Tarefa: Blockchains Corporativos Hyperledger Fabric Módulo 1

Gabriel dos Santos Schmitz

Outubro 2024

1. Chaves Públicas e Privadas

PROBLEMA 1. *O site https://andersbrownworth.com/blockchain/public-private-keys/transaction contém ferramentas interativas para demonstrar o funcionamento de chaves públicas e privadas, e também a utilização delas para assinar transações. Explore o site e o utilize para responder às questões abaixo.*

1-a. *Qual o valor da assinatura de uma transação com os dados da tabela abaixo?*

Valor	**De**
35.00	041e728b6c57cf4c6be2f2d593cfddad442523f7f316e483d0b2216b38fdfd55652fb13d2b61983e696abf8e9badb1002e08e9bad1a882dd787fdc2598969c67bd
Para	**Chave Privada**
04cc955bf8e359cc7ebbb66f4c2dc616a93e8ba08e93d27996e20299ba92cba9cbd73c2ff46ed27a3727ba09486ba32b5ac35dd20c0adec020536996ca4d9f3d74	44704561232094925999702040688802456114780336345827441713705004851108031018522

Solução:

O valor da assinatura baseado na transação é de:
3045022100960016f1a50a1d36934f233a24b571ecadc7c045fd830c93b510b3f0f73f367a02205b56171bc8a545ec30d64b60f139fba98093f13deef7b9205e976d615fad8405

1-b. *Usando os mesmos dados de De, Para e Chave Privada da tabela na questão 1, identifique quais das transações na tabela abaixo são válidas:*

Tx	**Assinatura**	**Valor**
1	304502210092d7a8c41c090fb9d26f495dc381297e17a3961cf2c60e7826179023bbaf6ef602201658154e537e55de6064f3a781902cef1541b7b75a29bbf3616d8d3aaba7eca8	5.00
2	3046022100befb38ad806de564f12f50db48027fe7ccdf5fcfabbb9f228055cd2bf8a80c2f022100b7f4e0283b1ba099a206e1328bb23ff7d2b413a9cbe8070ccb0dd83334bce53e	3.00
3	304402200ff25c5e99b891f7f4ddf8c5acc18c1b0db52bccc9664bcee5b80452fb6ee99602203e499de01b0be560dc6d8efb9e0d03df6f011eb75d16359abf5bcc90bdfd09ff	9.00
4	3045022100d799c67ccb033646b284b3cdbbf133b437757c03564279bc6c7200b877910620022005a12c62b203da939b4201368b49fcdfaae95bc0bbac14f4b14eb77c30b84eb0	1.00
5	304502206fd040f1a2377bbb4e95a46ff60e9ea9a1de162739b527d287e551ad826cc89a022100ea7fc1ff3e4e05eb6211d9d07e94cd3c1d015bb8a9f48b1e40bd80d19518a0e2	2.00

TABLE 1. Tabela de Transações

Solução:

Verificando as tranções com as assinaturas providas as transções validas são as de Tx = [1, 4, 5].