფუძნებულ სისტემებზე.
    - ელექტრონული სწავლება: გთავაზობთ დისტანციურ ტრენინგს და განათლებას.
    - ტელეჯანმრთელობა: უზრუნველყოთ ჯანდაცვის სერვისები დისტანციურად.
    - ელექტრონული კომერცია: განახორციელეთ ონლაინ ტრანზაქციები და სერვისები.
    - დისტანციური მხარდაჭერა: შესთავაზეთ მომხმარებლის მხარდაჭერა შორიდან.

2 ქვიზი

1. რას წარმოადგენს permissionless შეთანხმების პროცედურა?
   უნებართვო შეთანხმების პროცედურაში ნებისმიერ კვანძს შეუძლია მონაწილეობა უნებართვო შეთანხმების პროცედურები საშუალებას აძლევს ნებისმიერ კვანძს მონაწილეობა მიიღოს კონსენსუსის პროცესში წინასწარი თანხმობის გარეშე. ეს აუცილებელია მრავალი ბლოკჩეინის აპლიკაციისთვის, რადგან ის იძლევა უსაფრთხო და დეცენტრალიზებულ გადაწყვეტილების მიღების საშუალებას.

2. მოკლედ აღწერე ბიზანტიელი გენერლების პრობლემა.
   ბიზანტიელი გენერლების პრობლემა მოიცავს გენერლების ჯგუფს, რომელიც მეთაურობს არმიის სხვადასხვა დივიზიას, კოორდინაციას უწევს მათ თავდასხმას ან

უკან დახევას პოტენციურად მოღალატე გენერლების თანდასწრებით. გამოწვევაა სანდო კონსენსუსის ალგორითმის შემუშავება, რომელიც უზრუნველყოფს, რომ ყველა ლოიალური გენერალი თანხმდება საერთო გადაწყვეტილებაზე, მიუხედავად ზოგიერთი გენერლის მხრიდან გაუმართავი ან მატყუარა ინფორმაციის შესაძლებლობისა.

3. რა როლს ასრულებს SHA-256 ჰეშირების ფუნქცია ბლოკჩეინ სისტემებში? პასუხი დაასაბუთე
   SHA-256 (Secure Hash Algorithm 256-bit) გადამწყვეტ როლს ასრულებს ბლოკჩეინ სისტემებში, რადგან ის გამოიყენება უნიკალური, ფიქსირებული ზომის ჰეშის მნიშვნელობის შესაქმნელად მონაცემთა თითოეული ბლოკისთვის. ეს ჰეში უზრუნველყოფს მონაცემთა მთლიანობას, უცვლელობას, და უსაფრთხოებას. ის უზრუნველყოფს ბლოკების დაკავშირების მდგრად გზას, რაც ქმნის ბლოკჩეინის უსაფრთხოების ფუნდამენტურ მექანიზმს.

4. როგორ უნდა მოვიქცე, თუკი, მსურს, რომ მხოლოდ გარკვეულ დამდასტურებელთა წრეს ქონდეს ახალი ბლოკების წარმოების უფლება?

   გამოიყენეთ ნებადართული ბლოკჩეინი.

   ნებადართული ბლოკჩეინი არის ბლოკჩეინის ქსელი, რომელიც ხელმისაწვდომია მხოლოდ წინასწარ დამტკიცებული მონაწილეთა ნაკრებისთვის. ეს ნიშნავს, რომ თქვენ შეგიძლიათ აკონტროლოთ ვის აქვს ტრანზაქციების ვალიდაციის და ახალი ბლოკების წარმოების უფლება. ეს არის განსხვავებით საჯარო ბლოკჩეინებისგან, რომლებიც ღიაა ყველასთვის.

   მეორე პასუხი

   იმისათვის, რომ შეზღუდოთ ბლოკის წარმოება ვალიდატორების კონკრეტულ წრეზე, განახორციელეთ ნებადართული კონსენსუსის ალგორითმი ან გამოიყენეთ ნებადართული ბლოკჩეინის ჩარჩო. ეს ჩვეულებრივ გულისხმობს ვალიდატორების წინასწარ განსაზღვრულ სიის შექმნას ბლოკების წარმოების ექსკლუზიური უფლებებით.

5. რა შემთხვევაში შეიძლება არ დამჭირდეს ბლოკჩეინის სისტემაში წაკითხვის უფლება?
   შეიძლება არ დაგჭირდეთ წაკითხვის წვდომა ბლოკჩეინ სისტემაზე, თუ თქვენ აპირებთ მხოლოდ ტრანზაქციების წარდგენას ან მოქმედებების შესრულებას, რომლებიც არ საჭიროებს ბლოკჩეინიდან მონაცემების მოთხოვნას ან მოძიებას.

6. რომელი შეთანხმების მოდელის დროს შეიძლება წარმოიშვას ცენტრალიზებულობის პრობლემა?
   ცენტალიზაციის პრობელმა შეიძება წამრმოიშვას proof of work და proof of stake -ის დროს
7. რა პრობლემის წინაშე შეიძლება აღმოჩნდეს მუშაობის დადასტურების შეთანხმების მოდელი?

Proof of work საჭიროებს მაინინგის პროცეს რაც მოითხოვს ძალიან დიდი რაოდენობთ ენერგიას. ანუ ასეტი მოდელი არ არის ენერგო ეფექტური და მთავარი პრობლემაც ამაში მდომარეობს.

ცენტრალიზაციის პრობლემა შეიძლება წარმოიშვას ბლოკჩეინში, როგორც Proof of Work (PoW) ასევე Proof of Stake (PoS) შეთანხმების მოდელების მიხედვით. PoW-ში მაინინგის სიმძლავრის კონცენტრაცია შეიძლება მოხდეს, ხოლო PoS-ში მონაწილეთა მცირე რაოდენობამ, რომლებიც ფლობენ კრიპტოვალუტის მნიშვნელოვან რაოდენობას, შეიძლება გამოიწვიოს ცენტრალიზებული კონტროლი.

8. რას ნიშნავს შეთანხმების პროტოკოლში სიცოცხლისუნარიაობა?

   სისტემა მუშაობას განაგრძობს ქსელის მონაწილე ერთრდოულად რამოდენიმე კვანძის ჩავარდნის შემდეგაც.

9. ჩამოთვალე და აღწერე, რა და რა ელემენტების გამოყენებით აღწევს ბლოკჩეინის სისტემა დაცულობის მაღალ დონეს?
   დეცენტრალიზაციის, რაც გულისხმობს იმას რომ ყველა კვანძს აქვს უფლება ნახოს მონაცმეები.
   ასევე კრიპტოგრაფიის, ძლიერი კრიპტოგრაფიული ტექნიკა გამოიყენება ტრანზაქციების დასაცავად და ახალი ბლოკების შექმნის გასაკონტროლებლად.
   ელემენტი: საჯარო და კერძო გასაღების წყვილი, ჰეშის ფუნქციები.
   ჭკვიანი კონტრაქტები, კონტრაქტები წინასწარ განსაზღვრული წესებით, აძლიერებს ტრანზაქციების ავტომატიზაციას და უსაფრთხოებას.

10. ბლოკჩეინ სისტემების დაყოფა მონაცემებზე წვდომის მხრივ მოვახდინეთ სამ კატეგორიად. ჩამოთვალე და აღწერე მათ შორის სხვაობა.

    ღია ბლოკჩენის დროს შეტანხმების პროცედურა ღიაა შესაბამისად ყველა იღებს შეთანხმების პროცესში მონაწილეობას. ასეთ დროს ცენტარლიზებულობა არ არის.

    კონსორტიუმის დროს შეთანხმების პროცედურა ნების დართვით არის, პროცესში მონაწილეობას წინასწარ შეთანხმებული კვანძები იღებენ, ასეთ დროს ცენტრალიზებულობა ანწილობრივარის და წაკითხვის უფლება ღიაა ან შეზღუდულია.

    დახურული ბლოკშცენის დროს შეთანხმების პროცესში მონაწილეობს ერთი ორგანიზაცია, შესაბამისად წაკითხვის უფლება ძირითადად შეზღუდულია და ცენტრალიზებულია.

11. რომელი კონცეფცია შეიმუშავეს ჯერ კიდევ 1991 წელს? აღწერე მისი მუშაობის პრინციპი.
    1991 წელს მსოფლიო ქსელის (WWW) კონცეფცია შეიმუშავა ტიმ ბერნერს-ლიმ. WWW არის სისტემა, რომელიც საშუალებას აძლევს დოკუმენტებსა და რესურსებს

დაუკავშირდეს ჰიპერტექსტის საშუალებით, შექმნას ურთიერთდაკავშირებული ინფორმაციის ქსელი. ის მუშაობს ერთიანი რესურსების გამოყენების პრინციპზე, რათა იდენტიფიცირება და წვდომა იქონიოს ვებ სერვერებზე განთავსებული კონტენტზე, რაც ინფორმაციის ადვილად მისაწვდომს და ნავიგაციას ხდის ვებ ბრაუზერებში.

12. **ეთანხმები, თუ არა, რომ ბლოკჩეინ სისტემაში ქსელის მონაწილეთა შეთანხმების ალგორითმი მნიშვნელოვან როლს თამაშობს? პასუხი დაასაბუთე.**
ვეთანხმები, რომ ქსელის მონაწილეთა კონსენსუსის ალგორითმი გადამწყვეტია ბლოკჩეინ სისტემაში. ეს არის მექანიზმი, რომელიც საშუალებას აძლევს კვანძებს შეთანხმდნენ ტრანზაქციების მართებულობაზე და ბლოკების რიგითობაზე. ამით მიიღწევა ნდობა, უსაფრთხოება და დეცენტრალიზაცია. სხვადასხვა ალგორითმები, როგორიცაა Proof of Work და Proof of Stake, განსაზღვრავს, თუ როგორ მიიღწევა კონსენსუსი, რაც გავლენას ახდენს სისტემის მუშაობაზე.

3 ქვიზი

1. ჩამოთვალე ცივი ტიპის საფულის ძირითადი ქვეტიპები, დაახასიათე ისინი.
ცივი ტიპის საფულე არის კოპტოვალუტის საფულე რომელიც არ არი დაკავშირებული ინტერნეტთან.
ამის მაგალითებია:
აპარატურის საფულე ან ქაღალდის საფულე

2. ჩამოთვალე სამი „საუკეთესო პრაქტიკა “, როგორ უნდა მოვქცეთ იმისათვის, რომ ჩვენი საფულე მეტად იყოს დაცული არასასურველი შემთხვევებისგან?

   დავაყენოთ ძლიერი პაროლი და ხშირად შევცვალოთ ის, ჩავრთოთ 2-ფაქტორიანი აუთენთიფიკაცია და ვიქონიოთ რამდენიმე საფულე და ანგარიშები.

3. რას შეიძლება მივაკუთვნოთ BTC, ETH, SOL, ADA, BNB?
ყველა ჩამოთვლილი არის კრიპტო ვალუტა ბლოკჩენის ეკოსისტემაში.

4. რა დადებითი/უარყოფი მხარეები აქვს მობილური ტიპის საფულეს?
დადებითი მხარეები: მოსახერხებელი, UI-ს საშუალებით მარტივია გამოყენება გამარტივებული ტრანზაქციის განხორციელება.

   უარყოფითი მხარეები: ნაკები უსაფრთხოება შესაძლოა მობილური დაიკაროს ან ვინმემ მოგპაროს. დამოკიდებული ხარ დივაისზე თუ ის მწყობრიდან გამოვიდა შესაძლოა საფულეც დაკარგო.

5. რას წარმოადგენს თოქენის სრული მარაგი?
თოქენის სრული მარაგი არის თოქენები რომლებიც ჩაშვებულია ბრუნვაში და ამავდროულად ისეთი თოქენები რომლებიც ჩაკეტილია ან რეზერვირებულია

6. რისთვის არსებობს ბლოკჩეინ საფულეში ანგარიშები?
   არსებობს იმისთვის რომ ცალ-ცალკე იყოს აქვივები და არ დაგვჭირდეს ამისთვის სხვა და სხვა საფულეების შექმნა.

7. რა განსხვავებაა კრიპტოვალუტასა და კრიპტოთოქენს შორის?
   თოქენი არის პროექტების შექმნილი ციფრულიაქტივი, მას იყენებნე ტრანზაქციებისთვის დაასევე ხელმოწერებისთვის. თოქენები მუშაობენ უკვე არსებულ ბლოკჩეინებში.
   ქოინი არის ეგრედწოდებული ციფრული ფული რომელიც ძირითადად გამოიყენება გადახდებში. ისნი მუშაობენ საკუთარი პროტოკოლით საკუთარ ბლოკჩეინში.

8. განავრცე აზრი: ცვლადი თოქენი (Fungible Token) არის ციფრული აქტივი, რომელიც ...
   მოიყვანე ასეთი თოქენის მაგალითი.
   მის მსგავს აქვივი შეიძლება გაიცვალოს. ამის მაგალითია ბიტკოინი ან ეთერიუმი

9. ეთანხმები, რომ ცხელი ტიპის საფულის შემთხვევაში აქცენტი თანხის რაოდენობაზე კეთდება? პასუხი დაასაბუთე.
   არ ვეთანხმები რადგან ძირიტადი აქცენტი ხელმისაწვდომაობაზე კეთდება

10. რა განსხვავებაა Layer 1 და Layer 2 თოქენს შორის?
    Layer 1 ძირითადად წარმოადგეს სხვადასხვა ტიპის ტრანზაქციებს
    Layer 2 კი წარმადგენს დეცენტრალიზებული აპლიკაციების.

ჯიოს ქვიზები

1. რას წარმოადგენს md5 და sha256 და სად შეიძლება გამოგვადგეს ბლოკჩეინში? (0.5)

   md5 არის კრიპტოგრაფიული ჰეშის ფუნქცია რომელიც მიდრეკილია დაუცველობისკენ და არ არის შესაფერისი ბლოკჩეინის უსაფრთხოებისთვის ხოლო sha256 არის უსაფრთხო ჰეშის ფუნქცია რომელიც ფართოდ გამოიყენება ბლოკჩეინში მონაცემთა მთლიანობის გადამოწმებისა და მაინინგის პროცესებისთვის

2. აღწერე, რომელი კონცეფცია შეიმუშავეს ჯერ კიდევ 1991 წელს ბლოკჩეინთან მიმართებაში? (0.5)

   1991 წელს ს. ჰაბერმა და ვ. სტორნეტმა შეიმუშავეს ბლოკების კრიპტოგრაფიულად დაცული ჯაჭვის კონცეფცია რომელიც წარმოადგენს თანამედროვე ბლოკჩეინის ტექნოლოგიის წინამორბედს დოკუმენტების დროის შტამპირებისა და უცვლელობის უზრუნველსაყოფად

3. ჩამოთვალე და აღწერე ბლოკის ძირითადი თვისებები. (0.5)

   1.კრიპტოგრაფიული ჰეში,თითოეულ ბლოკს აქვს უნიკალური ციფრული თითის ანაბეჭდი რაც ცხადყოფს მას და ადასტურებს ჯაჭვის მთლიანობას
   2.დროის შტამპი,ბლოკები მონიშნულია დროის მითითებით რაც იძლევა

ქრონოლოგიური მონაცემების ორგანიზებას
3.მითითება წინა ბლოკზე,ბლოკები მიუთითებს წინა ბლოკის ჰეშზე ქმნიან დაკავშირებულ ჯაჭვს უსაფრთხოებისთვის
4.უცვლელობა,როდესაც მონაცემები დაემატება ბლოკს, მისი შეცვლა თითქმის შეუძლებელია რაც უზრუნველყოფს მონაცემთა მთლიანობას და ნდობას.

4. ეთანხმები, თუ არა, რომ ნებისმიერი არაავტორიზებული ცვლილება ბლოკში იწვევს მომდევნო ბლოკების ვალიდურობის ანულირებას? პასუხი დაასაბუთე. (0.5)

   დიახ ბლოკში არაავტორიზებული ცვლილებები არღვევს შემდგომ ბლოკებს, რადგან თითოეული ბლოკის კრიპტოგრაფიული ჰეში ეფუძნება ბლოკში არსებულ მონაცემებს და წინა ბლოკის ჰეშს, რაც ქმნის დამოკიდებულებების ჯაჭვს.თუ ერთი ბლოკი შეიცვლება ეს გამოიწვევს შეუსაბამობას მომდევნო ბლოკთან რაც არღვევს ჯაჭვის მთლიანობას

5. აღწერე, რას წარმოადგენს DLT და რა განასხვავებს მას სხვა სისტემებისგან? (0.5)

   DLT არის დეცენტრალიზებული ციფრული სისტემა ტრანზაქციების ჩაწერისა და გადამოწმებისთვის.რაც განასხვავებს მას არის მისი დეცენტრალიზებულობა და გამჭვირვალეობა.ის ამცირებს შუამავლებს,რაც აძლიერებს ნდობას და უსაფრთხოებას

6. რა სხვაობაა ღია და კონსორტიუმის ტიპის ბლოკჩეინ სისტემებს შორის? (0.5)

   ღია ბლოკჩეინები არის საჯარო და არ ჭირდება ნებართვა რაც საშუალებას აძლევს ნებისმიერს მიიღოს და შევიდეს ქსელში მაგალითად ბიტკოინი.კონსორციუმის ბლოკჩეინები ნახევრად კერძოა და ნებადართულია,შეზღუდული მომხმარებლებით, რომლებიც აკონტროლებენ წვდომას

7. როგორ უნდა მოვიქცე, თუ არ მინდა, რომ ჩემი ბლოკჩეინის ტრანზაქციების შესახებ ინფორმაცია ყველასთვის იყოს ხელმისაწვდომი? (0.5)

   ბლოკჩეინის ტრანზაქციის ინფორმაციის კონფიდენციალურობისთვის უნდა გამოვიყენოთ კონფიდენციალურობაზე ორიენტირებული კრიპტოვალუტები ან ბლოკჩეინის ქსელები რომლებიც შექმნილია კონფიდენციალური ტრანზაქციებისთვის

8. მოკლედ აღწერე შეთანხმების პროტოკოლის ძირითადი პარამეტრები. (0.5)

   შეთანხმების პროტოკოლის ძირითადი პარამეტრები მოიცავს მონაწილე მხარეებს, კონსენსუსის მექანიზმს ან წესებს,რათა ქმედებები იყოს ვალიდური და აღრიცხული

9. აღწერე ბიზანტიელი გენერლების პრობლემა. (1)

   ბიზანტიელი გენერლების პრობლემა არის პრობლემა სადაც კვანძები უნდა იყვნენ კოორდინირებული, რათა მიაღწიონ კონსენსუსს მიუხედავად არასანდო ან მავნე მონაწილეების არსებობისა. ეს არის იმის უზრუნველყოფა სადაც ქსელის ყველა კვანძი თანხმდება ერთ თანმიმდევრულ მდგომარეობაზე მაშინაც კი როდესაც ზოგიერთმა კვანძმა შეიძლება გაუგზავნოს კონფლიქტური ინფორმაცია ან იმოქმედოს მავნედ

10. ჩამოთვალე ორი განსხვავებული შეთანხმების მოდელი, აღწერე მათ შორის სხვაობა. (1)

    მუშაობისს დადასტურება PoW ეყრდნობა მაინერებს, რომლებიც წყვეტენ რთულ მათემატიკური თავსატეხებს ტრანზაქციების დასადასტურებლად და რომელიც გადაჭრის მას შემდეგ ბლოკს უმატებს და გამოიყენება ბიტკოინში

    აქტივების დადასტურება PoS ამოწმებს ტრანზაქციების მონაწილეთა მიერ შენახულ კრიპტოვალუტას.ის გამოიყენება ისეთი ქსელების მიერ, როგორიცაა Ethereum 2.0, რაც ამცირებს ინტენსიური გამოთვლებს

11. რა შემთხვევაში შეიძლება არ დამჭირდეს ბლოკჩეინის სისტემაში ჩაწერის უფლება? (0.5)

    საჯარო ბლოკჩეინში როგორიცაა ბიტკოინი სადაც ყველას შეუძლია გააკეთოს ტრანზაქციები ბლოკჩეინზე ნებართვის მოთხოვნის გარეშე თუ დაიცავენ ქსელის წესებს და პროტოკოლებს

12. რომელ სისტემაში გამოიყენება PBFT შეთანხმების მოდელი და რა განასხვავებს მას სხვა შეთანხმების მოდელებისგან? (1)

    PBFT ანუ პრაქტიკული ბიზანტიურ ჩავარდნებზე მედეგობა არის შეთანხმების მოდელი რომელიც გამოიყენება ნებადართული ბლოკჩეინის სისტემებში და ცნობილია თავისი ეფექტურობითა და უნარით რომ მიაღწიოს კონსენსუსს კვანძების უფრო მცირე რაოდენობით მაშინაც კი როდესაც ზოგიერთმა კვანძმა შეიძლება გაუგზავნოს კონფლიქტური ინფორმაცია ან იმოქმედოს მავნედ

13. რისი თვისებებია ანონიმურობა, უცვლელობა, პროგრამირებადობა, დისტრიბუციულობა? (0.5)

    ესენია გაზიარებული მონაცემთა დაცვის თვისებები DLT
    ანონიმურობა,ბევრ ბლოკჩეინის ქსელის მომხმარებლებს საშუალებას აძლევს მონაწილეობა მიიღონ თავიანთი რეალურ ვინაობის გამჟღავნების გარეშე
    უცვლელობა,ბლოკჩეინი უზრუნველყოფს რომ მონაცემების ჩაწერის შემდეგ მისი შეცვლა თითქმის შეუძლებელი იყოს
    პროგრამირებადობა, ჭკვიანი კონტრაქტები, რომლები ამცირებს შუამავლების საჭიროებას
    დისტრიბუციულობა: ბლოკჩეინი მუშაობს კვანძების დეცენტრალიზებულ ქსელზე, რომლებიც ერთად მუშაობენ კონსენსუსის მისაღწევად სრული გამჭირვალეობისთვის

14. აღწერე ცვლად (Fungible) და უცვლად (Non-Fungible) თოქენებს შორის სხვაობა. (1)
    ცვლადი ტოქენები არის ციფრული აქტივი, რომელიც შეიძლება გადაიცვალოს მისსავე მსგავ აქტივში,ხოლო უცვლადი ტოქენები არის უნიკალური ციფრული აქტივი, რომელიც არ იცვლება მისსავე მსგავს აქტივში.

15. „ბრაუზერისთვის, მობილურისთვის, დესკტოპ-აპლიკაციისვის“ - რაზეა საუბარი? (0.5)
    საუბარია ცხელ საფულეზე რომელიც განკუთვნილია ბრაუზერისთვის, მობილურისთვის, დესკტოპ-აპლიკაციისვის.

16. რა განსხვავებაა Layer 1 და Layer 2 თოქენს შორის? (0.5)
    Layer 1 არის ინვესტირება, შენახვა, ყიდვა-გაყიდვა და ტრანზაქციები,
    ხოლო Layer 2 არის დეცენტრალიზებული აპლიკაციები, საწყისი ქსელის შესაძლებლობების დახვეწა.

17. ეთანხმები, რომ ცივი ტიპის საფულის შემთხვევაში აქცენტი შეთანხმების ალგორითმზე კეთდება? პასუხი დაასაბუთე. (0.5)
    არა რადგან ცივი ტიპის საფულის შემთხვევაში, აქცენტი კეთდება არა შეთანხმების ალგორითმზე, არამედ ოფლაინში პირადი გასაღებების უსაფრთხოდ შენახვაზე, რათა დაიცვას კრიპტოვალუტები ონლაინ საფრთხეებისგან.

18. თუკი მე ხშირად ვაწარმოებ ტრანზაქციებს, რომელი ტიპის კრიპტოსაფულე გამომადგება და რატომ? (0.5)
    ხშირი ტრანზაქციებისთვის საუკეთესოა ცხელი საფულე, როგორიცაა მობილური ან ვებ საფულე, რადგან ის გვტავაზობს მარტივ წვდომას. ცივი საფულეები უფრო უსაფრთხოა, მაგრამ ნაკლებად მოსახერხებელი ხშირი გამოყენებისთვის.

19. ეთანხმები მოსაზრებას, რომ კრიპტოვალუტები ძირითადად არსებულ ბლოკჩეინებში მუშაობენ? პასუხი დაასაბუთე. (0.5)
    დიახ, კრიპტოვალუტები ძირითადად მოქმედებენ ბლოკჩეინის ქსელებში, რადგან ბლოკჩეინი უზრუნველყოფენ საფუძვლიან ტექნოლოგიას უსაფრთხო, დეცენტრალიზებული და გამჭვირვალე ტრანზაქციებისთვის. კრიპტოვალუტები დამოკიდებულია ბლოკჩეინზე ტრანზაქციების ჩასაწერად და გადამოწმებისთვის.

20. ეთანხმები მოსაზრებას, რომ საფულეებში 12/24 სიტყვიანი აღდგენის ფრაზა ბლოკების დასადასტურებლად გამოიყენება? პასუხი დაასაბუთე. (1)
    კი რადგან ის აუცილებელია საფულის აღდგენისთვის და ემსახურება როგორც სარეზერვო მექანიზმს პირადი გასაღებების აღსადგენად. ის უზრუნველყოფს საფულეზე წვდომას მოწყობილობის დაკარგვის ან გაუმართაობის შემთხვევაში.

21. რას შეიძლება მივაკუთვნოთ USDT, Cake, AXS, SHIB? (0.5)
    USDT, Cake, AXS, SHIB უნდა მივაკუთვნოთ ბლოკჩეინს რომელიც არის ციფრული აქტივი.

22. რა უპირატესობა აქვს ვებ-ბრაუზერის საფულეს ქაღალდის საფულესთან შედარებით? (0.5)
    მოხერხებულობა: ვებ ბრაუზერის საფულეები უფრო მოსახერხებელია მომხმარებლისთვის რადგან თავაზობს მარტივ წვდომას ტრანზაქციებზე, ვიდრე ქაღალდის საფულეები.ასევე ხელმისაწვდომობა: ვებ ბრაუზერის საფულეები საშუალებას გვაძლევს ვმართოთ ჩვენი კრიპტოვალუტები ინტერნეტთან დაკავშირებული ნებისმიერი მოწყობილობიდან, ხოლო ქაღალდის საფულეები ფიზიკურია და შეიძლება დაიკარგოს ან დაზიანდეს.

23. თუკი მაქვს საფულე რომელიმე ერთი ქსელის ანგარიშით. შემიძლია, თუ არა, იმავე საფულეში ვიქონიო სხვა ანგარიში, სხვა ქსელით? პასუხი დაასაბუთე. (1)
    კი სხვადასხვა ქსელში ერთსა და იმავე საფულეში მრავალი ანგარიშის არსებობამ შეიძლება უზრუნველყოს თავსებადობის სარგებელი, მაგრამ ასევე შეიძლება გაზარდოს სირთულე და ტრანზაქციის ხარჯები.

24. როგორ განისაზღვრება თოქენის მაქსიმალური მარაგი? (0.5)
    ტოკენის მაქსიმალური მიწოდება განისაზღვრება პროტოკოლით, წინასწარ განსაზღვრული ლიმიტით ან გაცემის განრიგით, რომელიც დადგენილია ტოქენის შექმნისას ანუ ყველა ის თოქენი, რომელიც ოდესმე შეიძლება აწარმოონ.

25. აღწერე თოქენის დეფლაციური მოდელი. (0.5)
    დეფლაციური ტოკენის მოდელი შექმნილია იმისათვის, რომ შეამციროს მისი მთლიანი მიწოდება დროთა განმავლობაში ისეთი მექანიზმებით, როგორიცაა ტოქენების მიმოქცევიდან ამოღება, რაც პოტენციურად გაზრდის თითოეული დარჩენილი ტოკენის ღირებულებას დეფიციტის გამო.

26. ბიტკოინის ბლოკჩეინ სისტემა ინფლაციურია, თუ დეფლაციური? ახსენი მიზეზი. (0.5)
    ბიტკოინის ბლოკჩეინი დეფლაციურია, რადგან მისი მიწოდება შემოიფარგლება 21 მილიონი მონეტით, ხოლო ახალი მონეტები იქმნება კლებადი ტემპით, რაც მას დროთა განმავლობაში მწირს ხდის.

ირინას ქვიზები

რა არის ჰეშირება და რისთვის გამოიყენება ის ბლოკჩეინში? (0.5)

ბლოკჩეინში ჰეშირება არის კრიპტოგრაფიული ალგორითმის გამოყენებით მონაცემების ,უნიკალური სიმბოლოების სტრიქონად გადაქცევის პროცესი. ჰეშირება გამოიყენება მონაცემთა მთლიანობის დასაცავად და ბლოკჩეინში ტრანზაქციების შესამოწმებლად.

რომელი კონცეფცია შეიმუშავეს ჯერ კიდევ 1991 წელს? აღწერე მისი მუშაობის პრინციპი. (1)

1991 წელს შეიმუშავეს კრიპტოგრაფიულად დაცული ბლოკების ჯაჭვის კონცეფცია რომელიც წარმოადგენს თანამედროვე ბლოკჩეინის ტექნოლოგიის წინამორბედს დოკუმენტების დროის შტამპირებისა და უცვლელობის უზრუნველსაყოფად

რა არის გენეზისის ბლოკი და რით არის უნიკალური? (0.5)

Genesis Block არის პირველი ბლოკი ბლოკჩეინში და რაც მას უნიკალურს ხდის არის ის, რომ მას არ აქვს მშობელი ბლოკი, მას აქვს განსაკუთრებული მახასიათებლები და მას აქვს ისტორიული მნიშვნელობა, როგორც ბლოკჩეინის საწყისი წერტილი.

როგორ ხდება ბლოკჩეინში არავალიდური ბლოკის გამოვლენა? (0.5)

არასწორი ბლოკები ბლოკჩეინში აღმოჩენილია, როდესაც ისინი ვერ აკმაყოფილებენ კონსენსუსის წესებს და ქსელის მიერ დადგენილ ვალიდაციის კრიტერიუმებს, რაც იწვევს კვანძების უარყოფას ბლოკის ჯაჭვში ჩართვას.

რას წარმოადგენს permissionless შეთანხმების პროცედურა? (0.5)

permissionless შეთანხმების პროცედურა არის დეცენტრალიზებული მექანიზმი, რომელიც საშუალებას აძლევს მონაწილეებს მიაღწიონ კონსენსუსს ან შეთანხმებას ცენტრალური ხელისუფლებისგან ნებართვის მოთხოვნის გარეშე. ის საშუალებას აძლევს ღია და საჯარო მონაწილეობას, როგორც წესი, იყენებს ორ შეთანხმების მოდელს, ესენია სამუშაოს დადასტურება (Proof of Work) და ფსონის დადასტურება (Proof of Stake).

ჩამოთვალე და აღწერე DL T-ს სამი მახასიათებელი თვისება. (0.5)

DLT-ის სამი მახასიათებელი თვისებაა:

დეცენტრალიზაცია- DLT მუშაობს განაწილებული კვანძების ქსელზე, თითოეული ჩანაწერის ასლს. ეს დეცენტრალიზებული სტრუქტურა გამორიცხავს ცენტრალური ხელისუფლების აუცილებლობას, რაც მას ხდის უფრო საიმედოს, რადგან ამცირებს მანიპულირების რისკს.

შეუცვლელი ჩანაწერი - მას შემდეგ, რაც ტრანზაქციის ისტორია დაემატება ჩანაწერებს , ძალიან რთულია მისი შეცვლა ან წაშლა. ეს უცვლელობა მიიღწევა კრიპტოგრაფიული ტექნიკის საშუალებით, როგორიცაა ჰეშირებისა და კონსენსუსის მექანიზმები.

გამჭვირვალობა და ნდობა: DLT უზრუნველყოფს გამჭვირვალობას, რადგან ქსელში ჩართულ მონაწილეებს შეუძლიათ ნახონ მთელი ტრანზაქციის ისტორია.

რა სხვაობაა კონსორტიუმის და დახურული ტიპის ბლოკჩეინ სისტემებს შორის? (0.5)

კონსორციუმის ბლოკჩეინები მოიცავს სანდო სუბიექტების ჯგუფს, რომლებიც თანამშრომლობენ საერთო ბლოკჩეინზე, ხოლო დახურულ ბლოკჩეინს აკონტროლებს

ერთი სუბიექტი ან მონაწილეთა ძალიან შეზღუდული ნაკრები, ხშირად შიდა მიზნებისთვის.

რას ნიშნავს შეთანხმების პროტოკოლში ჩავარდნების მიმართ მედეგობა? (0.5)

შეთანხმების პროტოკოლში შეცდომებზე რეაგირება ნიშნავს, რომ სისტემას შეუძლია აღმოაჩინოს და მოერგოს მოულოდნელ საკითხებს ან შეცდომებს მონაწილეთა შორის კონსენსუსის ან შეთანხმების მიღწევის პროცესში. ეს პასუხისმგებლობა ხელს უწყობს პროტოკოლის მთლიანობისა და სანდოობის შენარჩუნებას.

აღწერე, PoET შეთანხმების მოდელი და მოიყვანე შესაბამისი მაგალითი. (1)

PoET (Proof of Lapsed Time) არის შეთანხმების მოდელი, სადაც მონაწილეები ეჯიბრებიან კრიპტოგრაფიული თავსატეხის ამოხსნაში. ვინც პირველი დაასრულებს, იღებს ჯერ ლოდინის პერიოდს და შემდეგ ამატებს ახალ ბლოკს ჯაჭვს.ეს უზრუნველყოფს, რომ პროცესი იყოს შემთხვევითი და სამართლიანი, ენერგიის ინტენსიური გამოყენების გარეშე, რომელიც საჭიროა Proof of Work (PoW) კრიპტოვალუტაში, როგორიცაა Bitcoin.

რა შემთხვევაში შეიძლება გასცემდეს განსხვავებულ ბრძანებებს რომელიმე ქსელური კვანძი? სად გვხვდება მსგავსი პრობლემა? (0.5)

მსგავსი პრობლემა შეიძლება აღმოჩნდეს განაწილებულ სისტემებში და Peer-to-peer ქსელებში, სადაც მრავალ მონაწილეს შეუძლია დამოუკიდებლად წარადგინოს ქმედებები ან მონაცემები, რაც პოტენციურად გამოიწვევს კონფლიქტურ ან არაავტორიზებულ ქმედებებს, თუ სათანადოდ არ იმართება ან რეგულირდება.

რა ძირითადი სხვაობაა PoS და PoW შეთანხმების მოდელებს შორის? მოიყვანე ასეთი სისტემების მაგალითები. (1)

მთავარი განსხვავება ისაა, თუ როგორ მიაღწევენ კონსენსუსს:
PoW (Proof of Work) ეყრდნობა გამოთვლით მუშაობას (მაინინგს) ბლოკჩეინში ბლოკების დასადასტურებლად და დასამატებლად (მაგ., ბიტკოინი).

PoS (ფსონის დამადასტურებელი საბუთი) ამოწმებს და ქმნის ბლოკებს კრიპტოვალუტის ოდენობის საფუძველზე (მაგ., Ethereum 2.0).

რატომ შეიძლება დაგვჭირდეს რომელიმე ტიპის ბლოკჩეინ სისტემაში მასში მონაწილეების შესახებ ინფორმაციის გაგება? (0.5)

ბლოკჩეინის სისტემაში მონაწილეთა შესახებ ინფორმაციის გაგება გადამწყვეტია ნდობის დასამყარებლად, ანგარიშვალდებულების უზრუნველსაყოფად, მმართველობის გასააქტიურებლად, ნებართვების მართვისა(მონაწილისათვის წვდომის მინიჭების ან შეზღუდვისთვის) და კონფლიქტების მოსაგვარებლად.

რა შემთხვევაში შეიძლება არ დამჭირდეს ბლოკჩეინის სისტემაში წაკითხვის უფლება? (0.5)

იმ შემთხვევაში, თუ მონაცემები და ტრანზაქციები არის საჯარო ,სრულიად გამჭირვალე და შესაბამისად ყველასთვის ხელმისაწვდომი.

ეთანხმები, რომ ცხელი ტიპის საფულის შემთხვევაში აქცენტი შეთანხმების ალგორითმზე კეთდება? პასუხი დაასაბუთე. (0.5)

არ ვერთანხმები, რადგან ცხელი საფულის შემთხვევაში აქცენტი პირველ რიგში არ კეთდება შეთანხმების ალგორითმზე. ცხელი საფულეები პრიორიტეტს ანიჭებენ ხელმისაწვდომობას და მოხერხებულობას კრიპტოვალუტით ტრანზაქციების სწრაფად განსახორციელებლად.

რა უპირატესობა აქვს ქაღალდის საფულეს ვებ-ბრაუზერის საფულესთან შედარებით? (0.5)

ქაღალდის საფულის მთავარი უპირატესობა ვებ-ბრაუზერის საფულესთან შედარებით არის ის, რომ ის უზრუნველყოფს გაძლიერებულ უსაფრთხოებას თქვენი კრიპტოვალუტის გასაღებების ქსელში ჩართვის გარეშე შენახვით და პოტენციური ონლაინ საფრთხეებისგან მოშორებით.

ეთანხმები მოსაზრებას, რომ კრიპტოვალუტები ძირითადად არსებულ ბლოკჩეინებში მუშაობენ? პასუხი დაასაბუთე. (0.5)

დიახ, კრიპტოვალუტები ძირითადად მუშაობს არსებულ ბლოკჩეინებზე. კრიპტოვალუტების უმეტესობა აგებულია დამკვიდრებულ ბლოკჩეინ ქსელებზე. ახალი ბლოკჩეინის შექმნა ნულიდან უფრო რთული და ნაკლებად უსაფრთხოა, ამიტომ არსებული ბლოკჩეინის გამოყენება საერთო და ეფექტური მიდგომაა.

რით განსხვავდება security თოქენი utility თოქენისგან? (1)

security თოქენი გამოიყენება ინვესტიციებში, ანუ ის წარმოადგენს საკუთრებას ან ფინანსურ ინტერესს აქტივზე, რომელიც ექვემდებარება რეგულაციებს და არის დარეგულირებული, ხოლო utility ტოკენი ანიჭებს პირს წვდომას კონკრეტულ სერვისებზე ბლოკჩეინის პლატფორმის ფარგლებში და არ არის დარეგულირებული.

განავრცე აზრი: უცვლადი თოქენი (Non-Fungible Token) არის ციფრული აქტივი, რომელიც, ... (0.5)

Non-Fungible Token არის უნიკალური ციფრული აქტივი, რომელიც არ იცვლება მისსავე მსგავს აქტივში.

რას წარმოადგენს თოქენის საბრუნავი მარაგი? (0.5)

თოქენის საბრუნავი მარაგი წარმოადგენს თოქენების რაოდენობას, რომლებიც ჩაშვებულია ბრუნვაში.

რატომ გამოიყენება კრიპტოსაფულეებში 12/24 სიტყვიანი აღდგენის ფრაზა? (1)

12/24-სიტყვიანი აღდგენის ფრაზების სისტემა უზრუნველყოფს უსაფრთხო და მოსახერხებელ გზას კრიპტოვალუტის აქტივების დასაცავად და საჭიროების შემთხვევაში მათ აღსადგენად.

რა და რა მონაცემებს შეიძლება ინახავდნენ საფულეები ბლოკჩეინ

სისტემაში? (0.5)

საფულე შეიძლება ინახავდეს ანგარიშებს, სხვადასხვა ციფრულ აქტივებს და ასევე, ქონდეს ჩაშენებული ბრაუზერი.

აღწერე, როგორ იანგარიშება თოქენის კაპიტალიზაცია? (0.5)

კაპიტალიზაცია იანგარიშება, როგორც ბრუნვაში ჩაშვებული თოქენის საბრუნავი მარაგი X ღირებულებაზე

მაქვს, თუ არა უფლება, გავცე საკუთარი კრიპტოსაფულის ანგარიშის შესახებ ინფორმაცია? პასუხი დაასაბუთე. (1)

შენ შეგიძლია გააზიარო შენი კრიპტოსაფულის ანგარიშის ინფორმაცია, თუ გინდა. თუმცა, ეს ზოგადად არ არის რეკომენდებული უსაფრთხოებისა და კონფიდენციალურობის რისკების გამო.

რომელი მოდელის დროს არ გვაქვს თოქენის მაქსიმალური მარაგი წინასწარ განსაზღვრული? (0.5)

ინფლაციური მოდელის (inflationary model) დროს.

აღწერე თოქენის ინფლაციური მოდელი. (0.5)

ინფლაციური მოდელის (inflationary model) დროს ჩვენ არ გვაქვს თოქენის მაქსიმალური მარაგი წინასწარ განსაზღვრული და შესაბამისად, ემისიის პროცესი შეიძლება უსასრულოდ გაგრძელდეს

ბიტკოინის ბლოკჩეინ სისტემა ინფლაციურია, თუ დეფლაციური? ახსენი მიზეზი. (0.5)

ბიტკოინი დეფლაციურია, რადგან მას აქვს თოქენის მაქსიმალური მარაგი წინასწარ განსაზღვრული(21 მილიონი ერთეული) შესაბამისად, ემისიის, ანუ წარმოშობის პროცესი დროთა განმავლობაში სრულდება.

სასწავლო კურსის სახელწოდება:	**BLOCKCHAIN ტექნოლოგიები (IBM BLOCKAIN)**
ლექტორი:	დავით ყიფშიძე
სტუდენტის სახელი და გვარი	

შუალედური გამოცდის დეტალური ინსტრუქცია

დახურული კითხვა - 1 ქულა (სულ 10 კითხვა)

ღია კითხვა - 2 ქულა (სულ 10 კითხვა)

კითხვების ჯამური ოდენობა - 20 კითხვა

ქულების მაქსიმალური ოდენობა - 30 ქულა

ჯგუფი 1 - ვარიანტი 2

- შეთანხმების პროტოკოლის ძირითად პარამეტრად განიხილება:
  - მონაცემთა ბაზა
  - ჩავარდნების მიმართ მედეგობა
  - ქსელური ადმინისტრატორი
  - პროგრამირებადობა
- ცივი ტიპის საფულეს განეკუთვნება:
  - ვებ-ბრაუზერის საფულე
  - ქაღალდის საფულე
  - მობილურის საფულე
  - დესკტოპის საფულე
- მაქსიმალური მარაგი არის ის თოქენები, რომლებიც:
  - უკვე ჩაშვებულია ბრუნვაში
  - შეიძლება ოდესმე აწარმოონ
  - ინახება საფულეებში
  - მონაწილეობენ ფასის დადგენაში
- ცხელი ტიპის საფულის შემთხვევაში, ძირითადი აქენტი კეთდება:
  - თანხის რაოდენობაზე
  - ხელმისაწვდომობაზე
  - შეთანხმების ალგორითმზე
  - ბლოკების ჯაჭვზე
- ბლოკჩეინში ყოველი ახალი ბლოკის ფორმირება:
  - ხდება დამოუკიდებლად, საკუთარი ჰეშის მიხედვით
  - დამოკიდებულია წინა ბლოკის ჰეშის მნიშვნელობაზე
  - ხდება დამოუკიდებლად, მომდევნო ბლოკის ჰეშით
  - დამოკიდებულია სხვა ტიპის ბლოკჩეინზე
- როდესაც გამომთვლელი კვანძი PoW-დან იღებს შედეგს, ის ამ შედეგს:
  - ანიჭებს დიდ მნიშვნელობას
  - უზიარებს ქსელს
  - ინახავს საიდუმლოდ
  - აარქივებს ხელსაყრელი შემთხვევისათვის
- საგნების ინტერნეტი (IOT) იძლევა იმის საშუალებას, რომ:
  - შეიქმნას საწარმოო ხაზი
  - მოწყობილობები დაუკავშირდნენ ერთმანეთს
  - დამუშავდეს დიდი ზომის მონაცემები
  - გაიაფდეს პროდუქტის საბოლოო ღირებულება
- Pretty Good Privacy (PGP):
  - ერთ-ერთ ნდობის მოდელის მაგალითია
  - ბლოკჩეინის უსაფრთხოების გარანტია
  - ვირტუალური რეალობის განუყოფელი ნაწილია
  - გაზიარებული ბაზების თანმდევი მოვლენაა
- ბლოკჩეინის სისტემა დაცულია, რადგან:

    - მასში გამოიყენება კრიპტოგრაფიის ელემენტები
    - ინდუსტრია 2.0 სტანდარტებს აკმაყოფილებს
    - სისტემის ყველა მონაწილე აუცილებლად სანდოა
    - ცენტრალიზებული სისტემაა
- ბლოკის ძირითად თვისებებს არ განეკუთვნება:
    - დროითი შტამპი
    - ბლოკის ჰეში
    - მონაცემები ტრანზაქციების შესახებ
    - ნდობის მექანიზმი

- ეთანხმები, თუ არა, რომ მაინინგის პროცესის ყოველი წარმატებული დასასრულისას ქსელის ყველა მონაწილე თანაბრად ინაწილებს გასამრჯელოს? პასუხი დაასაბუთე.

პასუხი: არ ვეთანხმები, რადგანაც როდესაც სისტემა აგზავნის მათემატიკურ თავსატეხს და შემდგომ იწყება უკვე შეჯიბრი სწორი ამონახსნის საპოვნელად, პირველი სწორად ამომხსნელი იღებს გასამრჯელოს და არა თანაბრად ინაწილებენ.

- განავრცე აზრი: კიბერუსაფრთხოება არის თანამედროვე ინფორმაციული სისტემების განუყოფელი ნაწილი, რადგან...

პასუხი: რადგანაც 21-ე საუკუნე არის ტექნოლოგიების ეპოქა ძალიან ბევრი რამ არის გაციფრულებული და ქსელშია ჩართული, შესაბამისად ნებისმიერი სისტემა/მოწყობილობა/ინფორმაცია რომელიც ქსელთან არის დაკავშირებული არის მეტად სახიფათო, ამის გამო მომრავლებულია კიბერშეტევები, ხოლო კიბერუსაფრთხოების თანამშრომლები კი სწორედ ამის თავის არიდებისთვის არიან, რათა მოხდეს დაცვა ჰაკერული თავდასხმებისგან

- რატომ გამოიყენება საფულეებში 12/24 სიტყვიანი აღდგენის ფრაზა?

პასუხი: 12/24 სიტყვიანი recovery phrase გამოიყენება დაცვისთვის, იგი არის რენდომად დაგენერირებული სიტვების ერთობილობა, რომლის გაზიარებაც არ შეიძლება და ისეთ ადგილას უნდა შევინახოთ, რომ არავის ჰქონდეს წვდომა.

- რომელი უფრო ეკომეგობრული შეთანხმების მოდელია: PoW, თუ PoS? პასუხი დაასაბუთე.

პასუხი: უფრო ეკომეგობრული არის PoS (აქტივების დადასტურება), რადგანაც PoW (მუშაობის დადასტურება) მოდელისთვის საჭიროა ელექტროენერგია და კომპიუტერული გამოთვლები, რაც ბევრ სითბოს გამოყოფს, ხოლო PoS მოდელის დროს კი საჭიროა რაღაც კონკრეტული აქტივების რაოდენობის ქონა, შესაბამისად უფრო ეკომეგობრული არის PoS

- მოკლედ აღმიწერე ბიზანტიელი გენერლების პრობლემა.

პასუხი: შეტევის დროს, როდესაც რამდენიმე ერთდროულად უტევს და მოგებისთვის აუცილებელია ყველა გენერლის ერთდროული შეტევა, მაგრამ შეიძლება რომელიმე გენერალმა გადაწყვიტოს რომ არ უტევს, ან რაიმე სხვას განიზრახოს, რის შედეგადაც მთელი გეგმა აირევა, ირღვევა კოორდინაცია და რა თქმა უნდა შეტევა წარუმატებელია

- აღმიწერე, როგორ იანგარიშება თოქენის კაპიტალიზაცია?

პასუხი: კაპიტალიზაცია იანგარიშება ბრუნვაში ჩაშვებული თოქენის საბრუნავი მარაგი X ღირებულებაზე

- ეთანხმები, თუ არა, რომ ნებისმიერი არაავტორიზებული ცვლილება ბლოკში ახდენს მომდევნო ბლოკების ვალიდურობის ანულირებას? პასუხი დაასაბუთე.

პასუხი: ვეთანხმები, რადგანაც ნებისმიერი ცვლილება ბლოკში როგორც მაღლა წერია ახდენს ანულირებას, ამიტომ ჩვენ არ შეგვიძლია რაიმეს შეცვლა, რადგანაც ამ ბლოკის ასლი ყველას აქვს და ნებისმიერი ცვლილება გამოჩნდება, შესაბამისად სისტემა მას თავად გაანულებს

- რა როლს ასრულებს SHA-256 ჰეშირების ფუნქცია თანამედროვე ბლოკჩეინ სისტემებში? პასუხი დაასაბუთე.

პასუხი: SHA-256 ჰეშირების ალგორითმი უზრუნველყობს მონაცემთა გარდაქმნას კრიპტოგრაფულ მონაცემებად. ერთსა და იმავე input-ზე კი ვიღებთ ერთსა და იმავე output-ს, შესაბამისად ნებისმიერი ასოს შეცვლა სიტყვაში იწვევს სულ სხვა output-ს რაც შესამჩნევია. შესაბამისად ეს განსაზღვრავს უსაფრთხოებას, იქედან გამომდინარე, რომ ქსელის ყველა მონაწილეს შეუძლია ცვლილების დანახვა, რაშიც sha256 ჰეშირების ფუნქცია ეხმარება, შესაძლებელი ხდება არავალიდური ცვლილებების თავიდან აცილება

- განავრცე აზრი: ინდუსტრია 2.0 არის ამ სფეროში დღეს არსებული მდგომარეობის წინაპირობა, რადგან ...

პასუხი: ინდუსტრია 2.0 დაიწყო მე-19 საუკუნეში, როცა შეიქმნა საწარმოო ხაზი, დღეს კი უკვე გვაქვს ინდუსტრია 4.0, რომელიც ხასიათდება საწარმოო პროცესებში ინფორმაციული და საკომუნიკაციო ტექნოლოგიების ფართო გამოყენებით, შესაბამისად რომ არ გვქონოდა საწარმოო ხაზი არც იმის ინტერესი/მოტივაცია გაჩნდებოდა რომ ინფორმაციული ტექნოლოგიები გამოგვეყენებინა.

- რა შეიძლება გავაკეთოთ იმისათვის, რომ ჩვენი ანგარიშები და საფულე მეტად იყოს დაცული არასასურველი შემთხვევებისგან?

პასუხი: პირველ რიგში თუ არ გვჭირდება არ უნდა გამოვიყენოთ ცხელი საფულე, რადგანაც იგი დაკავშირებულია ქსელთან და მეტია გატეხვის ალბათობა, თუმცა თუ მუდმივად გვჭირდება ტრანზაქციები რა თქმა უნდა ცხელი საფულის გამოყენება მოგვიწევს, ასევე საჭიროა დაცული ინტერნეტის გამოყენება (SSL/VPN) და რამდენიმე საფულე/ანგარიშის ქონა, რადგანაც ნებისმიერი ანგარიშის დაზიანების შემთხვევაში მეორეთი განვაგრძოთ მუშაობა და სრული დანაკარგი არ გვქონდეს აქტივების, ასევე საჭიროა მოწყობილობების ხშირად განახლება და პაროლების მუდმივი ცვლა, ხოლო ბოლო რაც ყველამ ნათლად იცის არ უნდა გავცეთ ინფორმაცია ჩვენი საფულის მონაცემების შესახებ