Tecnologia *Blockchain* para Auditoria em Redes Móveis

Luiza Odete Herback de Carvalho Macedo[1] **e Miguel Elias M. Campista**[1*]

[1]Grupo de Teleinformática e Automação (GTA-DEL/Poli-PEE/COPPE)
Universidade Federal do Rio de Janeiro (UFRJ)

{luiza,miguel}@gta.ufrj.br

Resumo. *O Sistema de Sinalização nº 7 (SS7) define uma pilha de protocolos usados principalmente na troca de sinalização das redes de provedores de serviço móveis. Originalmente, tais protocolos foram baseados em relações de confiança mútua entre as partes, sem preocupação com segurança de rede. Com o sucesso da Internet e o crescimento do número de operadoras, as redes móveis ficaram expostas a ataques em SS7 que podem levar a problemas de privacidade e até indisponibilidade de serviços.*
Este trabalho propõe o uso da tecnologia blockchain como forma de introduzir auditabilidade e rastreabilidade das operações de rede, servindo como complemento às contramedidas já existentes (p.ex., firewalls). Torna-se possível, portanto, identificar ameaças e determinar o impacto das próprias na rede. A viabilidade da proposta é avaliada através de medições do consumo de recursos computacionais, vazão e latência das transações da blockchain. Os experimentos realizados no Hyperledger Fabric mostram que é possível implantar a tecnologia proposta sem causar grandes impactos a infraestrutura existente na rede da operadora.

1. Introdução

O aumento acelerado do número de dispositivos móveis conectados à Internet tem trazido enormes preocupações aos provedores de serviço quanto a questões de segurança de rede. Uma das razões é o uso legado do SS7 ou Sinalização por Canal Comum nº7, que é uma antiga pilha de protocolos de sinalização usada principalmente para interconexão de redes entre operadoras. Quando o SS7 foi concebido, não se pensava em segurança como hoje, já que as relações entre os provedores de serviço eram mutuamente confiáveis. Atualmente, o reflexo do relaxamento da segurança no projeto do SS7 fica evidente com as muitas ameaças às redes móveis.

O SS7 é uma tecnologia legada das redes móveis 2G/3G. Logo, por impulso, alguém poderia sugerir a completa substituição dessas redes por uma de geração mais atual que não mais utilizaria o SS7. Essa solução, entretanto, está longe de ser alcançada, uma vez que somente em 2018 o 4G ultrapassou o uso do 2G, tornando-se a tecnologia líder das gerações móveis [Intelligence 2019]. Mesmo considerando a inegável tendência de declínio do 2G/3G, a manutenção dessas redes ainda se faz necessária para suporte a aplicações corporativas M2M (*Machine-to-Machine*), utilizadas por exemplo,

*Trabalho realizado com apoio do CNPq; da FAPERJ; da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior Brasil (CAPES), Código de Financiamento 001; e da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), processos nº 15/24494-8 e 15/24490-2.

nas máquinas de cartão de crédito. Sendo assim, o 2G/3G permanece sem data definida de desligamento por parte das operadoras.

O sucessor do SS7 a partir do 4G, o Diameter, ainda apresenta vulnerabilidades para determinados tipos de ataque, como por exemplo, o de rastreamento de usuário [Rao et al. 2016, Tu et al. 2015, Roth et al. 2017]. Ademais, a conversão do SS7 para o Diameter tem sido feita de forma gradual a fim de manter serviços legados, como citado anteriormente. Outro problema é que o LTE não suporta voz nativamente, já que é uma rede puramente baseada em pacotes de dados. Logo, se a operadora não possuir uma rede de núcleo IMS (*IP Multimedia Subsystem*), que dê suporte a chamadas VoLTE (*Voice over Long Term Evolution*), é necessário que haja um rebaixamento de tecnologia para 2G/3G para disponibilização dos serviços de voz [Bautista et al. 2013]. Portanto, mesmo as redes mais recentes de telefonia móvel não estão imunes aos ataques em SS7. Para se ter uma ideia do problema, em uma grande operadora de telecomunicações do Brasil[1], entre dezembro de 2018 e maio de 2019, foram disparados 21.900 ameaças por dia em média contra a operadora com diferentes objetivos. A quantidade e o número de tipos de ataques possíveis indica a vulnerabilidade da rede da operadora.

Este artigo propõe o uso da tecnologia *blockchain* com o objetivo de prover a auditoria da rede móvel, sendo portanto um complemento às contramedidas tradicionais como os *firewalls*. Dessa forma, é possível armazenar informações que não foram bloqueadas em um primeiro momento pelas técnicas tradicionais. A ideia por trás do uso de uma *blockchain* é manter uma forma de registro imutável e transparente para rastreabilidade de operações realizadas na rede. Com isso, torna-se possível o reconhecimento de movimentações suspeitas dentro da rede móvel, bem como a determinação do impacto de um ataque pela supervisão do histórico das ações decorrentes. A *blockchain* proposta considera mensagens SS7 como transações, particularmente mensagens MAP (*Mobile Application Part*) da pilha SS7, usadas em ataques a operadoras móveis. Além disso, a proposta considera ameaças decorrentes de personificação, na qual atacantes conseguem simular um elemento legítimo de rede SS7, e assim, obter informações sensíveis dos usuários ou da própria rede. A *blockchain* proposta é para redes privadas, caracterizadas pelas rede de uma operadora móvel. Ainda, a *blockchain* é permissionada, apesar da rede ser privada, já que esta é suscetível a ameaças externas, como ataques que usem mensagens das categorias 2 e 3 do GSMA [Association 2016]. Isso significa que qualquer indivíduo com recursos necessários pode enviar mensagens MAP verdadeiras à rede, e como consequência, emitir uma transação legítima. Na *blockchain* proposta apenas nós confiáveis (pertencentes à rede da operadora) podem participar dos processos de validação de transações, geração de blocos e algoritmo de consenso. O algoritmo de consenso escolhido é o PoA (*Proof of Authority*), por se tratar de um algoritmo para *blockchain* privadas, além da simplicidade na submissão de blocos e baixo fluxo de mensagens trocadas.

A implantação da *blockchain* proposta em redes móveis é avaliada no *Hyperledger Fabric* através de um contrato inteligente. O contrato inteligente desenvolvido é executado no *Hyperledger Caliper* para realização dos testes de desempenho. Com o *Hyperledger Caliper*, resultados de vazão, latência e recursos computacionais, como o consumo de memória e CPU, são obtidos para quantidade de transações e tamanhos de blocos diferentes [Nasir et al. 2018, Sukhwani et al. 2018, Gorenflo et al. 2019]. Os resultados

[1]Por questões de confidencialidade, não é possível revelar maiores detalhes sobre a operadora.

mostram que é possível implantar a tecnologia proposta sem causar grandes impactos à infraestrutura existente na rede da operadora.

Este trabalho está organizado da seguinte forma. A Seção 2 apresenta os trabalhos relacionados. Já a Seção 3 revisa conceitos de redes celulares, descreve os ataques conhecidos para o sistema de sinalização SS7 e traz resultados de caracterização dos ataques a redes de operadoras. A Seção 4 apresenta a proposta de auditoria para redes móveis usando *blockchain*, enquanto a Seção 5 apresenta experimentais obtidos. Por fim, a Seção 6 faz considerações finais e propõe trabalhos futuros.

2. Trabalhos Relacionados

Algumas iniciativas vêm sendo implementadas para solucionar o problema dos ataques a redes SS7. Rupprecht *et al.* apresentam as características das defesas adotadas contra os ataques em SS7 a partir de uma subdivisão baseada nos principais motivos dos ataques [Rupprecht et al. 2018]. Dentre as contramedidas estão o uso de *firewalls* que bloqueiam as principais mensagens de sinalização utilizadas em ataques já conhecidos; o uso de aplicativos para *Android* para detecção de *"IMSI Catchers"*, dispositivos *"Man-In-The-Middle"* usados por atacantes para simular um elemento móvel e enviar mensagens legítimas para a rede das operadoras [Dabrowski et al. 2014]; e o uso de sistemas de detecção de Estações Rádio Base falsas [Li et al. 2017]. Também foi proposto o uso do protocolo SSL (*Secure Sockets Layer*) para suprir a deficiência de autenticação mútua e de privacidade da comunicação em redes móveis [Kambourakis et al. 2004]. A literatura também apresenta a utilização de técnicas de aprendizado de máquinas para detecção de anomalias na rede SS7 [Jensen et al. 2016], permitindo identificar a ocorrência de um ataque. Essas abordagens, porém, tendem a atacar vulnerabilidades particulares, sem se preocupar com questões de auditoria e armazenamento de informações de uso.

As características inerentes à *blockchain* como transparência, imutabilidade e privacidade têm despertado interesse na resolução de problemas em redes móveis. Babu *et al.* propuseram o uso da *blockchain* como meio de inserção de segurança na rede SS7 [Babu et al. 2018]. Os atacantes aproveitam-se de uma limitação de segurança no canal de comunicação entre o usuário e a estação base, e escutam a transmissão da interface aérea, descobrindo informações de localização do usuário divulgadas via *broadcast*. Ao invés dessa difusão, os elementos de rede seriam inseridos na *blockchain* e utilizariam criptografia com chaves privadas e públicas para a comunicação, na qual somente a chave pública é propagada. Como todas as estações base são nós pertencentes a uma *blockchain* comum, não há necessidade de autenticação do usuário cada vez que este mude de estação base, pois tais informações públicas já são conhecidas por todos os nós através da replicação das informações na própria *blockchain*. Mafakheri *et al.* propuseram o uso da *blockchain* para prover uma forma segura de autenticação e armazenamento de informações de usuários em redes 4G, através da descentralização do banco de dados HSS (*Home Subscriber Server*) [Mafakheri et al. 2018]. Na proposta, os processos de registro e desativação de usuários são feitos através de um contrato inteligente via *blockchain*, ao invés do procedimento normal utilizando o HSS. A ideia é descentralizar as informações dos usuários para que não fiquem dependentes de um único elemento de rede, que é susceptível a falhas. No entanto, o esquema proposto concentra-se na possibilidade de falha ou vulnerabilidade apenas do banco de dados da rede, não se preocupando com requisições legítimas originadas por usuários maliciosos que dispariam ataques

ainda que em um ambiente descentralizado.

A proposta deste trabalho não se baseia em apenas um único tipo de ameaça e também não possui como objetivo a mitigação de ataques. Entende-se que para ser efetivo, o primeiro passo é a auditoria da rede e o conhecimento das mensagens trocadas.

3. Vulnerabilidades do SS7 e Caracterização dos Ataques

A arquitetura tradicional das tecnologias 2G (ou *Global System for Mobile Communications* – GSM) e 3G (ou *Universal Mobile Telecommunication System* – UMTS) é composta por uma rede de acesso e uma rede de núcleo. Ademais, como é comum a interconexão com redes externas, p.ex. redes IP ou redes de telefonia fixa, considera-se por conveniência que as redes externas são um subsistema adicional à arquitetura. A Figura 1 mostra a interconexão entre as redes de acesso e de núcleo da arquitetura 2G/3G, assim como a interconexão com as redes externas.

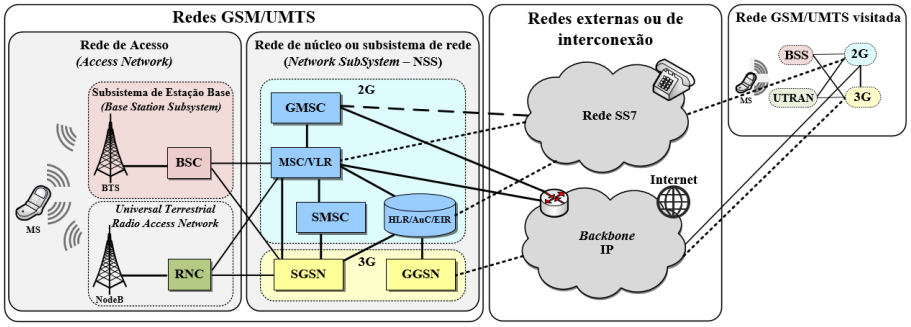

Figura 1. Arquitetura básica de uma rede móvel 2G/3G e interconexões.

A rede de acesso BSS (*Base Station Subsystem*) ou UTRAN (*Universal Terrestrial Radio Access Network*), respectivamente às tecnologias 2G e 3G, é o subsistema que viabiliza a entrada do usuário na rede, provendo a conexão do terminal móvel com os elementos responsáveis pela disponibilização dos serviços de voz e dados. Já a rede de núcleo ou o subsistema de comutação de redes (*Network Switching Subsystem* - NSS) é o responsável por todas as funções de controle assim como as de operação e manutenção, incluindo qualidade de serviços e realização de chamadas. Na Figura 1, os elementos inseridos no retângulo azul pertencem à rede 2G e os que estão no amarelo, fazem parte da rede 3G. Arquiteturalmente, o NSS se subdivide ainda em três componentes principais: central de comutação, bases de dados de usuários e elementos de interconexão, que por falta de espaço não são detalhados.

O SS7 permite que as informações de sinalização e controle trafeguem por um único canal dedicado, deixando livres os canais de voz, o que aumenta o desempenho da rede [Dryburgh and Hewett 2004]. As redes SS7 utilizam uma pilha de protocolos na qual a camada de transferência de mensagens executa as tarefas das camadas física, de enlace e de rede do modelo OSI; enquanto a parte de usuário e de aplicações corresponde às camadas de transporte até aplicação, também do modelo OSI. Apesar do SS7 ser antigo, ainda hoje continua sendo utilizado pelas operadoras para serviços de interoperabilidade, roteamento de chamadas e *roaming*.

3.1. Vulnerabilidades do SS7

As vulnerabilidades do SS7 surgiram em sua origem, já que seu projeto foi baseado em relações confiáveis entre operadoras. Esse cenário, porém, mudou nos últimos anos com a explosão no número de operadoras, principalmente com o advento das operadoras móveis virtuais (*Mobile Virtual Network Operators* - MVNOs). Ademais, a partir das redes IP, o SS7 tornou-se vulnerável, deixando a rede móvel exposta a diferentes ataques [Technologies 2018].

Um dos protocolos mais explorados nos ataques é o MAP (*Mobile Application Part*), definido na camada de aplicação da pilha SS7. O MAP especifica as mensagens de sinalização que são trocadas nos principais procedimentos que ocorrem na rede móvel, sendo responsável pela comunicação intra e inter-núcleo de rede. Como exemplos de suas funcionalidades estão o suporte à mobilidade na rede 2G e 3G (*roaming*) e o suporte a serviços básicos e suplementares de chamadas. Como não há autenticação para a comunicação entre os elementos de rede, qualquer mensagem MAP ou de outro protocolo da pilha SS7 destinada à rede de núcleo móvel ou a algum ponto de sinalização SS7 é respondida, assumindo-se que o emissor é um nó de rede legítimo. Com isso, a rede não diferencia as origens das mensagens MAP recebidas, considerando a mensagem advinda de uma fonte segura e atende às solicitações feitas. Como exemplo de viabilidade de entrada na rede, é possível alugar ou adquirir diretamente um *hub* SS7 que possua acesso à rede da operadora. Esta facilidade é oferecida geralmente para que MVNOs ou pequenas operadoras tenham acesso à rede SS7 de uma grande provedora de serviços de telecomunicações, a fim de permitir a terceirização e extensão de serviços, como *Roaming* e SMS. Um atacante pode comprar este acesso e tornar-se um gerador de mensagens SS7 legítimas à rede.

Além da vulnerabilidade entre os nós de rede, há ainda fragilidade no canal entre o usuário e a rede, onde há apenas autenticação unilateral da estação móvel para a rede e presume-se que a outra parte (estação base) que está solicitando dados para o usuário seja legítima. Um atacante que possua um rádio ativo (chamados de *"Cell-Site simulators"* ou "*IMSI Catcher"*) ou uma caixa DRT (*Digital Receiver Technology*), pode executar um ataque MiM ("*Man-In-The-Middle*"), estabelecendo uma conexão intermediária a fim de obter informações para gerar requisições MAP legítimas à rede. Esse tipo de ataque em que pedidos externos são enviados à rede por meio de elementos falsos é classificado como *"fake Base Stations"* [Rupprecht et al. 2018] ou de personificação de elementos de rede. A partir desse ponto, o atacante pode executar vários ataques, como apresentado adiante.

3.2. Caracterização dos Ataques

Esta seção caracteriza as ameaças as SS7 enfrentadas pelas operadoras de telefonia móvel. Para isso, é feita a análise de um traço de 150 dias (entre 15/12/2018 e 15/05/2019) contendo dados de ameaças a uma rede de um provedor de serviço brasileiro de grande porte. Os dados utilizados foram coletados pela operadora nacional a partir da sinalização SS7 recebida de operadoras internacionais. Para isso, o tráfego de *roaming* internacional foi espelhado para um servidor interno com função de *firewall* de sinalização que fazia a detecção de ameaças em SS7. Nesse *firewall* foram aplicados filtros específicos para identificação das ameaças destinadas à operadora e suas parceiras.

Além disso, foi utilizado um sistema de detecção de mensagens suspeitas de fraude (*IDS – Intrusion Detection System*) que trabalha em conjunto com o *firewall*. No IDS foram criados perfis de classificação de ataques. Essa definição pode ser subjetiva, pois nem todas as classificações correspondem a um ataque de fato, gerando um falso positivo. Portanto, nesta seção, a palavra "ameaça" é usada ao invés de "ataque" e, ao longo deste trabalho, as duas palavras são usadas de forma intercambiável.

A Figura 2(a) mostra a quantidade total de ameaças identificadas durante o período de avaliação. Essa quantidade aproxima-se da média na maior parte do tempo, que é de 21.900 ameaças/dia. Aconteceram picos nos meses de dezembro e março, mais especificamente nos feriados de Natal e Carnaval, provavelmente pela chance de sucesso do atacante ser maior em períodos fora do expediente da operadora ou em períodos de maior uso por parte dos usuários. Ainda, um pico aconteceu entre os dias 17 e 19/03, no qual verifica-se que no dia 18/03, as ameaças chegaram a ser disparadas 118.162 vezes. A escolha de tais datas carece de maiores investigações. Não foi possível identificar a real quantidade de ameaças bem sucedidas, pois essa informação é confidencial.

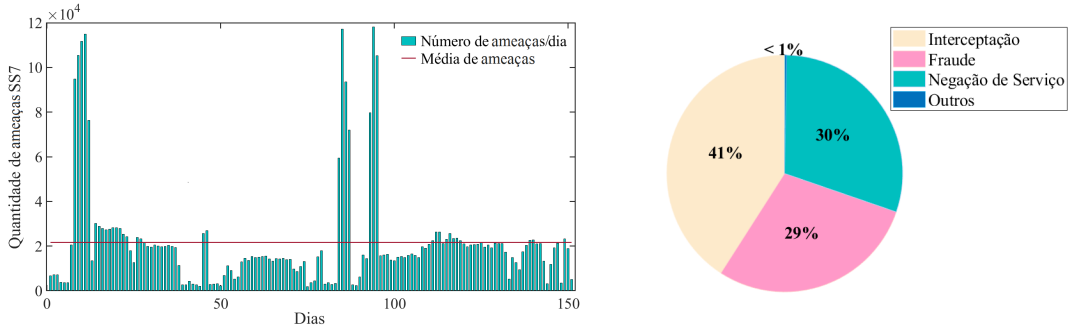

Figura 2. (a) Quantidade de ameaças ao longo do período de observação. (b) Distribuição entre as classes de ameaças encontradas.

A Figura 2(b) mostra as classes de ameaças encontradas nos dados analisados. A classe "Interceptação" é a principal, apresentando 41% do total de ameaças. Nessa classe, a intenção do atacante é ler dados originalmente enviados para outro usuário, como conversas, senhas, SMS's, comprometendo a privacidade dos clientes. Em sequência, com 30% e 29%, encontram-se as classes de "Negação de Serviço" e "Fraude", respectivamente. A Negação de Serviço consiste em interromper o serviço dos assinantes (por exemplo, a realização de chamadas e de SMS) ou tornar algum elemento de rede indisponível. Já a Fraude consiste em obter vantagens financeiras de algum usuário da rede, alterando as configurações de encaminhamento de chamadas de modo que o usuário legítimo arque com os custos das mesmas. Por fim, com menos de 1%, outras classes com menor intensidade são também disparadas contra a rede da operadora. Dentre elas está a classe de "Rastreamento" que consiste em seguir o posicionamento da estação móvel em tempo real.

4. Proposta de Auditoria para Redes Móveis

Este trabalho propõe uma forma de auditoria de redes móveis com foco principal no monitoramento das atividades de possíveis atacantes, sendo um complemento às con-

tramedidas existentes. Nesse contexto, a introdução da tecnologia *blockchain* é proposta, já que permite a verificação de todas as alterações que são feitas na rede e, consequentemente, a identificação dos atacantes e a frequência com que a rede é ameaçada. Tais informações permitem mapear a rede e desenvolver estratégias que mitiguem as ameaças. Para isto, é apresentada uma proposta de auditoria aplicando *blockchain* ao problema de vulnerabilidades em SS7 para as redes móveis.

4.1. Auditoria das redes móveis usando *blockchain*

Com o intuito de verificar preliminarmente a aplicabilidade da solução proposta e mensurar a vazão de transações emitidas na *blockchain*, foi feita a verificação da quantidade de mensagens MAP trocadas na rede. Para isso, a partir dos mesmos dados usados na Seção 3.2, foi selecionado um trecho de 1 hora de duração para extração e contagem do número de mensagens MAP. A Figura 3 exibe o resultado da análise. No pico de mensagens, a quantidade de mensagens atingiu 317 requisições MAP/min, o que em segundos, chegaria a aproximadamente 6 requisições MAP/s. Essa quantidade é atendida tanto por algoritmos de consenso probabilísticos (p.ex., o PoW (*Proof of Work*), que permite o processamento de 7 transações/s [Li et al. 2018]); quanto determinísticos, como os protocolos BFT, que possuem maior escalabilidade devido à pouca quantidade de nós [Vukolić 2015].

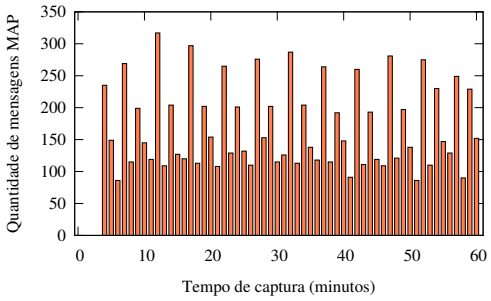

Figura 3. Quantidade de mensagens MAP recebidas na rede da operadora no intervalo de uma hora.

As ameaças de personificação que foram abordadas neste trabalho consistem na intrusão de elementos falsos na rede SS7, ou seja, um usuário malicioso que consegue simular um elemento legítimo de rede e, assim, obter informações sensíveis dos usuários ou da própria rede. Trazendo os conceitos de *blockchain* ao contexto de redes móveis, cada mensagem MAP representa uma *transação*. Portanto, cada pedido MAP (*Request* ou *Response*) independente da fonte, é considerado uma transação. Com o objetivo de promover uma auditoria na rede que permita identificar as ameaças e garantir rastreabilidade das movimentações de rede, idealmente todas as transações MAP geradas são aceitas. A ideia é construir um histórico permanente de todas as operações realizadas na rede. Algumas condições de validação, porém, são estabelecidas. Por exemplo, uma transação somente é aceita caso obedeça os requisitos mandatórios da especificação do 3GPP para o protocolo MAP (isso é, caso seja legítima). Adicionalmente, caso haja alguma transação vazia, sem nenhum conteúdo, a mesma também é descartada. A validação de cada transação é feita localmente em cada nó pertencente ao algoritmo de consenso.

Como pretende-se aplicar a *blockchain* a redes corporativas, governadas por uma instituição, a escolha por redes privadas é a mais adequada. Uma rede de operadora

pode ser caracterizada como privada e distribuída. Ademais, sobre a classificação de permissão, apesar da rede ser privada, esta é suscetível a ameaças externas, já que ainda não existem ferramentas de bloqueio efetivas a mensagens das categorias 2 e 3 do GSMA [Association 2016]. Isso significa que qualquer indivíduo com recursos suficientes pode enviar mensagens MAP verdadeiras à rede, desde que atenda às especificações do 3GPP. Sendo assim, um elemento de rede que emita uma transação legítima torna-se um nó que atende os requisitos da rede. Isso posto, a rede é permissionada, pois assume-se que os nós podem executar papéis distintos. Porém, apenas nós confiáveis (pertencentes à rede da operadora) podem participar dos processos inerentes à tecnologia *blockchain* na rede, como validação de transações, geração de blocos e algoritmo de consenso. Caso componentes do sistema sejam comprometidos (ou seja, nós que deixem de ser confiáveis ou nós maliciosos que entrem no consenso) ou se algum nó passar a agir maliciosamente, é feita uma votação entre os nós para exclusão da autoridade maliciosa [De Angelis et al. 2018]. Como a finalidade é a auditoria da rede, é necessário que o algoritmo de consenso aceite o máximo de transações (idealmente todas), sem descartá-las, para manutenção de um histórico completo das transações submetidas à inserção na *blockchain*. Como algoritmo de consenso, o escolhido foi o PoA, com uma implementação chamada *Clique*, por se tratar de um algoritmo para *blockchains* privadas, com simplicidade na submissão de blocos e baixo fluxo de mensagens trocadas na rede.

4.2. Consenso com PoA

Os algoritmos de consenso aplicáveis a redes públicas, como o PoW e o PoS (*Proof of Stake*) foram descartados para aplicabilidade no problema, visto que o modelo adotado é o de redes privadas. Angelis *et al.* comparam os algoritmos de consenso PBFT e PoA através do teorema CAP (*Consistency, Availability, Partition Tolerance*) [De Angelis et al. 2018], no qual consistência refere-se ao sincronismo de informações entre os nós da rede; disponibilidade refere-se à operacionalidade do sistema e; tolerância à partição refere-se à capacidade do sistema em se manter operacional em caso de falhas. Os autores afirmam que é impossível um sistema distribuído apresentar plenamente as três propriedades. Uma análise com relação ao desempenho dos dois protocolos foi conduzida em termos de tempo de convergência. Na avaliação, em termos de consistência, o PBFT se mostrou melhor do que o PoA, já que a versão "*Clique*"do algoritmo (usada no trabalho atual) pode possuir bifurcações. Além disso, por se tratar de um algoritmo baseado em prova, o PoA é um protocolo probabilístico, onde há uma sincronia eventual, garantindo que os nós irão receber atualizações das informações da *blockchain* eventualmente, comprometendo a consistência do sistema. O PBFT, por sua vez, é determinístico, no qual após a decisão feita pelo quórum, todos os nós são atualizados de maneira síncrona. Com relação às outras propriedades, como disponibilidade, tolerância a partições e desempenho, o *Clique* (PoA) se mostrou uma alternativa melhor, pois o PBFT possui mais rodadas para chegar a um consenso e também impõe mais mensagens à rede, apresentando maior complexidade para execução. Portanto, para este trabalho, foi priorizado o desempenho já que para os elementos da rede móvel (onde incorpora-se a funcionalidade de execução de uma *blockchain*) não é desejável o aumento da complexidade de mensagens e nem a indisponibilidade do sistema de consenso.

O PoA atribui autoridade aos nós e baseia-se em períodos definidos. A cada rodada, um subconjunto dos nós de autoridade pode propor um bloco, sendo um desses

nós o líder da rodada. Esse subconjunto é composto por no máximo $N - (\frac{N}{2} + 1)$ autoridades, sendo N o número total de nós de autoridade na rede [De Angelis et al. 2018]. Por exemplo, caso existam seis nós de autoridade, apenas dois podem enviar blocos a cada intervalo de tempo, sendo o primeiro deles o líder. Além disso, uma autoridade deve submeter um bloco a cada $\frac{N}{2} + 1$ blocos (para evitar falhas Bizantinas). A partir do início de uma nova rodada, o líder atual deve propor um bloco, ainda que este não possua nenhuma transação, i.e., propor um bloco mesmo que esteja vazio. Os nós não-líderes podem propor um bloco quando estiverem habilitados para fazê-lo, dentro de sua rodada, após aguardarem um tempo aleatório. O envio de um bloco pelos nós habilitados é feito em *broadcast* para todo o conjunto de nós de autoridade. Cada bloco proposto pelo líder é diretamente inserido na *blockchain* em todos os nós participantes. Porém, neste trabalho, adota-se como premissa que blocos sem nenhuma transação são imediatamente descartados. O bloco emitido pelo líder tem um peso maior com relação ao bloco de um nó comum para evitar bifurcação na *blockchain*.

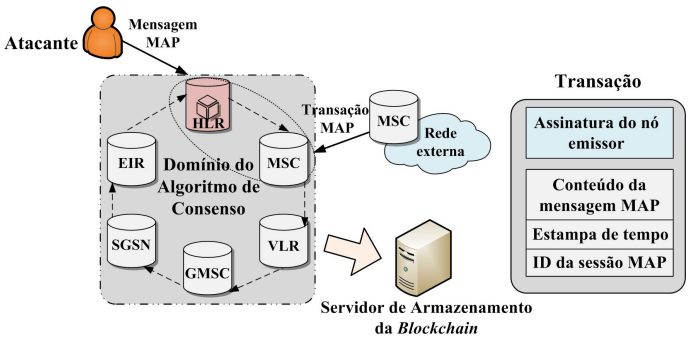

Figura 4. Arquitetura proposta com base no algoritmo PoA.

A Figura 4 apresenta a arquitetura proposta baseada no modelo PoA. Cada elemento de núcleo da rede móvel da operadora (vide Figura 1) compõe o conjunto de nós de autoridade, que são os nós confiáveis que participam efetivamente dos processos executados na formação da *blockchain*. O conteúdo da transação proposta é constituído pela mensagem MAP (pedido ou resposta), por uma estampa de tempo, assinatura do nó emissor da transação (o primeiro nó que recebeu a requisição) e um ID que caracteriza a sessão na qual essa transação é pertencente. Entende-se como sessão o conjunto de todas as operações geradas decorrentes de uma transação inicial, percorrendo o caminho desde a sua entrada na rede até o retorno para o remetente da transação.

A Figura 5 mostra o fluxo de operações a serem executadas para inserção de um bloco na *blockchain*. Quando a rede receber uma mensagem MAP, esta é validada localmente pelo nó que a recebeu. Após a validação, este nó encapsula a mensagem em uma transação e a assina, a fim de que todas as mensagens relativas àquela sessão sejam encaminhadas a ele para montagem do bloco, demonstrando a sua responsabilidade sobre a emissão do mesmo. Feito isso, o nó processa a transação, executando na rede a ação correspondente à requisição recebida. Cada nova transação resultante deste pedido é identificada com o mesmo valor (ID) de sessão. Paralelamente, os nós executam o algoritmo PoA. Na Figura 4, por exemplo, o HLR é o líder da rodada e precisa propor um bloco. O bloco será formado por todas as transações pertencentes à mesma sessão, organizadas cronologicamente pela estampa de tempo. O líder da rodada somente envia

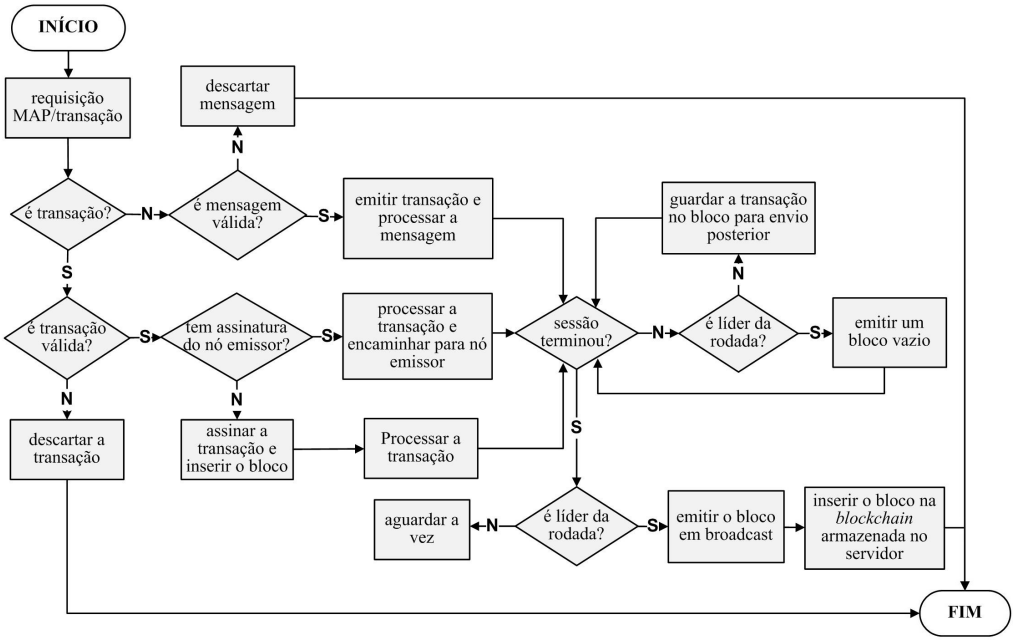

Figura 5. Emissão de um bloco e inserção na *blockchain* proposta.

um bloco quando possuir o conjunto total de transações da mesma sessão. Cada novo bloco inserido é armazenado no servidor de armazenamento da *blockchain*. Este servidor é opcional, sendo utilizado apenas se a rede não possuir capacidade de armazenamento em seus nós. Cada nó de autoridade possui uma réplica da *blockchain* divulgada a todos a cada nova rodada do algoritmo de consenso. Desse modo, todos os nós enxergam a *blockchain* da mesma forma.

5. Avaliação da Proposta

Um contrato inteligente foi desenvolvido na plataforma *Hyperledger Fabric* (HLF) para avaliação da proposta. As transações são definidas em contratos inteligentes no HLF. O código apresenta as seguintes funções: o cadastro de um assinante na rede, a consulta de informações de um assinante já registrado e a remoção de um assinante do banco de dados. Cada função é uma transação a ser executada na rede. Uma vez que o atacante possua o número de telefone do assinante e acesso à rede SS7, ele se torna apto a efetuar consultas legítimas à rede para obtenção de mais informações. Dessa forma, o atacante pode ocasionar um ataque de maior proporção, incluindo a remoção do assinante da rede. Além das funções listadas, também foi desenvolvida uma função para emissão de uma transação com o objetivo de executar a proposta na *blockchain* contendo a assinatura do nó originador das transações MAP (inserção, consulta ou remoção), uma estampa de tempo e um ID da transação, que caracteriza a sessão à qual a transação pertence.

5.1. Ambiente de avaliação

O *Hyperledger Fabric*[2] (HLF) é um ambiente de desenvolvimento para *blockchain* baseado em redes par a par privadas e permissionadas [Androulaki et al. 2018]. Um contrato inteligente (*chaincode*) na linguagem *Go* foi desenvolvido para a avaliação

[2]https://www.hyperledger.org/projects/fabric

da proposta. Além disso, foi desenvolvida a função "*setTransaction"* que estabelece alguns parâmetros para a transação a ser gerada, tais como: a assinatura do nó emissor e o autor da transação; o ID de sessão calculado como a assinatura criptográfica do nó emissor; e a estampa de tempo. Além dessa função, o contrato possui outras três: *"setMAP"*, *"query"* e *"delete"*. O objetivo da *setMAP* é inserir um usuário na rede, simulando um processo de registro. Para fins de simplificação no cadastro, apenas o nome e o número do usuário são armazenados. Nessa função, são realizados dois testes: um para verificar se os dados são vazios, o que não é permitido para a transação, sendo o dado automaticamente descartado; e a segunda para verificar se os dados seguem os critérios do 3GPP. Para isso, como exemplo, é feita uma verificação do comprimento do número informado. Caso seja menor do que a quantidade estabelecida, a informação é descartada. Para o teste, foi estabelecido o valor de 13 dígitos, sendo 2 dígitos para o país, 2 dígitos para a operadora e 9 dígitos para o número do assinante. Para as funções de consulta e remoção, basta informar o nome do usuário para executar a operação.

O *Hyperledger Caliper*[3] (HC) é uma ferramenta que permite a avaliação de desempenho de aplicações que usem *blockchain*. Os indicadores gerados pelo *Caliper* mostram resultados de vazão (transações por segundo), latência e uso de recursos computacionais (CPU e memória). Para execução dos testes de desempenho no *Caliper*, foi utilizada uma máquina virtual na nuvem oferecida pela Google. A máquina possui como configuração 1vCPU com 4GB de memória RAM, processador Intel Xeon E5-2650 V3 (*Haswell*), 500GB de HD e sistema operacional Linux Ubuntu 16.04 com *kernel* versão 4.15.0-1040. A versão 1.4.0 do *Hyperledger Fabric* foi usada. Como topologia para os testes, foi adotado um modelo que possui três organizações e dois nós pares pertencentes a cada uma, totalizando seis nós (nomeados de "*peerX.OrgY.example.com"*, onde X é o número do par e Y é o número referente à organização). O *Caliper* executa em *docker* e cada nó está distribuído em um *docker* diferente. Além dos nós pares, há ainda o nó ordenador que faz a organização dos blocos dentro da *blockchain*. Como modelo de base de dados, foi usado o *LevelDB*. Os testes foram feitos variando-se a quantidade de transações emitidas e o tamanho do bloco gerado pela *blockchain*. O código do contrato inteligente foi importado ao *Caliper* e foram avaliadas as funções de inserção ("*setMAP*") e consulta ("*query*"). Os dados gerados pela ferramenta são analisados posteriormente.

5.2. Resultados obtidos

O *Caliper* faz a simulação de uma *blockchain* emitindo várias transações por segundo, a fim de verificar alguns parâmetros como latência, vazão e consumo de recursos (memória e CPU). A Figura 6(a) mostra a latência encontrada nos testes, sendo que os valores apresentados são da latência média encontrada. Latência no contexto da *blockchain* é o tempo necessário para a plataforma em questão, *Hyperledger Fabric*, responder à uma transação. Pode-se observar que para a função de consulta, o tempo de resposta é praticamente constante e inferior ao tempo utilizado para cadastro de um usuário. Conforme esperado, quanto maior o número de transações a serem processadas, maior o tempo de latência. A Figura 6(b), exibe a vazão encontrada na avaliação, sendo que vazão corresponde ao número de transações bem sucedidas por segundo. Da mesma forma que a latência, para a função de consulta, a vazão se mostrou constante. Como a função *query* é apenas uma função de consulta, esta apresentou resultados melhores com relação à função

[3]https://github.com/hyperledger/caliper

setMAP, que exige maior processamento. As Figuras 6(c) e 6(d) correspondem aos valores de latência e vazão com alteração do tamanho do bloco. Os tamanhos utilizados foram 99, 128, 256, 512, 1024 e 2048MB. Nota-se que não há uma grande discrepância nos valores para ambos os gráficos apesar da modificação do tamanho do bloco utilizado.

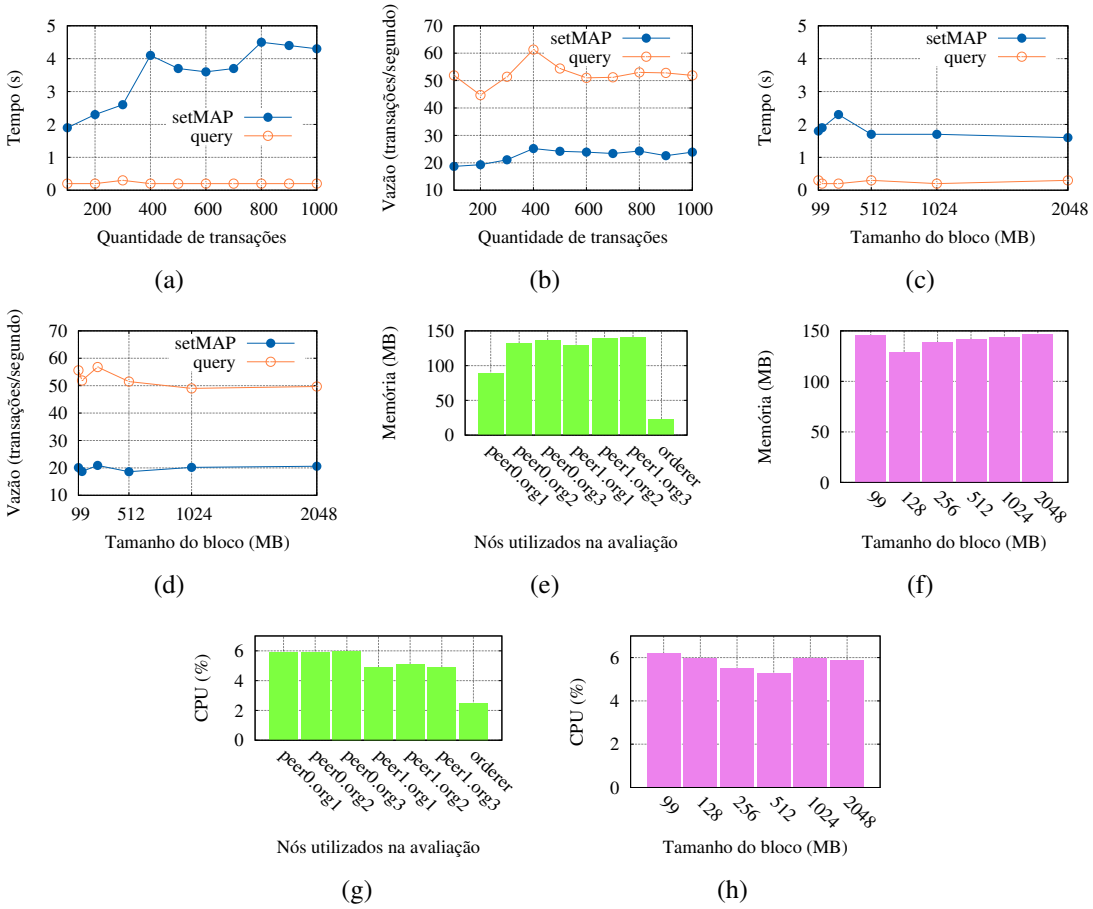

Figura 6. Latência (a) e vazão (b) encontradas nos testes de desempenho do *Hyperledger Fabric* para variação da quantidade de transações. Latência (c) e vazão (d) encontradas nos testes de desempenho do HLF para variação do tamanho do bloco. (e) Consumo de memória nos pares utilizados nos testes de desempenho para 100 transações. (f) Consumo de memória nos testes de desempenho para variação do tamanho do bloco. (g) Consumo de CPU nos pares utilizados nos testes de desempenho para 100 transações. (h) Consumo de CPU nos testes de desempenho para variação do tamanho do bloco.

Resultados sobre os recursos computacionais da máquina para a execução das transações do contrato inteligente foram também observados. Todos os resultados para CPU e memória representam os valores máximos encontrados. No caso do consumo de memória, nota-se que os pares consomem mais recursos do que o nó ordenador, por estes efetivamente executarem as transações. Isso pode ser visto na Figura 6(e). Também foi alterado o tamanho do bloco para observar a variação do consumo de memória, que também tende a ser constante, vide Figura 6(f). No início do projeto, foi utilizada uma máquina de 4vCPUs, porém, esta estava superdimensionada, visto que com 1vCPU foi possível executar os testes sem problemas. Para o consumo de CPU, novamente os nós pares apresentaram maior valor, conforme mostrado na Figura 6(g). O tamanho do bloco

também não impactou significativamente no consumo de CPU, conforme pode ser visto na Figura 6(h). Isso pode ocorre pois independente de quantas transações caibam em um bloco, o que está sendo verificado é a capacidade do sistema em processar as transações. Com esses gráficos, pode-se concluir que o uso da *blockchain* é factível em um ambiente real de uma provedora de serviços, visto que a capacidade utilizada na nuvem é bem semelhante ao que existe hoje em planta. Nas operadoras, os novos elementos já utilizam máquinas virtuais ao invés de uma solução proprietária. A *blockchain* nessa configuração, não comprometeria, portanto, a execução de outros processos já existentes nos elementos de rede. A proposta deste trabalho não se baseia em apenas um único tipo de ameaça e também não possui como objetivo a mitigação das mesmas em um primeiro momento. Entende-se que para o desenvolvimento de uma solução efetiva de mitigação, é necessário conhecer previamente o cenário dos ataques (tipos de ataques realizados, a relação entre os ataques e impacto na rede, a frequência dos ataques, etc.) e essa avaliação pode ser obtida de maneira confiável através de uma auditoria por meio da *blockchain*.

6. Conclusão e Trabalhos Futuros

Este trabalho teve como objetivo promover auditoria em redes móveis através do registro e identificação de forma permanente de todas as ações não filtradas por mecanismos de segurança já existentes. A ideia é complementar trabalhos relacionados permitindo que possíveis ataques não identificados sejam posteriormente investigados e bloqueados. Para isso, foi proposto o uso da tecnologia *blockchain* com característica privada, permissionada e com o uso do *Proof-of-Authority* (PoA) como algoritmo de consenso. Os experimentos realizados no *Hyperledger Fabric* mostraram que é possível implantar a tecnologia proposta sem causar grandes impactos a infraestrutura existente na rede da operadora. Como trabalhos futuros, pretende-se avaliar a eficiência da proposta com o uso de outros algoritmos de consenso, como o PBFT.

Referências

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., et al. (2018). Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference*, page 30. ACM.

Association, G. (2016). Ss7 security network implementation guidelines. Version 5.0.

Babu, A., Davis, B., Bruwer, T., Sallaba, M., and René, M. (2018). How blockchain can impact the telecommunications industry. Technical report, Delloite.

Bautista, J. E. V., Sawhney, S., Shukair, M., Singh, I., Govindaraju, V. K., and Sarkar, S. (2013). Performance of cs fallback from lte to umts. *IEEE Communications Magazine*, 51(9):136–143.

Dabrowski, A., Pianta, N., Klepp, T., Mulazzani, M., and Weippl, E. (2014). Imsi-catch me if you can: Imsi-catcher-catchers. In *Proceedings of the 30th annual computer security applications Conference*, pages 246–255. ACM.

De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., and Sassone, V. (2018). Pbft vs proof-of-authority: applying the cap theorem to permissioned blockchain. In *Italian Conference on Cybersecurity*.

Dryburgh, L. and Hewett, J. (2004). *Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services (Networking Technology)*. Cisco Press.

Gorenflo, C., Lee, S., Golab, L., and Keshav, S. (2019). Fastfabric: Scaling hyperledger fabric to 20,000 transactions per second. *arXiv preprint arXiv:1901.00910*.

Intelligence, G. (2019). The mobile economy 2019.

Jensen, K., Van Do, T., Nguyen, H. T., and Arnes, A. (2016). Better protection of ss7 networks with machine learning. In *IT Convergence and Security (ICITCS), 2016 6th International Conference on*, pages 1–7. IEEE.

Kambourakis, G., Rouskas, A., and Gritzalis, S. (2004). Performance evaluation of public key-based authentication in future mobile communication systems. *EURASIP Journal on wireless Communications e Networking*, 2004(1):184–197.

Li, C., Li, P., Zhou, D., Xu, W., Long, F., and Yao, A. (2018). Scaling nakamoto consensus to thousands of transactions per second. *arXiv preprint arXiv:1805.03870*.

Li, Z., Wang, W., Wilson, C., Chen, J., Qian, C., Jung, T., Zhang, L., Liu, K., Li, X., and Liu, Y. (2017). FBS-Radar: Uncovering fake base stations at scale in the wild. In *Network and Distributed System Security Symposium (NDSS)*, pages 1–15.

Mafakheri, B., Subramanya, T., Goratti, L., and Riggio, R. (2018). Blockchain-based Infrastructure Sharing in 5G Small Cell Networks. In *14th International Conference on Network e Service Management (CNSM)*, pages 313–317.

Nasir, Q., Qasse, I. A., Abu Talib, M., and Nassif, A. B. (2018). Performance analysis of hyperledger fabric platforms. *Security and Communication Networks*, 2018.

Rao, S. P., Kotte, B. T., and Holtmanns, S. (2016). Privacy in lte networks. In *9th EAI International Conference on Mobile Multimedia Communications*, pages 176–183. ACM.

Roth, J. D., Tummala, M., McEachen, J. C., and Scrofani, J. W. (2017). On location privacy in lte networks. *IEEE Transactions on Information Forensics and Security*, 12(6):1358–1368.

Rupprecht, D., Dabrowski, A., Thorsten, H., Weippl, E., and Pöpper, C. (2018). On security research towards future mobile network generations. *arXiv*.

Sukhwani, H., Wang, N., Trivedi, K. S., and Rindos, A. (2018). Performance modeling of hyperledger fabric (permissioned blockchain network). In *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, pages 1–8. IEEE.

Technologies, P. (2018). Telecom Attack Discovery, SS7 and Diameter protection, SS7 signaling firewall, threat prevention for telecom networks.

Tu, G.-H., Li, C.-Y., Peng, C., and Lu, S. (2015). How voice call technology poses security threats in 4g lte networks. In *2015 IEEE Conference on Communications and Network Security (CNS)*, pages 442–450. IEEE.

Vukolić, M. (2015). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In *International Workshop on Open Problems in Network Security (iNetSec)*, pages 112–125.