Lista de Exercícios

Nome: Vinícius de Moraes **- nUSP:** 13749910

1) O bitcoin não é Turing completo, mas o Ethereum é. Uma tecnologia Turing completa permite o uso de condicionais e repetições para o desenvolvimento de aplicações.
2) World State é um conjunto de dados que guarda os valores de um conjunto de endereços e estados de conta. A blockchain pode ser vista como uma máquina de estados replicada, pois ela possui a mesma lógica de uma máquina de estados, só que baseada em transações, onde ela parte de um início e então começa a executar transações de forma incremental para transformar a blockchain em algum estado atual.
3) Novas transações mudam o estado atual de uma Blockchain
4) A motivação para participar de uma rede blockchain pública é que os seus usuários são anônimos, então um determinado usuário seria capaz de realizar transações de forma segura e eficiente sem precisar revelar seu nome verdadeiro, assim, protegendo seu anonimato. Além disso, redes blockchain públicas são completamente descentralizadas, desregulamentadas (não existem regras específicas sobre o uso do servidor da rede) e são imutáveis, ou seja, assim que algum bloco é criado e inserido na rede, ele não pode ser removido, modificado ou alterado
5) Merkle Trees são um tipo de estrutura de dados que são árvores onde cada leaf node é rotulado com o valor hash de um bloco e cada non-leaf node é rotulado com o valor hash dos rótulos dos seus nós filhos.
6) O algoritmo PoW utilizado pelo Ethereum antes do merge era o Ethash. Os mesmos ASICs utilizados para minerar Bitcoin não eram lucrativos para minerar Ether, pois os ASICs só funcionando para realizar uma única tarefa, que no caso dos ASICs para minerar bitcoin era decifrar a função hash SHA256, o que não seria útil para decifrar a função hash do Ethereum
7) O livro de transações do protocolo bitcoin e do protocolo ethereum são abertos, permitindo que qualquer indivíduo possa verificar as transações que ocorreram entre determinadas contas. Em contraposição, os protocolos Zcash e Monero cada usuário é completamente anônimo e todas as transações são camufladas usando tecnologias que tornam cada transação privada e não rastreável, ocultando os endereços, as assinaturas e a quantidade.
8) No método Proof of Stake, são selecionados validadores aleatórios que estão conectados na rede para criar novos blocos e confirmar transações.
9) O determinismo é fundamental na blockchain, pois cada node de uma rede deve ser capaz de gerar o mesmo resultado quando um mesmo valor de entrada é dado. Um exemplo de um conflito que seria gerado caso a blockchain não fosse de natureza determinística seria que isso poderia causar com que diferentes nodes não concordassem com os saldos das pessoas e com coisas como se transações são válidas ou não, pois diferentes nodes gerariam diferentes resultados dado a mesma

entrada, fazendo com que enquanto uma parte vê que uma conta possui saldo insuficiente, a outra vê como se estivesse tudo bem.
10) Transações são instruções com uma assinatura criptografada feitas por uma pessoa e construídas e disseminadas por um programa para dentro de uma Blockchain. Uma transação pode ser outras coisas além do envio de coins, uma transação é nada além que a transmissão de dados entre uma rede de computadores no sistema da blockchain.
11) A mempool é como se fosse uma “sala de espera” para transações que ainda não foram mineradas na Blockchain. Essa mempool armazena transações novas, que ainda não foram confirmadas, e transações arquivadas, que já foram confirmadas, antes de serem adicionadas em um bloco novo na blockchain.
12) Hardfork é quando acontece uma mudança radical no protocolo da rede que faz com que blocos e transações que antigamente seriam inválidos agora sejam válidos ou vice-versa. Isso pode ser iniciado pelos desenvolvedores ou membros da comunidade que estão insatisfeitos com as atuais funcionalidades dessa blockchain. Hardforks aconteceram antes como quando a blockchain da Ethereum criou uma hardfork para reverter os danos de quando hackearam a DAO e também quando a rede Bitcoin criou uma hardfork para dividi-la em duas redes, a Bitcoin, e a Bitcoin Cash, em 2017.
13) O “halving interval” é um processo de reduzir pela metade as recompensas de se minerar um bitcoin a cada conjunto de 210 mil blocos minerados. Em média, 210 mil blocos levam 4 anos para serem minerados, então consequentemente os períodos de halving levam em média intervalos de 4 anos para acontecer. O próximo período de halving é esperado para acontecer em 2024
14) O algoritmo de criptografia de chave pública do Bitcoin é o Algoritmo de Assinatura Digital de Curva Elíptica, o “SHA2 256-bit hash scheme” que foi desenvolvido pela NSA dos Estados Unidos.