**...**

Henrique Chaves Lopes | RA 11202130079

1. **Introdução**

O advento da blockchain, uma tecnologia proposta no artigo publicado por Satoshi Nakamoto (cuja identidade é desconhecida) em 2008, representou uma ruptura no modo como dados sensíveis, como o registro de transações financeiras, são armazenados. Mas, para além das criptomoedas, cujo surgimento foi concomitante à invenção da blockchain, novas aplicações da tecnologia estão sendo desenvolvidas, inclusive no campo da saúde.

Escrever: o que são e como funcionam as blockchains; o que são os algoritmos de consenso; o que é a prova de trabalho; quais são algumas das funções de prova de trabalho; e quais testes eu vou fazer.

\*Algumas funções de prova de trabalho para pesquisar: hashcash (usado no bitcoin); scrypt (usado no litecoin); equihash (usado no zcash); ethash (ethereum); cuckoo cycle (eficiência energética); blake2b (menor consumo de energia do que o hashcash); primecoin; verifiable delay functions (reduz a vantagem de hardware, mas ainda está sendo desenvolvido).

1. **Descrição do software e dos testes**

A implementação da blockchain foi feita com a linguagem de progamação Python, de acordo com o guia explicitado abaixo, nas referências bibliográficas. O código fonte contém a classe **Blockchain**, onde foram definidos:

* O método de inicialização, onde o bloco de gênese é criado.
* O método **new\_block** que cria um novo bloco e cujos parâmetros são: o hash do bloco anterior e o *nonce* (número) da prova de trabalho.
* O método **new\_transaction** que cria uma nova transação e cujos parâmetros são: o endereço do pagador, o endereço do recebedor e o valor da transação.
* O método **hash** que calcula o hash do bloco passado como parâmetro.
* O método **last\_block** que retorna o último bloco da blockchain.
* O método **proof\_of\_work** que calcula a prova de trabalho.

Além disso, a comunicação com a blockchain é realizada por meio de uma *Application Programming Interface* (API) criada com a biblioteca Flask do Python.

1. **Resultados**
2. **Conclusão**

**Referências**

NAKAMOTO, Satoshi. Bitcoin: a peer-to-peer electronic cash system. **Bitcoin**, 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 10 de dez. de 2024.

CONTERNO, Ivan. Tecnologia blockchain pode reduzir risco de roubos e fraudes na área da saúde. **Jornal da USP**, São Paulo, 29 de mai. de 2023. Disponível em: <https://jornal.usp.br/ciencias/tecnologia-blockchain-pode-reduzir-risco-de-roubos-e-fraudes-na-area-da-saude/>. Acesso em: 10 de dez. de 2024.

Proof of work. **Wikipedia**, 2024. Disponível em: <https://en.wikipedia.org/wiki/Proof_of_work>. Acesso em: 10 de dez. de 2024.

TRISTIANTO, Bimo Putro. Build your own blockchain in Python: a practical guide. **Medium**, 2022. Disponível em: <https://bimoputro.medium.com/build-your-own-blockchain-in-python-a-practical-guide-f9620327ed03>. Acesso em: 10 de dez. de 2024.