Guia do TCC

Gerenciamento do 5G Core com DLT permissionada: validação e auditoria de operações

Dos fundamentos ao plano de experimento, alinhado ao draft ITU-T Y.DLT.Trust.IMT

Item	Situação
Versão	2.0 · novembro de 2026 (substitui a versão de 29/09/2026)
Tema	Integração entre o gerenciamento do núcleo 5G e uma DLT permissionada para validação e auditoria de operações de rede
Base normativa	Draft new Recommendation ITU-T Y.DLT.Trust.IMT, documento de saída da reunião da Questão 16/13 (Seul, 18–25/08/2026). **Não é recomendação aprovada.**
Resultados	Nenhum experimento foi executado ainda. Números citados vêm de artigos, com a fonte indicada.

Como ler este guia
Cada afirmação está em um de três tipos. **Fato**: vem do draft, de uma especificação ou de um artigo, com a fonte indicada. **Interpretação**: leitura feita para o TCC, que pode ser discutida. **Proposta**: decisão de projeto ainda em aberto, a confirmar com o orientador. As caixas verdes trazem fatos; as azuis, propostas; as laranja, cuidados.

Parte	Conteúdo
1–3	Fundamentos: redes, 5G Core e SBA, DLT e Hyperledger Fabric
4	O draft ITU-T Y.DLT.Trust.IMT e onde o TCC se encaixa
5–7	Pergunta de pesquisa, arquitetura proposta e modelo de ameaças
8	Plano de avaliação: cenários, métricas e laboratório
9–11	Referências do acervo, decisões para a orientação e glossário

1. Fundamentos de redes que o TCC usa

O trabalho não exige dominar toda a área de redes. Exige entender bem quatro ideias, porque elas aparecem em cada decisão do protótipo.

Conceito	O essencial	Por que importa no TCC
Cliente e servidor	Um lado pede, o outro responde. Uma requisição pode falhar, demorar ou ter resultado desconhecido.	O adaptador precisa tratar os três casos, não só o sucesso.
IP e porta	O IP identifica a máquina; a porta, o serviço dentro dela.	Cada função do core, o adaptador e cada nó do Fabric têm seu endereço e porta.
TCP e UDP	TCP entrega em ordem e retransmite; UDP envia sem garantia.	As APIs do core e o Fabric usam TCP. O tráfego do usuário no túnel GTP-U usa UDP.
HTTP/2, REST e JSON	HTTP/2 multiplexa várias requisições numa conexão; REST usa verbos (GET, PUT, POST, PATCH, DELETE); JSON é o formato das mensagens.	As funções do 5G Core conversam exatamente assim. É o que o adaptador vai observar ou intermediar.

Idempotência é um conceito extra que vale aprender cedo: uma operação é idempotente quando repeti-la produz o mesmo efeito que executá-la uma vez. O registro de uma função no NRF usa PUT com o identificador da instância, que é idempotente por definição do HTTP. Isso será central para tratar repetições e falhas (seções 6 e 7).

2. O 5G Core e a arquitetura baseada em serviços

2.1 Do 4G ao 5G, sem exageros

A virtualização de funções de rede (NFV) já começou na era do 4G. A mudança do 5G Standalone é de arquitetura: o núcleo passa a ser um conjunto de **funções de rede (NFs)** em software, que se comunicam por APIs HTTP/2. É a **Service-Based Architecture (SBA)**, definida pelo 3GPP. Isso facilita executar o core em containers e nuvem, mas não elimina hardware dedicado em toda a rede: rádio e partes do plano de usuário continuam exigindo desempenho específico.

Fato · metas do IMT-2020 (ITU-R M.2410)
eMBB: pico de 20 Gbit/s no downlink. URLLC: latência de 1 ms no plano de usuário e alta confiabilidade. mMTC: 1 milhão de dispositivos por km². São **metas mínimas de desempenho do sistema**, não garantias de uma rede comercial.

2.2 Planos de controle, gerenciamento e usuário

Esta separação é a base do argumento de que a DLT não atrasa o tráfego dos usuários.

Plano	O que faz	Relação com a DLT
Usuário	Transporta os dados dos usuários. Função principal: UPF.	Nenhuma. Pacotes nunca passam pelo ledger.
Controle	Registro e descoberta de NFs, autenticação, sessões, mobilidade (NRF, AMF, SMF, AUSF…).	Só se o TCC escolher uma operação deste plano (Opção B, seção 5).
Gerenciamento	Configuração, ciclo de vida de NFs/VNFs, slices, regras SDN (orquestradores, MANO).	É o foco do draft ITU-T (seção 4).

Cuidado
“A DLT não está no plano de usuário” é verdade, mas não basta. Se o adaptador exigir confirmação do ledger **antes** de uma operação de controle, ele atrasa essa operação. Por isso o TCC mede o custo (seção 8) em vez de presumir que ele é zero.

2.3 As funções que mais importam

NF	Papel	Interesse para o TCC
NRF	Repositório: cada NF se registra e é descoberta por ele.	Candidata natural para a Opção B. Operação NFRegister: PUT `/nnrf-nfm/v1/nf-instances/{nfInstanceID}` (3GPP TS 29.510).
SCP	Proxy opcional por onde podem passar as chamadas entre NFs.	Ponto possível para observar eventos sem alterar o código do core. Interpretação, a validar.
AMF / SMF	Acesso e mobilidade / sessões PDU do usuário.	Eventos frequentes e com dados pessoais: exigem cuidado de privacidade.
NSSF	Seleção de network slice (S-NSSAI).	Relaciona-se ao gerenciamento de slices do draft (8.4).
UPF	Encaminha o tráfego do usuário.	Fora do escopo da DLT.

Network slicing divide a mesma infraestrutura em redes lógicas com requisitos diferentes. Atenção para não confundir **criar ou alterar um slice** (operação de gerenciamento, coberta pelo draft) com **abrir uma sessão de usuário dentro de um slice** (operação de controle).

3. DLT permissionada e Hyperledger Fabric

Uma **DLT** é um registro de transações replicado entre nós de organizações diferentes, que só aceita novas entradas segundo regras de consenso. Cada bloco referencia o hash do anterior, então alterar o histórico é **detectável**. Isso não torna o passado "impossível de mudar": se as entidades que controlam a rede conspirarem, a garantia acaba. O valor está em dar a participantes que não confiam integralmente uns nos outros um histórico que nenhum deles altera sozinho.

Critério	Pública (ex.: Ethereum)	Permissionada (ex.: Hyperledger Fabric)
Participação	Aberta	Só organizações identificadas por certificados
Consenso	Prova de participação (o Ethereum deixou a prova de trabalho em 2022)	Ordenação por serviço de ordering com Raft, tolerante a falhas por parada
Custo por transação	Taxa (gas) paga em criptomoeda	Sem criptomoeda; custo é a infraestrutura
Privacidade	Dados visíveis a todos	Canais e coleções privadas; acesso controlado
Latência	Segundos a minutos por confirmação	Depende de configuração e carga; precisa ser medida no seu ambiente

3.1 Como uma transação acontece no Fabric

O Fabric usa o modelo **executar → ordenar → validar**:

1. Endosso peers executam o chaincode e assinam o resultado → **2. Ordenação** o ordering service agrupa transações em blocos → **3. Validação** cada peer confere política de endosso e conflitos de versão → **4. Commit** bloco gravado; transação marcada válida ou inválida

Componente	Função
Peer	Guarda o ledger e executa chaincode.
Orderer	Ordena transações e forma blocos (Raft).
CA / MSP	Emite e reconhece identidades; define quem pertence a cada organização.
Canal	Ledger separado entre um subconjunto de organizações.

Componente	Função
Chaincode	Smart contract do Fabric: valida a entrada e grava o estado.
Fabric Gateway	API para aplicações clientes. SDKs documentados: Go, Node.js e Java.

Cuidado · avaliar não é gravar
`Evaluate` consulta um peer e não altera o ledger. `Submit` envia a transação, mas ela só vale depois do commit, que pode marcá-la como inválida (por exemplo, por conflito de versão). O adaptador precisa acompanhar o status do commit; receber a transação não significa ter gravado a evidência.

Fontes: documentação do Hyperledger Fabric (Gateway e fluxo de transações).

4. O draft ITU-T Y.DLT.Trust.IMT

Fato · identificação do documento
Título: Requirements for DLT-enabled trustworthy network management in IMT-2020 and beyond. Documento de saída da Questão 16/13 do ITU-T SG13 (Seul, 18–25/08/2026), baseado na contribuição C96. Editores: João Zanon e José Umberto Sverzut (Anatel), Eduardo Alchieri e Priscila Solis (UnB). É um **draft**: o texto ainda pode mudar e não deve ser citado como recomendação aprovada.

O draft define **requisitos** (o que componentes de gerenciamento devem suportar), não uma implementação. Ele é organizado em requisitos gerais e em três áreas de gerenciamento:

Cláusula · pág.	Requisitos (resumo fiel)	Pergunta para o TCC
8.1 Gerais · pp. 9–10	8.1.1 integrar-se a DLTs · 8.1.2 governança de papéis, permissões e participação · 8.1.3 não degradar operações sensíveis a latência além de limites aceitáveis · 8.1.4 operar de forma escalável	Qual atraso é aceitável? Quem concede e revoga permissões?
8.2 SDN · p. 10	Controle descentralizado; regras de fluxo registradas de forma imutável; ações rastreáveis; integridade entre planos; smart contracts opcionais	A evidência permite reconstruir quem alterou uma regra?
8.3 NFV · p. 11	8.3.1 operações de ciclo de vida de VNF autenticadas por registros de identidade e autorização na DLT · 8.3.2 operações registradas de forma imutável · 8.3.3 resiliência · 8.3.4 smart contracts opcionais	Qual etapa do ciclo de vida é autorizada e qual resultado é confirmado?
8.4 Slicing · pp. 11–12	8.4.1 operações de ciclo de vida de slice autenticadas via DLT · 8.4.2 registradas de forma imutável · 8.4.3 coordenação de recursos por consenso · 8.4.4 compartilhamento transparente (recomendado) · 8.4.5 smart contracts opcionais	Como relacionar pedido, alteração e evidência?

Fonte: versão local do draft, páginas físicas do PDF. Estrutura: cláusula 7 (visão geral, Figuras 1 e 2) nas pp. 6–8; cláusula 8 (requisitos) nas pp. 9–12; cláusula 9 (segurança) nas pp. 12–13; bibliografia na p. 14.

Palavra-chave (cláusula 5)	Significado no draft
are required to	Requisito obrigatório para declarar conformidade
are recommended to	Recomendado, mas não obrigatório
can optionally	Opcional, sem implicar recomendação. É o caso de todos os smart contracts (8.2.5, 8.3.4, 8.4.5)

Fato · o que o draft deixa fora do escopo
A cláusula 9 (pp. 12–13) declara fora do escopo a segurança interna das plataformas DLT: consenso, primitivas criptográficas, gestão de chaves e ataques contra a própria infraestrutura DLT. O draft trata a DLT como tecnologia habilitadora. Isso apoia o modelo de ameaças da seção 7: o TCC também não precisa provar a segurança do Fabric, só declarar a premissa.

Interpretação · os dois pilares do TCC já estão no draft
Pilar 1, validação ≈ REQ-8.3.1 e REQ-8.4.1: operações autenticadas e autorizadas por registros mantidos na DLT. **Pilar 2, auditoria** ≈ REQ-8.2.2, 8.3.2 e 8.4.2: operações registradas de forma imutável. O REQ-8.1.3 justifica medir o custo de latência. Citar esses números dá ao trabalho uma ligação direta e verificável com o draft.

Cuidado
O draft fala de controladores SDN, NFV-MANO e orquestradores de slice. **Ele não cita NRF, AMF ou SMF.** Usar o NRF é uma interpretação legítima do trabalho, mas deve ser apresentada como escolha do TCC, não como exigência do draft.

5. Pergunta de pesquisa e recorte

Proposta · pergunta de pesquisa
Em que medida uma DLT permissionada melhora a verificabilidade e a rastreabilidade de operações de gerenciamento do núcleo 5G entre organizações que não confiam integralmente umas nas outras, e qual é o custo dessa integração em latência e recursos?

Hipótese (a testar, não presumida): um registro compartilhado entre organizações permite detectar alteração do histórico que um log centralizado não detecta, a um custo de latência mensurável e possivelmente aceitável para operações de gerenciamento.

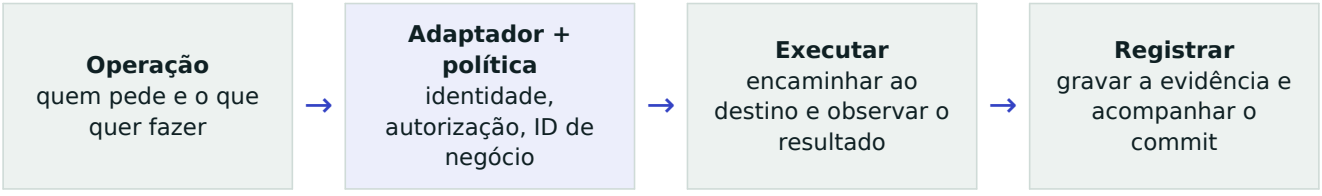
Uma operação. Um risco. Uma medida. Para caber num TCC, escolha **um** fluxo principal:

	Opção A · seguir o draft	**Opção B · função do core**
Exemplo de operação	Implantar, escalar ou encerrar uma VNF; criar ou alterar um slice	Registrar uma NF no NRF (NFRegister)
Ligação com o draft	Direta: REQ-8.3.x ou 8.4.x	Indireta: interpretação dos requisitos gerais 8.1.x
Ferramentas	Orquestrador ou MANO de teste (mais complexo)	Open5GS ou free5GC + UERANSIM (mais simples)
Risco principal	Montar o orquestrador consome o tempo do TCC	Banca questionar a aderência ao draft

A escolha entre A e B é a primeira decisão a levar ao orientador (seção 10).

6. Arquitetura proposta

O núcleo do protótipo é um **adaptador** entre quem pede a operação, o destino (core ou orquestrador) e o ledger.



6.1 Ciclo de uma operação

1. Receber a operação e verificar identidade, autorização e identificador de negócio.
2. Persistir a intenção, conforme a política escolhida (abaixo).
3. Encaminhar ao destino e observar sucesso, falha ou resultado desconhecido.
4. Registrar o resultado no ledger e acompanhar o status de commit.

5. Reconciliar pendências sem executar de novo uma operação já concluída.

6.2 Duas políticas, com custos diferentes

	Estrita	Assíncrona
Como funciona	Exige confirmação no ledger antes de executar	Autoriza com política local e audita depois, por fila durável
Ganho	Nenhuma operação sem evidência prévia	Latência da operação quase igual à original
Custo	Soma a latência do commit à operação; ledger fora do ar bloqueia o gerenciamento	Janela em que a operação já ocorreu e a evidência ainda não; exige reconciliação

Correção em relação à versão 1
A versão anterior dizia que a DLT atua “estritamente de forma assíncrona” e, ao mesmo tempo, que valida “antes de executar”. As duas coisas não valem juntas: validar antes é o modo estrito. O TCC deve escolher a política, ou comparar as duas.

6.3 O que fica dentro e fora do ledger

No ledger (on-chain)	Fora do ledger (off-chain)
ID do evento, tipo de operação, origem, horário, resultado, hash do conteúdo, referência ao registro anterior	Payload completo, logs detalhados, dados pessoais. Ficam em armazenamento próprio; o hash prova que não foram alterados

Cuidado · privacidade e LGPD
Gravar o hash de um IMSI/SUPI **não** anonimiza o dado. O espaço de IMSIs é pequeno o bastante para descobrir o original por força bruta, então o hash simples continua sendo dado pessoal. Prefira não registrar identificadores de assinante. Se for necessário correlacionar, use um identificador derivado com chave secreta (HMAC) mantida fora do ledger, e documente a decisão.

Exemplo de registro (dados fictícios):

```
{ "eventId": "evt-0001", "source": "orquestrador-org1", "operation": "NF_REGISTER", "timestamp": "2026-12-01T14:00:00Z", "payloadHash": "sha256:af3c…", "result": "SUCCESS" }
```

7. Modelo de ameaças

A DLT protege a **integridade do histórico**. Ela não protege contra tudo, e o trabalho fica mais forte quando diz exatamente o que fica de fora.

Risco	Condição para acontecer	Teste proposto / limite
Contornar o adaptador	O atacante alcança a API do destino diretamente, com credenciais aceitas	Testar as rotas autorizadas. A DLT não fecha caminhos alternativos.
Repetir um evento	Uma requisição válida é reenviada e a aplicação não controla duplicatas	Reenviar o mesmo ID de negócio e exigir resultado idempotente.
Fonte comprometida	Um emissor autorizado produz informação falsa	Integridade do registro não prova a verdade do conteúdo. Declarar o limite.
Perder evidência	O destino conclui a operação e o adaptador cai antes de registrar	Interromper nessa janela; verificar fila durável, reconciliação e alerta de pendência.
Abuso de administração	Chaves suficientes da governança são comprometidas	Explicitar o limite de confiança; não prometer resistência a controle total do consórcio.

8. Plano de avaliação

8.1 Três cenários para uma comparação justa

Cenário	O que mede
A · operação sem adaptador	Custo original
B · adaptador + log convencional	Custo da validação e da auditoria centralizada
C · adaptador + DLT	Custo e benefício adicionais do ledger

Sem o cenário B, não dá para separar o custo do adaptador do custo do ledger. B e C devem aplicar a mesma regra de autorização. Fixe hardware, versões, payloads e taxa de chegada; separe aquecimento, repetições e falhas.

8.2 Métricas

Métrica	Definição operacional	Cuidado
Latência p50/p95/p99	Da chegada ao adaptador até a resposta ao cliente	No modo assíncrono, medir a confirmação do ledger separadamente
Operações e commits por segundo	Sucessos no destino e registros válidos no ledger, em janelas iguais	Taxa de envio não é taxa de conclusão; não descartar falhas
Pendências de auditoria	Tamanho da fila e idade do evento mais antigo sem confirmação	Resposta rápida pode esconder acúmulo
Correção	Pedidos indevidos negados, duplicatas evitadas, evidências reconciliadas	Definir antes quais entradas são válidas
Custo operacional	CPU, RAM, armazenamento e tempo de recuperação após falha	Medir o adaptador isoladamente
Detecção de adulteração	Alterar um registro off-chain e verificar se o hash denuncia	Teste qualitativo, mas essencial para o pilar 2

Fato · ordem de grandeza na literatura do acervo
Num testbed 5G SA com Open5GS e srsRAN, um artigo do IEEE ICC 2026 relata 1–4 ms a mais na latência fim a fim e commit de bloco de cerca de 250 ms (linha 4 da exportação IEEE em `export2026.10.21-11.52.16.csv`). Um estudo com OpenDaylight e smart contracts relata o registro de política passando de 45 ms para 210 ms (linha 208). São referências para comparar, não resultados deste TCC.

8.3 Laboratório planejado

Proposta: ambiente local, isolado e descartável, com dados fictícios: Open5GS ou free5GC, UERANSIM (gNB e UE simulados), Fabric test network com duas organizações e ordering Raft, o adaptador e Prometheus para as métricas, em Docker Compose. A ideia é começar com um destino simulado para validar política, idempotência e reconciliação, e só depois ligar ao core.

Critério de avanço: antes de ampliar a topologia, demonstrar o ciclo completo de uma operação autorizada, uma negada e uma falha recuperável. Uma rede de teste mínima não demonstra disponibilidade de produção.

9. Referências do acervo e como usá-las

Referência	Use para
Zanzi et al. (2020). NSBchain. IEEE TNSM / arXiv:2003.07748	Implementação com Fabric e Raft; métricas de latência e conflitos MVCC
Xiao et al. (2021). SLA audit scheme. EURASIP JWCN 2021:165	Auditoria de SLA de slices com preservação de privacidade
Boukessessa et al. (2024). VNF package protection. Transport and Telecommunication 25(3)	Validação de pacotes VNF e defesa anti-replay (ligação com 8.3)
Nguyen et al. (2020). Blockchain for 5G and beyond. IEEE COMST / JNCA 166	Fundamentação teórica e taxonomia
Rahman et al. (2022). Blockchain and SDN. JNSM 30:73	Controle SDN distribuído (ligação com 8.2)
Tahir et al. (2020). Blockchain in 5G: field-trials. IEEE Access 8	Casos de operadoras e testes em campo
Liu et al. (2024). Blockchain and 6G. PLoS ONE 19(4)	Consenso em DAG, sharding e armazenamento off-chain
Chaer et al. (2019). Blockchain for 5G: opportunities and challenges	Oráculos, IPFS e fluxos de slicing
Kalla et al. (2022). Blockchain for future 6G. J. Ind. Inf. Integration 30	Governança multi-operadora e ETSI ZSM
3GPP TS 29.510 (ETSI TS 129 510 v18.8.0)	Operação NFRegister do NRF
ITU-R M.2410	Metas de desempenho do IMT-2020
Documentação do Hyperledger Fabric	Gateway, fluxo de transações, ordering Raft

Cuidado · arquivo divergente no acervo
O arquivo legado `referencias/Boukessessa2024_Blockchain_VNF_Package_Protection.pdf` contém outro artigo (Hadi et al., estações de recarga de veículos elétricos). Cite Boukessessa a partir do arquivo `03_Boukessessa_2024_VNF_Protection_AntiReplay.pdf`. Detalhes nas fichas de estudo do painel.

10. Decisões para levar à orientação

Em vez de respostas prontas, leve as decisões que só o orientador pode ajudar a fechar:

#	Decisão	Opções ou critério
1	Qual operação representa o problema?	Opção A (VNF/slice, aderente ao draft) ou B (NRF, mais simples de montar)
2	Quais organizações não confiam integralmente entre si?	Sem essa resposta, não há motivo para uma DLT em vez de um log
3	Quanto atraso e indisponibilidade são aceitáveis?	Define a política estrita ou assíncrona (REQ-8.1.3)
4	Qual teste poderia refutar a hipótese?	Ex.: o cenário C não detecta nada que o B não detecte
5	Core de referência	Open5GS ou free5GC; fixar versão
6	O que fica on-chain	Somente metadados e hash; sem identificador de assinante

Proposta · abertura da conversa
“Professor, estruturei o TCC sobre o draft Y.DLT.Trust.IMT. A ideia é um adaptador que valida e registra uma operação de gerenciamento numa DLT permissionada, ligando os pilares aos requisitos 8.x.1 e 8.x.2, e medir o custo comparando três cenários: sem adaptador, com log convencional e com DLT. Preciso da sua ajuda para fechar qual operação usar e qual atraso é aceitável.”

11. Glossário

Termo	Significado
3GPP	Consórcio que especifica as redes móveis (3G, 4G, 5G)
ITU-T / SG13	Setor de padronização da UIT; Study Group 13 trata de redes futuras
IMT-2020	Nome da UIT para o sistema 5G
SBA	Arquitetura do 5G Core em que as NFs se comunicam por APIs HTTP/2
NF / VNF	Função de rede / função de rede virtualizada
NRF / SCP	Repositório de NFs / proxy de comunicação entre NFs
AMF / SMF / UPF	Acesso e mobilidade / sessões / plano de usuário
NFV-MANO	Gerenciamento e orquestração de funções virtualizadas
S-NSSAI	Identificador de um network slice
DLT	Registro distribuído e replicado entre organizações
Chaincode	Smart contract do Hyperledger Fabric
Peer / Orderer	Nó que guarda o ledger e executa chaincode / nó que ordena transações
MSP / CA	Definição de membros de uma organização / autoridade que emite certificados
Endosso	Execução e assinatura de uma transação pelos peers exigidos pela política
Idempotência	Repetir a operação produz o mesmo efeito que executá-la uma vez
Reconciliação	Conferir pendências entre o que foi executado e o que foi registrado
p95 / p99	Valor abaixo do qual ficam 95% / 99% das medições