Sistema de Consulta de Dados Gravados nos Blocos da Blockchain Ethereum[1]

João Pedro Nascimento de Lima[2,7], Gabriel Emidio Teixeira Costa[3], Fabio Cesar da Silva[4], Alexandre de Castro[5] e Inacio Henrique Yano[6]

[1]Trabalho realizado com apoio financeiro da Embrapa, CNPq e Faped. [2]Graduado em Engenharia da Computação, Anhanguera Educacional, Campinas, SP. [3]Pesquisador da Embrapa Agricultura Digital, Campinas, SP. [5]Pesquisador da Embrapa Agricultura Digital, Campinas, SP. [6]Pesquisador da Embrapa Agricultura Digital, Campinas, SP. [7]lima.jp98@hotmail.com

Resumo - Blockchain é uma tecnologia emergente que pode ser usada para registrar dados das mais diversas aplicações, principalmente para rastreabilidade de ativos e processos, devido às suas características de segurança, entre elas, está a imutabilidade dos dados. Em havendo algum erro nos dados gravados, a solução é gravar novo bloco com os dados corretos, entretanto, o bloco com os dados errados permanece na estrutura de blocos e, portanto, em situações como esta, faz-se necessária uma justificativa para o erro ocorrido. Isto torna o blockchain um importante instrumento de auditoria. Boa parte dos sistemas baseados em blockchain fazem uso dos contratos inteligentes para as regras de negócios e armazenamento e recuperação de dados. Contratos inteligentes são como programas de computador orientados a eventos, ou seja, na ocorrência de determinados eventos, certas ações acontecem automaticamente. Apesar de todos os dados gravados nos contratos inteligentes serem também gravados na blockchain, não existe uma forma de recuperar os dados contidos nos blocos para confrontá-los com os dados do contrato inteligente. Sendo que no contrato inteligente somente é possível recuperar o dado mais recentemente gravado, não sendo possível recuperar ou saber se houve algum valor alterado em uma determinada variável, diferentemente dos blocos, onde uma vez gravado o dado ali permanece imutável e, conforme descrito, se houver necessidade de alguma alteração, é necessário gravar novo bloco. O objetivo deste trabalho é apresentar os procedimentos para a recuperação de dados nos blocos, pois isto pode vir a ser útil como instrumento de auditoria para várias empresas.

Termos para indexação: auditoria, contrato inteligente, imutabilidade dos dados, rastreabilidade

Query system for data recorded in blockchain Ethereum blocks

Abstract - Blockchain is an emerging technology to record data from the most diverse applications, mainly for asset and process traceability due to its security characteristics, among them the immutability of data. If there is an error in the recorded data, the solution is to record a new block with the correct data. However, the block with the wrong data remains in the block structure. Therefore, in situations like this, the error that occurred needs justification. Making blockchain a powerful audit tool. Most blockchain-based systems use smart contracts for business rules and data storage and retrieval. Smart contracts are like event-driven computer programs, i.e., when certain events occur, some actions happen automatically. Although all data recorded in smart contracts is also recorded in the blockchain, there is no way to retrieve the data contained in the blocks to match them with the smart contract data. Since in the smart contract, it is only possible to retrieve the most recently recorded data, it is not possible to recover or know if a given variable had its value changed. Unlike blocks, where once data is recorded, it remains immutable, and, as described, if there is a need for any changes, it is necessary to record a new block. This work aims to present the procedures for the data recovery in the blocks, as this can be useful as an audit tool for several companies.

Index terms: audit, immutability of data, smart contract, traceability.