ბლოკჩეინ ტექნოლოგიები, როგორც თვითორგანიზებადი სისტემები

ქეთევან კოტრიკაძე, დავით ყიფშიძე
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განხილულია ბლოკჩეინი, როგორც თვითორგანიზებადი სისტემა, სადაც შემთხვევითად ან გამიზნულად მოხვედრილი შეუსაბამო ტრანზაქციების მართვა ხდება თვითონ სისტემის მიერ. ბლოკჩეინ სისტემა ნებისმიერ ტრანზაქციას ამოწმებს სხვადასხვა მექანიზმით და სისტემის სამოქმედო წესებთან შეუსაბამობის აღმოჩენის შემთხვევაში, ნებისმიერი ასეთი ტრანზაქცია ვარდება ბლოკების ჯაჭვიდან, ხოლო სისტემა უბრუნდება წინა მდგრად მდგომარეობას.

საკვანძო სიტყვები: ბლოკჩეინი. ტექნოლოგია. ჯაჭვი. თვითორგანიზებადი სისტემა.

1. შესავალი

ბლოკჩეინი ტრანზაქციების ჩანაწერების წინასწარ განსაზღვრული წესების ერთობლიობით შექმნილი ბლოკების ჯაჭვია, სადაც თითოეული ასეთი ტრანზაქცია შეიძლება იყოს ფულის, სხვადასხვა საქონლის ან უსაფრთხო მონაცემების მოძრაობა.

დაცული გამოთვლებით წარმოებული ბლოკების ჯაჭვის პირველი ნამუშევრები აღწერილია 1991 წელს. სისტემაში ხდებოდა დოკუმენტების ჰეშირება (შემავალ მონაცემთა გარდაქმნა კრიპტოგრაფიულ მონაცემებად მათემატიკური ალგორითმების გამოყენებით), ერთიანი უნიკალური ჰეშის მისაღებად [1].

ბლოკჩეინის, როგორც თანამედროვე კონცეფციის გამოყენების აუცილებლობა წარმოაჩინა სატოში ნაკამოტომ 2008 წელს. მან განავითარა თანამედროვე ბლოკჩეინის ერთ-ერთი მნიშვნელოვანი ფაქტორი, მესამე მხარისგან დამოუკიდებლად ბლოკების ჯაჭვში ჩასმის და დადასტურების შესაძლებლობა. ამ კონცეფციის დანერგვა ნაკამოტომ შეძლო მომდევნო წელს, ცნობილი კრიპტოვალუტის, ბიტკოინის გამოგონებით [2].

ბლოკჩეინის ქსელი კონსენსუსზე - ანუ შეთანხმებაზეა დამოკიდებული, რომელიც წინასწარ განსაზღვრული პერიოდის შუალედებით ავტომატურად ამოწმებს ქსელში ყველა ოპერაციას. ბლოკჩეინი აკეთებს ორ რამეს: კრებს მონაცემებს და ალაგებს მათ სპეციალურ ბლოკებში, შემდეგ კი ეს ჯაჭვები უკავშირდებიან ერთმანეთს დაცული გამოთვლებით კრიპტოგრაფიის ალგორითმების გამოყენებით. ბლოკჩეინის ერთ-ერთი რეალიზაციის, ბიტკოინის შემთხვევაში ეს არის Sha-256 ჰეშირების ალოგირთმი, [3] ეთერიუმის შემთხვევაში - ელიფსური მრუდეები და ა.შ. [4]

მარტივად რომ ავხსნათ, ბლოკჩეინი არის თვითორგანიზებადი სისტემა ორი პარამეტრით:

პირველი - ნებისმიერი ცვლილება რომელიმე ბლოკში ახდენს მომდევნო ბლოკების ვალიდურობის ანულირებას. რაც ნიშნავს იმას, რომ ფაქტიურად ვერ შეცვლი ტრანზაქციების ისტორიულ ჩანაწერებს. სისტემა თვითონ აღადგენს მას ქსელის სხვა

მონაწილეების სისტემების საშუალებით და არასასურველი ცვლილებები ავტომატურად ანულირდება.

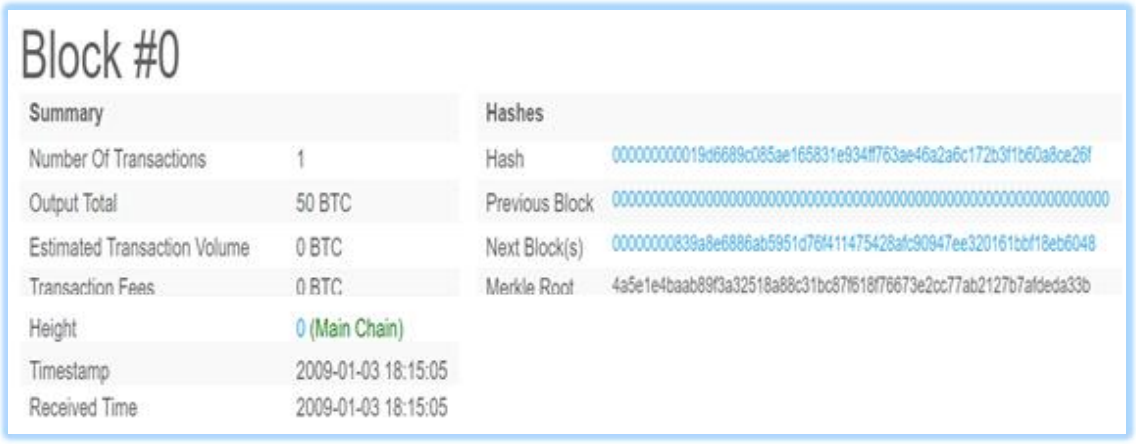
მეორე არანაკლებ მნიშვნელოვანი პარამეტრი არის ის, რომ ბლოკჩეინში წესები მათემატიკურად არის გამყარებული - არ არის საჭირო რაიმე ცენტრალური მმართველი ორგანოს ჩარევა იმის გასარკვევად, რომ მიხვდე - შენი ტრანზაქცია მცდარია, თუ არა დროის ნებისმიერ მონაკვეთში.

2. ძირითადი ნაწილი

ბლოკჩეინის მონაცემთა სტრუქტურას აქვს ორი ძირითადი თვისება, ჰეში და წინა ჰეში. ბლოკის ჰეში შეიძლება წარმოვიდგინოთ, როგორც თითის ანაბეჭდი, რომელიც უნიკალურს ხდის თითოეულ ბლოკს. თუკი რაიმეს შევცვლით ბლოკის შიგთავსში, ეს გამოიწვევს მთელი ჰეშის ცვლილებას (გამოჩნდება ცვლილება). წინა ჰეში ქმნის ბლოკების ჯაჭვს და შესაბამისად ბლოკჩეინი ხდება დაცული (ნახ.1).

ნახ.1. ბლოკების ჰეშები დროითი შტამპებით

თუკი შევცვლით ბლოკს, მისი ჰეშიც შეიცვლება, ანუ მომდევნო ბლოკს ექნება არავალიდური წინა ბლოკი. ეს ნიშნავს, რომ ყოველი მომდევნო ბლოკი გახდება არავალიდური. პირველი ბლოკი განსაკუთრებული ბლოკია, რადგან მას არ აქვს წინა ვალიდური ჰეში (არ არსებობს წინა ბლოკი). ამ ბლოკს ეწოდება გენეზისის ბლოკი და მისი წინა ჰეშის მნიშვნელობა უბრალოდ ნულების ერთობლიობაა (ნახ.2) [5].



ნახ.2. ბიტკოინის პირველი, გენეზისის ბლოკი

იმის გამო, რომ ყველა მონაწილეს აქვს მთელი ბლოკჩეინის ასლი, მათ შეუძლიათ დაინახონ სისტემაში ნებისმიერი ცვლილება. ანუ, როდესაც ჰეშები მთელ ჯაჭვში ემთხვევიან ერთმანეთს, ყველა მონაწილემ იცის, რომ შეუძლიათ ენდონ ჩანაწერებს.

განვიხილოთ ასეთი მაგალითი. წარმოვიდგინოთ, რომ გვაქვს შემდეგი ბლოკების ჯაჭვი (ნახ.3)

ნახ.3. ვალიდური ბლოკების ჯაჭვი

და ჩვენ შევცვალეთ რაიმე მეორე ბლოკში, ისე როგორც ეს ნაჩვენებია მე-4 ნახაზზე.

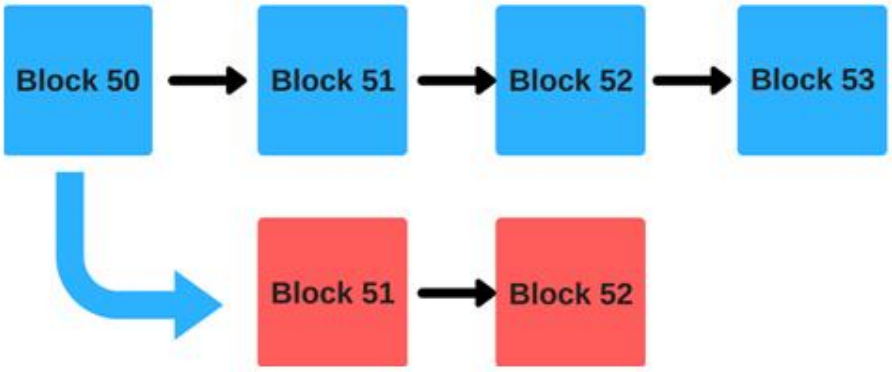
ნახ.4. არავალიდური ბლოკების ჯაჭვი

ამ მცირე ცვლილების შედეგი არის ის, რომ მომდევნო ბლოკს ექნება არავალიდური წინა ჰეში, ანუ ყოველი მომდევნო ბლოკი იქცევა არავალიდურად. მაგრამ ეს არ არის საკამარისი იმისათვის, რომ არასასურველი ცვლილებები აიკრძალოს. იმისათვის, რომ ეს არ მოხდეს, ბლოკჩეინის შემქმნელებმა გაითვალისწინეს წესების მთელი ერთობლიობა, რომელიც რთული და დროზე დამოკიდებული მოქმედებების შედეგად ახდენს ვალიდური ჰეშების ხელახალ კალკულაციას.

იმისათვის, რომ გაერთულებინათ ჰეშების კალკულაცია, პირველივე ბლოკჩეინის ვერსიაში შემოღებული იქნა ე.წ. მუშაობის დადასტურების მექანიზმი (Proof of Work) [6]. მუშაობის დადასტურება, მარტივად რომ ავხსნათ, ეს არის გამოგონილი შეზღუდვა იმისათვის, რომ გართულდეს გამოთვლები. ეს შეზღუდვა ამბობს, რომ თითოეული ბლოკის ჰეში უნდა დაიწყოს რაღაც X რაოდენობის ნულებით. ეს არავალიდურ გამოთვლებს ართულებს, რადგან ან უნდა გამოიცნო ჰეში ან გატეხო, სხვა გზა არ არის. რეალურად გიწევს ისეთი ჰეშის გამოცნობა, რომელსაც თავისი რთული ალგორითმის მიღმა, თავში მოყვება გაურკვეველი რაოდენობის ნულები.

კიდევ ერთი გზა, რითაც ბლოკჩეინი ახდენს თავის დაცვას, არის მისი დისტრიბუციულობა. ის იყენებს წყვილური კავშირების ქსელს (P2P Network), სადაც ნებისმიერ მსურველს შეუძლია მიერთება. თითოეულ მომხმარებელს აქვს ბლოკჩეინის სრული ასლი (ბიტკოინის შემთხვევაში, დღეის მდგომარეობით ის დაახლოებით 200 გიგაბაიტის ზომისაა [7]). და როდესაც ვინმე ქმნის ახალ ბლოკს, ის ეგზავნება ყველა მონაწილეს. თითოეული მონაწილე ავტომატურ რეჟიმში ადასტურებს, რომ ეს ბლოკი არ იქნა შეცვლილი ხელოვნურად და შემდეგ ამატებს ჯაჭვში, წინააღმდეგ შემთხვევაში ბლოკი

უარყოფილი ხდება (ნახ.5) ამ გზით, იმისათვის, რომ ბლოკი დაემატოს ქსელს, მინიმუმ 51% მომხმარებლებისა უნდა დაეთანხმოს იმას, რომ ბლოკში არასასურველი ცვლილებები არ მომხდარა.



ნახ.5. არავალიდური ბლოკების უგულვებელყოფა

ზემოთ აღწერილი ინფორმაციიდან შეიძლება ასეთი დასკვნის გაკეთება - იმისათვის, რომ ბლოკჩეინის ჯაჭვზე წარმატებით განხორციელდეს არასასურველი შეტევა. შემტევს ერთდროულად უნდა ჰქონდეს გადათვლილი როგორც ყველა ჰეში, ასევე უნდა რაიმე გზით მოატყუოს დაკავშირებული მონაწილეების 50%-ზე მეტი. ეს ფაქტობრივად, (ამჟამად) შეუძლებელია. ამიტომაც არის ბლოკჩეინი ასეთი დაცული. ის დაცულია არა რაიმე ცენტრალიზებული აპარატით, არამედ რთული მათემატიკური პრობლემების გადაჭრით.

3. დასკვნა

ბლოკჩეინ ტექნოლოგიები თანამედროვეობის ერთ-ერთი დიდი გამოწვევაა, რომელიც მოიცავს რთულ მათემატიკურ გამოთვლებს, ავტომატიზაციის კომპლექსურ მექანიზმებს და უსაფრთხოების მაღალ სტანდარტებს. სტატიაში განვიხილეთ ბლოკჩეინი, როგორც თვითორგანიზებადი სისტემა, რომელიც მიუხედავად გარე ხელისშემშლელი ფაქტორების ზემოქმედებებისა, ისეთი მექანიზმების საშუალებით, როგორიცაა დისტრი-ბუტიულობა და მესამე მხარისგან დამოუკიდებლობა, ავტომატურ რეჟიმში უბრუნდება სტაბილურ მდგომარეობას და განაგრძობს წინასწარ განსაზღვრული რეჟიმით მუშაობას.

ლიტერატურა - References – Литература:

1. Bayer Dave, Haber Stuart, Stornetta W. Scott. (1992). Improving the Efficiency and Reliability of Digital Time-Stamping. Sequences. 2. pp.329–334.

2. Nakamoto Satoshi (2009). Bitcoin. v0.1 released. metzdowd.com/msg10142.html

3. https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/what-is-hashing

4. Gavin Wood, Andreas M. Antonopoulos, O'Reilly (2018). Mastering Ethereum – Ch.4. Cryptography. Media, Inc. November 2018

5. https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

6. https://cointelegraph.com/explained/proof-of-work-explained
7. https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/

BLOCK CHAIN TECHNOLOGIES, AS SELF-ORGANIZING SYSTEMS

Kotrikadze Ketevan, Kipshidze Davit
Georgian Technical University

Summary

In this article we discuss the block chain as a self-organizing system where the unintended transactions that are put in the system accidentally or intentionally, are managed by the system themselves. The block chain system checks every transaction through the various mechanisms and in case of discrepancies with the operating rules, any such transaction is rejected from the chain of blocks and the system returns to the previous stable state.

БЛОКЧЕЙН ТЕХНОЛОГИИ, КАК САМООРГАНИЗУЮЩИЕ СИСТЕМЫ

Котрикадзе К., Кипшидзе Д.
Грузинский Технический Университет

Резюме

Рассматривается блокчейн, как самоорганизующая система, в которой непреднамеренные транзакции, которые вводятся в систему случайно или преднамеренно, управляются самой системой. Система блокчейна проверяет каждую транзакцию с помощью различных механизмов, и в случае расхождений с правилами работы, любая такая транзакция отклоняется из цепочки блоков, и система возвращается в предыдущее стабильное состояние.