Proposta de avaliação do desempenho de um mecanismo de consenso probabilístico baseado em Proof-of-Stake para blockchains públicas

Felipe Benedet da Silva, Diego Fernandes Gonçalves Martins, Marco Aurelio Amaral Henriques

[1]Faculdade de Engenharia Elétrica e de Computação
Universidade Estadual de Campinas (Unicamp)
Campinas – SP – Brazil

f324180@dac.unicamp.br,diegofgm@dca.fee.unicamp.br,maah@unicamp.br

Abstract. *The blockchain is a distribuited system used for registration of financial transactions and other sensitive information, following a specific consensus mechanism to ensure its security. Currently, Proof-of-Work is the most used consensus, but it has limitations related to the efficiency and electric power consumption, raising interest on other mechanisms, as Proof-of-Stake. Our research group has proposed previously a new Proof-of-Stake consensus that does not require validating committees, being more efficient than other consensus. The purpose of this paper it to propose new methods to evaluate the new consensus mechanism in real scenarios, considering a heavy creation and dissemination of transactions among all nodes. The evaluation also considers the creation and transmission of blocks completely full of transactions, making the network activity more intense and closer to that of an application under severe workloads.*

Resumo. *A blockchain é um sistema distribuído utilizado para registro de transações financeiras e de outras informações confidenciais, seguindo um mecanismo de consenso específico para garantir sua segurança. Atualmente, o Proof-of-Work é o consenso mais utilizado, mas tem limitações relacionadas a sua eficiência e consumo de energia elétrica, aumentando o interesse em outros mecanismos, como o Proof-of-Stake. Nosso grupo de pesquisa propôs anteriormente um novo consenso Proof-of-Stake que não requer comitês de validação, sendo assim mais eficiente que outros consensos. O propósito deste artigo é propor novos métodos para avaliar o novo mecanismo de consenso em cenários reais, considerando uma forte criação e disseminação de transações entre todos os nós. A avaliação também considera a criação e transmissão de blocos completamente carregados de transações, tornando a atividade da rede mais intensa e próxima de uma aplicação sob uma carga severa de trabalho.*

1. Introdução

Blockchains públicas são sistemas de consenso distribuído que se popularizaram com a utilização de criptomoedas, sendo o Bitcoin a principal e mais utilizada. Esses sistemas distribuídos permitem, sem a necessidade de uma terceira entidade regulamentadora, a realização de transações entre duas partes que não possuem necessariamente uma relação

de confiança entre si. Para isso, a blockchain funciona como um livro razão entre os diversos usuários da rede que passam a concordar sobre as transações inseridas nele, fazendo com que elas sejam confiáveis após a obtenção de um consenso.

Nas blockchains, os nós armazenam as transações em blocos que por sua vez são indexados uns aos outros de maneira sequencial formando uma cadeia, sendo que cada bloco proposto é avaliado por todos os nós da rede. A avaliação de cada bloco é realizada pelos nós seguindo as regras estabelecidas pelo mecanismo de consenso adotado pela blockchain. De acordo com [Bashir 2018], um mecanismo de consenso define um conjunto de regras que a maioria dos nós (usuários) devem seguir para que se atinja o acordo sobre um valor ou um estado do sistema. Considerando sua utilização em uma rede pública, é necessário que o mecanismo seja bem estabelecido e tenha um funcionamento confiável uma vez que, nesse tipo de rede, não existe um controle ou verificação a respeito de seus participantes, o que colabora para a existência de nós maliciosos, que buscam subverter os consenso em andamento ou já realizados. Além disso, a rede tem comportamento assíncrono, o que torna impossível diferenciar um nó falho de um nó desonesto [Fischer et al. 1985]. Neste sentido, o Proof-of-Work (PoW) é o mecanismo de consenso mais utilizado nas blockchains públicas, principalmente naquelas que foram constituídas para registros de transações financeiras envolvendo criptomoedas, como o Bitcoin. Porém, este mecanismo apresenta fortes limitações relacionadas ao seu desempenho e ao consumo de energia relacionada ao processo.

O Proof-of-Stake (PoS ou Prova-de-Posse) é uma proposta alternativa de consenso que despertou o interesse devido ao seu melhor desempenho e menor consumo de energia elétrica, quando comparado ao PoW. O trabalho de Martins [Martins 2021] sobre consenso em blockchains públicas apresentou um novo mecanismo de consenso baseado em Proof-of-Stake, que tem como principal característica a não exigência de comitês de validação para as transações propostas na blockchain, como é comum em outros consensos baseados em Prova de Posse. A ausência desses comitês é uma vantagem deste novo mecanismo, já que, em geral, a implementação de comitês distribuídos para que os blocos produzidos sejam confirmados, é bastante complexa.

A fim de complementar a avaliação de desempenho desse novo mecanismo de consenso, este trabalho propõe novos e mais pesados métodos de testes capazes de verificar o funcionamento do mecanismo em situações nas quais os nós da rede são submetidos a cargas de trabalho mais pesadas e mais próximas de uma rede com grandes demandas de processamento e comunicação.

2. Proof-of-Stake

Uma vez conhecido o funcionamento geral do PoW e as limitações enfrentadas por ele e, consequentemente, pela maioria das tecnologias de blockchain atuais, é possível compreender a necessidade de propostas alternativas, capazes de aumentar a eficiência dessas tecnologias e ampliar sua aplicação. As principais propostas alternativas, seguem premissas baseadas em Proof-of-Stake (PoS ou Prova-de-Posse), onde a participação dos nós é associada a uma quantidade de *stake* finito controlada por eles. De maneira geral, é comum associar o *stake* à quantidade de moedas controladas pelo nó.

As propostas mais relevantes baseadas no conceito de PoS utilizam a formação de comitês que são responsáveis por decidir qual dos blocos propostos será de fato

mantido permanentemente na blockchain. Além disso, de acordo com Fischer et al. [Fischer et al. 1985], um consenso determinístico não pode ser alcançado considerando as condições normais de operação de uma rede distribuída. Portanto, considerando as condições de funcionamento de uma rede distribuída pública, ou seja, que é assíncrona e pode ter participantes desonestos, é necessário limitar o tempo de operação de cada nó a fim de obter um certo grau de sincronismo, garantindo a evolução da blockchain.

Os comitês utilizados nesse tipo de protocolo se baseiam no problema dos generais Byzantinos, elaborado por Lamport [Lamport et al. 1982], que preconiza que, em um sistema distribuído, é possível alcançar um consenso determinístico somente se o número de nós desonestos for menor que um terço dos participantes da rede. Desta forma, as limitações para o mecanismo PoS estão associadas ao sincronismo exigido na rede e ao fato de, em geral, possuírem um alto grau de complexidade para sua implementação, envolvendo a construção de comitês descentralizados.

Dentre os mecanismos PoS, destaca-se uma nova proposta, que está em desenvolvimento na FEEC pelo grupo de pesquisa ReGrAS [Martins 2020]e que é uma alternativa mais eficiente aos consensos baseados em PoS tradicionais. A principal diferença entre a nova proposta e os outros mecanismos PoS, é que ela não exige comitês de validação.

De maneira geral, o novo mecanismo define rodadas com um tempo de duração fixo garantindo um grau de sincronismo na rede. Para a produção de blocos, cada nó realiza no início de cada rodada um sorteio independente utilizando seus *stakes*, os quais influenciam as probabilidades de sucesso no sorteio e dão ao nó o direito de propor ou não blocos para a rede. Ao receber blocos durante a rodada, os nós seguem parâmetros estabelecidos pelo mecanismo de tal forma que todos os nós entram em consenso e selecionam os mesmos blocos para inserir em sua visão local da cadeia. A confirmação de blocos é feita de maneira probabilística, onde os nós comparam a quantidade de blocos recebidos com a expectativa de blocos por rodada (parâmetro do mecanismo).

3. Novas avaliações de desempenho para o mecanismo PoS sem comitês

3.1. Motivação

Apesar do novo mecanismo de consenso proposto ter sido alvo de vários testes e avaliações de desempenho, algumas características ainda não foram plenamente avaliadas sob situações de carga mais pesadas. Em uma aplicação real, esse desempenho é afetado não só pelas operações realizadas pelos nós para produzir os blocos e atingir um consenso, mas também por operações como receber as transações, administrá-las em uma base de dados local e inseri-las dentro dos blocos. Por esse motivo, foram desenvolvidos módulos capazes de simular a criação, a transmissão e o armazenamento de transações para os nós que compõem a blockchain do novo mecanismo proposto. Além disso, estas transações são incorporadas a blocos durante a fase de mineração, permitindo assim que todo o sistema trabalhe com um volume de dados próximo àquele que se encontra em uma situação de carga máxima.

3.2. Transações

Como apresentado em [Antonopoulos 2017] a estrutura de uma transação financeira real apresenta o tipo da transação, indicando suas especificações, os *inputs* da transação, que

representam as moedas não gastas da rede e que, portanto, são consumidas como gastos em novas transações, os *outputs*, que representam quantias que poderão ser gastas futuramente e, por fim, seu *locktime* que pode tornar a transação inválida por um certo período de tempo. Assim, as transações são encadeadas umas as outras a partir dos *inputs* e *outputs* e suas validações são feitas a partir de consultas a uma tabela chamada UTXOs (*unspent transaction outputs*) que mantém todas as moedas não gastas da rede de forma a garantir que não ocorram gastos duplos no sistema.

Para o modelo de testes, foi considerada uma abordagem com o objetivo de determinar a eficiência do novo mecanismo ao utilizar transações individuais que são transmitidas na rede e permitem que os nós realizem seu encapsulamento em novos blocos. Assim, neste primeiro momento, não foram implementados procedimentos de verificação da validade destas transações, ou seja, o foco principal foi o de avaliar o desempenho do novo mecanismo de consenso em relação à sua capacidade de confirmar blocos, quando um grande volume de transações está presente na rede. Neste cenário, o conteúdo das transações não possui muita relevância a não ser pelos seguintes itens: tamanho da transação, seu *hash* identificador e taxa financeira responsável por estabelecer prioridades entre as transações que estão aguardando para serem inseridas em novos blocos.

O tamanho do *payload* é utilizado para realização de consultas rápidas a respeito do tamanho da transação. Com isso é possível calcular o valor total pago como taxa, que depende desse tamanho e da taxa por byte paga pelo emissor da transação. Assim, os nós participantes do consenso podem escolher as transações com as maiores taxas para inserir no novo bloco. Vale ressaltar que, em transações reais, a taxa e as informações a seu respeito não estão explicitadas nas transações. Para obtê-la na blockchain do Bitcoin, por exemplo, o nó calcula a diferença entre o saldo presente nos *inputs* com o saldo dos *outputs* de forma que essa diferença de saldo, sendo maior que zero, é a taxa que deve ser destinada a uma nova transação, a qual indica o próprio endereço do nó como *output*.

3.3. Geração de transações

Para a geração de transações, é necessário que sejam seguidas especificações na rede que garantam uma consistência do experimento com uma rede real. Para isso, foi estabelecida uma entidade independente da rede, que se diferencia dos nós e que é responsável por gerar as transações de maneira paralela à execução do novo mecanismo de consenso. De maneira geral, o gerador de transações é responsável por simular a presença de *wallets* na rede, permitindo que os nós executem suas tarefas ligadas ao consenso enquanto administram novas transações que são recebidas por meio de seus *peers*. No modelo proposto, esse gerador produz novas transações seguindo uma taxa de produção configurável, onde a partir do conhecimento de todos os endereços IP dos nós da rede, a transação é enviada para um subconjunto aleatório contendo n nós. Posteriormente, esses nós selecionados distribuem essa transação pela rede *peer-to-peer* até que todos os nós da rede tenham uma cópia da mesma.

Além dos endereços de todos os nós da rede e do número n de nós para enviar novas transações, o gerador de transações possui parâmetros para definir a frequência média de geração de transações, o valor médio das transações e o tamanho médio do *payload*, simulando a produção contínua de transações diferentes no sistema. Com esses parâmetros, para definir uma transação é necessário que esta possua um identificador

único. Para isso, o gerador utiliza o *hash* do tempo *UTC* de criação da transação concatenado com o endereço do gerador e outros parâmetros relacionados ao *payload*, e esse *hash* é utilizado como o identificador da transação.

Em seguida, o gerador utiliza algumas distribuições aleatórias para determinar o restante dos parâmetros de cada transação individual. Para o tamanho das transações, é utilizada uma distribuição normal uma vez que essa distribuição é capaz de representar diversos fenômenos. Além disso, o Teorema Central do Limite demonstra que, com um grande número de amostras, a distribuição amostral das médias de um fenômeno se aproxima de uma distribuição normal. Para a frequência de criação, o gerador determina o tempo que deve aguardar desde a última transação criada. Para esse fim, é utilizada uma distribuição exponencial negativa uma vez que essa distribuição representa o intervalo de tempo entre dois eventos consecutivos em sistemas que apresentam um comportamento de fila. Para a definição das taxas, foi utilizada uma distribuição exponencial negativa, já que as mesmas são utilizadas apenas para priorizar as transações que devem ser colocadas na blockchain mais rapidamente.

Por fim, a partir destes parâmetros, o gerador passa a utilizar o valor da taxa e o tamanho do *payload* gerados de maneira pseudoaleatória para definir o valor da taxa por byte e o *Payload* da transação. Já os endereços de origem e destino são mantidos como parâmetros fixos para todas as transações, uma vez que eles não têm influencia direta na avaliação de desempenho proposta neste trabalho. Em síntese, as operações do gerador de transações podem ser apresentadas por meio do diagrama apresentado da figura 1.

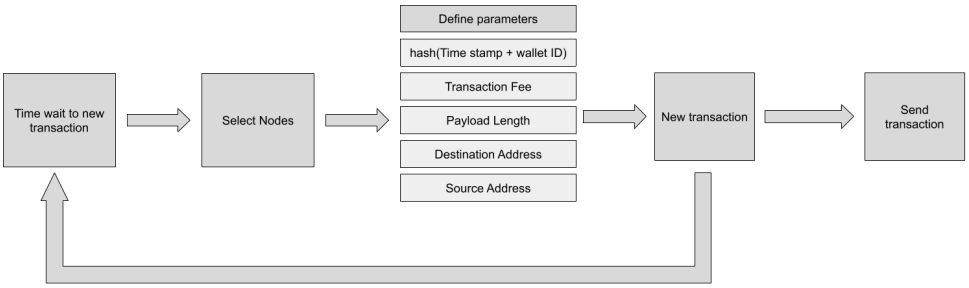

Figura 1. Diagrama de funcionamento do gerador de transações.

Com a introdução de transações na rede, as operações realizadas pelos nós são alteradas consideravelmente durante a execução do novo mecanismo de consenso. De maneira geral, o nó precisa de um protocolo de recepção de novas transações e compartilhamento das mesmas na rede. Além disso, será necessário para o nó a manutenção de uma base de dados local que conterá as transações pendentes da rede. Por fim, é necessário estabelecer as operações realizadas com as transações, ou seja, utilizá-las na construção dos blocos e armazená-las na blockchain juntamente com os blocos.

3.4. Base de dados de transações (*mempool*)

Em uma *blockchain* real, o *mempool* é uma estrutura descentralizada onde cada nó armazena temporariamente as transações recebidas dos usuários. Assim, pode haver diferenças em relação a quais transações estão presentes em cada *mempool* de cada nó da rede. Cada nó seleciona em seu *mempool* transações para compor um novo bloco, realizando a gerência dessas transações. Por outro lado, existem situações em que os nós não têm um

mempool próprio, compartilhando um *mempool* com um conjunto de outros nós. No modelo de testes de avaliação de desempenho aqui proposto, todos os nós são elementos independentes, têm seus próprios *mempools* e realizam as mesmas operações, simplificando o funcionamento e os testes. Dessa forma, o *mempool* é uma nova funcionalidade implementada em todos os nós da rede da mesma maneira, armazenando todas as transações recebidas da rede pelo compartilhamento entre seus pares.

Na prática, o *mempool* é armazenado localmente em cada nó como um banco de dados específico e, para garantir que o nó sempre tenha transações disponíveis para inserir nos blocos, cada *mempool* é populado antes dos testes com um número de transações suficiente para garantir que existam transações disponíveis durante a execução do protocolo.

3.5. Protocolo de mineração do nó.

Para realizar a construção dos blocos considerando as transações presentes na rede, os nós precisam incluir um novo conjunto de operações durante o desenvolvimento das rodadas. No novo mecanismo, para definir um único bloco vencedor na rodada, algumas condições são estabelecidas para que o bloco escolhido seja o mesmo para todos os nós que estão sincronizados com a rede. Considerando que o bloco respeite as condições de aceitação estabelecidas, o bloco vencedor deve atender uma das seguintes condições: possuir a menor rodada dentre todos os candidatos ou, se possuir uma rodada igual ao bloco com menor rodada dentre os candidatos, possuir o menor *hash* de prova [Martins 2020].

Considerando as condições de seleção do melhor bloco, é estabelecido o parâmetro *bestblock*, responsável por representar em um dado momento o melhor bloco e todas as suas transações no decorrer de uma rodada. Para isso, ao longo de todo o período de uma rodada, para todo bloco válido recebido, o nó avalia se este bloco atende alguma das condições de aceitação estabelecidas e decreta se este bloco será ou não o novo *bestblock*. Realizando essa operação para todos os blocos recebidos durante uma rodada, o parâmetro *bestblock* conterá o bloco vencedor desta rodada no início da rodada seguinte.

Com um mecanismo de seleção do melhor bloco de uma rodada, os nós são capazes de inserir e confirmar as transações selecionadas na blockchain. Para isso, foi criada uma nova tabela *transactions_block* responsável por armazenar todas as transações confirmadas na rede e associá-las a seus respectivos blocos. Considerando que não ocorrerão reversões de blocos já inseridos na blockchain no modelo apresentado, no início de uma rodada as únicas operações necessárias são: inserir as transações presentes no *bestblock* nesta tabela definitiva, remover tais transações da *mempool* local e remover o conteúdo do parâmetro *bestblock* a fim de prepará-lo para a próxima rodada. É possível acompanhar as etapas apresentadas no diagrama da Figura 2.

Nesse diagrama, é possível notar as operações realizadas em uma rodada r de acordo com o bloco vencedor da rodada $r - 1$. Nota-se que as operações que atualizam a visão da blockchain de acordo com os eventos da rodada $r - 1$ ocorrem logo no início da rodada r. Em seguida, ocorrem as operações padrão de criação e divulgação de blocos do mecanismo, utilizando as transações da *mempool*. De maneira paralela, os blocos produzidos em toda a rede são candidatados a *bestblock* e, por fim, o bloco vencedor da rodada r e suas transações são inseridos na blockchain no início da rodada $r + 1$.

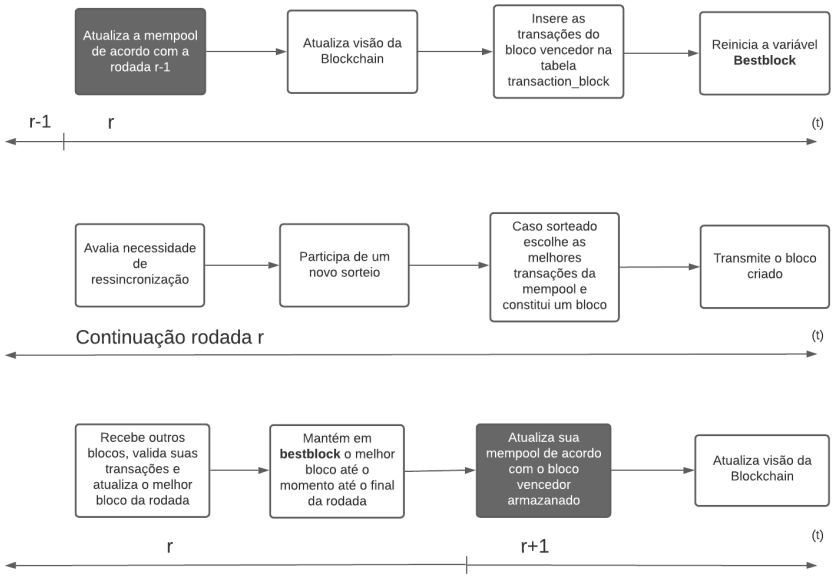

Figura 2. Diagrama de operações no nó durante uma rodada.

3.6. Estrutura da rede e testes

Considerando todos os conceitos apresentados, é possível determinar a estrutura geral da rede utilizada para testar o novo mecanismo de consenso em uma infraestrutura mais próxima a de uma rede real. Como é possível observar na Figura 3, a rede adotada possui dois tipos de entidades responsáveis por operações na rede: o nó participante do consenso, responsável por fazer as operações no novo mecanismo como, por exemplo, compartilhar blocos e transações recebidos da rede, manter uma cópia completa dos registros da blockchain e administrar um *mempool* local. Além deste nó, temos o gerador de transações que seleciona alguns nós para que as transações produzidas sejam enviadas.

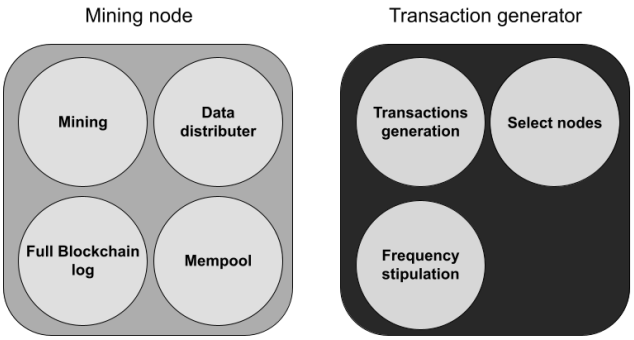

Figura 3. Entidades presentes na rede e suas funcionalidades.

A partir destes dois tipos de nós, é possível modelar um exemplo para demostrar a estrutura da rede (Fig. 4). Nessa figura, é possível observar a presença de um gerador de transações que possui dois canais de envio de transações que mudam a cada transação criada (o gerador não recebe informações dos nós) e seis nós mineradores que realizam conexões do tipo *peer-to-peer* com dois outros nós da rede.

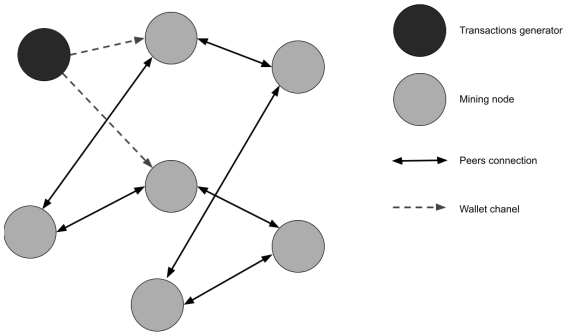

Figura 4. Estrutura da rede com as entidades apresentadas.

O novo modelo de teste viabiliza avaliações mais precisas do novo mecanismo de consenso proposto em [Martins 2021]. Para isso é necessária a utilização de uma rede distribuída geograficamente. Foram feitos testes preliminares, que mostraram um funcionamento adequado dos elementos da rede com as operações descritas enquanto produzem blocos e participam do consenso. Porém, para testes em maior escala, surgiram limitações relacionadas ao banco de dados utilizado (SQLite3), visto que o sistema passou a demandar a manipulação de um maior volume de dados. Por esse motivo, o banco está sendo substituído por outro mais robusto (MySQL) e várias partes do código estão sendo modificadas para fins de compatibilidade com o mesmo.

4. Conclusões e trabalhos futuros

A realização de testes utilizando a estrutura exposta com uma carga alta em redes descentralizadas, com espaçamento geográfico e com vários nós operando de maneira simultânea provê dados mais precisos sobre o comportamento do mecanismo de consenso em situações de sobrecarga. Assim, é possível avaliar seu desempenho em um contexto mais próximo de aplicações reais e identificar casos de uso mais adequados e promissores para a aplicação de um mecanismo de consenso probabilístico sem comitês de validação.

Referências

Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the Open Blockchain*. O'Reilly, 2 edition.

Bashir, I. (2018). *Mastering Blockchain Second Edition*. Packt Publishing, 2 edition.

Fischer, M. J., Lynch, N. A., and Paterson, M. D. (1985). Impossibility of distributed consensus with one faulty process. *Journal of ACM*, 32(2):374–382.

Lamport, L., Shostak, R., and Pease, M. (1982). The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401.

Martins, D. F. G. (2021). *Um novo mecanismo de consenso probabilístico para blockchains públicas*. Unicamp, Campinas, SP. Dissertação de Mestrado, FEEC.

Martins, D. F. G; Henriques, M. A. A. (2020). Avaliação da incidência deforksno algoritmo de consenso probabilistic proof-of-stake (ppos). In *XXXVIII SimpósioBrasileiro de Redes de Computadores e Sistemas Distribuídos - Blockchains Workshop*, Rio de Janeiro - RJ. Sociedade Brasileira de Computação.