Correntes de Blocos em Redes Virtualizadas: Protocolos de Consenso e Fatiamento Seguro da Rede

Gabriel Antonio Fontes Rebello[1],
Orientador: Otto Carlos M. B. Duarte[1]

[1] Universidade Federal do Rio de Janeiro, RJ, Brasil

Resumo. *A corrente de blocos (blockchain) é uma tecnologia disruptiva que deve revolucionar o nosso modo de viver, trabalhar e negociar. Assim como a Internet permite hoje a transferência de arquivos, esta nova tecnologia construirá uma Internet de Valores, na qual é possível transferir recursos de valor, como dinheiro, ações, propriedade intelectual, votos, etc. sem o intermédio de agentes reguladores. No entanto, um dos principais desafios de sistemas baseados em correntes de blocos é selecionar o protocolo de consenso distribuído mais adaptado para cada caso de uso. A primeira parte deste trabalho discute os conceitos e os modelos de consenso para diferentes tipos de correntes de blocos. Diversos protocolos de consenso são apresentados especificando suas características, suas vantagens, suas desvantagens e finalidades. A seguir, o trabalho propõe uma arquitetura para prover segurança à Internet baseada no fatiamento da rede (network slicing), que objetiva oferecer serviços fim-a-fim de rede ágeis e sob demanda para cada tipo de aplicação. A arquitetura provê auditabilidade às operações de orquestração de fatias de rede. O trabalho desenvolve e implementa um protótipo da arquitetura proposta através de contratos inteligentes na plataforma Hyperledger Fabric. Os resultados mostram que é possível prover segurança à orquestração de fatias de rede, mas que a latência de obtenção do consenso e a vazão de transações requeridas pelas fatias de rede constituem um desafio a ser investigado caso a caso.*

Abstract. *Blockchains are a disruptive technology that will revolutionize our way of living, working and negotiating. Like the Internet today allows transfering files, this new technology will build an Internet of Value, in which it is possible to transfer unique resources such as money, stock, intellectual property, votes, etc. without the need for intermediate entities. One of the main challenges of blockhain-based systems, however, is to select the distributed consensus protocol that suits each use case. The first part of this work discusses the consensus concepts and models for different types of blockchains. We present several consensus protocols and clarify their features, advantages, disadvantages and main goals. Then, in a second part, we propose an architecture to secure a network-slicing-based Internet, which aims to offer agile and on-demand end-to-end services for each type of application. The proposed architecture provides auditability to network slicing orchestration operations. We develop and implement a prototype of the proposed architecture with smart contracts on the Hyperledger Fabric platform. The results show that it is possible to provide security to network slice orchestration, but consensus latency and transaction throughput might still pose a challenge for some cases.*

1. Caracterização do Problema e Motivação

Hoje, as tecnologias de corrente de blocos (*blockchain*) de primeira geração, baseadas no Bitcoin [Nakamoto 2008], e de segunda geração, baseadas nos contratos inteligentes do Ethereum [Wood 2014] já revolucionaram o mundo atual ao criar uma camada de confiança para transferências seguras de ativos e execução segura de contratos. As diversas aplicações de correntes de blocos em criptomoedas já atingiram um capital de mercado global de mais de 800 bilhões de dólares em 2018 [Coin Market 2019], o que corresponde a metade do PIB brasileiro no mesmo ano [Instituto Brasileiro de Geografia e Estatística 2019]. No entanto, a corrente de blocos pode ser utilizada na Internet do Futuro para prover confiança distribuída mesmo quando não há troca de moedas ou valores. A confiança distribuída sem intermediários provida pela corrente de blocos permitirá múltiplas ofertas de funções virtualizadas de rede e seleção criteriosa entre provedores de infraestrutura, produzindo uma concorrência sem precedentes na área de telecomunicações. Em especial, as correntes de blocos atenderão a diversas aplicações, desde redes veiculares tolerantes a atraso até serviços críticos como saúde eletrônica (*e-Health*), cidades inteligentes (*smart cities*) e redes elétricas inteligentes (*smart grids*). Por estes motivos, as tecnologias baseadas em corrente de blocos são consideradas tanto pela indústria como pela academia como a tecnologia mais disruptiva dos últimos tempos [Glaser 2017, Cachin e Vukolić 2017, Xiao et al. 2019].

No entanto, todo sistema baseado em corrente de blocos deve ser capaz de obter consenso[1] entre os participantes para incorporar novos blocos à corrente. A proposta do Bitcoin, a primeira criptomoeda, resolve o problema do consenso através da prova de trabalho (*Proof-of-Work* – PoW), um protocolo baseado em competição entre os participantes para definir o líder da rodada de consenso. O crescimento do Bitcoin, porém, evidencia as limitações, gargalos de desempenho e problemas de sustentabilidade da prova de trabalho, como: i) consumo de energia excessivo; ii) baixa vazão de transações; e iii) tendência de centralização em participantes com maior poder computacional. A latência de consenso, de aproximadamente uma hora, e a vazão de transações, de até 7 transações por segundo, consistem em um desafio para atender às necessidades dos sistemas atuais [Popov 2017, Eyal et al. 2016]. O processo de mineração da prova de trabalho no Bitcoin gera um consumo insustentável de energia sem retorno proporcional, atingindo mais de 70 TWh [Digiconomist 2019] gastos por ano. Para se ter uma ideia, esse valor é mais de quatro vezes maior que os cerca de 15 TWh de energia gerada pelas usinas nucleares de Angra [Eletrobras 2017]. O gasto energético para processar uma única transação no Bitcoin é suficiente para abastecer uma residência média brasileira durante três meses [Digiconomist 2019, Ministério de Minas e Energia 2017].

Em resposta às limitações de desempenho do consenso baseado em prova de trabalho, diversos protocolos de consenso foram propostos como alternativas ao protocolo do Bitcoin. Dentre eles, destacam-se: i) protocolos alternativos baseados em prova, como a prova de posse (*Proof-of-Stake* – PoS) [NXT community 2014]; ii) protocolos baseados em quórum, como os protocolos clássicos tolerantes a falhas de parada (e.g. RAFT [Ongaro e Ousterhout 2014] e Paxos [Lamport 1998]) e protocolos tolerantes a fa-

[1]Consenso é um tipo de acordo produzido por consentimento entre todos os membros de um grupo. O consenso se estabelece quando dois ou mais membros chegam a um ponto comum de decisão durante uma negociação.

lhas bizantinas (e.g. PBFT [Castro e Liskov 1999] e BFT-Smart [Bessani et al. 2014]); iii) protocolos híbridos, como o Casper FFG [Buterin e Griffith 2017] e Tendermint [Kwon 2014]; e protocolos baseados em grafos acíclicos direcionados (*Directed Acyclic Graph* – DAG), como o IOTA [Popov 2017]. Cada protocolo e cada categoria possui características específicas de desempenho e escalabilidade que devem ser consideradas para cada caso de uso. A primeira parte desta dissertação discute em detalhes as características de cada protocolo e propõe a categorização citada acima. As vantagens e desvantagens de cada protocolo são abordadas, de forma a clarificar qual selecionar em cada caso de uso.

Além disso, no novo paradigma da Internet do Futuro, as redes definidas por *software* (*Software-Defined Networking* - SDN) e a virtualização de funções de rede (*Network Function Virtualization* - NFV) criam uma fatia de rede (*network slice*) composta por funções virtuais de rede (*Virtual Network Function* - VNF) para fornecer serviços sob demanda e adaptados a cada aplicação. Neste cenário surgem novos desafios de segurança [Medhat et al. 2017] e o impacto de possíveis ataques aumenta porque os ataques aos hospedeiros de funções de rede podem comprometer simultaneamente milhares de usuários [Bhamare et al. 2016]. Portanto, é de grande importância reduzir os possíveis vetores de ataque a fatias de rede e fornecer um gerenciamento de configuração seguro e confiável. O ambiente multi-inquilino e multidomínio aumenta a possibilidade de ataques dentro da nuvem, ao mesmo tempo que dificulta a responsabilização dos provedores de serviços quando ocorre uma falha. Logo, a capacidade de auditoria é obrigatória para identificar uma configuração de VNF defeituosa ou comprometida, e a tecnologia de corrente de blocos atende a esta necessidade, pois fornece as características necessárias de não repúdio e imutabilidade do histórico de configuração de uma fatia de rede. Esta dissertação propõe utilizar a tecnologia de corrente de blocos para registrar, como transações assinadas, todos os comandos que criam, modificam, configuram, migram ou destroem as funções de rede de cada fatia da rede. Portanto, todos os problemas de funcionamento da rede podem ser verificados e um erro pode ser atribuído corretamente a um provedor de serviço em um ambiente de concorrência e sem confiança.

2. Objetivos e Contribuições

O objetivo desta dissertação é abordar a utilização de corrente de blocos para criar redes virtualizadas seguras. A primeira parte do trabalho objetiva discutir em detalhes os conceitos e os modelos de consenso para diferentes tipos de correntes de blocos. A principal contribuição desta parte é apresentar e categorizar os diversos protocolos de consenso existentes para correntes de blocos, especificando suas características, suas vantagens, suas desvantagens e finalidades. Assim, é possível selecionar o melhor protocolo de consenso para cada caso de uso.

A segunda parte objetiva analisar o uso de correntes de blocos em um ambiente de fatiamento da rede. As principais contribuições desta segunda parte são: i) a proposta e desenvolvimento de uma arquitetura baseada em correntes de blocos para prover auditabilidade às operações de orquestração de fatias de rede, ilustrada na Figura 1; e ii) uma proposta de categorização das correntes de blocos para atender os diversos cenários presentes nas redes do futuro, ilustrada na Figura 2. A proposta de categorização presente na segunda parte é uma contribuição construída a partir da análise dos protocolos realizada na primeira parte da dissertação, efetivamente conectando as duas partes. Ainda, a

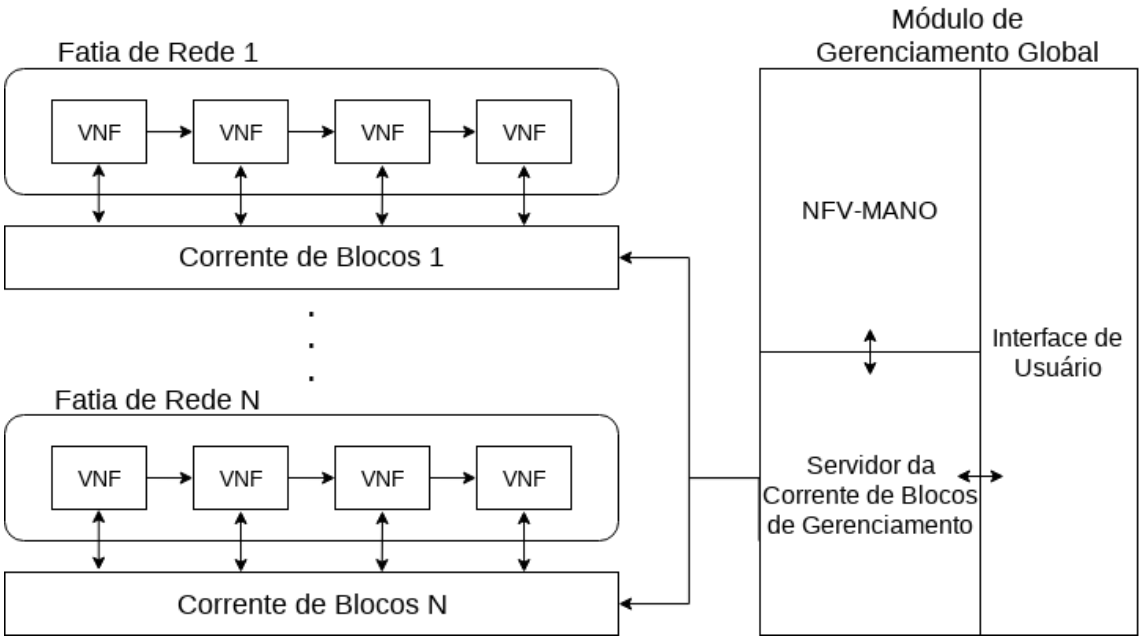

Figura 1. A arquitetura proposta baseada em corrente de blocos para fatiamento de rede. O usuário interage com o módulo de gerenciamento global para criar fatias de rede seguras. Cada VNF em uma fatia de rede é conectada a uma corrente de blocos responsável por registrar solicitações de configuração e informações relevantes, conforme especificado pelo usuário.

proposta de arquitetura leva em consideração o estudo dos protocolos de consenso para selecionar o protocolo utilizado no protótipo. Um protótipo de caso de uso que segue a arquitetura proposta com diferentes tipos de correntes de blocos é implementado usando a plataforma de código aberto Hyperledger Fabric [Androulaki et al. 2018]. O protótipo implementa dois contratos inteligentes com formatos de transação específicos para proteger o gerenciamento de fatias de rede e as operações de configuração de VNFs. Cada fatia de rede é executada em um canal Hyperledger isolado. Os resultados mostram que é possível proteger a construção de fatias de rede, mas que estruturas de dados otimizadas são necessárias para aumentar a taxa de transações necessárias para atender às fatias.

3. Trabalhos Relacionados

Diversos trabalhos exploram o estado da arte de corrente de blocos aplicada a problemas de redes de comunicação e redes de quinta geração (5G). Yahiatene *et al.* e Ortega *et al.* propõem o uso de corrente de blocos como um mecanismo para fornecer segurança em redes veiculares [Yahiatene e Rachedi 2018, Ortega et al. 2018], enquanto Thuemler *et al.* e Capossele *et al.* discutem os requisitos necessários ao 5G para prover saúde eletrônica (*e-Health*) com base em experiências reais [Thuemmler et al. 2018, Capossele et al. 2018]. Rawat *et al.* propõem uma solução baseada em corrente de blocos para redes sem fio virtuais que permite a confiança em provedores de nuvem [Rawat e Alshaikhi 2018]. Boudguiga *et al.* apresentam uma solução para atualizar dispositivos IoT através de informações armazenadas na corrente de blocos [Boudguiga et al. 2017]. Diferente dos trabalhos citados, a proposta apresentada nesta dissertação fornece uma arquitetura de fatias de rede baseadas em corrente de blocos que busca englobar todas as aplicações de corrente de blocos que envolvem ambientes multi-domínio e multi-inquilino.

Outros trabalhos investigam o problema de vulnerabilidades de segurança

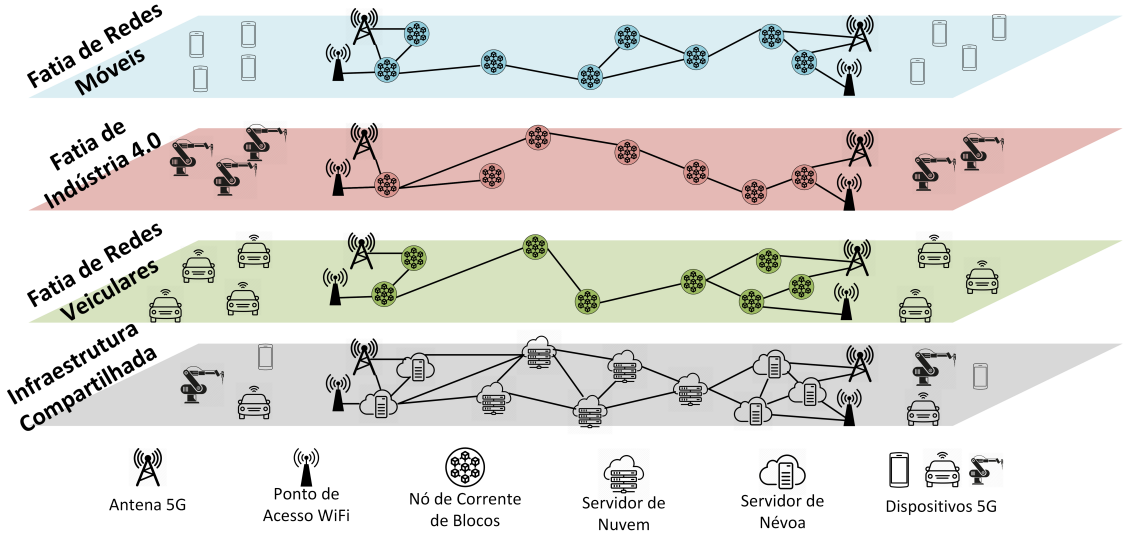

Figura 2. Fatias de rede isoladas através de corrente de blocos em uma infraestrutura física compartilhada. Cada fatia de rede é adaptada às necessidades de um caso de uso.

em ambientes NFV multi-inquilino e multidomínio [Pattaranantakul et al. 2018, Paladi et al. 2018]. Os autores mostram que a confiança nos provedores de nuvem é incerta e que o comprometimento de uma única VNF no núcleo da rede põe em risco todo o serviço fim-a-fim, porém não propõem soluções para o problema. Bozic *et al.* propõem uma arquitetura para gerenciar estados de execução de máquinas virtuais usando um sistema baseado em corrente de blocos [Bozic et al. 2017]. O sistema usa uma estrutura de corrente de blocos para registrar as instruções do hipervisor de virtualização do sistema na forma de transações. No entanto, o trabalho limita-se a proteger operações de máquinas virtuais em centros de dados, não tratando a segurança de uma fatia de rede composta por múltiplas funções de rede em domínios concorrentes.

Com relação à segurança do fatiamento de rede, Bordel *et al.* propõem uma solução baseada em geradores de números pseudo-aleatórios para fornecer segurança dentro de fatias de rede para dispositivos IoT e estações-base em sistemas 5G [Bordel et al. 2018]. Khettab *et al.* propõem utilizar tecnologias NFV e SDN para proteger fatias de rede de múltiplos domínios instanciando funções de rede de segurança, como *firewalls* e sistemas de detecção de intrusão [Khettab et al. 2018]. As soluções propostas, no entanto, são vulneráveis aos possíveis comportamentos maliciosos de provedores de nuvem apontados por [Pattaranantakul et al. 2018] e [Paladi et al. 2018].

Outros trabalhos propõem o uso de corrente de blocos para prover confiança nos administradores de rede e intermediários responsáveis pelo fatiamento da rede. Valtanen *et al.* analisam o uso de corrente de blocos em provedores de fatia de rede para coletar, configurar e alocar recursos em automação industrial [Valtanen et al. 2018]. O artigo aponta as vantagens de usar corrente de blocos em casos de uso do 5G. Backman *et al.* propõem o uso de corrente de blocos para gerenciar recursos de rede 5G virtualizados em um cenário de múltiplos administradores [Backman et al. 2017]. Esta dissertação baseia-se em algumas das descobertas desses trabalhos para propor soluções. Portanto, no melhor conhecimento do autor desta dissertação, este é o primeiro trabalho a propor

uma arquitetura baseada em corrente de blocos para prover a auditabilidade da criação de fatias de redes e também a atualização das funções de rede das fatias isoladas. A proposta atende ao ambiente multi-inquilino e multidomínio sem confiança entre os pares.

4. Resultados Obtidos e Subprodutos do Trabalho

O estudo realizado na primeira parte desta dissertação serviu de base para dois minicursos apresentados em congressos nacionais: i) o minicurso "Segurança na Internet do Futuro: Provendo Confiança Distribuída através de Correntes de Blocos na Virtualização de Funções de Rede", apresentado no Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2019); e ii) o minicurso "Correntes de Blocos: Algoritmos de Consenso e Implementação na Plataforma Hyperledger Fabric", apresentado no Congresso da Sociedade Brasileira de Computação (CSBC 2019).

A pesquisa sobre aplicação de corrente de blocos em redes virtualizadas, realizada na segunda parte do trabalho, recebeu dois prêmios de melhor artigo consecutivos nas primeiras edições do Workshop em Blockchain do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (WBlockchain SBRC 2018 e 2019) com os artigos "SINFONIA: Gerenciamento Seguro de Funções Virtualizadas de Rede através de Corrente de Blocos" e "Provendo uma Infraestrutura de Software Fatiada, Isolada e Segura de Funções Virtuais através da Tecnologia de Corrente de Blocos", respectivamente. Cada um dos artigos premiados possui códigos completos disponíveis ao público[2].

A dissertação completa representa um conjunto de seis publicações principais, listadas a seguir em ordem temporal:

- Rebello, G. A. F., Camilo, G. F., Silva, L. G. C., Souza, L. A. C., Guimarães, L. C. B., Alchieri, E. A. P., Greve, F. G. P. and Duarte, O. C. M. B. - "Correntes de Blocos: Algoritmos de Consenso e Implementação na Plataforma Hyperledger Fabric", in 38º Jornada de Atualização em Informática (JAI) do XXXIX Congresso da Sociedade Brasileira de Computação (CSBC 2019), Belém, July 2019;
- Rebello, G. A. F., Alvarenga, I. D., Sanz, I. J. and Duarte, O. C. M. B. - "BSec-NFVO: A Blockchain-based Security for Network Function Virtualization Orchestration", in IEEE International Conference on Communications (ICC 2019), Shanghai, China, May 2019;
- Rebello, G. A. F., Camilo, G. F., Silva, L. G. C., Guimarães, L. C. B., Souza, L. A. C., Alvarenga, I. D. and Duarte, O. C. M. B. - "Providing a Sliced, Secure, and Isolated Software Infrastructure of Virtual Functions Through Blockchain Technology", in IEEE International Conference on High Performance Switching and Routing (HPSR 2019), Xi'An, China, May 2019;
- Rebello, G. A. F., Camilo, G. F., Silva, L. G. C., Guimarães, L. C. B., Souza, L. A. C., Alvarenga, I. D. and Duarte, O. C. M. B. - "Provendo uma Infraestrutura de Software Fatiada, Isolada e Segura de Funções Virtuais através da Tecnologia de Corrente de Blocos", in II Workshop em Blockchain: Teoria, Tecnologias e Aplicações (WBlockchain SBRC 2019), Gramado, May 2019. Best paper award;
- Rebello, G. A. F., Camilo, G. F., Silva, L. G. C., Souza, L. A. C., Guimarães, L. C. B., and Duarte, O. C. M. B. - "Segurança na Internet do Futuro: Provendo

[2]Códigos disponíveis em `https://github.com/gfrebello/sinfonia` e `https://github.com/gta-ufrj-team/hpsr-smart-contracts`. Acessado em 10 de maio de 2020.

Confiança Distribuída através de Correntes de Blocos na Virtualização de Funções de Rede", in Minicursos do XXXVII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2019), Gramado, Brazil, May 2019;

- Rebello, G. A. F., Alvarenga, I. D., Sanz, I. J., e Duarte, O. C. M. B. "SINFONIA: Gerenciamento Seguro de Funções Virtualizadas de Rede através de Corrente de Blocos", em I Workshop em Blockchain: Teoria, Tecnologias e Aplicações (WBlockchain - SBRC 2018). Campos do Jordão, Brasil. Best paper award.

Referências

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

Backman, J., Yrjölä, S., Valtanen, K. e Mämmelä, O. (2017). Blockchain network slice broker in 5G: Slice leasing in factory of the future use case. Em *Internet of Things Business Models, Users, and Networks*, páginas 1–8.

Bessani, A., Sousa, J. e Alchieri, E. (2014). State machine replication for the masses with BFT-SMaRt. Em *IEEE/IFIP Int. Conf. on Dependable Systems and Networks (DSN)*.

Bhamare, D., Jain, R., Samaka, M. e Erbad, A. (2016). A survey on service function chaining. *Journal of Network and Computer Applications*, 75:138–155.

Bordel, B., Orúe, A. B., Alcarria, R. e Sánchez-De-Rivera, D. (2018). An intra-slice security solution for emerging 5G networks based on pseudo-random number generators. *IEEE Access*, 6:16149–16164.

Boudguiga, A., Bouzerna, N., Granboulan, L., Olivereau, A., Quesnel, F., Roger, A. e Sirdey, R. (2017). Towards better availability and accountability for IoT updates by means of a blockchain. Em *IEEE EuroS&PW*, páginas 50–58.

Bozic, N., Pujolle, G. e Secci, S. (2017). Securing virtual machine orchestration with blockchains. Em *1st Cyber Security in Networking Conference*.

Buterin, V. e Griffith, V. (2017). Casper the friendly finality gadget. *arXiv preprint arXiv:1710.09437*.

Cachin, C. e Vukolić, M. (2017). Blockchains consensus protocols in the wild. *arXiv preprint arXiv:1707.01873*.

Capossele, A., Gaglione, A., Nati, M., Conti, M., Lazzeretti, R. e Missier, P. (2018). Leveraging blockchain to enable smart-health applications. Em *IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI)*, páginas 1–6.

Castro, M. e Liskov, B. (1999). Practical byzantine fault tolerance. Em *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, OSDI '99, páginas 173–186, Berkeley, CA, USA. USENIX Association.

Coin Market (2019). Cryptocurrency global charts: Total market capitalization. Relatório técnico, Coin Market. Acessado em 31 de agosto de 2019.

Digiconomist (2019). Bitcoin Energy Consumption Index. Acessado em 31 de agosto de 2019.

Eletrobras (2017). Relatórios de sustentabilidade socioambiental. Relatório técnico, Eletrobras S.A. Acessado em 31 de agosto de 2019.

Eyal, I., Gencer, A. E., Sirer, E. G. e Van Renesse, R. (2016). Bitcoin-ng: A scalable blockchain protocol. Em *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, páginas 45–59.

Glaser, F. (2017). Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis. Em *50th Hawaii International Conference on System Sciences*.

Instituto Brasileiro de Geografia e Estatística (2019). Produto interno bruto - PIB. Acessado em 31 de agosto de 2019.

Khettab, Y., Bagaa, M., Dutra, D. L. C., Taleb, T. e Toumi, N. (2018). Virtual security as a service for 5G verticals. Em *IEEE Wireless Communications and Networking Conference (WCNC)*, páginas 1–6.

Kwon, J. (2014). Tendermint: Consensus without mining. Acessado em 31 de agosto de 2019.

Lamport, L. (1998). The Part-Time Parliament. *ACM Transactions Computer Systems*, 16(2):133–169.

Medhat, A. M., Taleb, T., Elmangoush, A., Carella, G. A., Covaci, S. e Magedanz, T. (2017). Service Function Chaining in Next Generation Networks: State of the Art and Research Challenges. *IEEE Communications Magazine*, 55(2):216–223.

Ministério de Minas e Energia (2017). Anuário estatístico de energia elétrica 2017. Relatório técnico, Ministério de Minas e Energia do Brasil. Acessado em 31 de agosto de 2019.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Acessado em 31 de agosto de 2019.

NXT community (2014). Nxt whitepaper. Acessado em 31 de agosto de 2019.

Ongaro, D. e Ousterhout, J. (2014). In Search of an Understandable Consensus Algorithm. Em *2014 USENIX Annual Technical Conference (USENIX ATC 14)*, páginas 305–319, Philadelphia, PA. USENIX Association.

Ortega, V., Bouchmal, F. e Monserrat, J. F. (2018). Trusted 5G vehicular networks: Blockchains and content-centric networking. *IEEE Vehicular Technology Magazine*, 13(2):121–127.

Paladi, N., Michalas, A. e Hai-Van, D. (2018). Towards secure cloud orchestration for multi-cloud deployments. Em *EuroSys-CrossCloud*.

Pattaranantakul, M., He, R., Song, Q., Zhang, Z. e Meddahi, A. (2018). NFV security survey: From use case driven threat analysis to state-of-the-art countermeasures. *IEEE Communications Surveys & Tutorials*.

Popov, S. (2017). The Tangle. *cit. on*, página 131. Acessado em 31 de agosto de 2019.

Rawat, D. B. e Alshaikhi, A. (2018). Leveraging distributed blockchain-based scheme for wireless network virtualization with security and QoS constraints. Em *International Conference on Computing, Networking and Communications (ICNC)*.

Thuemmler, C., Rolffs, C., Bollmann, A., Hindricks, G. e Buchanan, W. (2018). Requirements for 5G based telemetric cardiac monitoring. Em *14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*.

Valtanen, K., Backman, J. e Yrjölä, S. (2018). Creating value through blockchain powered resource configurations: Analysis of 5G network slice brokering case. Em *IEEE WCNCW'18*, páginas 185–190.

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Acessado em 31 de agosto de 2019.

Xiao, Y., Zhang, N., Lou, W. e Hou, Y. T. (2019). A survey of distributed consensus protocols for blockchain networks. *CoRR*, abs/1904.04098.

Yahiatene, Y. e Rachedi, A. (2018). Towards a blockchain and software-defined vehicular networks approaches to secure vehicular social network. Em *IEEE Conference on Standards for Communications and Networking (CSCN)*, páginas 1–7.