DI/FCT/UNL
Mestrado Integrado em Engenharia Informática

Confiabilidade de Sistemas Distribuídos
2º Semestre, 2015/2016

Teste de Avaliação nº 1 (22/Abril/2017) T1-A
Componente: Teste da Parte Teórica

PARTE I (Sem Consulta, 30 min)

Questão 1

Comente a seguinte afirmação: "Um sistema que tolere f falhas bizantinas consegue resistir a ataques de hackers que tomem o controlo de f máquinas do sistema".

Questão 2

Porque é que no Paxos, um *acceptor* tem de aceitar sempre uma proposta com um *prepare number* superior ao anteriormente aceite? Apresente um *run* em que mostre e argumente tal ser necessário.

Questão 3

No algoritmo PBFT, indique o que é que impede um primário bizantino de executar operações que não tenham sido propostas por um cliente.

Questão 4

O protocolo do *Bitcoin* pode ser visto como implementando um sistema de replicação de máquinas de estado tolerante a falhas bizantinas. Quando um nó gera um novo bloco contendo um conjunto de transações, é seguro considerar que essas transações são definitivas? Justifique.

Questão 5

Comparando um algoritmo de consenso probabilístico com um algoritmo de consenso determinístico, quais das seguintes propriedades são definidas de forma diferente e em que consiste a diferença ?
(a) Validade (b) Terminação (c) Acordo e (d) Integridade

PARTE II (Com Consulta, 1h)

Questão 5

Considere o protocolo Paxos usado para executar replicação de máquina de estados num modelo de falhas fail-stop (em que cada réplica mantém um número de sequência com a última operação executada na réplica).

Para executar uma operação de leitura com semântica de atomicidade (*linearizability*) é suficiente enviar a operação de leitura para um quórum de réplicas e retornar ao cliente o valor da réplica com maior número de sequência? Justifique.

Questão 6

Considere a primeira fase da operação de leitura do protocolo ABD Tolerante a Falhas Bizantinas:

```
- Step 1:
Send( <read(nonce)>) to all processes (or to a quroum)
Wait for a quorum Q of valid replies (with nonce and authenticated) Let
<tagmax,valmax,sigmax> ∈ Q be the reply with largest tagmax
```

Porque é que é correto escolher o valor com a maior *tag*, mesmo que esse valor seja retornado por apenas uma réplica? Justifique.

Questão 7

Considere o protocolo PBFT. Explique brevemente porque é que uma réplica não pode executar uma operação após receber 2f(+1) prepares. Apresente um *run* em que após uma réplica receber 2f(+1) prepares, ao contactar 2f+1 réplicas, uma maioria vai indicar que não fez prepare.

NOTA: 2f(+1) prepares significa 2f prepares mais o *pre-prepare* do primário.

Questão 8

Considere o algoritmo de consenso probabilístico Ben-Or. Explique em que condições, durante a execução do protocolo, aumenta a probabilidade de obter o consenso.

Questão 9

O protocolo do Bitcoin pode ser visto como mantendo uma base de dados contendo uma sequência de transações e fornecendo apenas uma operação para adicionar uma nova transação (ou sequência de transações) no fim da lista.

a) Explique como se verifica, numa transferência de A para B, que A tem o valor a transferir.
b) Discuta porque é interessante criar um novo par de chaves assimétricas sempre que se pretende receber uma transferência.
c) Suponha que se substituía o mecanismo de geração de uma nova chave por um mecanismo computacionalmente leve (e rápido). Quais as implicações no funcionamento do sistema, em particular, na consistência do sistema.