UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Caciano dos Santos Machado

Aplicação de blockchains para incentivos em redes cooperativas

Florianópolis
2021

Caciano dos Santos Machado

Aplicação de blockchains para incentivos em redes cooperativas

Tese submetida ao Programa de Pós-Graduação em Ciência da Computação para a obtenção do título de Doutor em Ciência da Computação.
Orientadora: Prof[a]. Carla Merkle Westphall, Dr[a].

Florianópolis
2021

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Machado, Caciano dos Santos
Aplicação de blockchains para incentivos em redes cooperativas / Caciano dos Santos Machado ; orientadora, Carla Merkle Westphall, 2021.
152 p.

Tese (doutorado) - Universidade Federal de Santa Catarina, Centro Tecnológico, Programa de Pós-Graduação em Ciência da Computação, Florianópolis, 2021.

Inclui referências.

1. Ciência da Computação. 2. contratos inteligentes. 3. redes comunitárias. 4. problema do caroneiro. 5. multi assinatura. I. Westphall, Carla Merkle. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Ciência da Computação. III. Título.

Caciano dos Santos Machado

Aplicação de blockchains para incentivos em redes cooperativas

O presente trabalho em nível de doutorado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

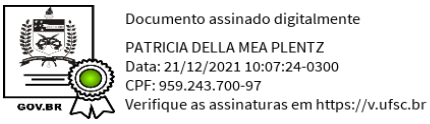
Prof. Christian Esteve Rothenberg, Dr.
Universidade Estadual de Campinas

Prof. Elias Procópio Duarte Jr., Dr.
Universidade Federal do Paraná

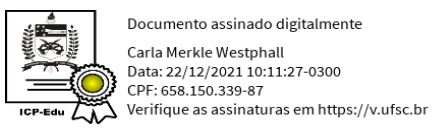
Prof. Luiz Fernando Rust do Carmo, Dr.
Instituto Nacional de Metrologia, Qualidade e Tecnologia

Prof. Jean Everson Martina, Dr.
Universidade Federal de Santa Catarina

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de Doutor em Ciência da Computação.



Prof[a]. Patricia Della Méa Plentz, Dr[a].
Coordenadora do Programa



Prof[a]. Carla Merkle Westphall, Dr[a].
Orientadora

Florianópolis, 2021.

Dedico esta tese aos profissionais de saúde que vem batalhando
incansavelmente no combate à pandemia da COVID-19.

AGRADECIMENTOS

Um agradecimento especial aos meus pais Ilsa Machado e Ivan Machado, pela vida, e aos meus irmãos Adriano Machado e Luana Machado.

À minha querida companheira Maria Munaro pela amizade, afeto e apoio que foram fundamentais.

Aos ex-colegas de graduação e mestrado em Ciência da Computação da Universidade Federal do Rio Grande do Sul (UFRGS).

Aos colegas e ex-colegas do Centro de Processamento de Dados da UFRGS, Alexandre Marchi, André Kunzler, Arthur Boos, Everton Foscarini, Felipe Sheeren, Gustavo Duarte, Hubert Ahlert, Jussara Issa Musse, Leandro Rey, Leonardo Bitzki, Liliane Xerxenevsky, Mauro Dias de Castro, Rui Ribeiro, Thiago Motta, em especial aos integrantes da Divisão de Engenharia de Redes, Bruno Engracio, Gabriela Todeschini, Jerônimo Menezes e Marcio Pohlmann.

Aos colegas do Laboratório de Integração de Software e Hardware e do Laboratório de Redes e Gerência da UFSC, especialmente para César Huegel, Cristiano de Souza, Davi Resner, Juliano Zatta, Leandro Loffi, Lucas Feitosa, Mateus Ludwich, Ricardo Boing, Roberto Scheffel, Rodolfo Borges, Wesley Bezerra e Prof. Carlos Westphall.

Ao meu ex-orientador Antônio Augusto Fröhlich que me auxiliou no início do doutorado e à minha orientadora Carla Merkle Westphall pelo apoio, críticas e sugestões na elaboração deste trabalho.

Aos amigos novos e antigos, de perto e de longe, que estiveram próximos mesmo que virtualmente durante as restrições sanitárias da pandemia, seja compartilhando memes, despertando ideias ou com longas discussões filosóficas, Alexandre Junges, Aramis Tisott, Cristiano Mariotto, Daniel Cabello Corrêa, Daniel Corrêa da Silva, Flavia Aline, Guilherme Constantino da Silva, Jaçanã Ribeiro, Jean Winter, Jefferson Meister Pires, Mauricio Mulinari e Paulo Macedo.

À UFSC e à UFRGS por possibilitarem os anos de estudo e dedicação neste tema de pesquisa.

A todos aqueles que contribuíram de uma forma ou de outra no decorrer desses quatro anos de doutorado para a conclusão deste trabalho, muito obrigado!

“A tecnologia do futuro é um fato técnico.
O futuro da tecnologia é um fato social.”
Álvaro Vieira Pinto – O Conceito de Tecnologia (Vol. II)

RESUMO

O problema do caroneiro (*free rider*) em redes comutadas por pacotes afeta a dependabilidade de redes cooperativas como redes D2D, VANETs e redes comunitárias. Nesse caso, o caroneiro é um roteador egoísta que não encaminha dados na mesma medida que tem seus dados encaminhados na rede. Uma forma de mitigar esse problema é através de mecanismos de incentivo que estimulem o encaminhamento de dados. Recentemente, as blockchains vem sendo utilizadas na implementação de mecanismos de incentivo baseados em crédito. No entanto, os sistemas encontrados no estado da arte requerem um terceiro confiável ou apresentam custos proibitivos com transações em blockchains públicas. A principal contribuição desta tese é uma arquitetura de sistema chamado HARPIA que implementa incentivos ao encaminhamento de dados sem a necessidade de um terceiro confiável e com custos significativamente menores na blockchain pública. O HARPIA realiza uma contabilização de tráfego de rede distribuída chamada DPIFA e automatiza a compensação dos créditos e débitos entre os roteadores através de um contrato inteligente Solidity. As transações que fazem a compensação são validadas e assinadas por um percentual mínimo dos roteadores da rede com um esquema de multi-assinatura antes de serem enviadas para a blockchain pública a cada ciclo do sistema (ex: diariamente, semanalmente, mensalmente). O HARPIA foi descrito utilizando um caso de uso típico de redes comunitárias. Foram realizadas análises quantitativas dos seus componentes em termos de desempenho, escalabilidade e custos na blockchain pública. Além disso, foi realizada uma análise preliminar das ameaças de segurança e das respectivas contramedidas para mitigá-las. Os resultados demonstraram que é possível utilizar o HARPIA em redes com até 64 roteadores de infraestrutura com hardware de propósito geral atual utilizando configurações específicas de um esquema de multi-assinatura com limiar m-de-n.

Palavras-chave: contratos inteligentes. redes comunitárias. problema do caroneiro. multi-assinatura.

ABSTRACT

The free rider problem in packet-switched networks affects the dependability of cooperative networks such as D2D networks, VANETs, and community networks. In this context, free riders are selfish routers that take advantage of cooperation from others but do not contribute reciprocally. Incentive mechanisms have been proposed to encourage cooperation in data forwarding. Recently, blockchains have been applied to credit-based incentive mechanisms. However, state-of-the-art systems require a trusted third-party and present prohibitive costs in terms of public blockchain transactions. The main contribution of this thesis is a new system architecture called HARPIA that implements data forwarding incentives without the need for a trusted third party and significantly reduces public blockchain costs. HARPIA performs a distributed network traffic accounting called DPIFA and automatizes credits and debits settlements among routers using a Solidity smart contract. Settlement transactions are validated and signed by a minimum percentage of the network routers using a threshold multi-signature scheme before being transmitted to the public blockchain in every system cycle (e.g., daily, weekly, monthly). A use case is given that describes a typical architecture application in community networks. HARPIA components were evaluated regarding performance, scalability, and public blockchains costs. Also, a preliminary threat assessment is presented with the respective countermeasures. Results show that HARPIA architecture is suitable for community networks with up to 64 infrastructure routers with handy general-purpose computers under specific m-of-n multi-signature thresholds.

Keywords: smart contracts. community networks. free riding. muti-signature.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ALGORITMOS

LISTA DE ABREVIATURAS E SIGLAS

ALM *Application Layer Multicast*

AODV *Ad hoc On-Demand Distance Vector Routing*

AP *Access Point*

AS *Autonomous System*

ASIC *Application Specific Integrated Circuits*

BATMAN *Better Approach to Mobile Ad-hoc Networking*

BGP *Border Gateway Protocol*

BLS Boneh–Lynn–Shacham

BMX7 *BatMan-eXperimental*

BSC *Binance Smart Chain*

CAPEX *Capital Expenditure*

CM *Credit Manager*

CPS *Cyber-Physical Systems*

D2D *Device-to-Device*

DTN *Delay Tolerant Network*

ECDH *Elliptic-Curve Diffie-Hellman*

ECDSA *Elliptic Curve Digital Signature Algorithm*

ETX *Expected Transmission Count*

EVM *Ethereum Virtual Machine*

GRE *Generic Routing Encapsulation*

HARPIA *Hop-by-hop Accounting and Rewards for Packet dIspAtching*

HSM *Hardware Security Module*

IoT *Internet of Things*

IoV *Internet of Vehicles*

IPFS *InterPlanetary File System*

MANET *Mobile Ad Hoc Network*

MDP *Mesh Datagram Protocol*

MEC *Mobile Edge Computing*

NFV *Network Function Virtualization*

OPEX *Operational Expenditure*

P2P *Peer-to-peer*

PBFT *Practical Byzantine Fault Tolerance*

PIFA *Protocol Independent Fairness Algorithm*

PKI *Public Ley Infrastructure*

PoA *Proof of Authority*

PoET *Proof of Elapsed Time*

PoN *Proof of networking*

PoR *Proof of routing*

PoS *Proof of Stake*

PoSA *Proof of Staked Authority*

PoV *Proof of Velocity*

PoW *Proof of Work*

QoS *Quality of Service*

RSA Rivest–Shamir–Adleman

RSU *Road-Side Unit*

SLA *Service Level Agreement*

STP *Settlement Transaction Proposal*

tps *transactions per second*

TRSM *Tamper-Resistant Security Module*

TTP *Trusted Third-Party*

V2I *Vehicle-to-Infrastructure*

V2V *Vehicle-to-Vehicle*

VANET *Vehicular Ad hoc NETwork*

VPN *Virtual Private Network*

YAC *Yet Another Consensus*

SUMÁRIO

1 INTRODUÇÃO

Desde sua criação, a Internet tem sido uma poderosa ferramenta para os mais variados fins. O que era tecnologia praticamente restrita ao âmbito militar, acadêmico e de alguns entusiastas, expandiu sua base de usuários e alcance geográfico com a exploração comercial e a *World Wide Web*. Após todos esses anos de evolução, grande parcela da população mundial se beneficia diretamente ou indiretamente das facilidades que a Internet trouxe. Toda infraestrutura de redes de empresas de telecomunicações, governos e consórcios público-privados dá suporte a uma infinidade de serviços que encurtam distâncias, otimizam processos e reduzem custos.

Todavia, o panorama atual indica limitações para que o acesso à Internet alcance determinadas regiões e populações. Diversos fatores socioeconômicos segregaram uma parcela da população com o que é definido por *divisão digital* (NORRIS, 2001). Segundo a Internet Society (INTERNET SOCIETY, 2017), após 25 anos de existência da Internet, em 2017, 53% da população mundial ainda não possuía acesso à Internet, a maior parte concentrada em países periféricos, economicamente dependentes e subdesenvolvidos. Conforme o Banco Mundial (BANCO MUNDIAL, 2016), o acesso à Internet contribui para o desenvolvimento socioeconômico, e as populações desconectadas acabam sofrendo uma grande desvantagem. Com esse entendimento, a Organização das Nações Unidas, incluiu nos seus Objetivos de Desenvolvimento Sustentável a seguinte meta

> *aumentar significativamente o acesso às tecnologias de informação e comunicação e se empenhar para procurar ao máximo oferecer acesso universal e a preços acessíveis à Internet nos países menos desenvolvidos, até 2020.* (ONU, 2015)

Os esforços nessa direção e a própria aceleração imposta pela pandemia da COVID-19 aumentaram substancialmente a penetração da Internet ao redor do mundo. Todavia, ficaram aquém do acesso universal almejado, permanecendo desconectada cerca de 34,4% da população mundial (International Telecommunication Union, 2021). As estratégias de mercado com indução estatal e as políticas públicas adotadas ainda estão muito longe de levar a Internet a todos. As primeiras estratégias ficaram limitadas a regiões e comunidades nas quais há viabilidade comercial. Nas últimas, a limitação é o próprio orçamento público e o interesse político.

Nesse contexto, a motivação desta tese é a investigação de estratégias cooperativas que podem ser alternativas de conectividade em locais cuja demanda não é atendida por infraestruturas convencionais de acesso devido a limitações técnicas ou econômicas. Durante os estudos preliminares foram identificados três tipos de redes de computadores que apresentam uma característica em comum que precisa ser controlada para promover a cooperação entre seus participantes a fim de melhorar a conectividade. As redes D2D (*device-to-device*) (NISHIYAMA; ITO; KATO, 2014), as VANETs (*Vehicular Ad hoc NETwork*) (HARTENSTEIN, 2010) e as redes comunitárias (MICHOLIA et al., 2018) são formadas por elementos de rede que pertencem a diferentes participantes e que precisam alocar seus recursos cooperativamente para a operação

correta dessas redes. Assim, essas redes se tornam suscetíveis a um fenômeno conhecido como problema do caroneiro (*free rider*) que compromete a dependabilidade da rede.

O problema do caroneiro consiste em um comportamento egoísta dos proprietários dos roteadores que acabam privilegiando o próprio tráfego de rede em detrimento do tráfego dos demais participantes, visando economizar seus recursos computacionais, energéticos e de rede (ROUGHGARDEN, 2010; BAIG et al., 2015). Existe uma série de mecanismos de incentivo a cooperação na literatura que visam mitigar o problema do caroneiro entre os quais destacam-se os mecanismos baseados em crédito e reputação (MARIAS et al., 2006). Os baseados em crédito precificam o serviço de encaminhamento de dados da rede, e possuem alguma forma de cobrar os dispositivos que tem seus dados encaminhados e remunerar os dispositivos que encaminham os dados. No entanto, esses mecanismos dependem de um terceiro confiável (*Trusted Third-Party* ou TTP) ou de módulos de segurança resistentes a adulteração (*Tamper-Resistant Security Module* ou TRSM).

Recentemente, as tecnologias de blockchain abriram a possibilidade de suplantar essas limitações ao servir como uma base descentralizada para a mediação dos incentivos de maneira segura (MACHADO; WESTPHALL, 2021). Com a utilização das técnicas de blockchains, abre-se a possibilidade de reduzir a assimetria de poder e de informação decorrente da necessidade de um TTP que poderia se aproveitar da posição para realizar fraudes e bloqueios de forma unilateral nos mecanismos de incentivo baseados em crédito (ASGHARI et al., 2013).

1.1 PERGUNTA DE PESQUISA E OBJETIVOS

Dentro do contexto de soluções descentralizadas, ou seja, que não necessitam de confiança em um TTP, elaborou-se a seguinte pergunta de pesquisa:

> *É possível implementar incentivos ao encaminhamento de pacotes em redes cooperativas de forma descentralizada?*

Esse é um problema em aberto, sem solução consagrada. Dada a existência de diversas iniciativas nesse sentido mas uma carência de estudos sistematizados que as sintetizem através de um mesmo prisma, foi elaborada uma revisão detalhada do estado da arte. A revisão permitiu compreender melhor as estratégias, limitações, desafios e possibilidades dos trabalhos, e direcionar a pesquisa. A partir das constatações desse estudo, encontrou-se apenas soluções descentralizadas que adotam blockchains. Partiu-se da hipótese de que é possível descentralizar os mecanismos de incentivo e que as blockchains são as tecnologias habilitadoras para essa finalidade. Assim, após identificar limitações no estado da arte quanto à dependência de TTP e custos proibitivos nas blockchains, o objetivo geral delineado para a pesquisa foi:

> *Verificar se a utilização de blockchains pode servir para a elaboração de mecanismos de incentivo ao encaminhamento de dados em redes cooperativas sem depender de TTP e sem custos proibitivos.*

O objetivo geral se justifica considerando que: (a) a inovação das blockchains reside justamente na eliminação do estabelecimento de confiança em TTP para transações seguras entre os participantes (WERBACH, 2018); (b) a eliminação da necessidade de confiança em TTP é uma propriedade desejada em mecanismos de incentivo de redes cooperativas pois elimina a assimetria de poder que existiria caso se utilizassem serviços centralizados controlados por determinados participantes.

A partir desse objetivo geral, os objetivos específicos desta tese são:

1. A concepção de uma arquitetura de sistema que proporcione incentivos ao encaminhamento de dados utilizando blockchains sem a necessidade de TTP ou custos proibitivos nas blockchains.

2. Uma avaliação quantitativa e qualitativa da arquitetura concebida para estimar seu desempenho, escalabilidade, custos com blockchains e identificar as ameaças de segurança.

A pesquisa foi focada em mecanismos de incentivo baseados em crédito, considerando que os baseados em reputação podem sofrer do problema do caroneiro de segunda ordem (EFSTATHIOU; FRANGOUDIS; POLYZOS, 2006), descrito no Cap. 2, e que as blockchains já fornecem os incentivos positivos de crédito automaticamente através de transações de pagamento seguras. Além disso, na mesma linha do que foi encontrado no estado da arte, a tese considera somente o encaminhamento simples de dados, ou seja, sem mecanismos para diferenciação de tipo de tráfego de rede ou qualidade de serviço, como latência e *jitter* máximos dos pacotes, ou vazão mínima.

1.2 MÉTODO DE PESQUISA

A pesquisa desta tese é de natureza aplicada abordando de forma quantitativa e qualitativa a intersecção entre os sistemas de blockchain e redes cooperativas incentivadas. Os procedimentos dessa pesquisa foram divididos em três etapas.

A etapa de pesquisa bibliográfica foi baseada no levantamento de artigos, produtos e patentes relacionados com o problema de pesquisa para compreender melhor as estratégias, limitações, desafios e possibilidades, e direcionar a pesquisa. Para essa finalidade foi realizada inicialmente uma revisão da literatura em bases de dados de artigos científicos nas áreas de ciência da computação e de redes de computadores. Também foram incluídos nessa pesquisa produtos e patentes encontrados a partir dos artigos científicos e em grupos de trabalho de organismos de desenvolvimento de padrões, como o IETF.

A etapa de concepção de uma nova arquitetura de sistema, primeiro objetivo específico, foi um processo que levou em consideração tanto as técnicas de blockchains mais recentes quanto técnicas adotadas por mecanismos de incentivo tradicionais de redes cooperativas. Para isso foi necessário resgatar também estudos prévios, anteriores à existência de blockchains.

A etapa de avaliação da nova arquitetura de sistema, segundo objetivo específico, se baseou em experimentos quantitativos dos componentes da arquitetura modelada. Os componentes escolhidos para a análise foram os que apresentariam maior impacto em termos de desempenho, escalabilidade e custos na blockchain. Adicionalmente, a avaliação também inclui uma análise qualitativa preliminar das suas características de segurança.

1.3 CONTRIBUIÇÕES

Os objetivos delineados nessa introdução foram realizados integralmente e seus resultados são descritos no decorrer dessa tese. As principais contribuições podem ser sintetizadas da seguinte maneira.

O levantamento, sistematização e síntese do estado da arte que permite uma compreensão mais abrangente e aprofundada sobre quais são e como operam os mecanismos de incentivo baseados em blockchains. A sistematização inclui também classificações dos sistemas de acordo com propriedades e funcionalidades em comum, de forma que seja possível identificar facilmente as semelhanças e as diferenças entre os sistemas. Também foram identificadas as limitações e os desafios atuais do estado da arte, que servem de ponto de partida para novas pesquisas e avanços.

Foi modelada uma arquitetura de sistema que implementa incentivos ao encaminhamento de dados em redes cooperativas utilizando blockchains. Essa arquietura é independente de TTP e de protocolo de roteamento de rede, além de produzir custos moderados na blockchain se comparado com outras propostas do estado da arte. Todas essas características são apropriadas para os mecanismos de incentivo de redes cooperativas que se deseja aprimorar. Além disso, a arquitetura foi descrita através de um caso de uso típico de uma rede comunitária, de forma que seja possível compreender melhor o problema que se deseja solucionar e as estratégias adotadas.

Foi implementado um contrato inteligente em linguagem Solidity que representa a parte central da arquitetura proposta em torno do qual os demais componentes do sistema operam. Foram implementados também protótipos de componentes do sistema. Os protótipos foram escritos em Python e como aplicações do simulador OMNet++. Essas implementações, além de servir para validação dos componentes, podem servir futuramente como referência para a implementação do sistema como um todo.

Foram modelados cenários de simulação com o OMNet++ com topologias e características de rede inspiradas em redes comunitárias como a GUIFI.net. Esses cenários poderão ser utilizados futuramente para modelar análises de comportamentos dos participantes dessas redes, tendo em vista mitigar o problema do caroneiro.

Os principais componentes do sistema foram avaliados através de experimentação quantitativa em termos de desempenho, escalabilidade e custos com a blockchain através dos protótipos dos componentes, aplicações do simulador OMNet++, programas escritos em R e *scripts* Gnuplot. Essas avaliações permitiram estimar o impacto que os componentes produzem

em termos de tempo de processamento, requisitos de armazenamento, sobrecusto de comunicação e custos com escritas na blockchain nos cenários modelados. Adicionalmente, foi realizada uma análise qualitativa com identificação preliminar das ameaças de segurança em potencial que podem servir como referencial para outras iniciativas nesse tema. Importante observar que, mesmo que os componentes tenham sido avaliados dentro do contexto do tema desta tese, algumas dessas avaliações podem ter utilidade em outros escopos, como, por exemplo, a avaliação do esquema de multi-assinaturas MuSig.

Complementarmente, durante o doutorado também foi elaborado um trabalho indiretamente relacionado com o tema desta tese. Esse trabalho é uma proposta de utilização de blockchains para verificação de integridade de dados produzidos por dispositivos da Internet das Coisas (IoT ou *Internet of Things*) e armazenados em uma infraestrutura de nuvem de terceiros semi-confiável no contexto de sistemas ciber-físicos (CPS ou *Cyber-Physical Systems*).

Parte das contribuições desta tese foi publicada em artigos científicos em periódicos e eventos referenciados a seguir:

- *Blockchain incentivized data forwarding in MANETs: Strategies and challenges* (MACHADO; WESTPHALL, 2021)
- *Hop-by-hop Accounting and Rewards for Packet dIspAtching* (MACHADO; SANTOS; WESTPHALL, 2021)
- *IoT Data Integrity Verification for Cyber-Physical Systems Using Blockchain* (MACHADO; FRÖHLICH, 2018)

1.4 ORGANIZAÇÃO DA TESE

O restante da tese está organizado conforme detalhado a seguir. O Cap. 2 explica o problema do caroneiro em redes cooperativas e os mecanismos de incentivo encontrados na literatura para mitigá-lo. O Cap. 3 aborda conceitos fundamentais para a compreensão dos capítulos posteriores da tese, como blockchains, contratos inteligentes, multi-assinaturas e um mecanismo de incentivo baseado em crédito chamado PIFA. O Cap. 4 mostra o estado da arte em sistemas que utilizam blockchains como base para os mecanismos de incentivo para encaminhamento de dados. O Cap. 5 apresenta a arquitetura do sistema HARPIA (*Hop-by-hop Accounting and Rewards for Packet dIspAtching*), proposto nesta tese. O Cap. 6 é uma análise dos componentes do HARPIA que inclui análises de desempenho, escalabilidade, custos na blockchain pública e uma análise preliminar das ameaças de segurança potenciais. Finalmente, o Cap. 7 conclui, apresenta algumas considerações finais e trabalhos futuros.

2 PROPRIEDADE E DEPENDABILIDADE EM REDES COOPERATIVAS

Para que as redes de computadores funcionem de forma confiável é necessário que os elementos de rede operem de maneira orquestrada seguindo as regras estabelecidas por um protocolo de comunicação em comum (CERF; KAHN, 1974). Tal requisito é trivial quando os elementos de rede (roteadores, switches, pontos de acesso, etc) são gerenciados por uma mesma equipe técnica em um mesmo domínio administrativo. Em geral, um mesmo domínio administrativo implica também que esses elementos de rede são propriedade de um mesmo indivíduo ou organização. No entanto, em situações específicas, como zonas de desastre, parcerias militares e consórcios público-privados, a propriedade dos equipamentos, apesar de não ser de um mesmo indivíduo ou organização, é delegada a uma mesma equipe técnica. Nesses casos, o que ocorre, de fato, é que os proprietários (indivíduos ou grupos) dos diferentes equipamentos concedem a gerência destes à uma mesma equipe técnica. Em síntese, em qualquer uma dessas situações, os proprietários autorizam que uma determinada equipe técnica assuma a responsabilidade pelo funcionamento dos equipamentos de rede. Para os fins dessa explicação, equipamentos alugados (ex: *on-premise*) também são considerados propriedade do arrendatário.

Nas ciências sociais, os problemas que envolvem ações coletivas para atingir um resultado foram estudados com o intuito de investigar o comportamento de participantes com interesses conflitantes em relação ao resultado almejado pelo grupo. Quando um certo número de participantes adere a comportamentos inapropriados, visando obter ganhos individuais para satisfação imediata, em vez de atuar de forma cooperativa para os ganhos coletivos de mais longo prazo, o objetivo do grupo pode ser comprometido (OLSON, 2012).

Nas redes cooperativas cujos elementos de rede pertencem a proprietários distintos é fundamental que esses colaborem alocando seus recursos (equipamentos, cabeamento, energia elétrica, força de trabalho) de forma a atender as necessidades dos demais membros (GUPTA; STAHL; WHINSTON, 1999). Em relações comerciais de prestação de serviços de trânsito de rede, a cooperação acontece mediante pagamento, de forma que parte desse pagamento serve para financiamento da operação, custeio e expansão das redes, e o lucro serve como uma forma de incentivo aos proprietários dos provedores. Assim, a relação comercial se torna uma forma jurídica de impor a cooperação entre os participantes por meio de contratos de prestação de serviços. Nas situações que o estabelecimento de contratos é indesejado ou impossível de ocorrer, são necessárias outras formas de imposição ou incentivo à cooperação.

A inexistência de um mecanismo que imponha a cooperação ou de um incentivo que torne a cooperação mais desejável do que os ganhos com o comportamento inapropriado dá margem ao surgimento de participantes com interesses conflitantes com o do grupo da rede. Essa situação pode degradar significativamente a qualidade do serviço prestado em termos de dependabilidade. Por dependabilidade entende-se aqui as propriedades de disponibilidade, confiabilidade, integridade e manutenibilidade da rede (ROUGHGARDEN, 2010; AVIZIENIS et al., 2004). Alguns exemplos de comportamentos inapropriados que prejudicam a dependabilidade de redes cooperativas são discutidos no trabalho de Machado e Westphall *et al.* (MA-

CHADO; WESTPHALL, 2021) e estão listados a seguir.

- Disputas por canais de radiofrequência no espectro não licenciado que pode levar à alocação ineficiente dos canais disponíveis e interferências (LEHR; CROWCROFT, 2005; WANG; LIU, 2011).
- Manipulação dos tempos de contenção de protocolos de controle de acesso ao meio, como o CSMA, com objetivo de maximizar a utilização de um participante egoísta sobre o meio (SAMI et al., 2016).
- Elementos roteadores que priorizam o próprio tráfego, evitando encaminhar pacotes de dados de outros participantes, com o objetivo de preservar seus recursos computacionais, energéticos e de rede.
- Omissão de participantes sobre as manutenções preventivas, corretivas e evolutivas dos elementos de rede sob sua responsabilidade.

Em todos os casos apresentados, a indisponibilidade de recursos de infraestrutura (canais de rádio, acesso ao meio, encaminhamento de pacotes, equipamentos de rede confiáveis) decorrente do comportamento inapropriado de alguns participantes poderá prejudicar a dependabilidade da comunicação de outros membros dessa rede. Esses problemas se tornam mais prováveis de ocorrer devido a grande disponibilidade de hardware programável que permite que os participantes subvertam protocolos de comunicação com o intuito de priorizar o serviço de rede para si mesmos (RAYA; HUBAUX; AAD, 2004).

Marias *et al.* (MARIAS et al., 2006) afirmam que alguns comportamentos inapropriados são classificados como comportamentos egoístas na literatura e apresentam alguns exemplos desses tipos de comportamento. No entanto, salientam que não existe categorização consagrada para distinguir comportamentos egoístas de comportamentos maliciosos, ou seja, ataques explícitos, como negação de serviço (DoS). Os autores afirmam também que não encontraram uma definição homogênea de comportamento egoísta passivo (no qual não há ação deliberada do participante) ou ativo (no qual a intenção do participante é explícita). Mesmo assim, para fins de ilustração, será utilizada a definição adotada por esses autores para o comportamento egoísta focando em duas situações.

O comportamento egoísta passivo, é considerado aqui aquele no qual o participante deixa de agir para promover a melhoria do serviço na rede que ele faz parte. Por exemplo, um responsável por um roteador de uma rede cooperativa que, por omissão, acaba deixando de realizar as manutenções preventivas, corretivas ou evolutivas necessárias para garantir a confiabilidade e a disponibilidade do encaminhamento de dados. O comportamento egoísta ativo, é aquele que o responsável configura deliberadamente seus equipamentos de rede para que o seu tráfego seja priorizado em relação ao tráfego alheio (ex: com filas de QoS), ou até mesmo para descartar esse tráfego, como forma de economizar recursos energéticos, computacionais e de rede.

Daqui em diante, o participante será tratado como sendo um roteador de rede que é propriedade de um determinado indivíduo ou organização. Um roteador é um elemento de rede ativo, com responsabilidade parcial pelo serviço de comunicação na rede e que trabalha sobre o paradigma *store-and-forward*, ou seja, recebe pacotes da sua vizinhança, analisa para onde estão sendo destinados e encaminha para o próximo salto de roteamento em direção ao destino. A próxima seção explica como o comportamento egoísta de um roteador pode levar ao problema do caroneiro (*free rider*) em redes cooperativas.

2.1 PROBLEMA DO CARONEIRO (FREE RIDER)

O problema do caroneiro (*free rider*) é um exemplo desse tipo de comportamento que foi extensivamente estudado no âmbito de redes peer-to-peer (P2P) (FELDMAN et al., 2006). No contexto de redes de computadores, o caroneiro consiste em um roteador com comportamento egoísta que, apesar de se aproveitar do trabalho dos demais roteadores da rede, não contribui com o seu funcionamento na mesma medida (ROUGHGARDEN, 2010; BAIG et al., 2015). Tal comportamento pode se refletir em diversos aspectos do funcionamento de redes cooperativas entre os quais destaca-se o encaminhamento dos pacotes de redes cooperativas, conforme ilustrado na Fig. 1.

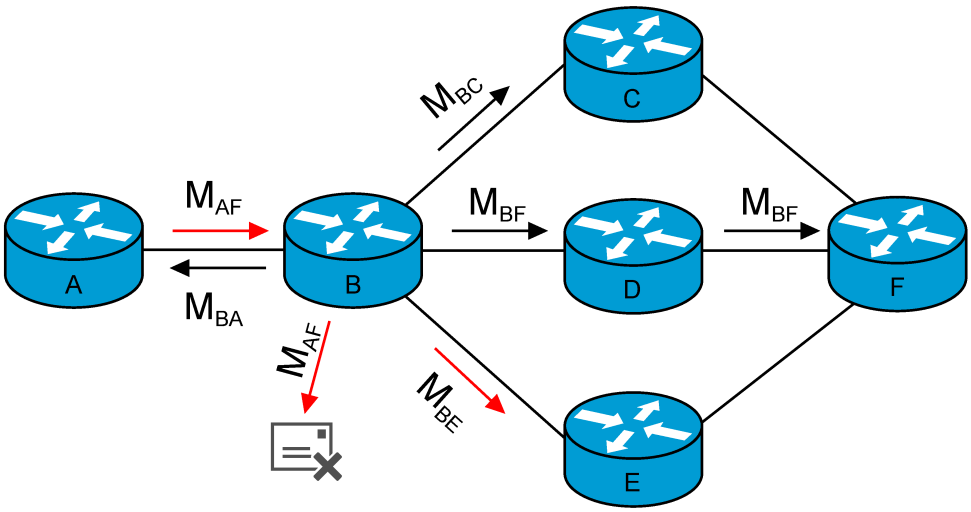


Figura 1 – Problema do caroneiro.

A figura ilustra uma rede cooperativa composta por um conjunto de roteadores rotulados de A a F, cada qual propriedade de um dono diferente. A rede opera através da comutação de pacotes representados por M_{SD}, onde S é o roteador origem do pacote e D é o roteador de destino. Cada mensagem M_{SD} possui uma única origem e um único destino, mas a descrição do problema pode ser facilmente estendida para os casos que as mensagens possuem múltiplos destinos. O caminho do pacote M_{AF} inclui o roteador B, que apresenta comportamento característico do problema do caroneiro. Esse roteador descarta mensagens como a M_{AF} ou limita significativamente a banda disponível para os demais roteadores, para priorizar o próprio

tráfego. Mesmo assim, o roteador B permanece tirando vantagem da cooperação dos demais roteadores e continua produzindo novos pacotes (ex: M_{BA}, M_{BC}, M_{BE} e M_{BF}) que são encaminhados corretamente pelos demais roteadores.

2.2 REDES SUSCETÍVEIS AO PROBLEMA DO CARONEIRO

Alguns tipos específicos de redes de computadores cooperativas são formadas pela interconexão de elementos roteadores que são propriedade de diferentes indivíduos ou organizações, e cuja gerência não está sob controle de uma mesma equipe técnica. Pode-se incluir nessa classificação redes móveis *ad hoc* (MANET), como as redes de dispositivos pessoais (D2D) (NISHIYAMA; ITO; KATO, 2014) e redes veiculares (VANET) (HARTENSTEIN, 2010), além das redes comunitárias (MICHOLIA et al., 2018) ilustradas na Fig. 2. Dentro dessas classificações também estão incluídas as variações correspondentes a redes tolerantes a atraso (DTN) (KHABBAZ; ASSI; FAWAZ, 2012).

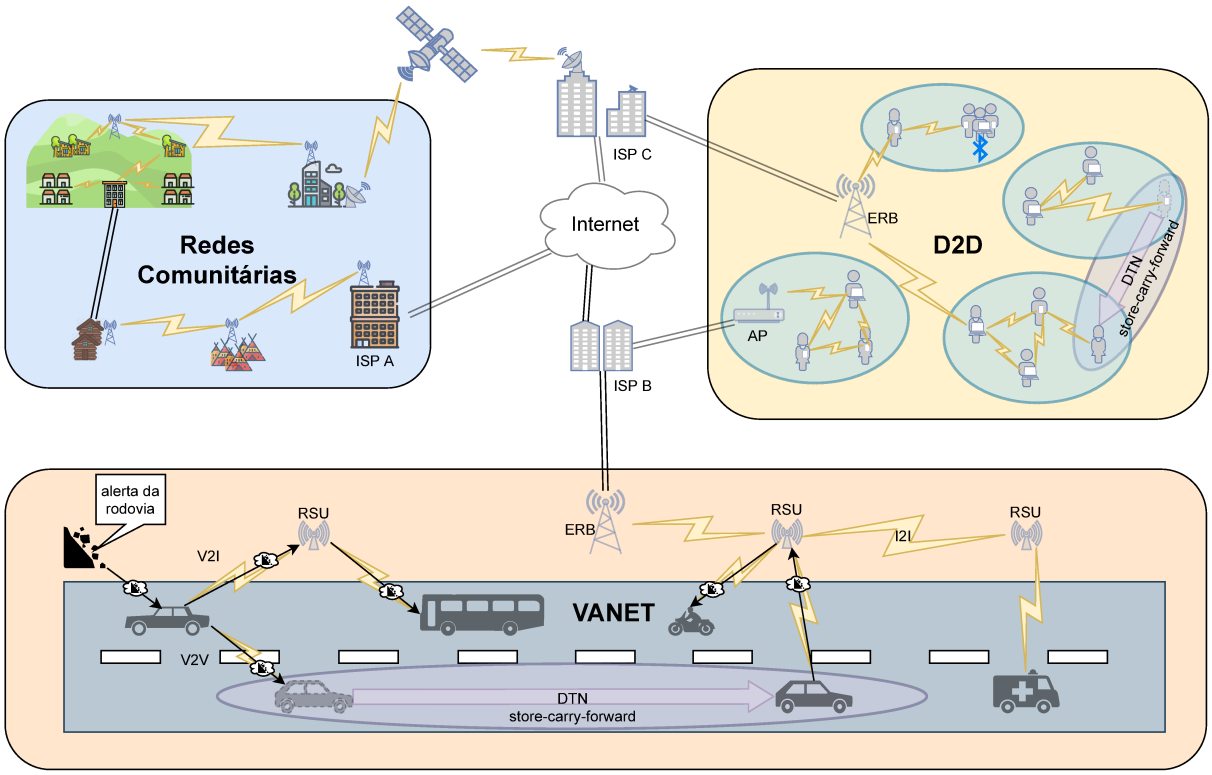


Figura 2 – Redes cooperativas suscetíveis ao problema do caroneiro.

Redes comunitárias, como a GUIFI.net (VEGA et al., 2015), a Freifunk (FREIFUNK, 2021), a AlterMundi (ALTERMUNDI, 2021) e a Rhizomatica (RHIZOMATICA, 2021) são infraestruturas de rede implantadas de forma cooperativa que visam fornecer o acesso de última milha à Internet. Essas soluções são tipicamente implementadas em áreas nas quais há pouco interesse comercial ou que as políticas públicas não conseguem atender com eficiência, como zonas rurais, favelas e comunidades economicamente isoladas. O barateamento de tecnologias

de rede sem fio e o surgimento de novos protocolos de redes *mesh* favoreceu a disseminação das redes comunitárias (AKYILDIZ; WANG, 2009), apesar dessas também serem implementadas com tecnologias cabeadas. A implantação dessas redes permite que as comunidades economizem em custos de infraestrutura e até mesmo que desenvolvam serviços locais.

Em contraste com as redes comunitárias, que se baseiam em uma infraestrutura relativamente estática e de longo prazo, as redes D2D são inerentemente mais dinâmicas e efêmeras. No caso, os roteadores são dispositivos móveis pessoais, como notebooks, celulares, tablets e outros dispositivos que possuem conectividade como WiFi ou Bluetooth. Os nodos podem ingressar e sair da rede utilizando os recursos e contribuindo com a operação da rede enquanto ativos. Além disso, alguns dispositivos conectados via estações rádio base (ERB) de telefonia móvel ou pontos de acesso WiFi (AP) podem compartilhar seu acesso à Internet com outros dispositivos locais. Nesse tipo de rede, é mais difícil estabelecer confiança entre os nodos e identificar comportamentos inapropriados, já que a vizinhança está constantemente mudando e a informação de reputação se torna obsoleta rapidamente. É importante salientar a diferença de redes D2D para as redes da Internet das coisas (IoT). As redes D2D consistem em redes cujos dispositivos são propriedade de distintos donos e que requerem cooperação para o seu funcionamento. Já as redes IoT podem ter todos os dispositivos pertencendo a uma mesma organização ou indivíduo. Além disso, redes D2D podem servir de infraestrutura para dispositivos IoT.

As redes veiculares (VANET) são tipos de MANETs nas quais os veículos são elementos de rede. Tipicamente, essas redes servem para a coordenação de veículos, transmissão de informações de tráfego e serviços de estrada (emergência, sinalização, postos de combustíveis, restaurantes e hotéis). Também podem servir como última milha de acesso à Internet para passageiros e veículos próximos. As VANETs possuem pilhas de protocolos de rede específicas sobre tecnologias de rádio e luz infravermelha (CUNHA et al., 2016) que consideram os padrões de mobilidade dos veículos e sua orientação ao longo das faixas de rodagem. Os tipos de comunicação nas VANETs são classificados de acordo com os tipos de elementos de rede da arquitetura que se comunicam. V2V indica comunicação entre dois veículos. V2I indica a comunicação entre um veículo e um elemento da infraestrutura. As RSU são unidades de infraestrutura posicionadas ao longo das pistas para permitir comunicação V2I.

Redes tolerantes a atraso (DTN) (KHABBAZ; ASSI; FAWAZ, 2012), também conhecidas como redes tolerantes a disrupção ou redes oportunísticas, permitem a comunicação em redes cujos segmentos estão frequentemente particionados. DTNs seguem o paradigma *store-carry-forward* que estende o paradigma *store-and-forward* de redes comutadas por pacotes com a mobilidade física dos dispositivos. Em vez de encaminhar os dados imediatamente, os roteadores carregam os dados até encontrar uma oportunidade de encaminhá-los para um outro roteador em direção ao destino. Esse processo aumenta a latência e o *jitter* significativamente mas permite a comunicação para classes de aplicações menos sensíveis a esses efeitos.

Tantos redes D2D quanto VANETs podem ser projetadas como DTNs (HUI et al., 2005; PEREIRA et al., 2012), conforme ilustrado na Fig. 2. No exemplo das redes D2D, ilustrado com uma elipse em roxo para a comunicação DTN, um dos participantes migra de uma

rede D2D que não possui conectividade com a Internet e carrega uma mensagem de forma oportunística para outra rede D2D que possui conectividade com a Internet através do dispositivo de um participante que possui conexão a uma ERB de telefonia móvel. No exemplo da VANET, também chamado VDTN, ilustrado com uma elipse em roxo para a comunicação DTN, um dos veículos detecta um alerta de deslizamento de terra na pista e envia as informações da condição da estrada diretamente para outros carros (V2V) que por sua vez encaminharão para outros veículos ou RSUs no decorrer dos seus trajetos.

2.3 MECANISMOS DE INCENTIVO À COOPERAÇÃO

Um mecanismo de incentivo pode ser definido como uma regra do sistema cujo propósito é induzir os participantes a agirem de uma maneira desejada. A cooperação dos roteadores pode ser alcançada através de recompensas que estimulam a cooperação ou sanções que desencorajam o comportamento inapropriado. Com o objetivo de mitigar comportamentos inapropriados dos roteadores de redes cooperativas, em particular os que causam o problema do caroneiro, vários trabalhos investigaram formas de implementar incentivos à cooperação no encaminhamento de dados (BOGLIOLO et al., 2012; SILVA et al., 2017; JEDARI; XIA; NING, 2018).

Os mecanismos de incentivo levantados assumem que os participantes agem racionalmente, sob uma perspectiva meramente econômica. De fato, existem casos que proprietários dos roteadores cooperam sem ter como objetivo os benefícios econômicos, mas sim por motivações mais subjetivas e sutis, como altruísmo, reputação social ou afeição. Entretanto, tais motivações são insuficientes para sustentar o funcionamento de uma rede de computadores pois mesmo o voluntarismo requer investimento econômico. O investimento necessário se divide basicamente em gastos de capital (CAPEX: roteadores, antenas, cabeamento, licenças) e de operação (OPEX: contratos de *backhaul*, energia elétrica, refrigeração, custos de manutenção e homem-hora de técnicos). O investimento tende a cessar no caso dos recursos do voluntariado se tornarem escassos. Por outro lado, alguns trabalhos, como o de Félegyházi *et al.* (FELEGYHAZI; HUBAUX; BUTTYAN, 2006), que partiam da hipótese que a cooperação baseada apenas no auto-interesse poderia existir naturalmente, sugerem nas suas simulações e resultados que, na prática, tais condições de cooperação são pouco prováveis de ocorrerem sem mecanismos explícitos de incentivo ao encaminhamento de pacotes.

Existe uma extensa literatura que investiga mecanismos de incentivo para a cooperação em redes comutadas por pacotes. A bibliografia encontrada recai em duas categorias principais de mecanismos: baseados em reputação e baseados em crédito. A maioria desses mecanismos adota protocolos de segurança com esquemas criptográficos para punir roteadores com comportamento inapropriado e recompensar roteadores cooperativos. Outras classificações incluem abordagens com técnicas baseadas em teoria dos jogos que, em geral, resultam em mecanismos baseados em reputação ou crédito (YANG; FANG; XUE, 2012). Em seguida são descritos alguns dos principais mecanismos de incentivo para redes cooperativas.

2.3.1 Mecanismos baseados em crédito

Os mecanismos baseados em crédito, ilustrados na Fig. 3, modelam a tarefa de encaminhamento de pacotes como um serviço que pode ser valorado e cobrado. Esses modelos incorporam alguma forma de moeda virtual para regular as negociações entre os vários roteadores da rede no encaminhamentos dos pacotes. A moeda virtual é utilizada pelo remetente e/ou pelo destinatário para pagar os roteadores que cooperam com o encaminhamento dos pacotes. Assim, os roteadores são incentivados a encaminhar os pacotes dos demais roteadores para receber crédito e gastam esse crédito quando assumem o papel de remetente ou destinatário.

Os mecanismos dessa categoria utilizam algoritmos distribuídos e técnicas de criptografia para realizar o pagamento seguro e contabilização correta do tráfego. Existem duas abordagens amplamente adotadas para a segurança dos mecanismos de crédito ilustradas na Fig. 3. A primeira consiste em módulos de segurança resistentes a adulteração (TRSM) embutidos nas interfaces de rede, como o FRAME (LI; WU, 2009). A segunda abordagem se baseia em bancos virtuais, que dependem de um terceiro confiável (*Trusted Third-Party* ou TTP) responsável pela contabilização centralizada, como o SMART (ZHU et al., 2009).

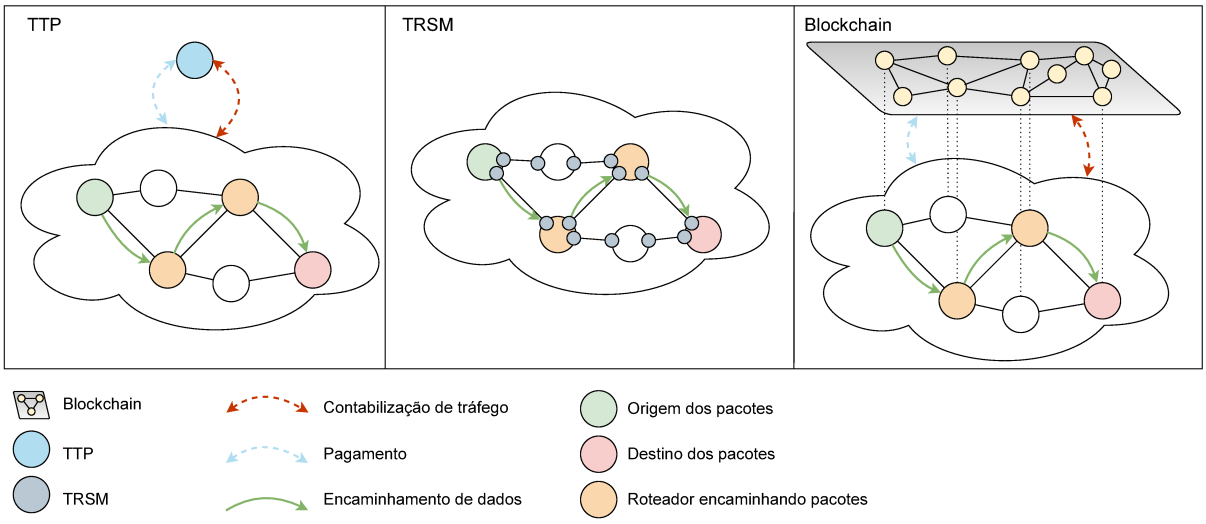


Figura 3 – Mecanismos de incentivo à cooperação baseados em crédito.

Existe uma limitação nos mecanismos de crédito referente à necessidade de reciprocidade na cooperação. O crédito de cada roteador é limitado à sua cooperação. Ou seja, se não existir demanda de encaminhamento de tráfego na vizinhança de um determinado roteador com a qual ele possa contribuir com o encaminhamento, esse roteador terá seu próprio tráfego limitado à essa baixa demanda de sua vizinhança, pois não terá como obter créditos para pagar seus vizinhos para que encaminhem os seus pacotes. Alguns mecanismos de crédito resolvem esse problema introduzindo uma moeda externa (MAHMOUD; SHEN, 2010).

Importante lembrar que serviços de rede mediados por relações comerciais com provedores de Internet ou trânsito entre sistemas autônomos (AS) já possuem o incentivo implícito. No entanto, nesses casos há uma assimetria de informação e poder sobre a operação da rede e

na contabilização do tráfego. Essa assimetria permite que o provedor do serviço realize contabilizações indevidas e cobranças abusivas, ou que faça conformação do tráfego de rede abaixo da capacidade contratada. Tais conflitos normalmente são tratados por meio de agências de regulação ou pelo sistema jurídico estatal. Os mecanismos de incentivo por crédito são uma forma de mediar tais conflitos algoritmicamente, com regras claras impostas pelo próprio sistema.

Bogliolo *et al.* (BOGLIOLO et al., 2012) foram os primeiros a sugerir a utilização de blockchains no suporte a mecanismos de incentivo à cooperação baseados em crédito para eliminar a necessidade de TTP ou de TRSM. A Fig. 3 ilustra, no lado direito, um mecanismo de incentivo baseado em crédito hipotético que se baseia em uma blockchain para implementar métodos seguros para contabilização de tráfego e respectivos pagamentos. O Cap. 4 trata desses mecanismos com blockchain.

2.3.2 Mecanismos baseados em reputação

Os mecanismos baseados em reputação (BUCHEGGER; BOUDEC, 2002; HE; WU; KHOSLA, 2004; MENAKA; RANGANATHAN; SOWMYA, 2017; KALIDOSS et al., 2019) avaliam a atividade dos roteadores para encaminhar os pacotes através dos roteadores mais confiáveis. A reputação de um roteador aumenta conforme esse desempenha a tarefa de encaminhamento de pacotes da vizinhança corretamente. Os mecanismos dessa categoria medem a reputação dos outros roteadores da rede e incorporam técnicas que isolam ou conformam o tráfego de roteadores com comportamento inapropriado, ou seja, dos roteadores com baixos valores de reputação. Por outro lado, os mecanismos de reputação podem priorizar o tráfego de roteadores com bom comportamento. O protocolo CONFIDANT (BUCHEGGER; BOUDEC, 2002) é um exemplo de mecanismo de reputação para MANET. Já o ICARUS (CHARILAS; GEORGILAKIS; PANAGOPOULOS, 2012) é um mecanismo híbrido, com reputação e crédito.

Um problema conhecido nos mecanismos de reputação é o caroneiro de segunda ordem (*second-order free rider*) (PANCHANATHAN; BOYD, 2004; EFSTATHIOU; FRANGOUDIS; POLYZOS, 2006), ou seja, roteadores que optam por não cooperar com os mecanismos de reputação para economizar seus recursos computacionais, energéticos e de rede. Roteadores como esses ainda se aproveitam dos esforços de outros roteadores que executam as tarefas corretamente de forma semelhante ao problema do caroneiro simples. Assim, percebe-se que os esforços para mitigar o problema do caroneiro de uma determinada ordem pode permanecer apresentando o mesmo dilema na próxima ordem.

Existe uma série de trabalhos que implementam mecanismos de reputação utilizando blockchains para gerenciar comportamento inapropriado de roteadores em redes cooperativas (GOKA; SHIGENO, 2018; DAVID; DOWSLEY; LARANGEIRA, 2018; LI; TANG; WANG, 2019; CAREEM; DUTTA, 2020; LWIN; YIM; KO, 2020). Em geral, esses trabalhos adaptam mecanismos já existentes e utilizam blockchains como meios de distribuição seguro das informações de reputação. No entanto, partindo do pressuposto que os mecanismos de reputação são suscetíveis ao problema do caroneiro de segunda ordem, descrito no parágrafo anterior, decidiu-

se por não abordar esses sistemas. É importante observar que os mecanismos de crédito, foco desta tese, não necessitam cooperação dos participantes para detectar e aplicar sanções em caroneiros, portanto, não são suscetíveis ao problema do caroneiro de segunda ordem.

2.3.3 Mecanismos baseados em teoria dos jogos

A teoria dos jogos (MYERSON, 1997) visa modelar situações nas quais múltiplos participantes escolhem estratégias que possuem consequências mútuas. Um jogo consiste em um conjunto de n participantes, $1,2,\ldots,n$, sendo que, cada participante i possui um conjunto de estratégias S_i. Em uma partida do jogo, cada participante i escolhe uma estratégia $s_i \in S_i$. Seja $s = (s_1,\ldots,s_n)$ o vetor de estratégias escolhido pelos participantes de uma partida do jogo e $S = S_1 \times S_2 \times \ldots \times S_n$ o conjunto de todas as possíveis partidas jogadas pelos participantes. O vetor de estratégias $s \in S$ escolhido pelos participantes determina os ganhos de cada um deles. Suponha que um dos participantes sempre consiga um ganho melhor ao utilizar uma determinada estratégia do que outras estratégias, independentemente das estratégias dos outros participantes. Nesse caso, essa é a estratégia dominante do participante. Além disso, se os participante escolhem estratégias tais que nenhum deles consegue mudar de estratégia para obter maior ganho, o jogo alcança o Equilíbrio de Nash. Na teoria dos jogos, os jogos podem ser classificados em: cooperativos ou não-cooperativos, dependendo da possibilidade de formação de coalizão entre os participantes; estáticos ou dinâmicos, a depender dos jogadores decidirem suas jogadas simultaneamente ou um após o outro; repetidos ou com uma interação; finitos ou infinitos; com 2 ou N jogadores.

O projeto algorítmico de teoria dos jogos (ROUGHGARDEN, 2010) é uma subárea que visa estudar problemas de otimização nos quais os dados subjascentes não são conhecidos *a priori* pelo projetista e podem ser, implicitamente ou explicitamente, extraídos de participantes que buscam o interesse próprio. Por exemplo, a determinação do preço de um produto em um leilão. Em linhas gerais, o objetivo é projetar protocolos, ou seja, mecanismos de estímulo à cooperação, que interajam com os participantes de forma que mesmo comportamentos não cooperativos e egoístas desencadeiem os resultados desejados. Particularmente, se o mecanismo desencadeia uma estratégia dominante em que todos os participantes colaboram, se diz que o mecanismo é compatível com o incentivo.

Han *et al.* (HAN et al., 2012) apresentam uma compilação abrangente de trabalhos sobre teoria dos jogos aplicados a redes de computadores, incluindo investigações de mecanismos de incentivo à cooperação no encaminhamento de dados em redes comutadas por pacotes. O encaminhamento de pacotes em uma rede com roteadores não cooperativos pode ser modelado como um jogo repetido. Nesse caso, a cada rodada os roteadores podem se basear em comportamentos anteriores dos demais roteadores e mudar suas estratégias de acordo, permitindo a avaliação da reputação, punição e retribuição. Han *et al.* (HAN; PANDANA; LIU, 2005), por exemplo, modelaram um jogo repetido com auto-aprendizado no qual cada roteador ajusta sua probabilidade de encaminhamento de pacotes iterativamente, a cada rodada, para prevenir que

seja punido pelos outros roteadores.

2.3.4 Efeitos indiretos dos mecanismos de incentivo

Além de servir como estímulo para a implantação de redes sustentáveis em áreas não cobertas por serviços de rede convencionais, os mecanismos de incentivo à cooperação também apresentam outros efeitos colaterais benéficos. Em síntese, os mecanismos de incentivos baseados em crédito repercutem minimizando o tráfego espúrio ou indesejado das redes, reduzindo, assim, o desperdício de recursos. Ao exigir consumo de créditos para enviar tráfego pela rede, esses mecanismos podem, por exemplo: reduzir envios de e-mails indesejados (SPAM) (GOODMAN; ROUNTHWAITE, 2004); minimizar o consumo de banda de *crawlers web* (THELWALL; STUART, 2006); estimular a otimização de protocolos de rede e da configuração de equipamentos para que evitem a produção de tráfego desnecessário; Desencorajar *hot potato routing* (TEIXEIRA et al., 2004) pois cada sistema autônomo tende a utilizar o máximo de sua própria infraestrutura para evitar pagar outros sistemas autônomos pelo tráfego.

Além disso, a diversidade de requisitos de qualidade de serviço (QoS) entre as distintas aplicações pode acarretar em precificações diferentes nos mecanismos de incentivo baseados em crédito (GUPTA; STAHL; WHINSTON, 1999). Aplicações de rede com requisitos mais estritos de banda, latência, *jitter* ou tempo real custam mais para a infraestrutura de rede, logo tendem a ser cobrados de acordo com esse custo. Da mesmo forma, os custos de encaminhamento podem variar de acordo com o horário, sendo os de pico mais caros e os horários com menor tráfego podendo oferecer descontos. No entanto, tais problemas estão fora do escopo desta tese que se limita a tratar do encaminhamento de pacotes sem diferenciação de tráfego. Mesmo assim, o Cap. 4 aborda brevemente esse problema no contexto do estado da arte, tendo em vista avanços em trabalhos futuros que possam considerar os requisitos de QoS no mecanismo de incentivo.

3 CONCEITOS BÁSICOS

Este capítulo aborda conceitos fundamentais utilizados no restante da tese. Primeiramente, são descritos os conceitos de blockchains e contratos inteligentes. Na sequência, são mostrados outros serviços cujo funcionamento é incentivado através de técnicas com blockchains. Em seguida, são apresentados conceitos de multi-assinatura, particularmente o MuSig. Por último, será descrito o princípio de funcionamento do PIFA, um mecanismo de incentivo ao encaminhamento de pacotes baseado em crédito. Os contratos inteligentes Solidity, o esquema de multi-assinatura com limiar *m*-de-*n* MuSig e o mecanismo de incentivo PIFA são utilizados em uma proposta de mecanismo de incentivo baseado em crédito apresentada no Cap. 5.

3.1 BLOCKCHAINS

Blockchains são bancos de dados distribuídos que armazenam transações organizadas em blocos encadeados. Novas transações são validadas e acordadas entre os participantes através de protocolos de consenso distribuído específicos que definem os novos blocos de transações a serem encadeados na blockchain. As blockchains aplicam técnicas de criptografia para garantir a integridade dos blocos e de suas respectivas transações. As transações consistem tipicamente em registros de transferências financeiras ou de alteração de estados de programas, denominados contratos inteligentes (*smart contracts*) (ZHENG et al., 2020).

O Bitcoin (NAKAMOTO, 2008) foi o primeiro sistema de blockchain a se popularizar. Foi proposto como um meio de pagamentos através da Internet que não depende da confiança em terceiros (TTP), em oposição ao sistema financeiro dominante. Para isso, o sistema gerencia de forma segura a propriedade e as transações de transferência de uma moeda digital própria, também chamada de criptomoeda. Nessa aplicação, que é a mais difundida, as blockchains também são chamadas de livros-razão distribuídos (*distributed ledgers*) como analogia aos livros utilizados em registros contábeis.

O Bitcoin opera sobre uma rede P2P que serve para a transmissão das transações pendentes e dos blocos de transações criados pelos participantes do sistema. O mecanismo de consenso distribuído do Bitcoin é baseado na dificuldade de criar novos blocos em um processo chamado de mineração. Nesse mecanismo, participantes denominados mineradores competem para solucionar um desafio computacionalmente intensivo, conhecido e verificável por todos. O minerador que resolver o desafio antes é recompensado com tarifas pagas pelos requisitantes das transações mineradas e com emissão de nova criptomoeda, como forma de incentivo à cooperação no trabalho de mineração. A solução do problema é chamada de prova de trabalho (PoW) e seu resultado serve para o encadeamento do novo bloco de transações criado pelo minerador. No Bitcoin, o desafio do PoW é o cálculo por tentativa e erro de um resumo criptográfico SHA-256 (EASTLAKE; HANSEN, 2011) cujo valor seja menor que um número conhecido. A entrada do cálculo do resumo criptográfico é o conteúdo do bloco, o resumo criptográfico do bloco anterior, e um *nonce* variável. A Fig. 4 mostra a estrutura típica de um bloco encadeado na

blockchain do Bitcoin. Nela é possível identificar o resumo criptográfico (*hash*) utilizado para encadear os blocos de forma segura, o *nonce* que derivou esse resumo criptográfico, e as transações (TX), cuja integridade é garantida com uma árvore de Merkle (DAHLBERG; PULLS; PEETERS, 2016).

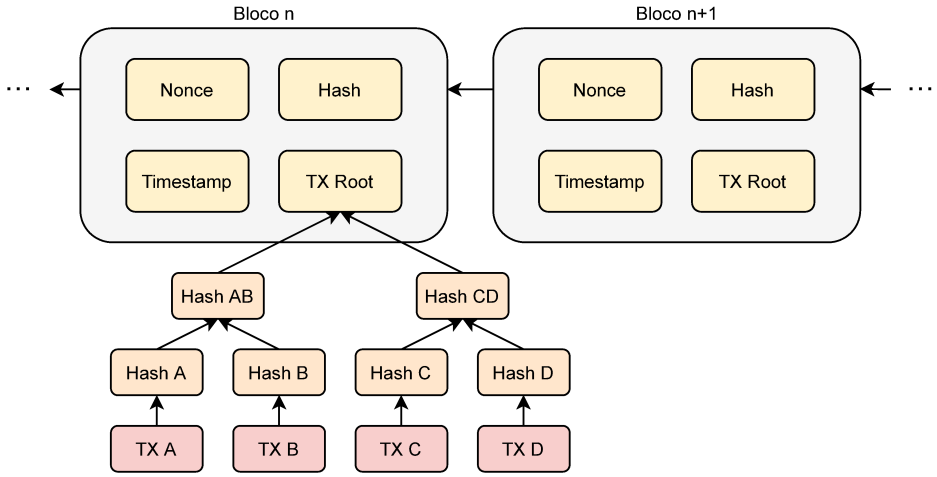


Figura 4 – Estrutura típica de uma blockchain.

A Tab. 1 classifica os principais tipos de mecanismo de consenso empregados em blockchains de acordo com Zheng *et al.* (ZHENG et al., 2017). Nesta classificação as blockchains podem ser públicas, de consórcio ou privadas. As públicas são como as blockchains pioneiras nas quais não existe necessidade de autorização prévia para participar no mecanismo de consenso. As blockchains de consórcio (ou federadas) e as blockchains privadas, requerem que o sistema conceda permissão para que se participe do mecanismo de consenso, por isso são chamadas também de blockchains permissionadas. A diferença básica entre as duas é que nas de consórcio os participantes são representantes de organizações e nas privadas os participantes são indivíduos. Além de precisarem de permissão para entrada de participantes, em ambos os casos, esses são em número limitado, com tendência à centralização, ou seja, propriedades em oposição à motivação das blockchains pioneiras como o Bitcoin, que não exigem o estabelecimento de confiança entre os participantes.

O surgimento do Bitcoin inspirou outras criptomoedas que também foram criadas com o princípio do PoW, mas não tardou para que surgissem alternativas a esse mecanismo de consenso. As críticas ao PoW dizem respeito ao custo computacional e, principalmente, energético, que, no caso do Bitcoin, hoje supera até mesmo o consumo total de diversos países (VRANKEN, 2017). Assim, vários protocolos surgiram com a finalidade de evitar o dispêndio de energia do PoW. Além dos protocolos de consenso bizantino, como o PBFT (GRAMOLI, 2020), que são muito adotados em blockchains de consórcio e privadas, a prova de participação (PoS) (NGUYEN et al., 2019) é um princípio de funcionamento bastante disseminado. No PoS, o grau de poder decisório de cada participante sobre o conteúdo dos novos blocos da blockchain é determinado pela quantidade de criptomoeda que o participante possui alocada no sistema.

Tabela 1 – Tipos de blockchains.

Propriedades da Blockchain	**Pública**	**Consórcio**	**Privada**
Determinação do consenso	Sem restrição	Membros	Membros
Participação no consenso	Sem permissão	Com permissão	Com permissão
Permissão de Leitura	Pública	Pública ou restrita	Pública ou restrita
Imutabilidade	Difícil adulterar	Possível adulterar	Possível adulterar
Eficiência	Baixa	Alta	Alta
Centralização	Não	Parcial	Sim

Os sistemas de blockchain apresentaram problemas de escalabilidade que impediram seu uso em várias aplicações. Entre esses problemas, podem-se destacar: baixa vazão, medida em transações por segundo (tps); alto custo nas tarifas cobradas pelas transações; alto custo de armazenamento, necessário para a cópia do arquivo da blockchain. O tempo de confirmação das transações também é um problema que está relacionado com a frequência que novos blocos de transações são criados.

Diversos trabalhos foram desenvolvidos com o objetivo de mitigar essas limitações de escalabilidade (KIM; KWON; CHO, 2018; ZHOU et al., 2020). Os trabalhos podem ser classificados como soluções de camada 1 (*on-chain*) (LAU, 2016; EYAL et al., 2016; ZAMANI; MOVAHEDI; RAYKOVA, 2018; LOMBROZO; LAU; WUILLE, 2015; SILVANO; MARCELINO, 2020) e de camada 2 (*off-chain*). As soluções de camada 1 modificam aspectos dos mecanismos de consenso distribuído e conseguem obter uma sensível melhora na escalabilidade. As soluções de camada 2 são desacopladas do mecanismo de consenso distribuído e conseguem alcançar melhoras de escabilidade muito mais significativas que as soluções de camada 1. Nesse caso, múltiplas transações são efetuadas em um mecanismo paralelo seguro, muito mais rápido e barato, para posteriormente serem compensadas na blockchain. As principais soluções de escalabilidade de camada 2 são os canais e as *childchains*.

Canais foram amplamente aplicados nos mecanismos de incentivo encontrados no estado da arte (Cap. 4) para implementar ideias similares a cheques e cauções. O estabelecimento de um canal, ilustrado na Fig. 5, exige dos participantes um caução em criptomoeda que é retido na blockchain como garantia para as transações de micropagamentos. Os micropagamentos no canal podem ser comparados a cheques, e se tratam de transações seguras mantidas no canal e fora da blockchain até que alguma das partes faça a compensação do canal na blockchain. O número de transações permitidas em um canal é praticamente infinito, mas o total de criptomoeda trocado nessas transações é limitado pelo caução depositado. O Lightning (POON; DRYJA, 2016) e o Raiden (NETWORK, 2019) são implementações de canais para o Bitcoin e o Ethereum, respectivamente, e funcionam para micropagamentos. Existem também propostas de canais de estado (*state channels*) (DZIEMBOWSKI; FAUST; HOSTÁKOVÁ, 2018) cujo

propósito é permitir transações para contratos inteligentes na mesma perspectiva dos canais de micropagamentos.

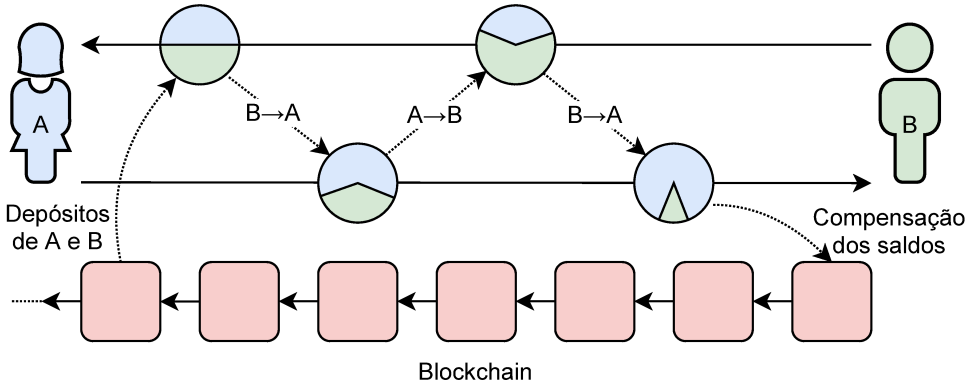


Figura 5 – Canais de micropagamentos.

Childchains (POON; BUTERIN, 2017; POLYGON, 2021) são mecanismos que permitem conectar blockchains filhas a uma blockchain base, também chamada *rootchain*, em uma estrutura de árvore. Durante o funcionamento sem fraudes as blockchains filhas operam de forma rápida e com custos relativamente baixos, se comparados à blockchain base. A integridade das transações é assegurada registrando a raiz de uma árvore de Merkle dos blocos da blockchain filha na blockchain base. Essa operação é realizada por nodos específicos chamados operadores. Disputas devido a fraudes devem ser escaladas para a blockchain base, o que pode tornar a operação das *childchains* onerosa. Tanto os canais como as *childchains* são implementados através de contratos inteligentes, ou algum esquema de *scripts*, no caso do Bitcoin.

Apesar do nome, a tecnologia de contratos inteligentes consiste na realidade em *programas ou scripts persistentes* que não são necessariamente contratos e não possuem nenhuma característica que possa ser chamada de inteligente (LITAN, 2020). Os contratos inteligentes garantem a execução do mesmo código por todos os participantes de um determinado sistema sem a necessidade de TTP. A plataforma de contratos inteligentes de blockchain mais disseminada é a *Ethereum Virtual Machine* (EVM) do Ethereum que executa programas compilados em um *bytecode* específico, escritos em linguagens de programação como a Solidity, com compilador de mesmo nome, conforme ilustrado na Fig. 7. A execução de programas na EVM produz uma série de transações que alteram o estado do programa, de forma que todo o histórico de alterações do programa permanece registrado na blockchain e não pode ser alterado.

Assim como as transações de transferência de criptomoeda, as transações que alteram os estados desses programas também consomem criptomoeda. A quantidade de criptomoeda que as funções dos contratos inteligentes Solidity consomem é medida em unidades de gás, cujo preço em criptomoeda oscila de acordo com a demanda por transações na blockchain. Além disso, contratos inteligentes podem depender de dados externos. Nesse caso, o problema da dependência de TTP reaparece e a solução atual são os oráculos (ZHENG et al., 2020), ou seja, serviços que funcionam como agentes que coletam as informações e as disponibili-

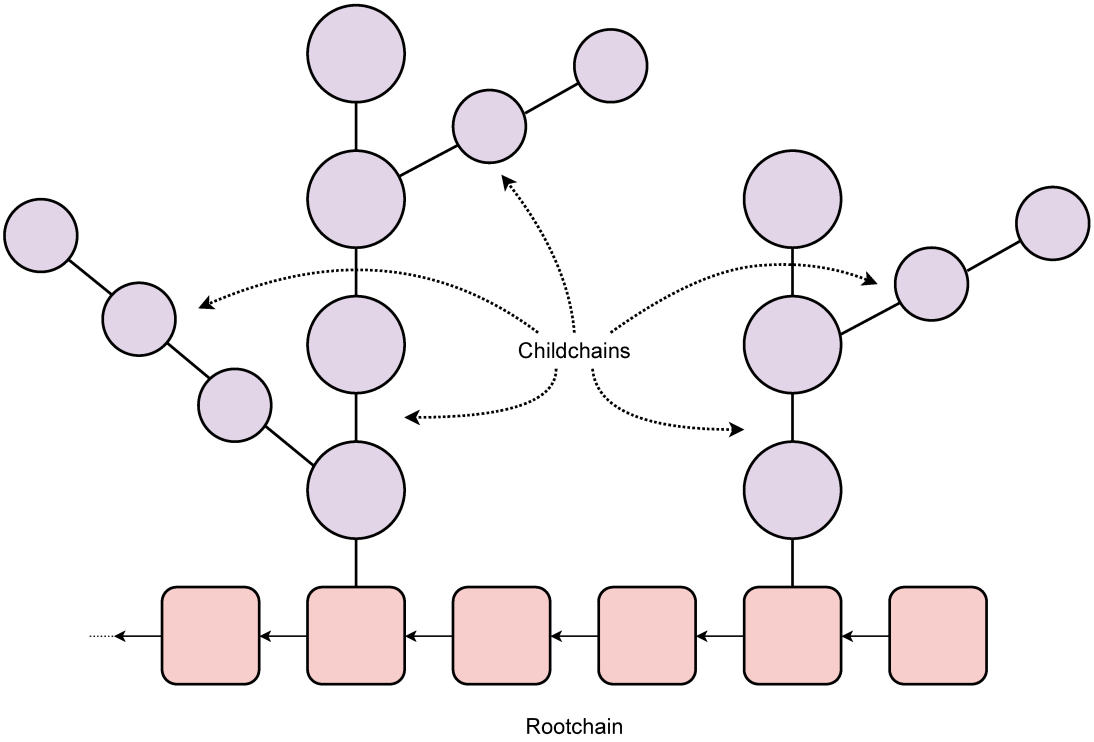


Figura 6 – Childchains.

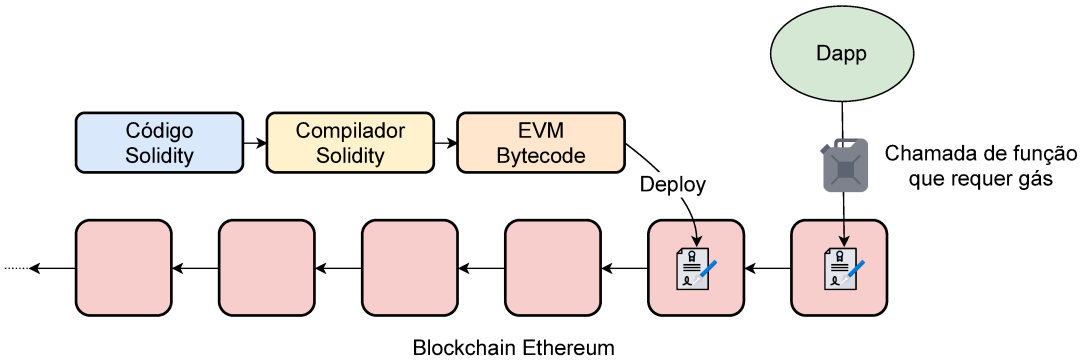


Figura 7 – Compilação de contrato inteligente Solitity e implantação na EVM.

zam para os contratos inteligentes. Por último, os contratos inteligentes também podem servir para criar *tokens* lastreados em uma criptomoeda específica. Nesse contexto, o ERC-20 é um padrão de protocolo que define regras para contratos inteligentes para emitirem *tokens* no Ethereum (DOURLENS, 2020).

3.1.1 Serviços incentivados com blockchains

Desde o seu surgimento, as tecnologias de blockchain vêm sendo exploradas para criação de incentivos à cooperação e intermediação de serviços de forma independente de TTP. Por exemplo, no contexto de economia de compartilhamento (*sharing economy*) (HU, 2019) (ex: Blablacar, Couchsurfing e Zipcar), as blockchains podem viabilizar plataformas digitais descentralizadas (PAZAITIS; DE FILIPPI; KOSTAKIS, 2017; HAWLITSCHEK; NOTHEISEN;

TEUBNER, 2018) para mutualização de bens, espaços e instrumentos, além da organização das pessoas em redes ou comunidades. As abordagens dos incentivos vão desde a adaptação dos mecanismos de consenso para recompensar participantes que contribuem com seu funcionamento até a simples utilização de *tokens* para pagamentos pelos serviços. No entanto, com frequência, as propostas tratam as tecnologias de blockchain como uma panaceia, não conseguem implementar incentivos eficientes e são vulneráveis a ataques Sybil (IQBAL; MATULEVIČIUS, 2021). Nesta seção, são apresentados alguns sistemas que visam produzir incentivos para serviços, além do encaminhamento de pacotes para comunicação de dados, que é foco desta tese. Os mecanismos de incentivo e conceitos adotados por estes sistemas apresentam características que podem ser exploradas futuramente para aprimoramento do estado da arte.

Mineração útil

Os mecanismos de consenso baseados em PoW exigem a resolução de problemas computacionalmente intensivos pelos participantes da blockchain. Alguns sistemas procuraram combinar cálculos com alguma utilidade extra nos desafios do PoW (WANG et al., 2019). Por exemplo: o Primecoin (KING, 2013), que calcula números primos; o Nooshare (COVENTRY, 2012), que executa simulações de Monte Carlo; e o Proof of eXercise (SHOKER, 2017), que resolve matrizes para problemas científicos.

Armazenamento de dados

Também foram propostas alternativas que fornecem serviços de armazenamento de dados distribuído incentivados por blockchains (HUANG et al., 2020). O Filecoin (BENET; GRECO, 2017), por exemplo, é um sistema de pagamentos baseado em blockchains que suporta um serviço de armazenamento de dados chamado IPFS. Esse sistema utiliza uma série de provas no seu mecanismo de consenso, como provas da replicação dos dados e da capacidade de armazenamento dos participantes. A partir dos valores dessas provas é realizado um sorteio para designar o participante que definirá o próximo bloco de transações da blockchain. O Dtube (DOAN et al., 2020) é uma proposta de serviço de vídeo sob demanda que utiliza o IPFS como meio de armazenamento do conteúdo além da blockchain de redes sociais Steem (LI; PALANISAMY, 2019) para recompensar os usuários pela interação nos vídeos (compartilhamentos, comentários e reações).

Comércio de dados

Plataformas de comércio de dados (*Data Trading*) facilitam a compra e venda de conjuntos de dados (*datasets*), colocando vendedores e compradores em contato. Chen *et al.* (CHEN et al., 2019a) propuseram uma plataforma de comércio de dados para IoV que implementa um mecanismo de leilão duplo que garante a privacidade dos participantes. No

trabalho de Dai *et al.* (DAI et al., 2020), tanto a plataforma de comércio de dados quanto os compradores não conseguem obter acesso aos dados brutos do vendedor, apenas ao resultado de uma análise específica desejada sobre esses dados.

Comércio de energia

Os avanços em energias renováveis como painéis solares e turbinas eólicas permitiram a produção de energia também nos consumidores finais que podem vender energia excedente. Nesse contexto, as blockchains podem coordenar mercados de energia locais e incentivar a participação desses produtores locais (MENGELKAMP et al., 2018; ANDONI et al., 2019). Além disso, criptomoedas de crédito de energia foram propostas no PETCON (KANG et al., 2017) e no BEST (CHAUDHARY et al., 2019) para transações de comércio de energia entre veículos elétricos e *microgrids* de energia utilizando blockchains de consórcio.

Cloud/fog e edge computing

Muitos trabalhos foram propostos para a Internet das Coisas (IoT) no contexto de computação em nuvem/névoa (*cloud/fog*) e borda (*edge*) para alugar a capacidade de processamento ociosa dos equipamentos e para aliviar a carga de dispositivos com recursos limitados. O trabalho de Taghavi *et al.* (TAGHAVI et al., 2020) apresenta uma federação colaborativa de provedores de nuvem que podem comercializar sua capacidade de processamento entre si e implementar um monitoramento baseado em blockchain para detectar violações nos acordos de nível de serviço (SLA). Xiong *et al.* (XIONG et al., 2018) propõem um sistema no qual dispositivos móveis com recursos limitados compram capacidade de processamento de servidores de borda para tarefas de mineração cuja partilha da recompensa é calculada através de um modelo de Stackelberg. Um esquema similar foi proposto para computação em nuvem/névoa utilizando mecanismos de leilão (JIAO et al., 2019). Liu et. al. (LIU et al., 2019) propuseram recompensas para nodos de borda para computação de serviços móveis (MEC) que realizam tarefas de transcodificação de vídeo em um serviço de *streaming* distribuído. Lin *et al.* (LIN et al., 2020) projetaram uma blockchain privada para permitir que servidores de borda calculem emparelhamentos bilineares de forma segura para nodos IoT com recursos limitados.

3.2 MULTI-ASSINATURAS

Assinaturas digitais representam um componente fundamental das blockchains. Servem para autenticar as transações de transferências de criptomoeda e de chamadas de função dos contratos inteligentes. No Bitcoin, por exemplo, cada participante possui um par de chaves assimétricas que servem para derivar endereços do Bitcoin e assinar transações de transferência de criptomoeda. Cada participante pode ter vários endereços derivados dessas chaves e cada transação transfere criptomoeda de um endereço para outro. A Fig. 8 ilustra como isso acontece

no Bitcoin para o caso de transferência de 4 BTC de um endereço do participante A para um endereço do participante B utilizando assinaturas ECDSA (JOHNSON; MENEZES; VANSTONE, 2001). As chaves públicas são distribuídas e servem para que qualquer participante da rede do Bitcoin verifique a validade das transações.

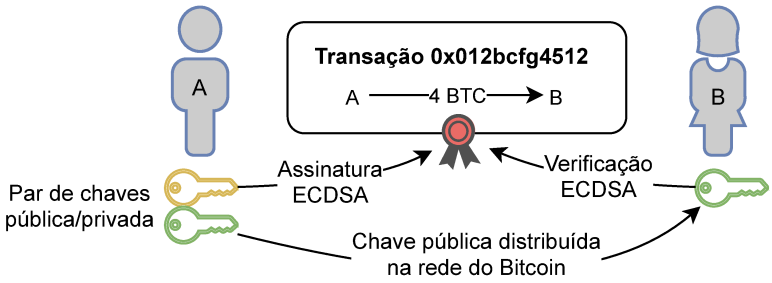


Figura 8 – Assinatura de transação no Bitcoin.

Multi-assinaturas (ITAKURA; NAKAMURA, 1983) são esquemas de criptografia que permitem que um conjunto de signatários assinem um mesmo conjunto de dados simultaneamente utilizando suas chaves privadas. Entre as aplicações desses esquemas em blockchains pode-se destacar as transações multi-assinatura e votações de blocos em consensos PoS, de consórcio ou federado, conforme ilustrado na Fig. 9. Nas transações multi-assinatura, a exemplo do Bitcoin MultiSig, as transações são consideradas válidas quando um determinado número dos signatários assina (ANDRESEN, 2011). Nas votações de consenso, um mínimo de participantes estipulado pelo protocolo de consenso deve assinar o novo bloco da blockchain para que ele seja incluído (DRIJVERS et al., 2020). Em ambos os casos, a solução trivial é cada signatário produzir uma assinatura sobre a mesma transação (ou bloco) independentemente dos demais signatários. No entanto, tal solução traz como desvantagem a necessidade de muito espaço de armazenamento para as assinaturas e para as respectivas chaves públicas, o que acaba provocando problemas de escalabilidade para a blockchain.

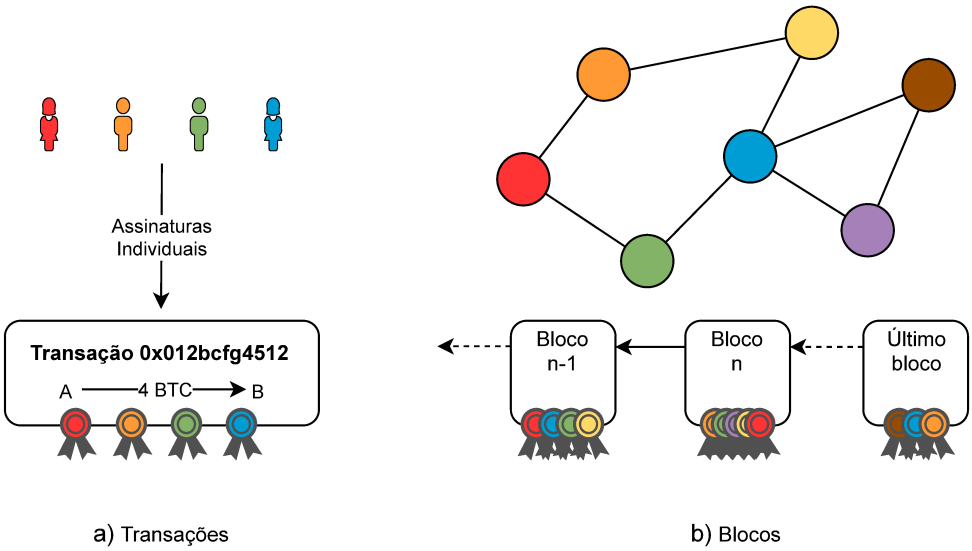


Figura 9 – Aplicação de multi-assinaturas para transações (a) e blocos (b).

Para ser útil e prático, um esquema de multi-assinaturas precisa produzir assinaturas cujo tamanho é independente do número de signatários e o mais próximo possível de uma assinatura individual comum (Fig. 10). Esses esquemas foram estudados extensivamente com abordagens baseadas em RSA (ITAKURA; NAKAMURA, 1983; OHTA; OKAMOTO, 1993; OKAMOTO, 1993; KOMANO et al., 2006), logaritmos discretos (HARDJONO; ZHENG, 1993; LI; HWANG; LEE, 1995; HARN, 1994; HORSTER; MICHELS; PETERSEN, 1995; CHANG et al., 1998; OHTA; OKAMOTO, 1999; BURMESTER et al., 2000; MICALI; OHTA; REYZIN, 2001; CASTELLUCCIA et al., 2005; BELLARE; NEVEN, 2006; BAGHERZANDI; CHEON; JARECKI, 2008; BAGHERZANDI; JARECKI, 2008; MA et al., 2010; MAXWELL et al., 2019), emparelhamentos bilineares (BOLDYREVA, 2002; LU et al., 2006; RISTENPART; YILEK, 2007; BOLDYREVA et al., 2007; LE; BONNECAZE; GABILLON, 2009) e reticulados (BANSARKHANI; STURM, 2016).

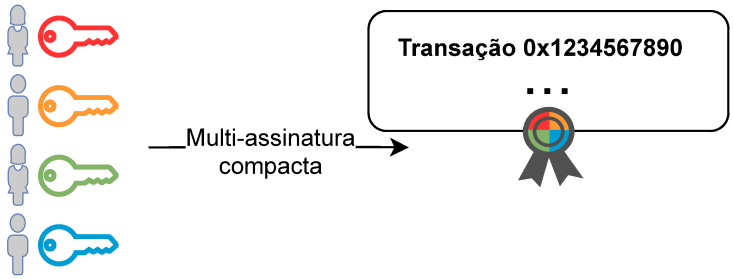


Figura 10 – Multi-assinatura compacta.

Um problema importante quando se lida com esquemas de multi-assinaturas são os ataques de chave forjada (*rogue-key attacks*). Nesse tipo de ataque, um dos signatários pode agir como um adversário se tiver a oportunidade de ler as chaves públicas dos demais participantes antes da divulgação da sua própria chave pública. Esse adversário pode enganar os demais participantes criando uma chave pública especialmente forjada, de forma que possa produzir facilmente multi-assinaturas falsas para mensagens. Diante desse problema, foram criados esquemas de multi-assinatura com mecanismos mais robustos para o estabelecimento de chaves. Apesar desses esquemas serem resistentes aos ataques de chave forjada, eles introduzem um sobrecusto muito alto, envolvem pressupostos irrealistas ou dependem de requisitos de configuração inviáveis para infraestruturas de chaves públicas (PKI) convencionais (HORSTER; MICHELS; PETERSEN, 1995; MICHELS; HORSTER, 1996; MICALI; OHTA; REYZIN, 2001; BOLDYREVA, 2002; BONEH et al., 2003; BELLARE; NEVEN, 2006; LU et al., 2006; BELLARE; NAMPREMPRE; NEVEN, 2007; RISTENPART; YILEK, 2007).

Bellare e Neven criaram o primeiro esquema multi-assinatura resistente a ataques de chave forjada que permitiu operar sobre um modelo de chave pública simples (*plain public-key model*) (BELLARE; NEVEN, 2006). Nesse modelo, não é necessário que cada signatário apresente uma prova de conhecimento da chave privada correspondente à sua chave pública aos co-signatários ou a uma autoridade certificadora, como exigiam as outras estratégias que buscavam prevenir ataques de chave forjada. Basta que cada signatário apresente sua chave

pública aos co-signatários através de algum método que garanta sua autenticidade, como uma PKI convencional ou mesmo presencialmente.

Mesmo com essa vantagem, o esquema de Bellare e Neven ainda requer que o verificador possua todas as chaves públicas envolvidas na multi-assinatura. Esse requisito é inadequado para blockchains em diversos cenários pois implica em maiores custos de armazenamento, comunicação e verificação. Com o intuito de eliminar esse requisito, foram criados esquemas multi-assinatura com agregação de chaves públicas que permitem assinaturas mais compactas (Fig. 11). Nesses esquemas, o verificador precisa conhecer apenas uma chave pública agregada da multi-assinatura, gerada com base nas chaves públicas de todos os signatários da mensagem. Entre esses esquemas destacam-se os trabalhos de Boneh *et al.* (BONEH; DRIJVERS; NEVEN, 2018) e Maxwell *et. al.* (MAXWELL et al., 2019). O primeiro utiliza emparelhamentos bilineares e o segundo utiliza logaritmos discretos.

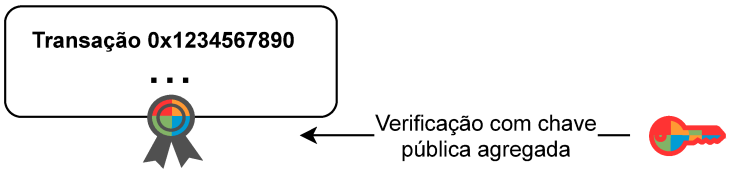


Figura 11 – Multi-assinatura com chaves públicas agregadas.

Outra funcionalidade importante é a possibilidade de multi-assinaturas com limiar (*threshold signatures*) ou multi-assinaturas m-de-n, nas quais um mínimo de m de um total de n signatários possíveis deve assinar a mensagem para que ela seja considerada válida. Conforme Maxwell *et al.* (MAXWELL et al., 2019), tal funcionalidade é possível de ser implementada gerando todas as combinações possíveis de chaves públicas agregadas e é viável quando $\sum_{k=m}^{n} \binom{n}{k}$ resultar em um número que permita gerar uma árvore de Merkle (DAHLBERG; PULLS; PEETERS, 2016) que garanta a integridade dessas chaves.

Importante ressaltar que o próprio Bitcoin Multisig já permite assinaturas m-de-n, mas não representa um mecanismo multi-assinatura no sentido estrito, visto que depende de múltiplas assinaturas ECDSA convencionais dos signatários, em vez de produzir uma assinatura conjunta compacta. Além disso, não possui agregação de chaves públicas, exigindo que cada transação informe as chaves públicas de todos os signatários, tornando o Bitcoin Multisig bastante limitado em relação ao número de signatários. A atualização BIP340 (WUILLE; NICK; RUFFING, 2020) do Bitcoin, conhecida como Taproot, introduz vários aprimoramentos, incluindo a eliminação dessas limitações do Multisig utilizando o esquema MuSig. A versão do MuSig do Taproot é chamada MuSig2 (NICK; RUFFING; SEURIN, 2021) e consiste em um aprimoramento para precisar de apenas duas rodadas de interação em vez de três rodadas como a versão do MuSig original.

O esquema de multi-assinatura MuSig original foi escolhido para o trabalho desta tese por permitir multi-assinaturas com limiar m-de-n no modelo de chaves públicas simples e sem exigir que os signatários comprovem a posse da chave privada correspondente à sua chave pú-

blica. O MuSig2 além de outros esquemas de multi-assinatura como o baseado em BLS (BONEH; DRIJVERS; NEVEN, 2018) e o FROST (KOMLO; GOLDBERG, 2021) serão avaliados em trabalhos futuros.

3.2.1 MuSig

MuSig (MAXWELL et al., 2019) é um esquema multi-assinatura baseado no algoritmo de Schnorr (SCHNORR, 1991) que permite agregação de chaves públicas. O esquema é demonstravelmente seguro sob o pressuposto do problema do logaritmo discreto e no modelo de chaves públicas simples (signatários precisam ter uma chave pública mas não precisam provar que possuem a respectiva chave privada a uma autoridade certificadora ou para os demais participantes antes de iniciar o protocolo). Isso permite que um grupo de signatários produza uma assinatura conjunta compacta para uma mensagem em comum.

O MuSig é parametrizado com os parâmetros de grupo $(\mathbb{G}, p, g)$ onde p é um inteiro com k bits, $\mathbb{G}$ é um grupo cíclico de ordem p, e g é um gerador de $\mathbb{G}$, e por três funções de resumo criptográfico $(\mathrm{H}_{com}, \mathrm{H}_{agg}, \mathrm{H}_{sig})$ de $\{0,1\}^*$ para $\{0,1\}$. O processo de multi-assinatura é subdividido em três rodadas como segue:

Rodada 1

Dado um grupo de n signatários que desejam assinar uma mensagem m. Seja X_1 e x_1 o par de chaves pública e privada, respectivamente, de um signatário específico, sejam $X_2, ..., X_n$ as chaves públicas dos demais co-signatários, e seja $\langle L \rangle$ o multiconjunto de todas as chaves públicas envolvidas no processo de assinatura. Para todo $i \in \{1, ..., n\}$, o signatário computa

$$a_i = \mathrm{H}_{agg}(\langle L \rangle, X_i) \tag{3.1}$$

assim como a chave pública agregada

$$\tilde{X} = \prod_{i=1}^{n} X_i^{a_i} \tag{3.2}$$

Rodada 2

O signatário gera aleatoriamente um *nonce* privado $r_1 \leftarrow \mathbb{Z}_l$, computa $R_1 = g^{r_1}$ (o *nonce* público), o compromisso $t_1 = \mathrm{H}_{com}(R_1)$, e envia t_1 para todos os outros co-signatários. Assim que o signatário recebe os compromissos $t_2, ..., t_n$ de todos os co-signatários, ele envia R_1 como resposta. Esse procedimento garante que o *nonce* público não será exposto para um eventual co-signatário adversário antes que todos os compromissos sejam recebidos. Assim que recebe $R_2, ..., R_n$ dos demais co-signatários, o signatário verifica se $t_i = \mathrm{H}_{com}(R_i)$ para todo $i \in \{2, ..., n\}$. Se essa condição não for satisfeita então o protocolo é cancelado.

Rodada 3

Se todos os *nonces* públicos puderem ser verificados utilizando os compromissos, então computar

$$\begin{aligned} R &= \prod_{i=1}^{n} R_i \\ c &= \mathrm{H}_{sig}(\tilde{X}, R, m) \\ s_1 &= r_1 + c a_1 x_1 \mod p \end{aligned} \tag{3.3}$$

A assinatura s_1 é enviada para todos os co-signatários. Assim que receber $s_2, ...s_n$ dos co-signatários, o signatário pode computar

$$s = \sum_{i=1}^{n} s_i \mod p. \tag{3.4}$$

A multi-assinatura é

$$\sigma = (R, s) \tag{3.5}$$

Dada uma chave pública agregada $\tilde{X}$ e uma mensagem m, para verificar se uma multi-assinatura σ é válida, o verificador pode calcular

$$c = \mathrm{H}_{sig}(\tilde{X}, R, m), \tag{3.6}$$

e aceitar a multi-assinatura σ se

$$g^s = R\tilde{X}^c. \tag{3.7}$$

O MuSig também permite implementar uma política de limiar na qual é necessário que no mínimo m (não confundir com a mensagem m que é assinada) de um total de n signatários possíveis assinem a mensagem para a multi-assinatura ser válida. Essa funcionalidade pode ser implementada construindo uma árvore de Merkle na qual as folhas são as combinações permitidas de chaves públicas (na forma de chaves públicas agregadas), e os nodos são resumos criptográficos H_{tree} (ex: SHA-256). A árvore de Merkle deve ser uma árvore binária cheia, por isso, a última chave pública agregada deve ser repetida até que o número de folhas seja uma potência de 2. O processo de verificação da multi-assinatura deve receber como entrada a chave pública agregada $\tilde{X}$ correspondente ao conjunto de signatários da mensagem, a multi-assinatura $\sigma = (R, s)$ e a prova Merkle $\mathcal{M}_{proof}$ correspondente à folha. Assim, a validade vai depender da multi-assinatura ser válida com a chave pública agregada $\tilde{X}$ informada, e uma prova de que essa chave é uma das folhas da árvore de Merkle, identificada pelo resumo criptográfico da sua raiz $\mathcal{M}_{root}$. Essa abordagem só é possível quando o total de chaves públicas agregadas permitidas $\sum_{k=m}^{n} \binom{n}{k}$ for viável.

A Fig. 12 ilustra um exemplo de árvore de Merkle com uma prova Merkle ($\mathcal{M}_{proof} = F_6, F_{12}, F_{13}$) que permite verificar se a chave pública agregada $\tilde{X}_5$ é uma folha válida para uma determinada raiz dessa árvore ($\mathcal{M}_{root}$).

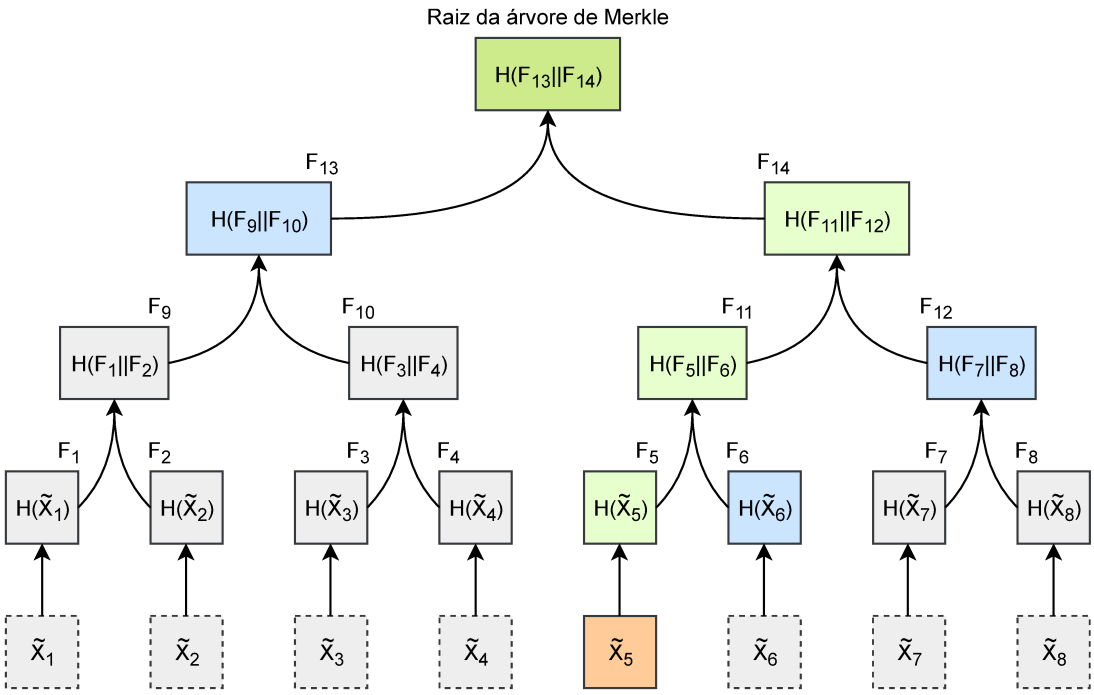


Figura 12 – Exemplo de prova Merkle em uma árvore de Merkle para a mensagem M_5.

Nesse exemplo, os resumos criptográficos de $\mathcal{M}_{proof}$ (em azul) servem para calcular os resumos criptográficos do percurso da árvore (em verde claro) de forma que produzam um valor igual ao de $\mathcal{M}_{root}$ (em verde escuro). Assim, para verificar $\tilde{X}_5$ (em laranja) não é necessário possuir toda a árvore de Merkle, apenas $\mathcal{M}_{proof}$ e $\mathcal{M}_{root}$.

3.3 PIFA

O *Protocol Independent Fairness Algorithm* (PIFA) (YOO; AHN; AGRAWAL, 2005) é um mecanismo de incentivo ao encaminhamento de dados baseado em crédito para redes cooperativas. O seu princípio de funcionamento é um esquema de contabilização de tráfego que permite detectar e isolar roteadores maliciosos que tentarem trapacear os outros roteadores na contabilização do número de pacotes de dados encaminhados para tentar obter mais créditos do que eles têm direito de receber. O algoritmo do PIFA assume que os roteadores não conhecem os caminhos completos entre a origem e o destino dos pacotes de forma que pode ser aplicado independentemente de protocolo de roteamento.

A versão original do PIFA possui um serviço centralizado de contabilização de crédito chamado *Credit Manager* (CM) que recebe mensagens com informações de contabilização de tráfego de todos os roteadores da rede. Periodicamente, cada roteador envia mensagens de contabilização de tráfego das suas interfaces para o CM. Para cada interface que o roteador

que está reportando o tráfego (RID) possui com um roteador vizinho, é enviada uma mensagem PIFA cujos campos estão detalhados na Tab. 2. Cada mensagem possui as estatísticas do tráfego trocado com um roteador vizinho específico (NID) durante um período identificado por um número de sequência (SEQ).

Tabela 2 – Mensagem PIFA de RID contabilizando tráfego do enlace com NID.

Campo	**Nome**	**Descrição**
RID	*Router Identifier*	Identificador do roteador que está enviando a mensagem de contabilização
NID	*Neighbor Identifier*	Identificador do roteador vizinho do enlace sendo contabilizado
I	*Input*	Pacotes que entram em RID pelo enlace com NID
O	*Output*	Pacotes que saem de RID para o enlace com NID
S	*Source*	Pacotes criados por RID enviados para o enlace com NID
T	*Termination*	Pacotes destinados a RID recebidos no enlace com NID
OFN	*Originated From Node*	Pacotes que entram em RID pelo enlace com NID e que foram originados por NID

De posse das contabilizações de tráfego individuais, o CM pode inferir a topologia de rede atual e a credibilidade do que foi reportado por cada um dos roteadores com base nos critérios a seguir, considerando que $\mathrm{Q}_{n,m}$ denota o campo Q de uma mensagem na qual n = RID e m = NID são vizinhos.

1. O número de pacotes que saem de um roteador n deve ser o mesmo que o número de pacotes que chegam no roteador m na outra terminação do enlace.

$$\mathrm{O}_{n,m} = \mathrm{I}_{m,n} \tag{3.8}$$

2. O número de pacotes encaminhados por um roteador n (F_n) que possui um conjunto de vizinhos A_n deve ser o mesmo que

   a) O número de pacotes que entram nele e que não terminam nele

   b) O número de pacotes que saem dele e que não foram originados por ele

$$\mathrm{F}_n = \sum_{m \in A_n} \mathrm{I}_{n,m} - \sum_{m \in A_n} \mathrm{T}_{n,m} = \sum_{m \in A_n} \mathrm{O}_{n,m} - \sum_{m \in A_n} \mathrm{S}_{n,m} \tag{3.9}$$

3. O valor S de um roteador deve ser idêntico ao valor de OFN do roteador da outra terminação do enlace. OFN visa prevenir que um roteador malicioso manipule F_n alterando $\sum \mathrm{T}$ e $\sum \mathrm{S}$ ao mesmo tempo no critério (2). O OFN é calculado contando o número de pacotes de entrada de um enlace que foram originados do próprio vizinho nesse enlace.

$$\mathrm{OFN}_{m,n} = \mathrm{S}_{n,m} \tag{3.10}$$

As Figuras. 13, 14 e 15 ilustram os critérios de credibilidade apresentados. Na Fig. 13, o roteador a possui um enlace com um roteador vizinho b. Nesse caso, todo o tráfego de saída do roteador a através desse enlace deve corresponder ao tráfego de entrada do roteador b nesse enlace. Nas Figuras. 14 e 15, o roteador a possui quatro enlaces com outros quatro roteadores nomeados de b até e, logo, $A_a = \{b,c,d,e\}$. A Fig. 14 ilustra o total de tráfego encaminhado pelo roteador a nas linhas tracejadas, cujo valor deve ser o mesmo que a soma do tráfego que entra pelos enlaces dos vizinhos de a subtraído pela parte desse tráfego que é destinada ao próprio roteador a. Além disso, esse total também deve ser o mesmo que a soma do tráfego de saída do roteador a para os enlaces com b, c, d, e e, subtraído pela parte desse tráfego que foi originada pelo próprio roteador a. Na Fig. 15, o roteador b contabiliza o tráfego que recebe pelo enlace com o roteador a que é originado pelo próprio roteador a.

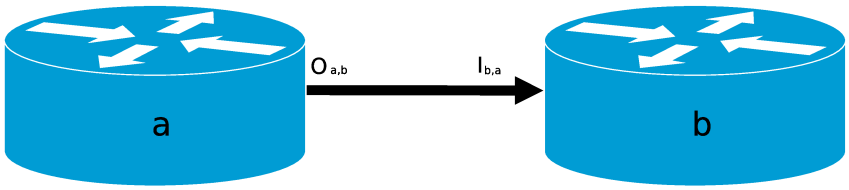


Figura 13 – Critérios de credibilidade PIFA: $O_{n,m} = I_{m,n}$.

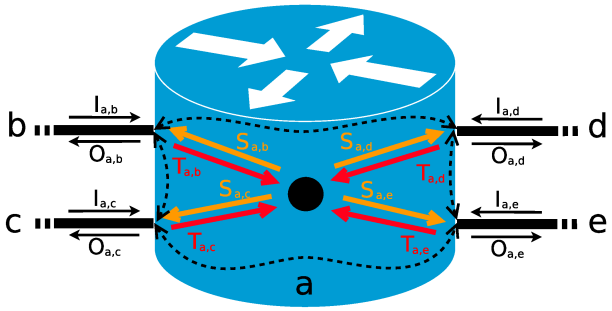


Figura 14 – Critérios de credibilidade PIFA: F_n.

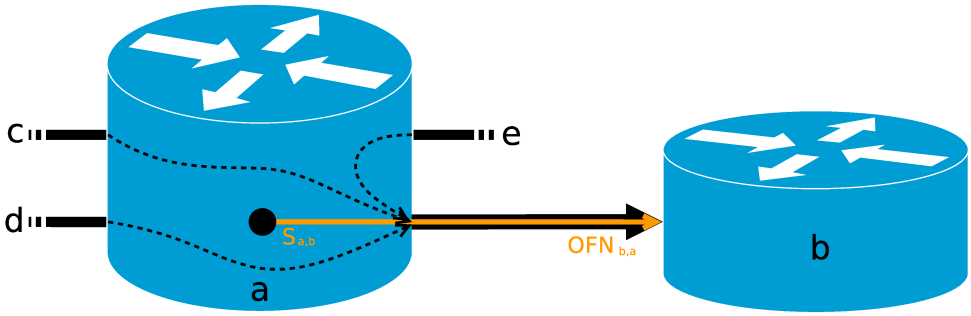


Figura 15 – Critérios de credibilidade PIFA: $OFN_{m,n} = S_{n,m}$.

O CM incrementa o crédito de cada roteador na proporção de F_n e cada roteador precisa pagar uma quantia de créditos correspondente a $\sum S \times H_{avg}$, de acordo com o número de pacotes que ele origina, sendo H_{avg} o número médio de saltos entre dois roteadores na rede. Nas redes

que utilizam o PIFA, assume-se que os roteadores não evitarão o encaminhamento de pacotes deliberadamente, já que necessitam adquirir créditos para poder enviar os seus próprios pacotes.

Para detectar roteadores maliciosos, o CM utiliza os três critérios de credibilidade apresentados. No caso do critério 3, se houver inconsistências na contabilização em algum enlace, o CM dá preferência para o parâmetro OFN para a contabilização. A razão para isso é que o próximo salto do roteamento normalmente não tem motivação para tentar adulterar as informações sobre a quantidade de tráfego que recebeu do roteador vizinho. Já as estatísticas de tráfego de saída de um roteador (S) podem ser adulteradas com o objetivo de reduzir o quanto o roteador será cobrado pelo CM. Mesmo assim, um roteador pode agir maliciosamente adulterando OFN para comprometer o próprio funcionamento do PIFA, sem necessariamente ter como objetivo fraudar a contabiliação em benefício próprio. Além disso, as inconsistências de contabilização podem ser causadas por erros não intencionais, como falhas em interfaces de rede, interferência nos canais de rádio ou mobilidade dos nodos roteadores. Consequentemente, o PIFA precisa de algum método para distinguir erros não intencionais de erros causados por ação maliciosa, além de identificar o agente malicioso nesse último caso. Para esse propósito, o CM mantém uma matriz chamada IRT (*Inconsistency Record Table*) ilustrada na Tab. 3.

Tabela 3 – *Inconsistency Record Table*.

	a	b	c	d	...	Total
a	–	$m_{a,b}$	$m_{a,c}$	$m_{a,d}$	...	$\sum m_{a,i}$
b	$m_{b,a}$	–	$m_{b,c}$	$m_{b,d}$	...	$\sum m_{b,i}$
c	$m_{c,a}$	$m_{c,b}$	–	$m_{c,d}$	...	$\sum m_{c,i}$
d	$m_{d,a}$	$m_{d,b}$	$m_{d,c}$	–	...	$\sum m_{d,i}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$

Cada $m_{i,j}$ da matriz IRT corresponde a um contador para indícios de manipulação (NAM ou *Number of Alleged Manipulation*) que um roteador i pode ter tentado para trapacear o CM a respeito da contabilização do tráfego de entrada ou de saída no enlace com o roteador j. No entanto, cada inconsistência é apenas um indício, pode ser apenas um erro não intencional e não identifica qual é o participante malicioso no enlace. Por isso, sempre que uma inconsistência é detectada em um enlace entre os roteadores i e j, tanto o NAM de $m_{i,j}$ quanto o de $m_{j,i}$ são incrementados. O CM só considera um roteador como malicioso quando o somatório de NAMs (coluna mais à direita da matriz IRT) atinge um determinado limite. Nessa situação, o roteador é excluído da rede, ou seja, todos os outros roteadores passam a descartar pacotes desse roteador e deixar de encaminhar pacotes para ele.

Por último, o PIFA possui um esquema para evitar que roteadores inocentes sejam responsabilizados por inconsistências causadas por outros roteadores conectados. O esquema baseia-se na ideia de que um roteador malicioso tentará trapacear a contabilização de mais de

um enlace. Assim, sempre que os roteadores a e b notificarem uma inconsistência ao CM, as entradas NAM acumuladas até então por cada um dos outros roteadores conectados a a e b são reduzidas pela metade: $m_{i,a} = \lfloor \frac{m_{i,a}}{2} \rfloor$ e $m_{i,b} = \lfloor \frac{m_{i,b}}{2} \rfloor, \forall i \notin \{a,b\}$. Dessa forma, roteadores com inconsistências eventuais terão o peso do NAM reduzido e roteadores que reiteradamente apresentem inconsistências com vários outros roteadores terão o peso do NAM aumentado.

4 ESTADO DA ARTE

Neste capítulo, será apresentado o estado da arte em mecanismos de incentivo baseados em crédito para o encaminhamento de pacotes em redes cooperativas que adotam estratégias descentralizadas. Todos os trabalhos encontrados utilizam blockchains para mediação dos incentivos. Os princípios de funcionamento das blockchains permitem a elaboração de mecanismos de incentivo à cooperação que não dependem necessariamente da confiança em intermediários (Seção 3.1.1). Seus fundamentos permitiram a retomada de trabalhos sobre o problema do caroneiro no encaminhamento de pacotes em redes de computadores (Seções 2.1 e 2.3) sob uma nova perspectiva. Estratégias de crédito que antes dependiam de terceiros confiáveis (TTP) ou mesmo de módulos de segurança resistentes a adulteração (TRSM), ilustrados na Fig. 3, agora podem ser implementadas sem a necessidade desses elementos. Além disso, a utilização de remuneração e recompensas com criptomoedas como forma de incentivo elimina também a limitação de reciprocidade no serviço de encaminhamento existente em muitos dos mecanismos baseados em crédito anteriores às blockchains. No total foram encontrados 8 artigos acadêmicos, 8 produtos e uma patente. A próxima seção apresenta cada um desses sistemas, na sequência são analisadas as blockchains utilizadas, as estratégias e os desafios identificados e, finalmente, um resumo dos pontos de destaque desse capítulo.

4.1 SISTEMAS NO ESTADO DA ARTE

Nas próximas subseções, são apresentados os sistemas encontrados no estado da arte. Para cada um deles será descrito o princípio de funcionamento do mecanismo de incentivo ao encaminhamento de dados e os seus principais elementos.

4.1.1 Kadupul

O Kadupul (SKJEGSTAD; MADHAVAPEDDY; CROWCROFT, 2015) é um sistema que visa incentivar o encaminhamento de pacotes em enlaces locais de baixa latência em redes DTN D2D. Nesse sistema, dispositivos próximos podem criar rotas locais alternativas para comunicação de baixa latência em vez de utilizar os enlaces dos provedores. O encaminhamento através dessas rotas é incentivado utilizando *time-locked puzzles* (GWERN.NET, 2019) do Bitcoin.

Time-locked puzzles são mecanismos que escondem informação por um período específico de tempo ou até que certas condições sejam satisfeitas. A implementação de *time-locked puzzles* do Bitcoin permite reter uma recompensa em criptomoeda até que uma das três condições a seguir seja satisfeita: quando um período específico de tempo passar; quando um roteador resolver o desafio; ou quando a solução do desafio for revelada. O Kadupul incentiva os roteadores a encaminharem os dados o mais rapidamente possível para que esses recebam uma chave que decifra o *time-locked puzzle*. Esse sistema é independente de protocolo de roteamento de

rede e sugere um esquema P2P para descoberta de vizinhança. Os autores propõem cinco estratégias diferentes com *time-locked puzzle*, das quais destacam-se três: incentivo duplo, tudo ou nada, contrato de encaminhamento. Todas as estratégias apresentam um sobrecusto alto pois, para cada pacote, exigem escritas diretamente na blockchain na criação dos *time-locked puzzles*.

A estratégia de *incentivo duplo* faz com que os roteadores recebam a recompensa apenas se encaminharem os pacotes intactos para o próximo salto de roteamento o mais rapidamente possível, antes do prazo dos *time-locked puzzles*. A estratégia se chama incentivo duplo pois recompensa o roteador que cooperar tanto com o salto anterior como com o próximo salto do pacote. Nessa estratégia, o remetente precisa negociar previamente as taxas que serão pagas a cada roteador. Após isso, o remetente gera e publica uma sequência de recompensas na blockchain utilizando *time-locked puzzles*. O próximo passo é distribuir as senhas dos *time-locked puzzles* e os respectivos *nonces* para todos os roteadores no caminho. Cada roteador n mantém seu *nonce* e cada rotedor $n+1$ mantém a senha do roteador do salto anterior. Assim, quando o roteador $n+1$ recebe um pacote, ele responde com uma confirmação para o roteador n contendo a respectiva senha necessária para que n receba o pagamento.

A estratégia tudo ou nada paga a recompensa para todos os roteadores apenas após os pacotes serem entregues ao destino final. Em vez da distribuição de senhas prévia, o destino final confirma a entrega para o remetente, que por sua vez desbloqueia os desafios para todos os roteadores. Esse esquema requer maior coordenação entre remetente e destinatário, mas dificulta coalizões maliciosas entre roteadores. Também aumenta o risco no encaminhamento já que nenhum dos roteadores receberá a sua recompensa se o pacote for perdido durante o percurso ou a entrega atrasar.

A estratégia de contrato de encaminhamento funciona sem precisar de estabelecimento prévio de um caminho como nas duas estratégias anteriores. O remetente negocia um contrato de encaminhamento com um roteador vizinho que se encarrega de levar os pacotes de dados para o destino. Fica a cargo desse roteador vizinho a responsabilidade de entregar os pacotes o mais rápido possível para poder receber a recompensa. Esse roteador pode fazer subcontratações com outro roteador vizinho e esse processo pode se repetir até que se estabeleça um caminho completo até o destino final.

4.1.2 Truthful Incentive

He *et al.* (HE et al., 2018) propuseram um mecanismo de incentivo baseado em crédito para DTN que utiliza transações com Bitcoin. Os roteadores de origem das mensagens pagam os roteadores intermediários que cooperam com o encaminhamento depois que confirmam que a mensagem é entregue com sucesso ao destinatário.

Basicamente, o roteador de origem faz um depósito na blockchain e anuncia uma tarefa de transmissão de pacotes para a vizinhança. O depósito será utilizado para recompensar os roteadores que contribuírem com o encaminhamento. A tarefa anunciada contém dois números aleatórios, R1 e R2, onde R1 é utilizado como prova de que o primeiro salto de roteamento

recebeu os dados corretamente e R2 é utilizado como prova de que o destino final recebeu os dados com sucesso. Cada salto do encaminhamento envolve uma transação de compromisso de pagamento para o roteador anterior. O primeiro salto encaminha os dados para o segundo salto e utiliza um esquema de cifragem comutativa (LIAN et al., 2007) para validar que recebeu R1 do roteador de origem e que recebeu a confirmação (ACK) do roteador seguinte. O processo se repete para os próximos saltos, apenas com o ACK, sem o R1, até o destino do pacote.

As recompensas são pagas aos roteadores intermediários e ao roteador destino se quatro condições forem satisfeitas: (a) O roteador destino conseguir comprovar que recebeu o valor R2; (b) Existir uma rota do roteador origem ao roteador destino que possa ser verificada pela cadeia de provas fornecidas pelos roteadores intermediários; (c) O roteador do primeiro salto conseguir comprovar que conhece o número R1; (d) Todos os roteadores intermediários conseguirem comprovar que receberam os ACKs.

4.1.3 RouteBazaar

O RouteBazaar (CASTRO et al., 2015) utiliza o Bitcoin para construir um esquema automatizado de contabilização e pagamentos do tráfego de rede consumido por sistemas autônomos (AS) na Internet. O sistema fornece meios para estabelecer e verificar os acordos de conectividade fim-a-fim com BGP.

Cada participante é um AS que anuncia sua capacidade de conectividade através de *pathlets* que descrevem os fragmentos de caminho, incluindo custos e qualidade de serviço (QoS). Por exemplo, um *pathlet* com identificador `0xf48d4c4`, do AS 234 até o AS 343, com latência de 5ms, vazão de 3Gbps e com custo de $50/GB. Um caminho é formado combinando *pathlets* até completar a origem e destino desejados. Um cliente do RouteBazaar é uma sistema autônomo que paga pela conectividade fim-a-fim dado um determinado caminho. Os acordos de serviço são registrados na blockchain e identificados por rótulos anônimos. Cada um desses rótulos é válido para um *pathlet* específico e é criado utilizando um gerador de números pseudoaleatórios alimentado por uma chave simétrica negociada entre as partes via ECDH.

A prova de que um roteador encaminhou corretamente os pacotes também é escrita diretamente na blockchain com o seguinte formato: o rótulo anônimo do acordo de serviço, um resumo criptográfico de uma amostra de tráfego (ex: cada 50º pacote), um *timestamp* e a média de vazão desde a última amostra capturada. Essas provas também servem para estimar a qualidade do serviço fornecido pelos roteadores. Os pagamentos também são realizados diretamente na blockchain e permitem que os provedores verifiquem se os clientes são bons ou maus pagadores.

4.1.4 Post-disaster DTN

Chakrabarti e Basu (CHAKRABARTI; BASU, 2019) propõem um sistema para DTN D2D para comunicação em áreas afetadas por desastres que necessitem da implantação de me-

canismos de comunicação temporária emergencial. O sistema utiliza Bitcoin para incentivar o encaminhamento de pacotes em uma área virtualmente dividida em várias zonas sem intersecção, cada qual representando um abrigo.

A arquitetura da rede é composta por quatro tipos de nodos. Os nodos de abrigo que geram mensagens situacionais e disseminam para nodos encaminhadores. Os nodos de controle representam centros de operação de emergência da área do desastre e que precisam receber as mensagens geradas pelos abrigos. Nodos encaminhadores atuam como os roteadores e são dispositivos móveis em posse de pessoas voluntárias que se deslocam dentro da área de desastre e encaminham as mensagens em direção aos centros de controle de forma oportunística. Os nodos observadores coletam transações de recompensa geradas pelos nodos encaminhadores e enviam para a rede do Bitcoin. O sistema assume que os nodos encaminhadores não possuem acesso à Internet e que a área de desastre depende dos nodos observadores para realizar transações na blockchain.

Um nodo de abrigo pertencente a uma zona particular envia as mensagens para o nodo de controle através de um ou mais nodos encaminhadores. Esse nodo paga um quantia de Bitcoin igual para cada um dos nodos encaminhadores que cooperarem com o encaminhamento da mensagem e um montante fixo α para o nodo observador. Adicionalmente, cada nodo intermediário paga uma quantia de incentivo para o nodo encaminhador do próximo salto e recebe desse uma mensagem de confirmação assinada digitalmente (ACK) que serve como prova de encaminhamento do pacote. Importante notar que cada recompensa é na verdade um compromisso que só pode ser resgatado pelos nodos encaminhadores após o nodo de abrigo confirmar que a mensagem foi entregue ao nodo de controle.

4.1.5 VDTN

Vários trabalhos propuseram mecanismos de incentivo para encaminhamento de mensagens em VDTN (DTNs em VANETs). No caso de VANETs, as mensagens são alertas e anúncios para veículos em estradas com cobertura de rede de comunicação insuficiente ou com defeito. Além do problema do caroneiro, o encaminhamento de mensagens em VANETs também apresenta um problema de privacidade, pois as informações de trajetória dos veículos que encaminham as mensagens podem vazar.

VDTN (Park et al.)

Park *et al.* (PARK; SUR; RHEE, 2018) propuseram um sistema baseado no Bitcoin para incentivar a comunicação oportunística de uma RSU_s de origem até uma RSU_d de destino através de um veículo V_c em uma estratégia similar à do Kadupul. Nesse caso as informações de tráfego produzidas na área de uma RSU_s são transmitidas à uma RSU_d que, por sua vez, transmite essa informações aos veículos que estejam passando pela sua área.

Cada veiculo V_c e RSU participa da rede do Bitcoin e tem suas chaves públicas emitidas por uma autoridade certificadora do sistema denominada *Service Manager*. Essas chaves geram os endereços Bitcoin que permitem que a RSU pague os veículos quando as mensagens são encaminhadas. O incentivo funciona através de transações multi-assinatura que requerem assinaturas tanto da RSU_s quanto da RSU_d. Quando a RSU_s cria uma mensagem e envia para V_c ele assina uma transação de pagamento com um *time-lock*. Assim, é necessário que RSU_d assine a transação antes do *time-lock* expirar, incentivando V_c a encaminhar a mensagem o mais rapidamente possível.

VDTN (Li et al.)

Diferentemente da abordagem de Park *et al.*, na qual as mensagens são encaminhadas dos veículos para uma RSU intermediária, que posteriormente dissemina as mensagens dentro da sua área de alcance, a estratégia de Li *et al.* (LI et al., 2019) visa incentivar veículos a encaminharem mensagens diretamente uns para os outros. Além disso, essa proposta utiliza o Ethereum em vez do Bitcoin. Na proposta deles, um anunciante A delega a uma RSU a tarefa de distribuir a mensagem M para veículos V_c que estejam cruzando a área da RSU. Esses veículos são incentivados com recompensas em criptomoeda a encaminhar mensagens oportunisticamente para outros veículos que estejam fora do alcance da RSU. O número de veículos que a mensagem M pode alcançar depende da recompensa de cada entrega bem sucedida e do total de recompensa depositado na blockchain pelo anunciante A. Um contrato inteligente gerencia o depósito com *time-locks* e as recompensas.

Como pagamento, são utilizados *tokens* de criptomoeda que garantem não-repúdio para impedir que anunciantes trapaceiem os veículos que encaminham as mensagens. Os *tokens* são associados a esses veículos através resumos criptográficos produzidos com os endereços de Bitcoin da origem e destino das mensagens, para impedir que os *tokens* sejam resgatados por algum adversário. Além disso utilizam assinaturas cegas (FEIGE; FIAT; SHAMIR, 1988) para garantir a privacidade.

De forma similar à proposta de Park et al. (PARK; SUR; RHEE, 2018), esse trabalho possui também uma autoridade certificadora responsável pela geração e gerência de chaves. A comunicação V2V e V2I é realizada com o protocolo DSRC. Os autores avaliaram o sobrecusto computacional do sistema através do simulador VANETSim. Também avaliaram o desempenho das transações utilizando uma blockchain privada Ethereum com protocolo de consenso com prova de autoridade (PoA).

VDTN (Ayaz et al.)

O trabalho de Ayaz *et al.* (AYAZ et al., 2020) visa a produção de mensagens de alerta mais confiáveis por veículos em uma VDTN. Para isso, cada mensagem é tratada como uma transação de blockchain que precisa passar por um processo de validação. Cada transação é

criada no local da rodovia pelo próprio veículo envolvido em um incidente (*originator*) que paga uma compensação de crédito (CC) para que outros veículos encaminhem essa mensagem. Essa transação precisa ser votada por veículos próximos (*endorsers*), que atuam como testemunhas da transação, utilizando o protocolo de consenso bizantino YAC (MURATOV et al., 2018). O resultado dessa validação é gravado na blockchain como um novo bloco. Além disso, esses veículos também votam para determinar qual será o veículo responsável pelo próximo salto (*relay*) na transmissão da transação que deverá ser realizado de forma oportunística. A cada salto do roteamento o processo de validação e votação do próximo salto é repetido. A seleção do próximo salto leva em consideração diversos parâmetros da camada física de rede e uma classificação de reputação do veículos. Tanto os *endorsers* quanto os *relays* têm um valor de seu crédito descontado ao validarem transações ou ao selecionarem um próximo *relay*. Isso é feito para desincentivar transações falsas. Se a mensagem alcança um mínimo de saltos, o último salto grava todas as votações de escolha de salto como um novo bloco na blockchain. Finalmente, os *endorsers* e *relays* envolvidos são recompensados com uma parcela de CC. O sistema utiliza uma autoridade certificadora responsável por emitir as chaves assimétricas, gerenciar a identidade, a reputação e o crédito dos veículos.

4.1.6 Althea

O objetivo do sistema Althea (TREMBACK et al., 2020) é produzir incentivos para a implantação de conectividade de última milha em redes comunitárias. O Althea utiliza o protocolo de roteamento Babel (CHROBOCZEK, 2011) para determinar as rotas de redes *mesh* de infraestrutura. O protocolo de roteamento também incorpora métricas de preço que consideram quanto cada roteador deseja receber como pagamento para encaminhar pacotes e mecanismos que verificam as métricas anunciadas. Assim, as rotas são determinadas pelos roteadores de acordo com as métricas de custo e de preço anunciadas. O peso de cada métrica no protocolo de roteamento é ajustável de acordo com a preferência de cada roteador entre a qualidade do serviço e o preço.

Na sua primeira versão, o incentivo ao encaminhamento de pacotes foi implementado através de canais de micropagamentos com um mecanismo próprio do Althea chamado Guac (TREMBACK, 2017) sobre o Ethereum. Cada par de roteadores vizinhos que deseja negociar o encaminhamento de pacotes deve estabelecer canais de micropagamentos Guac e túneis VPN Wireguard (WIREGUARD, 2019) entre si. Os túneis servem como um mecanismo rudimentar de contabilização de tráfego de rede entre os vizinhos. Além disso, os vizinhos pagam após os seus pacotes terem sido encaminhados. Assim, maus pagadores só são detectados *a posteriori*. O tratamento dado aos maus pagadores é o bloqueio ou conformação de tráfego. A contabilização através de VPN também serve como mecanismo de reputação para evitar roteadores que fornecem um serviço de encaminhamento de pacotes de baixa qualidade. Por último, o Althea cria também túneis VPN com nodos de saída (servidores bem posicionados na Internet para fornecer acesso com privacidade e resistência à censura) que também servem para

contabilizar o tráfego de rede e auditar as estatísticas de tráfego contabilizado entre vizinhos locais.

A solução de micropagamentos com Guac está sendo substituída por uma solução com a rede Cosmos (KWON; BUCHMAN, 2019), um sistema que visa interconectar múltiplas blockchains através de uma blockchain principal chamada Cosmos Hub. Nesse caso, cada subrede do Althea deve possuir seu próprio protocolo de consenso PoS, permitindo transações rápidas e com baixo custo, e o Cosmos Hub se encarrega de controlar a quantidade de criptomoeda e as transações entre as blockchains secundárias.

4.1.7 Rightmesh

O Rightmesh (ERNST et al., 2019) propõe incentivos em DTNs D2D com micropagamentos Ethereum. O sistema possui uma API para Android para desenvolvimento de aplicações sobre uma pilha de protocolos de rede proprietária que opera sobre Bluetooth e WiFi.

O encaminhamento de pacotes é incentivado utilizando canais de micropagamentos μraiden (Brainbot Labs, 2018) com *tokens* ERC-20 (RMESH). Na visão do Rightmesh, o estabelecimento de canais de micropagamentos entre os pares de vizinhos pode ser muito sensível devido à dinamicidade dessas redes. Assim, os micropagamentos são intermediados por nodos chamados *superpeers* posicionados em servidores da nuvem com acesso mais estável à Internet e à blockchain do Ethereum. Além disso, os *superpeers* intermediam o tráfego de rede permitindo realizar a contabilização. Como consequência, os roteadores precisam confiar nos *superpeers*. O Rightmesh altera o protocolo de rede de forma que os dados de micropagamentos são embutidos nos pacotes de dados e pacotes de confirmação.

Cada roteador do Rightmesh possui um endereço público Ethereum utilizado como identificador tanto para pagamentos quanto para o roteamento. O protocolo de roteamento do Rightmesh utiliza contagem de saltos e preços como métricas. Assim, os roteadores definem os caminhos de acordo com os preços dos enlaces e da distância, em termos de número de saltos.

Cada pacote originado carrega um compromisso de pagamento indicando quanto será pago após a entrega do pacote. Esse compromisso é calculado com base nas métricas de preço anunciadas pelo protocolo de roteamento. É possível que o remetente da mensagem informe um valor desatualizado no pacote. Nesse caso, o roteador descartará o pacote e aguardará uma retransmissão que inclua o valor atualizado.

4.1.8 LOT49

O LOT49 (MYERS, 2019) propõe redes D2D incentivadas com pagamentos Bitcoin utilizando o protocolo de micropagamentos Lightning. Os autores também propõem um esquema multi-assinaturas com agregação para minimizar o sobrecusto das transações de micropagamentos no protocolo de rede (DECKER; RUSSELL; OSUNTOKUN, 2018) (MAXWELL et al., 2019). O protótipo do LOT49 foi avaliado em uma rede sobre o protocolo de roteamento

AODV (CHAKERES; BELDING-ROYER, 2004) para estimar a taxa de entrega de pacotes com diferentes densidades de roteadores.

No LOT49, se um roteador remetente deseja enviar dados para um roteador destinatário através de um caminho com múltiplos saltos, então cada roteador no caminho deve possuir um canal de micropagamentos estabelecido com seu próximo salto. O envio de pacotes requer uma transação de compromisso do canal de micropagamentos que inclui uma recompensa do roteador remetente para o próximo salto. Essa transação só pode ser completada com um recibo do destinatário final. Cada roteador no caminho deve criar uma transação de compromisso com o próximo salto da mesma maneira e sob a mesma condição de entrega da mensagem até o destinatário final. Cada salto reduz a recompensa para o próximo salto sendo que a diferença representa a recompensa do roteador do salto atual.

Assim que o dado é entregue, o destinatário final transmite um recibo de pagamento com uma senha que havia sido cifrada no envio da mensagem. Os roteadores usam esse recibo para atualizar os estados dos seus canais de micropagamentos entre si. Os roteadores que receberem a senha podem liquidar seus canais a qualquer momento, mesmo que seus pares não cooperem. Além disso, os roteadores podem observar as transações que são liquidadas na blockchain por outros roteadores envolvidos no encaminhamento da mesma mensagem para descobrir a senha que precisam para liquidar os próprios canais.

Se um canal de micropagamento não existir entre dois roteadores vizinhos, ele precisa ser criado. A transação que cria o canal precisa ser confirmada na blockchain para ser considerada confiável e prevenir ataques de gasto duplo. No entanto, manter os roteadores sincronizados com a blockchain pode ser impraticável em redes com baixa capacidade e dispositivos com recursos computacionais escassos. Assim, o LOT49 depende de nodos dedicados e melhor posicionados, como um gateway, que serve como testemunha sobre o estado atual da blockchain.

4.1.9 AMMBR

Assim como o Althea, o AMMBR (AMMBR Foundation, 2017) tem o propósito de disseminar a Internet incentivando a implantação de redes comunitárias com blockchain na última milha de provedores. O AMMBR suporta o protocolo de roteamento para redes *mesh* chamado BATMAN-Adv (SEITHER; KÖNIG; HOLLICK, 2011) e propõe o desenvolvimento de um novo chamado BMX7 (NEUMANN; NAVARRO; CERDÀ-ALABERN, 2018). O projeto propõe um roteador modular extensível com suporte a módulos para blockchain, múltiplos rádios e funcionalidades para IoT. Além disso, possui um *token* próprio chamada AMR.

No primeiro relatório técnico (AMMBR Foundation, 2017), a proposta do sistema é a utilização de um método de pagamentos seguro diretamente em uma blockchain que utiliza um hardware dedicado que combina uma prova de tempo decorrido PoET (CHEN et al., 2017) com um novo algoritmo chamado de prova de velocidade (PoV). Os autores descrevem o PoV como uma variação do PoW utilizando desafios com uso intensivo de memória (FENG; LUO, 2020)

a serem calculados por um ASIC proprietário de silício-germânio com clock superior a 20GHz. No segundo artigo (AMMBR Foundation, 2018), omitem discussões sobre o PoV e propõem a utilização de *childchains* Plasma (POON; BUTERIN, 2017) para maior escalabilidade.

4.1.10 Routing Based Blockchain

A patente de Trautmann e Burnell (TRAUTMANN; BURNELL, 2020) descreve um sistema que introduz um esquema de prova de roteamento (*Proof of Routing*) para blockchain pública que recompensa roteadores que encaminham pacotes com emissão de criptomoeda. A ideia inclui tipos diferentes de nodos que processam pacotes de dados. Os nodos podem ser nodos roteadores, que analisam e roteiam os pacotes de dados e nodos de bloco, que gerenciam coleções de pacotes especialmente rotulados e geram novos blocos na blockchain.

Quando um roteador recebe um pacote, ele o assina utilizando algum esquema de agregação de assinaturas como o BLS (BONEH et al., 2003). O roteador avalia o pacote para determinar se ele é ou não um *root packet*. Esse tipo de pacote deve satisfazer critérios específicos. Por exemplo, um resumo criptográfico do conteúdo desse pacote deve ser menor que um determinado número, de forma similar ao consenso PoW do Bitcoin. Esse critério garante que apenas uma pequena fração dos pacotes de uma determinada rede serão classificados e encaminhados para um nodo de bloco.

Os nodos de bloco coletam os *root packets* de um ou mais roteadores e os combinam para produzir um novo bloco da blockchain. O bloco deve satisfazer critérios como: (a) ser baseado na coleta de no mínimo 1000 *root packets*; (b) cada *root packet* deve ter sido assinado e roteado por no mínimo 100 roteadores diferentes. Se um nodo de bloco consegue descobrir um grupo de *root packets* que permita criar um novo bloco na blockchain, então esse nodo e todos os roteadores que contribuíram com esse grupo de *root packets* são recompensados com a emissão de nova criptomoda.

4.1.11 MeshDapp

O MeshDapp (DIMOGERONTAKIS et al., 2019; MIGUEL et al., 2019) foca em encontrar o equilíbrio entre oferta e demanda dos custos de serviço de redes (CAPEX e OPEX) e respectivos pagamentos para viabilizar uma infraestrutura de rede sustentável. Os autores propõem a utilização de contratos inteligentes do Ethereum e oráculos para automatizar a contabilização justa e as transferências financeiras para os serviços fornecidos.

Os autores comparam o serviço de rede a um mercado de fornecimento de energia elétrica, assumindo a necessidade de um mediador que calcula o preço ótimo de mercado e a melhor alocação de recursos de conectividade. Na analogia que eles utilizam, comparam a unidade de consumo de eletricidade kWh (kilowatt/hora) com o MBh (megabyte/hora) dos serviços de encaminhamento de pacotes. Os autores assumem que a demanda por serviço de encaminhamento é próxima da oferta.

Cada rede é chamada de ilha e possui o seu próprio consenso Ethereum PoA (ANGELIS et al., 2018). Cada ilha possui um mediador que executa em contratos inteligentes que recebe informações de um serviço de oráculo responsável pelo monitoramento do tráfego de rede. Adicionalmente, os autores realizaram trabalhos experimentais para avaliar a viabilidade de utilizar protocolos de consenso PoA (KABBINALE et al., 2019).

4.1.12 Outros sistemas

Alguns sistemas que podem ser considerados no estado da arte não fornecem material razoável que permitam detalhar suas características. Mesmo assim, esses sistemas são apresentados a seguir baseando-se no material disponível.

O Blockmesh (PROMETHEUS INDUSTRIES, 2017) possui seu próprio *token* ERC-20 (BHM) para ser utilizado como recompensa para os roteadores que contribuem com o funcionamento de redes comunitárias. Seus autores utilizam um protocolo de redes *mesh* chamado *Mesh Datagram Protocol* (MDP) (BAUMGÄRTNER et al., 2016) do Projeto Serval (GARDNER, 2021) que não fornece confirmação nem ordenamento de pacotes. No protocolo, os identificadores dos roteadores são chaves ECDH que servem para cifrar, assinar e validar os pacotes transmitidos. O Blockmesh propõe também um roteador com hardware dedicado chamado *mesh extender* (MeshEx) cujo objetivo é servir como ponto de acesso e integrar a rede *mesh* com a blockchain. O Blockmesh é limitado a um pequeno conjunto de aplicações que executam sobre o protocolo MDP e atualmente consistem em aplicativos de mensagem, chamadas de voz e transferência de arquivos.

O Smartmesh (SMARTMESH FOUNDATION, 2017) possui uma proposta similar ao Rightmesh, para dispositivos móveis utilizando seu *token* ERC-20 chamado SMT. A documentação mostra que o sistema funciona sobre uma nova versão do Ethereum chamada Spectrum que utiliza um protocolo de consenso chamado *Proof of Capability* que os autores afirmam ser menos oneroso que o PoW. No entanto, não há documentação pública sobre esse protocolo de consenso. Para os incentivos no encaminhamento de pacotes propõem mecanismos de camada 2 como micropagamentos com uma nova versão do Raiden chamada Photon e *childchains* Plasma.

O Skywire (SKYCOIN, 2017) faz parte de um sistema chamado Skycoin. Os autores do Skycoin planejam desenvolver uma linguagem de contratos inteligentes chamada CX, uma blockchain chamada Fiber e um algoritmo de consenso chamado Obelisk. A documentação afirma que o sistema será uma alternativa para conectividade na Internet para prevenir censura e vigilância, eliminando a dependência dos monopólios de provedores. A estratégia anunciada é a disseminação de roteadores chamados Skyminers que são incentivados a operar a rede recebendo criptomoeda (Skycoin) como recompensa. No entanto, desde o primeiro anúncio, nenhuma especificação ou código do Skywire foi disponibilizado publicamente para permitir avaliar o seu funcionamento.

4.2 BLOCKCHAINS ADOTADAS

A Tab. 4 classifica o estado da arte de acordo com a blockchain adotada no mecanismo de incentivo: Bitcoin, Ethereum ou Outra/Indefinida. Parte dos sistemas baseados em Ethereum, em vez de utilizar ether (criptomoeda do Ethereum), implementam seus próprios *tokens* ERC-20 (TREMBACK et al., 2020; ERNST et al., 2019; PROMETHEUS INDUSTRIES, 2017; SMARTMESH FOUNDATION, 2017).

Tabela 4 – Blockchains utilizadas no estado da arte.

Bitcoin	**Ethereum**	**Outra/Indefinida**
RouteBazaar	Althea	Althea (Cosmos)
Kadupul	AMMBR	Routing Based Blockchain
LOT49	Rightmesh	Skywire
Post-disaster DTN	Blockmesh	VDTN (Ayaz *et al.*)
VDTN (Park *et al.*)	VDTN (Li *et al.*)	
Truthful Incentive	MeshDapp	
	Smartmesh	

A Tab. 5 apresenta características de desempenho das duas principais blockchains públicas, o Bitcoin e o Ethereum, em termos de tempo para efetivação das transações, preço por transação e requisitos de espaço de armazenamento para o arquivo da blockchain. Tais características podem ser proibitivas para a implementação de incentivos em determinadas aplicações. Por exemplo, preços por transação muito altos podem ser inviáveis em redes comunitárias cujo objetivo é fornecer conectividade a um preço mais acessível que as opções de provedores comerciais. O tempo para concretizar cada transação apresentado pelas blockchains públicas pode tornar o pagamento pelo encaminhamento de pacotes muito oneroso no caso desse ser feito para cada pacote transmitido. Além disso, o armazenamento do arquivo completo da blockchain pode ser um requisito inviável para dispositivos pessoais móveis ou com recursos computacionais limitados. As blockchains permissionadas adotadas por alguns sistemas (DIMOGERONTAKIS et al., 2019; AMMBR Foundation, 2017; TREMBACK et al., 2020; AYAZ et al., 2020) permitem um desempenho melhor em todos esses aspectos, no entanto, não tem confiança descentralizada como as blockchains públicas pois requerem autorização para cada novo membro.

Devido a limitações de escalabilidade (Seção 3.1) para as transações nas blockchains (camada 1), muitos sistemas do estado da arte adotaram mecanismos de camada 2 (*off-chain*), como canais e *childchains* para permitir transações mais rápidas e baratas. A Tab. 6 classifica o estado da arte de acordo com o uso de mecanismos de camada 1 e 2. Os sistemas que utilizam canais acoplam os micropagamentos ao próprio protocolo de rede para automatizar a cobrança dos pacotes encaminhados. As *childchains* possuem poucas propostas nos mecanis-

Tabela 5 – Desempenho de blockchains públicas.

Parâmetro	**Bitcoin**	**Ethereum**
Tempo para transação (s)	600	15
Preço por transação (US$)	8.38	5.08
Tamanho do arquivo da blockchain	432GB	438GB

Fonte: Tokenview em 03 de Junho de 2021 (TOKENVIEW, 2021)

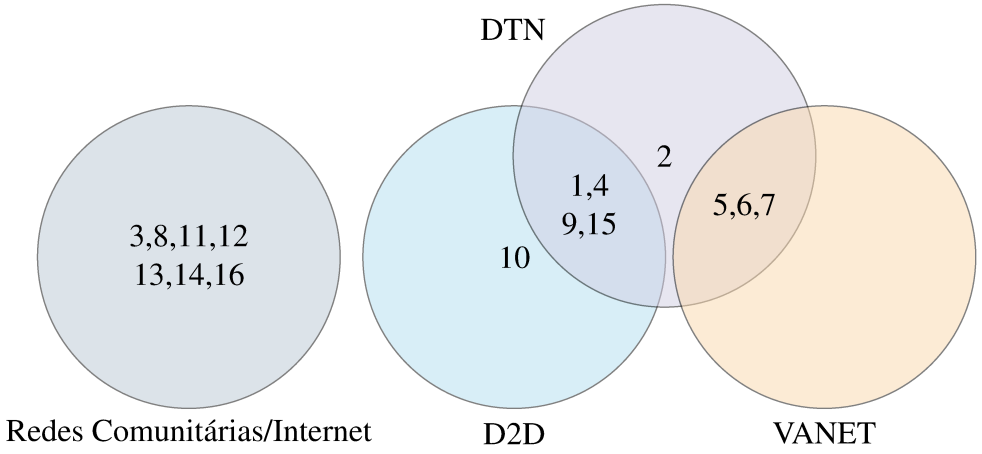
mos de incentivo no estado da arte e nenhuma implementação até o momento. Por exemplo, o AMMBR (AMMBR Foundation, 2018) propôs a utilização do Plasma (POON; BUTERIN, 2017). Nessa abordagem, os roteadores em uma rede podem utilizar uma blockchain filha com consenso local e menor custo, para depois compensar os resultados em uma blockchain pai.

Tabela 6 – Uso de transações de camada 1 e de camada 2 no estado da arte.

Camada 1	**Camada 2**		**Desconhecido/Não aplicável**
Kadupul	Canais	*Childchains*	Routing Based Blockchain
RouteBazaar	Althea	AMMBR	Blockmesh
MeshDapp[a]	LOT49		Skywire
Post-disaster DTN	Rightmesh		
VDTN (Park *et al.*)	Smartmesh		
VDTN (Li *et al.*)			
VDTN (Ayaz *et al.*)[a]			
Truthful Incentive			
Althea (Cosmos)[a]			

[a] Blockchain permissionada

Os canais de micropagamentos ou *childchains* dos mecanismos de incentivo são implementados com contratos inteligentes (ou *scripts*, no caso do Bitcoin). Outro exemplo de uso de contratos inteligentes é encontrado no Althea (TREMBACK et al., 2020) que os utiliza para o gerenciamento do endereçamento das subredes. Além disso, o MeshDapp (DIMOGERONTAKIS et al., 2019) implementa uma série de contratos inteligentes para estimar a oferta e a demanda de serviços de encaminhamento de pacotes de dados, e define os preços com base nessas estimativas. O MeshDapp também utiliza um serviço de oráculo para fornecer a contabilização do monitoramento de rede para os contratos inteligentes de forma que eles possam calcular quanto cada roteador consumiu e contribuiu no encaminhamento de pacotes.



[1] Kadupul
[2] Truthful Incentive
[3] RouteBazaar
[4] Post-disaster DTN
[5] VDTN (Park *et al.*)
[6] VDTN (Li *et al.*)
[7] VDTN (Ayaz *et al.*)
[8] Althea
[9] Rightmesh
[10] LOT49
[11] AMMBR
[12] Routing Based Blockchain
[13] MeshDapp
[14] Blockmesh
[15] Smartmesh
[16] Skycoin

Figura 16 – Estado da arte de acordo com a aplicação.

4.3 ESTRATÉGIAS E DESAFIOS

Nesta seção, as estratégias do estado da arte são analisadas para comparar suas estratégias, ressaltando suas vantagens, limitações e os desafios existentes. A Fig. 4.3 classifica os trabalhos do estado da arte de acordo com a sua aplicação, ou seja os tipos de rede que se destinam, conforme descrito na Seção 2.2. Uma parte dos trabalhos se destina a redes comunitárias ou para conectividade entre sistemas autônomos da Internet. Outra parcela prevê requisitos de redes DTN, que podem ser aplicadas em redes D2D ou VANETs.

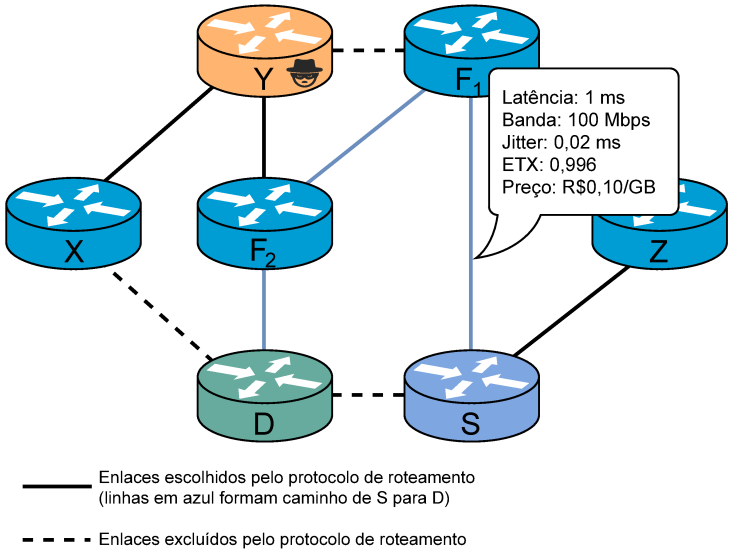


Figura 17 – Possíveis métricas para os enlaces em um protocolo de roteamento de rede.

A Fig. 17 ilustra alguns tópicos discutidos nesta seção através de um exemplo de rede com um protocolo de roteamento que forma caminhos sem ciclos entre os roteadores. Nesse exemplo, o roteador S possui um caminho até o roteador D para transmitir os pacotes. O protocolo de roteamento pode utilizar um conjunto de métricas dos enlaces para a definição das rotas, por exemplo, a latência, a banda, a taxa de transmissão esperada (ETX), e também o preço cobrado para transmissão através desse enlace. Em redes com incentivo ao encaminhamento de pacotes, os roteadores, como F_1 e F_2, precisam de algum método para comprovarem que encaminharam efetivamente os pacotes. Além disso, a rede pode possuir roteadores maliciosos que representam ameaças de segurança como, por exemplo, o roteador Y, que espiona tráfego dos demais roteadores e as transações na blockchain.

4.3.1 Provas de pagamento e de encaminhamento

A maior parte do estado da arte trabalha com o problema do caroneiro de forma similar aos mecanismos de incentivo à cooperação baseados em crédito (Seção 2.3). Nesse contexto, o encaminhamento de pacotes é um serviço recompensado com criptomoeda. O método utilizado para confirmar que um determinado roteador (ex: origem dos pacotes S ou destino D, na Fig. 17) pagou ou que um outro roteador (ex: F_1 ou F_2, na Fig. 17) realizou o encaminhamento dos pacotes corretamente é diferente em cada sistema. Assim, os mecanismos de incentivo precisam implementar duas funcionalidades: as provas de pagamento e as provas de encaminhamento. Em alguns sistemas os mecanismos produzem as duas funcionalidades ao mesmo tempo.

Provas de pagamento seguras fazem parte das funcionalidades inerentes às blockchains. Na Seção 3.1, foram discutidas as limitações de desempenho das blockchains e os respectivos mecanismos que visam aprimorar a escalabilidade. Aqui são discutidas as estratégias do estado da arte que adaptam os mecanismos de pagamento das blockchains às limitações e requisitos específicos de cada tipo rede de computador.

Em redes com baixa capacidade e com conectividade intermitente, como algumas DTNs, os dispositivos podem permanecer sem sincronização com a blockchain por longos períodos e sem possibilidade de realizar transações temporariamente. Mecanismos de camada 2 permitem que as transações possam ser realizadas de forma segura entre os roteadores da rede mesmo quando ela estiver particionada e sem conectividade com a Internet. Por exemplo, canais de micropagamentos permitem pagamentos até um valor que é limitado pelos depósitos que os roteadores realizam no estabelecimento do canal. Cada micropagamento do canal pode ser considerado seguro se os dispositivos envolvidos puderem se conectar à blockchain antes do *time-lock* das transações de compromisso do micropagamento expirarem.

Dispositivos com pouca capacidade de armazenamento não conseguem armazenar o arquivo completo de uma blockchain. Esse é um requisito importante em blockchains públicas para que um determinado roteador seja independente de TTP nas provas de pagamento (DE FILIPPI; MANNAN; REIJERS, 2020). Uma alternativa é a adoção de elementos de rede confiáveis com mais recursos de armazenamento que intermediam a sincronização com a block-

chain (MYERS, 2019; ERNST et al., 2019; CHAKRABARTI; BASU, 2019). Todos os trabalhos sobre VDTN (PARK; SUR; RHEE, 2018; LI et al., 2019; AYAZ et al., 2020) ainda requerem uma autoridade certificadora que emite as chaves dos roteadores. Tanto no caso da intermediação do acesso à blockchain, quanto no caso da autoridade certificadora, os roteadores precisam confiar em um TTP.

Além das provas de pagamento, os trabalhos do estado da arte também implementam formas de provar que os roteadores da rede realmente contribuíram com o encaminhamento de pacotes para possibilitar cobranças justas. Existem redes comunitárias que implementam mecanismos de contabilização de tráfego de rede convencionais para estimar a contribuição e consumo de rede de cada roteador, como a GUIFI.net (CERDÀ-ALABERN; BAIG; NAVARRO, 2020). Tais mecanismos se baseiam no monitoramento de tráfego em pontos estratégicos da topologia da rede. As provas de encaminhamento com blockchains podem permitir uma automação e confiabilidade superior a esses mecanismos, sem a necessidade de TTP. Além disso, a forma de contabilização praticada em redes comunitárias não é adequada para o caso de MANETs mais dinâmicas, cuja atividade dos membros na rede costuma ser mais efêmera, tornando ineficientes eventuais sanções como bloqueios e conformação de tráfego. Assim, os mecanismos de incentivo dessas redes elaboram mecanismos com provas de encaminhamento que assumem essa dinamicidade. As provas de encaminhamento foram classificadas a partir de dois critérios: de acordo com o tipo de mecanismo que utilizam (Tab. 7) e de acordo com a necessidade de confiança em TTP (Tab. 8).

Quanto ao critério de classificação pelo mecanismo da prova de encaminhamento, os sistemas podem ter mecanismos de monitoramento ou mecanismos de recibo. Os mecanismos de monitoramento implementam medição de tráfego de rede através de equipamentos intermediadores ou de túneis. O RouteBazaar sugere a utilização de túneis GRE para permitir a contabilização de amostras de tráfego em sistemas autônomos intermediários (CASTRO et al., 2015) e posterior armazenamento dessa informação na blockchain. O Althea utiliza túneis VPN Wireguard (WIREGUARD, 2019) para contabilizar o tráfego entre vizinhos (TREMBACK et al., 2020). O Rightmesh utiliza nodos intermediários localizados na nuvem chamados *superpeers* que intermediam tráfego para permitir a contabilização (ERNST et al., 2019).

Já os mecanismos de recibo, utilizam conteúdo criptográfico embutido nos pacotes e nas suas mensagens de confirmação de entrega para comprovar a cooperação dos roteadores. Os esquemas de recibo permitem que um determinado roteador resgate a recompensa pelo serviço de encaminhamento de pacotes prestado. A posse do recibo é suficiente como prova de encaminhamento pois significa que o destino já reconheceu que o pacote foi entregue. Essa estratégia pode estar associada com canais de micropagamentos (MYERS, 2019; ERNST et al., 2019), confirmação de entrega na própria blockchain (SKJEGSTAD; MADHAVAPEDDY; CROWCROFT, 2015; HE et al., 2018; AYAZ et al., 2020), ou outros mecanismos como *tokens* anônimos (LI et al., 2019).

Pelo critério confiança, as provas de encaminhamento dos sistemas dividem-se em dependentes de TTP e independentes de TTP. Nas dependentes, pressupõe-se a confiança em um

Tabela 7 – Provas de encaminhamento – Mecanismo.

Monitoramento de tráfego	**Recibos**
Althea	LOT49
RouteBazaar	Rightmesh
	Kadupul
	VDTN (Li *et al.*)
	VDTN (Ayaz *et al.*)
	Truthful Incentive

elemento da arquitetura de rede que garanta a segurança das provas de encaminhamento. Importante observar que um sistema que possua provas de pagamento em uma blockchain pública, de forma independente de TTP, ainda pode ser dependente de TTP para as provas de encaminhamento. No Althea (TREMBACK et al., 2020) os roteadores precisam confiar nos seus vizinhos para a contabilização de tráfego de rede nos túneis. O RouteBazaar (CASTRO et al., 2015) precisa confiar em ASs intermediários que realizam o monitoramento do tráfego de rede dos túneis GRE (FARINACCI et al., 2000). O Rightmesh (ERNST et al., 2019) depende da contabilização dos *superpeers*. Todos os sistemas de VDTN apresentados (PARK; SUR; RHEE, 2018; LI et al., 2019; AYAZ et al., 2020) precisam confiar em autoridades certificadoras. O Post-Disaster DTN (CHAKRABARTI; BASU, 2019) precisa confiar nos nodos de controle.

Tabela 8 – Provas de encaminhamento – Dependência de TTP.

Dependente de TTP	**Independente de TTP**
Althea	Routing Based Blockchain
RouteBazaar	Kadupul
Rightmesh	Truthful Inc.
LOT49	
VDTN (Park *et al.*)	
VDTN (Li *et al.*)	
VDTN (Ayaz *et al.*)	
Post-disaster DTN	

Tanto o serviço de encaminhamento de pacotes quanto as criptomoedas podem ser consideradas mercadorias que podem ser trocadas. Existe uma infinidade de mecanismos baseados em blockchains públicas para transferir quantias de criptomoeda entre duas partes de forma segura e sem a necessidade de TTP. A possibilidade de realizar provas de encaminhamento sem a necessidade de TTP é propícia para redes de computadores pois impede essa TTP manipule o sistema com contabilizações incorretas que poderiam causar cobranças indevidas. Um TTP é indesejado também devido à assimetria de informação e poder concentrado em um mesmo

elemento da rede. Até o momento, esse é um desafio sem solução consagrada. O Kadupul (SKJEGSTAD; MADHAVAPEDDY; CROWCROFT, 2015) e o Truthful Incentive (HE et al., 2018) permitem provas de encaminhamento independentes de TTP, no entanto, requerem um número proibitivo de transações na blockchain.

Soluções distribuídas e cooperativas para contabilização que poderiam garantir provas de encaminhamento mais confiáveis, podem recair no problema do caroneiro de segunda ordem que afeta mecanismos de reputação. Ou seja, os roteadores podem agir de forma egoísta, evitando até mesmo a execução das tarefas de contabilização, e se aproveitando da cooperação dos outros roteadores que realizam a contabilização. Acredita-se que uma solução eficiente para provas de encaminhamento deve ser projetada com base em conceitos de teorias dos jogos para modelar incentivos na contabilização distribuída. A ideia de *Proof of Routing* apresentada na patente de Trautmann e Burnell (TRAUTMANN; BURNELL, 2020) vai nessa direção, apesar de precisar ser investigada em detalhe. Além disso, esta tese de doutorado propõe uma alternativa independente de TTP apresentada no Cap. 5.

4.3.2 Protocolos de roteamento

Os protocolos de roteamento utilizados pelos sistemas analisados são apresentados na Tab. 9. Além dos incentivos à cooperação no encaminhamento de pacotes, alguns sistemas procuraram criar protocolos de roteamento com métricas baseadas no preço dos enlaces. Por exemplo, o protocolo de roteamento Babel implementado no Althea (TREMBACK et al., 2020), além das métricas típicas de custo como a velocidade e a qualidade do serviço de um enlace, também incorpora os custos baseados no preço do serviço de encaminhamento através desse enlace, como ilustrado na Fig. 17. Assim, os caminhos são determinados de acordo com regras de mercado, nas quais o preço dos enlaces é levado em consideração. Similarmente, o RouteBazaar implementa um catálogo na blockchain contendo os caminhos de roteamento definidos pelo BGP, com preço e qualidade de serviços (QoS), que podem ser contratados por um AS interessado (CASTRO et al., 2015). O AMMBR foi modelado para operar sobre vários protocolos de roteamento diferentes e, assim como o Althea, previa a criação de uma extensão de protocolo de roteamento para estabelecimento de caminhos levando em consideração o preço dos enlaces (AMMBR Foundation, 2017). O LOT49 (MYERS, 2019) foi avaliado sobre uma rede com AODV, mas não vinculou o mecanismo de incentivo a esse protocolo de roteamento. O MeshDapp (DIMOGERONTAKIS et al., 2019) separa os incentivos econômicos das decisões de roteamento alegando que misturá-los pode levar a problemas de convergência de rotas.

Algumas plataformas, como o Android, limitam a conectividade de redes *mesh ad hoc* (Paul Gardner-Stephen, 2013; AOSP ISSUE 36904180, 2015). Para que esse recurso funcione é necessário que o usuário tenha permissões privilegiadas no dispositivo, como superusuário (*root*). Os dois sistemas afetados por essa limitação são o Rightmesh (ERNST et al., 2019) e o Blockmesh (PROMETHEUS INDUSTRIES, 2017). O Rightmesh procurou contornar essa limitação através da definição dos caminhos de roteamento na camada de aplicação. No

Tabela 9 – Protocolos de roteamento.

Protocolo de Roteamento	**Sistema**
BGP	RouteBazaar
Babel	Althea
Batman-Adv	AMMBR
AODV	LOT49

entanto, não há especificação de como funcionam os incentivos ao encaminhamento de dados em uma rede *mesh* sem a intermediação dos *superpeers*.

Parte do sistemas de DTN não precisa saber o caminho dos pacotes de dados de antemão e a transmissão ocorre de forma oportunística (PARK; SUR; RHEE, 2018; LI et al., 2019; AYAZ et al., 2020; CHAKRABARTI; BASU, 2019; MYERS, 2019). Outros sistemas de DTN exigem que esse caminho seja conhecido antes do envio do pacote de dados para preparação das recompensas pelo seu encaminhamento (SKJEGSTAD; MADHAVAPEDDY; CROWCROFT, 2015; HE et al., 2018). Já os sistemas não-DTN exigem que o caminho seja conhecido (CASTRO et al., 2015; TREMBACK et al., 2020; AMMBR Foundation, 2018). No caso da patente de Trautmann e Burnell (TRAUTMANN; BURNELL, 2020), é necessário saber o caminho para que cada roteador de cada salto participe de um esquema de agregação de assinaturas BLS (BONEH et al., 2003).

4.3.3 Proof of Networking

Alguns trabalhos sugerem que o próprio serviço de rede seja utilizado para produzir uma prova no consenso da blockchain (AMMBR Foundation, 2017; PROMETHEUS INDUSTRIES, 2017; SKYCOIN, 2017; TRAUTMANN; BURNELL, 2020). Por exemplo, um roteador que prova que contribuiu com o trabalho de encaminhamento de pacotes ou na convergência de um protocolo de roteamento, poderia receber uma recompensa em criptomoeda ao fornecer uma de prova de rede (*Proof of networking* ou PoN) válida, da mesma forma que ocorre com o PoW do Bitcoin. A ideia mais próxima de PoN foi proposta por Trautmann e Burnell (TRAUTMANN; BURNELL, 2020) no esquema de prova de roteamento (*Proof of routing* ou PoR).

4.3.4 Qualidade de serviço

Um problema que é pouco discutido nos trabalhos do estado da arte é como lidar com os requisitos distintos de qualidade de serviço (QoS). Por exemplo, aplicações de tempo real, como chamadas de áudio e vídeo, possuem requisitos diferentes de serviços online ou de aplicações em redes DTN. As diferenças se dão em termos de garantias de vazão, latência, *jitter* e da própria estabilidade da conectividade. Para garantir tais requisitos, alguns sistemas possuem protocolos que permitem a reserva de recursos e políticas de filas. Para que tais recursos

possam ser aproveitados em sistemas de incentivo à cooperação, devem, no mínimo, permitir que os roteadores consigam detectar de alguma maneira se os serviços estão sendo prestados de acordo com o ofertado. Funcionalidades desse tipo requerem provas mais complexas do que simplesmente comprovar se o pacote foi entregue ou não.

Apesar dos *pathlets* do RouteBazaar informarem a qualidade de serviço dos caminhos, não há nada no sistema que garanta que o serviço será fornecido da maneira anunciada, nem formas de detectar que o acordo de serviço tenha sido cumprido. Foram encontrados dois trabalhos nessa direção, apesar de eles estarem fora do escopo de incentivos ao encaminhamento de pacotes de dados, que é o foco desta tese: PayFlow (CHEN et al., 2019b), que permite que dispositivos façam alocação de banda pré-paga com criptomoedas em redes definidas por software (*software defined networks* ou SDN); uma proposta de aferição de SLA com contratos inteligentes que faz a compensação automaticamente (SCHEID et al., 2019).

4.3.5 Orquestração de serviços de rede virtualizados

Existem várias iniciativas para orquestração de serviços de conectividade entre provedores de serviço de rede (SD WAN (YANG et al., 2019), *network slicing* (ZHANG, 2019), NFVIaaS (ADAMUZ-HINOJOSA et al., 2018)). A orquestração permite compor caminhos de rede com trechos de diferentes domínios administrativos de maneira auto-escalável e sob demanda. Rosa e Rothenberg (ROSA; ROTHENBERG, 2018) propuseram um arcabouço genérico bastante abrangente baseado em blockchains para permitir essa orquestração de forma descentralizada. Esse arcabouço permite a automação e coordenação do aluguel de fatias dos recursos de rede virtualizados e prevê fases para todo o ciclo de vida do serviço. Os autores argumentam sobre a necessidade de medições de tráfego desses trechos para permitir a verificação dos custos associados à utilização dos ativos de rede e para confirmar o cumprimento dos acordos de nível de serviço (SLA). Tal problema é análogo a alguns tipos de provas de encaminhamento apresentados nesse capítulo, lembrando que as provas de cumprimento de requisitos de QoS são um problema mais complexo, conforme discutido na Seção 4.3.4.

4.3.6 Privacidade e anonimato

Os mecanismos de incentivo tratados nesta tese podem vazar informação a respeito da localização e trajetória dos roteadores quando esses criam transações na blockchain pública. Alguns trabalhos assumem que isso é um problema de segurança que pode inibir a participação no sistema e propuseram soluções para evitar a exposição de dados sensíveis dos roteadores. Li *et al.* (LI et al., 2019) propõem a utilização de técnicas de assinaturas cegas (FEIGE; FIAT; SHAMIR, 1988) e o trabalho de Park *et al.* (PARK; SUR; RHEE, 2018) utiliza os endereços do Bitcoin dos veículos como pseudônimos. O RouteBazaar (CASTRO et al., 2015) possui mecanismos para anonimização das provas de encaminhamento e das provas de pagamento. Na estratégia *all or nothing* do Kadupul (SKJEGSTAD; MADHAVAPEDDY; CROWCROFT,

2015) é possível esconder a identidade dos roteadores. Para conseguir isso, o Kadupul pressupõe que o destino final da mensagem pode enviar uma resposta diretamente para o remetente através de algum meio de broadcast anônimo. Após isso, o remetente desbloqueia o *time-locked puzzle* que recompensa todos os roteadores.

4.3.7 Common washing e fraudes

O projeto Netcommons (NETCOMMONS, 2019) levanta preocupações sobre possíveis conflitos de interesse em projetos de criptomoedas e redes comunitárias. A questão levantada é se projetos desse tipo agem legitimamente visando uma infraestrutura comum ou predominantemente com interesses comerciais visando lucro. Inclusive, um dos participantes do projeto criou o termo *common washing* que significa a apropriação do discurso sobre conceitos e valores do que é coletivo por atores privados. Somado a isso, há um extenso histórico de fraudes envolvendo criptomoedas (ZETZSCHE et al., 2019) que intensifica essas preocupações.

4.4 RESUMO DO ESTADO DA ARTE

Esse capítulo apresentou uma revisão dos trabalhos que criam incentivos baseados em crédito para o encaminhamento de dados em redes de computadores utilizando conceitos de blockchains. A Tab. 10 resume os trabalhos de acordo com as classificações utilizadas no capítulo. Alguns sistemas não possuem informação pública suficiente para uma análise mais detalhada, por isso a tabela possui algumas lacunas.

Os sistemas que conseguem operar sem a necessidade de TTP são o Kadupul, o Truthful Incentive e o Routing Based Blockchain. O dois primeiros requerem custos proibitivos, necessitando de várias transações na blockchain para o encaminhamento de um único pacote de dados. O último é uma patente que ainda requer experimentos mais aprofundados para validação da ideia proposta. A última linha da tabela mostra a solução proposta nesta tese, concebida para ser independente de TTP utilizando blockchains públicas e sem custos proibitivos. A solução é uma proposta de arquitetura de sistema chamada HARPIA e que será apresentada no próximo capítulo.

Tabela 10 – Resumo do estado da arte.

Sistema	**Blockchain**	**Tipo de Rede**	**Prot. Rot.**	**Prova Pag.**	**Prova Enc.**	**TTP**
Kadupul	Bitcoin	D2D DTN	—	Camada 1	Recibos	Independente
Truthful Inc.	Bitcoin	DTN	—	Camada 1	Recibos	Independente
RouteBazaar	Bitcoin	Internet	BGP	Camada 1	Contab. GRE	Contab. tráf. AS interm.
Post-disaster DTN	Bitcoin	D2D DTN	—	Camada 1	Recibos	Nodo de controle
VDTN (Park *et al.*)	Bitcoin	VDTN	—	Camada 1	—	*Service manager*
VDTN (Li *et al.*)	Ethereum	VDTN	—	Camada 1	Recibos	Autor. certificadora
VDTN (Ayaz *et al.*)	Própria	VDTN	—	Camada 1	Recibos	Autor. certificadora
Althea[a]	Ethereum Cosmos	Redes Com.	Babel	Camada 2 Guac Camada 1	Contab. VPN	Contab. tráf. vizinho
Rightmesh	Ethereum	D2D DTN	—	Camada 2 μRaiden	Recibos	*Superpeers*
LOT49	Bitcoin	D2D	AODV	Camada 2 Lightning	Recibos	Nodo testemunha
AMMBR	Ethereum	Redes Com.	Batman-Adv	Camada 2 Plasma	?	?
Rout. Based Blockc.	Própria	Internet	?	Proof of Routing	Proof of Routing	Independente
MeshDapp	Ethereum	Redes Com.	?	Camada 1	?	?
Blockmesh	Ethereum	Redes Com.	?	?	?	?
Smartmesh	Ethereum	D2D DTN	?	Camada 2 Raiden	?	?
Skywire	Própria	Redes Com.	?	?	?	?
HARPIA	Ethereum	Redes Com.	Independente	Camada 1 MuSig	Contab. DPIFA	Independente

—: Não aplicável, ?: Sem informação

[a] Implementações com as blockchains Ethereum e Cosmos

5 HARPIA

Este capítulo apresenta o *Hop-by-hop Accounting and Rewards for Packet dIspAtching* (HARPIA), uma arquitetura de sistema que utiliza contratos inteligentes sobre a blockchain pública para implementar mecanismos de incentivo baseados em crédito para estimular o encaminhamento de dados em redes cooperativas. Como o próprio nome sugere, o HARPIA se baseia na contabilização (*accounting*) de encaminhamento de pacotes (*packet dispatching*) de cada salto da rede (*hop-by-hop*) e respectivas recompensas (*rewards*). A contabilização de tráfego é baseada em uma versão descentralizada do protocolo PIFA de Yoo *et al.* (YOO; AHN; AGRAWAL, 2005) chamada DPIFA. No HARPIA, em vez de confiar em TRSM ou TTP, os roteadores da rede compartilham as informações de contabilização de tráfego entre si para que cada um deles possa validá-las independentemente. Além disso, o HARPIA não requer transações frequentes na blockchain, mas apenas gravações periódicas (a cada hora, dia, semana, mês, etc), asseguradas com multi-assinaturas MuSig *m*-de-*n*, que compensam os débitos e créditos pendentes correspondentes à utilização e contribuição de cada roteador no encaminhamento de pacotes.

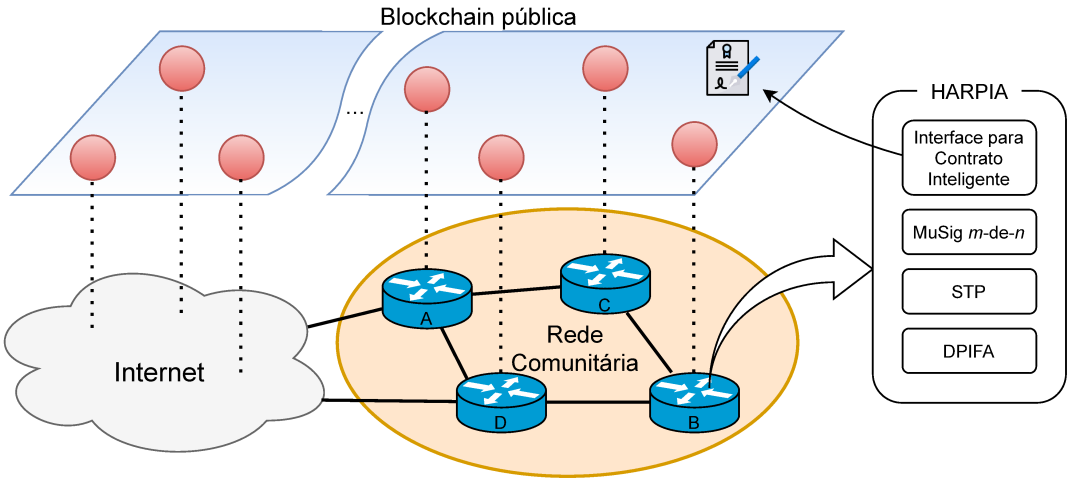


Figura 18 – Arquitetura do HARPIA.

O objetivo deste capítulo é apresentar a arquitetura do HARPIA de forma qualitativa, ou seja, descrevendo seus componentes e seu funcionamento. Os componentes dessa arquitetura que são implementados em cada roteador da rede local estão ilustrados nas Figuras. 18 e 19. A Fig. 18 mostra os componentes da arquitetura em uma aplicação de rede comunitária com dois *backhauls* para a Internet. Cada roteador é um nodo Ethereum completo [1] integrado a uma blockchain pública cuja rede P2P sobreposta à rede de infraestrutura é representada pelos nodos em vermelho. As próximas seções apresentam cada um dos componentes da arquitetura e um caso de uso típico para exemplificar o seu funcionamento.

[1] Neste capítulo, será considerado o caso da rede Ethereum Mainnet, a principal blockchain Ethereum, mas o HARPIA pode ser implantado em qualquer outra blockchain com suporte a contratos inteligentes Solidity, como a Ethereum Classic (DHILLON; METCALF; HOOPER, 2017), a Polygon (POLYGON, 2021) e a BSC (BINANCE, 2021).

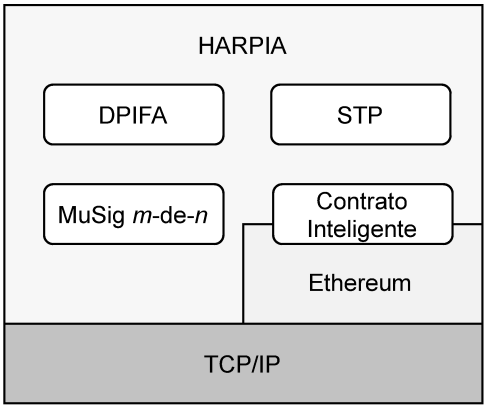


Figura 19 – Arquitetura do HARPIA – Componentes e pilha de protocolos de rede.

5.1 VISÃO GERAL

No HARPIA, assim como no PIFA, os roteadores que originam os pacotes de dados pagam os roteadores no próximo salto da rede pelo serviço de encaminhamento. Assume-se que os roteadores do próximo salto cooperarão com o encaminhamento com o objetivo de serem remunerados. A Fig. 20 ilustra o roteador A que produziu um total de 100 GB de dados destinados ao roteador C e que foram encaminhados pelo roteador B através de um enlace B-C cuja tarifa para o serviço de encaminhamento de dados é R$ 0,10/GB. Os pagamentos e cobranças não são realizados diretamente entre os roteadores vizinhos, mas sim através de cálculos que agregam a contabilização distribuída do DPIFA. Nesse exemplo, o HARPIA ressarce o roteador B com um valor correspondente aos 100 GB encaminhados, ou seja R$ 10,00, considerando a tarifa do enlace B-C. Já o valor cobrado do roteador A pelo sistema depende do número de saltos médio da rede e da tarifa média dos enlaces, conforme o cálculo das STPs explicado mais adiante.

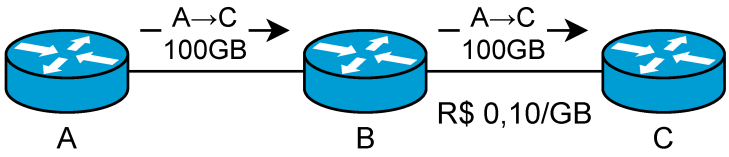


Figura 20 – Pagamento pelo encaminhamento de dados no HARPIA.

É importante observar que o HARPIA não distribui créditos de criptomoeda previamente entre os membros. Estes devem obter créditos externamente através de mineração na blockchain, doações, publicidade em conteúdo transmitido, ou quaisquer outros meios. Os valores em criptomoeda depositados para os roteadores são convertidos em *tokens* HARPIA que são utilizados para as cobranças e pagamentos pelo encaminhamento de dados.

O HARPIA é focado na automação e na segurança das negociações entre os roteadores da infraestrutura e não impõe limitações quanto ao número de dispositivos cliente dentro das redes locais atendidas por cada roteador de infraestrutura. A Fig. 21 ilustra roteadores de infraestrutura (em azul), os enlaces entre esses roteadores (em vermelho) e os dispositivos de cada

rede interna (em cinza). Além disso, o desempenho do HARPIA é independente do volume e do perfil do tráfego de rede e se baseia na contabilização dos contadores das interfaces.

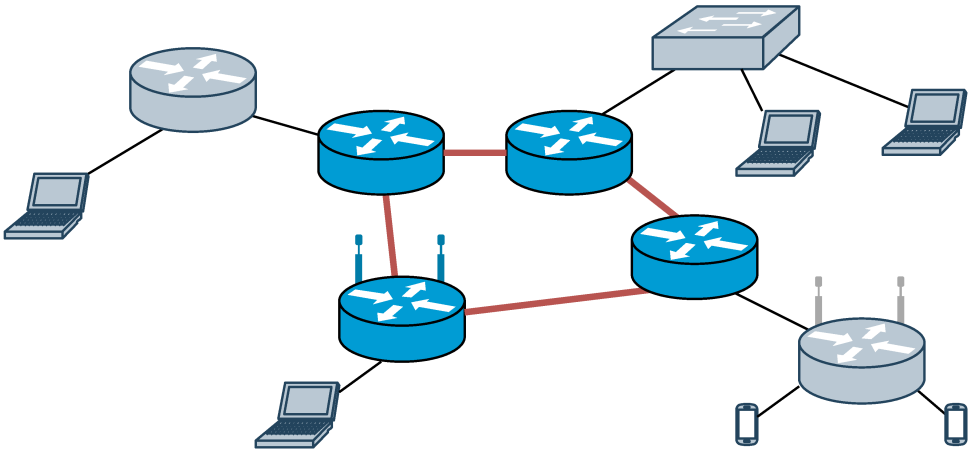


Figura 21 – Rede de infraestrutura e redes internas.

O DPIFA é o componente responsável pela contabilização do tráfego dos enlaces entre os roteadores de infraestrutura. O seu funcionamento é inspirado no PIFA (YOO; AHN; AGRAWAL, 2005) e a sua principal diferença é a eliminação da necessidade de TTP, no caso, do serviço CM. Em vez do CM, todos os roteadores compartilham suas informações de contabilização, produzidas com os mesmos parâmetros do PIFA original, e calculam quanto de criptomoeda cada roteador deve pagar ou tem direito de receber. Apesar de utilizar os mesmos parâmetros do PIFA, no DPIFA é contabilizada a quantidade de dados em vez da quantidade de pacotes. Assim como o PIFA, o HARPIA é independente de protocolo de roteamento. Pode ser aplicado em redes cooperativas bastando que os endereços dos roteadores nessas redes estejam associados à chave pública do roteador cadastrada no HARPIA. Apesar do HARPIA não exigir que todos os roteadores participem da rede, apenas os membros do HARPIA podem se envolver no esquema de contabilização de tráfego e nas negociações de criptomoedas. Também é necessário que os membros do HARPIA sejam vizinhos para que seja possível produzir contabilização confiável.

A cada ciclo [2] do HARPIA uma transação compensa os débitos e créditos de criptomoeda que estão pendentes. Cada roteador agrega as informações de contabilização de todos os outros roteadores que foram recebidas dentro de um ciclo para validar a sua credibilidade e calcular os débitos e créditos pendentes. Assim, cada roteador pode propor uma transação para atualizar o saldo de criptomoedas de todos os roteadores. Se um percentual mínimo dos roteadores assinarem a transação, o roteador que a propôs pode fazer uma chamada a uma função de contrato inteligente que verifica sua validade e finaliza a compensação dentro desse ciclo. As próximas seções descrevem cada um dos componentes da Fig. 19.

[2] Um ciclo é o intervalo de tempo entre duas compensações de créditos e débitos entre os participantes.

5.2 DPIFA

Cada roteador de infraestrutura mantém o registro das estatísticas de tráfego dos seus enlaces de rede ativos com os vizinhos para pacotes unicast recebidos e enviados de acordo com os parâmetros DPIFA (RID, NID, I, O, S, T e OFN) detalhados na Seção 3.3. Em uma rede com n roteadores, a cada período λ (ex: 10 minutos), cada roteador dissemina as informações de contabilização de tráfego desse período para todos os outros $n-1$ roteadores e guarda as mensagens recebidas desde a última compensação do HARPIA.

A possibilidade de descarte seletivo de mensagens DPIFA por roteadores maliciosos visando adulterar a contabilização dos outros roteadores ou mesmo a perda dessas mensagens por erros de comunicação são tratados com números de sequência e temporizadores. O DPIFA utiliza protocolos sem confirmação de entrega, como UDP, para minimizar o impacto sobre a rede. Eventuais mensagens perdidas são solicitadas novamente para os roteadores via unicast através de RPC sobre TLS. Como são em número reduzido, o restante das mensagens do HARPIA pode ser transmitida via unicast com RPC sobre TLS e confirmação de entrega.

O tamanho da mensagem DPIFA produzida por um roteador depende do número de enlaces ativos com roteadores vizinhos que esse roteador possui, conforme ilustrado na Fig. 22. Essa é uma diferença quanto ao PIFA original, que envia uma mensagem para cada enlace ativo. No caso do DPIFA, cada mensagem contém: o identificador do roteador (RID), o *timestamp* (t), o número de sequência (seq), o número de enlaces do roteador (n), as estatísticas de cada enlace (E_1 a E_n) e a assinatura ECDSA da mensagem.

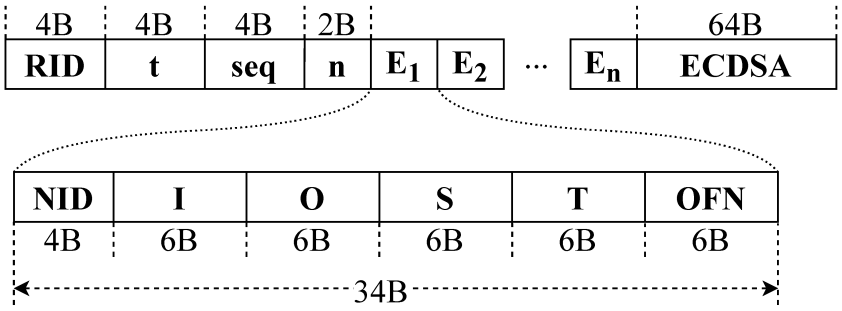


Figura 22 – Mensagens de contabilização do DPIFA.

Após o recebimento das informações de contabilização dos demais roteadores, cada roteador pode calcular a quantidade de dados que cada um dos outros roteadores encaminhou e a quantidade de dados originados desse roteador que foram encaminhados pelos seus vizinhos. Se um roteador perder seus dados durante um ciclo, ele pode recuperá-los solicitando-os diretamente a qualquer vizinho que deve guardar as mensagens até que a contabilização correspondente a elas seja realizada. Assim, em uma rede com n roteadores, cada roteador precisa armazenar uma quantidade de mensagens DPIFA equivalente a, no mínimo, $n^2(\frac{\beta \cdot \gamma}{\lambda})$, sendo β o número de blocos mínimos para um ciclo, γ o tempo médio necessário para a mineração de um bloco Ethereum e λ o período de envio de mensagens DPIFA.

É importante observar que no HARPIA quem paga pelo serviço de encaminhamento de dados é quem os origina. Uma consequência imediata disso é que provedores de conteúdo que estejam dentro da rede comunitária precisam pagar para que os dados sejam encaminhados para os seus clientes nessa rede. Nesse caso, dependendo do modelo de negócio do provedor de conteúdo, pode ser necessário algum esquema entre ele e seus clientes para ressarcimento desses custos. O cliente pode negociar diretamente com o provedor de conteúdo ou o provedor pode incluir publicidade no conteúdo como contrapartida para seus custos.

Outra situação importante, que pode ser reduzida ao mesmo problema é o de contabilização de tráfego dos *backhauls* das redes comunitárias. Não é possível fazer a contabilização desses enlaces através do DPIFA. Seria necessário que os roteadores dos provedores de Internet fossem membros da rede HARPIA. Mesmo assim, o problema se estenderia para o próximo salto de roteamento da Internet além do provedor. A solução para esse problema é a utilização de túneis ou *proxies* de cada roteador da rede comunitária para um dos roteadores de saída que possuem *backhaul*. Assim, o problema fica reduzido à negociação desse cliente da rede interna com o responsável pelo roteador de saída, de maneira similar à negociação com um provedor de conteúdo que esteja na rede comunitária.

Matriz de inconsistências

A matriz de inconsistências é um mecanismo herdado da IRT do PIFA. Nesse sistema as inconsistências detectadas nas estatísticas de tráfego de rede são contabilizadas de acordo com seus critérios de credibilidade, conforme explicado na Seção 3.3. No HARPIA, da mesma maneira, as inconsistências são divergências nos parâmetros contabilizados detectadas através desses critérios. Outras situações específicas do HARPIA também são consideradas inconsistências, como STPs inválidas (explicada na próxima seção) ou mensagens não recebidas no esquema de multi-assinatura MuSig. Por exemplo, um roteador j que não tenha recebido uma mensagem do MuSig de um determinado roteador i, notificará os demais roteadores uma inconsistência no roteador i.

No início de cada ciclo, cada um dos n roteadores que tenha detectado inconsistências no ciclo anterior faz a distribuição da sua lista para os demais $n-1$ roteadores. Os roteadores agregam as listas em uma matriz como a da Tab. 11 na qual cada entrada $m_{i,j}$ é um contador de inconsistências de um roteador i detectada pelo roteador j. Para manter a matriz de inconsistências, o parâmetro ρ indica a janela de tempo, em número de ciclos passados, que são considerados na contabilização.

A matriz de inconsistências opera como um mecanismo de monitoramento no qual os responsáveis pelos roteadores podem verificar quantas inconsistências cada roteador detectou em cada um dos outros roteadores. Quando um roteador recebe várias acusações de inconsistência de distintos roteadores, seu responsável deve providenciar a verificação do funcionamento dos seus enlaces de rede e procurar resolver eventuais problemas de conectividade até que a quantidade de inconsistências seja reduzida a limites toleráveis. Em alguns casos pode

Tabela 11 – Matriz de inconsistências.

	a	b	c	d	...	Total
a	–	$m_{a,b}$	$m_{a,c}$	$m_{a,d}$	...	$\sum m_{a,i}$
b	$m_{b,a}$	–	$m_{b,c}$	$m_{b,d}$	...	$\sum m_{b,i}$
c	$m_{c,a}$	$m_{c,b}$	–	$m_{c,d}$	...	$\sum m_{c,i}$
d	$m_{d,a}$	$m_{d,b}$	$m_{d,c}$	–	...	$\sum m_{d,i}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$

ser necessário realizar diagnósticos de rede em conjunto com os responsáveis pelos roteadores adjacentes. Se as inconsistências não forem tratadas, qualquer roteador poderá propor a remoção desse membro através da função `Leave` do contrato inteligente do HARPIA, explicado na Seção 5.5.

As inconsistências podem ser causadas tanto pela ação maliciosa quanto por erros não intencionais, como falhas nos roteadores ou nos seus enlaces. Não há como saber imediatamente qual dos roteadores é responsável pela inconsistência. Também é possível que algum roteador acuse inconsistências em outros roteadores indevidamente. Por isso, o HARPIA não implementa nenhum mecanismo automatizado de reputação que aplique sanções ou punições a membros com mau comportamento. A matriz de inconsistências é apenas mais um subsídio para que os responsáveis pelos roteadores decidam pela remoção de membros mal comportados.

5.3 SETTLEMENT TRANSACTION PROPOSAL

No HARPIA, os pagamentos pelos serviços de encaminhamento de pacotes não são realizados diretamente entre os membros como em outros sistemas do estado da arte (SKJEGSTAD; MADHAVAPEDDY; CROWCROFT, 2015; CASTRO et al., 2015; HE et al., 2018; ERNST et al., 2019; AMMBR Foundation, 2018; MYERS, 2019; TREMBACK et al., 2020). Em vez disso, as informações de contabilização individuais de cada roteador são agregadas para calcular o total de criptomoeda que cada roteador n deve pagar ou tem direito de receber (C_n) de acordo com seu consumo ou contribuição no encaminhamento de pacotes. Isso é realizado com uma proposta de compensação de débitos e créditos chamada STP (*Settlement Transaction Proposal*).

Qualquer um dos n roteadores da rede pode propor uma STP para os outros $n-1$ roteadores através de uma mensagem *STP Disseminate*. Essa STP precisará ser assinada por um mínimo de m roteadores em um esquema MuSig m-de-n para poder ser compensada na blockchain. No máximo uma STP pode ser compensada a cada ciclo do HARPIA. Assim, o valor do tempo mínimo de ciclo deve ser definido de forma que permita compensações com uma periodicidade mínima acordada pelos membros da rede. O processo de criação, validação

e confirmação de STP é automático e os responsáveis pelos roteadores que desejem criá-las automaticamente com o intuito de serem recompensados devem configurar seus roteadores com essa preferência.

Uma STP inclui uma entrada C_n para cada roteador n calculada conforme a Eq. 5.1

$$C_n = \sum_{a \in A_n} \mathrm{F}_{n,a} \cdot P_{n,a} - \mathrm{S}_{n,a} \cdot P_{avg} \cdot H_{avg} \tag{5.1}$$

na qual o minuendo da subtração dentro do somatório corresponde aos ressarcimentos pelo encaminhamento de dados realizado pelo roteador n e o subtraendo corresponde a quanto esse roteador n deve pagar pelo tráfego que produziu na rede. As variáveis dessa equação são detalhadas a seguir considerando as mensagens de contabilização DPIFA reportadas por cada roteador n:

- $\mathrm{F}_{n,a}$ representa a quantidade de dados recebidos pelo roteador n (RID) e encaminhados em direção ao destino através do enlace com o roteador a (NID).

$$\mathrm{F}_{n,a} = \mathrm{O}_{n,a} - \mathrm{S}_{n,a} \tag{5.2}$$

- A_n é o conjunto de roteadores vizinhos de n.

- H_{avg} é o número de saltos médio dos caminhos de menor custo entre dois roteadores quaisquer em uma rede com um conjunto N de roteadores, onde $H(n,m)$ é o número de saltos do caminho de menor preço entre dois roteadores específicos n e m para se comunicarem na rede. O caminho de menor custo utilizado para determinar $H(n,m)$ é determinado pelo algoritmo de Dijkstra (JASIKA et al., 2012).

$$H_{avg} = \frac{\sum_{n \neq m} H(n,m)}{|N| \cdot (|N| - 1)} \tag{5.3}$$

- P_n é o preço médio do tráfego do roteador n para algum de seus vizinhos no conjunto A_n.

$$P_n = \frac{\sum_{a \in A_n} P_{n,a}}{|A_n|} \tag{5.4}$$

- P_{avg} é o preço médio do tráfego em cada enlace da rede.

$$P_{avg} = \frac{\sum_{n \in N} P_n}{|N|} \tag{5.5}$$

Para que seja possível calcular P_n, P_{avg}, H_n e H_{avg} cada roteador n deve especificar o preço $P_{n,a}$ de cada um de seus enlaces n-a, $\forall a \in A_n$, em um contrato inteligente do HARPIA detalhado mais adiante. Além disso, todos os roteadores cadastrados na rede devem pertencer a um mesmo grafo conexo, ou seja, todos devem possuir caminhos uns para os outros. Isso pode

ser verificado através das interfaces cadastradas no contrato inteligente. Outro requisito é que o preço da interface cadastrado por um roteador n em um enlace n-m deve ser o mesmo preço cadastrado pelo roteador m, como forma de confirmação da existência desse enlace e de que o preço cobrado é justo. Com esses requisitos atendidos é possível que qualquer roteador produza as STPs e os demais roteadores validem sua precisão através da Eq. 5.1 com os parâmetros DPIFA que recebeu dos demais roteadores.

Cada STP inclui também uma recompensa para o seu criador que é definida por ele mesmo e somada ao valor do seu C_n. A recompensa possui o propósito de servir como incentivo para que os roteadores criem essas propostas e para compensar os custos computacionais e tarifas envolvidas no seu processamento e na transação realizada na blockchain pública.

O HARPIA tolera um erro no cálculo de cada C_n até um limite percentual δ. Para cada roteador p que cria e dissemina uma STP_p, cada um dos outros roteadores l verifica se cada C_n^p dessa STP está dentro do limite local calculado $C_n^l \pm \delta$. Valores divergentes também são contabilizados como inconsistências conforme explicado na seção anterior. Além desse esquema de tolerância, o HARPIA permite que cada roteador valide as STPs de acordo com qualquer outro esquema arbitrário, como mecanismos de reputação.

Cada roteador que concordar com uma proposta de STP deve enviar uma mensagem de confirmação (*STP Confirmation*) com uma assinatura ECDSA ao criador dessa STP. Uma percentagem mínima ζ dos membros do HARPIA deve confirmar a STP para iniciarem sua multi-assinatura conforme explicado na próxima seção.

5.4 MULTI-ASSINATURA MUSIG M-DE-N

O esquema de multi-assinatura MuSig (Seção 3.2.1) possui algumas propriedades que são apropriadas para soluções descentralizadas. Além das propriedades que se referem à redução dos requisitos de armazenamento das blockchains, ele é demonstravelmente seguro sob o pressuposto do problema do logaritmo discreto e no modelo de chaves públicas simples. Assim, os signatários precisam ter uma chave pública mas não precisam comprovar que possuem a respectiva chave privada através de uma PKI. Isso simplifica muito o processo de troca de chaves entre vários participantes e elimina a necessidade de uma PKI. A PKI caracterizaria um serviço centralizado, com privilégios sobre os demais participantes, e passível de ser subvertido ou de comportar-se maliciosamente (ASGHARI et al., 2013).

Além da STP, existem outros dois tipos de transações do HARPIA que requerem uma multi-assinatura de no mínimo m dos n roteadores membro para ser efetivada. As transações que lidam com a associação dos membros (`Join` e `Leave`) também precisam ser aprovadas por um mínimo dos membros atuais do HARPIA. O parâmetro ζ é um valor percentual no intervalo $[50 - 100)$ que representa o limiar m-de-n de signatários necessários para o MuSig dada uma rede com n roteadores. Qualquer número de signatários m que satisfaça $\frac{100m}{n} \geq \zeta$ é uma configuração válida para um determinado valor de ζ. Por exemplo, se ζ = 75%, multi-assinaturas com 3-de-4, 4-de-5, and 5-de-6 signatários satisfazem ζ.

Uma vez que o criador da transação consegue o mínimo de confirmações, ele pode enviar uma cópia da lista dos roteadores que confirmaram essa transação para cada um deles. A partir de então é possível prosseguir com as 3 rodadas do esquema MuSig com esses signatários (Seção 3.2.1). Se o MuSig for concluído com sucesso, o criador da transação pode enviá-la para a função correspondente do contrato inteligente (`Settle`, `Join` ou `Leave`), descritas na próxima seção. Roteadores que confirmem a participação em uma multi-assinatura e que não completem as três rodadas do MuSig podem ser acusados de inconsistência pelos outros membros, conforme explicado na Seção 5.2.

O MuSig também garante a privacidade dos membros que executam uma determinada multi-assinatura na blockchain pública, pois não é possível identificar as chaves públicas que compõem uma determinada chave pública agregada. Mesmo assim, a maioria dos membros, definida pelo parâmetro ζ, pode identificar quais participantes que assinaram uma multi-assinatura através das mensagens das rodadas de negociação do quórum do MuSig. O MuSig do HARPIA utiliza a curva elíptica secp256k1 e o algoritmo de resumo criptográfico SHA-256. As mensagens de confirmação de participação do signatário na multi-assinatura, de confirmação do conjunto de membros que vão participar na multi-assinatura e das três rodadas do MuSig precisam de um número de mensagens muito menor que o DPIFA, por isso optou-se pelo uso de comunicação através de RPC sobre TLS com confirmação de entrega.

5.5 CONTRATO INTELIGENTE

O componente central do HARPIA é um contrato inteligente construído sobre a blockchain Ethereum utilizando a linguagem Solidity. Uma instância do contrato inteligente para uma determinada subrede (que de agora em diante será chamada apenas de instância do HARPIA) gerencia a associação de membros e as negociações de criptomoeda entre eles. A identificação de cada roteador membro é o endereço público de sua conta Ethereum. A Tab. 12 descreve os parâmetros do HARPIA que são definidos na implantação do contrato inteligente e a Tab. 13 sumariza as funções do contrato inteligente apresentadas nas próximas subseções.

O HARPIA assume que os membros responsáveis pelos roteadores possuem alguma forma de organização. Esse pressuposto é necessário pois o HARPIA precisa que os membros troquem suas chaves públicas de alguma maneira segura, que entrem em acordo sobre os parâmetros do HARPIA e que realizem um processo de admissão de novos membros. Considera-se que esse pressuposto é aceitável, pois a auto-organização dos membros é inerente a redes comunitárias, que já necessitam interagir para estabelecer os enlaces entre os roteadores e negociar as condições de uso dessas redes. A forma dessa organização, ferramentas e processos estão fora do escopo deste trabalho.

Tabela 12 – Parâmetros do HARPIA armazenados no contrato inteligente.

Parâmetro	**Descrição**
β	Ciclo HARPIA, em número de blocos Ethereum
λ	Período das mensagens DPIFA
ζ	Limiar do MuSig *m*-de-*n* em percentual
$P_{n,m}$	Preço (*tokens*/GB) do tráfego do roteador *n* para o *m* no enlace entre eles
δ	Erro tolerável para cada C_n de uma STP
ξ	Validade de uma STP, em número de blocos Ethereum
τ	Saldo mínimo que um roteador deve possuir para se manter como membro
ϕ	Depósito mínimo para se associar
ω	Número do bloco Ethereum quando o último STP foi compensado
ρ	Janela de tempo da matriz de inconsistências (em ciclos)
$\mathcal{M}_{root}$	Raiz da árvore de Merkle

Tabela 13 – Funções do contrato inteligente HARPIA.

Função	**MTU** [a]	**MuSig** [b]	**Sinc** [c]	**Adm** [d]	**Descrição**
Join	Sim	Sim	Sim	Sim	Associa roteador
Leave	Sim	Sim	Sim	Sim	Remove roteador
Info	Não	Não	Não	Não	Informações dos membros
BuyTokens	Não	Não	Não	Sim	Compra *tokens*
RedeemTokens	Não	Não	Não	Sim	Resgata *tokens*
AddIface	Não	Não	Não	Sim	Registra enlace de rede e seu preço
DelIface	Não	Não	Não	Sim	Remove registro de enlace de rede
UpdtIface	Não	Não	Não	Sim	Atualiza preço de enlace de rede
Settle	Não	Sim	-	Não	Compensação de débitos e créditos pendentes

[a] Requer atualização das chaves públicas agregadas e da árvore de Merkle
[b] Requer multi-assinatura MuSig de *m*-de-*n* dos membros atuais
[c] Operação é completada somente no final da próxima transação `Settle`
[d] Operação administrativa que requer interação dos proprietários dos roteadores

5.5.1 Implantação do contrato inteligente

Para habilitar o HARPIA em uma rede, os roteadores precisam ser nodos Ethereum completos (*full nodes*), por isso é necessário que armazenem todo o arquivo da blockchain para operar. Esse é um dos requisitos para que o roteador seja independente de TTP no HARPIA.

A implantação (*deploy*) do contrato inteligente grava uma nova instância dele na block-

chain Ethereum. Cada rede deve possuir uma instância própria para operar. Esse procedimento pode ser realizado por qualquer um dos roteadores iniciais da rede. No caso do HARPIA, esse roteador também fica responsável por gravar as chaves públicas dos demais roteadores e a raiz da árvore de Merkle ($\mathcal{M}_{root}$) correspondente no contrato. No entanto, ele não se responsabiliza por intermediar o depósito inicial de no mínimo ϕ ether necessário para o HARPIA dos outros roteadores, pois isso abriria a possibilidade de fraudes. Assim, cada um dos roteadores além do que está implantando o contrato permanece no estado *Setup* até que deposite o valor mínimo de ether ϕ exigido para a sua associação à instância do HARPIA. O HARPIA não inicia até que todos os roteadores possuam o depósito mínimo. Se restar algum roteador sem o depósito mínimo dentro de um prazo estabelecido então qualquer roteador pode destruir o contrato. Esse procedimento resgata o saldo depositado por cada um dos roteadores. Na implantação também são configurados os parâmetros globais da instância do HARPIA que devem ser acordados previamente entre os responsáveis pelos roteadores.

Cada roteador só realiza o depósito após algumas verificações. Primeiramente, deve verificar se os parâmetros do HARPIA estão de acordo com o que foi acordado entre os responsáveis dos roteadores iniciais. Depois, deve reconhecer sua chave pública e a dos demais participantes iniciais no contrato inteligente. Por último, deve calcular as chaves públicas agregadas e a árvore de Merkle, para comparar com a raiz gravada no contrato implantado. Assim, o prazo para o depósito inicial deve ser no mínimo o tempo necessário para esse cálculo por todos os roteadores.

5.5.2 Associação de membros

Depois da implantação do contrato inteligente é possível que novos roteadores vizinhos da rede se associem à essa instância utilizando uma chamada à função `Join`. As funções `Join` e `Leave` (Algs. 2 e 3) são tarefas administrativas que requerem a interação entre os proprietários dos roteadores e a aprovação dos membros atuais da instância do HARPIA. Assume-se que a interação entre os vizinhos é inerente às redes físicas na qual o HARPIA está sendo implantado, pois é necessária para o próprio estabelecimento dos enlaces de comunicação. Além disso, é necessário que os membros atuais avaliem a entrada dos novos membros e aprovem seu ingresso através de um processo de votação de no mínimo m-de-n membros. A votação resulta em uma multi-assinatura MuSig para a transação `Join`. Da mesma maneira, para remover um membro da rede é necessária uma votação com multi-assinatura de no mínimo m dos n membros em uma transação `Leave`, ou uma transação `Leave` com assinatura individual do próprio membro que deseja abandonar a instância. No caso de uma operação `Leave` sobre um roteador que tenha sido liquidado (conforme descrito na próxima subseção), o roteador que faz a chamada à função resgata o saldo remanescente do roteador sendo removido. As operações de `Join` requerem um depósito inicial de ether, cujo valor mínimo (ϕ) é definido na implantação do contrato inteligente. Esse depósito é convertido em *tokens* do HARPIA que são válidos apenas para essa instância.

5.5.3 Settle

A função `Settle` do contrato inteligente, descrita no Alg. 1, pode ser executada até uma vez por ciclo, e realiza a validação e execução de uma STP. No final dessa função, qualquer transação que altere a composição de membros da instância HARPIA (`Join` ou `Leave`) que esteja pendente é completada e uma nova raiz de árvore de Merkle ($\mathcal{M}_{root}$) correspondente à nova composição de membros é gravada. Assim, essas funções não são finalizadas imediatamente quando são chamadas, mas apenas informam o endereço Ethereum do roteador a ser incluído ou removido, e a nova $\mathcal{M}_{root}$. Na versão atual, o HARPIA possui um limite de até uma operação `Join` ou `Leave` por transação `Settle` (consequentemente até uma por ciclo) pois a necessidade de implementação de filas para tratar os membros pendentes no contrato inteligente elevaria seu custo de execução na blockchain. Essa limitação restringe a aplicação do HARPIA a redes mais estáticas, como redes comunitárias.

Ao completar uma operação `Leave` pendente, a função `Settle` resgata uma quantidade de ether correspondente ao saldo de *tokens* HARPIA para a conta Ethereum do roteador que está saindo da instância. A função `Settle` também sinaliza a liquidação automática de roteadores que estão abaixo do saldo mínimo de *tokens* τ com o propósito de remover roteadores inativos, desligados ou defeituosos que possam comprometer o quorum do MuSig. Ao ser sinalizado como liquidado, qualquer outro roteador da instância pode preparar uma chamada à função `Leave` para remover esse roteador e para resgatar o seu saldo remanescente.

A STP é válida por um tempo correspondente a ξ blocos Ethereum. Assim, o número de blocos minerados desde que a STP foi proposta até a transação da função `Settle` ser minerada não pode exceder ξ, do contrário, a função `Settle` falha e uma nova proposta deve ser criada para esse ciclo incluindo novas contabilizações DPIFA que tenham sido produzidas desde a criação da STP que expirou. Essa validade determina o limite de tempo para as assinaturas do MuSig serem realizadas e também agiliza a compensação das contabilizações DPIFA já que impõe um prazo para os roteadores confirmarem e assinarem a STP. A Fig. 23 mostra uma linha do tempo com a duração típica de um ciclo quando o `Settle` é realizado dentro da sua validade. Já na Fig. 24, é mostrado um exemplo de STP expirada, que causa a extensão da duração do ciclo.

A recompensa para o roteador que faz a chamada à função `Settle` cria novos *tokens* para ele e, por isso, gera desvalorização dos *tokens* dos roteadores. A desvalorização consiste em um aumento na relação $\frac{\text{Saldo de } tokens}{\text{Saldo de ether}}$ no contrato inteligente e representa uma redução da taxa de câmbio entre *token* e ether. Essa desvalorização produzida no HARPIA visa inibir membros inativos e tende a manter apenas os membros que utilizam a rede, que encaminham dados ou que criam STPs. Assim, assume-se que os roteadores não terão interesse em ingressar em uma rede HARPIA para permanecer ociosos, pois os *tokens* desse roteador tendem a se desvalorizar em relação ao ether caso não sejam utilizados.

Algoritmo 1: Função `Settle` do contrato inteligente.

Entrada:
Multi-assinatura: σ
Chave pública agregada e prova Merkle: $\tilde{X}, \mathcal{M}_{proof}$
Timestamp, *nonce* e número do bloco Ethereum na criação do STP: t, n, b
Proposta de transação para compensação de débitos e créditos: STP
Resultado:
Validação e compensação da STP
Recompensa ao criador da STP
Finalização de operações pendentes (`Join` e `Leave`)
Liquidação de roteadores com saldo abaixo do limite τ

```
1  início
2      se STP não expirou e último Settle ocorreu há mais de β · γ segundos então
3          se Chave pública agregada é válida então
4              se Multi-assinatura é válida então
5                  para C ∈ STP faça
6                      Ajusta saldo de cada roteador de acordo com C
7                      Liquida roteadores com saldo abaixo de τ
8                  Cria tokens de recompensa para quem criou a STP
9                  se Existe pendência de Join então
10                     Ativa novo roteador como membro do HARPIA
11                     Atualiza M_root
12                 se Existe pendência de Leave então
13                     Remove roteador e resgata seu saldo em ether
14                     Atualiza M_root
15                 Registra número do bloco atual em ω
```

Algoritmo 2: Função `Join` do contrato inteligente.

Entrada:
Multi-assinatura: σ
Chave pública agregada e prova Merkle: $\tilde{X}, \mathcal{M}_{proof}$
Timestamp, *nonce* e número do bloco Ethereum atual: t, n, b
Nova raiz da árvore de Merkle: $\mathcal{M}_{root}$
Chave pública do roteador: pk
Resultado:
Inserção de roteador como membro da instância HARPIA

```
1  início
2      se Depósito enviado para Join é maior que φ então
3          Obtém endereço Ethereum do roteador a partir de sua chave pública
4          se Chave pública agregada é válida então
5              se Multi-assinatura é válida então
6                  Cria novo roteador em estado Joining
7                  Ajusta seu saldo em tokens de acordo com o depósito em ether
8                  Armazena nova M_root em variável temporária
```

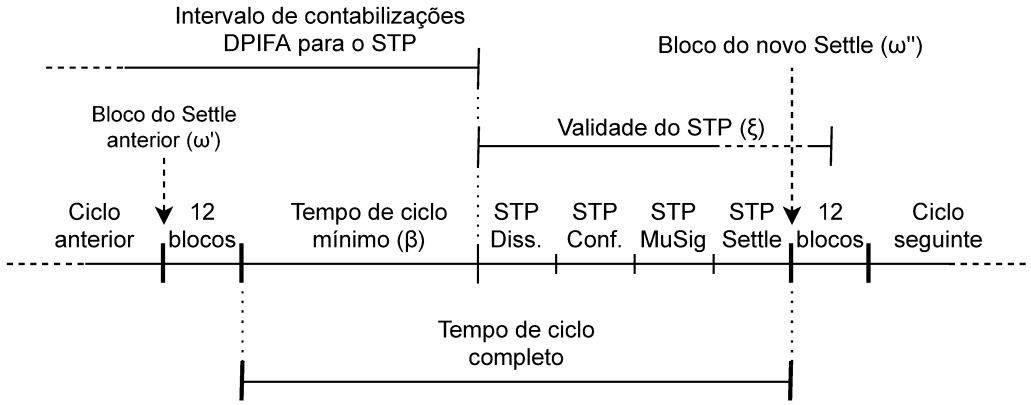


Figura 23 – Duração de um ciclo e validade da STP.

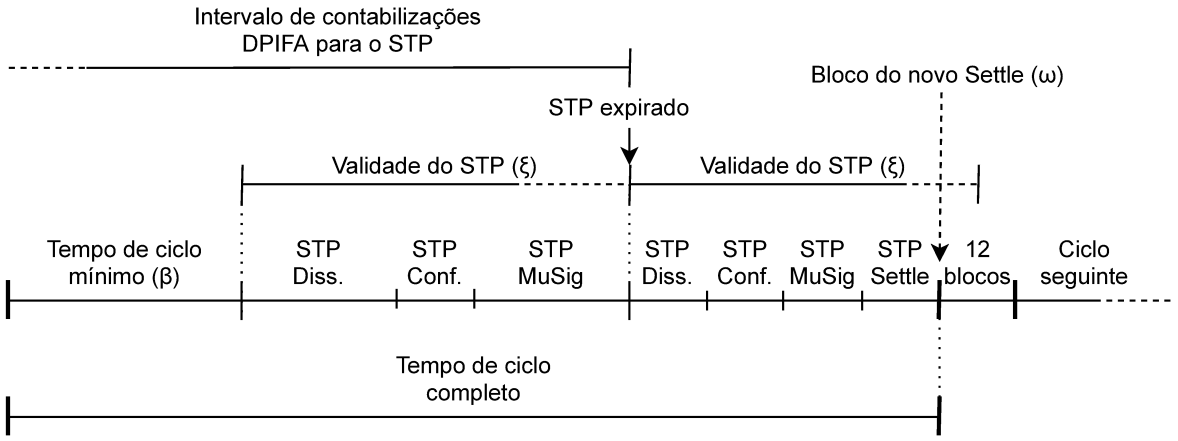


Figura 24 – Duração de um ciclo quando uma STP expira.

5.5.4 Verificação do MuSig

As funções `Join`, `Leave` e `Settle` exigem transações com multi-assinaturas MuSig válidas assinadas por no mínimo m-de-n dos roteadores membro. Essas funções recebem como parâmetro a multi-assinatura σ dos parâmetros da transação, a respectiva chave pública agregada $\tilde{X}$ e a prova Merkle $\mathcal{M}_{proof}$. A execução da função valida a multi-assinatura em dois passos. Primeiramente, valida $\tilde{X}$ utilizando $\mathcal{M}_{proof}$ e a raiz da árvore de Merkle $\mathcal{M}_{root}$ armazenada no contrato inteligente. Depois, valida σ utilizando $\tilde{X}$. Chamadas `Join` em instâncias HARPIA com apenas um membro exigem apenas uma assinatura ECDSA do membro atual em vez do MuSig. Além disso, sempre que for realizado um `Join` ou um `Leave`, é necessário calcular novamente todas as combinações válidas de chaves públicas agregadas e a respectiva árvore de Merkle. Essa tarefa é computacionalmente intensiva e deve ser realizada por todos os membros remanescentes individualmente para que o sistema seja efetivamente independente de TTP. O roteador que cria uma transação para a função `Join` ou para a função `Leave` informa também uma nova raiz da árvore de Merkle ao contrato inteligente que só será atualizada na próxima transação da função `Settle`.

Algoritmo 3: Função `Leave` do contrato inteligente.

Entrada:
Multi-assinatura: σ
Chave pública agregada e prova Merkle: $\tilde{X}, \mathcal{M}_{proof}$
Timestamp, *nonce* e número do bloco Ethereum atual: t, n, b
Nova raiz da árvore de Merkle: $\mathcal{M}_{root}$
Chave pública do roteador: pk
Resultado:
Remoção de roteador membro da instância HARPIA

```
1  início
2      Obtém endereço Ethereum do roteador a partir de sua chave pública
3      se Solicitante é o último roteador membro então
4          Destrói instância do contrato inteligente e resgata saldo
5      se Chave pública agregada é válida então
6          se Multi-assinatura é válida então
7              se Roteador foi liquidado então
8                  Solicitante recebe saldo do roteador liquidado
9              Altera estado do roteador para Leaving
10             Armazena nova M_root em variável temporária
```

5.5.5 Outras funções

O contrato inteligente também possui funções que não exigem multi-assinatura. A função `Info` retorna as informações atualizadas sobre os membros da instância do HARPIA. Essa função não consome ether, já que não precisa escrever nada na blockchain. A função `BuyTokens` deposita um valor de ether que é convertido em *tokens* válidos para um roteador na instância do HARPIA. A função `RedeemTokens` faz o processo inverso, ou seja, resgata os *tokens* de um roteador na forma de ether. Os *tokens* são utilizados para pagar pelo serviço de encaminhamento de pacotes e cada roteador precisa manter um mínimo de *tokens* τ.

O preço para encaminhamento de dados em um enlace da rede do HARPIA é definido arbitrariamente pelos responsáveis pelos roteadores do enlace no contrato inteligente de acordo com o valor que eles consideram justo. As funções `AddIface`, `DelIface`, e `UpdtIface` inserem, removem e atualizam os registros e os preços dos enlaces dos roteadores. Assim que um roteador ingressa na instância do HARPIA ele precisa registrar seus enlaces e seus preços (em unidades de *token*). Um enlace entre os roteadores X e Y só passa a ser contabilizado no DPIFA quando ambos os roteadores tiverem registrado ele no contrato com o mesmo preço. Além disso, o tráfego que passa por esse enlace só será cobrado em STPs quando o seu preço for maior que zero.

Devido à possibilidade de ramificações (*forks*) da blockchain que poderiam desfazer as operações já gravadas (KIFFER; LEVIN; MISLOVE, 2017), no HARPIA, as transações que escrevem na blockchain, incluindo as chamadas `Settle`, `Join`, e `Leave`, só são consideradas

confiáveis após a mineração de um determinado número de blocos. Assim, seguindo as convenções do Ethereum, assume-se que os valores gravados são imutáveis após a confirmação de 11 novos blocos depois do bloco minerado com a transação (WEBER et al., 2017).

5.6 ENDEREÇAMENTO DE REDE

No HARPIA, cada interface faz parte de um enlace ponto-a-ponto, ou seja, conecta dois roteadores. Cada interface é identificada pelo seu IP em uma subrede local do enlace, para as quais convenciona-se arbitrariamente o uso de máscara de rede de 30 bits para IPv4 e 64 bits para IPv6. Além disso, cada roteador deve cadastrar as subredes internas que atende. Dessa forma, é possível que os roteadores identifiquem os pares de roteadores dos enlaces e calculem o custo do encaminhamento de tráfego pelo DPIFA.

O endereçamento de rede dos roteadores em uma instância HARPIA deve ser atribuído pelos proprietários dos roteadores e as rotas definidas por protocolos de roteamento convencionais, ou até mesmo estaticamente. A alocação dos endereços para os roteadores deve ser realizada coletivamente pelos seus proprietários. Em redes IPv4, os roteadores podem utilizar endereços privados ou públicos, sendo que a utilização de endereços públicos depende de alocação prévia desses endereços em registros de números da Internet (HOUSLEY et al., 2013).

5.7 CASO DE USO

Para ilustrar o seu funcionamento, esta seção apresenta um caso de uso no qual o HARPIA pode ser aplicado. O cenário consiste em uma zona rural com serviço de Internet deficiente e caro. Na região existem quatro vizinhos dos quais apenas o vizinho D consegue conectividade por um preço aceitável com um provedor de serviços de Internet, conforme ilustrado na Fig. 25. Assim, os vizinhos que estão desconectados propõem implantar uma rede comunitária na qual o enlace de D com P (provedor) servirá como *backhaul*. O cenário também restringe as possibilidades de interconexão viáveis economicamente entre os participantes devido a obstáculos naturais como a montanha ilustrada na figura.

Como forma de incentivo para os roteadores que contribuírem com o encaminhamento de pacotes, os vizinhos decidem também utilizar o HARPIA para automatização da contabilização de tráfego e respectivas cobranças com criptomoeda. As subseções a seguir descrevem a implantação e operação do HARPIA nessa rede comunitária.

Equipamentos e conectividade

Primeiramente, os vizinhos precisam de equipamentos roteadores que atendam os requisitos de processamento e de armazenamento do HARPIA, que são apresentados no Cap. 6. Os requisitos de conectividade não são altos para o HARPIA e redes comunitárias típicas conseguem facilmente atingir velocidades de 100 Mbps com enlaces *full duplex* utilizando compu-

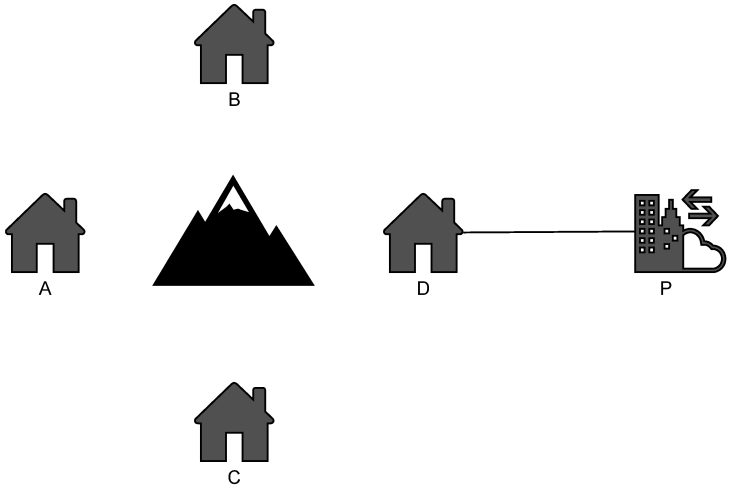


Figura 25 – Caso de uso: rede comunitária em zona rural.

tadores de propósito geral (MACCARI et al., 2019). Após análise das condições da região e custos de conectividade, os vizinhos decidem estabelecer a topologia ilustrada na Fig. 26 para interligarem seus respectivos roteadores.

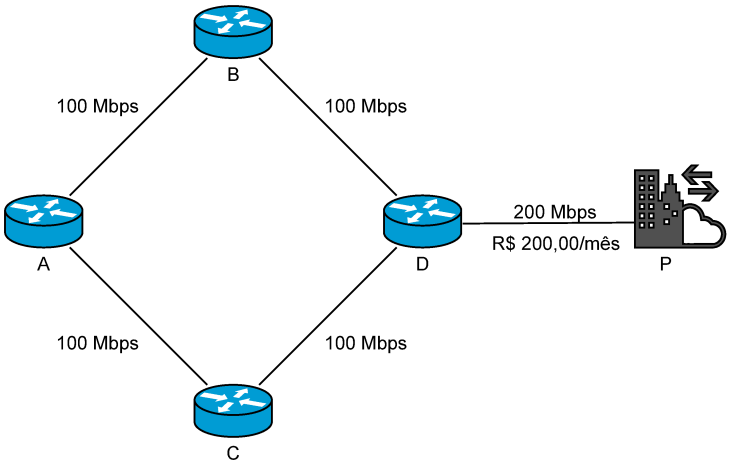


Figura 26 – Caso de uso: topologia da rede.

Cada um dos roteadores que vai participar da rede precisa ser configurado como um nodo completo Ethereum. Para isso é necessário que ele realize a cópia da blockchain. O restante dos detalhes de implantação física da rede, operação, custeio e questões regulatórias são abstraídos neste caso de uso e podem ser encontrados em diversos guias de implantação de redes comunitárias (INTERNET SOCIETY, 2021; NUPEF, 2021).

Implantação do contrato inteligente

Após os responsáveis definirem conjuntamente os parâmetros da instância do HARPIA, eles trocam as suas chaves públicas (Fig. 27) e um deles se responsabiliza pela implantação do contrato inteligente na blockchain Ethereum. Na implantação, são gravadas as chaves

públicas de todos os membros iniciais, a raiz da árvore de Merkle das chaves públicas agregadas e os parâmetros do HARPIA na blockchain Ethereum (Fig. 28a). Para esse exemplo, são utilizados os parâmetros apresentados na Tab. 14.

Tabela 14 – Parâmetros do HARPIA para o caso de uso.

Parâmetro	**Valor**
β	172800 blocos ($\beta \cdot \gamma = 1$ mês, sendo $\gamma = 15$s)
λ	15 minutos
ζ	75%
δ	5%
ξ	24 blocos
τ	R$ 50,00
ϕ	R$ 200,00
ρ	30 ciclos

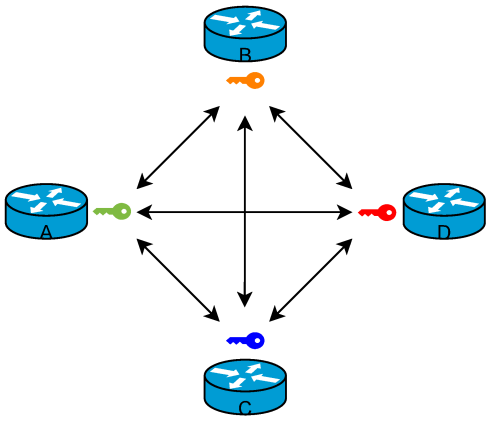


Figura 27 – Caso de uso: troca de chaves públicas dos membros iniciais.

Cada um dos outros roteadores verifica se os parâmetros do HARPIA, as chaves públicas dos membros e a raiz da árvore de Merkle estão corretos no contrato inteligente. Se todos esses valores corresponderem com o que foi acordado, cada um dos membros deposita o valor mínimo de ether ϕ exigido para o ingresso de membros (Fig. 28a). Assim que todos os roteadores informados na implantação alcançarem o valor mínimo de depósito inicial, a instância do HARPIA inicia.

Definição dos preços dos enlaces

O preço que cada roteador cobra pelo tráfego nos seus enlaces é definido por regras de mercado que devem levar em consideração os custos de sua implantação, operação, além da

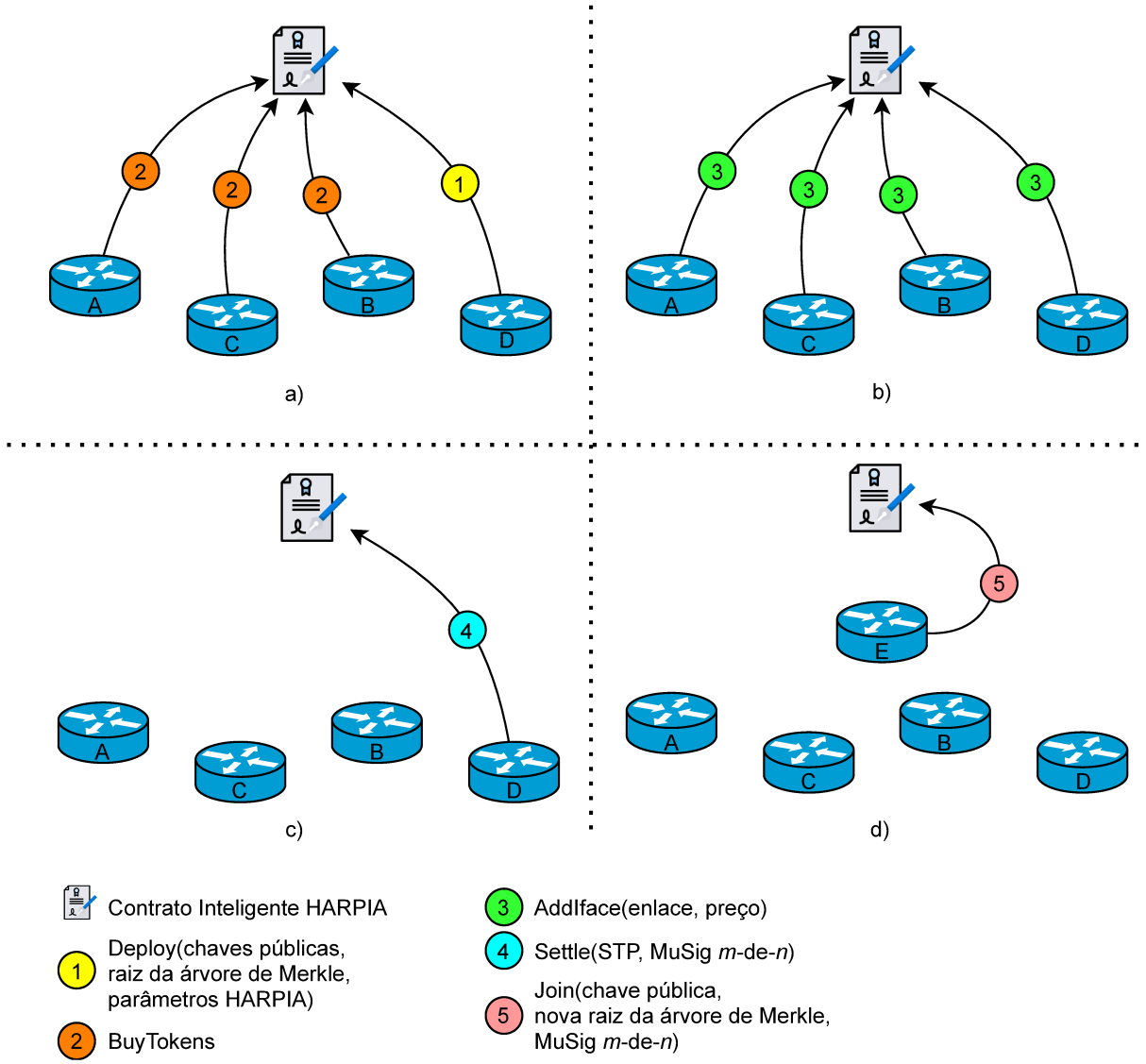


Figura 28 – Caso de uso: transações do contrato inteligente.

oferta e demanda de enlaces na região. Cada proprietário de roteador deve encontrar o preço justo que cubra suas despesas e permita que sua vizinhança obtenha um serviço com preço mais acessível que os serviços comerciais convencionais disponíveis no local.

No exemplo desse caso de uso, a precificação dos enlaces não será detalhada e os preços utilizados seguirão arbitrariamente o próprio preço do enlace de *backhaul* como referência. No caso, considerando a rede com quatro roteadores, com custo mensal do enlace de *backhaul* de R$ 200,00 e com consumo médio por residência de 5 GB por dia, o preço por enlace pode ser definido por $\frac{200}{4\times5\times30}/H_{avg}$, sendo $H_{avg} = \frac{4}{3}$ (distância média entre dois roteadores, em número de saltos), o que resulta em aproximadamente R$ 0,25/GB. Esse cálculo considera que a maior parte do tráfego será com serviços da Internet e tem o objetivo de promover um rateio dos custos do enlace de *backhaul* que é pago pelo roteador D.

Cada um dos roteadores registra cada um de seus enlaces com esse preço através da função `AddIface` do contrato inteligente (Fig. 28b). A partir do momento que um enlace de

rede é registrado com o mesmo preço pelos dois roteadores que são interligados através desse enlace, o DPIFA começa a contabilização distribuída desse enlace.

Contabilização de tráfego e compensação

A cada período λ cada roteador envia uma mensagem DPIFA para todos os demais roteadores contendo as estatísticas de tráfego de rede dos seus enlaces registrados. Por exemplo, cada mensagem DPIFA do roteador A contém as estatísticas dos enlaces A-B e A-C e é enviada para os roteadores B, C e D, conforme ilustrado na Fig. 29.

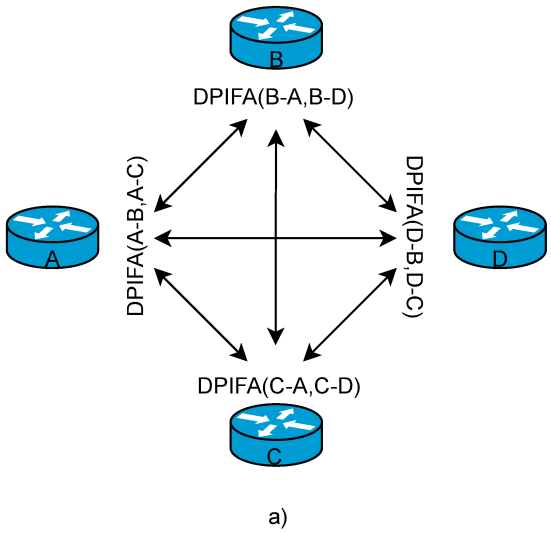


Figura 29 – Caso de uso: troca de mensagens DPIFA com estatísticas de tráfego.

Com a contabilização DPIFA e os preços dos enlaces é possível calcular as STPs. Para isso, também é necessário que o grafo formado pelos enlaces cadastrados com seus preços no contrato inteligente seja conexo e que todos os roteadores possuam caminhos uns para os outros. Assim, é possível calcular P_n, P_{avg} e H_{avg} necessários para o cálculo da STP conforme a Eq. 5.1. Nesse exemplo, após o tempo mínimo de ciclo do HARPIA ($\beta \cdot \gamma$) o roteador D constrói uma STP. O roteador D envia essa STP para todos os outros roteadores (Fig. 30a) e, assim que $m-1$ ou mais roteadores confirmam essa STP para D (Fig. 30b), D envia outra mensagem para cada um deles contendo a lista dos roteadores que vão participar do MuSig m-de-n (Fig. 30c).

Os roteadores confirmados produzem uma multi-assinatura com as três rodadas do MuSig cujas mensagens são ilustradas na Fig. 31. Por último, D faz a chamada à função `Settle` do contrato inteligente que realiza a compensação de débitos e créditos pendentes (Fig. 28c).

O DPIFA só contabiliza o tráfego entre os roteadores membro da instância e não possui mecanismo para contabilizar quanto que cada um deles utilizou dos enlaces de *backhaul*. Uma maneira de os participantes contornarem essa limitação é estabelecendo túneis de rede ou *proxies* de aplicação para saída para Internet através do roteador D conforme explicado na Seção 5.2. Assim todo tráfego com a Internet e a rede comunitária será cobrado do roteador D, que deve negociar uma compensação com cada um dos outros roteadores.

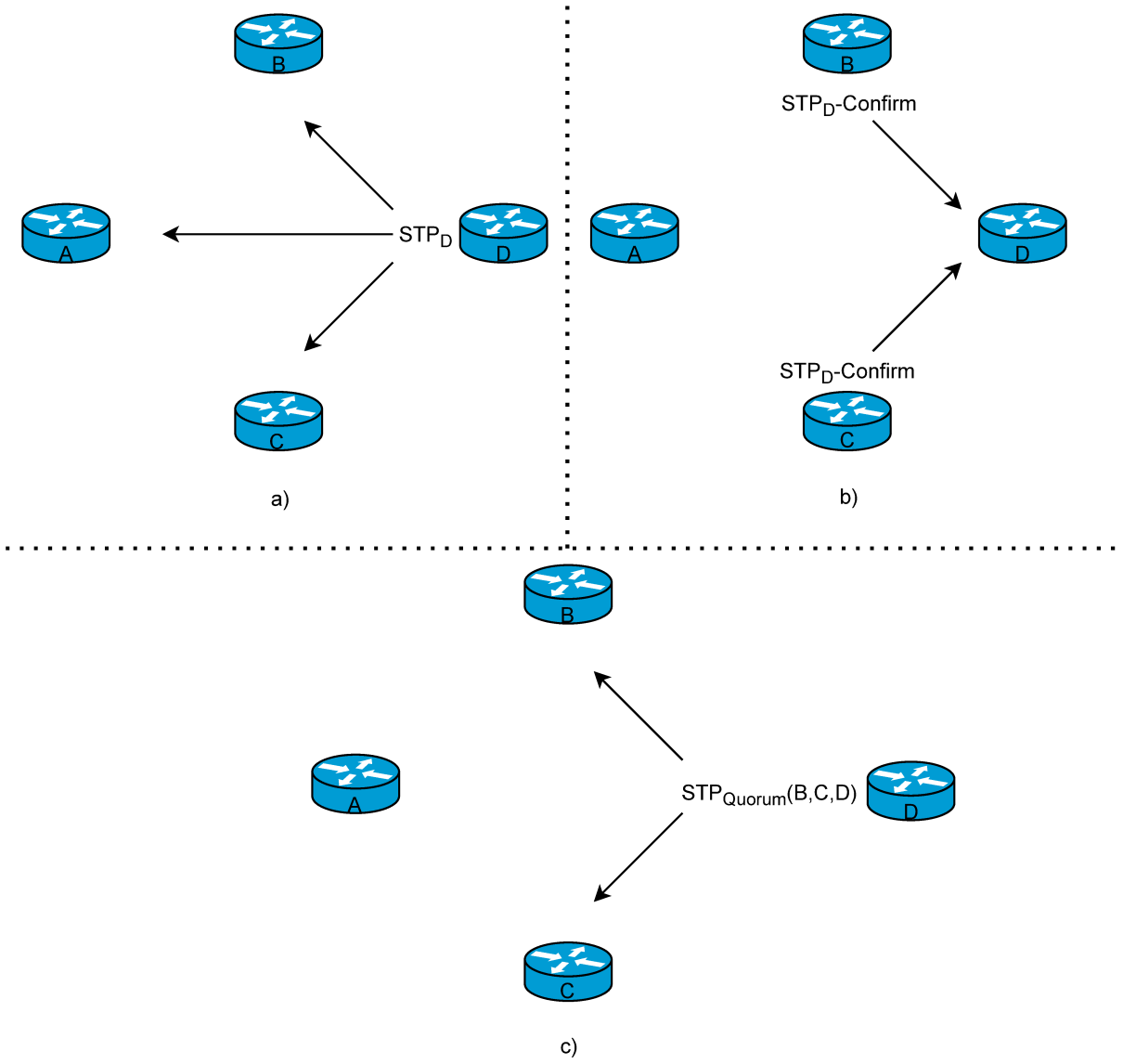


Figura 30 – Caso de uso: proposta e confirmação de STP.

Ingresso de roteadores

Supondo que um novo membro E deseje ingressar na rede comunitária integrado ao HARPIA. Primeiramente, ele deve negociar com os demais membros seu ingresso, a conectividade e realizar a troca de chaves públicas com esses membros. Posteriormente, após a configuração do roteador E, dos seus enlaces e da blockchain Ethereum, o roteador calcula as chaves públicas agregadas e a respectiva árvore de Merkle.

O roteador E constrói uma transação `Join` com um depósito de criptomoeda acima de ϕ e a nova raiz da árvore de Merkle. Em um processo semelhante ao da confirmação de uma STP ilustrado na Fig. 30, a transação `Join` é enviada para todos os outros participantes na rede entre os quais A, B e D respondem com uma mensagem assinada confirmando que concordam com o ingresso do novo membro. Como um percentual maior ou igual a ζ dos roteadores ativos confirmou o ingresso de E, ele pode proceder enviando uma mensagem para cada um

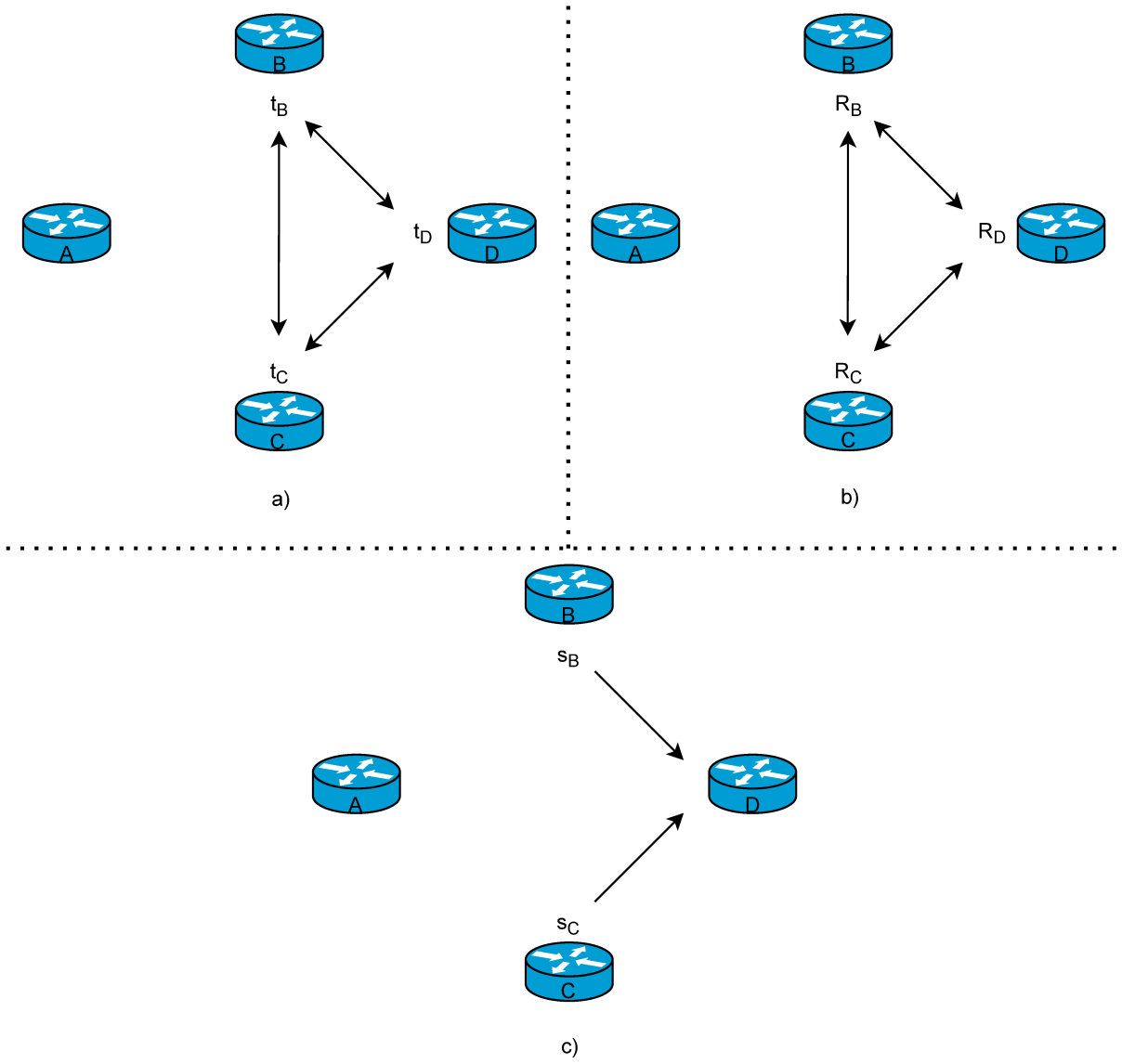


Figura 31 – Caso de uso: troca de mensagens das três rodadas do MuSig *m*-de-*n*.

desses roteadores informando quais deles que participarão do MuSig *m*-de-*n*. Os roteadores confirmados produzem uma multi-assinatura com as três rodadas do MuSig (Fig. 31). Por último, o roteador E faz a chamada à função `Join` do contrato inteligente com a transação construída e assinada com MuSig (Fig. 28d).

A transação só será efetivada após a próxima chamada de *Settle* que é realizada conforme detalhado na subseção anterior. Ainda é necessário que o roteador E e seus vizinhos registrem os preços de seus enlaces através da função `AddIface` para que o DPIFA os inclua nas contabilizações e para que o tráfego deles seja cobrado nas STPs.

5.8 DISCUSSÃO

Esse capítulo apresentou uma proposta de arquitetura de sistema dentro do estado da arte que é independente de TTP e com custos moderados na blockchain pública. O capítulo tam-

bém inclui um caso de uso típico para auxiliar no entendimento do funcionamento da proposta. Durante a modelagem desse sistema foram identificadas algumas limitações em potencial. O desempenho de alguns componentes como o MuSig ou o DPIFA poderia se tornar um gargalo dependendo do número de roteadores ou dos valores dos parâmetros utilizados na instância do HARPIA. Além disso, algumas ameaças de segurança em potencial foram identificadas e decidiu-se elaborar uma análise de ameaças com o propósito de remodelar a arquitetura ou elaborar contramedidas. No decorrer desse processo, a remodelagem incorporou subcomponentes, como a matriz de inconsistências, ou mecanismos de incentivo adicionais, como o resgate de saldo e liquidação de roteadores ociosos. O próximo capítulo apresenta os elementos mais importantes das análises quantitativas e qualitativas realizadas durante e após a modelagem do HARPIA.

6 AVALIACÃO DO HARPIA

Este capítulo apresenta uma análise quantitativa e qualitativa do HARPIA que visa avaliar o impacto tecno-econômico e a segurança da sua utilização em redes cooperativas. A análise quantitativa foi baseada em protótipos e simulações dos principais componentes do HARPIA e foi subdividida em três partes: uma análise de desempenho dos componentes com maior impacto de processamento e comunicação; uma análise de escalabilidade para processamento, armazenamento e comunicação, com a finalidade de identificar potenciais gargalos; uma análise dos custos de operação do contrato inteligente em blockchains públicas. A análise qualitativa consiste em uma identificação preliminar das ameaças de segurança e das respectivas contramedidas para mitigá-las.

6.1 CENÁRIOS UTILIZADOS

Foram modelados 4 cenários para as análises quantitativas com 8, 16, 32 e 64 roteadores para representar as características de redes comunitárias da maneira mais próxima possível. Esses cenários foram utilizados para as análises de desempenho, de escalabilidade e de custos na blockchain. Não foram realizadas análises com mais do que 64 roteadores considerando que, acima desse número, o HARPIA apresenta limitações de tempo de processamento e de requisitos de armazenamento de dados que impedem sua utilização. Cada um desses cenários é ilustrado nas Figuras. 32-35. Cada elemento `rte` das figuras representa um roteador de infraestrutura de uma rede comunitária. Esses roteadores podem também dar acesso a dispositivos das suas redes locais. No entanto, esses dispositivos são abstraídos dos cenários, que se limitam a ilustrar os elementos de infraestrutura.

Para esta análise, assume-se que cada roteador possui hardware e software equivalente ao apresentado na Tab. 15. Essa plataforma corresponde a um computador de propósito geral que foi utilizado para as análises de desempenho. É importante observar que a plataforma utilizada não representa um requisito mínimo para execução dos componentes avaliados. Além disso, é possível utilizar virtualização de funções de rede (NFV) (HERRERA; BOTERO, 2016) em cada roteador para alocar os recursos de forma adaptativa de acordo com os requisitos de processamento, memória e armazenamento necessários de cada componente.

Tabela 15 – Hardware e software utilizado na avaliação de desempenho.

Hardware	CPU Intel Core i7-8550U 4GHz, Cache L2 8MB, RAM 16GB, SSD 32 Gbps
Software	Linux Kernel 5.4.0, glibc 2.31, Python 3.8.5 com fastecdsa 2.1.5

A topologia dos cenários modelados segue padrões de conectividade semelhantes aos identificados no trabalho de Vega *et al.* (VEGA et al., 2012) para as redes comunitárias da GUIFI.net (VEGA et al., 2015). Os autores desse trabalho mostram que a GUIFI.net é uma rede que cresceu sem planejamento com diversos aglomerados de roteadores interconectados.

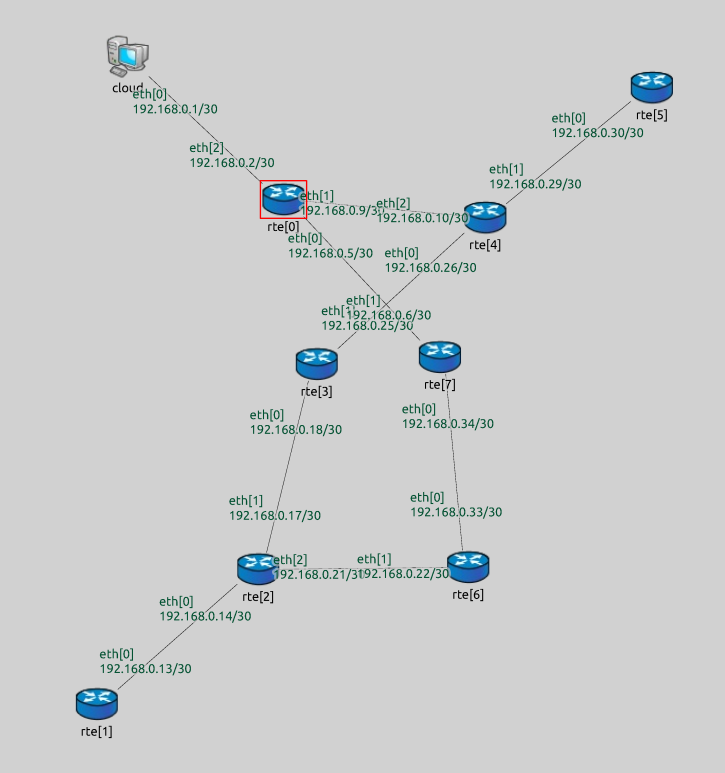


Figura 32 – Cenário com 8 roteadores.

A GUIFI.net também apresenta um grande número de saltos, ou seja, grafos com um diâmetro grande, particularmente entre os roteadores que são folhas dos grafos (terminais, como o roteador `rte[1]` das Figuras. 32-35) e as saídas para a Internet.

É importante ressaltar que os terminais dos cenários modelados não são dispositivos de usuários finais. Na verdade, esses terminais atendem suas redes locais e se conectam a um único roteador. O trabalho de Vega *et al.* salienta que esses terminais são indesejados em uma rede comunitária, visto que, devido à sua posição, utilizam a rede mas não contribuem com o encaminhamento de dados. No entanto, no caso do HARPIA, esse problema não deve afetar a dependabilidade da rede por esse motivo específico, pois o pagamento que esses terminais precisam fazer aos roteadores que se conectam compensa a falta de contribuição dos terminais na operação da rede. Ou seja, os roteadores que atendem esses terminais são incentivados a fornecer o serviço de forma adequada por meio do pagamento.

A Tab. 16 apresenta a quantidade de enlaces bidirecionais *full duplex* de 100 Mbps e 1Gbps utilizados para interconectar os elementos de rede e a quantidade de enlaces que apresentam perdas de pacotes de 0,1% e de 10%. Os enlaces de 100Mbps foram configurados com atraso de 400 a 500 μs seguindo uma distribuição uniforme, representando enlaces wireless de acordo com os testes de desempenho de Kolahi *et al.* (KOLAHI et al., 2021). Os enlaces de 1Gbps, foram configuradas com latência entre 3 a 4 μs também com distribuição uniforme, seguindo as especificações típicas de switches Ethernet de fibra ótica (SPURGEON; ZIMMERMAN, 2014). Em todos os cenários, os roteadores foram endereçados com IPv4 e a rede foi configurada com roteamento ótimo, ou seja, cada roteador alcança os demais roteadores atra-

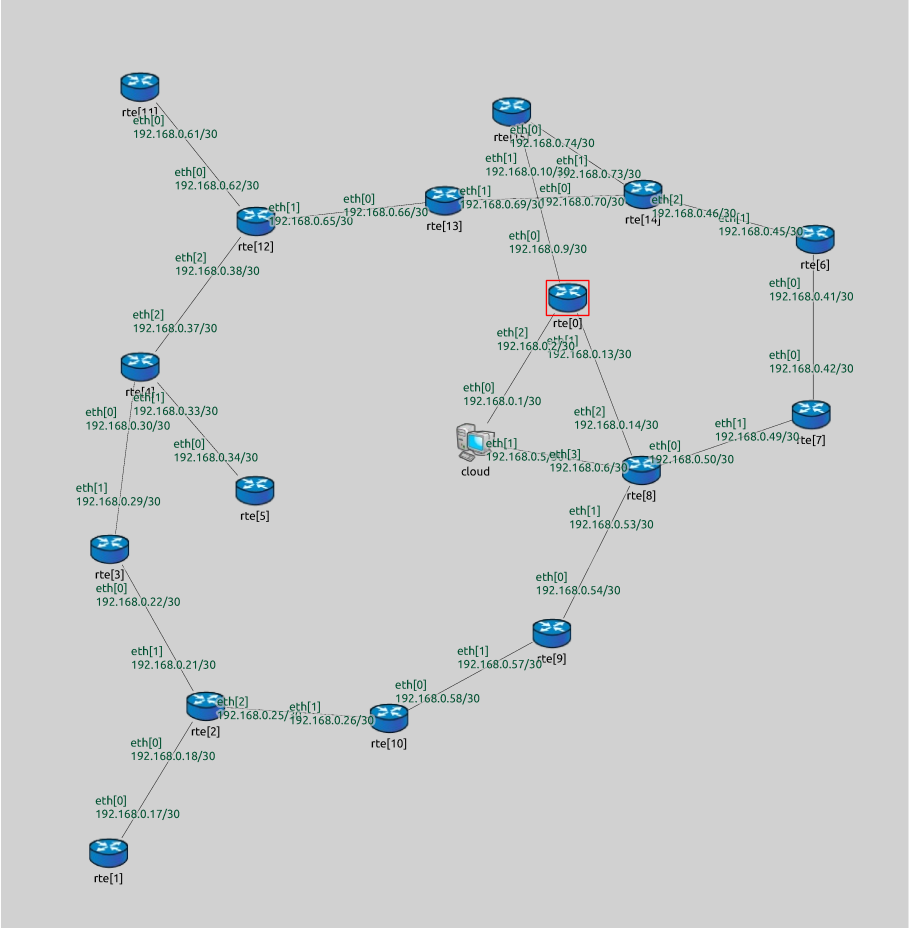


Figura 33 – Cenário com 16 roteadores.

vés dos melhores caminhos. Nas Figuras. 34 e 35 não são apresentados os endereços IP dos roteadores para não dificultar a visualização.

Tabela 16 – Parâmetros dos cenários – Enlaces de rede.

	Número de roteadores			
	8	16	32	64
Enlaces 100Mbps	8	16	32	64
Enlaces 1Gbps	1	3	9	18
Enlaces com perda de 0,1%	1	3	7	16
Enlaces com perda de 10%	0	0	2	2

Por último, com o objetivo de caracterizar cenários mais próximos dos reais, um servidor foi conectado a $n/8$ roteadores em cada cenário, representando o tráfego de serviços da Internet através de conexões de *backhaul* das redes comunitárias. Foi gerado tráfego de pacotes UDP de download (servidor para roteador) e upload (roteador para servidor) com tamanhos e intervalos de criação aleatórios, seguindo uma distribuição uniforme, dentro dos valores especificados na Tab. 17.

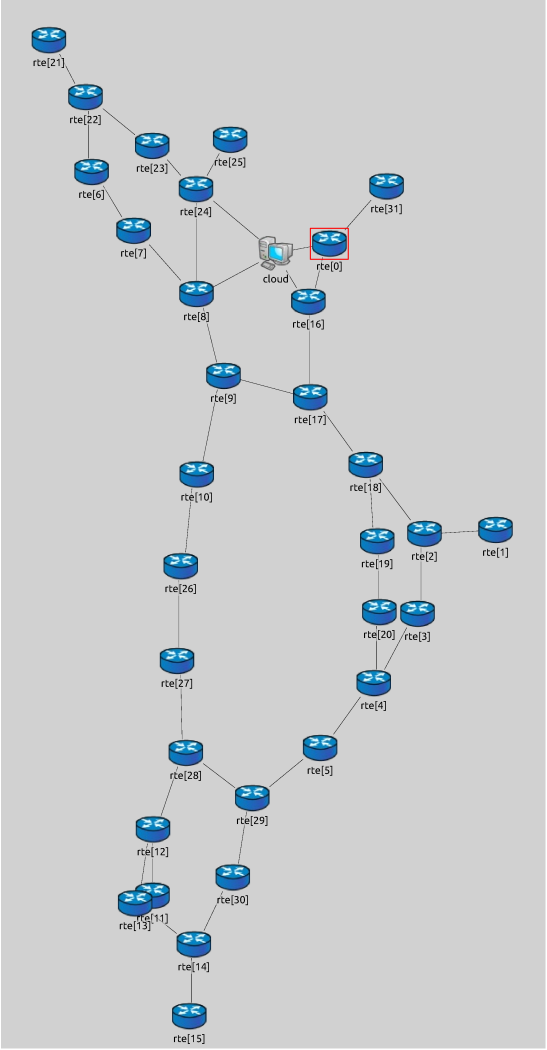


Figura 34 – Cenário com 32 roteadores.

Tabela 17 – Parâmetros dos cenários – Serviços da Internet.

Direção do tráfego	**Tamanho dos pacotes**	**Intervalo de criação**
Upload	100 a 200 bytes	0 a 20s
Download	1000 a 10000 bytes	0 a 0.2s

6.2 ANÁLISE DE DESEMPENHO

Esta seção apresenta análises de desempenho de componentes selecionados do HARPIA que foram realizadas para estimar o impacto da sua execução utilizando a plataforma descrita na seção anterior. A análise consiste de: (a) aferição dos tempos de execução do MuSig, componente com maior custo de processamento; (b) simulações do DPIFA, componente com maior sobrecusto de comunicação.

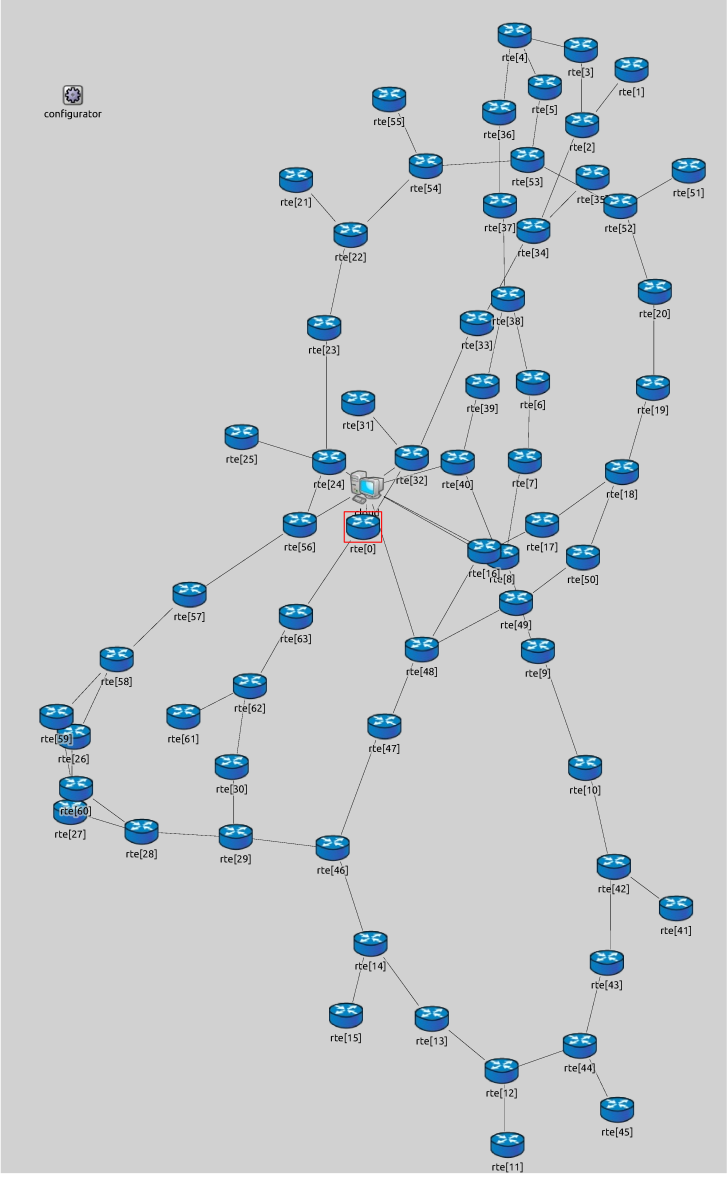


Figura 35 – Cenário com 64 roteadores.

Tempo de processamento

Foi analisado o tempo de processamento dos componentes do HARPIA mais intensivos computacionalmente. Para isso foram implementados e executados protótipos desses componentes em Python na plataforma da Tab. 15. Apesar da plataforma possuir mais núcleos de processamento, a avaliação foi feita com uma aplicação com uma única *thread* sendo que os trechos de código mais oneroso, que realizam cálculos com aritmética de curvas elípticas, podem ser facilmente paralelizados para explorar arquiteturas multiprocessadas.

O principal gargalo identificado está na criação das chaves públicas agregadas $\tilde{X}$ do esquema MuSig m-de-n devido ao número considerável de operações em curvas elípticas que é necessário no cálculo de cada $\tilde{X} = \prod_{i=1}^{k} X_i^{a_i}$. Essas chaves precisam ser calculadas novamente sempre que se realiza uma transação `Join` ou `Leave` no contrato inteligente para que as

multi-assinaturas e verificações MuSig funcionem com o novo conjunto de membros. Dado um limiar mínimo de signatários m e o número de chaves públicas de roteadores n, o número de chaves públicas agregadas válidas $C_{\tilde{X}}$ é calculado conforme a Eq. 6.1 e cada $\tilde{X}$ é calculado pelas Eqs. 3.1 e 3.2. Além disso, a produção da árvore de Merkle que serve para validar cada chave pública agregada $\tilde{X}$ requer a execução de $2C_{\tilde{X}} - 1$ operações H_{tree} (SHA-256).

$$C_{\tilde{X}} = \sum_{k=m}^{n} \binom{n}{k} = \sum_{k=m}^{n} \frac{n!}{k!(n-k)!} \tag{6.1}$$

A Tab. 18 mostra os resultados da execução com limiares ζ arbitrários para o MuSig. Os resultados demonstram que determinadas configurações m-de-n são viáveis de serem executadas em hardware de propósito geral similar à plataforma utilizada na análise e, portanto, em roteadores com custo relativamente baixo atualmente. Os testes de escalabilidade apresentados na próxima subseção complementam essa análise mostrando as estimativas de tempo de processamento para números maiores de roteadores.

Tabela 18 – Tempos de execução para calcular $C_{\tilde{X}}$ e respectiva árvore de Merkle.

ζ = mín(m-de-n)	**Média de tempo**[a]			
	8 roteadores	16 roteadores	32 roteadores	64 roteadores
75%	0,308s	39,17s	–	–
87,5%	0,100s	2,490s	1547s	–
93,75%	–	0,335s	21,15s	53458s

[a] Média de 30 execuções, exceto para 64 roteadores e ζ = 93,75% cuja média é de duas execuções.

As medições de tempo de processamento necessário para produzir as multi-assinaturas e respectivas verificações com MuSig em cada roteador com uma arquitetura equivalente à da Tab. 15 estão apresentadas na Fig. 36. Os gráficos correspondem à média de 30 execuções para $m = 4$, 8, 16, 32 e 64 e intervalo de confiança de 99%. Os resultados obtidos variam de 11,2 ms com 4 signatários até 163 ms com 64 signatários. A multi-assinatura precisa também de 3 rodadas de comunicação para as mensagens de t_i, R_i e s_i do MuSig que não são contabilizadas nesse gráfico. Assim, o tempo total da assinatura depende também da qualidade de comunicação entre os signatários. A verificação não precisa de comunicação entre os roteadores e o seu tempo de processamento não varia com o número de signatários, levando entre 2.5 ms a 3.0 ms.

Uma multi-assinatura σ no MuSig m-de-n precisa acompanhar também a chave pública agregada utilizada $\tilde{X}$ e a respectiva prova Merkle $\mathcal{M}_{proof}$. Assim, o roteador que está assinando a transação precisa produzir também $\mathcal{M}_{proof}$, que consiste em um conjunto reduzido de H_{tree} da árvore de Merkle que permite recalcular $\mathcal{M}_{root}$ a partir de $\tilde{X}$. Essa operação é trivial e consiste em uma busca pela folha da árvore correspondente a $\tilde{X}$ e na construção de um vetor contendo entre $\log_2(C_{\tilde{X}})$ e $\log_2(C_{\tilde{X}}) + 1$ nodos-irmão do percurso dessa folha até a raiz conforme ilustrado na Fig. 12. A verificação de $\tilde{X}$ com $\mathcal{M}_{proof}$ é realizada no próprio contrato inteligente cuja avaliação será apresentada na Seção 6.4.

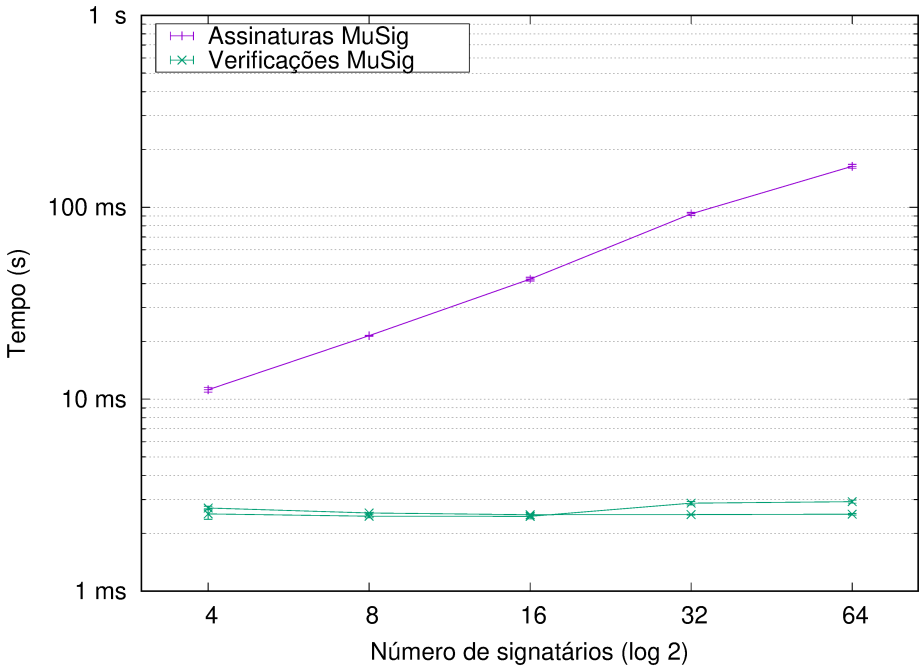


Figura 36 – Tempos de processamento por roteador para assinaturas e verificações MuSig.

O restante da arquitetura do HARPIA não apresenta custos de processamento significativos para o hardware utilizado na avaliação. O custo de processamento da blockchain Ethereum também não é significativo já que o roteador realizará apenas a sincronização da blockchain e não operações de mineração de blocos.

Sobrecusto de comunicação

O sobrecusto de comunicação do HARPIA é causado basicamente pelas mensagens de contabilização DPIFA e pelo MuSig. Outras mensagens, como STP, listas de inconsistências e as transações dos contratos inteligentes possuem sobrecusto insignificante. Além disso, a sincronização da blockchain Ethereum necessita em média de 144 Kbps de tráfego agregado por roteador (PUSTIŠEK; UMEK; KOS, 2019), que não inclui o download inicial do arquivo da blockchain (462GB no caso do programa OpenEthereum ou 875GB no caso do programa geth, conforme ilustrado no gráfico da Fig. 37) e serve apenas para atualizar os blocos. Importante observar que, tratando-se de uma rede incentivada com criptomoeda, o sobrecusto de rede implica também em custos na blockchain pública.

Devido à dificuldade de avaliação das características de comunicação dos componentes do HARPIA em um cenário real, como através da implantação e instrumentação de redes comunitárias, optou-se por um simulador de rede. Foram realizadas simulações dos cenários descritos na Seção 6.1 com o OMNet++, um simulador de eventos discretos amplamente utilizado para projeto e validação de novos protocolos de rede. Também foi utilizada a biblioteca INET do OMNet++ que fornece componentes para emular as tecnologias de interconexão e a pilha de protocolos IP.

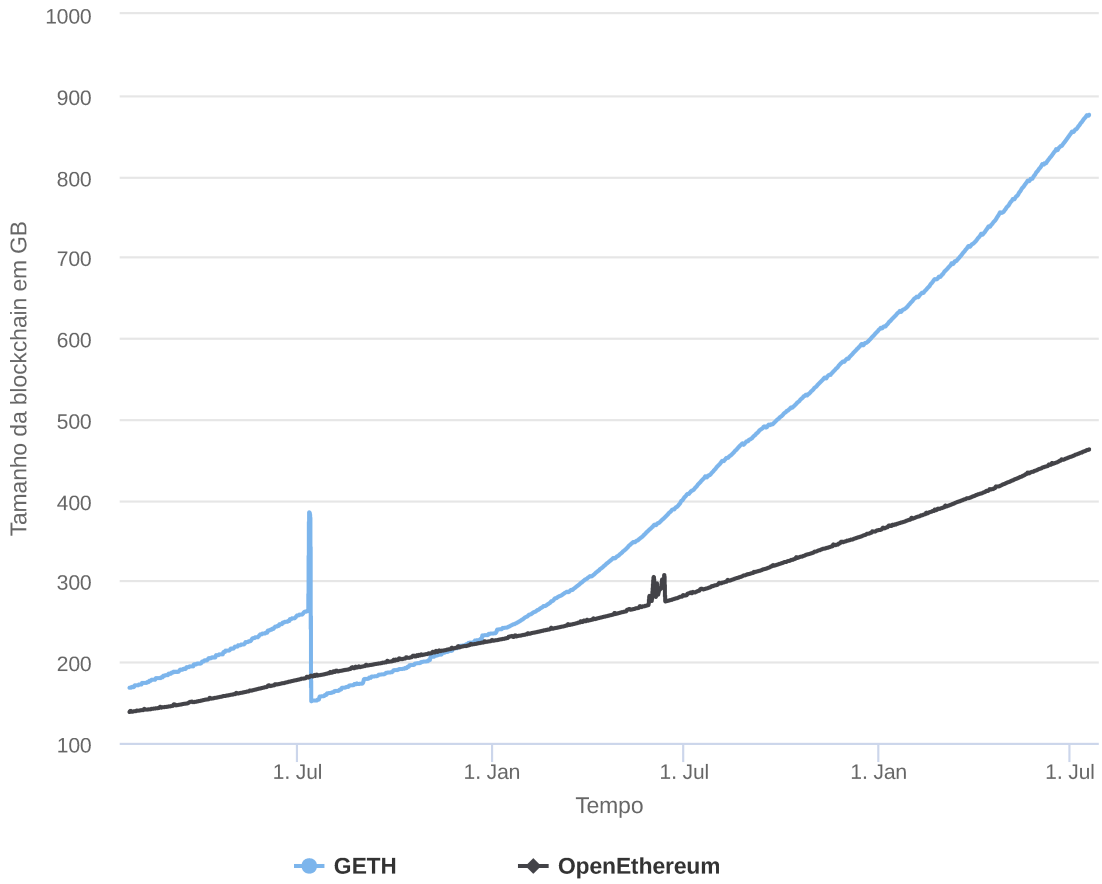


Figura 37 – Tamanho do arquivo da blockchain Ethereum. (Fonte: https://etherscan.io)

Inicialmente, o simulador foi utilizado para analisar a latência da comunicação DPIFA com UDP, considerando como latência o tempo que a mensagem leva desde seu envio pela aplicação remetente até a sua entrega na aplicação destino. O DPIFA possui comunicação todos para todos entre os roteadores, assim, essa análise permite verificar os tempos máximos e mínimos para comunicação entre qualquer par de roteadores da rede. Além disso, essa análise permite também estimar quais seriam as latências para comunicação dos demais componentes do HARPIA.

Para a simulação do DPIFA, foi criada uma aplicação do OMNet++ que dissemina mensagens de contabilização com período $\lambda = 15$ minutos durante 90 minutos, ou seja, por 4 períodos. A aplicação utiliza UDP unicast para enviar as mensagens de cada um dos roteadores para os outros $n-1$ roteadores, totalizando $4n(n-1)$ mensagens na rede a cada simulação. Para cada contabilização DPIFA de cada roteador, o envio das mensagens para os $n-1$ roteadores foi distribuído dentro do período λ para evitar enviar todas as mensagens ao mesmo tempo. O tamanho de cada mensagem da simulação foi arbitrariamente determinado considerando o caso de roteadores com quatro vizinhos, assim como nos testes de comunicação, totalizando 214 bytes. Além disso, o tráfego UDP do DPIFA concorre com o tráfego de usuários da rede simulado conforme descrito na Seção 6.1.

A Fig. 38 apresenta os resultados de latência para entrega das mensagens DPIFA. Cada diagrama de caixas do gráfico indica a mediana, o máximo e o mínimo, e os quartis superior e

inferior de latência para cada um dos 4 cenários modelados. Os resultados demonstram que o impacto de comunicação do DPIFA é insignificante para redes comunitárias com até 64 roteadores, que produziu um total de 16128 mensagens (3,29 MB) com $\lambda = 15$ minutos durante uma simulação de 90 minutos. Esse resultado equivale a uma média de 5,11 Kbps para toda a rede, ou 79,8 bps por roteador. A latência máxima obtida para as entregas das mensagens foi de 5,76 ms no cenário com 64 roteadores.

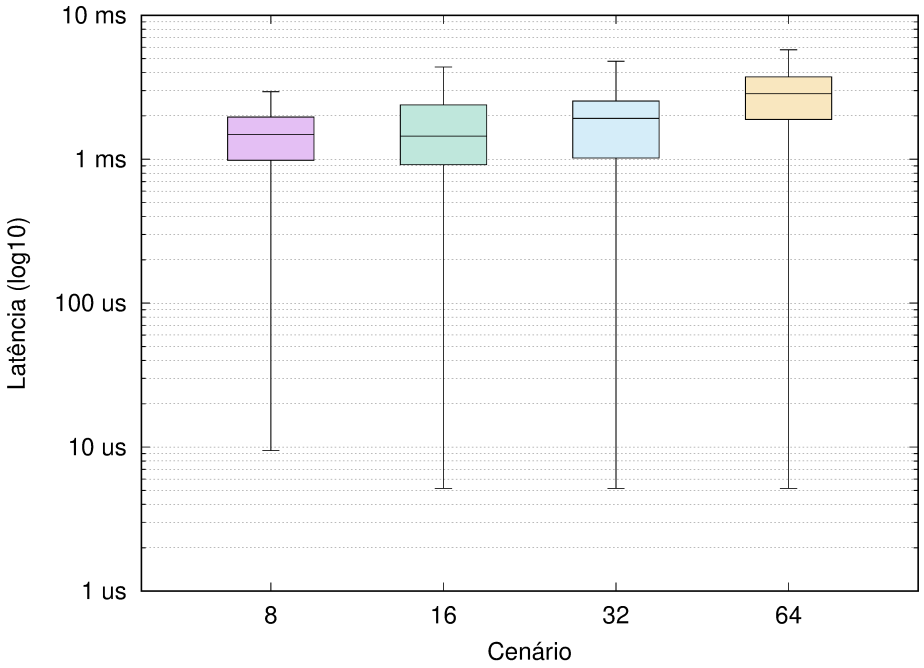


Figura 38 – Latência das mensagens DPIFA.

A latência é diretamente proporcional ao número de saltos e ao atraso no envio da mensagem que cada enlace causa. A latência máxima representa o caminho mais longo entre dois roteadores do cenário e a latência mínima representa o caminho mais curto. O caminho mais curto corresponde a dois roteadores diretamente conectados através do enlace com menor latência. Redes menos conectadas e com maior diâmetro apresentarão maior latência pois as mensagens necessitam de mais saltos para alcançarem seus destinos. Mesmo assim, considerando que o limite de membros do HARPIA é 64, seria impossível um número de saltos que aumentasse a latência de comunicação dessas mensagens a ponto de comprometer o funcionamento do HARPIA, utilizando tecnologias de interconexão atuais. Não foi avaliado o desempenho da troca de mensagens do STP, matriz de inconsistências, nem do MuSig por representarem uma parcela pouco significativa da comunicação se comparados ao DPIFA.

6.3 ANÁLISE DE ESCALABILIDADE

Com o intuito de estimar a escalabilidade do HARPIA, foram calculados os requisitos dos seus componentes para configurações mais estritas. Devido à limitação previamente iden-

tificada para tempo de processamento, não são apresentadas as estimativas para redes com um número de roteadores acima de 64. Os cálculos foram realizados utilizando R e Gnuplot.

Tempo de processamento

A Fig. 39 mostra as estimativas de tempo de processamento necessário para o cálculo das chaves públicas agregadas e da respectiva árvore de Merkle, baseadas em execuções parciais do protótipo implementado. Essas estimativas permitem avaliar quais configurações de número de roteadores n e de limiar de signatários m são viáveis de serem executadas, dada uma plataforma de execução. Por exemplo, se o tempo do ciclo HARPIA ($\beta \cdot \gamma$) for de 1 dia, então qualquer limiar ζ que resulte em um tempo de execução abaixo de 1 dia é aceitável. Na Fig. 39 foi desenhada uma curva de nível cujo plano está posicionado em 16 horas ($\approx 10^{4,76}$ segundos) no eixo do tempo de execução. Se for definido arbitrariamente que 16 horas é o limite de tempo tolerável para a execução, qualquer combinação de m e n que resultar em valores abaixo do plano representa uma configuração m-de-n aceitável.

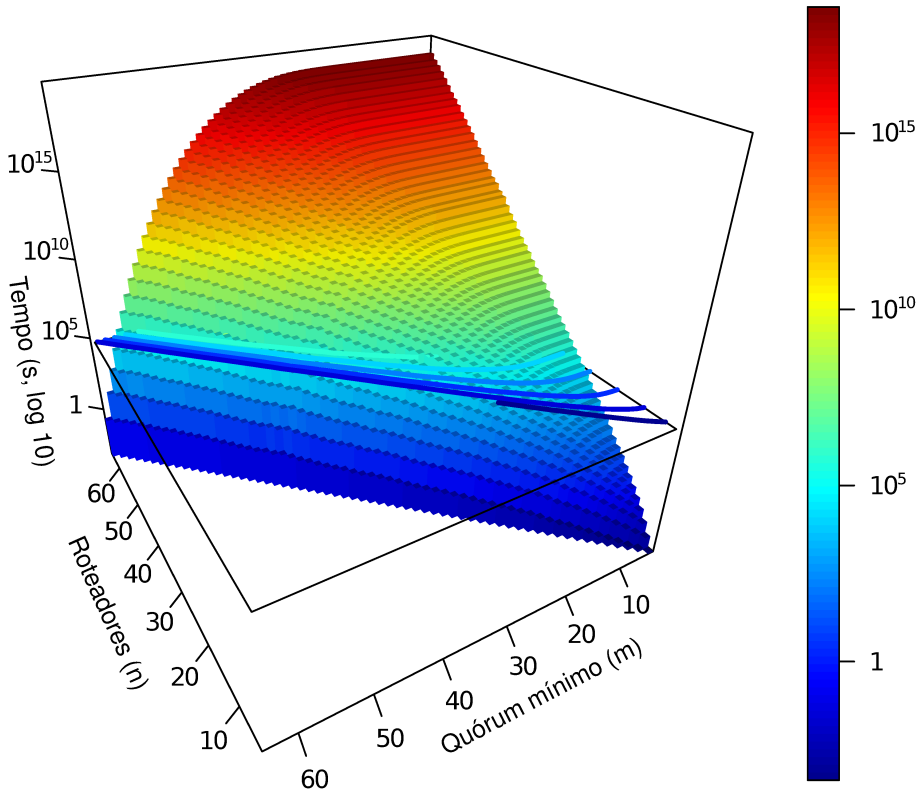


Figura 39 – Estimativas de tempo para calcular o conjunto de chaves públicas agregadas e sua árvore de Merkle.

Requisitos de armazenamento

Os custos de armazenamento do HARPIA são decorrentes, principalmente, do armazenamento das chaves públicas agregadas do MuSig m-de-n, da respectiva árvore de Merkle, e das contabilizações DPIFA. Além disso, os roteadores precisam de espaço para armazenar o

arquivo completo da blockchain. A Eq. 6.2 apresenta o cálculo de espaço de armazenamento mínimo necessário para o MuSig m-de-n, considerando que cada chave pública agregada $\tilde{X}$ possui 33 bytes (tamanho do ponto na curva elíptica na forma compacta) e cada resumo criptográfico H_{tree} da árvore de Merkle é um SHA-256 com 32 bytes. A Fig. 40 apresenta os requisitos de armazenamento dependendo do número de roteadores e do quorum mínimo do MuSig. Se considerarmos arbitrariamente um limite de 1TB como tolerável para os requisitos de armazenamento, qualquer combinação de m e n que resulte em um valor abaixo do plano com curvas de nível que está fixo em 1TB é uma configuração válida para o HARPIA.

$$33\mathcal{C}_{\tilde{X}} + 32(2\mathcal{C}_{\tilde{X}} - 1) \tag{6.2}$$

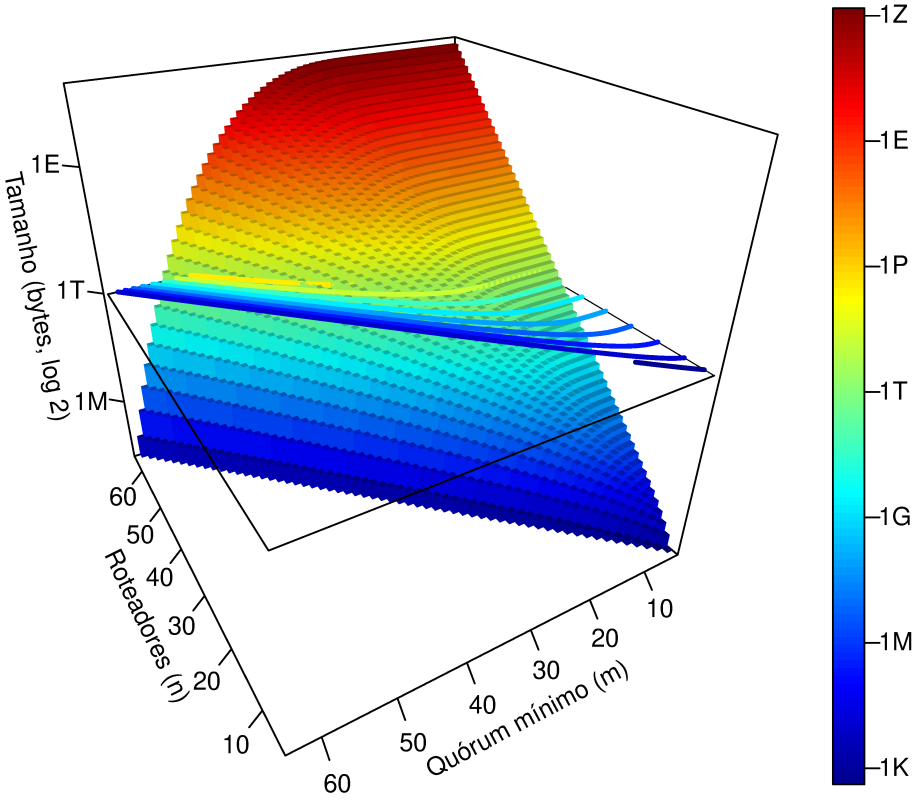


Figura 40 – Requisitos de espaço de armazenamento para chaves públicas agregadas e sua árvore de Merkle.

Sobrecusto de comunicação

A cada período λ, cada roteador envia uma mensagem cujo tamanho depende do seu número de enlaces de rede, ou seja, do número de vizinhos conectados a esse roteador. Por simplicidade, assume-se que cada par de vizinhos se conecta por no máximo um enlace de rede. Assim, um roteador com x vizinhos cadastrados no HARPIA terá x enlaces de rede contabilizados em uma mensagem DPIFA. Para a estimativa dos requisitos de armazenamento considerou-se um número médio de vizinhos $\nu = 4$ que resultam em mensagens DPIFA com 214 bytes (conforme os campos ilustrados na Fig. 22).

As mensagens DPIFA são guardadas até o final do ciclo HARPIA por cada roteador para o caso de outros roteadores perderem contabilizações devido à falhas de rede ou de hardware. Dessa forma, é possível que os roteadores recuperem mensagens perdidas e possam realizar os cálculos necessários para validarem as STPs. Considerou-se que a duração de um ciclo pode durar até duas vezes o tempo mínimo de ciclo, ou seja até $2(\beta \cdot \gamma)$, já que pode se estender em casos como STPs que não alcançam o quorum mínimo m dentro do tempo de validade da STP. A Fig. 41 mostra os requisitos de armazenamento das mensagens DPIFA de acordo com várias configurações de tempo de ciclo β e de período λ calculados para redes com n roteadores através da fórmula

$$2n(214)\frac{\gamma \cdot \beta}{\lambda} \tag{6.3}$$

Observa-se que, mesmo com parâmetros β e γ produzindo tempos de ciclo longos (1 mês) e com o parâmetro λ produzindo períodos curtos (2 minutos), os requisitos de armazenamento são moderados e adequados para computadores de propósito geral atuais de baixo custo.

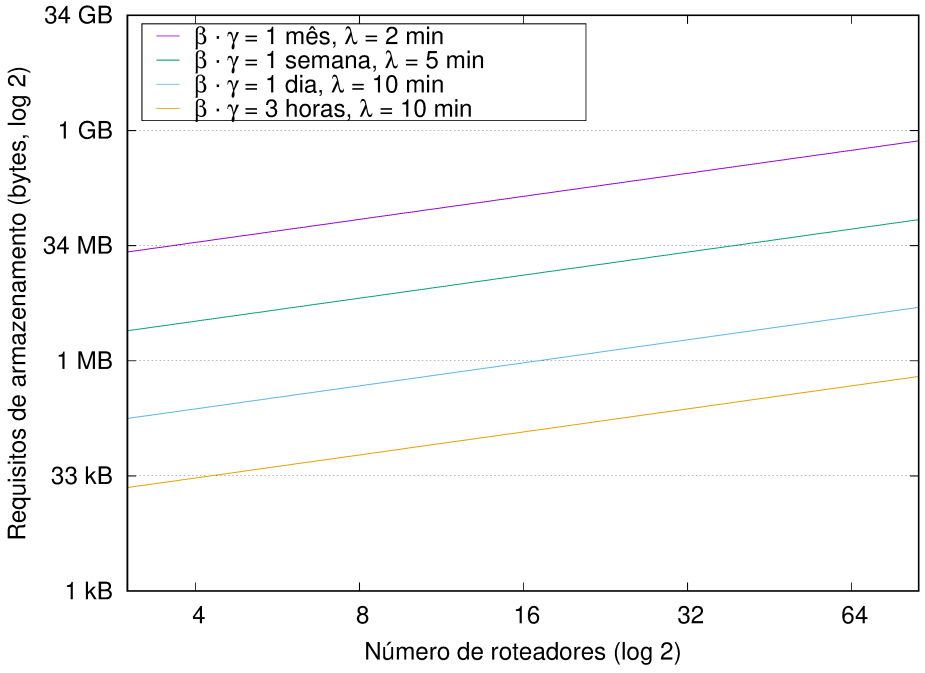


Figura 41 – Requisitos de espaço de armazenamento para o DPIFA.

Os dois parâmetros que mais influenciam o sobrecusto de comunicação próprio do HARPIA são o período λ das mensagens DPIFA e o número de roteadores membro. A Fig. 42 apresenta o número total de mensagens DPIFA a serem transmitidas por segundo na rede para diferentes períodos λ, calculado com $\frac{n(n-1)}{\lambda}$. Períodos típicos estão entre 1 minuto e 1 hora. Períodos maiores aumentam o risco dos roteadores perderem contabilizações devido a falhas antes dessas serem transmitidas e períodos muito pequenos podem causar um sobrecusto considerável na rede sem trazer nenhum benefício.

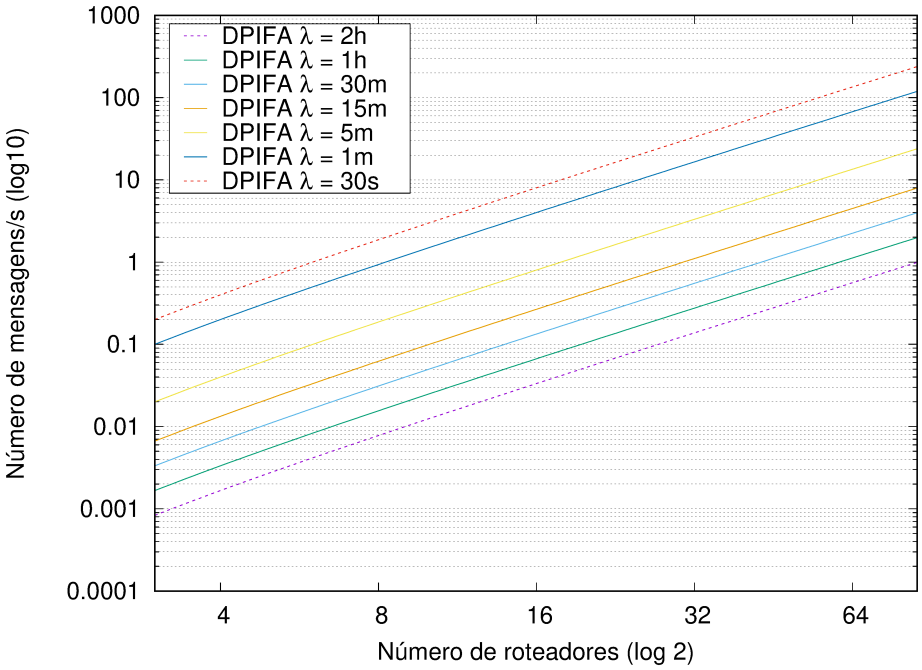


Figura 42 – Número total de mensagens DPIFA por segundo dependendo do período λ.

Outros parâmetros que influenciam o sobrecusto de comunicação, mas em escala muito menor que o parâmetro λ, são o ciclo β e o prazo de validade das transações ξ. Como só é possível efetivar uma transação de `Join` e `Leave`, ou de `Settle` por ciclo, a taxa de mensagens do MuSig necessárias para essas transações é indiretamente proporcional ao tamanho do ciclo. Além disso, quanto menor a validade ξ de uma transação, mais rapidamente as mensagens do MuSig precisam ser trocadas para efetivar a multi-assinatura a tempo de enviar a transação à blockchain, aumentando a taxa de mensagens do MuSig. Mesmo assim, o número de mensagens de uma operação MuSig com até 64 membros é pequeno se comparado ao DPIFA, conforme ilustrado na Fig. 43.

6.4 ANÁLISE DE CUSTOS NA BLOCKCHAIN

O custo da execução dos contratos inteligentes é medido em unidades de gás. É crucial estimar os custos de gás das transações das funções do contrato inteligente por duas razões principais: (a) porque as blockchains que suportam contratos inteligentes Solidity impõem um limite para o consumo de gás em uma transação (*gas limit*); (b) para definir os cenários nos quais o HARPIA é aplicável de acordo com os custos na blockchain pública. Para realizar essa estimativa foi utilizada a plataforma Remix (REMIX, 2021), uma interface integrada de desenvolvimento para a linguagem Solidity que permite analisar quanto gás cada função do contrato inteligente consome. O preço do gás, o limite de gás permitido para as funções e as cotações das criptomoedas foram obtidos dos sites dos provedores de serviços de blockchain Tokenview (TOKENVIEW, 2021), Polygonscan (POLYGONSCAN, 2021) e BscScan (BSCSCAN, 2021). Para a avaliação, o contrato inteligente foi compilado com a versão 0.7.5 do Solidity.

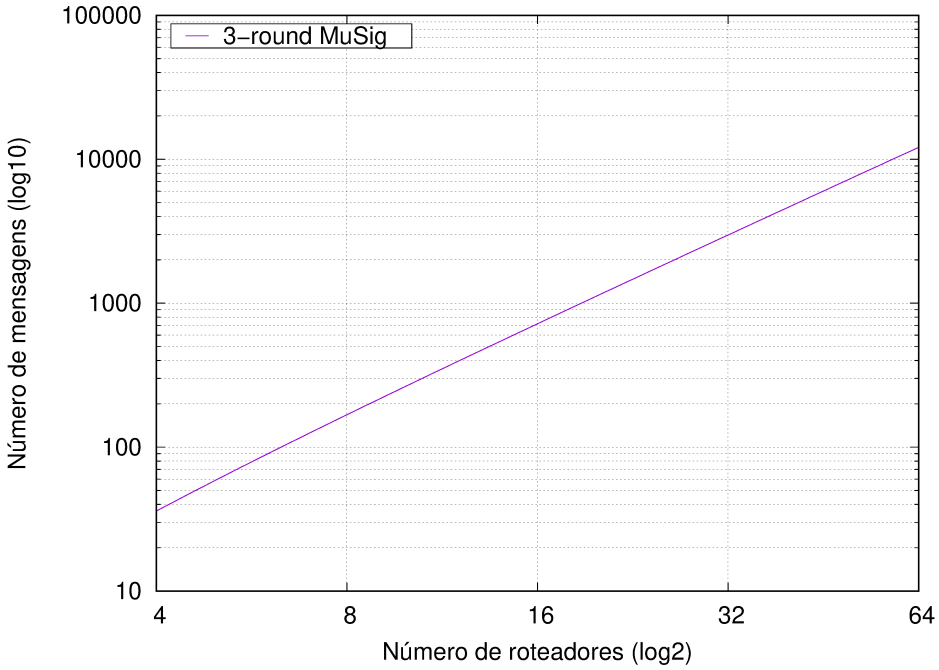


Figura 43 – Número de mensagens necessárias para uma operação MuSig.

A Fig. 44 mostra a quantidade de gás consumido pelas funções que exigem verificação de multi-assinaturas MuSig. O cálculo foi realizado para vários limiares ζ diferentes. Foi identificado que o número de roteadores membro na instância do HARPIA e o número de signatários das transações do contrato inteligente possui pouca influência no consumo de gás das funções. A função mais cara é a `Join` que consome 4,52M unidades de gás. Mesmo assim, ela ainda está bem abaixo do limite de gás imposto para transações nas blockchains analisadas, exibidos a seguir na Tab. 19. As funções `Leave` e `Settle` consomem entre 4,35M e 4,5M unidades de gás por transação, dependendo do limiar ζ configurado para o MuSig.

A Tab. 19 mostra o consumo de gás das transações do contrato inteligente convertidos em US$ com a cotação atual da Ethereum Classic e da Ethereum Mainnet, as duas principais blockchains públicas Ethereum. Também foram verificados os custos em outras duas blockchains que suportam contratos inteligentes Solidity: a Polygon, que opera sobre PoS e a BSC que funciona com PoSA. Os valores do preço de gás estão em unidades da criptomoeda utilizada em cada blockchain: ether ou ETH na Ethereum Mainnet, ETC na Ethereum Classic, MATIC na Polygon e BNB na BSC. A blockchain Ethereum Mainnet apresentou custos consideravelmente altos com US$ 269,41 por chamada da função `Settle`, mas a Ethereum Classic teve custos bastante reduzidos com apenas US$ 0,73. Ambas blockchains com PoS apresentaram custos relativamente baixos. É importante ressaltar que os custos estimados não representam uma medida definitiva e dependem da cotação das criptomoedas e das transações nos contratos inteligentes que varia conforme a oferta e a demanda.

A escolha da blockchain deve considerar um compromisso entre a confiabilidade da blockchain (SAAD et al., 2020), o orçamento disponível para os membros da rede comunitária e a frequência das transações do contrato inteligente. A frequência das transações pode ser ajus-

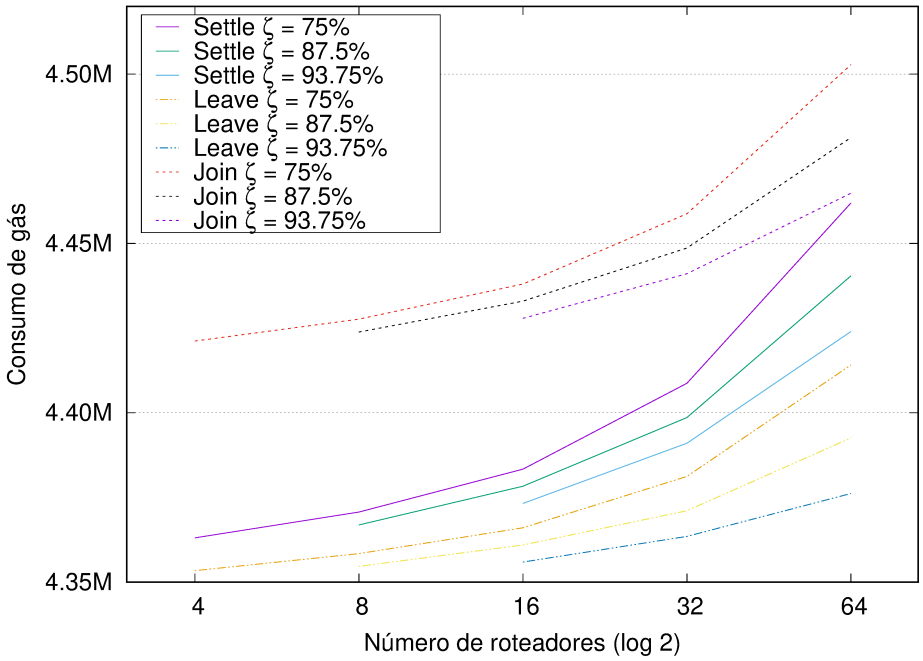


Figura 44 – Consumo de gás no HARPIA.

Tabela 19 – Custos de gás nas transações do HARPIA para várias blockchains[a].

	Mainnet	**Classic**	**Polygon**	**BSC**
Preço do gás[b]	22 Gwei	4,8 Gwei	28 Gwei	7 Gwei
Limite de gás	15M	8M	20M	45M
Cotação	US$ 2709,34	US$ 34,02	US$ 0,89	US$ 599,7
Custo[c]	US$ 269,41	US$ 0,73	US$ 0,11	US$ 18,97

[a] Valores de 28/04/2021 para a função `Join` com 64 roteadores cujo consumo é de 4.52M de gás
[b] Preço médio do dia, sendo 1 Gwei = 1 unidade de criptomoeda $\times 10^{-9}$
[c] Custo em gás $\times$ Preço do gás $\times$ Cotação

tada com um ciclo HARPIA mais longo que implica em uma redução do número de chamadas `Join`, `Leave` e `Settle` possíveis dentro de um intervalo de tempo. Essas são as funções que mais consomem gás no contrato inteligente do HARPIA pois dependem de uma biblioteca de curvas elípticas escrita em Solidity utilizada para implementar a verificação do MuSig *m*-de-*n*. Outra possibilidade de reduzir os custos na blockchain pública é o suporte a primitivas para aritmética de curvas elípticas na própria linguagem Solidity.

6.5 ANÁLISE DE AMEAÇAS DE SEGURANÇA

Esta seção descreve uma série de ameaças de segurança que podem afetar o HARPIA. A Tab. 20 resume as ameaças identificadas e lista as respectivas contramedidas. Em seguida, são explicadas as formas como cada ameaça é explorada e as contramedidas para evitá-las.

Tabela 20 – Resumo das ameaças e contramedidas.

Ameaça	**Contramedidas**
Gerenc. de chaves [1, 7, 11]	1 Processo de admissão para troca de chaves dos roteadores
DPIFA malicioso [1, 2, 4, 5, 8]	2 Depósito em criptomoeda para admissão de membros
Tráfego forjado [1, 3]	3 Autenticação do tráfego de rede entre os roteadores
STP malicioso [1, 4, 6, 9]	4 Detecção de inconsistências
Quorum do MuSig [4, 10]	5 Remoção de membros com inconsistências reiteradas
Ataques Sybil [1]	6 Recompensa para roteadores que executam função `Settle`
Ataques à blockchain [12]	7 HSM
	8 Autenticação ECDSA das mensagens DPIFA
	9 Autenticação MuSig da STP
	10 Desvalorização do *token* e remoção de roteadores com saldo abaixo do limite τ para eliminar membros inativos
	11 Esquema de multi-assinatura demonstravelmente seguro sob o modelo de chaves públicas simples
	12 (SAAD et al., 2020)

Gerenciamento de chaves

O HARPIA não necessita de uma PKI ou qualquer outro tipo de TTP. Em vez disso, as chaves públicas secp256k1 dos roteadores que são utilizadas para as assinaturas ECDSA e MuSig precisam ser registradas no contrato inteligente durante as operações `Join`. A própria transação da chamada da função `Join` requer uma multi-assinatura MuSig envolvendo no mínimo m dos n membros atuais da instância do HARPIA (ou uma assinatura ECDSA, no caso de existir um só membro). Essas assinaturas do `Join` dependem de um processo de admissão prévio do novo membro que é independente do HARPIA.

O processo de admissão pode envolver reuniões entre os membros para definir requisitos de conectividade e qualidade de serviço da rede. Os detalhes desse processo são dependentes dos vários contextos que o HARPIA pode ser aplicado e estão fora do escopo desta tese. Assume-se que o momento desse processo de admissão é oportuno para que o novo membro forneça sua chave pública para os membros atuais de forma segura.

Além disso, o esquema de multi-assinatura do MuSig é demonstravelmente seguro sob o modelo de chaves públicas simples (*provably secure under the plain public-key model*), o que significa que os novos membros não precisam provar que possuem a chave privada correspondente à chave pública fornecida, simplificando o processo de admissão. Quanto ao problema de roubo de chaves privadas, uma solução possível é a utilização de algum módulo de hardware seguro (HSM) para armazená-las.

Informações DPIFA maliciosas

Um roteador poderia disseminar informações incorretas na contabilização de tráfego de rede com o intuito de reduzir seus débitos e aumentar indevidamente seus créditos de criptomoeda correspondentes à sua utilização e cooperação no encaminhamento de dados da rede. O DPIFA possui mecanismos para detectar inconsistências desse tipo, dentro de certos limites, agregando as contabilizações de tráfego para verificar sua credibilidade, conforme explicado nas Seções 3.3 e 5.2.

Mesmo assim, um roteador atacante conseguiria fraudar a contabilização dentro dos limites de tolerância δ, ou seja, se para cada roteador n da instância do HARPIA a compensação resultante C_n da STP permanecer dentro do intervalo $C_n \pm \delta$. Do contrário, se a adulteração nas contabilizações resultar em compensações além da tolerância, a respectiva STP não conseguirá quorum suficiente no MuSig m-de-n para que seja efetivada.

A lógica de tolerar erros está no fato de que pequenas fraudes são indistinguíveis de contabilizações incorretas causadas por erros devido a falhas de hardware, interferências de rádio ou sobrecargas de rede. Portanto, concede-se o benefício da dúvida aos roteadores e tolera-se erros dentro dos limites. Assim como o PIFA, o DPIFA assume que a estratégia dominante dos roteadores será de reportar contabilizações corretas e que não haverá coalizão de roteadores pois, do contrário, a vizinhança abandonará o HARPIA assim que perceber inconsistências frequentes nas contabilizações. Esse pressuposto é mais forte para redes comunitárias, visto que essas são mais estáticas e a vizinhança não muda com frequência. Em redes *ad hoc* mais dinâmicas esse pressuposto pode se tornar inválido, pois um roteador malicioso pode se mover, realizar fraudes na contabilização, e abandonar a rede em seguida.

A exigência de um processo de admissão e de um depósito de criptomoeda para novos membros dificulta ataques desse tipo. O processo de admissão minimiza a entrada de membros maliciosos e possibilita identificar os responsáveis, permitindo que os demais membros cobrem por eventuais inconsistências diretamente. O depósito mínimo também serve como um incentivo para que esse membro atue de forma honesta, pois, do contrário, corre o risco de ter seu saldo liquidado e resgatado por algum outro roteador. Quando um responsável por um roteador considerar que um outro roteador apresenta incorformidades reiteradas e acima do nível tolerável, ele pode propor a remoção desse roteador para os demais membros da instância do HARPIA através de uma chamada da função `Leave`. Nesse caso, se conseguir co-signatários suficientes para o MuSig e completar a transação `Leave` esse roteador remove o roteador malicioso e recebe seu saldo remanescente.

Por último, as mensagens DPIFA são autenticadas com assinaturas ECDSA utilizando a chave privada Ethereum do roteador que a produz para prevenir mensagens falsas. Essa assinatura utiliza *timestamps* e *nonces* para prevenir ataques de replicação.

Tráfego forjado

Um roteador pode forjar o endereço de origem do tráfego (*spoofing*) com o intuito de fazer o roteador do próximo salto da rede acreditar que esse tráfego foi originado pela rede de um outro roteador. O objetivo dessa fraude seria enviar dados para um destino e contornar a contabilização de tráfego evitando o pagamento pelo serviço. Uma contramedida que pode ser aplicada para essa ameaça é a autenticação de tráfego de rede utilizando um esquema de chaves públicas com IPSEC (FRANKEL; KRISHNAN, 2011) ou Wireguard (WIREGUARD, 2019). Nesse caso, uma alternativa para eliminar a necessidade de confiança em TTP, é utilizar as mesmas chaves do Ethereum, quando possível, ou cadastrar as chaves necessárias no contrato inteligente durante o processo de admissão de membro.

STPs maliciosos

Assim como no DPIFA, assume-se que a maioria dos roteadores age honestamente na criação e validação de STPs. Não é do interesse dos roteadores criar STPs maliciosas com débitos e créditos incorretos pois eles desejam que suas STPs tenham a maior credibilidade possível para que sejam validadas pelos outros roteadores de forma que possam receber a recompensa pela execução da função `Settle`. Da mesma maneira, assume-se que os roteadores não vão interromper maliciosamente o processo de criação de STPs. Um roteador poderia agir assim para comprometer a instância do HARPIA criando STPs e adiando as operações de `Settle` indefinidamente. No entanto, é mais provável que o roteador crie a STP e execute a função `Settle` o mais rapidamente possível para que possa ser recompensado. Os roteadores que detectarem indícios de comportamento malicioso na criação de STPs ou atrasos na execução das chamadas `Settle` correspondentes podem denunciar inconsistências, conforme explicado na Seção 5.2.

A exigência de um processo de admissão para novos membros também minimiza STPs maliciosas da mesma maneira que os ataques com informações DPIFA maliciosas. Além disso, cada STP contém o resumo criptográfico do conteúdo do bloco Ethereum atual e a sua multi-assinatura MuSig também inclui *timestamps* e *nonces* para evitar ataques de replicação.

Quorum do MuSig

Há um risco do quorum do MuSig m-de-n não ser alcançado por vários motivos: particionamentos de rede por causa de enlaces comprometidos, roteadores desligados ou defeituosos, perda das chaves privadas, etc. Para reduzir esse risco, a função `Settle` remove da instância do HARPIA os roteadores que possuem um saldo de criptomoeda abaixo de um limiar pré-definido τ. Essa operação, em conjunto com o mecanismo de desvalorização do *token* HARPIA decorrente da criação de nova criptomoeda nas recompensas da STP, acaba desincentivando a manutenção de roteadores ociosos que poderiam comprometer o quorum do MuSig de uma STP. Além disso, roteadores que participam do MuSig de forma maliciosa, por exemplo,

participando apenas das primeiras rodadas, podem ser denunciados com indícios de inconsistência, podendo ser removidos da instância do HARPIA conforme explicado na Seção 5.2.

Ataques Sybil

Roteadores virtuais falsos poderiam ser criados e ingressar na instância do HARPIA produzindo contabilizações falsas e contando como voto para STPs fraudulentas no MuSig *m*-de-*n*. Esse problema está relacionado ao gerenciamento de identidade digital, ou seja, à vinculação dos proprietários dos roteadores a suas respectivas contas Ethereum. Uma solução é um método seguro para distribuição de chaves criptográficas que faça essa vinculação e impeça o ingresso de roteadores virtuais falsos na instância do HARPIA. A exigência de um processo de admissão para ingresso de novos roteadores, com a respectiva distribuição das chaves públicas é uma forma de evitar esse problema. Além disso, a entrada de novos roteadores exige o depósito mínimo ϕ, o que é mais um fator que limita a criação de identidades falsas.

Ataques à blockchain

Além das ameaças específicas do HARPIA apresentadas, também existem ameaças à própria blockchain que dá suporte aos contratos inteligentes. O artigo de Saad *et al.* (SAAD et al., 2020) detalha uma série de ataques que podem afetar a disponibilidade e a integridade da blockchain, comprometendo a confiabilidade das transações dos contratos inteligentes. No artigo, destacam-se os problemas relacionados a mineração egoísta, ataques de 51%, ataques ao DNS, DDoS, atraso no consenso, ramificações (*forks*) da blockchain (KIFFER; LEVIN; MISLOVE, 2017) e ataques à plataforma de contratos inteligentes. Os autores também detalham as contramedidas possíveis para cada ameaça e as classificam de acordo com sua efetividade.

6.6 DISCUSSÃO

A análise quantitativa desse capítulo permitiu estimar o desempenho e a escalabilidade da arquitetura proposta através dos cenários modelados. Foi possível verificar o impacto de cada parâmetro de configuração no desempenho do HARPIA. O tempo de ciclo do HARPIA é diretamente proporcional ao espaço de armazenamento consumido pelo DPIFA, e inversamente proporcional ao tráfego de rede produzido pelo MuSig e ao consumo de gás do contrato inteligente. O período do DPIFA é inversamente proporcional ao espaço de armazenamento consumido e ao tráfego de rede produzido pelo DPIFA. O número de combinações de chaves públicas agregadas do MuSig *m*-de-*n* é diretamente proporcional ao tempo de processamento para geração dessas chaves, ao espaço necessário para armazená-las junto com sua árvore de Merkle e ao consumo de gás das transações sendo assinadas com essa configuração de MuSig. O número de roteadores membro de uma instância do HARPIA é diretamente proporcional à comunicação necessária para o DPIFA e para outros componentes com menor custo de comu-

nicação. O número de signatários (entre m e n) de uma transação é diretamente proporcional aos custos de comunicação da multi-assinatura dessa transação na rede.

Os resultados obtivos mostraram o desempenho do HARPIA com até 64 roteadores de intraestrutura e limiares ζ específicos para o MuSig utilizando um computador de propósito geral. Os maiores gargalos identificados estão relacionados ao tempo de processamento e ao espaço de armazenamento necessário para as chaves públicas agregadas e a respectiva árvore de Merkle. As análises de escalabilidade mostraram que, devido à complexidade combinatorial das operações, seria inviável executar o MuSig para um número maior de roteadores com o hardware utilizado. Os requisitos de comunicação para redes com até 64 roteadores são relativamente baixos e não representam nenhum impedimento. Além disso, estabelecer um limite de 64 roteadores é aceitável pois esse número cobre grande parte de cenários reais, como no caso das redes comunitárias da Freifunk (FREIFUNK, 2021) que possuem 60% das redes com um número de roteadores de infraestrutura abaixo desse limite.

Em um cenário típico com as configurações $n = 32$ roteadores, $\beta \cdot \gamma = 1$ semana, $\lambda = 5$ minutos e $\zeta = 87.5\%$ ($m = 28$), o HARPIA requer 26,33 MB para o DPIFA (Eq. 6.3), 3.83 MB para o MuSig (Eq. 6.2). Além disso, o HARPIA requer espaço para o armazenamento da blockchain Ethereum que atualmente consome 462 GB utilizando o programa OpenEthereum e 875 GB utilizando o programa geth conforme ilustrado no gráfico da Fig. 37.

Uma forma de estender o número de roteadores possíveis em uma instância do HARPIA seria a utilização de outros esquemas de multi-assinatura que apresentem menor custo computacional e de armazenamento. Atualmente, os esquemas de multi-assinatura com limiar são uma área de pesquisa que vem evoluindo rapidamente, a exemplo do baseado em BLS (BONEH; DRIJVERS; NEVEN, 2018), do FROST (KOMLO; GOLDBERG, 2021) e do MuSig2 (NICK; RUFFING; SEURIN, 2021).

Supondo que os gargalos de escalabilidade para tempo de processamento e armazenamento sejam mitigados futuramente com algum esquema de multi-assinatura mais eficiente, a comunicação DPIFA se tornaria o novo gargalo do HARPIA para um número maior de roteadores. Nesse caso, a comunicação todos para todos sem o suporte de protocolos de difusão de mensagens mais eficientes poderia sobrecarregar os entroncamentos da rede dependendo da sua topologia. O problema se agravaria considerando que se trata de uma rede incentivada com criptomoeda, ou seja, na qual o tráfego de rede é cobrado.

Uma alternativa para redução do tráfego produzido seria a utilização de protocolos multicast de rede (RATNASAMY; ERMOLINSKIY; SHENKER, 2006) para a difusão de mensagens sem a necessidade de sua replicação nos enlaces. Porém, tais protocolos são difíceis de serem implantados, sobretudo em redes comunitárias, nas quais a heterogeneidade da capacitação técnica entre os responsáveis pelos roteadores é um fator significativo. Outra solução é a utilização de protocolos de disseminação de mensagens baseados em técnicas de P2P para implementação de multicast em nível de aplicação (ALM) (HOSSEINI et al., 2007). Nesse caso, algoritmos de P2P que estabelecem conexões entre os membros considerando a topologia física da rede poderiam se aproximar da eficiência de protocolos multicast de nível de rede.

A abordagem apresentada para o DPIFA para recuperação de mensagens na presença de falhas de roteadores e dos seus enlaces é bastante simples. Consiste apenas na requisição de retransmissão de informações de contabilização faltantes. Existem muitos estudos sobre mecanismos de difusão confiável (RUIZ; BOUVRY, 2015) que podem ser investigados com o objetivo de otimizar e melhorar a confiabilidade da disseminação das mensagens. No entanto, essa investigação será deixada para trabalhos futuros.

Em ambos os casos (multicast e difusão confiável) como o HARPIA já realiza a associação dos membros, os protocolos de descoberta e de associação de grupo são um sobrecusto desnecessário. A utilização de ALMs ou protocolos de difusão confiável próprios que aproveitem a lista de membros do contrato inteligente para construir os caminhos de disseminação das mensagens possibilitaria alcançar um bom compromisso entre a simplicidade de implantação e eficiência de disseminação de mensagens.

Os custos com o contrato inteligente dependem da frequência das transações, principalmente das funções `Join`, `Leave` e `Settle`, além do preço do gás e da cotação da criptomoeda da blockchain utilizada. Foram analisados os custos atuais com duas blockchains públicas Ethereum que suportam contratos inteligentes Solidity. A Ethereum Mainnet apresentou custos consideravelmente altos, mas a Ethereum Classic teve custos bastante reduzidos. Também foi analisado o custo em duas blockchains com consenso PoS: a Polygon e a BSC, que apresentaram custo relativamente baixo se comparado com o custo nas blockchains Ethereum. A escolha da blockchain deve considerar um compromisso entre a confiabilidade da blockchain, o orçamento disponível para os membros da rede e a frequência das transações do contrato inteligente. A frequência das transações pode ser reduzida aumentando o tempo mínimo de ciclo do HARPIA. Além disso, outra possibilidade de reduzir esses custos é o suporte a primitivas para aritmética de curvas elípticas na linguagem Solidity. Atualmente é necessário implementar essas operações na própria linguagem.

A análise qualitativa apresentou as ameaças de segurança identificadas durante a modelagem do HARPIA. As contramedidas para essas ameaças contam com as propriedades dos esquemas de criptografia para assinaturas ECDSA e MuSig, a blockchain que dá suporte aos contratos inteligentes, contabilizações de inconsistências, processos de admissão de membros, mecanismos para remoção de membros maliciosos ou inativos, autenticação de tráfego de rede e armazenamento seguro das chaves privadas. Além disso, o HARPIA implementa incentivos para que os roteadores ajam de maneira cooperativa e para que apliquem sanções de forma interativa a roteadores que apresentam erros. As sanções não podem ser automáticas e requerem interação dos responsáveis pelos roteadores devido à dificuldade de distinguir erros não intencionais de erros causados por ação maliciosa. A análise de ameaças ainda requer maior aprofundamento e formalização do modelo que serão tratados em trabalhos futuros.

7 CONCLUSÃO

Atualmente, a divisão digital é um problema que acentua as desigualdades socioeconômicas. Redes comunitárias são uma alternativa para mitigar esse problema preenchendo as lacunas de falhas de mercado e de políticas públicas através do trabalho cooperativo em comunidade para implantação de infraestrutura de rede em locais com acesso à Internet caro ou deficiente. No entanto, tais redes ainda são suscetíveis ao problema do caroneiro (*free rider*) que consiste em participantes com comportamento egoísta que não contribuem com o funcionamento da rede na mesma medida que utilizam o serviço. Tal problema pode afetar a dependabilidade das redes comunitárias, assim como de outros tipos de rede (D2D e VANET), por isso foram desenvolvidos mecanismos de incentivo para estimular a cooperação entre os participantes da rede. Os mecanismos de incentivo elaborados com técnicas de blockchains foram detalhadamente investigados nessa tese com o propósito de responder à seguinte pergunta de pesquisa:

> *É possível implementar incentivos ao encaminhamento de pacotes em redes cooperativas de forma descentralizada?*

O Cap. 4 detalhou como as blockchains são utilizadas para essa finalidade, apresentando as estratégias e os desafios existentes no estado da arte. A partir das lacunas identificadas, foi assumido como objetivo geral:

> *Verificar se a utilização de blockchains pode servir para a elaboração de mecanismos de incentivo ao encaminhamento de dados em redes cooperativas sem depender de TTP e sem custos proibitivos.*

A partir desse objetivo geral, foram delineados objetivos específicos que foram cumpridos conforme descrito nas próximas seções.

OBJETIVO 1: A CONCEPÇÃO DE UMA ARQUITETURA DE SISTEMA QUE PROPORCIONE INCENTIVOS AO ENCAMINHAMENTO DE DADOS UTILIZANDO BLOCKCHAINS SEM A NECESSIDADE DE TTP OU CUSTOS PROIBITIVOS NAS BLOCKCHAINS

No Cap. 5, foi apresentada a arquitetura de sistema que foi concebida a partir das ideias de mecanismos de incentivo encontrados na literatura com o objetivo de eliminar as principais limitações identificadas no estado da arte. A arquitetura se chama HARPIA (*Hop-by-hop Accounting and Rewards for Packet dIspAtching*) e apresenta as duas propriedades buscadas no objetivo 1: independência de TTP e custos moderados na blockchain. Para alcançar essas propriedades, o HARPIA se baseia na contabilização distribuída do tráfego de rede com compensação periódica dos débitos e créditos em criptomoeda correspondentes ao serviço de encaminhamento de dados pelos roteadores da infraestrutura de rede. Para isso, implementa

um mecanismo de incentivo baseado em crédito que utiliza uma versão distribuída do PIFA chamada DPIFA, e contratos inteligentes Solidity cujas transações são assinadas utilizando um esquema de multi-assinaturas com limiar *m*-de-*n* chamado MuSig.

OBJETIVO 2: UMA AVALIAÇÃO QUANTITATIVA E QUALITATIVA DA ARQUITETURA CONCEBIDA PARA ESTIMAR SEU DESEMPENHO, ESCALABILIDADE, CUSTOS COM BLOCKCHAINS E IDENTIFICAR AS AMEAÇAS DE SEGURANÇA

A análise quantitativa dos componentes do HARPIA, apresentada no Cap. 6, permitiu avaliar suas limitações e verificar sua aplicabilidade em redes cooperativas. A análise qualitativa realizada consiste em uma análise de ameaças preliminar. As etapas iniciais do seu processo de elaboração possibilitaram identificar fraquezas na arquitetura proposta cujas soluções já estão incorporadas no Cap. 5.

De acordo com as análises quantitativas, a arquitetura proposta é adequada para redes comunitárias com até 64 roteadores com hardware equivalente ao da plataforma descrita para os cenários modelados. As configurações da plataforma de análise são de um computador pessoal de mercado atual e o desempenho dos componentes analisados ainda pode ser consideravelmente otimizado com hardware dedicado, paralelização do software e avanços nas tecnologias dos processadores. A limitação de número de roteadores leva em consideração o custo computacional da geração das chaves públicas agregadas do MuSig *m*-de-*n* e da respectiva árvore de Merkle cujo tempo de processamento segue uma complexidade combinatorial. Considerando a grande quantidade de redes comunitárias que possuem menos de 64 roteadores (ex: 60% das redes Freifunk), o HARPIA pode ser aplicado nesses cenários. Há também a possibilidade de surgirem novos esquemas de multi-assinatura com limiar *m*-de-*n* sem as limitações de processamento e armazenamento apresentadas pelo MuSig. Nesse caso, o gargalo de escalabilidade do sistema passaria a ser na comunicação.

Em um cenário com 32 roteadores, com tempo mínimo de ciclo de 1 semana, período de 5 minutos, limiar do MuSig $\zeta = 87,5\%$ e número médio de vizinhos na rede igual a quatro, o HARPIA requer 26 MB para o DPIFA, 3,83 MB para o MuSig e 462 GB para a blockchain do Ethereum (Mainnet). Para o processamento, leva em média 1547 s para produzir as chaves públicas agregadas para o esquema do MuSig *m*-de-*n*. O maior sobrecusto de comunicação do sistema é causado pela própria sincronização P2P do arquivo da blockchain que requer 144 Kbps de tráfego por roteador. O sobrecusto de comunicação entre os componentes próprios do HARPIA é insignificante em cenários com até 64 membros. O componente DPIFA, maior produtor de mensagens, produziu um tráfego médio de até 79,8 bps por roteador e apresentou uma latência máxima de 5,76 ms para a entrega das mensagens nos cenários simulados com o OMNet++.

As operações de compensação de créditos e débitos que são executadas a cada ciclo do HARPIA através de transações com a função `Settle` na blockchain pública resultam em custos muito menores que outros sistemas do estado da arte que são independentes de TTP (SKJEGS-

TAD; MADHAVAPEDDY; CROWCROFT, 2015) (HE et al., 2018). Esses sistemas exigem várias transações na blockchain para cada pacote de dados transmitido e para cada salto de roteamento na rede, tornando seus mecanismos de incentivo economicamente inviáveis para serem aplicados em redes comunitárias atualmente. Além disso, no caso do HARPIA, o tempo mínimo de ciclo pode ser estendido para reduzir o número de transações até se adequar ao orçamento dos membros da rede comunitária.

A análise do consumo de gás do contrato inteligente Solidity em blockchains públicas mostrou que uma transação com verificação MuSig (`Join`, `Leave` ou `Settle`) consome até 4,52 M unidades de gás. Isso equivale a um valor de US$ 269,00 na Ethereum Mainnet, US$ 0,73 na Ethereum Classic. Também foram analisadas outras blockchains com consenso PoS que suportam contratos inteligentes Solidity. Os valores obtidos foram US$ 0,11 na Polygon e US$ 18,97 na BSC. Esses valores correspondem à cotação das criptomoedas em 28 de abril de 2021 e são custos considerados viáveis para redes comunitárias nessa data.

É importante ressaltar que blockchains públicas apresentam alta volatilidade no preço de mercado das suas criptomoedas e do gás necessário para a execução de funções dos contratos inteligentes. Os valores calculados hoje podem ser muito diferentes dentro de pouco tempo. Isso deve ser considerado ao utilizar o HARPIA. Assim, os participantes devem depositar valores em criptomoeda suficientes para os pagamentos pelo encaminhamento de pacotes, mas não utilizar o contrato inteligente como meio de armazenamento de valores, pois esses tendem a se desvalorizar com o tempo. Além disso, a escolha da plataforma de blockchain deve considerar um compromisso entre a confiabilidade da blockchain, o orçamento disponível para os membros da rede comunitária e a frequência das transações do contrato inteligente.

Na análise qualitativa, foram apresentadas contramedidas para as ameaças de segurança identificadas durante a concepção da arquitetura de sistema. As contramedidas contam com as propriedades dos esquemas de criptografia para assinaturas ECDSA e MuSig, a blockchain que dá suporte aos contratos inteligentes, contabilizações de inconsistências, processos de admissão de membros, mecanismos para remoção de membros maliciosos ou inativos, autenticação de tráfego de rede e armazenamento seguro das chaves privadas. Além disso, a arquitetura implementa incentivos para que os roteadores ajam de maneira cooperativa e para que apliquem sanções de forma interativa a roteadores que apresentam erros.

7.1 TRABALHOS FUTUROS

Para continuidade do trabalho apresentado aqui existe uma série de questões em aberto a serem investigadas. Os trabalhos futuros tem relação com: técnicas dos trabalhos relacionados e do estado da arte que não foram exploradas; limitações identificadas na proposta de arquitetura de sistema apresentada; limitações do esquema de multi-assinatura adotado; continuidade do modelo de ameaças iniciado.

Quanto ao primeiro item, existe a possibilidade de explorar as soluções de escalabilidade das blockchains (*childchains* e canais) para reduzir os custos envolvidos em escritas

nas blockchains públicas para os mecanismos de incentivo. Além disso, parte da lógica do HARPIA, como a matriz de inconsistências, poderia ser realizada em contratos inteligentes de camada 2 com *childchains*. Nesse caso, cada *childchain* poderia ser uma blockchain privada vinculada à rede cooperativa local e com protocolo de consenso próprio.

Os componentes do HARPIA poderiam ser modelados como módulos de função, no contexto de NFV. A vantagem seria a flexibilidade de provisionamento e alocação mais racional dos recursos com adaptação da capacidade de acordo com os requisitos da rede do HARPIA. Nesse caso, existe a restrição de que os módulos sejam de propriedade do mesmo responsável, dentro de um mesmo domínio administrativo, ou que exista uma relação de confiança estabelecida com o responsável por esse módulo. Assim, a plataforma que executa componentes como o DPIFA, a blockchain Ethereum ou o gerenciamento de chaves do MuSig poderiam escalar dinamicamente sua capacidade conforme a demanda. A modularização com NFV também eliminaria o risco do processamento de tarefas mais onerosas comprometer a capacidade de encaminhamento de tráfego dos roteadores.

Quanto às limitações do HARPIA, primeiramente, deseja-se realizar experimentos adicionais que permitam representar de maneira fidedigna o comportamento dos participantes de um ambiente real. O primeiro passo nesse sentido foi a modelagem de cenários no OMNet++ com base em redes comunitárias reais, como a GUIFI.net. Deseja-se, com isso, além de avaliar melhor o HARPIA, também caracterizar as limitações que se supõe existir e as respectivas oportunidades de melhoria. Também pretende-se dar continuidade a projetos de redes comunitárias que foram iniciados e tiveram que ser suspensos devido a dificuldades impostas pela pandemia da COVID-19. Essas redes comunitárias podem servir como plataformas para validação da arquitetura de sistema em um ambiente real.

Entre os experimentos almejados estão incluídas simulações de participantes com comportamento egoísta e malicioso. Isso permitirá avançar na compreensão de potenciais limitações com relação às topologias mínimas de rede nas quais o HARPIA pode funcionar. A lógica dessas topologias mínimas está no fato que o monitoramento do DPIFA só poderia funcionar com um mínimo de evidências de tráfego, produzidas a partir de pontos estratégicos da rede e geradas por participantes que podem também ter comportamento egoísta ou malicioso.

Outra questão em aberto é o funcionamento da matriz de inconsistências, que foi modelada como uma extensão do sistema de monitoramento. A decisão por modelar dessa forma, parte do princípio que os indícios de inconsistência podem ser produzidos também por participantes maliciosos, portanto, não seria adequado desencadear sanções automatizadas sem a anuência dos participantes. Assim, seria importante compreender melhor até que ponto a matriz de inconsistências serviria como subsídio para os participantes na determinação de participantes egoístas e maliciosos na rede. Para essa investigação das topologias mínimas e da matriz de inconsistências pode também ser necessário resgatar outros estudos sobre teoria dos grafos, teoria dos jogos, sistemas multigentes e sistemas distribuídos que auxiliem na compreensão dessas limitações.

Considerando a possibilidade de surgirem novos esquemas de multi-assinatura sem

as limitações existentes no MuSig, que permitiriam a aplicação do HARPIA em cenários com mais de 64 roteadores, uma característica que poderia ser otimizada é a comunicação do DPIFA. Uma alternativa seria implementar algum mecanismo de difusão de mensagens como multicast de aplicação. Dessa forma, seria reduzida significativamente a sobrecarga nos entroncamentos da rede comunitária na comunicação que é necessária para disseminar as mensagens de contabilização DPIFA. Um multicast de aplicação é mais adequado para esse cenário do que multicast de rede porque esse último é complexo de ser implementado em redes comunitárias cuja mão de obra técnica costuma ser mais heterogênea e menos especializada.

A forma como o DPIFA recupera mensagens na presença de falhas de roteadores e dos seus enlaces é bastante simples. Consiste apenas na requisição de retransmissão de informações de contabilização perdidas. Existem muitos estudos sobre mecanismos de difusão confiável que podem ser investigados futuramente com o objetivo de otimizar e melhorar a confiabilidade da disseminação dessas mensagens. Tanto a difusão confiável como o multicast de aplicação poderiam também utilizar as informações dos membros associados e as informações dos enlaces de rede cadastrados no contrato inteligente para eliminar a necessidade de gerência de associação de membros e para determinar os melhores caminhos para difusão das mensagens.

O esquema de multi-assinatura com limiar utilizado (MuSig) é o componente que produz o maior custo computacional do HARPIA. Avanços recentes nesses esquemas sugerem a possibilidade de reduzir esse custo, por isso, planeja-se avaliar esquemas como os baseados em BLS, o FROST e o MuSig2.

Além da escolha de blockchains com tarifas de gás menores, existem outras possibilidades de redução de custos na blockchain a serem estudadas. Uma delas é a utilização de outros esquemas de multi-assinatura com limiar mais eficientes, que consumam menos gás na verificação da assinatura realizada no contrato inteligente. Outra possibilidade é a incorporação de primitivas criptográficas (ex: aritmética de curvas elípticas) na linguagem Solidity em vez de sua implementação como uma biblioteca escrita na própria linguagem.

Por último, também deseja-se formalizar o modelo de ameaças iniciado e torná-lo mais abrangente. Espera-se que as simulações modeladas e os cenários reais implantados futuramente permitam caracterizar melhor as ameaças de forma que seja possível uma identificação mais rigorosa dos riscos envolvidos e das respectivas contramedidas.

REFERÊNCIAS

ADAMUZ-HINOJOSA, O. et al. Automated Network Service Scaling in NFV: Concepts, Mechanisms and Scaling Workflow. **IEEE Communications Magazine**, IEEE, v. 56, n. 7, p. 162–169, jul. 2018. ISSN 1558-1896.

AKYILDIZ, I.; WANG, X. **Wireless Mesh Networks**. 1. ed. Chichester, UK: John Wiley & Sons, 2009. (Advanced Texts in Communications and Networking). ISBN 978-0470032565.

ALTERMUNDI. **AlterMundi**. 2021. Disponível em: https://altermundi.net/. Acesso em: 14 de Agosto de 2021.

AMMBR Foundation. **AMMBR white paper v1**. 2017. Disponível em: https://web.archive.org/web/20181008145101/http://ammbr.com/docs/201708/Ammbr_Whitepaper_v1.1_15Aug2017.pdf. Acesso em: 20 de Fevereiro de 2021.

AMMBR Foundation. **AMMBR white paper v2**. 2018. Disponível em: https://web.archive.org/web/20210113063916/https://ammbr.com/docs/2018/11/Ammbr_Whitepaper.pdf. Acesso em: 20 de Fevereiro de 2021.

ANDONI, M. et al. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. **Renewable and Sustainable Energy Reviews**, v. 100, p. 143 – 174, 2019. ISSN 1364-0321.

ANDRESEN, G. **BIP 11: M-of-N Standard Transactions**. 2011. Disponível em: https://github.com/bitcoin/bips/blob/master/bip-0011.mediawiki. Acesso em: 20 de Fevereiro de 2020.

ANGELIS, S. D. et al. PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain. In: **Italian Conference on Cyber Security**. Milan, Italy: University of Southampton Institutional Repository, 2018. p. 1–11. Disponível em: https://eprints.soton.ac.uk/415083/.

AOSP ISSUE 36904180. **Support Wi-Fi ad hoc networking**. 2015. Disponível em: https://issuetracker.google.com/issues/36904180. Acesso em: 19 de Fevereiro de 2020.

ASGHARI, H. et al. Security economics in the HTTPS value chain. In: **Twelfth Workshop on the Economics of Information Security (WEIS 2013)**. Washington, EUA: SSRN, 2013. p. 1–36. Disponível em: https://ssrn.com/abstract=2277806.

AVIZIENIS, A. et al. Basic concepts and taxonomy of dependable and secure computing. **IEEE Transactions on Dependable and Secure Computing**, v. 1, n. 1, p. 11–33, jan. 2004. ISSN 1545-5971.

AYAZ, F. et al. A Voting Blockchain based Message Dissemination in Vehicular Ad-Hoc Networks (VANETs). In: **ICC 2020 - 2020 IEEE International Conference on Communications (ICC)**. Dublin, Ireland: IEEE, 2020. p. 1–6. ISBN 978-17281-5089-5a.

BAGHERZANDI, A.; CHEON, J.-H.; JARECKI, S. Multisignatures secure under the discrete logarithm assumption and a generalized forking lemma. In: **Proceedings of the 15th ACM Conference on Computer and Communications Security**. Nova Iorque, EUA: Association for Computing Machinery, 2008. (CCS '08), p. 449–458. ISBN 9781595938107.

BAGHERZANDI, A.; JARECKI, S. Multisignatures Using Proofs of Secret Key Possession, as Secure as the Diffie-Hellman Problem. In: OSTROVSKY, R.; PRISCO, R. D.; VISCONTI, I. (Ed.). **Security and Cryptography for Networks**. Berlin, Heidelberg: Springer, 2008. p. 218–235. ISBN 978-3-540-85855-3.

BAIG, R. et al. guifi.net, a crowdsourced network infrastructure held in common. **Computer Networks**, Elsevier, v. 90, p. 150–165, jul. 2015. ISSN 1389-1286.

BANCO MUNDIAL. **Relatório sobre o Desenvolvimento Mundial de 2016 – DIVIDENDOS DIGITAIS**. Washington, EUA: The World Bank, 2016. v. 1. ISBN 978-1-4648-0671-1.

BANSARKHANI, R. E.; STURM, J. An Efficient Lattice-Based Multisignature Scheme with Applications to Bitcoins. In: FORESTI, S.; PERSIANO, G. (Ed.). **Cryptology and Network Security**. Cham: Springer, 2016. p. 140–155. ISBN 978-3-319-48965-0.

BAUMGÄRTNER, L. et al. An experimental evaluation of delay-tolerant networking with serval. In: **2016 IEEE Global Humanitarian Technology Conference (GHTC)**. Seatle, EUA: IEEE, 2016. p. 70–79.

BELLARE, M.; NAMPREMPRE, C.; NEVEN, G. Unrestricted Aggregate Signatures. In: ARGE, L. et al. (Ed.). **Automata, Languages and Programming**. Berlin, Heidelberg: Springer, 2007. p. 411–422. ISBN 978-3-540-73420-8.

BELLARE, M.; NEVEN, G. Multi-signatures in the plain public-key model and a general forking lemma. In: **Proceedings of the 13th ACM Conference on Computer and Communications Security**. Nova Iorque, EUA: Association for Computing Machinery, 2006. (CCS '06), p. 390–399. ISBN 1595935185.

BENET, J.; GRECO, N. **Filecoin: A decentralized storage network**. 2017. 1–36 p. Disponível em: https://filecoin.io/filecoin.pdf. Acesso em: 02 de Setembro de 2020.

BINANCE. **Binance Smart Chain/**. 2021. Disponível em: https://docs.binance.org/. Acesso em: 02 de Maio de 2021.

BOGLIOLO, A. et al. Virtual currency and reputation-based cooperation incentives in user-centric networks. In: **2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC)**. Limassol, Cyprus: IEEE, 2012. p. 895–900. ISBN 978-1-4577-1379-8.

BOLDYREVA, A. Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme. In: DESMEDT, Y. G. (Ed.). **Public Key Cryptography — PKC 2003**. Berlin, Heidelberg: Springer, 2002. p. 31–46. ISBN 978-3-540-36288-3.

BOLDYREVA, A. et al. Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing. In: **Proceedings of the 14th ACM Conference on Computer and Communications Security**. Nova Iorque, EUA: Association for Computing Machinery, 2007. (CCS '07), p. 276–285. ISBN 9781595937032.

BONEH, D.; DRIJVERS, M.; NEVEN, G. Compact Multi-signatures for Smaller Blockchains. In: PEYRIN, T.; GALBRAITH, S. (Ed.). **Advances in Cryptology – ASIACRYPT 2018**. Cham: Springer, 2018. p. 435–464. ISBN 978-3-030-03329-3.

BONEH, D. et al. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In: BIHAM, E. (Ed.). **Advances in Cryptology — EUROCRYPT 2003**. Berlin, Heidelberg: Springer, 2003. (LNCS, v. 2656), p. 416–432. ISBN 978-3-540-39200-2.

Brainbot Labs. **μRaiden**. 2018. Disponível em: https://microraiden.readthedocs.io/. Acesso em: 05 de Abril de 2020.

BSCSCAN. **BscScan**. 2021. Disponível em: https://bscscan.com/. Acesso em: 20 de Junho de 2021.

BUCHEGGER, S.; BOUDEC, J.-Y. L. Performance Analysis of the CONFIDANT Protocol. In: **Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing**. Nova Iorque, EUA: ACM, 2002. (MobiHoc '02), p. 226–236. ISBN 1-58113-501-7.

BURMESTER, M. et al. A Structured ElGamal-Type Multisignature Scheme. In: IMAI, H.; ZHENG, Y. (Ed.). **Public Key Cryptography**. Berlin, Heidelberg: Springer, 2000. p. 466–483. ISBN 978-3-540-46588-1.

CAREEM, M. A. A.; DUTTA, A. Reputation based Routing in MANET using Blockchain. In: **2020 International Conference on COMmunication Systems NETworkS (COMSNETS)**. Bengaluru, India: IEEE, 2020. p. 1–6. ISBN 978-1-7281-3187-0.

CASTELLUCCIA, C. et al. A Robust Multisignature Scheme with Applications to Acknowledgement Aggregation. In: BLUNDO, C.; CIMATO, S. (Ed.). **Security in Communication Networks**. Berlin, Heidelberg: Springer, 2005. p. 193–207. ISBN 978-3-540-30598-9.

CASTRO, I. et al. Route Bazaar: Automatic Interdomain Contract Negotiation. In: **15th Workshop on Hot Topics in Operating Systems (HotOS XV)**. Kartause Ittingen, Switzerland: USENIX Association, 2015. p. 1–7.

CERDÀ-ALABERN, L.; BAIG, R.; NAVARRO, L. On the Guifi.net community network economics. **Computer Networks**, Elsevier, v. 168, p. 107067, 2020. ISSN 1389-1286.

CERF, V.; KAHN, R. A Protocol for Packet Network Intercommunication. **IEEE Transactions on Communications**, IEEE, v. 22, n. 5, p. 637–648, 1974. ISSN 0090-6778.

CHAKERES, I. D.; BELDING-ROYER, E. M. AODV routing protocol implementation design. In: **24th International Conference on Distributed Computing Systems Workshops, 2004. Proceedings.** Tokyo, Japan: IEEE, 2004. p. 698–703. ISBN 0-7695-2087-1.

CHAKRABARTI, C.; BASU, S. A Blockchain Based Incentive Scheme for Post Disaster Opportunistic Communication over DTN. In: **Proceedings of the 20th International Conference on Distributed Computing and Networking**. Nova Iorque, EUA: Association for Computing Machinery, 2019. (ICDCN '19), p. 385–388. ISBN 9781450360944.

CHANG, C. C. et al. A scheme for obtaining a message from the digital multisignature. In: IMAI, H.; ZHENG, Y. (Ed.). **Public Key Cryptography**. Berlin, Heidelberg: Springer, 1998. p. 154–163. ISBN 978-3-540-69105-1.

CHARILAS, D. E.; GEORGILAKIS, K. D.; PANAGOPOULOS, A. D. Icarus: hybrid incentive mechanism for cooperation stimulation in ad hoc networks. **Ad Hoc Networks**, v. 10, n. 6, p. 976–989, 2012. ISSN 1570-8705.

CHAUDHARY, R. et al. BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system. **Computers & Security**, v. 85, p. 288–299, 2019. ISSN 0167-4048.

CHEN, C. et al. A Secure and Efficient Blockchain-Based Data Trading Approach for Internet of Vehicles. **IEEE Transactions on Vehicular Technology**, IEEE, v. 68, n. 9, p. 9110–9121, 2019. ISSN 0018-9545.

CHEN, D. et al. PayFlow: Micropayments for Bandwidth Reservations in Software Defined Networks. In: **IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)**. Paris, França: IEEE, 2019. p. 26–31. ISBN 978-1-7281-1878-9.

CHEN, L. et al. On Security Analysis of Proof-of-Elapsed-Time (PoET). In: SPIRAKIS, P.; TSIGAS, P. (Ed.). **Stabilization, Safety, and Security of Distributed Systems**. Cham: Springer, 2017. p. 282–297. ISBN 978-3-319-69084-1.

CHROBOCZEK, J. **The Babel Routing Protocol**. [S.l.]: RFC Editor, 2011. 1–45 p. Internet Requests for Comments. Disponível em: https://tools.ietf.org/html/rfc6126. (Request for Comments, 6126).

COVENTRY, A. **NooShare: A decentralized ledger of shared computational resources**. 2012. Disponível em: http://web.mit.edu/alexc/www/nooshare.pdf. Acesso em: 19 de Outubro de 2019.

CUNHA, F. D. D. et al. Data Communication in VANETs: Protocols, Applications and Challenges. **Ad Hoc Networks**, Elsevier, v. 44, n. C, p. 90–103, dez. 2016. ISSN 15708705.

DAHLBERG, R.; PULLS, T.; PEETERS, R. Efficient sparse merkle trees. In: BRUMLEY, B. B.; RÖNING, J. (Ed.). **Secure IT Systems**. Cham: Springer, 2016. p. 199–215. ISBN 978-3-319-47560-8.

DAI, W. et al. SDTE: A Secure Blockchain-Based Data Trading Ecosystem. **IEEE Transactions on Information Forensics and Security**, IEEE, v. 15, p. 725–737, 2020. ISSN 1556-6013.

DAVID, B.; DOWSLEY, R.; LARANGEIRA, M. MARS: Monetized Ad-hoc Routing System (A Position Paper). In: **Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems**. Nova Iorque, EUA: ACM, 2018. (CryBlock'18), p. 82–86. ISBN 978-1-4503-5838-5.

DE FILIPPI, P.; MANNAN, M.; REIJERS, W. Blockchain as a confidence machine: The problem of trust & challenges of governance. **Technology in Society**, Elsevier, v. 62, p. 101284, ago. 2020. ISSN 0160-791X.

DECKER, C.; RUSSELL, R.; OSUNTOKUN, O. **eltoo: A simple layer 2 protocol for bitcoin**. 2018. Disponível em: https://blockstream.com/eltoo.pdf. Acesso em: 05 de Abril de 2020.

DHILLON, V.; METCALF, D.; HOOPER, M. The DAO Hacked. In: **Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You**. Berkeley, EUA: Apress, 2017. cap. 6, p. 67–78. ISBN 978-1-4842-3081-7.

DIMOGERONTAKIS, E. et al. Meshdapp – blockchain-enabled sustainable business models for networks. In: DJEMAME, K. et al. (Ed.). **Economics of Grids, Clouds, Systems, and Services - GECON 2019**. Cham: Springer, 2019. v. 11819, p. 286–290. ISBN 978-3-030-36027-6.

DOAN, T. V. et al. Measuring Decentralized Video Streaming: A Case Study of DTube. In: **2020 IFIP Networking Conference (Networking)**. Paris, França: IEEE, 2020. p. 118–126. ISBN 978-3-903176-28-7.

DOURLENS, J. **Understand the ERC-20 token smart contract**. 2020. Disponível em: https://ethereum.org/en/developers/tutorials/understand-the-erc-20-token-smart-contract/. Acesso em: 22 de Junho de 2021.

DRIJVERS, M. et al. Pixel: Multi-signatures for consensus. In: **29th USENIX Security Symposium (USENIX Security 20)**. Virtual Conference: USENIX Association, 2020. p. 2093–2110. ISBN 978-1-939133-17-5.

DZIEMBOWSKI, S.; FAUST, S.; HOSTÁKOVÁ, K. General State Channel Networks. In: **Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security**. Nova Iorque, EUA: Association for Computing Machinery, 2018. (CCS '18), p. 949–966. ISBN 9781450356930.

EASTLAKE, D.; HANSEN, T. **US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)**. [S.l.]: RFC Editor, 2011. 1–126 p. Internet Requests for Comments. Disponível em: https://tools.ietf.org/html/rfc6234. (Request for Comments, 6234).

EFSTATHIOU, E. C.; FRANGOUDIS, P. A.; POLYZOS, G. C. Stimulating Participation in Wireless Community Networks. In: **Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications**. [S.l.]: IEEE, 2006. p. 1–13. ISSN 0743-166X.

ERNST, J. et al. **The Power of Connectivity in the Hands of the People – Decentralized Mobile Mesh Networking Platform Powered by Blockchain Technology and Tokenization**. 2019. Disponível em: https://www.rightmesh.io/whitepapers. Acesso em: 20 de Fevereiro de 2021.

EYAL, I. et al. Bitcoin-NG: A Scalable Blockchain Protocol. In: **Proceedings of the 13th Usenix Conference on Networked Systems Design and Implementation**. Santa Clara, EUA: USENIX Association, 2016. (NSDI'16), p. 45–59. ISBN 978-1-931971-29-4.

FARINACCI, D. et al. **Generic Routing Encapsulation (GRE)**. [S.l.]: RFC Editor, 2000. 1–9 p. Internet Requests for Comments. Disponível em: https://tools.ietf.org/html/rfc2784. (Request for Comments, 2784).

FEIGE, U.; FIAT, A.; SHAMIR, A. Zero-knowledge proofs of identity. **Journal of Cryptology**, Springer, v. 1, n. 2, p. 77–94, jun. 1988. ISSN 1432-1378.

FELDMAN, M. et al. Free-riding and whitewashing in peer-to-peer systems. **IEEE Journal on Selected Areas in Communications**, IEEE, v. 24, n. 5, p. 1010–1019, maio 2006. ISSN 1558-0008.

FELEGYHAZI, M.; HUBAUX, J.-P.; BUTTYAN, L. Nash equilibria of packet forwarding strategies in wireless ad hoc networks. **IEEE Transactions on Mobile Computing**, IEEE, v. 5, n. 5, p. 463–476, maio 2006. ISSN 1536-1233.

FENG, Z.; LUO, Q. Evaluating memory-hard proof-of-work algorithms on three processors. **Proc. VLDB Endow.**, VLDB Endowment, v. 13, n. 6, p. 898–911, fev. 2020. ISSN 2150-8097.

FRANKEL, S.; KRISHNAN, S. **IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap**. [S.l.]: RFC Editor, 2011. 1–63 p. Internet Requests for Comments. Disponível em: https://tools.ietf.org/html/rfc6071. (Request for Comments, 6071).

FREIFUNK. **Lista de redes da Freifunk**. 2021. Disponível em: https://freifunk.net/. Acesso em: 30 de Maio de 2021.

GARDNER, S. P. **Serval Project**. 2021. Disponível em: http://servalproject.org. Acesso em: 30 de Maio de 2021.

GOKA, S.; SHIGENO, H. Distributed management system for trust and reward in mobile ad hoc networks. In: **2018 15th IEEE Annual Consumer Communications Networking Conference (CCNC)**. Las Vegas, EUA: IEEE, 2018. p. 1–6. ISBN 978-1-5386-4790-5. ISSN 2331-9860.

GOODMAN, J. T.; ROUNTHWAITE, R. Stopping outgoing spam. In: **Proceedings of the 5th ACM Conference on Electronic Commerce**. Nova Iorque, EUA: Association for Computing Machinery, 2004. (EC '04), p. 30–39. ISBN 1581137710.

GRAMOLI, V. From blockchain consensus back to byzantine consensus. **Future Generation Computer Systems**, Elsevier, v. 107, p. 760–769, jun. 2020. ISSN 0167-739X.

GUPTA, A.; STAHL, D. O.; WHINSTON, A. B. The Economics of Network Management. **Commun. ACM**, Association for Computing Machinery, Nova Iorque, EUA, v. 42, n. 9, p. 57–63, set. 1999. ISSN 0001-0782.

GWERN.NET. **Time-Locked Encryption**. 2019. Disponível em: https://www.gwern.net/Self-decrypting-files. Acesso em: 20 de Fevereiro de 2021.

HAN, Z. et al. **Game theory in wireless and communication networks : theory, models, and applications**. 1. ed. Cambridge, UK: Cambridge University Press, 2012. ISBN 9780521196963.

HAN, Z.; PANDANA, C.; LIU, K. J. R. A self-learning repeated game framework for optimizing packet forwarding networks. In: **IEEE Wireless Communications and Networking Conference, 2005**. Nova Orleans, EUA: IEEE, 2005. v. 4, p. 2131–2136. ISSN 1558-2612.

HARDJONO, T.; ZHENG, Y. A practical digital multisignature scheme based on discrete logarithms. In: SEBERRY, J.; ZHENG, Y. (Ed.). **Advances in Cryptology — AUSCRYPT '92**. Berlin, Heidelberg: Springer, 1993. p. 122–132. ISBN 978-3-540-47976-5.

HARN, L. Group-oriented (t, n) threshold digital signature scheme and digital multisignature. **IEE Proceedings - Computers and Digital Techniques**, IEEE, v. 141, p. 307–313(6), set. 1994. ISSN 1350-2387.

HARTENSTEIN, K. L. H. **VANET Vehicular Applications and Inter-Networking Technologies**. 1. ed. Nova Jérsei, EUA: Wiley, 2010. (Intelligent Transport Systems). ISBN 0470740566.

HAWLITSCHEK, F.; NOTHEISEN, B.; TEUBNER, T. The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. **Electronic Commerce Research and Applications**, Elsevier, v. 29, p. 50–63, maio 2018. ISSN 1567-4223.

HE, Q.; WU, D.; KHOSLA, P. SORI: a secure and objective reputation-based incentive scheme for ad-hoc networks. In: **2004 IEEE Wireless Communications and Networking Conference**. Atlanta, EUA: IEEE, 2004. v. 2, p. 825–830. ISSN 1525-3511.

HE, Y. et al. A Blockchain Based Truthful Incentive Mechanism for Distributed P2P Applications. **IEEE Access**, v. 6, p. 27324–27335, abr. 2018. ISSN 2169-3536.

HERRERA, J. G.; BOTERO, J. F. Resource Allocation in NFV: A Comprehensive Survey. **IEEE Transactions on Network and Service Management**, IEEE, v. 13, n. 3, p. 518–532, ago. 2016. ISSN 1932-4537.

HORSTER, P.; MICHELS, M.; PETERSEN, H. Meta-Multisignature schemes based on the discrete logarithm problem. In: ELOFF, J. H. P.; SOLMS, S. H. von (Ed.). **Information Security – the Next Decade**. Boston, MA: Springer, 1995, (IFIP Advances in Information and Communication Technology). cap. 11, p. 128–142. ISBN 978-0-387-34873-5.

HOSSEINI, M. et al. A survey of application-layer multicast protocols. **IEEE Communications Surveys Tutorials**, v. 9, n. 3, p. 58–74, 2007. ISSN 1553-877X.

HOUSLEY, R. et al. **The Internet Numbers Registry System**. [S.l.]: RFC Editor, 2013. 1–9 p. Internet Requests for Comments. Disponível em: https://tools.ietf.org/html/rfc7020. (Request for Comments, 7020).

HU, M. (Ed.). **Sharing Economy – Making Supply Meet Demand**. 1. ed. Cham, Suíça: Springer, 2019. 528 p. (Springer Series in Supply Chain Management). ISSN 2365-6395. ISBN 978-3-030-01863-4.

HUANG, H. et al. When Blockchain Meets Distributed File Systems: An Overview, Challenges, and Open Issues. **IEEE Access**, IEEE, v. 8, p. 50574–50586, mar. 2020. ISSN 2169-3536.

HUI, P. et al. Pocket Switched Networks and Human Mobility in Conference Environments. In: **Proceedings of the 2005 ACM SIGCOMM Workshop on Delay-Tolerant Networking**. Nova Iorque, EUA: Association for Computing Machinery, 2005. (WDTN '05), p. 244–251. ISBN 1595930264.

International Telecommunication Union. **Measuring digital development: Facts and figures 2021**. Gênova, Suíça: ITU Publications, 2021. ISBN 9789261354015.

INTERNET SOCIETY. **Global Internet Report – Paths to Our Digital Future**. 2017. Disponível em: https://future.internetsociety.org/2017/. Acesso em: 19 de Outubro de 2020.

INTERNET SOCIETY. **Community Networks**. 2021. Disponível em: https://www.internetsociety.org/issues/community-networks/. Acesso em: 08 de Agosto de 2021.

IQBAL, M.; MATULEVIČIUS, R. Exploring Sybil and Double-Spending Risks in Blockchain Systems. **IEEE Access**, IEEE, v. 9, p. 76153–76177, maio 2021. ISSN 2169-3536.

ITAKURA, K.; NAKAMURA, K. A public-key cryptosystem suitable for digital multisignatures. **NEC Research & Development**, Tóquio, Japão, n. 71, p. 1–8, 1983. ISSN 0547-051X.

JASIKA, N. et al. Dijkstra's shortest path algorithm serial and parallel execution performance analysis. In: **2012 Proceedings of the 35th International Convention MIPRO**. Opatija, Croácia: IEEE, 2012. p. 1811–1815. ISBN 978-953-233-068-7.

JEDARI, B.; XIA, F.; NING, Z. A Survey on Human-Centric Communications in Non-Cooperative Wireless Relay Networks. **IEEE Communications Surveys Tutorials**, IEEE, v. 20, n. 2, p. 914–944, jan. 2018. ISSN 1553-877X.

JIAO, Y. et al. Auction Mechanisms in Cloud/Fog Computing Resource Allocation for Public Blockchain Networks. **IEEE Transactions on Parallel and Distributed Systems**, IEEE, v. 30, n. 9, p. 1975–1989, mar. 2019. ISSN 1045-9219.

JOHNSON, D.; MENEZES, A.; VANSTONE, S. The elliptic curve digital signature algorithm (ECDSA). **International journal of information security**, Springer, v. 1, n. 1, p. 36–63, jul. 2001. ISSN 1615-5262.

KABBINALE, A. R. et al. Blockchain for economically sustainable wireless mesh networks. **Concurrency and Computation: Practice and Experience**, v. 32, n. 12, p. e5349, maio 2019. ISSN 1532-0626.

KALIDOSS, T. et al. QoS Aware Trust Based Routing Algorithm for Wireless Sensor Networks. **Wireless Personal Communications**, Springer, v. 110, n. 4, p. 1637–1658, out. 2019. ISSN 1572-834X.

KANG, J. et al. Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains. **IEEE Transactions on Industrial Informatics**, IEEE, v. 13, n. 6, p. 3154–3164, maio 2017. ISSN 1551-3203.

KHABBAZ, M. J.; ASSI, C. M.; FAWAZ, W. F. Disruption-Tolerant Networking: A Comprehensive Survey on Recent Developments and Persisting Challenges. **IEEE Communications Surveys & Tutorials**, IEEE, v. 14, n. 2, p. 607–640, segundo trimestre 2012. ISSN 2373-745X.

KIFFER, L.; LEVIN, D.; MISLOVE, A. Stick a Fork in It: Analyzing the Ethereum Network Partition. In: **Proceedings of the 16th ACM Workshop on Hot Topics in Networks**. Nova Iorque, EUA: Association for Computing Machinery, 2017. (HotNets-XVI), p. 94–100. ISBN 9781450355698.

KIM, S.; KWON, Y.; CHO, S. A Survey of Scalability Solutions on Blockchain. In: **2018 International Conference on Information and Communication Technology Convergence (ICTC)**. Jeju, South Korea: IEEE, 2018. p. 1204–1207. ISBN 978-1-5386-5041-7.

KING, S. **Primecoin**. 2013. Disponível em: https://primecoin.io. Acesso em: 19 de Outubro de 2019.

KOLAHI, S. S. et al. Performance Comparison of IEEE802.11ac vs IEEE 802.11n WLAN in IPv6. In: BAROLLI, L.; WOUNGANG, I.; ENOKIDO, T. (Ed.). **Advanced Information Networking and Applications**. Cham: Springer, 2021. v. 227, p. 426–435. ISBN 978-3-030-75078-7.

KOMANO, Y. et al. Formal Security Model of Multisignatures. In: KATSIKAS, S. K. et al. (Ed.). **Information Security**. Berlin, Heidelberg: Springer, 2006. p. 146–160. ISBN 978-3-540-38343-7.

KOMLO, C.; GOLDBERG, I. FROST: Flexible Round-Optimized Schnorr Threshold Signatures. In: DUNKELMAN, O.; JACOBSON JR., M. J.; O'FLYNN, C. (Ed.). **Selected Areas in Cryptography**. Cham: Springer, 2021. p. 34–65. ISBN 978-3-030-81652-0.

KWON, J.; BUCHMAN, E. **Cosmos – A Network of Distributed Ledgers**. 2019. Disponível em: https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md. Acesso em: 22 de Junho, 2021.

LAU, J. **Merkelized Abstract Syntax Tree**. 2016. Disponível em: https://github.com/bitcoin/bips/blob/master/bip-0114.mediawiki. Acesso em: 01 de Setembro de 2020.

LE, D.; BONNECAZE, A.; GABILLON, A. Multisignatures as Secure as the Diffie-Hellman Problem in the Plain Public-Key Model. In: SHACHAM, H.; WATERS, B. (Ed.). **Pairing-Based Cryptography**. Berlin, Heidelberg: Springer, 2009. (Pairing 2009), p. 35–51. ISBN 978-3-642-03298-1.

LEHR, W.; CROWCROFT, J. Managing shared access to a spectrum commons. In: **First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.** Baltimore, EUA: IEEE, 2005. p. 420–444. ISBN 1-4244-0013-9.

LI, C.; HWANG, T.; LEE, N.-Y. Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders. In: SANTIS, A. D. (Ed.). **Advances in Cryptology — EUROCRYPT'94**. Berlin, Heidelberg: Springer, 1995. p. 194–204. ISBN 978-3-540-44717-7.

LI, C.; PALANISAMY, B. Incentivized Blockchain-Based Social Media Platforms: A Case Study of Steemit. In: **Proceedings of the 10th ACM Conference on Web Science**. Nova Iorque, EUA: Association for Computing Machinery, 2019. (WebSci '19), p. 145–154. ISBN 9781450362023.

LI, F.; WU, J. FRAME: An Innovative Incentive Scheme in Vehicular Networks. In: **2009 IEEE International Conference on Communications**. Dresden, Germany: IEEE, 2009. p. 1–6. ISSN 1550-3607.

LI, M.; TANG, H.; WANG, X. Mitigating Routing Misbehavior using Blockchain-Based Distributed Reputation Management System for IoT Networks. In: **2019 IEEE International Conference on Communications Workshops (ICC Workshops)**. Shanghai, China: IEEE, 2019. p. 1–6. ISSN 2474-9133.

LI, M. et al. Toward Blockchain-Based Fair and Anonymous Ad Dissemination in Vehicular Networks. **IEEE Transactions on Vehicular Technology**, IEEE, v. 68, n. 11, p. 11248–11259, nov. 2019. ISSN 0018-9545.

LIAN, S. et al. Commutative Encryption and Watermarking in Video Compression. **IEEE Transactions on Circuits and Systems for Video Technology**, IEEE, v. 17, n. 6, p. 774–778, jun. 2007. ISSN 1051-8215.

LIN, C. et al. Blockchain-based system for secure outsourcing of bilinear pairings. **Information Sciences**, Elsevier, v. 527, p. 590 – 601, jul. 2020. ISSN 0020-0255.

LITAN, A. **Smart Contracts are Neither Smart nor are they Contracts**. 2020. Disponível em: https://blogs.gartner.com/avivah-litan/2020/03/03/smart-contracts-neither-smart-contracts/. Acesso em: 10 de agosto de 2021.

LIU, M. et al. Distributed Resource Allocation in Blockchain-Based Video Streaming Systems With Mobile Edge Computing. **IEEE Transactions on Wireless Communications**, IEEE, v. 18, n. 1, p. 695–708, dez. 2019. ISSN 1536-1276.

LOMBROZO, E.; LAU, J.; WUILLE, P. **Segregated Witness (Consensus layer)**. 2015. Disponível em: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki. Acesso em: 01 de Setembro de 2020.

LU, S. et al. Sequential Aggregate Signatures and Multisignatures Without Random Oracles. In: VAUDENAY, S. (Ed.). **Advances in Cryptology - EUROCRYPT 2006**. Berlin, Heidelberg: Springer, 2006. p. 465–485. ISBN 978-3-540-34547-3.

LWIN, M. T.; YIM, J.; KO, Y.-B. Blockchain-Based Lightweight Trust Management in Mobile Ad-Hoc Networks. **Sensors**, MDPI AG, v. 20, n. 3, p. 698, jan. 2020. ISSN 1424-8220.

MA, C. et al. Efficient discrete logarithm based multi-signature scheme in the plain public key model. **Designs, Codes and Cryptography**, Springer, v. 54, n. 2, p. 121–133, fev. 2010. ISSN 1573-7586.

MACCARI, L. et al. Towards scalable community networks topologies. **Ad Hoc Networks**, Elsevier, v. 94, p. 101949, nov. 2019. ISSN 1570-8705.

MACHADO, C.; FRÖHLICH, A. A. M. IoT Data Integrity Verification for Cyber-Physical Systems Using Blockchain. In: **2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC)**. Singapura: IEEE, 2018. p. 83–90. ISSN 2375-5261.

MACHADO, C.; SANTOS, R. R. S. dos; WESTPHALL, C. M. Hop-by-hop Accounting and Rewards for Packet dIspAtching. In: **2021 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)**. Shenyang, China: IEEE (Preprint), 2021. A ser apresentado em conferência adiada de 18–20 de agosto para 20–22 de outubro de 2021 devido às restrições sanitárias da COVID-19. Disponível em: https://arxiv.org/abs/2108.09509.

MACHADO, C.; WESTPHALL, C. M. Blockchain incentivized data forwarding in MANETs: Strategies and challenges. **Ad Hoc Networks**, Elsevier, v. 110, p. 102321, jan. 2021. ISSN 1570-8705.

MAHMOUD, M. E.; SHEN, X. PIS: A Practical Incentive System for Multihop Wireless Networks. **IEEE Transactions on Vehicular Technology**, IEEE, v. 59, n. 8, p. 4012–4025, out. 2010. ISSN 0018-9545.

MARIAS, G. F. et al. Cooperation enforcement schemes for MANETs: a survey. **Wireless Communications and Mobile Computing**, v. 6, n. 3, p. 319–332, 2006.

MAXWELL, G. et al. Simple schnorr multi-signatures with applications to bitcoin. **Designs, Codes and Cryptography**, Springer, v. 87, n. 9, p. 2139–2164, set. 2019. ISSN 1573-7586.

MENAKA, R.; RANGANATHAN, V.; SOWMYA, B. Improving performance through reputation based routing protocol for manet. **Wirel. Pers. Commun.**, Kluwer Academic Publishers, Boston, EUA, v. 94, n. 4, p. 2275–2290, jun. 2017. ISSN 0929-6212.

MENGELKAMP, E. et al. Designing microgrid energy markets: A case study: The Brooklyn Microgrid. **Applied Energy**, Elsevier, v. 210, p. 870–880, jan. 2018. ISSN 0306-2619.

MICALI, S.; OHTA, K.; REYZIN, L. Accountable-subgroup multisignatures. In: **Proceedings of the 8th ACM Conference on Computer and Communications Security**. Nova Iorque, EUA: Association for Computing Machinery, 2001. (CCS '01), p. 245–254. ISBN 1581133855.

MICHELS, M.; HORSTER, P. On the risk of disruption in several multiparty signature schemes. In: KIM, K.; MATSUMOTO, T. (Ed.). **Advances in Cryptology — ASIACRYPT '96**. Berlin, Heidelberg: Springer, 1996. (LNCS, v. 1163), p. 334–345. ISBN 978-3-540-70707-3.

MICHOLIA, P. et al. Community Networks and Sustainability: A Survey of Perceptions, Practices, and Proposed Solutions. **IEEE Communications Surveys Tutorials**, IEEE, v. 20, n. 4, p. 3581–3606, mar. 2018. ISSN 1553-877X.

MIGUEL, E. S. et al. Blockchain-Enabled Participatory Incentives for Crowdsourced Mesh Networks. In: DJEMAME, K. et al. (Ed.). **Economics of Grids, Clouds, Systems, and Services**. Cham: Springer, 2019. (LNCS, v. 11819), p. 178–187. ISBN 978-3-030-36027-6.

MURATOV, F. et al. YAC: BFT Consensus Algorithm for Blockchain. **CoRR**, abs/1809.00554, 2018. Disponível em: http://arxiv.org/abs/1809.00554.

MYERS, R. **A lightweight protocol to incentivize mobile peer-to-peer communication**. 2019. Disponível em: https://global-mesh-labs.gitbook.io/lot49/. Acesso em: 20 de Fevereiro de 2021.

MYERSON, R. B. **Game Theory: Analysis of Conflict**. Cambridge, EUA: Harvard University Press, 1997. ISBN 9780674341166.

NAKAMOTO, S. **Bitcoin: A peer-to-peer electronic cash system**. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 05 de Abril de 2020.

NETCOMMONS. **Network Infrastructure as Commons**. 2019. Disponível em: https://www.netcommons.eu/. Acesso em: 20 de Fevereiro de 2021.

NETWORK, R. **Raiden Network**. 2019. Disponível em: https://docs.raiden.network/. Acesso em: 05 de Abril de 2020.

NEUMANN, A.; NAVARRO, L.; CERDÀ-ALABERN, L. Enabling individually entrusted routing security for open and decentralized community networks. **Ad Hoc Networks**, Elsevier, v. 79, p. 20–42, out. 2018. ISSN 1570-8705.

NGUYEN, C. T. et al. Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities. **IEEE Access**, IEEE, v. 7, p. 85727–85745, jun. 2019. ISSN 2169-3536.

NICK, J.; RUFFING, T.; SEURIN, Y. MuSig2: Simple Two-Round Schnorr Multi-signatures. In: MALKIN, T.; PEIKERT, C. (Ed.). **Advances in Cryptology – CRYPTO 2021**. Cham: Springer, 2021. p. 189–221. ISBN 978-3-030-84242-0.

NISHIYAMA, H.; ITO, M.; KATO, N. Relay-by-smartphone: realizing multihop device-to-device communications. **IEEE Communications Magazine**, IEEE, v. 52, n. 4, p. 56–65, maio 2014. ISSN 0163-6804.

NORRIS, P. **Digital divide: Civic engagement, information poverty, and the Internet worldwide**. Cambridge, UK: Cambridge University Press, 2001. (Communication Society and Politics). ISBN 9781139164887.

NUPEF. **Espectro e Redes Comunitárias**. 2021. Disponível em: https://espectro.org.br/pt-br/formacao-em-redes/tutoriais. Acesso em: 21 de Agosto de 2021.

OHTA, K.; OKAMOTO, T. A digital multisignature scheme based on the Fiat-Shamir scheme. In: IMAI, H.; RIVEST, R. L.; MATSUMOTO, T. (Ed.). **Advances in Cryptology — ASIACRYPT '91**. Berlin, Heidelberg: Springer, 1993. (LNCS, v. 739), p. 139–148. ISBN 978-3-540-48066-2.

OHTA, K.; OKAMOTO, T. Multi-signature schemes secure against active insider attacks. **IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences**, The Institute of Electronics, Information and Communication Engineers, v. 82, n. 1, p. 21–31, jan. 1999. ISSN 0916-8508.

OKAMOTO, T. Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes. In: BRICKELL, E. F. (Ed.). **Advances in Cryptology — CRYPTO' 92**. Berlin, Heidelberg: Springer, 1993. (LNCS), p. 31–53. ISBN 978-3-540-48071-6.

OLSON, M. The logic of collective action [1965]. In: CALHOUN, C. et al. (Ed.). **Contemporary Sociological Theory**. Malden, EUA: Wiley-Blackwell, 2012. p. 124–128. ISBN 978-0-470-65566-5.

ONU. **Transformando Nosso Mundo: A Agenda 2030 para o Desenvolvimento Sustentável**. 2015. Disponível em: https://nacoesunidas.org/pos2015/agenda2030/. Acesso em: 19 de Outubro de 2019.

PANCHANATHAN, K.; BOYD, R. Indirect reciprocity can stabilize cooperation without the second-order free rider problem. **Nature**, Springer Nature, v. 432, p. 499–502, nov. 2004. ISSN 1476-4687.

PARK, Y.; SUR, C.; RHEE, K.-H. A Secure Incentive Scheme for Vehicular Delay Tolerant Networks Using Cryptocurrency. **Security and Communication Networks**, Hindawi, v. 14, n. 4, p. 73–85, jul. 2018. ISSN 2373-745X.

Paul Gardner-Stephen. **Root-free operation of the Serval Mesh**. 2013. Disponível em: https://servalpaul.blogspot.com/2013/04/root-free-operation-of-serval-mesh.html. Acesso em: 19 de Fevereiro de 2020.

PAZAITIS, A.; DE FILIPPI, P.; KOSTAKIS, V. Blockchain and value systems in the sharing economy: The illustrative case of Backfeed. **Technological Forecasting and Social Change**, Elsevier, v. 125, p. 105–115, dez. 2017. ISSN 0040-1625.

PEREIRA, P. R. et al. From Delay-Tolerant Networks to Vehicular Delay-Tolerant Networks. **IEEE Communications Surveys Tutorials**, IEEE, v. 14, n. 4, p. 1166–1182, abr. 2012. ISSN 2373-745X.

POLYGON. **Polygon**. 2021. Disponível em: https://polygon.technology/get-started/. Acesso em: 20 de Julho de 2021.

POLYGONSCAN. **Polygonscan**. 2021. Disponível em: https://polygonscan.com/. Acesso em: 20 de Junho de 2021.

POON, J.; BUTERIN, V. **Plasma: Scalable autonomous smart contracts**. 2017. Disponível em: https://www.plasma.io/plasma-deprecated.pdf. Acesso em: 19 de Julho de 2021.

POON, J.; DRYJA, T. **The bitcoin lightning network: Scalable off-chain instant payments**. 2016. Disponível em: http://lightning.network/docs. Acesso em: 05 de Abril de 2020.

PROMETHEUS INDUSTRIES. **Blockmesh**. 2017. Disponível em: https://www.blockmesh.io/pdf/BlockMesh-White_Paper-1.pdf. Acesso em: 20 de Fevereiro de 2021.

PUSTIŠEK, M.; UMEK, A.; KOS, A. Approaching the Communication Constraints of Ethereum-Based Decentralized Applications. **Sensors**, MDPI, v. 19, n. 11, jun. 2019. ISSN 1424-8220.

RATNASAMY, S.; ERMOLINSKIY, A.; SHENKER, S. Revisiting IP Multicast. **SIGCOMM Comput. Commun. Rev.**, Association for Computing Machinery, Nova Iorque, EUA, v. 36, n. 4, p. 15–26, ago. 2006. ISSN 0146-4833.

RAYA, M.; HUBAUX, J.-P.; AAD, I. Domino: A system to detect greedy behavior in ieee 802.11 hotspots. In: **Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services**. Nova Iorque, EUA: Association for Computing Machinery, 2004. (MobiSys '04), p. 84–97. ISBN 1581137931.

REMIX. **Remix**. 2021. Disponível em: https://remix.ethereum.org/. Acesso em: 20 de Abril de 2021.

RHIZOMATICA. **Rhizomatica**. 2021. Disponível em: https://www.rhizomatica.org/. Acesso em: 14 de Agosto de 2021.

RISTENPART, T.; YILEK, S. The Power of Proofs-of-Possession: Securing Multiparty Signatures against Rogue-Key Attacks. In: NAOR, M. (Ed.). **Advances in Cryptology - EUROCRYPT 2007**. Berlin, Heidelberg: Springer, 2007. (LNCS, v. 5229), p. 228–245. ISBN 978-3-540-72540-4.

ROSA, R.; ROTHENBERG, C. E. Blockchain-Based Decentralized Applications for Multiple Administrative Domain Networking. **IEEE Communications Standards Magazine**, IEEE, v. 2, n. 3, p. 29–37, set. 2018. ISSN 2471-2833.

ROUGHGARDEN, T. Algorithmic game theory. **Commun. ACM**, Association for Computing Machinery, Nova Iorque, EUA, v. 53, n. 7, p. 78–86, jul. 2010. ISSN 0001-0782.

RUIZ, P.; BOUVRY, P. Survey on Broadcast Algorithms for Mobile Ad Hoc Networks. **ACM Comput. Surv.**, Association for Computing Machinery, Nova Iorque, EUA, v. 48, n. 1, p. 1–35, jul. 2015. ISSN 0360-0300.

SAAD, M. et al. Exploring the Attack Surface of Blockchain: A Comprehensive Survey. **IEEE Communications Surveys Tutorials**, IEEE, v. 22, n. 3, p. 1977–2008, mar. 2020. ISSN 1553-877X.

SAMI, M. et al. A Survey and Taxonomy on Medium Access Control Strategies for Cooperative Communication in Wireless Networks: Research Issues and Challenges. **IEEE Communications Surveys Tutorials**, IEEE, v. 18, n. 4, p. 2493–2521, 2016. ISSN 1553-877X.

SCHEID, E. J. et al. Enabling Dynamic SLA Compensation Using Blockchain-based Smart Contracts. In: **2019 IFIP/IEEE Symposium on Integrated Network and Service Management**. Arlington, EUA: IEEE, 2019. p. 53–61. ISBN 978-3-903176-15-7.

SCHNORR, C. P. Efficient signature generation by smart cards. **Journal of Cryptology**, Springer, v. 4, n. 3, p. 161–174, jan. 1991. ISSN 1432-1378.

SEITHER, D.; KÖNIG, A.; HOLLICK, M. Routing performance of Wireless Mesh Networks: A practical evaluation of BATMAN advanced. In: **2011 IEEE 36th Conference on Local Computer Networks**. Osnabrück, Germany: IEEE, 2011. p. 897–904. ISBN 978-1-61284-928-7. ISSN 0742-1303.

SHOKER, A. Sustainable blockchain through proof of exercise. In: **2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)**. Cambridge, EUA: IEEE, 2017. p. 1–9. ISBN 978-1-5386-1465-5.

SILVA, B. M. C. et al. Cooperative Strategies for Challenged Networks and Applications: A Survey. **IEEE Systems Journal**, IEEE, v. 11, n. 4, p. 2749–2760, jul. 2017. ISSN 1932-8184.

SILVANO, W. F.; MARCELINO, R. Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. **Future Generation Computer Systems**, Elsevier, v. 112, p. 307–319, nov. 2020. ISSN 0167-739X.

SKJEGSTAD, M.; MADHAVAPEDDY, A.; CROWCROFT, J. Kadupul: Livin' on the Edge with Virtual Currencies and Time-Locked Puzzles. In: **Proceedings of the 2015 Workshop on Do-it-yourself Networking: An Interdisciplinary Approach**. Nova Iorque, EUA: ACM, 2015. (DIYNetworking '15), p. 21–26. ISBN 978-1-4503-3503-4.

SKYCOIN. **Skycoin - Edition 1.2**. 2017. Disponível em: https://www.skycoin.com/whitepapers. Acesso em: 20 de Fevereiro de 2021.

SMARTMESH FOUNDATION. **SmartMesh Tokenized Mobile Mesh Network**. 2017. Disponível em: https://smartmesh.io/SmartMeshWhitePaperEN.pdf. Acesso em: 20 de Fevereiro de 2021.

SPURGEON, C.; ZIMMERMAN, J. **Ethernet: The Definitive Guide: Designing and Managing Local Area Networks**. 2. ed. Sebastopol, EUA: O'Reilly, 2014. ISBN 9781449361846.

TAGHAVI, M. et al. A Blockchain-Based Model for Cloud Service Quality Monitoring. **IEEE Transactions on Services Computing**, IEEE, v. 13, n. 2, p. 276–288, out. 2020. ISSN 1939-1374.

TEIXEIRA, R. et al. Dynamics of Hot-Potato Routing in IP Networks. **SIGMETRICS Perform. Eval. Rev.**, Association for Computing Machinery, Nova Iorque, EUA, v. 32, n. 1, p. 307–319, jun. 2004. ISSN 0163-5999.

THELWALL, M.; STUART, D. Web crawling ethics revisited: Cost, privacy, and denial of service. **Journal of the American Society for Information Science and Technology**, John Wiley & Sons, v. 57, n. 13, p. 1771–1779, set. 2006. ISSN 1532-2882.

TOKENVIEW. **Tokenview**. 2021. Disponível em: https://tokenview.com/. Acesso em: 20 de Junho de 2021.

TRAUTMANN, T.; BURNELL, A. **Routing Based Blockchain**. 2020. Disponível em: https://patentimages.storage.googleapis.com/bd/9e/f3/23670e2db5676c/US10771384.pdf. U.S. Patent 10,771,384. Acesso em: 20 de Fevereiro de 2021.

TREMBACK, J. **Althea's multihop payment channels**. 2017. Disponível em: https://blog.althea.net/altheas-multihop-payment-channels/. Acesso em: 19 de Outubro de 2019.

TREMBACK, J. et al. **Althea white paper v1.51**. 2020. Disponível em: https://althea.net/whitepaper. Acesso em: 20 de Abril de 2021.

VEGA, D. et al. A technological overview of the guifi.net community network. **Computer Networks**, Elsevier, v. 93, p. 260–278, dez. 2015. ISSN 1389-1286.

VEGA, D. et al. Topology patterns of a community network: Guifi.net. In: **2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)**. Barcelona, Croácia: IEEE, 2012. p. 612–619. ISSN 2160-4894.

VRANKEN, H. Sustainability of bitcoin and blockchains. **Current Opinion in Environmental Sustainability**, Elsevier, v. 28, p. 1–9, out. 2017. ISSN 1877–3435.

WANG, B.; LIU, K. J. R. Advances in cognitive radio networks: A survey. **IEEE Journal of Selected Topics in Signal Processing**, IEEE, v. 5, n. 1, p. 5–23, fev. 2011. ISSN 1941-0484.

WANG, W. et al. A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. **IEEE Access**, IEEE, v. 7, p. 22328–22370, jan. 2019. ISSN 2169-3536.

WEBER, I. et al. On availability for blockchain-based systems. In: **2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)**. Hong Kong, China: IEEE, 2017. p. 64–73. ISBN 978-1-5386-1679-6.

WERBACH, K. **The Blockchain and the New Architecture of Trust**. Cambridge, EUA: The MIT Press, 2018. (Information Policy). ISBN 9780262038935.

WIREGUARD. **Wireguard – Fast, modern, secure VPN tunnel**. 2019. Disponível em: https://www.wireguard.com/. Acesso em: 20 de Fevereiro de 2021.

WUILLE, P.; NICK, J.; RUFFING, T. **Schnorr Signatures for secp256k1**. 2020. Disponível em: https://github.com/bitcoin/bips/blob/master/bip-0114.mediawiki. Acesso em: 01 de Maio de 2021.

XIONG, Z. et al. When Mobile Blockchain Meets Edge Computing. **IEEE Communications Magazine**, IEEE, v. 56, n. 8, p. 33–39, ago. 2018. ISSN 0163-6804.

YANG, D.; FANG, X.; XUE, G. Game theory in cooperative communications. **IEEE Wireless Communications**, IEEE, v. 19, n. 2, p. 44–49, abr. 2012. ISSN 1536-1284.

YANG, Z. et al. Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities. In: **2019 28th International Conference on Computer Communication and Networks (ICCCN)**. Valência, Espanha: IEEE, 2019. p. 1–9. ISSN 2637-9430.

YOO, Y.; AHN, S.; AGRAWAL, D. P. A credit-payment scheme for packet forwarding fairness in mobile ad hoc networks. In: **IEEE International Conference on Communications, 2005. ICC 2005. 2005**. Seoul, South Korea: IEEE, 2005. v. 5, p. 3005–3009. ISSN 1550-3607.

ZAMANI, M.; MOVAHEDI, M.; RAYKOVA, M. RapidChain: Scaling Blockchain via Full Sharding. In: **Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security**. Nova Iorque, EUA: Association for Computing Machinery, 2018. (CCS '18), p. 931–948. ISBN 9781450356930.

ZETZSCHE, D. A. et al. The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators. **Harvard International Law Journal**, Harvard Law School, v. 60, n. 2, p. 267–315, jul. 2019. ISSN 0017-8063.

ZHANG, S. An Overview of Network Slicing for 5G. **IEEE Wireless Communications**, IEEE, v. 26, n. 3, p. 111–117, abr. 2019. ISSN 1558-0687.

ZHENG, Z. et al. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In: **2017 IEEE International Congress on Big Data (BigData Congress)**. Honolulu, EUA: IEEE, 2017. p. 557–564. ISBN 978-1-5386-1996-4.

ZHENG, Z. et al. An overview on smart contracts: Challenges, advances and platforms. **Future Generation Computer Systems**, Elsevier, v. 105, p. 475–491, abr. 2020. ISSN 0167-739X.

ZHOU, Q. et al. Solutions to Scalability of Blockchain: A Survey. **IEEE Access**, IEEE, v. 8, p. 16440–16455, jan. 2020. ISSN 2169-3536.

ZHU, H. et al. SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks. **IEEE Transactions on Vehicular Technology**, IEEE, v. 58, n. 8, p. 4628–4639, apr 2009. ISSN 0018-9545.