UNIVERSIDADE FEDERAL FLUMINENSE

ERIC ZANGHI

SISTEMA COLABORATIVO DE MEDIÇÃO INTELIGENTE PARA REDES ELÉTRICAS USANDO BLOCKCHAIN

Niterói

2019

UNIVERSIDADE FEDERAL FLUMINENSE

ERIC ZANGHI

SISTEMA COLABORATIVO DE MEDIÇÃO INTELIGENTE PARA REDES ELÉTRICAS USANDO BLOCKCHAIN

Tese apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense, como requisito parcial para obtenção do Grau de Doutor em Computação. Área de Concentração: Computação Científica e Sistemas de Potência.

Orientadores:
Prof. Milton Brown Do Coutto Filho
Prof. Júlio Cesar Stacchini de Souza

Niterói
2019

Ficha catalográfica automática - SDC/BEE
Gerada com informações fornecidas pelo autor

Z29s Zanghi, ERIC
Sistema colaborativo de medição inteligente para redes elétricas usando Blockchain / ERIC Zanghi ; Milton Brown Do Coutto Filho, orientador ; Julio Cesar Stacchini de Souza, coorientador. Niterói, 2019.
184 f. : il.

Tese (doutorado)-Universidade Federal Fluminense, Niterói, 2019.

DOI: http://dx.doi.org/10.22409/PGC.2019.d.04535817731

1. Sistemas de potência. 2. Redes elétricas inteligentes. 3. Processamento distribuído. 4. Comunicação de dados. 5. Produção intelectual. I. Coutto Filho, Milton Brown Do, orientador. II. Souza, Julio Cesar Stacchini de, coorientador. III. Universidade Federal Fluminense. Instituto de Computação. IV. Título.

CDD -

Bibliotecária responsável: Fabiana Menezes Santos da Silva - CRB7/5274

ERIC ZANGHI

SISTEMA COLABORATIVO DE MEDIÇÃO INTELIGENTE PARA REDES ELÉTRICAS USANDO BLOCKCHAIN

Tese apresentada ao Programa de Pós-Graduação em Computação da Universidade Federal Fluminense, como requisito parcial para obtenção do Grau de Doutor em Computação. Área de Concentração: COMPUTAÇÃO CIENTÍFICA E SISTEMAS DE POTÊNCIA.

Aprovada em 11 de Julho de 2019.

BANCA EXAMINADORA

Milton Brown Do Coutto Filho, D.Sc. - UFF - Orientador

Julio Cesar Stacchini de Souza, D.Sc. - UFF - Orientador

Célio Vinicius Neves de Albuquerque, Ph.D. - UFF

Antônio Augusto de Aragão Rocha, D.Sc. - UFF

Reinaldo Castro Souza, Ph.D. - PUC-Rio

Tatiana Mariano Lessa de Assis, D.Sc. - COPPE/UFRJ

Alexandre Pinto Alves da Silva, Ph.D. - Vale S.A.

Niterói, 2019

"Truth is ever to be found in simplicity, and not in the multiplicity and confusion of things."

Sir Isaac Newton

À minha amada esposa

AGRADECIMENTOS

Agradeço a meus pais que foram fundamentais pela minha formação como indivíduo. Pelos seus esforços em conseguir o melhor com tão pouco. Pelos preceitos éticos e morais que nortearam minha vida.

Agradeço à minha esposa pelos anos de dedicação e energia emocional doada com tanto amor e compreensão. Pela força diária e abnegação, aceitando minhas escolhas como as suas próprias.

Agradeço aos meus orientadores que com sabedoria, inteligência e dedicação à profissão, me deram a oportunidade de continuar a minha trajetória acadêmica. Sua compreensão dos percalços e dificuldades da vida, me permitiram concluir esta grande etapa de minha jornada, que sem dúvida, foi enriquecedora e desafiadora.

RESUMO

A medição de energia é uma das questões mais importantes no ambiente atual das redes elétricas. A qualidade do serviço oferecido pelas concessionárias de energia elétrica tem sido avaliada modernamente com base na exploração de tecnologia aplicada na medição em sistemas de distribuição de média e baixa tensão. Especificamente em redes de baixa tensão, a grande quantidade de medidores nas regiões urbanas e, por outro lado a sua pouca quantidade em regiões rurais, geram alta complexidade para a implementação de medição remota. Tal fato abre uma gama de possíveis soluções para o problema, fruto de intensas pesquisas multidisciplinares.

Esta tese apresenta novas ideias para a medição remota e objetiva fornecer elementos para a construção de sistemas de medição remota que enfrentem o problema de aquisição distribuída e massiva de dados em redes elétricas que agregam novas tecnologias. Assim sendo, propõe-se aqui um Sistema Colaborativo de Medição Inteligente (SCMI), com base na tecnologia conhecida por Cadeia de Blocos (Blockchain), constituindo-se em ferramenta operacional importante para auxiliar concessionárias de energia elétrica a atingirem índices de qualidade de serviço estabelecidos por órgãos reguladores. Por meio de sistemas colaborativos, a solução proposta leva a investimentos substancialmente menores em custos de implementação e manutenção de infraestruturas de comunicação.

A abordagem proposta foi validada como “prova de conceito”, a partir da construção de um simulador do SCMI, tendo sido realizados testes correspondendo a diferentes situações adversas nas quais o sistema pode estar exposto. Os resultados obtidos evidenciam o potencial da abordagem proposta como solução para a aquisição, validação e comunicação de dados em redes elétricas modernas.

Palavras-chave: blockchain, engajamento do consumidor, redes colaborativas, redes inteligentes, sistemas de potência.

ABSTRACT

The energy metering is one of the most important issues in the present environment of electric networks. The quality of service (QoS) offered by the energy utilities has been nowadays evaluated by means of the technology applied in metering of medium/low voltage distribution systems. Specifically in low voltage networks, the large number of meters in urban regions and, in contrast, small number in rural ones, generate high complexity for the implementation of remote metering. This problem opens up a range of possible solutions as result of intensive researches in multidisciplinary areas.

This thesis presents new ideas for remote measurement and aims to provide elements for the construction of remote metering systems that address the problem of massive and distributed data acquisition in electrical networks that use an integrated set of technologies. Therefore, a Collaborative Intelligent Measurement System (CIMS), based on the technology known as Blockchain, is proposed as an important operational tool to assist electric power concessionaires in achieving quality of service indices established by regulatory agencies. Through collaborative systems, the proposed solution leads to substantially lower investments in implementation costs and maintenance of communication infrastructures.

The proposed approach was validated with a “proof-of-concept” to demonstrate its practical potential, from the construction of an CIMS simulator. Several tests were performed considering different situations to which the system can be exposed. The results show the feasibility of the proposed methodology in terms of its application for the acquisition, validation and communication of data in modern networks.

Keywords: blockchain, collaborative networks, consumer engagement, power systems, smart grid.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS

ADMS	*Advanced Distribution Management System*
AMI	*Advanced Metering Infrastructure*
AMR	*Automatic Meter Reading*
BC	*Blockchain*
BLE	*Bluetooth Low Energy*
BT	*Bluetooth*
CAPEX	*Capital Expenditure*
CC	Centro de Controle
CI	Contrato Inteligente
DMS	*Distribution Management System*
GIS	*Geographic Information System*
GPS	*Global Positioning System*
GUI	*Graphical User interface*
HIF	*High Impedance Faults*
IDE	*Integrated Development Environment*
IED	*Intelligent Electronic Device*
IoT	*Internet of Things*
KPI	*Key Performance Indicator*
LAN	*Local Area Network*
OPEX	*Operational Expenditure*
PLC	*Power Line Communications*
RC	Redes Colaborativas
SCADA	*Supervisory Control and Data Acquisition*
SCMI	Sistema Colaborativo de Medição Inteligente
SG	*Smart Grids* (Redes Inteligentes)
SIC	*Smart Intelligent Client*
SMC	*Smart Maintenance Client*
SS	Subestação Secundária
SVC	*Smart Vehicular Client*
THD	*Total Harmonic Distortion*
UTR	Unidade Terminal Remota
WAN	*Wide Area Network*

Capítulo 1

Introdução

1.1 CONSIDERAÇÕES INICIAIS

O amplo uso da energia elétrica, associado a exigentes padrões de qualidade e continuidade de fornecimento, torna complexo o planejamento, implantação, manutenção e monitoramento dos modernos sistemas de geração, transmissão e distribuição.

Os sistemas de energia elétrica do século XXI estão mudando gradualmente. A incorporação de inovações constantes busca viabilizar a construção das chamadas redes inteligentes (s*mart grids* - SGs): redes de energia eficientes e confiáveis que integram tecnologias digitais avançadas. Nesta tese, tais redes serão referidas como SGs. As transformações modernizadoras em andamento no setor de energia estão particularmente relacionadas ao estabelecimento de redes de comunicação integradas e abrangentes, suportando operações mais automatizadas, que permitirão à rede elétrica ser vista como mais inteligente.

A modernização da rede objetiva notadamente a redução da frequência e da duração das interrupções de energia, restaurando os sistemas mais rapidamente e melhorando continuamente a qualidade de serviço das concessionárias. No campo das SGs, problemas relacionados ao atendimento dos requisitos de qualidade de serviço em sistemas complexos de automação e monitoramento têm sido estudados de forma recorrente (CLARIZIA, GALLO, *et al.*, 2016), (FAN, KULKARNI, *et al.*, 2013). Comumente, as concessionárias acompanham de perto os índices de confiabilidade da distribuição de energia para avaliar o desempenho do sistema. Esse fato levou a indústria a perseguir soluções técnicas para problemas de telemedição, tais como a capilaridade, segurança e robustez. Além disso, há a necessidade de fortalecer, transformar e melhorar a infraestrutura de eletricidade para garantir o acesso a fontes de energia confiáveis, seguras e limpas. Para atingir esse objetivo, novos desafios emergentes relativos à introdução de recursos energéticos distribuídos - RED (RUSCHEL, MORO, *et al.*, 2018), segurança do sistema e privacidade das

informações dos consumidores, são adicionados à questão da qualidade de serviços e aos aspectos econômicos.

Escolher uma rede de comunicação apropriada é tarefa difícil que envolve aspectos-chave: quantidade expressiva de transferência de dados, restrição no acesso aos dados, acesso à informação do consumo do cliente, autenticidade dos dados, confidencialidade dos dados sensíveis e viabilização de expansões futuras. Soma-se a isto que os grandes centros urbanos demandam requisitos próprios (e.g., alta confiabilidade, porte, segurança). As chamadas áreas geográficas de alto risco, muitas vezes sem infraestrutura adequada e/ou com altos índices de criminalidade, são obstáculos reais para a leitura e manutenção dos ativos de medição. Estes problemas podem dificultar o acesso a certas partes da rede, em particular no que tange à aquisição de dados, medições e inspeções, que muitas vezes se destinam à avaliação de perdas técnicas e de comercialização. As soluções até então propostas para as redes de comunicação em SGs não têm sido satisfatórias, com limitações comentadas no próximo capítulo desta tese.

Para enfrentar os desafios impostos pelos aspectos descritos anteriormente, a incorporação de novas tecnologias se apresenta como promissora alternativa. Recentemente, a tecnologia conhecida por Cadeia de Dados ou Blochchain (usada por exemplo na criação de criptomoedas e banco de dados distribuídos) tem despertado o interesse da indústria e academia pelo seu caráter inovador, que permite realizar a troca de dados através de um ambiente de consenso e segurança mútua entre duas partes, sem intermediação certificada. Tais características são bastante desejáveis para a construção de sistemas colaborativos de medição que necessitam o compartilhamento de dados de forma confiável. Entende-se sistemas colaborativo como aquele que opera em rede com o propósito de otimizar trabalho em equipe, troca de dados/informações, transporte de elementos diversos, etc**.**

1.2 OBJETIVO

Esta tese propõe uma nova metodologia de medição remota, que visa lidar com grandes conjuntos de dados coletados para o monitoramento de SGs, contribuindo para o aperfeiçoamento das atuais soluções adotadas na infraestrutura de medição (*advanced monitoring infrastructure* – AMI), por meio da incorporação de novas tecnologias. A arquitetura de um sistema colaborativo de medição inteligente,

doravante referido como SCMI, será concebida com base na tecnologia Blockchain (ECONOMIST, 2016) (PECK, 2017). Este moderno sistema de medição remota e distribuída para a baixa tensão (BT) e média tensão (MT) torna-se capaz de atender às redes de distribuição de energia elétrica que demandam soluções complexas para o gerenciamento de seus dados, podendo estas estar inseridas em contextos de grande dificuldade logística e em mercados de multiagentes comercializadores de energia.

Para validar a abordagem proposta foi construído um simulador do SCMI e realizados testes como “prova de conceito”, referentes à confiabilidade e desempenho do sistema.

Ressalta-se que a solução de telemedição proposta neste trabalho se baseia no emprego de tecnologias inovadoras para o atendimento de requisitos de SGs, permitindo:

- O tratamento de grande quantidade de dados telemétricos distribuídos geograficamente ao longo das redes elétricas;
- A otimização de investimentos em infraestrutura de telecomunicações;
- A inserção de inteligência distribuída para a filtragem de informações;
- A implantação de medição remota e colaborativa em modelos de mercado multiagentes;
- O compartilhamento de serviços essenciais ao transporte de dados para a comercialização de energia;
- A garantia da segurança e integridade dos dados do início ao fim do processo de telemedição.

1.3 ARTIGOS ASSOCIADOS

Este trabalho de pesquisa gerou até o presente momento a seguinte publicação em periódico internacional especializado:

- E. Zanghi, M. B. Do Coutto Filho, J. C. Stacchini de Souza, "Conceptual Framework for Blockchain-Based Metering Systems", Multiagent and Grid Systems (MAGS), vol. 15, no. 1, pp. 77-97, Mar 2019.

Adicionalmente, o seguinte artigo obteve a aprovação de seu resumo submetido a *Power Systems Computation Conference* (PSCC), Porto, Portugal:

E. Zanghi, M. B. Do Coutto Filho, J. C. Stacchini de Souza, "Towards a Collaborative Smart Metering System Exploring Blockchain Technology".

1.4 ESTRUTURA DA TESE

Este manuscrito estrutura-se da seguinte maneira:

No Capítulo 2 são apresentados conceitos relativos a SGs, soluções técnicas atuais para os problemas de medição remota e aspectos técnico-econômicos de suas implementações.

No Capítulo 3 descreve-se o cenário atual dos sistemas colaborativos e suas diversas aplicações.

No Capítulo 4 mostra-se como a solução de medição remota SCMI pode ser implementada na prática em sistemas de distribuição hoje existentes.

No Capítulo 5 são detalhados todos os tópicos da inovação proposta. A aplicação da tecnologia Blockchain será abordada, enfatizando-se métodos, algoritmos criados e processos de mineração.

No Capítulo 6 são descritos os simuladores criados para a realização de uma "prova de conceito" referente à abordagem proposta na tese, bem como os principais resultados ilustrativos e numéricos do sistema de medição baseado em Blockchain.

No Capítulo 7 são resumidas as principais contribuições provenientes do uso do SCMI e apresentadas ideias para trabalhos futuros.

Capítulo 2

Redes Inteligentes

2.1 INTRODUÇÃO

As redes inteligentes (SGs), interpretadas como redes de energia eficientes e confiáveis que integram tecnologias digitais avançadas, destinadas à distribuição de energia elétrica vêm recebendo investimentos financeiros constantes para seu desenvolvimento, implantação e alcance, até mesmo em áreas mais carentes de serviços públicos. O presente capítulo reúne elementos descritivos de SGs, com o propósito de abordar os problemas de telemedição hoje enfrentados neste campo de pesquisa. A complexidade típica destas redes é descrita e suas características apontadas de maneira didática, desde seus princípios mais básicos.

Os sistemas que integram as SGs (M. ANNASWAMY e AMIN, 2013) são complexos, de porte variado, isolados ou interconectados, conforme ilustrado na Figura 2-1, com destaque para o uso de inteligência e sistemas computacionais de apoio à operação, manutenção e gestão, geralmente destinados a aumentar a disponibilidade e qualidade dos sistemas elétricos.

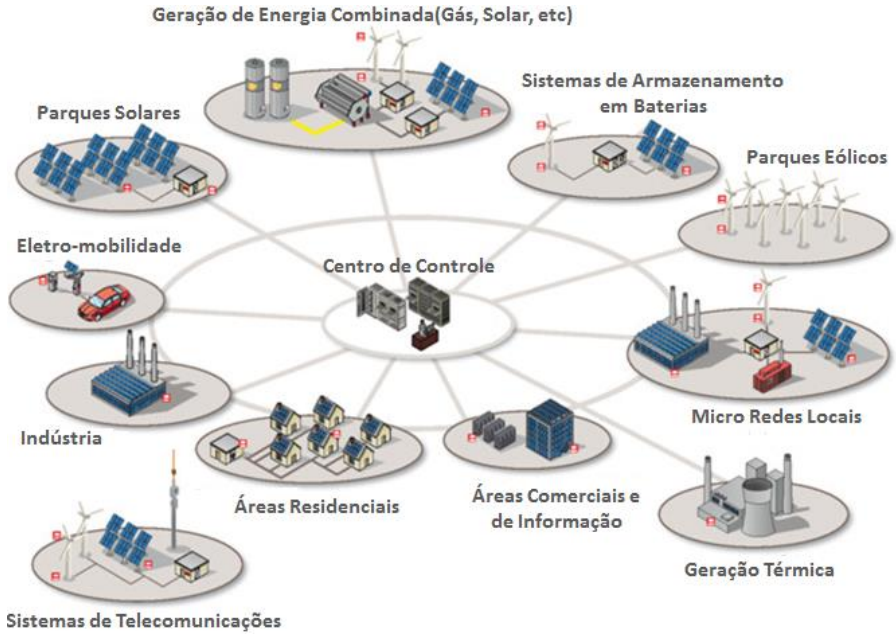


Figura 2-1: Sistema típico de integrantes de SGs (M. ANNASWAMY e AMIN, 2013)

Apesar de existirem diversas propostas de arquiteturas inovadoras de SGs (TREFKE, ROHJANS, *et al.*, 2013), alguns pré-requisitos permanecem inalterados para seu bom funcionamento, tais como os apontados a seguir:

- Capacidade de **comunicação** entre os dispositivos eletrônicos inteligentes e/ou entre estes dispositivos e um ou mais centros de processamento de dados, também chamados de Centros de Controle (CCs). A comunicação pode ser realizada através de redes do tipo WAN/LAN ou redes seriais por meio de fibras óticas ou via rádios (GUNGOR, SAHIN, *et al.*, 2011).

- O **Monitoramento** de todas as grandezas elétricas úteis para a operação e demais dados importantes de um sistema, tais como dados topológicos (estado de chaves e disjuntores). Os CCs são responsáveis pela coleta e análise de dados, e consequente tomada de ações operacionais de rotina ou contingência. Nos CCs, sistemas de supervisão (DMS/ADMS) e sistemas especialistas analisam a grande massa de dados dos SGs e realizam tarefas automáticas ou de apoio à operação (ARRIGONI, BIGOLONI, *et al.*, 2016). Com o aumento dos pontos de supervisão e controle, se tornou humanamente impossível a operação das SGs sem um auxílio computacional inteligente.

- Capacidade de poder considerar os clientes consumidores como **geradores independentes** de energia para a rede. A flexibilidade de geração pode ser controlada remotamente pelas subestações secundárias ou pelos próprios CCs em diversos tipos de métodos, inclusive com algoritmos preditivos (IRIA, SOARES e MATOS, 2017).

- Capacidade de gestão da **geração de energia distribuída** (GED) (RUSCHEL, MORO, *et al.*, 2018), controlando a disponibilidade de produção de energia nas redes de média e baixa tensão. Conforme as necessidades do sistema, as SGs devem ser capazes de gerenciar o armazenamento de energia excedente não consumida para ação contingencial futura.

- Capacidade de **recomposição automática**, também chamado de "*self healing"* (FERREIRA, SIEBERT, *et al.*, 2013) que se faz fundamental em sistemas de grande porte, tais como as redes dos grandes centros urbanos, possibilitando o comando e controle sem intervenção humana. A reconfiguração autômona

torna-se importante na mitigação de efeitos negativos nas interrupções de fornecimento de energia, podendo minimizar a quantidade de clientes afetados e o tempo de permanência das interrupções. Por ser um tema central na manutenção de bons índices de desempenho nas redes de distribuição, há diversas soluções para este problema descritas em vasta literatura (ELGENEDY, MASSOUD e AHMED, 2015).

- Capacidade de **gerenciamento,** armazenamento e processamento da grande massa de dados gerados pelos sistemas de monitoramento das SGs. A quantidade sempre crescente de informações, gera um dos principais problemas nas novas redes inteligentes e demanda auxílio multidisciplinar para a sua solução (BAEK, VU, *et al.*, 2015). A filtragem das informações e as tomadas de decisão automáticas são temas de pesquisa fundamentais ainda sem soluções de fácil implementação.

- **Disponibilidade/Confiabilidade** dos dados coletados para utilização em tempo real ou em modo de estudo (dados históricos). As informações devem estar nos centros de controle quando são necessárias e com informações fidedignas e com origem comprovada. Este se constitui em um dos aspectos de difícil implementação, levando as concessionárias a investir pesadamente em sistemas proprietários, com redes de dados isoladas, que evitem acesso externo.

As SGs possuem vários elementos fundamentais, responsáveis pela medição, controle, proteção (*Intelligent Electronic Devices* - IEDs) e comunicação, sendo que muitos outros são criados e também novas funcionalidades adicionadas às já existentes. Alguns destes elementos são elencados abaixo:

a) **Geração Distribuída:** diversas formas de geração podem ser utilizadas em SGs, tais como: geração eólica, solar, PCHs (Pequenas Centrais Hidroelétricas), biomassa, gás, carvão, maré-motriz, etc.**;**

b) **Unidades de Armazenamento de Energia**: sistemas de armazenamento de energia de corrente contínua para utilização programada e inteligente;

c) **Veículos Elétricos:** são considerados prosumidores nas SGs por consumirem energia da rede para carregar suas baterias e por também possuírem a capacidade de exportar a energia armazenada de volta para a rede (GRACKOVA, OLEINIKOVA e KLAVS, 2015). Seu impacto nas redes de distribuição já é substancial e digno de estudos aprofundados, devido ao crescimento exponencial de sua implementação nos países mais desenvolvidos;

d) **Relés de Proteção:** estes IEDs são responsáveis pela identificação de curtos-circuitos ou distúrbios elétricos no sistema, cabendo-lhes isolar falhas elétricas através da abertura de disjuntores/chaves;

e) **Controle e Medição (unidades terminais remotas - UTRs)**: IEDs responsáveis pela abertura e fechamento de chaves (Figura 2-2.A) e religadores (Figura 2-2.B) para a reconfiguração da rede, atendendo a uma condição operacional ou contingencial por conta da falha ocorrida no sistema. Também efetuam medições de grandezas elétricas de transformadores e linhas de distribuição;

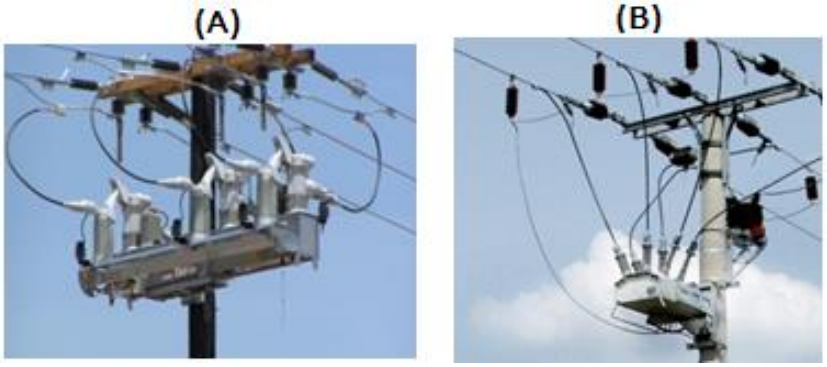


Figura 2-2: Chave de Corte (A) e Religador (B)

f) **Medidores Inteligentes**: estes elementos podem estar distribuídos ao longo da rede de maneira independente ou embutidos nos próprios IEDs de proteção e controle que geralmente possuem função de medição trifásica de grandezas elétricas. Eles fazem parte da chamada AMI (*Advanced Metering Infrastructure*). Os medidores inteligentes (JIXUAN ZHENG, GAO e LI LIN, 2013), ilustrados na Figura 2-3, são essenciais para o monitoramento dos sistemas elétricos quanto aos valores de tensão, corrente, potência e qualidade de energia;

Figura 2-3: Medidores Inteligentes

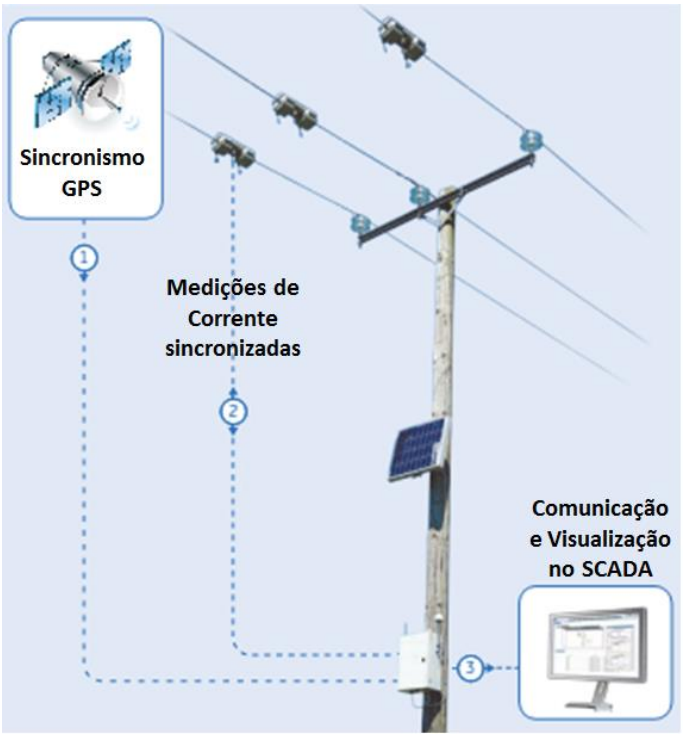


Figura 2-4: Sistema GE ILMS - Intelligent Line Monitoring System

g) **Subsistemas de localização de Falhas**: Estes sistemas são compostos de sensores, rádios e GPS para sincronização e possuem a finalidade de medição e identificação de curtos-circuitos ou mudanças bruscas das grandezas elétricas na rede de distribuição e subtransmissão. Estes sistemas funcionam como unidades de medição fasorial (UMFs) para redes de distribuição (THOLOMIER, KANG e CVOROVIC, 2009), (MANTUANO FILHO, SOLLERO, *et al.*, 2005). A Figura 2-4 ilustra um destes subsistemas.

h) **Rádios:** estes dispositivos estão presentes em todos os pontos de medição e também nos pontos de controle, a fim de transmitir as informações de cada

elemento da SG para os concentradores de dados e/ou para os CCs. Há rádios com tecnologia Mesh RF (MALANDRA e SANSO, 2017), Ponto-Multiponto (KIM, FONSECA, *et al.*, 2007) e GPRS conforme as necessidades e possibilidades geográficas da localização do elemento inteligente da rede;

i) **Redes de dados**: as SGs podem possuir diversos tipos de redes dentre três grupos bem definidos, a saber: redes de aquisição de dados dos elementos sensores; redes de distribuição de dados entre os elementos do SG; e redes de transmissão de dados para os CCs. Cada uma destas redes deve apresentar conjuntos de dispositivos que possibilitem a comunicação segura e confiável para a integração com a SG.

2.2 COMUNICAÇÃO DE DADOS

Quando se analisa o problema da comunicação entre os elementos de uma SG e seus CCs, pode-se traçar um paralelo com a própria topologia do sistema elétrico de distribuição. Fisicamente, a instalação dos elementos de comunicação de dados, utilizando cabos de fibra ótica ou cobre, apresenta problemas semelhantes aos encontrados no sistema radial de distribuição, visto que as suas linhas de distribuição de energia são utilizadas muitas vezes também como rota das suas linhas de transmissão de dados.

Na atualidade, existem diversas tecnologias que podem tentar evitar problemas de perda de comunicação por distúrbios topológicos na transmissão de dados, porém, não levam o sistema a 100% de disponibilidade. O cenário de uma grande massa de dados provenientes dos elementos de SGs e a diversidade das condições geográficas onde eles estão instalados impõem um grande desafio para a solução eficiente dos problemas de comunicação em tempo real (ou pelo menos próximo a isto), tendo sempre presente a questão da segurança e integridade das informações essenciais ao transporte de dados (WANG, XU e KHANNA, 2011).

Um dos importantes subsistemas de uma SG são as redes de medição tipo AMR (*automatic meter reading*) (YAN, QIAN, *et al.*, 2013), que possuem usualmente milhares de pontos de medição de grandezas elétricas, tais como: corrente, tensão e energia consumida. Essas informações são reunidas em concentradores setoriais, responsáveis por áreas delimitadas. Os concentradores por sua vez, distribuem estas informações para bancos de dados centralizados e responsáveis pelo

armazenamento histórico de informações dos medidores inteligentes. Vale enfatizar que existem premissas importantes para a comunicação em rede AMR, tais como:

- Possibilidade de **inclusão** de novos nós na rede de forma **fácil e rápida**;
- **Confiabilidade** na transmissão de pacotes de **dados**;
- **Robustez** necessária para restabelecimento de rotas, em caso de **perdas de conexão** por motivos diversos;
- Estabelecimento de **comunicação** fim-a-fim entre nós distantes, que podem ser alcançados através de diversos métodos tais como o de busca em profundidade (FINSTER e BAUMGART, 2013) ou por saltos múltiplos entre elementos de rede (BOJKOVIC e BAKMAZ), contanto que produzam **baixa latência**, ou seja, baixo atraso nos pacotes de dados recebidos.

Um dos pilares das SGs modernas é a infraestrutura de medição avançada (AMI), que inclui medidores inteligentes, redes de comunicação, sistemas de gerenciamento de dados de medidores e meios para integrar os dados coletados em plataformas e interfaces de software. As AMIs fornecem um sistema de monitoramento que se estende desde consumidores de energia até um provedor de serviços (YAN, QIAN, *et al.*, 2013), permitindo a comunicação bidirecional. Além disso, o AMI permite a implementação de muitas funções importantes, tais como a medição de consumo de energia (automática e remota) e outras que não estavam disponíveis anteriormente nas AMR, ou que eram realizadas manualmente, como a conexão e desconexão de serviço, detecção de adulterações em dispositivos de medição, identificação e isolamento de equipamentos com falha e monitoramento de tensão com alta frequência de leitura.

Até o momento, as tecnologias empregadas na comunicações das AMIs conectando dispositivos de medição (JIXUAN ZHENG, GAO e LI LIN, 2013) ao centro de controle da concessionária são numerosas: rede de RF, ponto-a-multiponto (KIM, FONSECA, *et al.*, 2007), serviço geral de rádio por pacotes etc. A grande massa de dados a transmitir impõe um grande desafio aos sistemas de comunicação. Portanto, é importante buscar soluções eficientes que atendam adequadamente aos requisitos associados à comunicação em tempo real, bem como à integridade e segurança dos dados.

As atuais infraestruturas de comunicação tipo AMI estão gradualmente substituindo as conhecidas e já largamente implementadas redes de medição AMR. As AMIs possuem comunicação bilateral e conseguem prover mais informações do que as AMRs, além de possibilitar envios de comando ao medidor de energia. Tais comandos são realizados remotamente pelo centro de controle (CC) e são referentes ao desligamento ou religamento do elemento medidor a fim de isolar o cliente da rede ou até mesmo religá-lo.

Alguns protocolos, tais como *Open Smart Grid Protocol* (OSGP), *Power line communication* (PLC) e ZigBee são utilizados mundialmente nas redes AMR e AMI, a fim de atender aos requisitos mínimos necessários. Apesar disto, muitos destes sistemas já implementados são vistos como experimentais e campos de prova para a obtenção de soluções mais robustas e adaptativas. Por essa razão há espaço para a pesquisa de protocolos inovadores que possam atender às diversas necessidades, que muitas vezes apresentam características especiais.

A escolha do protocolo de comunicação tangencia uma série de aspectos importantes, sendo um deles o custo de implementação (CAPEX) e o custo de operação e manutenção do sistema (OPEX). Para a minimização destes custos, devem-se observar os pré-requisitos necessários para a implementação da rede de dados, que podem incluir os custos de alocação de endereços IPs (*Internet Protocol*) para cada dispositivo de rede (e.g., medidores inteligentes), custo de cartões telefônicos (*SIM cards*) para sistemas GPRS e 3G, até o custo de cabeamento de rede para os sistemas de comunicação convencionais e ópticos.

2.2.1 Conceitos Importantes

Face às diversas possibilidades tecnológicas na área de comunicação de dados, vale ressaltar alguns importantes conceitos relacionados a SGs. Estas tecnologias fazem parte de um grande conjunto de soluções que atualmente são utilizadas em diversos mercados, atendendo também às demandas das SGs da atualidade.

Há que se reconhecer a tendência mundial pela integração ampla de tudo o que possui alguma informação e/ou inteligência. A ideia da Internet das Coisas, conhecida pela sigla em inglês IoT – *Internet of Things* (GUPTA e GUPTA, 2016) contribui para a discussão sobre um futuro próximo e promissor. A tecnologia IoT já

está presente nas SGs e requer cuidados na análise das normas (GHATIKAR, 2016) e na interoperabilidade entre os seus elementos para que se mantenha viável, consoante os conceitos descritos nesta seção.

Conforme pode-se ver em (MARINAKIS, WALSH e HARMS, 2017) a quantidade prevista de elementos conectados a redes ao longo dos próximos anos cresce bem mais do que a população mundial não sendo difícil imaginar que estas previsões mudarão a cada ano em consequência dos avanços tecnológicos e sociais que ocorrem de forma crescente. O próprio interesse da população em se conectar local ou remotamente, de maneira mais inteligente e lúdica, a equipamentos presentes em suas casas, transforma a ideia de IoT em uma forte tendência tecnológica mundial.

Quando se trata da comunicação de dados em grande escala e com grande diversidade tecnológica disponível, um dos pontos mais difíceis é a escolha da melhor solução para a transmissão de dados. O mercado de equipamentos e soluções para redes inteligentes têm se focado em redes de baixo alcance, tal como a tecnologia Bluetooth. Dentre os motivos relacionados a tal escolha, destacam-se:

- Fácil utilização dos rádios e do protocolo;
- Grande parque instalado em Smartphones, Tablets e outros dispositivos;
- Capacidade de escalabilidade;
- Tecnologia bem estabelecida desde 2002;
- Tendência de aceitação na indústria de forma crescente.

As especificações do Bluetooth (BLUETOOTH SIG PROPRIETARY, 2014) estão bem consolidadas e contam com grupos de trabalho ativos que proporcionam a evolução da norma de forma bem dinâmica. O grupo do IEEE 802.15 trata de redes sem fios pessoais, as chamadas WPAN (*Wireless Personal Area Network*), sendo a IEEE 802.15.1 especificamente do grupo Bluetooth que também avalia a interferência entre as diversas redes que usam a faixa de 2,4Ghz de frequência abertas para se comunicar.

O Bluetooth SIG (*Special Interest Group*) prevê brevemente grandes avanços na norma devido à grande demanda no mercado de automação residencial, industrial e no crescimento dos sistemas de SGs. Os trabalhos incluem melhorias significativas na tecnologia e dentre os principais avanços previstos encontram-se:

- Aumento da integração do Bluetooth com a filosofia de IoT (PEREIRA, ELIASSON, *et al.*, 2013) e suas funcionalidades;

- Aumento do alcance dos rádios que chegam hoje a pouco mais de 10 metros nos Smartphones e 100m em dispositivos mais complexos tais como notebooks;
- Maior velocidade de transmissão de dados que hoje pode chegar aos 3Mbps;
- Rede Mesh incorporada na própria norma possibilitando uma gama ainda maior de aplicações para as redes Bluetooth. Este tipo de rede ainda se encontra no estado da arte quando se trata de Bluetooth.

Com a evolução do Bluetooth (BT), surgiu em 2010 na versão 4.0, o chamado "*Smart Bluetooth*" ou "*Bluetooth Low Energy* (BLE)" (RAZA, MISRA, *et al.*, 2015). O Bluetooth regular consome muito mais energia do que o BLE (MACKENSEN, LAI e WENDT, 2012) quando está trabalhando em altas taxas de transferência. Por essa razão o BLE é usado comumente em fones de ouvido, em dispositivos de automação residencial, dispositivos na área de saúde tais como medidores de pressão arterial e balanças biométricas a base de baterias e em aplicações que apenas precisam enviar poucas informações e esporadicamente. O BLE apresenta taxas de transferências bem diferentes e quantidade máxima de dispositivos totalmente dependente da aplicação, contrariamente ao Bluetooth tradicional que trabalha com no máximo oito nós (7 escravos e 1 mestre).

Por sua característica principal ser a economia de energia, um dispositivo BLE permanece em modo *IDLE,* que significa "em repouso", durante a maior parte do tempo. Esta tecnologia foi desenvolvida para aplicações que apenas precisam enviar poucas informações, esporadicamente saindo do modo "em repouso" apenas para realizar conexões que duram apenas milissegundos. Dessa forma, se tem um consumo de corrente com picos de até 15 mA, mas com uma média de 1 uA apenas.

2.2.2 Uso de Redes Móveis

As infraestruturas de comunicação existentes, que contemplam os pontos de acesso (*Hotspots*) de internet e as redes celulares móveis, não devem ser ignoradas, pois fornecem tecnologias de troca de dados de forma eficiente e extremamente capilarizada.

Os sistemas de redes móveis celulares em funcionamento variam substancialmente em qualidade e tecnologia dependendo da sua localização geográfica. Sabe-se que há áreas com cobertura plena para serviços 4G, enquanto

que áreas adjacentes não conseguem fornecer sequer sinais 3G para seus usuários, por várias razões. O fator topográfico apresenta-se como um dos principais desafios a serem transpostos para uma cobertura de rede celular, principalmente quando se trata do transporte de dados em que a velocidade e largura de banda devem ser garantidas e estáveis (EL-SAYED e GAGEN, 2012).

Imaginando um cenário de transmissão de dados que se encontra em constante evolução (RAYCHAUDHURI e MANDAYAM, 2012), atualmente há alternativas tecnológicas em software e hardware que trabalham em paralelo dentro dos aparelhos móveis, minimizando a interrupção destes serviços alternando entre as bandas 2G (97 Kbps), Edge (236 Kbps), HPSA (*High Speed Packet Access* - 84Mbps), 3G (até 2Mbps), 4G (até 300 Mbps), 5G (até 20Gbps) (GOHIL, MODI e PATEL, 2013) e Wi-fi IEEE 802.11 (até 6Gbps e evoluindo para 100Gbps). Ou seja, há uma considerável disponibilidade dos serviços de transporte de dados no mercado de telefonia celular, o que pode ser exemplificado pelo sítio disponibilizado pela instituição brasileira reguladora de telecomunicações conhecida por Agência Nacional de Telecomunicações (ANATEL), que informa os tipos de cobertura em cada região através da ferramenta online (AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES - ANATEL, 2015) que permite a visualização da situação atual e histórica de cobertura e falhas na rede móvel celular na respectiva área selecionada, englobando todas as operadoras disponíveis. Na Tabela 2-1 abaixo, pode-se verificar que, tomando como exemplo a cidade de São Paulo (Brasil), entre os anos de 2017 e 2018, a cobertura de dados está acima de 98% em termos de disponibilidade, ou seja, de 100% de tentativas, menos de 2% falham, o que mostra uma grande estabilidade do sistema desta região em particular.

Tabela 2-1: Taxa de conexão de dados (%)

	Set17	Out17	Nov17	Dez17	Jan18	Fev18	Mar18	Abr18	Mai18
ALGAR	98.81	98.72	99.24	98.63	98.66	-	98.02	98.14	98.41
CLARO	98.44	98.29	98.37	98.38	98.43	98.3	98.32	98.61	98.79
NEXTEL	99.91	99.91	99.9	99.89	99.92	99.92	99.91	99.93	99.92
OI	96.85	96.92	96.56	97.05	98.06	98.41	98.53	98.65	98.64
TIM	98.89	98.97	98.94	98.64	98.46	98.86	98.93	99.13	99.26
VIVO	97.97	98.04	98.12	98.09	98.21	98.48	98.5	98.48	98.65

A utilização de redes móveis para a integração das SGs tem se ampliado há alguns anos, mas sempre com enfoques tecnológicos que demandam grandes investimentos em infraestrutura e telecomunicações conforme demonstrado em (SHERRINGTON e DICKS, 2011). Esta área técnica não é o foco de negócios das concessionárias de energia elétrica e gera grandes obstáculos à entrada de novas companhias no mercado. Para atender às complexas legislações locais e englobar tantas competências técnicas, são necessárias empresas de grande porte. A entrada de empresas menores no mercado de telecomunicações, poderia ajudar a capilarizar mais a cobertura destes serviços e provocar a redução de custos, aquecendo a livre concorrência.

2.2.3 Soluções Existentes

Quando são analisados os projetos de integração de redes AMI, contendo UTRs distribuídas em postes e outros elementos das SGs, vê-se que soluções adotadas por diversas concessionárias utilizam tecnologia de transmissão serial e Ethernet de dados através de concentradores, exigindo grande investimento em equipamentos e infraestrutura.

No que tange as soluções tecnológicas aplicadas no Brasil (APARECIDO PELEGRINI e VALE, 2014), pode-se verificar que geralmente adotam-se conexões de dados de telemedição via rádio, sistemas baseados em linhas privadas ou GPRS/GSM com a conexão de cada elemento da SG diretamente ao sistema de dados das operadoras de telefonia. Com isso, cada dispositivo do sistema SG se transforma em um ponto *wireless* no sistema com cartão telefônico (*SIM Card)* próprio. Estes tipos de soluções também necessitam de custosa infraestrutura e apresentam restrições contratuais com as operadoras de telefonia. Além disso, a dependência das empresas de distribuição elétrica às empresas de concessão de telefonia, gera problemas extras na logística de operação, manutenção e na disponibilidade dos sistemas, uma vez que estas empresas estão por vezes desacopladas nos projetos de SGs e normalmente não possuem cooperação tecnológica com as empresas do setor elétrico, sendo uma simples relação cliente/fornecedor.

Sistemas de distribuição que possuem rede subterrânea enfrentam ainda desafios adicionais, pois o uso de tecnologias “sem fio” é de implementação mais

complexa, forçando por vezes uma mescla de soluções (sistemas híbridos) com mídias de propagação diferentes em uma mesma rede.

Algumas soluções utilizam sistemas de comunicação em rádio com tecnologia Mesh (MANTUANO FILHO, SOLLERO, *et al.*, 2005) ou ponto-multiponto (MALANDRA e SANSO, 2017) para a coleta de dados das câmaras subterrâneas e envio destes para os centros de comando.

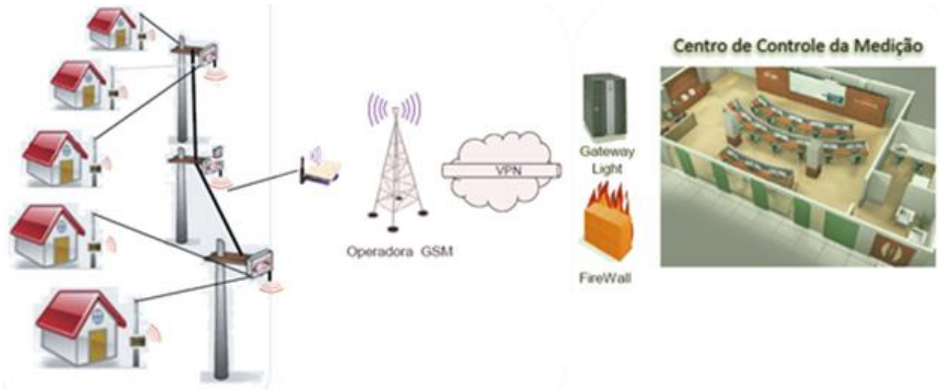


Figura 2-5: Solução GSM atual da concessionária Light

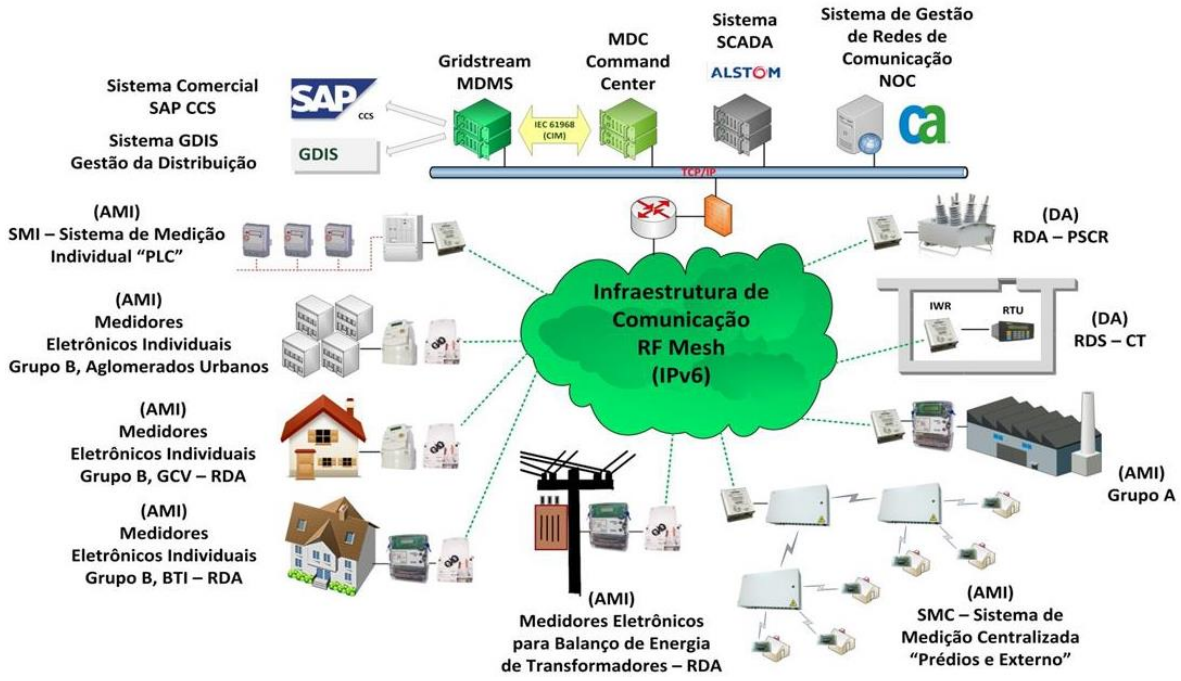


Figura 2-6: Solução MESH RF (IEEE 802.15.4) da concessionária Light

Nas Figura 2-5 e Figura 2-6, encontra-se o exemplo de implementação de SG na concessionária Light (http://redesinteligentesbrasil.org.br/smart-grid-light.html) que atende a cidade do Rio de Janeiro em que se indicam soluções híbridas, utilizando concentradores de dados, wireless e redes PLC, tendo em vista o parque instalado e as dificuldades adicionais encontradas na sua área de abrangência. Partindo de uma

solução dependente das redes GSM (Figura 2-5), a Light persegue atualmente uma solução autônoma do ponto de vista de infraestrutura de telecomunicações (Figura 2-6), utilizando como solução redes tipo Mesh para dispositivos de rádio frequência (RF) de modo a integrar em seu sistema SG 1,6 milhões de medidores inteligentes até 2019.

Um novo exemplo de aplicação é referente à concessionária *Silicon Valley Power* (www.siliconvalleypower) que possui um sistema de medição inteligente com infraestrutura de comunicação tipo Mesh (Figura 2-7) e conexão Wi-fi com pontos coletores proprietários.

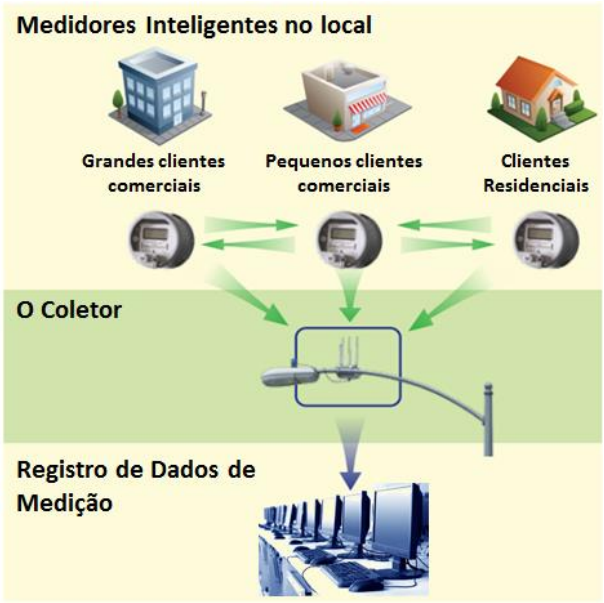


Figura 2-7: AMI da concessionária Silicon Valley Power

Esta solução implantada em Santa Clara na Califórnia (EUA) (ABB INC., 2012) utiliza medidores inteligentes do fabricante Elster com comunicação de média frequência e protocolo proprietário Elster 900 MHz EA_LAN e com protocolo padrão ZigBee em 2,4 GHz de frequência de comunicação. A solução Mesh utilizada, provoca grande número de pacotes trafegados por dia, expondo os moradores a radiação wireless por mais tempo, visto que seu respectivo medidor é utilizado de modo contínuo como ponte de comunicação dos demais medidores adjacentes com o Hotspot Wi-fi coletor. Um outro ponto que vale ressaltar, diz respeito aos custos de implantação. O Hotspot Wi-Fi proprietário na solução da SVP, demanda custo alto de infraestrutura tanto de CAPEX quanto de OPEX pela concessionária, sendo mais um ponto crítico de responsabilidade da concessionária.

Outras soluções mais conservadoras do ponto de vista tecnológico utilizam enlaces físicos de redes com cabeamentos de cobre e/ou óticos para integração dos elementos inteligentes de medição e controle aos centros de concentração de dados e operação. Uma destas soluções é a *Power Line Communication* (PLC) (BERGER, SCHWAGER e ESCUDERO-GARZÁS, 2013), que utiliza as linhas de corrente alternada para a transmissão de dados. O sinal de dados é modulado na própria senoide de tensão nominal da linha como onda portadora (*carrier*), se propagando na linha de transmissão ou de distribuição de energia.

Há muitos anos o *Power-line Carrier Communication* (PLCC) foi o padrão utilizado na comunicação entre subestações de energia para fins de teleproteção com grande confiabilidade. O PLC teve origem e derivou-se desta filosofia, mas a tecnologia adotada sofre por apresentar algumas limitações, tais como: o isolamento dos sinais em ramais que estão entre transformadores de potência; a taxa de transmissão de dados pode chegar somente a alguns megabits por segundo (Mbps). Por esses motivos e questões de regulamentação nos órgãos de telecomunicações, há vertentes no mercado que visam a utilização do PLC mais solidamente em ambientes controláveis e reduzidos. Por isso, esta tecnologia cresceu nas soluções confinadas dentro de construções residenciais e comerciais, a fim de integrar dispositivos de automação residencial, a chamada “Domótica” (e.g.: www.x10.com).

Esta tecnologia ainda enfrenta questões importantes sobre múltiplos padrões não interoperáveis na mesma linha de força e interferências mútuas entre dispositivos (GALLI e SCAGLIONE, 2010).

2.3 INVESTIMENTOS EM TELECOMUNICAÇÕES – CENÁRIO ATUAL

Segundo os relatórios europeus de investimentos (APARECIDO PELEGRINI e VALE, 2014), na implantação em SGs desde 2002, cerca de £3,15 bilhões foram gastos, contabilizando-se todas as fases destes projetos. As despesas relacionadas às instalações das SGs e as despesas operacionais de manutenção e operação dos ativos destes sistemas, são significativas. O relatório do Observatório da Inovação (SHERRINGTON e DICKS, 2011) prevê e analisa projetos de SGs no período de 2012-2030 e estima um CAPEX de cerca de 9% em telecomunicações em países desenvolvidos sobre o total de investimentos na implantação de SGs. Isso representa cerca de £270 milhões, somente de investimentos em estrutura de telecomunicações

mesmo. Considerando que comunicação não é a atividade fim das concessionárias de energia, esses percentuais são consideravelmente altos, como se vê a seguir:

- Serviços de dados GPRS e 3G/4G das concessionárias de telefonia;
- Instalação de equipamentos com modem GPRS ou unidades celulares 3G/4G;
- Instalação de sistemas de rádio com custos adicionais de pesquisa e testes em campo (*site survey*);
- Instalação de equipamentos concentradores de dados;
- Instalação de quilômetros de cabeamentos de rede de cobre e de fibra ótica nos casos de enlaces de comunicação proprietários;
- Aquisição de roteadores e switches de rede;
- Custos altos de operação e manutenção sistemática (OPEX) relacionados ao sistema de telecomunicações.

Vale salientar que em países desenvolvidos, é comum haver instalações bem estabelecidas de fibras óticas e WANs públicas. No caso de países em desenvolvimento, os valores gastos em telecomunicação podem chegar a mais de 20% de todo capital investido, visto que estes se encontram ainda com precária infraestrutura de telecomunicação, ou seja, demandam maiores investimentos para instalar a base mínima para as SGs.

Na Figura 2-8, pode-se observar o cenário da distribuição de investimentos em diversos países (i.e. Brasil, Alemanha, Estados Unidos, etc.) para a implementação de SGs no horizonte de 2012 até 2030 (SHERRINGTON e DICKS, 2011).

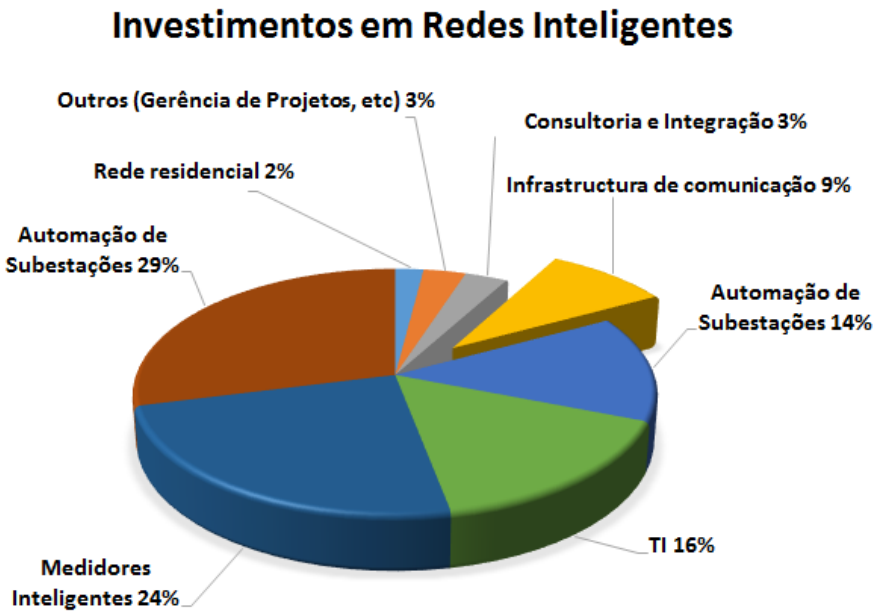


Figura 2-8: Previsões de investimentos em SGs entre 2012-2030 (SHERRINGTON e DICKS, 2011)

Nos países em desenvolvimento, podem-se ver soluções de integração de SGs na África Subsaariana (SMERTNIK, 2014), mais precisamente no Senegal, onde a tecnologia GSM de integração dos medidores inteligentes já é utilizada em conjunto com soluções menos tecnológicas, como o de medidores não inteligentes e pré-pagos. A abordagem *on-grid* (dentro da rede) e *off-grid* (fora da rede) é analisada para justificar a utilização ou não de infraestrutura de comunicação própria (e.g., PLC) ou infraestrutura já existente das operadoras de telefonia via GSM.

Aprofundando-se na problemática de sistemas de comunicação nos países em desenvolvimento, para se ter uma ideia da realidade nestas áreas denominadas de off-grid, ou seja, fora do sistema de distribuição integrada, existem milhões de clientes com acesso a redes GSM, porém, sem acesso à eletricidade. Ampliando-se a área de visão, pode-se verificar em (MULLER, VAN EEDEN, *et al.*, 2015) que no período entre 2000 e 2015, o aumento da cobertura GSM na África Subsaariana foi bem maior do que outros serviços, inclusive o de fornecimento de eletricidade.

Reforçando o entendimento sobre o cenário da penetração dos sistemas de telefonia móvel nas regiões de países em desenvolvimento da África, vê-se na Figura 2-9 que mesmo dentro das populações sem atendimento de eletricidade oficial pelas concessionárias, a disseminação dos serviços de telefonia móvel atinge quase 50% desta população (MULLER, VAN EEDEN, *et al.*, 2015). Nesta realidade, somente 358

milhões possuem acesso à eletricidade de forma oficial pelas concessionárias de energia elétrica.

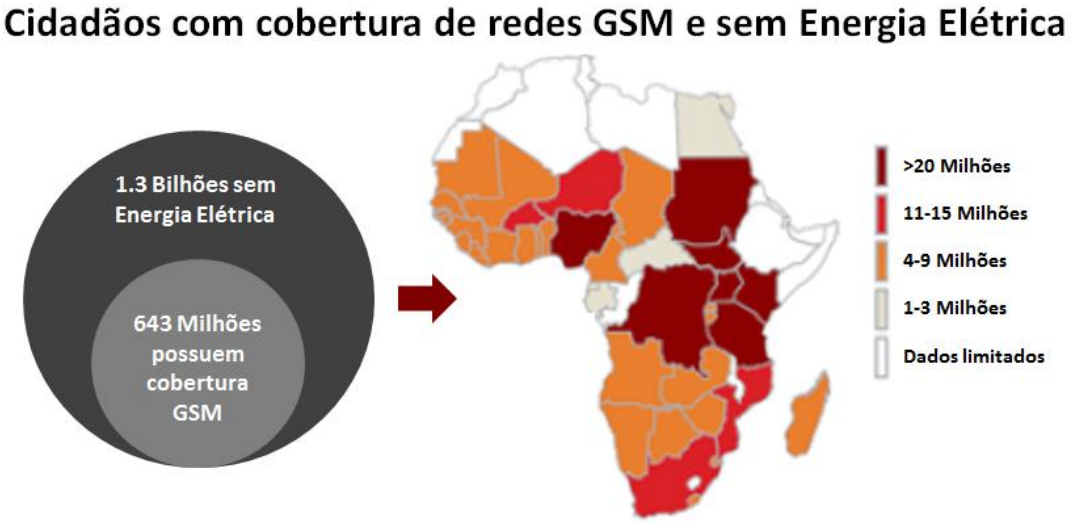


Figura 2-9: Energia vs Telefonia móvel celular na África (MULLER, VAN EEDEN, *et al.*, 2015)

No Brasil, o cenário se faz diferente quando são analisados os dados da ANATEL e da ANEEL sobre a evolução do atendimento dos serviços de telefonia móvel e de acesso à energia elétrica, respectivamente. Não se vê tamanha discrepância entre os dois tipos de coberturas como se vê em outros países em desenvolvimento. Para a realidade brasileira, o Instituto Brasileiro de Geografia e Estatística (IBGE - INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA, 2010) mostra que em 2010 havia mais de 97% da população brasileira com atendimento de energia elétrica. Dados ainda não consolidados de 2016, apontam para 99% das residências já atendidas pela energia elétrica. Na telefonia móvel celular, os percentuais de cobertura encontrados, somando todas as diversas operadoras, foram divulgados pela ANATEL (ANATEL, 2018) em outubro de 2018.

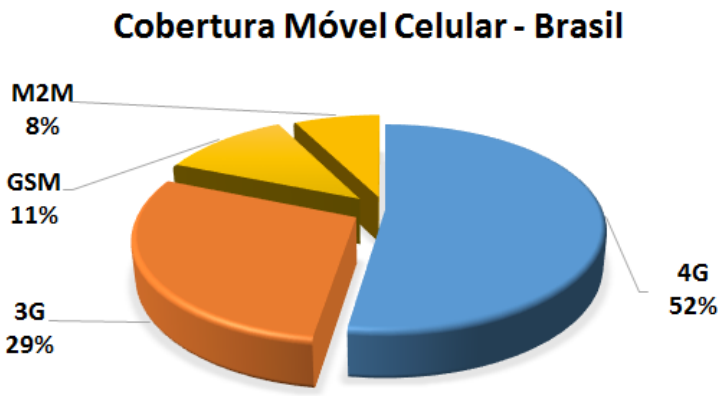


Figura 2-10: Cobertura móvel celular no Brasil em 2018 (ANATEL, 2018)

A menor cobertura nos estados da federação é de 79,7% (Maranhão) e a maior chega a 137,3% (São Paulo). A divisão das tecnologias é mostrada na Figura 2-10, e mostra uma parcela importante do uso das linhas M2M que se destinam a comunicação automática entre equipamentos sem interação ou intervenção humana, muito utilizada na chamada Internet das coisas (IoT).

Do exposto, fica claro que o investimento mundial em telefonia móvel celular foi bastante importante e eficaz, atendendo por vezes a uma maior gama da população do que os serviços mais essenciais, tais como saneamento básico e fornecimento de água potável.

Capítulo 3

Sistemas Colaborativos

3.1 INTRODUÇÃO

O fornecimento de energia elétrica, seja para residências, comércio e indústria, se dá por meio de tarifas diferenciadas, de acordo com a quantidade de energia e período de tempo em que ocorre o consumo. Muitas vezes, o consumidor não conhece de forma clara e objetiva tal fato e por consequência, não adota o que se entende por um padrão de uso consciente de energia. Os programas de conscientização energética das concessionárias tendem a reverter este quadro; visam trazer o consumidor para uma postura mais ativa, fazendo com que entenda qual a melhor maneira de usar seus aparelhos e equipamentos elétricos, no sentido de reduzir os custos com energia e sem gerar problemas logísticos no seu consumo diário. O foco de tais programas está nos consumidores residenciais, não por acaso. Atualmente, os consumidores residenciais perfazem de 30% a 40% do consumo mundial (HAIDER, SEE e ELMENREICH, 2016) e por isso, geram um grande impacto nos sistemas de distribuição e transmissão de energia elétrica, o que se percebe com maior intensidade nos horários de pico que refletem alguns comportamentos coletivos de diversos estratos da sociedade.

O incentivo ao engajamento do consumidor e prosumidor (CAMARINHA-MATOS, 2016) na busca pelo uso racional de energia promove diretamente um esforço para a mudança de hábitos de consumo em vários níveis, modificando assim aspectos da confiabilidade e disponibilidade dos sistemas elétricos, uma vez que todas as parcelas importantes deste sistema estariam em maior sintonia. Mas esta mudança não ocorre espontaneamente, de forma altruísta, na maioria das vezes. Há a necessidade de uma política clara de recompensa para motivar o consumidor a sair de um certo imobilismo como simples usuário para ser também um agente do sistema. Algumas iniciativas mostram que a economia de energia pode atingir patamares expressivos (e.g., 20%), dependendo do tipo de consumo (e.g., condicionamento de ambientes com aquecimento/refrigeração). A economia de energia, sem perda de

conforto do consumidor, é um grande desafio a ser enfrentado neste tipo de programa, principalmente quando envolve regiões de extremos, em termos de temperatura ambiente. Nestes casos, o aquecimento por exemplo deixa de ser conforto para ser um fator essencial.

Segundo estudo encontrado em (GANGALE, MENGOLINI e ONYEJI, 2013), 55 projetos europeus (de um total de 219) focalizaram o referido engajamento do consumidor (em inglês, "*Consumer Engagement"*). Pode-se verificar que o lançamento de programas que contam com o envolvimento do consumidor final tem aumentando ao longo dos anos e cada vez mais estes projetos se originam em empresas do mercado de energia, perfazendo 76% do total de projetos propostos, como se vê na Figura 3-1. Isso mostra a sensibilidade do mercado ao problema, percebendo-se que este é o caminho para futuro dos serviços prestados às populações consumidoras. A terminologia utilizada pelos autores da referência (GANGALE, MENGOLINI e ONYEJI, 2013) adota como DSO, operadoras de sistema de distribuição (em inglês, "*Distribution System Operators"*) e TSO, operadoras de sistema de transmissão (em inglês, "*Transmission System Operators"*).

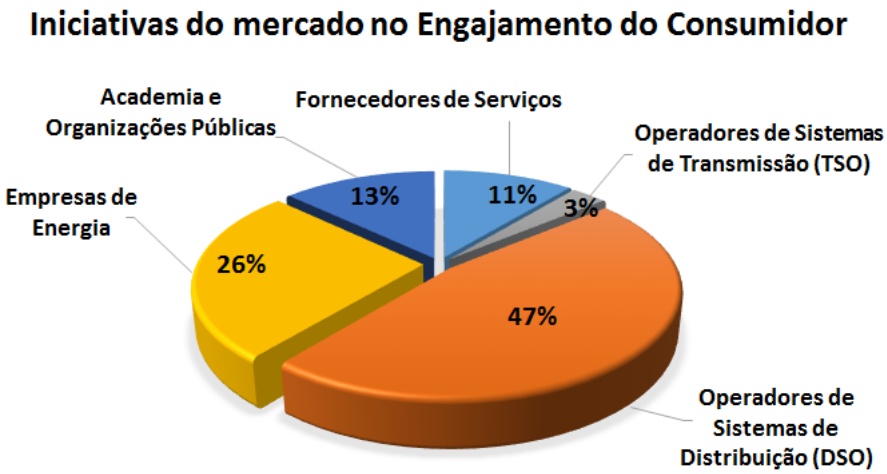


Figura 3-1: Iniciativa de projetos de *consumer engagement* (GANGALE, MENGOLINI e ONYEJI, 2013)

A principal indagação que se coloca quando em questão conceitos mundialmente utilizados como "*consumer engagement"*, "*consumer empowerment"* e "*demand response"* (HAIDER, SEE e ELMENREICH, 2016) é a seguinte: como convencer o consumidor a aderir consciente e determinadamente ao uso inteligente de energia? A resposta geralmente envolve aspectos financeiros, ou seja: através de recompensas monetárias pelo seu esforço sejam estas em termos de descontos em

serviços e produtos ou créditos diretos. A título de ilustração, vale fazer referência ao programa de economia de energia executado pela PG&E (https://www.pge.com), concessionária de energia da Califórnia (EUA), em que empresas e consumidores residenciais são informados sobre as condições atuais para o suprimento de energia frente ao consumo e têm a oportunidade para participar na redução do seu próprio consumo em tempo real. Também podem aderir a uma redução programada de acordo com metas pré-estabelecidas de consumo. Os incentivos monetários são claros e objetivos, podendo-se receber USD 0,10 por Wh, por mês, considerada a redução de energia contabilizada.

Atualmente, observa-se que os programas de consumo inteligente apontam para a participação meramente reativa do ponto de vista do consumidor e não criativa, ou seja, o cliente possui as informações prontas das concessionárias sobre o que fazer e quando fazer, mas não possui muito espaço criativo para inovar e isso também se deve à característica da problemática em si. Neste cenário, a possibilidade de recompensas que premiem este tipo de comportamento mais criativo é mínima. Para esta parcela da população que valoriza mais a colaboração como parte de uma co-criação de soluções (ROMERO e MOLINA, 2011), do que a participação como um mero instrumento ou peça de um sistema, as recompensas puramente financeiras podem ser complementadas pelo reconhecimento do esforço de inovação do indivíduo.

Nas abordagens implementadas pelo mundo, há uma tendência de se robotizar o comportamento do consumidor a ponto de informar o melhor horário de utilizar a lavadora de roupas, o ferro de engomar ou até mesmo a televisão. Sabe-se que os comportamentos regionais e pessoais muitas vezes seguem a lógica da necessidade e pelo desejo, ou seja, podem estar comandados pelo clima, rotina pessoal, ambiente social, nível de segurança, etc. Além disso, esses consumidores muitas vezes não conhecem as alternativas mais econômicas em termos de consumo e precisam de um guia para tal. Por isso, as abordagens destes programas devem ser cuidadosas, concentrando-se no esclarecimento/educação energética e não na imposição de regras. Em termos de recompensa ao engajamento do consumidor, alguns caminhos atrativos são elencados a seguir:

a) Descontos em implantação de unidades de geração de pequeno porte (e.g., placas solares) para consumo próprio e/ou injeção na rede (prosumidor), em conjunto com um programa educacional sobre pequena geração distribuída;

b) Créditos diretos nas contas de energia elétrica;

c) Descontos em serviços de análise energética da casa, apontando as deficiências em termos de consumo inteligente e equipamentos de baixo rendimento;

d) Possibilidade de criação de comunidades de agentes de apoio, aumentando a quantidade de medidas e cobertura de atuação. Com isso, não só um, mas vários consumidores poderiam ser premiados ao mesmo tempo pelo desempenho daquela comunidade. Pensando na realidade dos países em desenvolvimento, assim como naqueles que possuem grandes comunidades carentes (de alguma maneira impedem a presença de técnicos das concessionárias ou até do emprego de tecnologias de medição remota), estes tipos de agentes comunitários são de vital importância para o atingimento destas áreas;

e) Atendimento de áreas ou caminhos pré-determinados pelas concessionárias que apresentam maior carência de observação. Quanto mais caminhos forem percorridos nestas áreas, maior é a pontuação, ou seja, quanto mais dinâmico e participativo for o usuário, maiores serão suas premiações;

f) Plano de pontos a serem trocados por Bitcoins (ALAM, LI e PATIDAR, 2015), eletrodomésticos, lâmpadas econômicas, smartphones, upgrades de planos de Internet e telefonia móvel;

g) Programas especiais para idosos com serviços de manutenção residencial, em que a concessionária fornece alguns serviços (e.g., eletricista, gasista, etc.).

3.2 REDES COLABORATIVAS

Do exposto até aqui, está claro que a educação tecnológica e colaboração do consumidor/prosumidor (CAMARINHA-MATOS, 2016) (ROMERO e MOLINA, 2011) tornam-se importantes para a operação dos sistemas de energia, constituindo alguns

dos caminhos fundamentais para a implantação de SGs sustentáveis, robustas e de alta confiabilidade. Há fortes mudanças de paradigmas causadas pelas ideias que apareceram nas últimas décadas sobre sustentabilidade, energia limpa, liberdade de mercado, entre outras, que se espalham influenciando cidadãos e corporações provocando grandes mudanças de comportamento e resultando em maior noção filosófica do que é a qualidade de serviços e quais seus impactos na qualidade de vida e na qualidade do meio ambiente.

Cada vez mais, temas que remetem para a qualidade de vida da sociedade são levados mais seriamente e com mais importância nos indicadores-chave de desempenho (KPI) do mercado de energia.

Constata-se que não há mais espaço para uma simples aceitação da relação servidor/consumidor, visto que a sociedade depende cada vez mais profundamente da energia elétrica e deseja participar e entender mais das problemáticas que envolvem este mercado. Nos países em que a escolha das concessionárias é permitida com o livre comércio de fornecimento de energia para o usuário final, este último procura entender os diferenciais e atrativos oferecidos para escolher qual empresa lhe atenderá daqui para frente.

A utilização de sistemas de processamento e armazenamento distribuído de dados para auxiliar na solução de problemas de grande porte encontra-se bastante disseminada. Quando a qualidade na prestação de serviços públicos está em jogo, as redes colaborativas (RCs) podem agregar grandes vantagens pela sua enorme capilaridade tendendo a atingir zonas não observáveis aos olhos dos gestores destes serviços, mas que são acessíveis à população em geral.

Aliada a esta realidade observa-se a tendência mundial de compartilhamento e ação colaborativa, também chamada de economia do compartilhamento, manifestada por exemplo no transporte público (i.e., Waze, Uber, Zipcar, Velib, etc.), no mercado de hospedagem de pessoas (e.g., AirBnB, Couchsurfing, etc.), bem como na área de energia no que diz respeito às empresas que fazem comercialização de energia direta intra consumidores e entre eles e as concessionárias. Exemplos de tais iniciativas podem ser citadas as empresas Transactive Grid (http://transactivegrid.net/) e Grid Singularity (http://gridsingularity.com/) que comercializam energia entre consumidores de maneira transparente para a concessionária, em que um prosumidor vende energia para os consumidores individuais ou em grupo de consumidores que fizeram um contrato através da internet de modo simples e objetivo. Este comércio utiliza a

tecnologia Blockchain usada em larga escala pelo conhecido sistema monetário paralelo Bitcoin. Cada uma das transações é digitalmente assinada garantindo sua autenticidade e segurança contra qualquer adulteração, classificando as transações como de alta integridade.

A SolarCoin (http://solarcoin.org/) se foca no mercado de energia solar utilizando também a tecnologia Blockchain para criar a chamada "*crowdfunded feed-in tariff*" do mercado de energia. Chama-se de "*feed-in tariff*" a tarifa paga para os usuários pelo excedente de energia elétrica gerada através de um sistema de microgeração e o valor de cada MWh gerado é monetizado em uma moeda virtual que irá circular entre os usuários consumidores e prosumidores, ensejando incentivos pela geração de energia solar excedente e lançada na rede.

Outro grande exemplo de sucesso das redes colaborativas utilizando o Blockchain em sistemas de energia foi a *microgrid* virtual instalada no bairro do Brooklyn na cidade de Nova York (EUA) (BREUER, 2018) onde cada consumidor e prosumidor compra e vende energia solar através de um aplicativo que está preparado para a comercialização inclusive em casos de isolamento real da *microgrid* em relação ao sistema de distribuição de Nova York, ou seja, o sistema instalado possibilita que o bairro continue a operar de forma independente, sendo um dos passos para a implantação em larga escala de sistemas auto gerenciados de comercialização de serviços públicos. Estes sistemas também contam com a possibilidade de aplicação de sigilo (DIMITRIOU e KARAME, 2013) e segurança de informações através de criptografias características desta tecnologia.

Capítulo 4

Proposta de um Sistema Colaborativo de Medição Inteligente

4.1 INTRODUÇÃO

A ideia de se propor um SCMI aponta para a criação de um sistema AMI que utilize a tecnologia Blockchain no transporte de dados, usando todos os seus elementos aplicados ao problema de gerenciamento de dados nas SGs. Este capítulo objetiva reunir conceitos, elementos e bases estruturais necessárias à implementação deste tipo de sistema de telemedição.

O SCMI a ser proposto se apresenta como uma evolução das redes AMI e une diversas tendências tecnológicas e soluções existentes com modificações estratégicas. O sistema deve ser entendido como uma solução inovadora e segura do ponto de vista da integridade de informações, que seja capaz de gerar uma economia substancial em termos de infraestrutura de comunicação, em relação a soluções amplamente utilizadas hoje para integrar SGs aos centros de operação e tomada de decisão.

A solução proposta se apoia na ação colaborativa de indivíduos da sociedade que queiram atuar diretamente como agentes de medição do sistema de comercialização de energia em conjunto com a tecnologia de medição inteligente. Neste sentido, é preconizada também a colaboração entre concessionárias de energia no intuito de compartilhar os recursos materiais e humanos, disso decorrendo a denominação da proposta de “Sistema Colaborativo de Medição Inteligente” (SCMI).

4.2 CONCEITUAÇÃO

Neste novo conceito de AMI, a infraestrutura baseia-se na tecnologia Blockchain para transmissão e gerenciamento de dados de medição de grandezas elétricas em redes colaborativas de usuários finais de energia. Assume-se a utilização

de inteligência computacional embarcada em aplicativos, compatíveis com as plataformas mais usadas em *smartphones* e *tablets* (i.e., Android e iOS). Dessa maneira, cada usuário pode participar espontaneamente e ser chamado de “Agente” de telemedição para o sistema, não sendo desejável que essa tarefa comprometa o uso comum do seu aparelho móvel. Tal colaboração permite o estabelecimento de uma grande rede em que todos os seus elementos podem interagir na troca de dados úteis para a concessionária de energia.

O sistema proposto visa ainda a utilização de todo o parque instalado de comunicação móvel celular existente e *Hotspots wi-fi* públicas e privadas para a aquisição massiva, segura e distribuída de dados de medição de grandezas elétricas e *status* operativo de equipamentos, estando dentre eles: dispositivos de chaveamento (disjuntores, chaves seccionadoras, etc.), religadores, unidades remotas de medição e controle, medidores inteligentes de energia, e outros equipamentos de SGs com tecnologia compatível para comunicação e que estejam disponíveis no mercado.

4.3 DESAFIOS

As mudanças de paradigmas ou inclusão de novos partícipes em qualquer processo tecnológico ou de comportamento social, sempre constitui um grande desafio. A implantação de um sistema tal como o SCMI aqui proposto comporta diversos aspectos multidisciplinares, brevemente apontados a seguir:

- ***Captação e Capacitação de Agentes***: atrair o interesse dos usuários dos serviços públicos de energia a aderirem ao SCMI se coloca como ponto de partida. Para isso, a educação tecnológica sobre a temática e uma divulgação clara do propósito da rede colaborativa devem ser obrigatórias no processo;

- ***Sistema de recompensas***: deve ser objetivo e de fácil assimilação pelo usuário contemplando planos atrativos para o crescimento da rede;

- ***Aplicativo para aparelhos móveis***: o software desenvolvido deve ser simples, rápido e de baixo custo computacional;

- ***Implementação***: deve ser de menor impacto possível ao parque instalado em termos de custo de infraestrutura, software e hardware;

- ***Integridade & Segurança de informação***: deve-se garantir a garantia de origem pelo sistema de informação de geolocalização, a segurança e a integridade dos dados coletados e a total integração no compartilhamento de dados entre agentes cadastrados, aumentado a capilaridade do sistema;

- ***Big Data***: espera-se que seja coletada uma gigantesca massa de dados dos agentes da rede colaborativa, o que demandará um gerenciamento compatível com as melhores tecnologias atuais em termos de armazenamento e filtragem dos dados e fundamentalmente, deve-se realizar o tratamento dos dados coletados (sejam eles, redundantes, repetidos ou discordantes), a fim de se extrair somente os dados úteis ao centro de operação;

- ***Utilização dos dados coletados***: para utilizar os dados disponibilizados, o centro de controle deve possuir um sistema inteligente para a tomada de decisões (em que serão analisados os dados coletados) relativas à operação diária do sistema.

4.4 ELEMENTOS DO SISTEMA PROPOSTO

Todo sistema possui diversos elementos ativos e passivos e no SCMI não é diferente. Cada componente possui sua importância e características específicas e por vezes complementares, visando sempre que o SCMI proporcione uma disponibilidade e segurança condizentes com as aplicações em serviços essenciais.

Na Figura 4-1 são ilustrados os elementos do SCMI, onde colaboradores, aqui chamados de “Agentes” de medição, dispositivo de medição e outros elementos são devidamente explicados a seguir:

a) Centro de Controle:

O centro de controle do SCMI na verdade é o CC da concessionária onde se encontra os sistemas de gerenciamento da distribuição (DMS/ADMS), responsável pelo gerenciamento global do sistema em todas as regiões de concessão da empresa. No CC, todos os dados coletados no SCMI serão armazenados e tratados devidamente para a visualização do operador do sistema. Os dados já tratados no SCMI são encaminhados para as devidas áreas de atuação, sejam elas de manutenção, análise de ocorrências ou de operação.

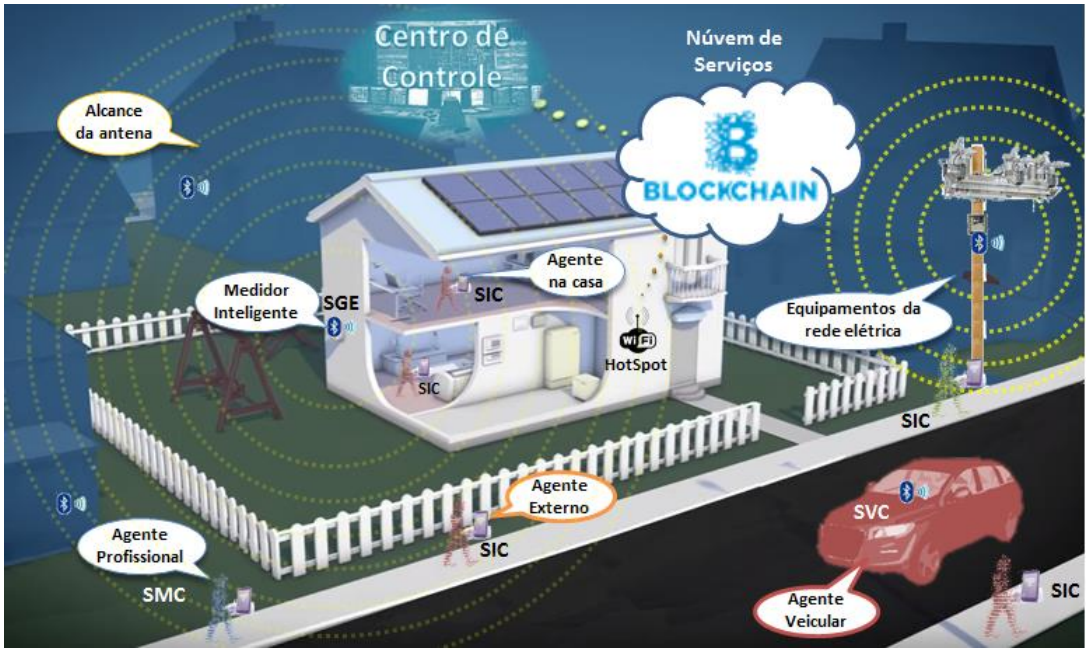


Figura 4-1: Elementos do SCMI em ação[1]

b) Nuvem de Serviços Blockchain:

A chamada nuvem, que é um conceito muito comum quando são tratados processos com grande quantidade de dados, o conhecido "*Big Data*" (MAYER-SCHÖNBERGER e CUKIER, 2014), é na verdade uma rede de serviços distribuída entre diversas plataformas computacionais de posse da concessionária ou contratadas por esta. As funções da nuvem de serviços Blockchain são de armazenar, analisar, filtrar e validar as transações de envio e recebimento de dados a fim de viabilizar a conexão entre os dispositivos de medição e Agentes de medição às concessionárias de energia com atuação na respectiva região. Ou seja, basicamente, a nuvem é responsável por armazenar e enviar ao CC somente dados relevantes da rede, evitando uma massa de dados sem utilidade sendo descarregada na concessionária.

c) Elementos da Rede Inteligente:

Os elementos da rede inteligente (*smart grid elements* – SGEs) podem ser representados por todos os dispositivos inteligentes e presentes em uma rede possuindo capacidade de comunicação de dados e fornecimento de medições, status

[1] Todas as figuras que não possuírem indicação de referências externas, foram construídas pelo autor.

ou informações de alarmes. Estes equipamentos podem ser Medidores, Religadores, Unidades Terminais Remotas (UTRs), chaves interruptoras inteligentes, disjuntores inteligentes, etc. Os SGEs podem ser de diferentes fabricantes, no entanto devem possuir a capacidade de se integrar em uma rede sem fio a fim de possibilitar a comunicação com os Agentes sem problemas de interoperabilidade. O SGE também pode atuar como um Agente, caso o dispositivo possua capacidade de conexão direta com a nuvem de serviços Blockchain. Nestes casos, o empacotamento dos seus próprios dados para o padrão de blocos de dados do SCMI é realizado pelo próprio SGE.

d) Clientes Independentes Inteligentes:

Os *smart independent clients* (SICs) são compostos basicamente por todos os usuários que participam ativamente do SCMI contemplados com uma ferramenta de software, ou seja, um aplicativo específico para *Smartphones* ou *Tablets*, capaz de se comunicar com os SGEs e com a nuvem de serviços Blockchain, servindo assim de ponte de conexão entre o campo e o CC. Espera-se que os Agentes não estejam dedicados aos serviços de medição pela sua característica colaborativa e não impositiva. Por isso, estes Agentes possuem uma característica aleatória em termos de localização e janela de disponibilidade de aquisição de medições. Este Agente precisa ser incentivado a participar cada vez mais efetivamente e de maneira mais eficaz, maximizando sua capacidade de monitoramento da rede. Para isso, programas de recompensas, conforme i.e., os apresentados na Seção 3.1, devem atingi-lo diretamente de forma que sua atuação seja sempre significativa.

e) Clientes Veiculares Inteligentes

Os s*mart vehicular clients* (SVCs) são agentes que se deslocam em maior velocidade e que podem atingir áreas muito distantes em pouco tempo, ou seja, podem coletar medidas em diferentes redes num único dia, porém, pela sua característica móvel de alta velocidade, poucos SGEs conseguiriam ser lidos pelo baixo tempo de aproximação entre os dois elementos, o que não permitiria uma comunicação completa entre SVC e SGE. SICs que se encontram dentro de veículos podem assumir temporariamente características de um agente SVC. Atualmente, a emergente tecnologia baseada na chamada comunicação Dedicada de Curto Alcance

(*Dedicated Short Range Communication* – DSRC) baseada na norma IEEE 802.11p *Automotive W-Fi* para sistemas de comunicação veicular (BRONZI, FRANK, *et al.*, 2014) é cada vez mais valorizada pela indústria automotiva, o que é uma tendência a ser aproveitada pelo SCMI. O SVC deve ser capaz de se comunicar com os SGEs, com a nuvem de serviços Blockchain e com outros SVCs a ponto de difundir as medições para muito além das áreas delimitadas de origem do agente. A Figura 4-2 ilustra um exemplo deste tipo de interação possível entre os Agentes de medição.

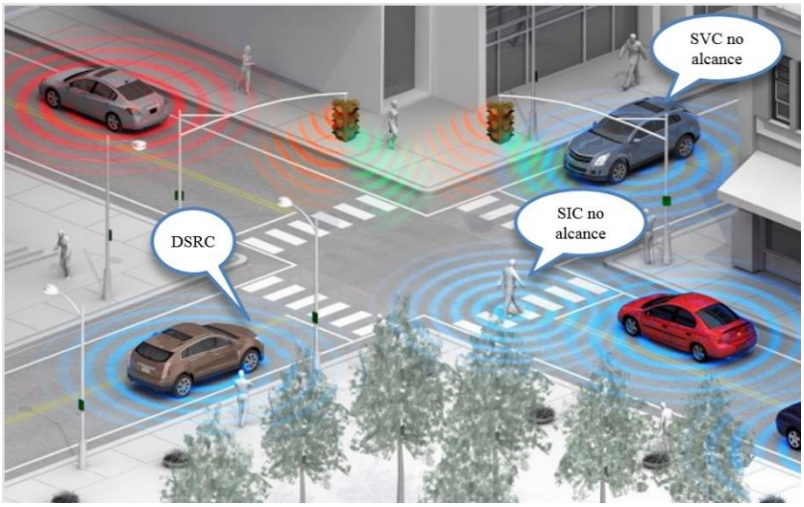


Figura 4-2: Comunicação inter-vehicular DSRC

f) Clientes de Manutenção Inteligentes:

Ao contrário do SIC, o s*mart maintenance client* (SMC) é um agente de engajamento obrigatório visto que se tratam de indivíduos que colaboram profissionalmente para a concessionária e possuem rotinas de varredura de área e clientes bem definida, a fim de reduzir as lacunas de monitoramento produzidas na aleatoriedade do sistema. Somente os SMCs são capazes de realizar coleta de medições de vários SGEs em plataforma Mesh (abordado em capítulos seguintes).

Os SMCs podem realizar atividades de maior nível de complexidade atuando como posto avançado de processamento local (Figura 4-3) assessorando o CC nas suas funções mais críticas assim como:

- Análise local de faltas e alarmes através de algoritmos especialistas;
- Análise do índice de observabilidade e Estimação de Estado Local dos ramos da rede de Distribuição definida pelo SMC, cobrindo as lacunas de medição e consolidando um relatório de medição diária para a concessionária;

- Análise de perfil de cargas locais, qualidade de energia e identificações de desvios ou perdas técnicas e não técnicas.

Figura 4-3: Atribuições do SMC

4.5 INFRAESTRUTURA PROPOSTA

O acesso pelo público em geral a modernas tecnologias vem sendo cada vez mais amplificado, materializando-se pela oferta de dispositivos multifuncionais e, principalmente, de fácil manuseio, mas com grandes funcionalidades.

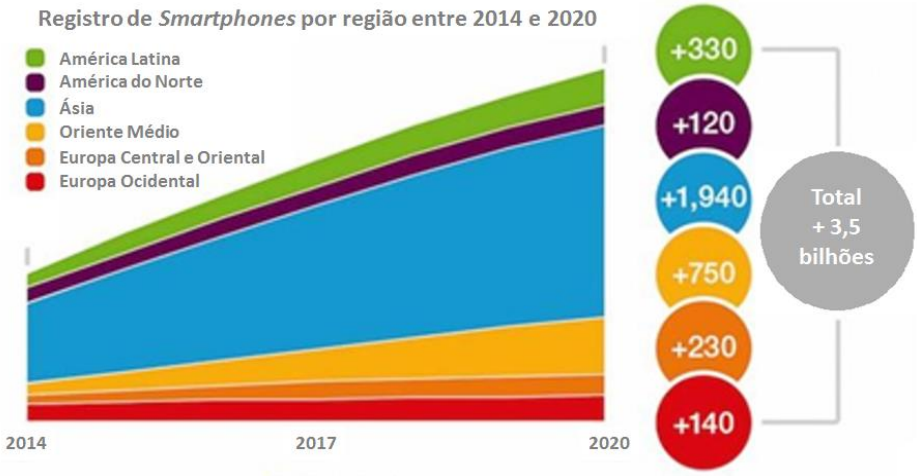


Figura 4-4: Previsão de crescimento de Smartphones (CHERNYI, 2015)

No que diz respeito à telefonia móvel, observa-se que o número de smartphones em funcionamento no mercado mundial tende a alcançar em 2020 o

patamar de 6 bilhões, de acordo com o último relatório da empresa Ericsson (CHERNYI, 2015), publicado em junho de 2015, do qual se extrai a ilustração apresentada na Figura 4-4.

Tamanho crescimento na plataforma móvel celular não deve ser ignorado, quando soluções para o problema de comunicação de dados nas redes inteligentes ainda são analisadas. Cada *smartphone* ou *tablet* contém uma plataforma computacional com unidades de processamento com capacidade considerável (CPUs dual, quad e até octa-*core*), assim como memória para armazenamento de dados que chegam às dezenas de Gigabytes. Todos estes recursos computacionais podem servir a objetivos comuns aos cidadãos, agregando valor considerável aos dispositivos eletrônicos que se conectem às redes de telefonia móvel existentes.

A base de infraestrutura tecnológica de todo o SCMI depende parcialmente das redes de comunicação móvel celular estabelecidas nas áreas de cobertura da operadora de energia elétrica. Na falta de cobertura de dados para a telefonia móvel celular, seria então necessária a presença de *Hotspots wi-fi* (http://www.wi-fi.org/certification) públicos ou privados de onde o usuário tenha acesso livre para transmissão de informações (*upstream*). Sendo assim, mesmo na indisponibilidade dos serviços de telefonia 3G/4G/LTE, dentre outros, o SCMI deve ser capaz de coletar e enviar os dados para os servidores de informação.

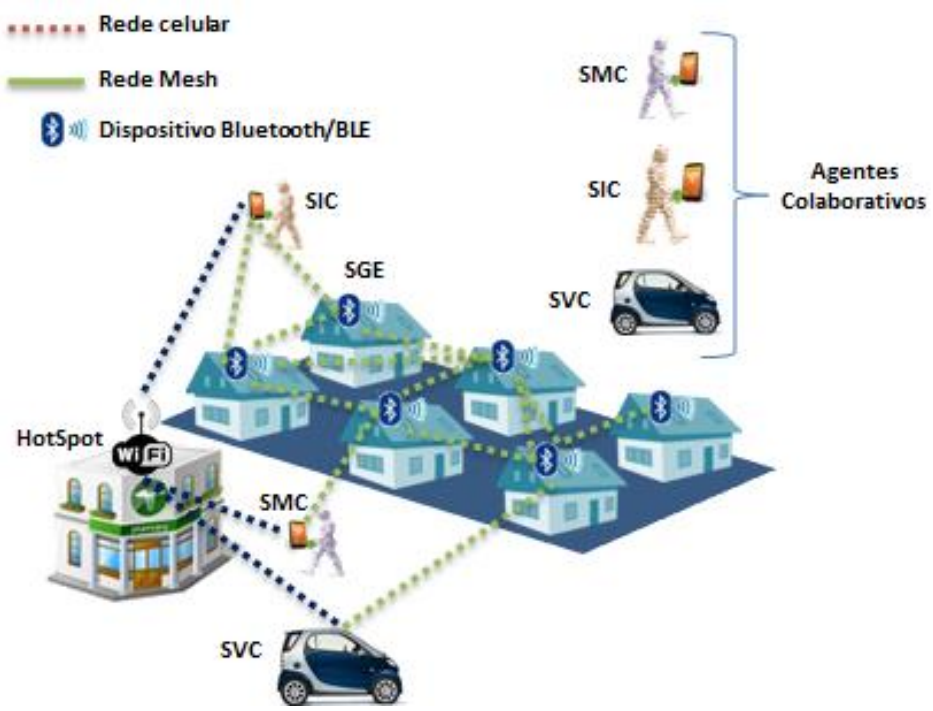


Figura 4-5: Rede Privada de comunicação do SCMI

Conforme ilustrado na Figura 4-5 apresentada, um *Hotspot wi-fi* instalado em um estabelecimento comercial serve como uma porta de conexão (*gateway*) à nuvem de serviços Blockchain quando há falta de serviços de dados proveniente da operadora de telefonia celular. Se faz importante notar que este tipo de situação, mostra a robustez do SCMI que não depende exclusivamente das redes de telefonia móvel, podendo funcionar apenas com interfaces *wi-fi* locais e conectadas em algum ponto com a Internet.

Outro ponto fundamental é o parque instalado de elementos da SG que são passíveis de medição remota. Estes equipamentos devem possuir interfaces de comunicação sem fio já operacionais, tais como, Bluetooth, Bluetooth Low Energy (BLE) ou protocolos que operem em redes *wi-fi*. A utilização da tecnologia Bluetooth/BLE vem crescendo a cada ano pela sua grande difusão nas tecnologias domésticas e comerciais de dispositivos *wi-fi*. O BLE se adequa aos avanços nas demandas das SGs, e sua comunicação realiza-se através de ondas de rádio na frequência de 2,4 GHz que não necessita licença especial de uso em espaços públicos, estando amplamente disponível.

Considerações sobre os medidores atualmente instalados e como integrá-los no SCMI são perguntas que surgem inicialmente. Respostas a estas perguntas podem ser obtidas no mercado de componentes de rede. Há uma série de soluções para a conversão de padrões de comunicação serial RS-232 e RS-485, http://www.ti.com/tool/TIDC-Bluetooth-Smart-to-RS-485-Gateway, muito usadas nos medidores atuais e que podem adequar as tecnologias existentes para *wireless* utilizando a tecnologia Bluetooth. Com conversores RS-232/Bluetooth por exemplo (MACKENSEN, LAI e WENDT, 2012), pode-se integrar um SGE convencional existente a uma rede Bluetooth. Outro exemplo de soluções para adequação de sistemas convencionais analógicos para digitais foi lançada pela empresa espanhola Circutor, http://circutor.es/, que desenvolveu um medidor digital que pode ser acoplado nos disjuntores de baixa tensão, conforme pode ser visto na Figura 4-6, disponibilizando as medições via wi-fi para um aplicativo proprietário. Esses elementos e sua instalação possuem muitas vezes custo bem mais competitivos do que a troca total do parque instalado para medidores digitais já com capacidade de comunicação Bluetooth ou Wi-fi. Ao longo dos anos, uma migração gradativa é inevitável para modernizar o parque atual e diminuir seus índices de obsolescência e já está sendo feita pela maioria das concessionárias.

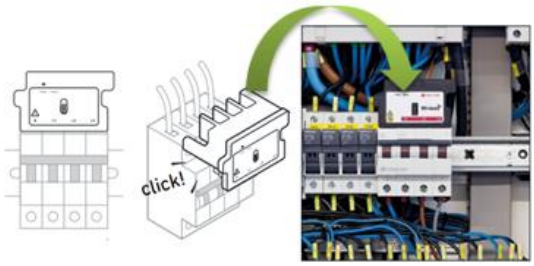


Figura 4-6: Medidor Wibeee (http://wibeee.circutor.com/)

Na Figura 4-7, pode-se notar uma rede híbrida contemplando interfaces Bluetooth, Wi-fi e utilizando o serviço de telefonia móvel local. A rede ainda apresenta a comunicação entre os elementos Bluetooth, o que depende do alcance da antena de cada dispositivo, e a comunicação entre as interfaces presentes nos veículos passantes e os dispositivos estáticos, dando uma dimensão das possibilidades do SCMI e que serão mais exploradas nos capítulos e seções seguintes.

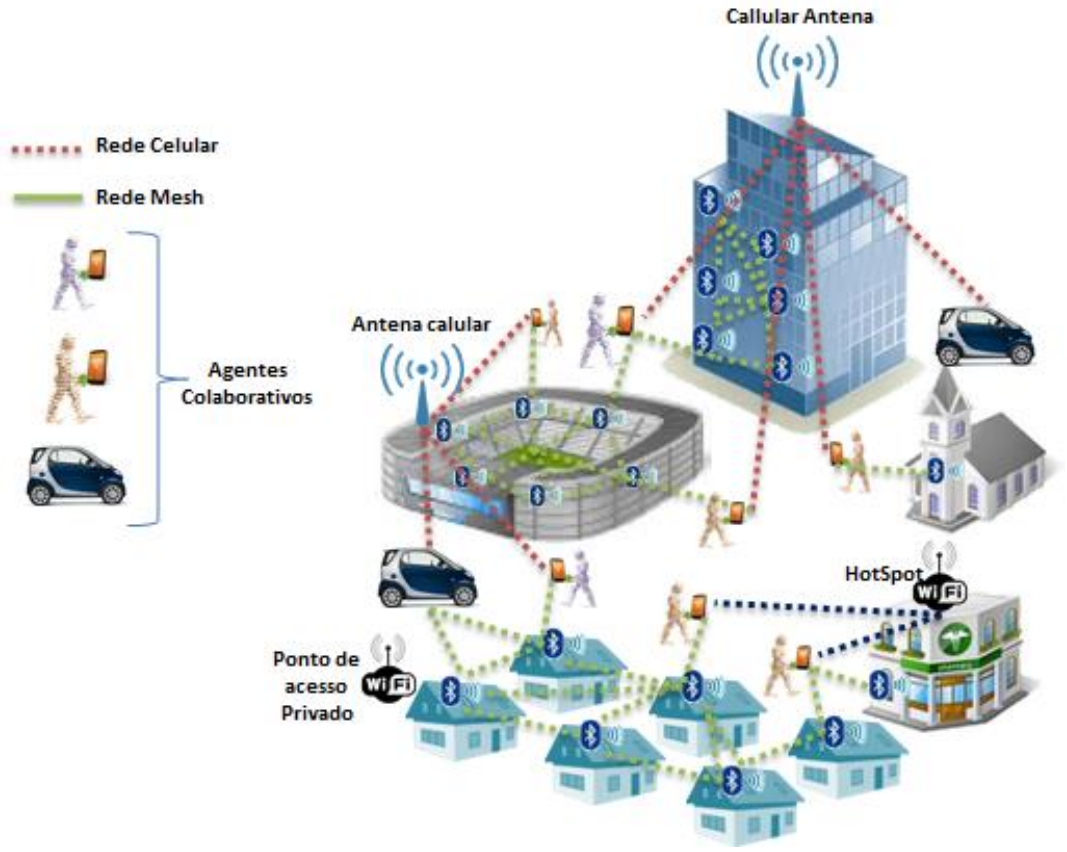


Figura 4-7: Rede Híbrida de comunicação do SCMI

4.6 AQUISIÇÃO ALEATÓRIA E DISTRIBUÍDA

No que diz respeito à aquisição de dados distribuída, imagina-se uma série de concentradores de dados ou elementos de medição instalados em áreas estratégicas

e de forma estática, ou seja, um ambiente controlado de medição em que a quantidade de dados e sua periodicidade estejam bem determinados, com poucas variações, salvo em casos de falhas de rede ou nos próprios equipamentos. No caso do SCMI a estrutura de rede de aquisição de dados de telemedição é na verdade totalmente distribuída e por vezes casuística ou aleatória. Por isso, surge uma questão importante: como estabelecer limites para a aquisição mínima de dados de modo a não haver áreas de “sombra” ou “cegas”, ou seja, áreas sem telemedição?

4.6.1 Dispersão de Agentes

Considerando redes colaborativas, deve-se ter em mente que está em jogo um grau de aleatoriedade considerável no que tange à presença dos agentes colaborativos em termos de quantidade, qualidade, dispersão geográfica e distribuição temporal. O SCMI prevê que qualquer indivíduo pode participar da rede e qualquer equipamento contemplado com o aplicativo do SCMI pode pertencer a esta rede. Se forem admitidos elementos estáticos/dinâmicos, aleatórios/previsíveis na aquisição de dados, pode-se notar que há um cenário de certeza alta (agentes estáticos) somado a cenários estocásticos e pseudoaleatórios (agentes dinâmicos). Na Figura 4-8 a seguir ilustra-se uma pequena rede circunscrita a um bairro com agentes de todos os tipos em ação.

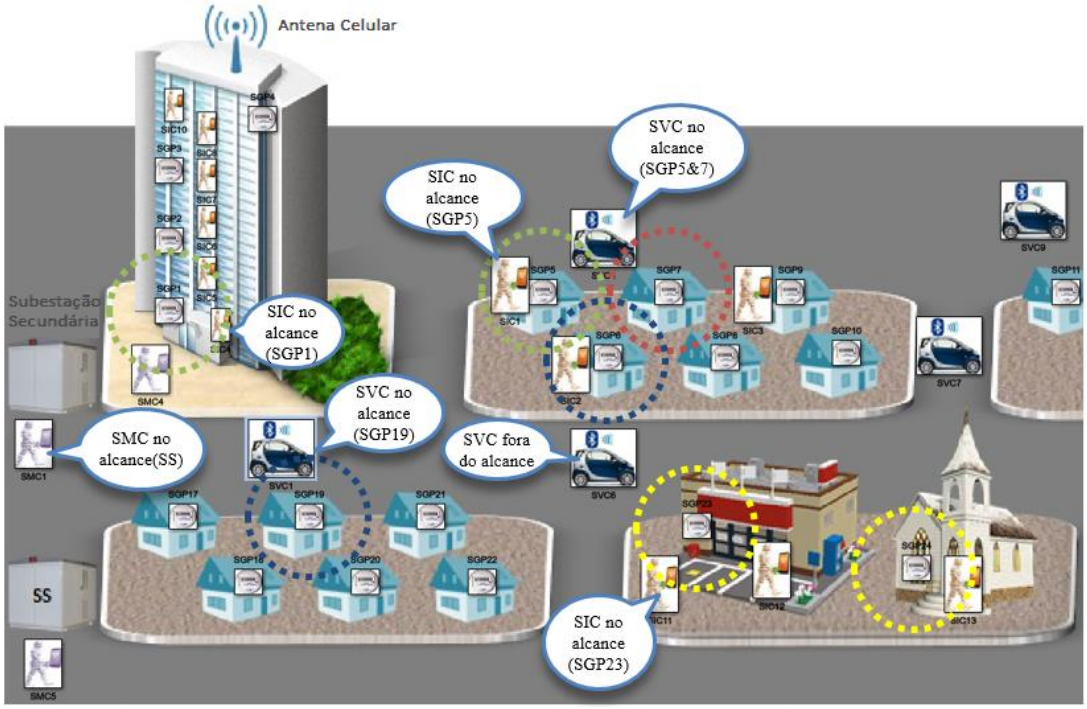


Figura 4-8: Agentes dispersos na coleta de dados distribuída

Vale ressaltar ainda sobre a Figura 4-8, que a imagem foi retirada de um simulador auxiliar de coleta dinâmica de medidas, que foi construído em Matlab™ especificamente para algumas provas de conceito quanto à coleta de dados em cenários dinâmicos de Agentes com deslocamentos programados.

Destaca-se que há dois tipos de coletas de medição: instantânea e histórica. A coleta instantânea ou de "tempo real" se faz no caso em que a aquisição é armazenada e enviada ao CC imediatamente pelo agente. Por sua vez, a coleta de dados históricos consiste na obtenção de toda ou parte das medições que se encontram armazenadas no medidor e que podem ser coletadas em um certo momento do dia quando este medidor estiver se comunicando com um determinado agente. Para efeitos de medição de faturamento de um usuário qualquer, é totalmente plausível e aceitável que os dados de medição sejam disponibilizados uma vez por dia pela concessionária, porém, para efeitos de supervisão e controle de resposta mais rápida, seria desejado uma medição com menor período de aquisição.

a) Medição Instantânea

Se tratando da demanda de medições com curtos espaços de tempo entre aquisições, numa análise inicial, pode-se levar em consideração que quanto maior o número de agentes dentro de uma população "β", maior a probabilidade de aquisição de dados de medição de um medidor específico. A equação (4.1) mostra que $P_s(SGE_x)_{\max(t)}$ é a máxima probabilidade de coleta de dados de um medidor "x" qualquer em um certo instante t na área de cobertura S, correspondendo ao somatório de todas as probabilidades de conexão dos m Agentes estáticos ($P_s(AE(t))$) e dos n Agentes dinâmicos ($P_s(AD(t))$) neste mesmo instante "t" em relação a este medidor.

$$P_s(SGE_x)_{\max(t)} = \sum_{k=1}^{m} P_s(AE(t)_k) \cup \lim_{n \to \beta} \sum_{k=1}^{n} P_s(AD(t)_k) \quad (4.1)$$

Ainda que o número de Agentes seja igual ao número de indivíduos da população ($n = \beta$), não se pode garantir 100% de certeza de monitoramento de um dado medidor no caso da falta de agentes estáticos. Esta afirmação se faz verdadeira pois, os agentes dinâmicos de uma determinada área S se deslocam para outras áreas e vice-versa, de maneira aleatória ou não. Com isso, não há como ter monitoramento 100% garantido contando somente com os agentes dinâmicos da própria área. Como presume-se que o Agente estático estará uma grande parcela do tempo próximo ao dispositivo de medição e hábil a realizar a conexão e coleta dos

dados de medição, a probabilidade de monitoramento do Agente estático, é igual à disponibilidade D. Este tipo de Agente pode ser o próprio medidor inteligente (*Smart Meter*), caso este possua a funcionalidade de envio automático *upstream* de medições. Sendo assim, o valor de D é o percentual de tempo que o fabricante garante que o equipamento consegue ficar em funcionamento, o que pode-se considerar sendo igual a 100%, pois em caso de falha, não adiantará a presença de nenhum outro tipo de Agente no raio de alcance de comunicação, pois não haverá medição a ser coletada no medidor que está fora de serviço.

Seguindo com os possíveis Agentes estáticos, os próprios computadores pessoais e/ou portáteis podem por sua vez participarem como Agentes estáticos enquanto em funcionamento perto dos pontos de instalação dos medidores inteligentes, coletando os dados em períodos pré-determinados. Um outro dispositivo de importância ainda não tão explorada nos lares modernos é a TV Inteligente (*Smart TV*) que possui características mínimas necessárias para ser um agente estático, que são: conexão com a Internet, capacidade de executar aplicativos locais e comunicação via Wi-fi (Bluetooth/BLE). Neste exemplo, a disponibilidade "D" seria o tempo em que a TV estivesse online e executando o aplicativo em modo escondido (*background*). Na Figura 4-9 é retratada uma típica cena do dia-a-dia com Agentes de todos os tipos e particularmente, uma família assistindo sua *Smart TV*, a qual está contribuindo para o SCMI coletando dados do medidor Inteligente da residência.

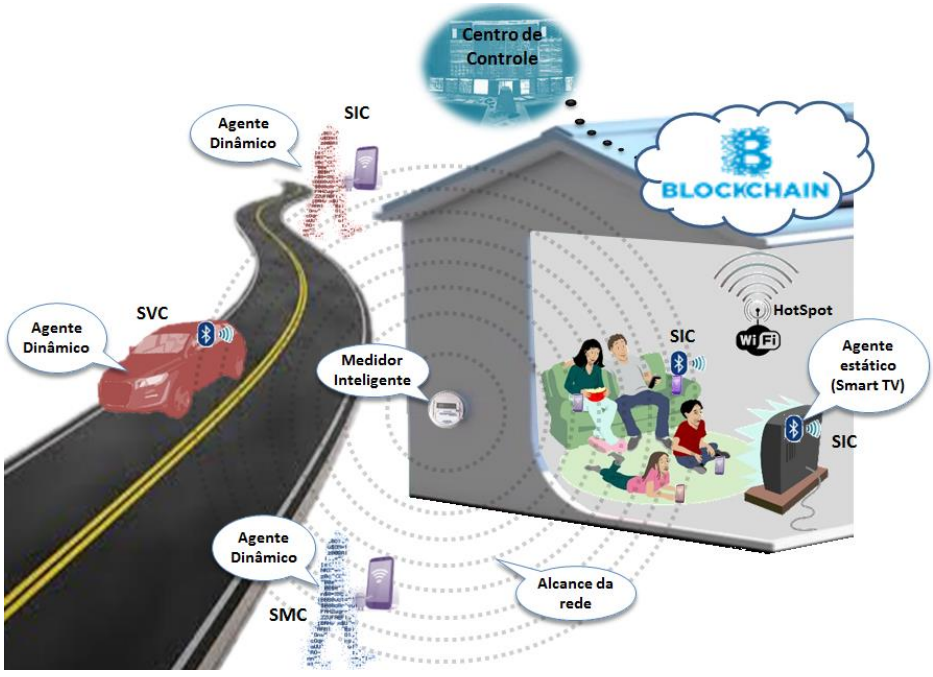


Figura 4-9: Medidor Inteligente e Smart TV como Agentes estáticos

b) Medição Histórica

Considerando que a medição de faturamento precisa de valores de energia acumulada no mês vencido, tem-se um cenário bem confortável no que tange a performance de telemedição, pois com apenas uma única aquisição de dados por mês, pode-se processar a conta de energia do usuário. Ao contrário deste tipo de cenário convencional e conservador, as soluções de SG perseguem uma filosofia de monitoramento em tempo contínuo e controle total das redes em um tempo mais breve possível. Seguindo a filosofia de quanto mais dados melhor, o SCMI prevê que além das leituras instantâneas de dados, há a possibilidade de leitura dos dados históricos gravados nos medidores, sendo assim, somando todos os tipos de agentes, se torna improvável que não haja pelo menos uma única coleta de dados diária em qualquer medidor instalado no SCMI. Esta função poderia ser acionada pelo Agente profissional de serviços SMC.

4.6.2 Redundância de Dados

Nos sistemas convencionais de aquisição de dados das SGs atuais, o volume de dados coletados está diretamente relacionado à quantidade de elementos de medição que estão conectados à SG, pois não prevê redundância de fonte de informação, ou seja, um medidor inteligente envia seus dados para o servidor sendo que estes dados são únicos e sem qualquer redundância.

No SCMI, a coleta de dados conta com diversos Agentes com seus respectivos dispositivos móveis. Vários Agentes poderiam coletar medições do mesmo medidor ao mesmo tempo ou em intervalos pequenos de tempo. Os dados serão enviados ao servidor com as informações de medições elétricas do mesmo medidor gerando uma massa de dados consideravelmente grande, pois se tratará de uma realidade de multi-redundância (Figura 4-10) com grau *n*. Serão possíveis situações em que dezenas (ou até centenas) de usuários poderão estar no raio de comunicação com o mesmo medidor. Cada medida seria enviada pelo usuário quando este estiver em conexão de dados ativa com a operadora ou mesmo através de uma rede *wi-fi* disponível, tema que será abordado adiante neste trabalho.

Figura 4-10: Aquisição multi-redundante

4.7 CLUSTERIZAÇÃO DA REDE SCMI

Do exposto nesta Tese, pode-se notar que o SCMI conta com diversos tipos de dados que podem ser coletados de maneira massiva e redundante em uma rede de energia qualquer. Esses dados são referenciados geograficamente e temporalmente, por isso a identificação de “onde” e “quando” uma aquisição de dados ocorreu é diretamente informada pelo agente, o que facilita a tomada de ações pela concessionária, de maneira geral de forma localizada. Para que isto venha a funcionar, o SCMI se divide em áreas delimitadas (Figura 4-11), denominadas aqui de *clusters*. Cada um destes possui uma quantidade de elementos inteligentes de SG, agentes residentes, voláteis, aleatórios e de serviço (SMC).

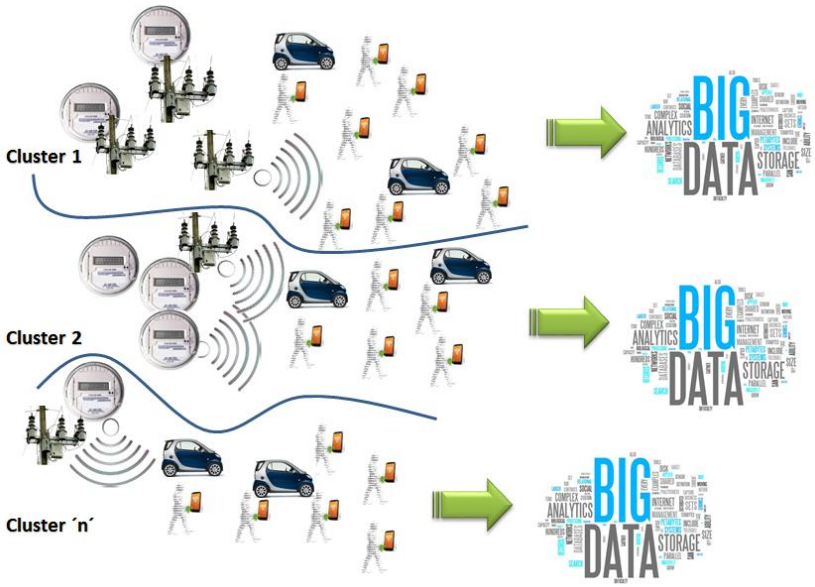


Figura 4-11: Clusterização do SCMI

Para cada uma destas áreas pode ser definida uma série de índices que auxiliam a identificar o perfil do Cluster e por consequência aumentam a eficácia de ações corretivas de manutenção em caso de problemas identificados e a eficácia dos planos de incentivo, visto que cada perfil pode demandar ações customizadas de incentivo à participação ao SCMI. São identificados abaixo alguns possíveis índices aplicáveis a cada Cluster:

- Índice de Cobertura no Cluster 'n' ($iCob_n$): relação entre os SGEs lidos e o total pertencente ao cluster.

$$\mathrm{iCob}_n = \frac{Número\ de\ SGEs\ lidos\ no\ dia}{Número\ total\ de\ SGEs\ no\ cluster} \quad (4.2)$$

- Índice de dados Redundantes ($iRed_n$): quantidade de SGEs com dados coletados por mais de 1 agente no mesmo intervalo de 15min;

- Índice de dados Descartáveis ($iDData_n$): quantidade de dados descartados pelos Mineradores;

- Índice de dados de Medição Críticas ($iCMeas_n$): quantidade de dados de medição denominadas como críticas ou estratégicas definidas pela concessionária;

- Índice de dados de Medição de Faturamento ($iRMeas_n$): quantidade de dados de medição de energia coletadas e validadas pelos Mineradores úteis para o faturamento;

- Índice de dados de Medição Manual ($iMMeas_n$): quantidade de dados digitados pelo agente diretamente no aplicativo, ou seja, provenientes de medidores que não são inteligentes, por opção ou não do usuário ligado ao medidor;

- Índice de dados de Alarme ($iAlm_n$): quantidade de alarmes coletados no cluster;

- Índice de dados de Evento do Sistema ($iEvt_n$): quantidade de eventos de faltas, distúrbios dentre outros e que foram coletados pelos agentes;

- Demais índices já conhecidos pelo mercado de energia tais como (ANEEL, Indicadores: http://www.aneel.gov.br/indicadores): DEC (Duração Equivalente

de Interrupção por Unidade Consumidora), FEC (Frequência Equivalente de Interrupção por Unidade Consumidora), DIeC (Duração de Interrupção por Unidade Consumidora), FIC (Frequência de Interrupção por Unidade Consumidora), DMIC (Duração Máxima de Interrupção por Unidade Consumidora).

A delimitação dos Clusters pode ser determinada pelos circuitos de baixa tensão derivados dos postos de transformação, ou dependendo da extensão do alimentador, cada um deles pode delimitar um cluster. É claro que cada concessionária possui áreas de atuação com características particulares o que pode demandar estratégias de delimitação de área diferentes. Regiões rurais e regiões urbanas com problemas sociais tais como as famosas favelas Brasileiras, podem ser delimitadas como um único cluster onde estratégias eficazes de mobilização colaborativa podem ser concretizadas dentro daquela realidade social.

4.8 ARQUITETURA SISTÊMICA DO SCMI

Vale ressaltar que esta tese se concentra na fase de transporte de dados entre os agentes e o CC, no entanto, é importante uma exemplificação da fase de coleta de dados de medição para que o ciclo completo do sistema seja apresentado de maneira mais concreta. Com isso, este capítulo tentou detalhar mecanismos que viabilizam a implantação do sistema proposto de transporte de dados.

A arquitetura consolidada do SCMI é apresentada na Figura 4-12 contemplando todos os elementos do sistema colaborativo e o fluxo de dados entre Agentes, SGEs e CC. Pode-se visualizar todos os elementos até aqui citados e as possíveis tecnologias de integração de rede existentes no mercado de comunicações nas redes inteligentes, tais como *Bluetooh* e *Wi-fi*. A arquitetura deixa claro o posicionamento de cada elemento no processo de telemedição e onde o sistema Blockchain se encaixa no problema apresentado. O detalhamento de todo o sistema de transporte de dados baseado na tecnologia Blockchain proposto, será realizado no próximo capítulo.

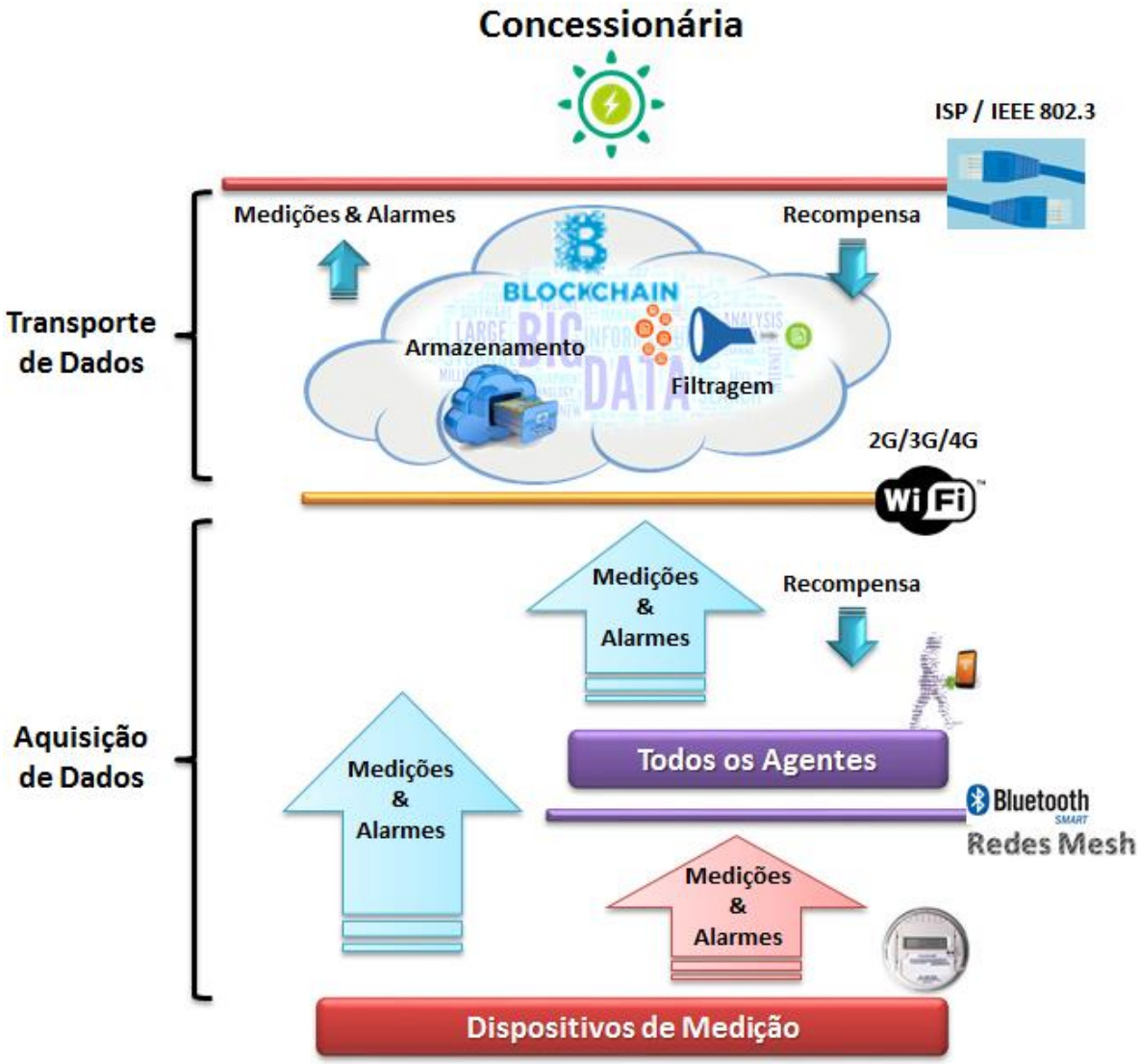


Figura 4-12: Arquitetura do SCMI

Capítulo 5

Blockchain e Telemedição

5.1 INTRODUÇÃO

Diversos tipos de redes de transporte de dados de telemedição são empregadas atualmente, utilizando interfaces ópticas, rádio frequência, linhas privadas de dados, Ethernet, Wi-fi entre outras já comentadas anteriormente neste trabalho. Porém, quando se considera redes em grande escala, com um gigantesco número de pontos fornecedores e consumidores de energia e uma demanda crescente de dados, tudo se faz mais complexo, sendo necessária uma análise mais profunda das reais necessidades de cada aplicação de telemedição, objetivando uma utilização mais prática e otimizada das tecnologias disponíveis.

Os sistemas de medição nas SGs incluem medições de grandezas elétricas e status de equipamentos em números abundantes. Atualmente, existem muitas maneiras de coletar dados de medidores de energia. Eles variam do mais básico, i.e., avaliação visual, para os mais avançados, como o uso de medidores inteligentes em redes AMI. A qualidade das tarefas de faturamento e manutenção depende da precisão e segurança do processo adotado para obter as telemedições necessárias. A metodologia Blockchain pode ajudar substancialmente a projetar um sistema de medição capaz de atingir esse objetivo.

Uma das principais diferenças entre as soluções SCMI e as AMIs tradicionais está no processamento e filtragem de dados. Embora não haja inteligência associada à solução padrão nas AMIs, o SCMI introduz um conceito de validação de dados, descartando ou aprovando blocos de dados antes destes chegarem aos centros de controle. Essa validação evita dados duplicados e inválidos, e possui uma detecção de fraude eficaz para cenários invasão cibernética e de corrupção de informação. O resultado geral é um sistema de medição que entrega apenas dados úteis e informa qualquer desvio indesejado para a concessionária de energia. Consequentemente, os sistemas de gerenciamento de distribuição tipo DMS e ADMS assim como os sistemas

de gerenciamento de dados de medição (MDMS) podem se beneficiar do aumento de desempenho e da qualidade do monitoramento dos sistemas elétricos de potência.

A seguir serão analisados alguns aspectos da telemedição aplicáveis diretamente ao SCMI proposto.

5.2 BLOCKCHAIN: CONCEITOS

O sistema Blockchain é uma poderosa ferramenta para grandes redes descentralizadas que possuam elementos cuja relação demande grande grau de confiança. O Blockchain envolve o gerenciamento de bancos de dados intrinsecamente seguros e descentralizados (PECK, 2017), evitando a interferência humana durante a transação de recebimento e entrega de blocos de dados. Não por acaso que o Blockchain é utilizado nas transações da moeda virtual Bitcoin com grande êxito. A tecnologia Blockchain oferece grandes benefícios para os sistemas de energia, onde estão presentes empresas comercializadoras, operadoras, mantenedoras, além dos usuários e clientes finais (consumidores e prosumidores).

As redes Blockchain podem ser públicas ou privadas, dependendo do grau de acessibilidade e governança. O tipo público (JAYACHANDRAN, 2017), usado comumente nas criptomoedas (e.g., Bitcoin e Ethereum), permite o acesso de qualquer indivíduo que tenha interesse no seu uso e finalidade e possuem, de forma geral, baixa performance em termos de tempo de entrega dos blocos, mas alto nível de segurança. O tipo privado, que usualmente são agéis na tomada de decisões, podem ser vistos em (KIM, PARK e RYOU, 2018) e em forma de consórcio em (GAI, WU, *et al.*, 2019), leva em consideração o acesso à rede de dados somente dos seus participantes.

Embora o Blockchain tenha sido implementado em aplicações muito complexas, como criptomoedas, interações máquina-máquina (M2M) (SIKORSKI, HAUGHTON e KRAFT, 2017), em projetos de cidades inteligentes (BISWAS e MUTHUKKUMARASAMY, 2016), controles da cadeia de suprimento (FENG TIAN, 2016) e comércio de energia (MENGELKAMP, NOTHEISEN, *et al.*, 2018), os conceitos envolvidos são relativamente simples. Eles são usados para estabelecer três etapas principais: envio de dados, mineração e entrega de dados. Pode-se observar na Figura 5-1 que o processo descrito de forma genérica, pressupõe a existência das partes interessadas (usuários “A” e “B”), responsáveis pela motivação

da transação e dos mineradores, que são responsáveis pelo processamento das informações.

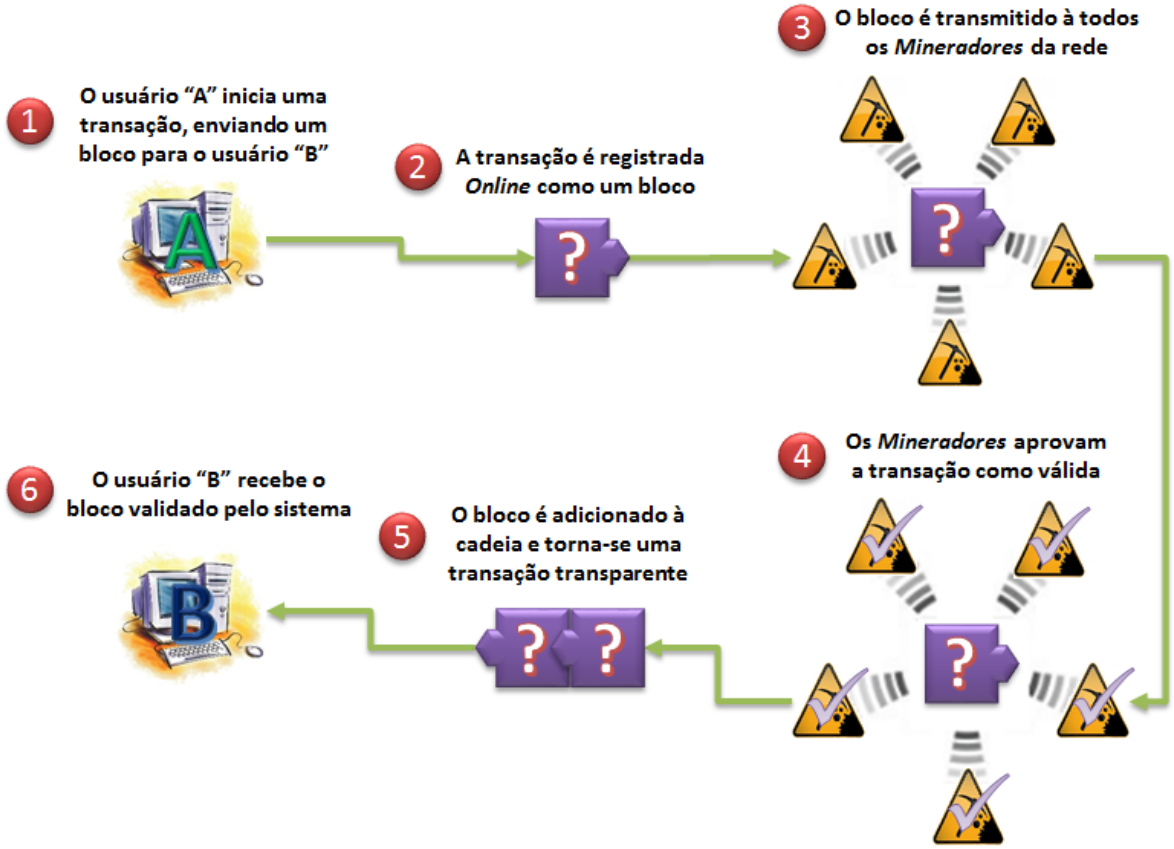


Figura 5-1: Fluxo dos blocos no Blockchain

Inicialmente, o dispositivo de origem envia um bloco de dados com uma identificação (ID) e registro de data e hora da origem da informação. Este bloco é registrado em cada um dos mineradores disponíveis no sistema, iniciando então a etapa de mineração. Todos os dados recebidos são criptografados e o processamento destes é realizado usando os chamados Contratos Inteligentes (CIs), conhecidos também pela sigla em inglês SCs (*smart contracts*), que contêm regras e métricas pré-definidas a serem satisfeitas. Todas as transações de dados são armazenadas e a rastreabilidade e criptografia do processo garantem a confiança desejada na entrega dos dados coletados, livres de manipulação externa. Os elementos citados e que compõem o processo de mineração são explicados a seguir.

5.2.1 Mineradores

Os mineradores compõem o núcleo principal de um sistema Blockchain e são responsáveis pela análise completa dos blocos de dados de entrada. Há diversos

métodos de uso de mineração dependem exclusivamente do tipo de aplicação que está sendo utilizado. O principal objetivo da mineração é a busca do consenso da maioria ou da totalidade dos mineradores sobre a análise dos dados criptografados recebidos no bloco de entrada (EYAL e SIRER, 2018). Caso a série de regras e testes criados para o bloco promovam resultados positivos, esses devem ser compartilhados com os demais mineradores a fim de verificar se o grau de consenso é suficiente para a aprovação final do bloco e a sua consequente adição à base de dados Blockchain. Devido ao número elevado de mineradores utilizados no âmbito das criptomoedas (CROSBY, PATTANAYAK e VERMA, 2016), há uma natural competição entre os mineradores pertencentes à rede. Por isso, se torna comum neste tipo de aplicação, o uso de mecanismos de consenso com premissas na premiação e que usam os protocolos de provas de trabalho (*POW – Proof of Work*) para mensurar os esforços despendidos por cada minerador. Este método motiva a inclusão de empresas especializadas no processo de mineração as quais usam a melhor tecnologia possível em hardware e software para alcançar altos índices de performance, recebendo assim uma melhor remuneração pelos seus serviços.

Os mecanismos de concenso existentes dos sistemas Blockchain como vistos em (BACH, MIHALJEVIC e ZAGAR, 2018), visam tornar o processo de mineração mais robusto e confiável, resolvendo problemas de escalabilidade, competição entre mineradores, consumo de energia dispendido na mineração, sincronismo de registro de blocos (SCHWARTZ, YOUNGS e BRITTO, 2014), performance na entrega das informações, dentre outras questões. No mercado de compra e venda de energia com comercialização ponto a ponto sem intermediários, algoritmos de consenso apresentados em (SORIN, BOBO e PINSON, 2019) tentam resolver problemas de múltiplas negociações bilaterais ocorrendo siultâneamente.

Os equipamentos utilizados para a mineração (BEDFORD TAYLOR, 2017) vem evoluindo a cada ano aumentando a capacidade de processamento aliado a baixo consumo de energia. A difusão das criptomoedas criou verdadeiros centros de mineração, com centenas e até milhares de máquinas processando algoritmos 24 horas por dia, gerando um mercado pujante de serviços de mineração.

A construção do algoritmo desenvolvido para a mineração em uma específica aplicação, deve levar em consideração o tempo de execução médio do programa em cada minerador e o tempo médio de entrega do bloco minerado para a base de dados do Blockchain. Dependendo da complexidade da aplicação, podem ser necessários

dezenas ou centenas de mineradores produzindo um tempo de entrega maior do que o esperado. Usualmente, a criptomoeda Bitcoin (ZHENG, XIE, *et al.*, 2017), com seus algoritmos de mineração complexos, leva cerca de 10(dez) minutos para processar um único bloco de transação financeira.

5.2.2 Contratos Inteligentes

Idealizado por N. Szabo (SZABO, 1997), os CIs podem ser entendidos como protocolos de validação com a finalidade de verificar termos e condições contratuais estabelecidos entre duas partes, mitigando a ação de intermediários. Qualquer transação que ocorra entre duas entidades em um processo, e que respeite uma série de regras, pode ser validada através dos contratos inteligentes de forma autônoma e digital, sem intervenções humanas. Este procedimento traz imediatamente a assertividade e previsibilidade desejada nos resultados das validações, transparecendo confiabilidade ao processo.

Os CIs se materializam na forma de programas que são executados dentro das plataformas computacionais dos mineradores. Os algoritmos são desenhados no sentido de atender às especificidades da aplicação a qual ele se destina, visando cobrir todas as condições necessárias que devem ser analisadas no conjunto de regras pré-estabelecidas no contrato.

Apesar dos CIs serem um dos elementos da tecnologia Blockchain, estes algoritmos são poderosas ferramentas usadas como processos determinísticos e independentes complementado as verificações de segurança de dados, inerente do Blockchain, com a verificação qualitativa dos dados recebidos pelo sistema.

A versatilidade dos CIs é demonstrada, por exemplo, nos mercados comercializadores de energias renováveis (RUTKIN, 2016) e no gerenciamento da flexibilidade de prosuidores em (POP, CIOARA, *et al.*, 2018). Neste exemplo, as cláusulas contratuais entre os consumidores e os produtores de energia renovável vizinhos são validadas em cada transação de compra e venda sem nenhuma intromissão das concessionárias de energia locais. Isso gerou maior liberdade de escolha dos produtores de energia, visto que o consumidor pode selecionar contratos que melhor se adequem às suas necessidades. Em um segundo exemplo, nos sistemas IoT (CHRISTIDIS e DEVETSIKIOTIS, 2016) os CIs são usados na identificação de ativos desde sua produção passando pelo transporte até chegar ao

destino final. Cada etapa é rastreada e validada pelo conjunto de regras previstas no algoritmo do CI. Este procedimento garante assertividade na estrega e impossibilita qualquer erro em todos o processo logístico pois trabalha em malha fechada, ou seja, necessita de comunicação do elemento IoT em todas as etapas do processo para que seja confirmada a etapa recém transposta.

Os CIs também são um importante recurso nos futuros sistemas autônomos de controle de tráfego de veículos (LEIDING, MEMARMOSHREFI e HOGREFE, 2016). O sistema aposta na plataforma da criptomoeda Ethereum para o autogerenciamento e controle de tráfego onde cada veículo respeita regras de trânsito e efetua mudanças de rotas baseado em informações de tráfego e de condições do tempo enviadas na rede de veículos que se comunicam diretamente entre si em uma rede VANET.

5.3 BLOCKCHAIN NO SCMI

As SGs possuem um número crescente de clientes consumidores e micro-produtores de energias renováveis que participam das redes cujas dinâmicas de consumo, fornecimento, armazenamento e preço da energia se tornam mais complexas a cada dia. Neste cenário, em que a qualidade e a confiabilidade dos fornecimentos de energia e dos processos de comercialização são extremamente necessários, é criado um terreno fértil para a aplicação do Blockchain (ECONOMIST, 2016).

Os operadores das SGs podem desenvolver contratos com base neste sistema definindo os parâmetros aplicáveis às operações de utilização dos serviços em questão. Todas as transações seriam registadas no sistema de transação de energia onde esta tecnologia permitiria a participação de usuários e fornecedores de maneira autônoma sem árbitros ou intermediários. O sistema funciona de forma transparente, permitindo que todos os participantes possam ver a situação do mercado de energia naquela SGs, possibilitando a monitoração da demanda, oferta e custo, dando poder aos usuários em decidir quando e como vender ou comprar sua própria energia seguindo parâmetros e regras já estipuladas em CIs (CHRISTIDIS e DEVETSIKIOTIS, 2016) que são consultados automaticamente a toda transação respectiva à um indivíduo ou conjunto de indivíduos registrados na rede.

Ainda se tratando das SGs, há constante movimento para se achar soluções viáveis e aplicáveis a curto e médio prazo para atender as necessidades sistêmicas

de grandes magnitudes e específicas para pequenos subsistemas. Nesta linha, em (DORRI, KANHERE, *et al.*, 2017) há uma tentativa que se apresenta como um método bastante criativo de envio de informações em uma rede inteligente residencial (*Smart Home*) e que tem como objetivo a comunicação de dados entre os dispositivos da mesma residência e entre estes e elementos externos de maneira segura e garantindo a privacidade das informações. O sistema prevê uma rede residencial em que a metodologia do sistema Blockchain é utilizada e há elementos mineradores representados por hardwares localizados em cada residência com algoritmos dedicados para esta função de verificação de consistência de blocos de informações que trafegam entre os elementos da rede. A ideia é uma solução de baixo custo, porém, de ambição escalar reduzida e visando apenas o atendimento da automação residencial e o controle da privacidade, não permitindo invasões externas nem a propagação das informações privadas do funcionamento da casa. O SCMI pode se utilizar desta tecnologia de maneira bastante importante e em grande escala, utilizando as características do Blockchain de maneira fundamental para o seu funcionamento.

5.3.1 O Fluxo de Dados

A primeira grande contribuição do sistema Blockchain no SCMI é o controle do tráfego de dados coletados por todos os agentes e medidores inteligentes. Conforme ilustrado no Capítulo 4, poderão ser usados dispositivos móveis, redes de comunicação em veículos (BRONZI, FRANK, *et al.*, 2014) e pontos de acesso wi-fi como *gateways* para transmitir dados das redes de distribuição de energia elétrica para centros de controle (INTANAGONWIWAT, GOVINDAN e ESTRIN, 2000).

Apesar de tratar de serviços públicos de medição de consumo de energia, o Blockchain proposto se caracteriza por uma rede do tipo privada, havendo cadastro prévio de todos os seus elementos, sejam eles, Agentes colaborativos ou os próprios elementos de medição do grupo de concessionárias que participam do sistema.

O sistema é capaz de entregar os blocos de dados coletados de maneira segura, criptografada (DIMITRIOU e KARAME, 2013) e rastreável para um determinado destino na rede que poderia ser o CC de uma ou mais concessionárias atuantes na região. Cada bloco gerado pelo Agente colaborativo ou pelo SGE, deverá possuir uma criptografia do tipo assimétrica (NAZEH, WAHID, *et al.*, 2018) que deverá

utilizar o conceito de assinatura digital, utilizando uma chave primária como base criptográfica para os blocos e utilizar chaves públicas para processo de descriptografia. Este método garantirá a confidencialidade, integridade, autenticidade e o não repúdio da transação (XU, REN, *et al.*, 2019), que se faz fundamental para a segurança das informações em todo o processo do Blockchain.

Conforme a Figura 5-2, considere a transação entre um agente tipo SMC e o centro de controle, na qual os dados de medição coletados de um dado medidor inteligente devem ser enviados para o centro de controle de uma concessionária.

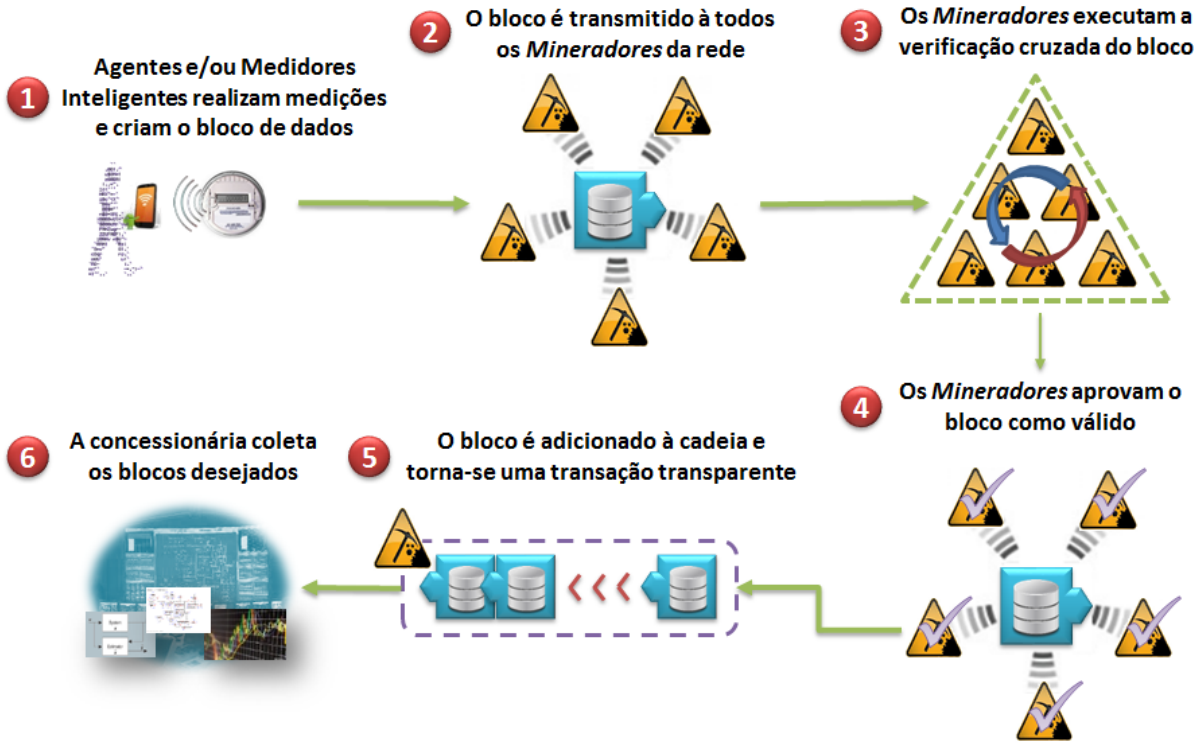


Figura 5-2: Blockchain na distribuição de telemedição

Usando Blockchain em (1) o SMC possui uma identificação única assim como o dispositivo de medição (SGE) e o CC de destino da informação. Em (2) O bloco de dados de medição é transmitido aos mineradores através dos agentes ou diretamente pelo SGE. Os elementos mineradores, que efetuam o trabalho de mineração à concessionária, recebem o bloco. Na etapa (3), todos os mineradores avaliam o bloco através de seus algoritmos. É uma fase decisiva no processo, cujo o bloco enviado pelo SMC pode ser ou não validado. Os mineradores verificam consistências básicas de segurança e todas as regras que definem a integridade e a categoria de cada informação enviada. Em (4) após aprovado por todos os mineradores, o bloco é

enviado para sua cadeia de blocos respectiva em (5), permitindo que a concessionária o colete do banco de dados dos mineradores em (6).

O CC pode usar os dados coletados para alimentar os SCADAs operacionais (i.e., DMS e ADMS) e algoritmos especialistas, como análise de alarme, estimadores de estado (GOMEZ-EXPOSITO, ABUR, *et al.*, 2011) ou simuladores de interrupção de fornecimento. Os operadores receberão os dados pertinentes às suas competências e assim ocorrerá respectivamente para os setores de manutenção e faturamento. Com isso, são garantidos o direcionamento seletivo e o sigilo de informação. O SCMI pode criar quantas cadeias de blocos quanto forem necessárias para guardar as informações de medições e alarmes. Na Figura 5-3 ilustra-se como se dá o direcionamento de um bloco enviado por um agente do SCMI e as opções de categorias de encadeamento.

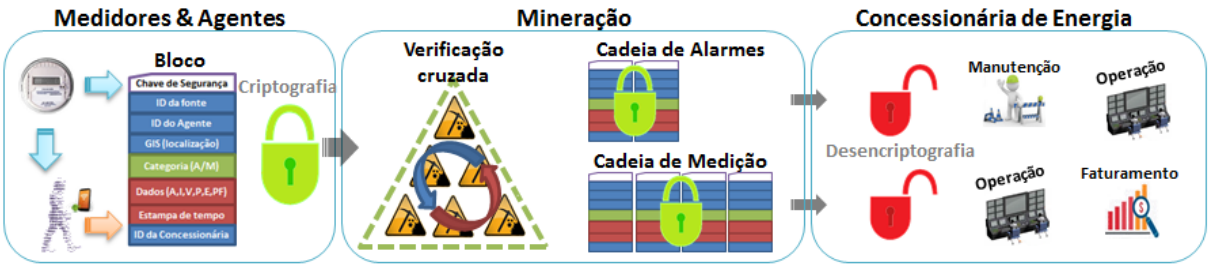


Figura 5-3: Encadeamento dos Blocos

As concessionárias possuem a liberdade de operação dos dispositivos de corte de fornecimento que estão montados nos medidores inteligentes como um de seus componentes principais. Por causa desta prerrogativa, que faz parte das SGs, se faz necessário um tipo de bloco que comporte as informações referentes a esta funcionalidade.

O Blockchain permite o processamento de dados de qualquer origem para qualquer destino passando pelos processos de mineração. Tanto os elementos que enviam dados ao sistema quanto os que recebem os blocos de dados são ativos no processo, exceto os medidores inteligentes. Uma ação proativa de todos os SGEs na busca de possíveis novos comandos nos bancos de dados dos mineradores geraria um custo proibitivo em termos de performance da rede de dados e de hardware de mineração. Por este motivo, os SGEs são os únicos elementos do SCMI que não buscam dados nos mineradores. No caso de comandos provenientes das concessionárias com destino aos medidores inteligentes, o processo de mineração ativa um elemento ativo de envio de bloco de comando diretamente para o medidor.

Figura 5-4: Blockchain na emissão de comandos

Conforme ilustrado na Figura 5-4 o processo de emissão de comandos começa na concessionária como indicado em (1) que possui sua identificação única assim como o dispositivo de medição (SGE) de destino do comando. Em (2) O bloco de comando é transmitido diretamente aos mineradores. Os elementos mineradores recebem o bloco e na etapa (3), todos os mineradores avaliam o bloco através de seus algoritmos. Os mineradores verificam as consistências básicas de segurança e todas as regras que definem a integridade do comando enviado. Após aprovado por todos os mineradores em (4), o bloco de dados é processado em (5) para seu envio espontâneo pela rede de dados até o medidor de destino. Já em (6), o bloco é enviado para sua cadeia de blocos respectiva.

5.3.2 Estrutura dos Blocos

Um sistema Blockchain começa basicamente com a criação dos blocos de dados. No caso do SCMI, cada bloco de dados contém o conjunto de campos pertinentes às informações aferidas e registradas pelo dispositivo de medição de energia (SGE). Este conjunto de dados fornece as informações necessárias ao processo de mineração. Todos os blocos de dados possuem exatamente a mesma

estrutura de dados que é suficiente para registrar as informações provenientes do dispositivo de medição.

Os blocos de medição foram concebidos neste trabalho a fim de integrar todas as informações necessárias para o processo da transmissão utilizando a tecnologia Blockchain. Os blocos carregam principalmente informações necessárias para serem usadas pela concessionária, tanto na cobrança de energia quanto para a operação e manutenção da rede. A Figura 5-5 ilustra um bloco com todos os seus respectivos campos sucedido por uma descrição detalhada de cada um destes quanto à sua importância e utilização em todo o processo.

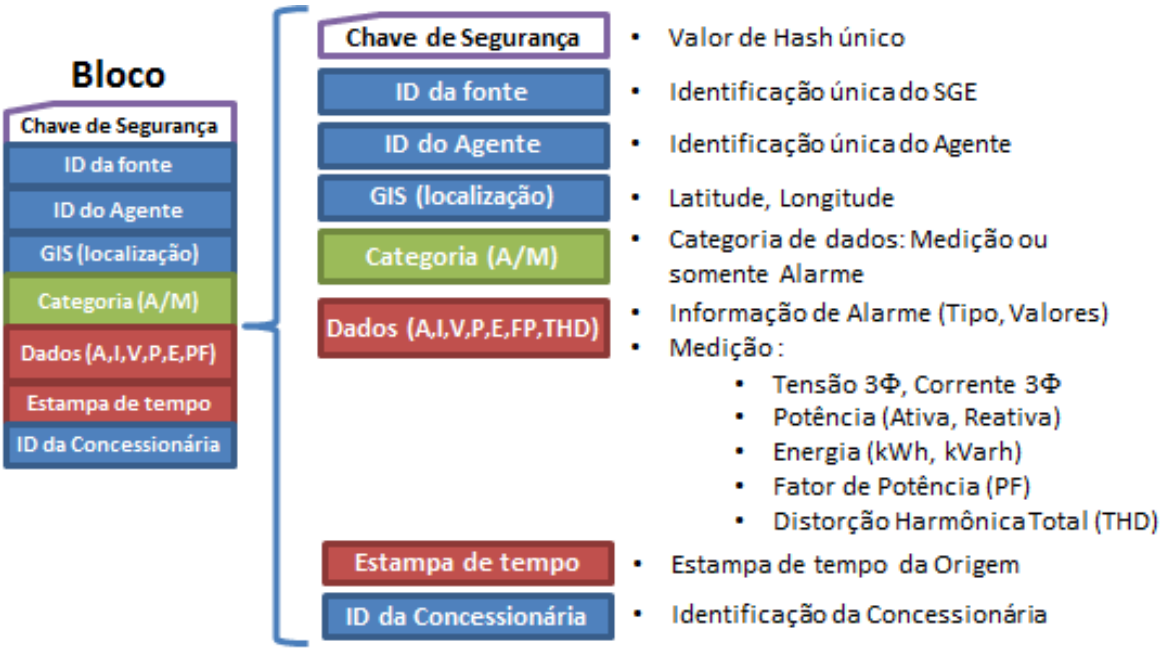


Figura 5-5: Estrutura do bloco de medição

a) **Chave de segurança**: O conhecido algoritmo de hash seguro de 256 bits (COURTOIS, GRAJEK e NAIK, 2014), criado pela agência de segurança nacional dos Estados Unidos (NSA), é geralmente adotado em criptografia de dados. Esse algoritmo cria anagramas em formato tipo *string* com valores únicos e foi escolhido para ser utilizado no campo Chave de Segurança devido à sua grande eficácia e vasta utilização na área de tecnologia da informação.

A Figura 5-6 ilustra os elementos que compõe o campo da “Chave de Segurança”. Este campo é usado na análise de consistência interna de segurança e no hash criptografado da cadeia de blocos que será apresentado na Seção 6.2.3. A função “sha256” é usada considerando a composição de

campos, que juntos, formam um anagrama único (formato *string*). Este anagrama representa as informações de onde se originou a medida, quais foram os valores medidos, quando foi medido e quem gerou as medidas.

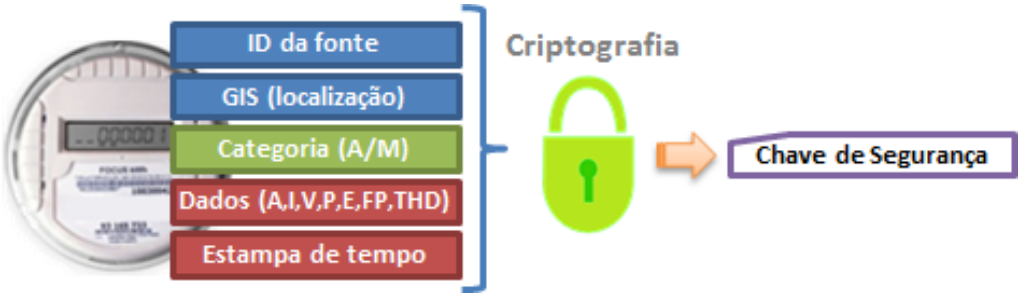


Figura 5-6: Campo de chave de Segurança do bloco de medição

A função apresentada em (5.1) ilustra a estrutura da função "sha256" responsável pela criptografia e consequente geração do anagrama que compõem o campo de "Chave de Segurança" (*SecurityKey*). Esta equação deve ser utilizada pelo SGE para a encriptação dos dados coletados já na origem. Caso o SGE não possua tal capacidade de encriptação, o Agente (SIC, SMC ou SVC) de coleta de dados de medição deve encriptá-lo para envio à nuvem de serviços Blockchain:

$$\text{SecurityKey} = \text{sha256}(\text{"GIS"}\ \text{";"}\ \text{"TimeStamp"}\ \text{";"}\ \text{"SGEID"}\ \text{";"}\ \text{"DataCat"}\ \text{";"}\ \text{"Data"}) \quad (5.1)$$

onde o campo "*GIS*" se trata da localização; "*TimeStamp"* é a estampa de tempo da leitura; "*SGEID*" é o identificar único da fonte de dados; "*DataCat*" é a categoria de dados (tipo); "*Data*" é uma string com os valores das medições. Todos estes campos estão detalhados a seguir.

b) **ID da Fonte**: A identificação da fonte da medição refere-se basicamente ao código único de identificação do medidor de energia na rede (SGE). Na filosofia de sistemas colaborativos, os ativos de medição podem ser utilizados por diversas concessionárias ao longo dos anos, conforme o desejo do cliente final. Caso este, mude de comercializadora de energia, uma nova concessionária passa a ser a detentora temporária deste medidor. Com isso, a identificação do medidor é perene e não muda ao longo do tempo.

c) **ID do Agente**: Este campo possui o código único de identificação do Agente colaborativo de medição que foi responsável pela coleta de dados do medidor (SGE). Caso o próprio SGE possua a capacidade de criação e emissão de blocos de medição direto para o SCMI, todas as informações serão transmitidas por ele utilizando-se do Blockchain. Neste caso, o SGE age como Agente e o ID do Agente é igual ao ID da Fonte de medição.

d) **GIS**: este campo refere-se à informação geográfica de latitude e longitude da qual o medidor está instalado. Em sistemas DMS e ADMS atuais, estas informações são essenciais para o monitoramento de ativos e para uma célere ação de manutenção corretiva.

e) **Categoria**: a categoria de dados (tipo), pode ser definida como de leitura de informações de dados de medição (“M”) ou blocos que também possuam eventuais alarmes (“A”). Este campo trata-se apenas de um modo de classificação do bloco, e pode ser usado pela concessionária de maneira a acionar diretamente a equipe de manutenção no caso de blocos de alarmes.

f) **Dados**: neste campo principal, são registrados todos os valores lidos das grandezas elétricas e informações de alarmes. Os dados de medição são aqueles obtidos por um medidor inteligente típico, tais como tensão (V), corrente (I), potência ativa (P), potência reativa (Q), energia (E), fator de potência (PF) e, eventualmente, a distorção harmônica total (THD). A taxa de atualização de cada valor de medição depende da tecnologia do dispositivo de medição empregado, variando entre 1 segundo e 15 minutos (tempo típico de integração de valores de energia). Os alarmes são compostos por tipo (i.e., falhas internas) e valores numéricos que representam a descrição do alarme.

De modo a de consolidar as informações desta seção, como exemplo prático, tomemos os seguintes valores dos campos abaixo referente à um dispositivo de medição hipotético:

- *GIS*: “-22.9690341,-43.1870259”
- *Time Stamp*: “01-01-2019 23:30:01.210”
- *SGEID*: “SGE0A0F”
- *Datacat*: “M”

- *Data* (Número de fases, Va, Ia, Vb, Ib, Vc, Ic, Pa, Pb, Pc, Qa, Qb, Qc, kWha, kWhb, kWhc, kVarha, kVarhb, kVarhc, PF, THD, Tipo de alarme, Valor do alarme):
  “3,220.01,3.01,220.02,3.02,220.03,3.03,662.23,664.46,666.69,0,0,0,251.01,252.02,253.03,0,0,0,0.97,4.8, 2,1”

A partir dos valores criados para os todos os campos que compõem o anagrama com hash criptografado, verifica-se como ficaria o resultado gerado pela função “sha256” referente ao campo de chave de segurança do bloco de medição:

SecurityKey = sha256(-22.9690341,-43.1870259;01-01-2019 23:30:01.210;SGE0A0F;M;3,220.01,3.01,220.02,3.02,220.03,3.03,662.23,664.46,666.69,0,0,0,251.01,252.02,253.03,0,0,0,0.97,4.8,2,1)

SecurityKey = “7D4EE7DE2AF66A74FBBBF18A9F52AD41B146377EC3A1F344935D323AFE645A22”

A composição do bloco de medição do exemplo acima é ilustrada na Figura 5-7 mostra como este bloco específico seria montado de acordo com os valores apresentados no exemplo.

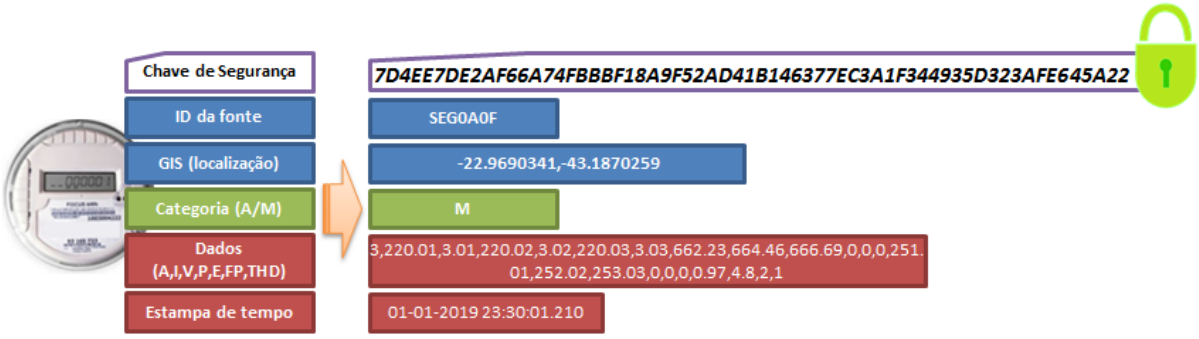


Figura 5-7: Bloco completo de dados de medição

Os blocos de comando são substancialmente menores que os blocos de medição e foram concebidos neste trabalho a fim de possibilitar a ação da concessionária sobre seus respectivos medidores inteligentes instalados na rede de distribuição. Através do serviço Blockchain, os blocos de comando são processados de forma prioritária em relação aos blocos de medição e se destinam diretamente à um determinado SGE para diversas finalidades. A função mais imediata e usada para os telecomandos é a de desligamento e religamento de serviços de fornecimento de energia à clientes à rede de fornecimento de energia (ABDULLA, 2015), contudo,

pode-se utilizar o telecomando para diversas outras funções. Uma delas é para o gerenciamento de energia sistêmico, que prevê um deslastre de cargas na rede de distribuição a fim de se manter a qualidade de serviço desejada. Esta ação ocorre em forma contingencial, ora por problemas de sub-frequência (KRZYSZTOF BILLEWICZ, 2015) ou por perdas de injeção nas redes, ou seja, o sistema de distribuição pode ser normalizado a qualquer momento e as cargas voltarem a serviço. O gerenciamento de energia tende a se aproximar cada vez mais dos clientes residenciais, transitando no universo interno das residências. Como pode ser visto em (CHARLY, REDDY e ASHOK, 2014) e (LIN e CHEN, 2017), há cada vez mais caminhos tecnológicos para que o descarte de cargas menos essenciais siga o caminho de micro cargas para o de macro cargas, começando dentro das instalações dos clientes para depois partir para a rede, com o desligamento total dos clientes.

Em termos de estado da arte, a reconfiguração automática de sistemas, conhecida como *Self-Healing* (ELGENEDY, MASSOUD e AHMED, 2015), está cada vez mais focada na utilização do potencial dos medidores inteligentes para serem instrumentos auxiliares em recomposição de redes de baixa tensão.

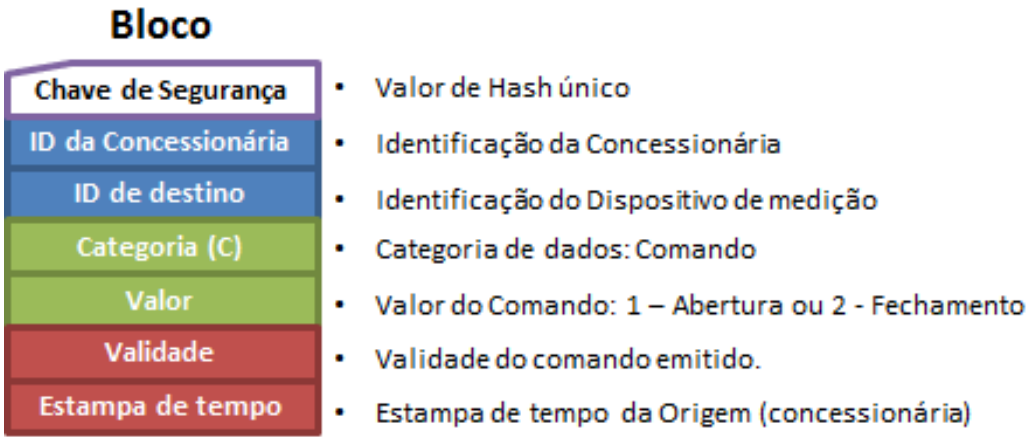


Figura 5-8: Estrutura do bloco de comando

Retornando à construção do bloco de comandos, a Figura 5-8 ilustra um bloco com todos os seus respectivos campos sucedido por uma descrição detalhada de cada um destes quanto à sua importância e utilização em todo o processo.

a) **Chave de segurança**: Assim como nos blocos de medição, o algoritmo hash de 256 bits (COURTOIS, GRAJEK e NAIK, 2014), é utilizado para a geração da chave de segurança do bloco. O anagrama em formato tipo string criado,

possui valor único é composto por todos os demais campos pertencentes ao bloco, conforme ilustrado na Figura 5-9.

Figura 5-9: Campo de chave de Segurança do bloco de comando

A função apresentada em (5.2), ilustra a estrutura do argumento da função de hash criptografado “sha256”, utilizada na geração do anagrama que compõem o campo de “Chave de Segurança” (*SecurityKey*):

$$\text{SecurityKey} = \text{sha256}(\text{"UtilityID" ";" "TimeStamp" ";" "SGEID" ";" "ValidTS" ";" "DataCat" ";" "CmdValue"}) \quad (5.2)$$

onde o campo “*UtilityID*” é o identificador da concessionária de origem do bloco; “*TimeStamp”* é a estampa de tempo do momento da solicitação de comando; “*SGEID*” é o identificador do dispositivo de medição de destino; “ValidTS” é a estampa de tempo da validade do comando; “*DataCat*” é a categoria de dados (tipo); “*CmdValue*” é o valor do comando emitido.

b) **ID da Concessionária (UtilityID*)***: A identificação da fonte de emissão do comando para o dispositivo inteligente de medição. Na prática, é o identificador da concessionária.

c) **ID do destino (SGEID)**: Este campo possui o código único de identificação do SGE de destino do bloco, ou seja, referente ao consumidor que terá seu serviço de fornecimento interrompido ou reestabelecido.

d) **Valor (CmdValue)**: o valor do comando poderá ser igual à 1 no caso de desligamento, 2 no caso de religamento ou qualquer outro valor que faça sentido conforme a implementação de novas funcionalidades no medidor inteligente afim de atender às tecnologias exemplificadas no início desta seção.

e) **Validade (ValidTS)**: neste campo é armazenada estampa de tempo de validade do comando, ou seja, até este momento definido, o bloco de comando poderá ser enviado ao SGE. Este campo se faz necessário pois as ações de desligamento e religamento podem ser efetuadas pela concessionária para testes de manutenção programada, ou até mesmo por funções já citadas nesta seção, referentes ao deslastre de cargas e à reconfiguração automática de rede. Nestes casos, é importante prever um prazo limite para a emissão do comando pelos mineradores afim de prever que algum atraso no envio de dados poderia entregar o bloco depois do prazo previsto.

Como exemplo prático, tomemos os seguintes valores dos campos abaixo referente à um bloco de comando proveniente de uma concessionária hipotética:

- *UtilityID*: “UT010A”
- *Time Stamp*: “12-02-2019 21:50:45.049”
- *SGEID*: “SGE0A0F”
- Validade: “12-02-2019 22:00:00.000”
- *Datacat*: “C”
- *CmdValue*: “1”

A partir dos valores criados para os todos os campos que compõem o anagrama hash, obtemos o seguinte resultado utilizando a função “sha256”:

SecurityKey = sha256(UT010A;12-02-2019 21:50:45.049;SGE0A0F;12-02-2019 22:00:00.000;1)

SecurityKey = “*744720794CC7F7AF81DA34D90AB4724C1F20B92150BF15B846A89174A034743E*”

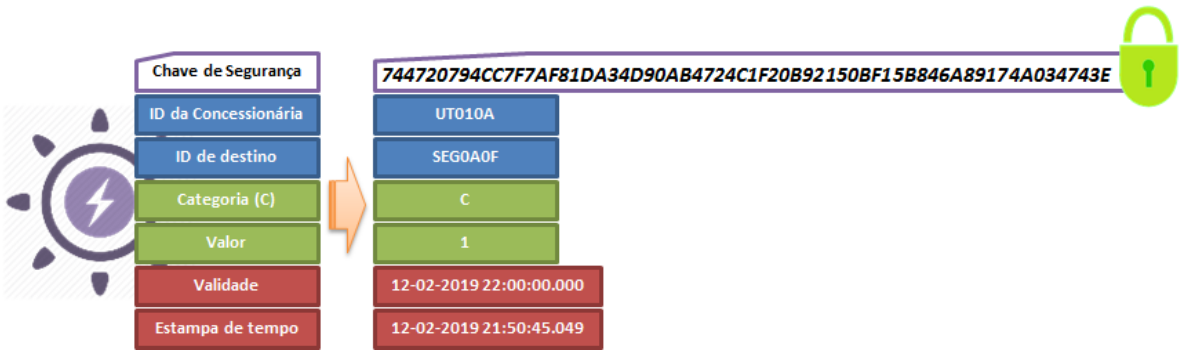


Figura 5-10: Bloco completo de dados de comando

A composição do bloco de comando do exemplo anterior é ilustrada na Figura 5-10 que mostra como este bloco específico seria montado de acordo com os valores apresentados no exemplo.

5.3.3 Mineração dos Blocos

Os mineradores, conforme mencionado anteriormente na Seção 5.2.1, geralmente exigem grandes recursos computacionais para resolver os complexos problemas matemáticos que demandam as aplicações na área financeira. Frequentemente são explorados os processamentos paralelos devido à computação de alto desempenho usada em criptomoedas e outras aplicações. No SCMI proposto, os algoritmos seguem regras com baixa complexidade computacional visando alcançar o melhor desempenho possível e entregar os dados em menor tempo possível às concessionárias de energia.

O SCMI pretende ser seguro e resiliente, evitando fraudes, mitigando eventuais problemas de comunicação e invasões cibernéticas. Para atingir esses objetivos, um mecanismo de verificação cruzada verifica os problemas de segurança, bem como o conteúdo de cada bloco recebido. Este processo tem três passos: (i) cada minerador valida o bloco de entrada; (ii) mais tarde, se o bloco foi aprovado, ele é enviado para os outros mineradores com uma sinalização de aprovação. Se todos os códigos hash dos mineradores coincidirem perfeitamente, o bloco é aprovado.

O caminho regular de qualquer bloco que ingressa no sistema Blockchain é a verificação cruzada entre mineradores seguida da entrega de dados para o elemento de destino dos dados, que podem ser a concessionária ou os próprios medidores inteligentes. A lógica do processo de mineração é dividida em três etapas, sendo a primeira parte do fluxograma ilustrada na Figura 5-11.

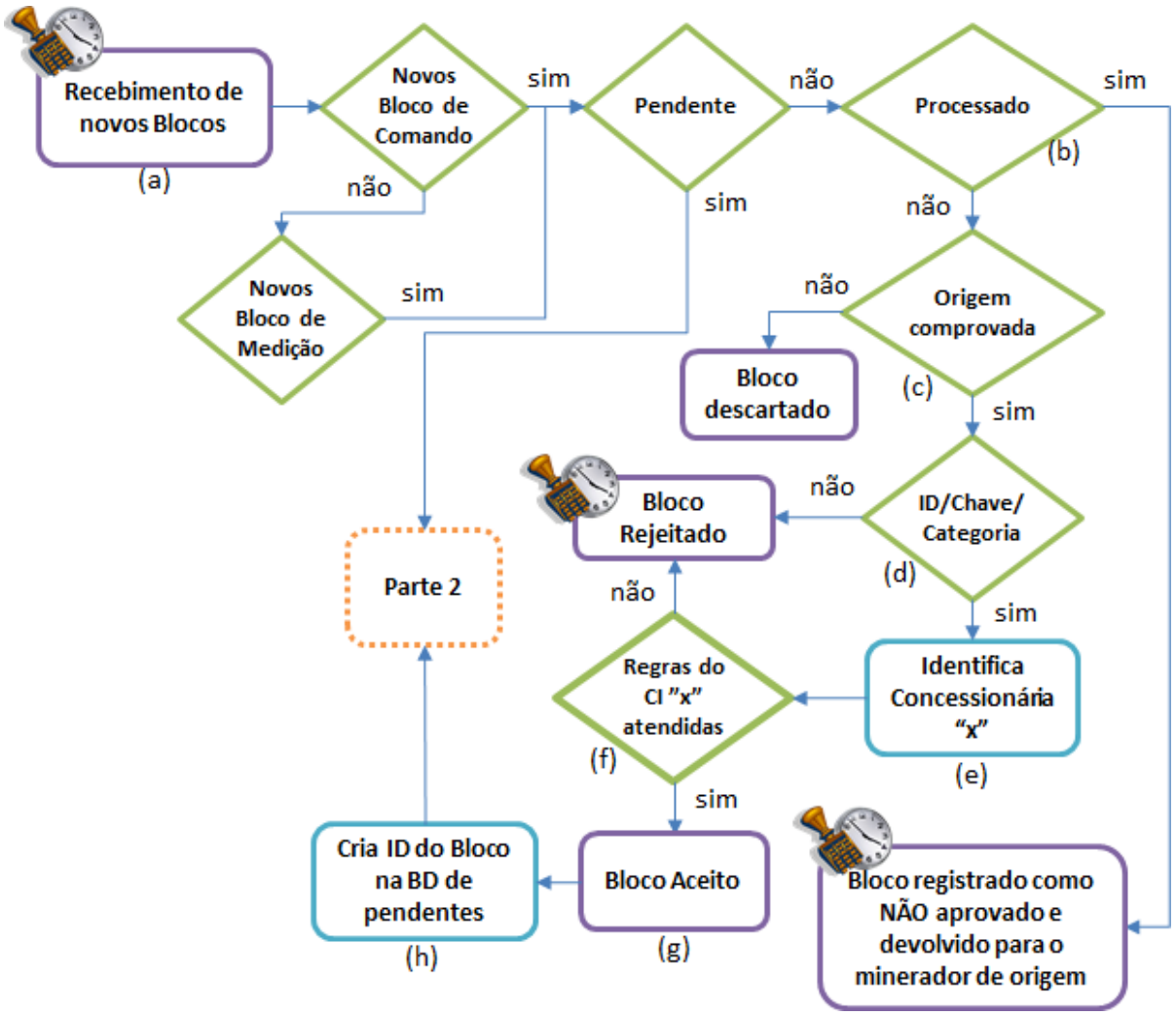


Figura 5-11: Fluxograma da Parte 1 – Filtragem de Dados

Os blocos são recebidos e passam pelo processo de filtragem dos blocos de entrada com verificações básicas de consistência. Nesta parte, também é chamado ao processamento, o contrato inteligente respectivo à concessionária que é o cliente final do bloco que está sendo processado. Na segunda parte são processadas as verificações cruzadas e finalmente na terceira parte, há a efetiva adição do novo bloco na cadeia de blocos (*Blockchain*). Apesar de fazerem parte integrante da mineração, os contratos inteligentes serão abordados de maneira separada na Seção 5.3.4. Os principais pontos do algoritmo do processo de mineração são detalhados a seguir:

a) Ao ser recebido um novo bloco, o sistema verifica se o tipo do bloco é de comando ou de medição. Os blocos de comando são prioritários e são processados antes de qualquer bloco de medição. O novo bloco de dados, é procurado na lista de blocos pendentes e na lista de dados processados. Caso

o bloco ainda não esteja pendente de aprovações e não tenha sido rejeitado, é considerado um bloco novo e passa pelo processo inicial de validação;

b) Caso o bloco já tenha sido processado anteriormente pelo minerador, ou seja, um bloco de mesma chave de segurança, quer dizer que este novo bloco é na verdade redundante à um outro recebido anteriormente. Este fato pode ocorrer nos blocos de medição no caso de múltiplos agentes terem coletado o mesmo bloco do dispositivo inteligente de medição. Como o bloco já foi processado, esta fase de filtragem evita um processamento repetido limitando a quantidade de dados que serão distribuídos para a concessionária. Neste ponto do algoritmo, o bloco é então marcado como não aprovado e devolvido para o minerador de origem, o que provocará uma reprovação em cascata pelo processo de busca de consenso realizada pela verificação cruzada. No caso de blocos de comando provenientes das concessionárias, não haverá redundância de fonte de dados, já que, somente um centro de controle da concessionária de energia emitirá o comando ao SGE.

c) Neste ponto, o novo bloco será processado somente no caso de ter sido originário diretamente da fonte conhecida pelo minerador, ou seja, de um Agente, SGE ou concessionária, no caso de comandos. Os blocos provenientes de outros mineradores, pelo processo de verificação cruzada, e que não estão no banco de dados de entrada ou no de blocos pendentes, serão rejeitados. Este procedimento evita a propagação de fraudes por mineradores adulterados;

d) Esta etapa do algoritmo verifica se a identidade única do SGE (SGEID) está na lista de SGEs cadastrados no sistema multiagente, ou seja, se está presente no banco de dados que contempla os dispositivos de medição de todas as concessionárias da região coberta pelo SCMI. A validação da chave de segurança do bloco é realizada comparando-se este campo (hash de origem) com um novo hash calculado (SecurityKey) conforme apresentado na equação (5.1), no caso de blocos de medição ou na equação (5.2), no caso de blocos de comando. Caso os valores sejam exatamente iguais, o bloco é validado. Por último, o campo de categoria dos dados é verificado. Caso o código da

categoria seja válido, o bloco finalmente passa para a próxima fase do processo;

e) Verifica se a identidade da concessionária, a qual possui os direitos das informações, é válida e direciona o processo para o contrato inteligente correspondente;

f) Nesta etapa, é acionado o contrato inteligente associado à concessionária detentora dos direitos do bloco. Conforme anteriormente mencionado, todas as regras serão verificadas para que o bloco possa ser aprovado pelo minerador;

g) Caso o bloco tenha sido aceito pelo contrato inteligente, este será incluído na tabela de blocos pendentes na base de dados (h) para ser utilizado em análises futuras. O bloco passará para a segunda parte do algoritmo.

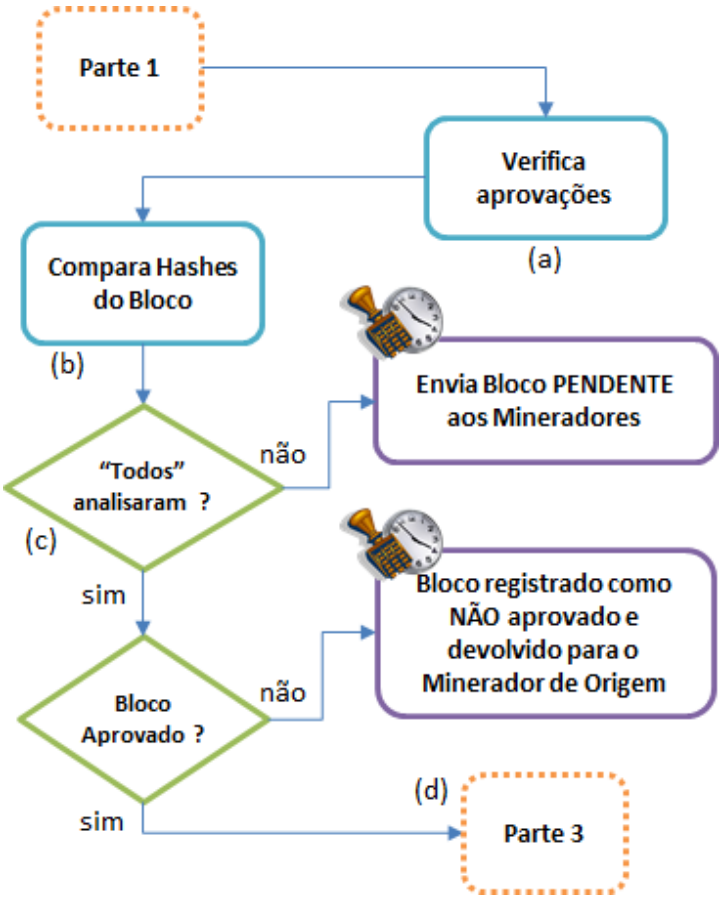


Figura 5-12: Fluxograma da Parte 2 – Verificação Cruzada

Na Figura 5-12 é ilustrada a segunda parte do fluxograma do módulo minerador cuja verificação cruzada se faz presente.Os principais pontos do algoritmo são detalhados a seguir:

a) Todos os blocos possuem identificação do hash calculado por cada minerador assim como a estampa de tempo de quando houve o processamento deste bloco por cada um deles. Neste caso, todos os hashs calculados são comparados quanto ao seu valor que deve ser exatamente igual em todos os mineradores;

b) Os hashes calculados (mesmo aqueles de outros mineradores) são comparados entre si para verificar se existem diferenças que representam alguma fraude ou erro no processo de mineração;

c) O bloco é enviado aos outros mineradores até que todos eles o aprovem. Esse procedimento de verificação cruzada garante que todos os mineradores recebam o bloco diretamente do dispositivo de origem ou através de um minerador que já o tenha analisado. Na Figura 5-13 é ilustrado o conceito da troca de blocos entre todos os mineradores no processo de verificação cruzada. Cada minerador possui o mesmo conjunto de contratos inteligentes e processa exatamente as mesmas lógicas de análise de consistências e de consenso;

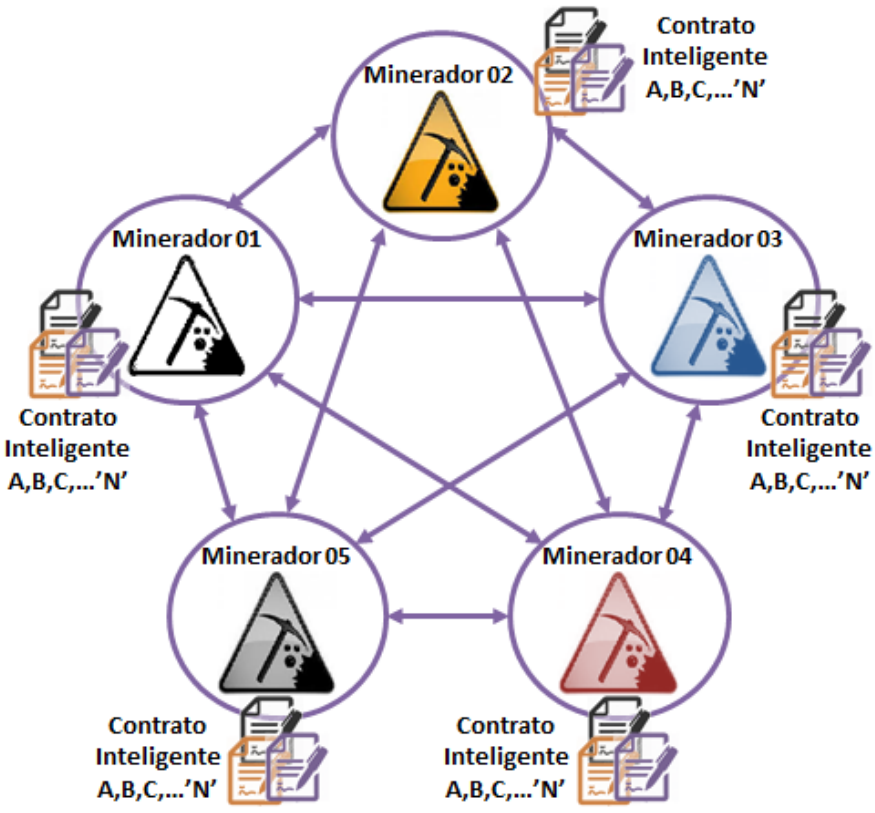
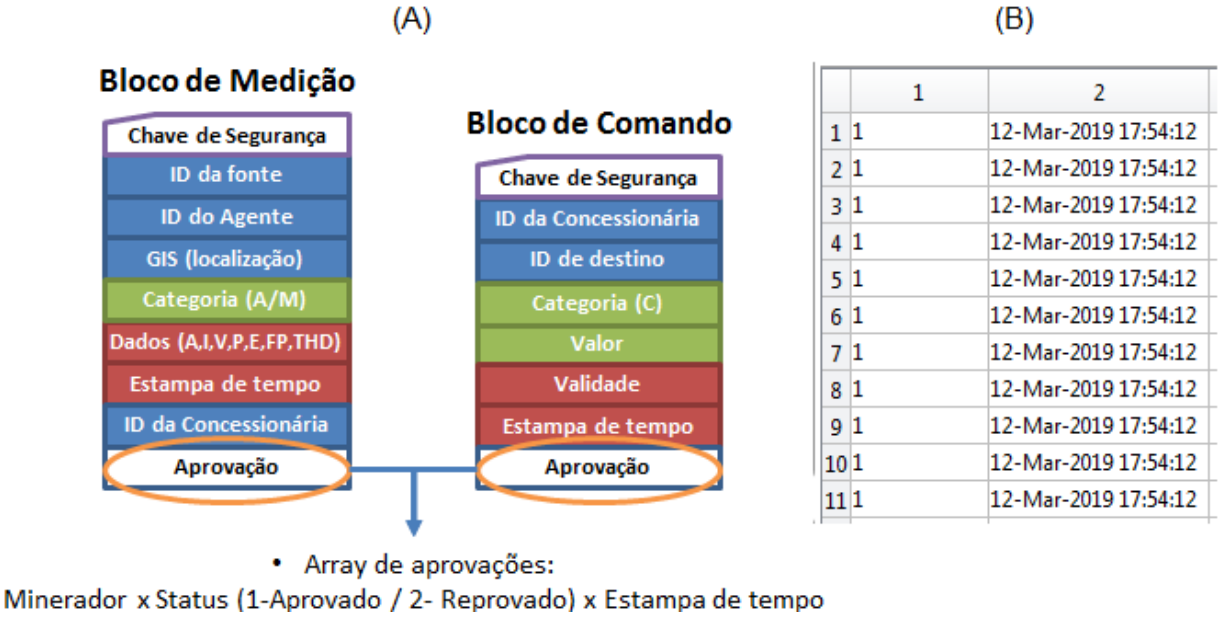


Figura 5-13: Verificação cruzada de mineradores

Na verificação cruzada, cada bloco que trafega entre os mineradores e que tenha sido minerado, é marcado pelo minerador que acabou de processá-lo com um indicador de status de aprovação (1 – aprovado e 2 – reprovado) e uma estampa de tempo referente ao momento da finalização da mineração. Esta marcação é realizada acrescentando um novo campo chamado de "Aprovação" conforme ilustrado na Figura 5-14. Este campo é composto por um array de "n" linhas referentes ao número do Minerador, e duas colunas contemplando respectivamente o status de aprovação (Figura 5-14 - A) e a estampa de tempo (Figura 5-14 - B).



	1	2
1	1	12-Mar-2019 17:54:12
2	1	12-Mar-2019 17:54:12
3	1	12-Mar-2019 17:54:12
4	1	12-Mar-2019 17:54:12
5	1	12-Mar-2019 17:54:12
6	1	12-Mar-2019 17:54:12
7	1	12-Mar-2019 17:54:12
8	1	12-Mar-2019 17:54:12
9	1	12-Mar-2019 17:54:12
10	1	12-Mar-2019 17:54:12
11	1	12-Mar-2019 17:54:12

Figura 5-14: Campo de aprovação das verificações cruzadas (A) e tabela de aprovações (B)

d) O bloco que foi aceito será enviado para o encadeamento de blocos da concessionária respectiva e fica disponível para ser coletado a qualquer momento.

Na Figura 5-15 é ilustrada a terceira e última parte do fluxograma do processo de mineração. Neste ponto, os blocos aprovados na verificação cruzada, são utilizados para o cálculo de novos códigos *hash*, mas estes, relacionados aos encadeamentos de blocos. A cadeia de blocos (CB) é atualizada com a adição do bloco aprovado por consenso entre todos os mineradores. Cada CB consiste em uma lista encadeada limitada que armazena todos os elementos até que um número máximo de elementos predefinido seja atingido. O tamanho desta lista depende

exclusivamente da capacidade de armazenamento dos mineradores e da estratégia de tecnologia da informação a ser aplicada. Este tema, não faz parte da discussão desta tese.

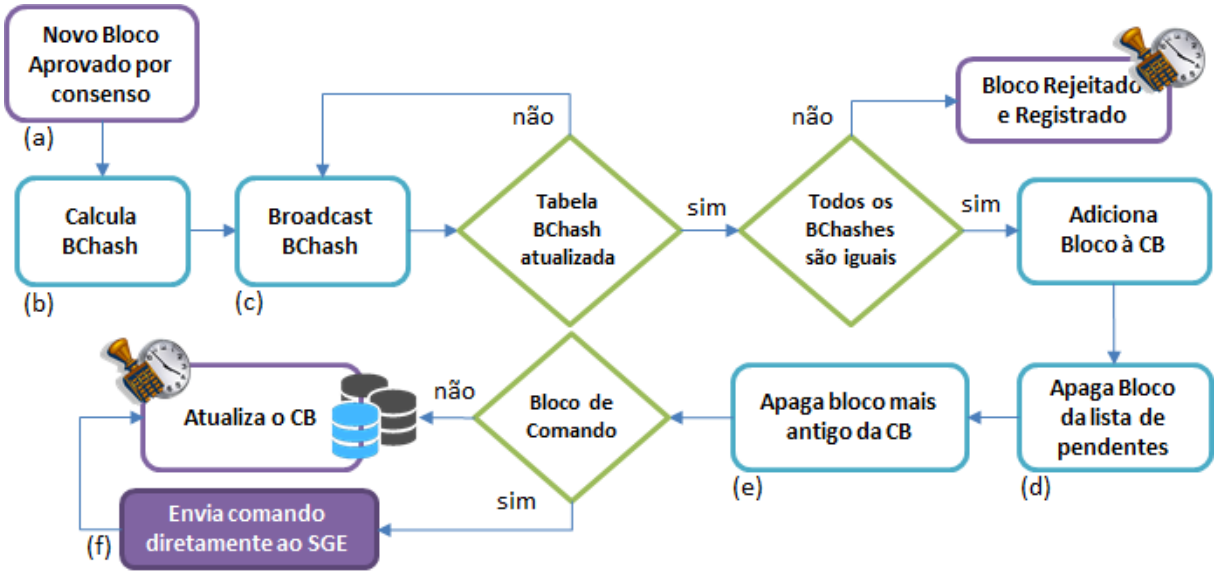


Figura 5-15: Fluxograma da Parte 3 – Encadeamento dos Blocos

Todos os passos do algoritmo do encadeamento de blocos são detalhados abaixo:

a) O bloco que foi aprovado pelo sistema de verificação cruzada é recebido na função para ser processado;

b) O código hash criptografado da CB, chamado de BChash (Blockchain hash) é calculado com base na composição do último hash disponível e o campo "Chave de Segurança" do novo bloco na cadeia. Com isso, todas as cadeias de blocos conterão um único código criptografado associado, não havendo necessidade de alteração em qualquer campo do bloco. Uma tabela com todos os BChash dos mineradores é atualizada. Esta tabela contém o BChash e o valor da chave de segurança do bloco testado. Com estas duas informações é possível verificar se cada minerador atualizou esta tabela com os BChash referente ao bloco em processamento. Esta função "sha256" (5.3) aplicada na CB segue descrita abaixo, onde "n" é o número da CB correspondente:

$$BChash_n = \text{sha256}(\text{Chave de Segurança}, \text{BChash}_{n-1}) \quad (5.3)$$

A Figura 5-16 abaixo ilustra o acréscimo de um bloco em uma cadeia já existente cujo BCHash atual será utilizado para o cáculo do próximo BCHash que já conta com a inclusão do novo bloco processado.

$BChash_{n-1}$ = "C960F6189F78BFBDC1584DED54B757F9430E826F53EA77E5EB2878698C394136"
$Chave\ de\ Segurança$ = "7D4EE7DE2AF66A74FBBBF18A9F52AD41B146377EC3A1F344935D323AFE645A22"
$BChash_n$ = "**283DF36DB4CE7B2C770CA5EB1135010BAADC8B71DB7124A0050AEE5AD9219B32**"

Figura 5-16: Cálculo do BCHash no encadeamento dos Blocos

c) Nesta etapa, a tabela de BChash dos mineradores é atualizada e o novo valor calculado pelo minerador é enviado via rede para os demais mineradores. Caso o BChash tenha sido calculado por todos e os códigos sejam exatamente iguais, o bloco segue adiante, caso contrário, o bloco é rejeitado. No caso de múltiplos BChashes discordantes em um mesmo minerador, este deverá ser descartado do sistema de mineração. Este é um fato extremo e denota inconsistência nas cadeias de blocos e uma possível corrupção de informações ou de códigos no minerador.

d) O bloco é apagado do banco de dados de blocos pendentes e fica armazenado somente no banco de dados de blocos processados;

e) O bloco mais antigo da cadeia deve ser eliminado caso o limite de armazenamento tenha sido alcançado;

f) Caso o bloco seja de comando, o processo prevê o envio direto do comando para o dispositivo de destino na rede. Mesmo neste caso, a cadeia de blocos de comando é atualizada juntamente com o BChash.

5.3.4 Contratos Inteligentes

Os algoritmos respectivos aos contratos inteligentes são implementados nos mineradores de maneira idêntica a fim de garantir o processamento nas mesmas

bases lógicas para a tomada de decisão quanto à aprovação ou não de um bloco. Cada contrato é pertinente à uma concessionária, ou seja, em um sistema aberto de comercialização de energia com dez empresas atendendo uma dada região coberta pelo SCMI, são necessários dez CIs, cada um com as suas próprias regras determinadas e programadas.

Os CIs são uma parte fundamental do sistema de telemedição e são preparados para atender tanto aos blocos de medição quanto aos blocos de comandos, conforme ilustrado na Figura 5-17. Eles são responsáveis por validar todos os termos, condições e restrições semânticas específicas para a aplicação em energia. Cada bloco testado não poderá ser rejeitado nesta fase, mas pode passar com observações que ajudam a concessionária a entender pequenos desvios, erros ou inconsistências descobertas para um dado bloco de medição ou um específico valor de grandeza medida.

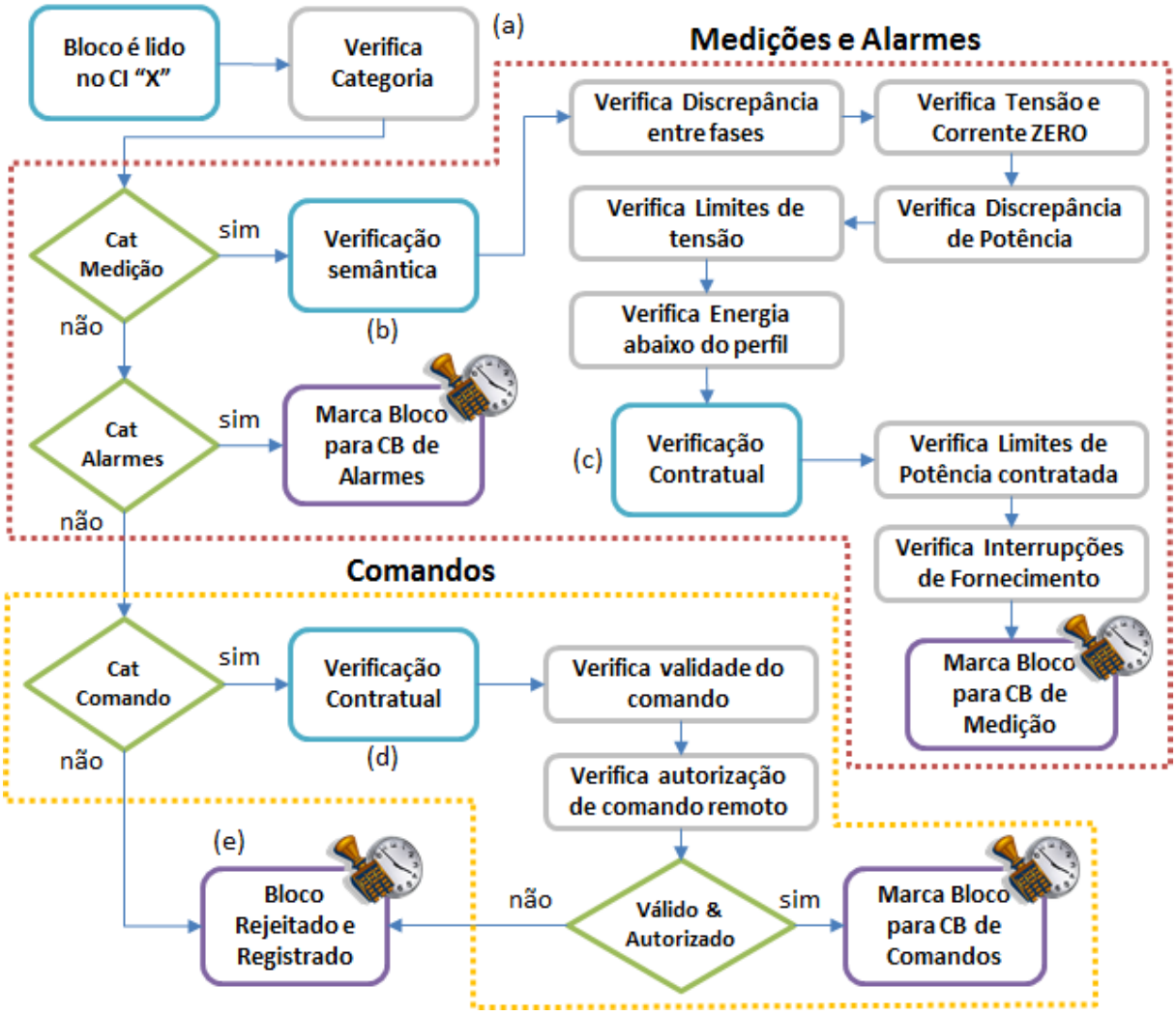


Figura 5-17: Fluxograma dos Contratos Inteligentes

O algoritmo dos CIs é descrito a seguir:

a) O bloco recebido no minerador já passou pela filtragem inicial de consistência e passa agora a ser verificado dentro da lógica do contrato virtual da concessionária cliente final do bloco. A categoria do bloco é verificada para encaminhar o bloco conforme o seu tipo (medição, alarme ou comando). Mais tipos de categorias podem ser utilizados de acordo com as necessidades da concessionária em subdividir a cadeia de blocos para um melhor processamento das informações;

b) Os blocos de medição passam por uma verificação semântica, a fim de verificar se os valores coletados são coerentes (do ponto de vista elétrico e de aplicação). Se o bloco não satisfizer algumas das restrições predefinidas, ele não será rejeitado, mas será marcado como não-conforme. Mais detalhes serão descritos a seguir em uma Seção específica;

c) Os blocos de medição passam pela avaliação de termos e condições contratuais, como aquelas relacionadas à potência contratada, interrupção do fornecimento de energia ou outras regras que se fizerem necessárias. Mais detalhes serão descritos a seguir em uma Seção específica;

d) Os blocos de comando passam pela avaliação de termos e condições contratuais onde primeiramente será verificado se o SGE definido como o destino do comando poderá sofrer telecomando. Esta informação está localizada no Banco de dados de configuração que será explicado na Seção 5.3.5. A segunda verificação avalia se a emissão de comando está dentro do seu prazo de validade. Mais detalhes serão descritos a seguir em uma Seção específica;

e) Neste ponto, os blocos com categorias desconhecidas são sumariamente descartados, já que não poderão ser avaliados pelo algoritmo implementado. No caso de blocos de comando, caso os critérios pertencentes à verificação contratual não forem satisfeitas, o bloco é rejeitado.

As verificações semânticas e contratuais são detalhadas a seguir:

i. Verificação Semântica

A análise semântica consiste na avaliação de todas as restrições e regras elétricas da aplicação específica. Se algumas restrições não forem satisfeitas ou forem parcialmente satisfeitas, serão emitidos sinalizadores. Quando isso ocorre, as situações sinalizadas são registradas no campo “Dados” (valor de alarme) e o bloco é enviado ao seu destino com essas informações. É possível encontrar um ou mais dos seguintes resultados finais listados abaixo, onde V, I, P, PF e kWh são respectivamente a tensão, corrente, potência ativa, fator de potência e consumo de energia medido:

- Aprovado sem restrições;
- Discrepância entre as amplitudes das fases A, B ou C, com base na discrepância entre fases permitida máxima (MAIPdis), é avaliada por:

$$\mathrm{MAIPdis} < \mathrm{abs}(V_{(1)} - V_{(2)}) \tag{5.4}$$

- Detecção do valor de tensão zero (ZVV) que utiliza um valor mínimo de tensão admissível para o fornecimento de energia no cliente: ZZV ≥ V;
- Detecção do valor de corrente zero (ZCV), que verifica se o valor de corrente sendo consumida está abaixo de um valor mínimo esperado para o cliente, a ser definido pela concessionária: ZCV ≥ I;
- Discrepância de potência medida com base na diferença máxima permitida de medição de potência (MAPMdis) entre o valor lido do medidor e o valor calculado com base nas informações de corrente, tensão e fator de potência lidas do medidor de energia:

$$\mathrm{MAPMdis} < \mathrm{abs}(P - (V * I * PF)) \tag{5.5}$$

- Carga acima do perfil sazonal com base na discrepância máxima permitida (MALMdis) para o valor de demanda lido no instante da medida em relação ao valor registrado na curva de carga típica no mesmo instante. O período de amostragem pode ser a cada minuto ou a cada segundo, dependendo exclusivamente do medidor utilizado:

$$\mathrm{MALMdis} < \mathrm{abs}(\mathrm{P} - \mathrm{LoadProfile(t)}) \tag{5.6}$$

Com esta verificação semântica, os desvios de medição de um estado de operação normal podem ser identificados e informados automaticamente para a concessionária, sem qualquer intervenção humana. Outras análises usando a disponibilidade de dados podem ser feitas em CIs, no entanto é preciso atenção especial ao desempenho do hardware dos mineradores e o impacto no tempo para entregar o bloco (BEDFORD TAYLOR, 2017).

ii. Verificação contratual de Blocos de Medição

Os termos e condições contratuais aplicáveis aos blocos de medição podem conter tantas cláusulas quantas forem necessárias para validar um bloco. Uma vez que o dispositivo de medição é conhecido (SGEID), até mesmo uma análise específica para cada tipo de cliente (por exemplo, residencial, comercial, etc.) pode ser implementada. Esta verificação foi composta de duas restrições básicas:

- Valores de potência que excederam a potência contratada:

Pmeas > Pcontract;

- Interrupção do suprimento de energia:

V < valor min de tensão admissível em todas as fases (usualmente 5%).

iii. Verificação contratual de Blocos de Comando

Os blocos de comando possuem duas condições definidas nesta tese a serem atendidas, porém, o CI poderia suportar mais critérios de verificação:

- A primeira verificação é quanto à autorização de telecomando. Caso o SGE esteja configurado como um dispositivo passível de telecomando, o algoritmo segue adiante para a segunda verificação. Em sistemas de SG, é comum o telecontrole de medidores inteligentes para os casos de interrupção de serviços de fornecimento e para o religamento do serviço. Algumas outras aplicações foram abordadas na Seção 5.3.2.
- No segundo critério testado, o campo “Validade” é comparado com a estampa de tempo do momento da mineração. Caso o prazo tenha se passado, o comando não poderá ser emitido. Esta verificação evita que comandos indevidos sejam enviados para o SGE em questão, levando por exemplo à uma possível interrupção acidental de fornecimento.

5.3.5 Integração dos Bancos de Dados

Ao longo das seções anteriores, foram explanadas funcionalidades no processo de mineração e sobre a leitura e escrita de blocos em bancos de dados (BD) residentes nos mineradores. Para ilustrar melhor a integração entre as bases de dados e o processo de mineração, a Figura 5-18 apresenta todas as etapas da mineração e as ações sobre os bancos de dados que são quatro:

a) BD de configuração (Figura 5-18 - 1) com os as listas de concessionárias, Agentes e SGEs que fazem parte da rede elétrica contemplada pelo sistema de mineração Blockchain;

b) BD de entrada ((Figura 5-18 - 2a e 2b), com os blocos enviados pelos Agentes do SCMI, SGEs e concessionárias aos mineradores;

c) BD de blocos pendentes (Figura 5-18 - 3) que ainda se encontram no processo de avaliação;

d) BD de blocos processados (Figura 5-18 - 4) que armazena o histórico de todos os blocos recebidos e aprovados ou reprovados pelo sistema.

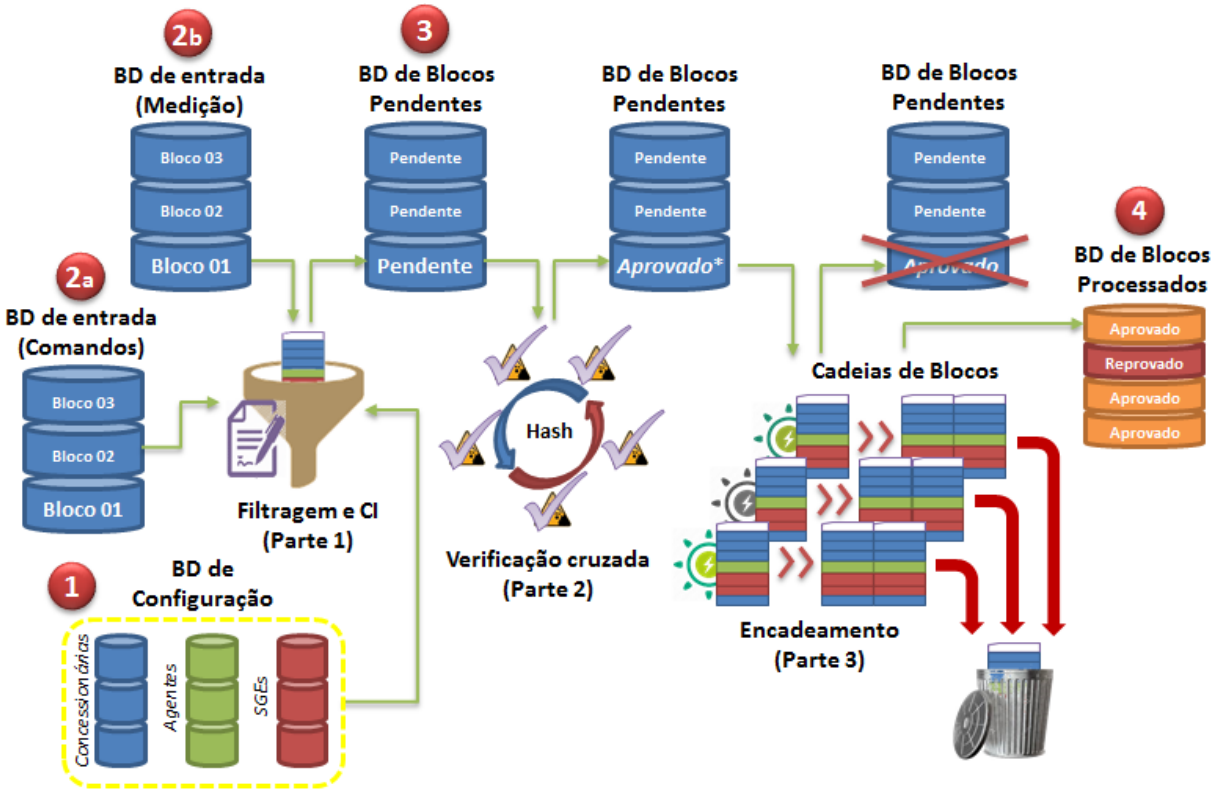


Figura 5-18: Bases de dados do Minerador

O banco de dados de entrada é responsável por armazenar todos os blocos de dados gerados pelos Agentes, SGEs e concessionárias. Nos casos de blocos de comando, estes possuem prioridade e devem ser processados antes de qualquer novo bloco de medição. Depois da primeira verificação, ou filtragem dos dados recebidos (Figura 5-11), os dados aprovados nesta faze são armazenados em um novo banco de dados de blocos pendentes.

Cada um dos blocos pendentes deverá ser testado no processo de verificação cruzada (Figura 5-12), e caso aprovado, deverá ser adicionado no encadeamento de blocos respectivo a cada concessionária. O BD de blocos pendentes é atualizado e os blocos aprovados ou reprovados são movidos para o banco de dados de blocos processados. Este último BD armazena todos os dados processados, tanto os aprovados quanto os reprovados.

Todos os BDs são gerenciados seguindo a filosofia *First in First Out* (FIFO) para manter os requisitos de limite de tamanho de armazenamento, ou seja, o primeiro bloco a entrar na BD é o primeiro bloco a sair para o descarte, caso seja necessário.

5.3.6 Blockchain integrado nas SGs

As SGs podem ser de pequeno, médio ou grande porte podendo se encontrar isoladas ou interligadas a outras redes. Os principais objetivos da comunicação de dados em projetos de SGs passam por disponibilidade, confiabilidade e segurança dos dados recolhidos. As tecnologias disponíveis e alguns conceitos aplicados ao problema de gestão e transporte de dados são abordados a seguir.

As soluções AMI tradicionais fornecem sistemas baseados em sensoriamento digital de grandezas elétricas que se estendem desde os consumidores de energia até o seu respectivo provedor de serviços (YAN, QIAN, *et al.*, 2013), admitindo comunicação bidirecional. Além disso, o AMI permite a implementação de muitas funções importantes que não se encontravam disponíveis em tecnologias anteriores, e.g., medição de consumo de energia automática e remota, conexão ou desconexão de serviços, detecção de adulteração em dispositivos de medição, identificação e isolamento de pontos com falhas e monitoramento de tensão ao longo das linhas de distribuição.

As tecnologias aplicadas em comunicações nas AMIs que conectam dispositivos de medição (JIXUAN ZHENG, GAO e LI LIN, 2013) aos CCs das

concessionárias são numerosas: rede de RF (ROTONDO, 2006); ponto-a-multiponto (KIM, FONSECA, *et al.*, 2007); serviço geral de rádio por pacotes; dentre outras. A grande massa de dados a ser transmitida impõe um grande desafio para os sistemas de comunicação. Por isso, é importante buscar soluções eficientes que atendam adequadamente aos requisitos associados à comunicação em tempo real, bem como à integridade e segurança dos dados.

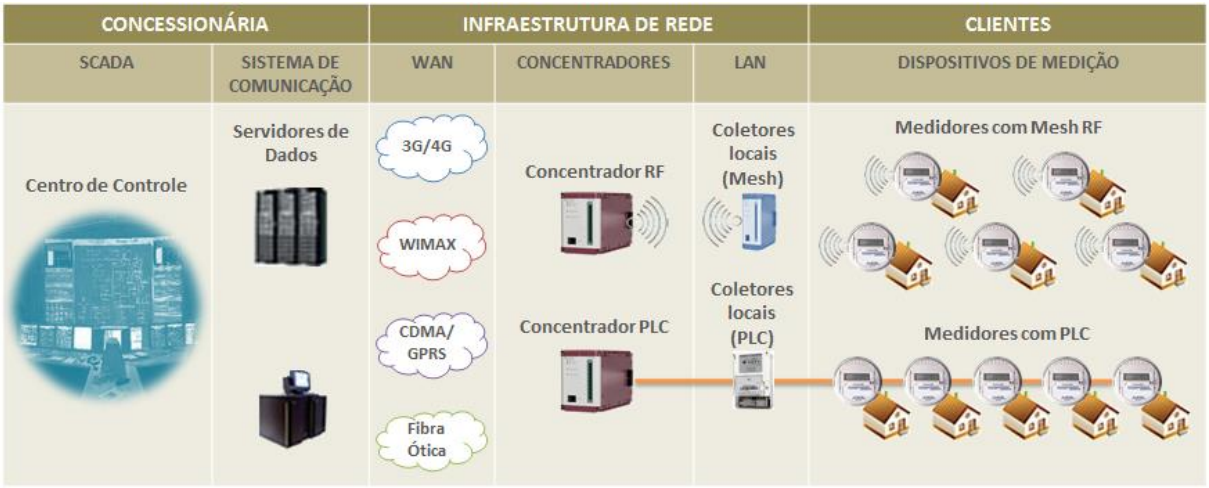


Figura 5-19: Soluções de infraestrutura avançada de medição

Na Figura 5-19 são ilustrados alguns tipos de redes adotadas atualmente como solução de AMI utilizando as disseminadas redes RF Mesh (i.e., ZigBee) e redes tipo PLC com os respectivos ativos mínimos necessários para o seu funcionamento. As soluções AMI possuem custos elevados em equipamentos e serviços, transitando desde os medidores inteligentes nos clientes finais, até os ativos referentes aos hardwares, softwares e serviços de instalação.

Normalmente, as SGs coletam dados de medição dos medidores inteligentes usando coletores locais localizados ao longo da área de cobertura e distribuem todos os dados para os concentradores. Os concentradores são conectados aos provedores de serviços de dados usando tecnologias diferentes (por exemplo, 3G, 4G, WiMAX, GPRS, outros) que entregarão os pacotes de dados ao servidor de dados específico dentro da concessionária de energia.

Tecnicamente, todo o processo de medição remota é crítico e existem muitos pontos passíveis de falha, nomeadamente os coletores, concentradores, serviço de dados e servidores de dados. Os coletores e concentradores, geralmente, não possuem nenhuma redundância e as falhas de hardware não são raras. Não há inteligência alguma nesses dispositivos que funcionam como interfaces de

comunicação; consequentemente, nenhuma validação qualitativa de dados pode ser realizada.

Como mencionado anteriormente, a escolha de uma rede de comunicação apropriada constitui tarefa difícil, mormente devido a: quantidade expressiva de dados, restrição no acesso aos dados, restrições de acesso à informação do consumo do cliente, autenticidade dos dados, confidencialidade dos dados sensíveis e facilidade de expansões futuras. Soma-se a isto que os grandes centros urbanos podem ter as chamadas áreas de alto risco, muitas vezes sem infraestrutura adequada e que são obstáculos para a leitura e manutenção dos medidores de energia. As infraestruturas de comunicação existentes que contemplam *hotspots* de internet e redes celulares móveis devem ser consideradas, uma vez que permitem a troca dados de forma eficiente. Os medidores inteligentes podem usar dispositivos móveis, redes de comunicação em veículos (BRONZI, FRANK, *et al.*, 2014) e pontos de acesso wi-fi como *gateways* para transmitir dados de sistemas de distribuição de energia elétrica para os CCs (INTANAGONWIWAT, GOVINDAN e ESTRIN, 2000).

Soluções tais como as utilizadas na concessionária Ausgrid da Austrália (KELLY, 2011), integram até dezenas de milhares de dispositivos de medição em concentradores móveis com tecnologia 4G. Estas soluções já estão em operação há alguns anos e seguem migrando para tecnologias mais econômicas e focadas na rede de dados denominada *Long Term Evolution* (LTE), criada com base no GSM e WCDMA**.** Esta tecnologia de quarta geração em telefonia está sendo cada vez mais procurada como alternativa ao 3G, por ser uma tecnologia móvel que prioriza o tráfego de dados em lugar do tráfego de voz, o que proporciona uma rede de dados mais rápida e estável. Estas soluções usualmente utilizam um sistema de alta confiabilidade com concentradores locais de dados para garantir a segurança das informações bem como a sua disponibilidade. Apesar da tecnologia e da robustez do desenho da solução, este caminho vem a acrescentar mais elementos ao sistema e sendo assim, mais pontos passíveis de falha e mais custo de manutenção.

As SGs lidam comumente com uma grande quantidade de dados enviados remotamente por medidores inteligentes, UTRs das subestações de MT e BT e equipamentos inteligentes da concessionária, instalados ao longo das redes. A proteção contra ameaças cibernéticas é uma demanda real e exigida por instituições reguladoras e operadoras dos sistemas de distribuição. A segurança de dados na

metodologia Blockchain utiliza a criptografia como uma das principais ferramentas, que pode garantir a fonte de dados, integridade e assertividade requeridas nas SGs.

O envio de todos os dados medidos remotamente diretamente para a nuvem de serviços Blockchain pode reduzir drasticamente os custos na infraestrutura de comunicação, considerando o uso dos hotspots e redes celulares existentes. A simplificação desta solução de AMI também proporciona uma menor demanda no gerenciamento dos ativos instalados na rede. Essa solução pode robustecer as SGs ao utilizar vários elementos de conexão (*gateways*) de comunicação (i.e, hotspots públicos, privados e antenas celulares) e redundância significativa de dados coletados através dos Agentes colaborativos e dos próprios dispositivos de medição inteligente.

A Figura 5-20 apresenta a solução de AMI na abordagem proposta que inclui os elementos do blockchain descritos neste trabalho. Iniciando a análise do diagrama no lado dos dispositivos de medição temos as seguintes etapas que demandam um detalhamento comparativo mais aprofundado:

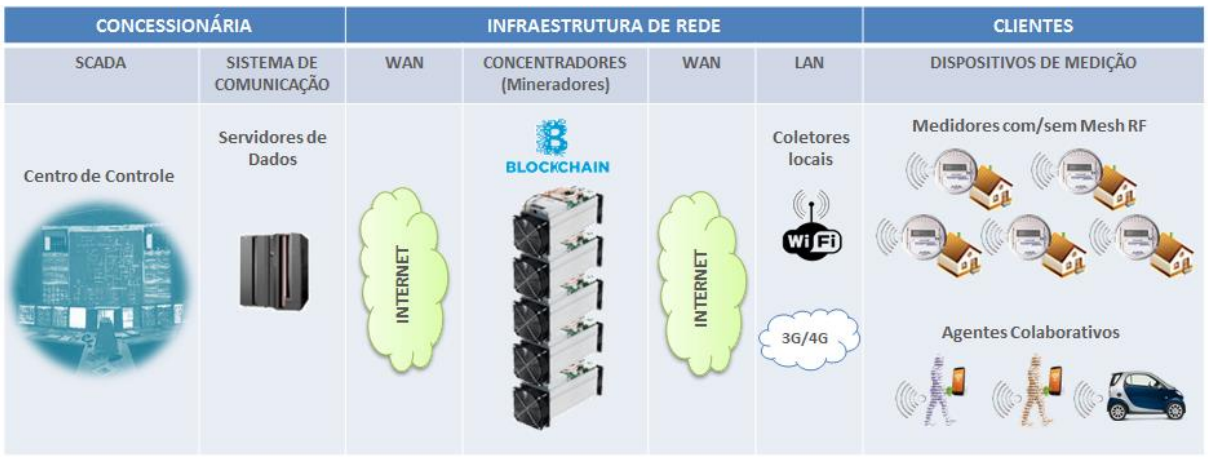


Figura 5-20: Soluções AMI baseada em Blockchain

a) **Clientes**: todas as informações referentes às medidas elétricas desejadas podem ser coletadas pelos agentes colaborativos e / ou pelos medidores inteligentes. Por este fato, o sistema possui a possibilidade de redundância na coleta de dados de medição. Nos sistemas tradicionais (Figura 5-19) os medidores inteligentes possuem interfaces de rede dependentes de concentradores proprietários e são a única fonte de informação de leitura de medições.

b) **Infraestrutura de Rede**: usando interfaces de comunicação existentes, como pontos de acesso wi-fi e redes de telefonia celular já instaladas, o fluxo de dados para os mineradores Blockchain se faz garantido com estes meios de transporte. Também nesta etapa, é presente a redundância de meios de comunicação auxiliando na robustez do processo de telemedição. Através de provedores de serviços de Internet (ISP), os pacotes de blocos de dados são entregues aos mineradores os quais realizam, em primeira instância, o trabalho análogo aos concentradores de dados das AMIs tradicionais. Após o processo de mineração (consulte a Seção 5.3.3), através de um ISP, os dados coletados e minerados vão para os servidores de dados da concessionária.

   Nesta etapa é clara a utilização de estruturas de comunicação já existentes em boa parte dos centros urbanos e em parte das áreas rurais. Nas soluções AMI tradicionais (Figura 5-19), a demanda de instalação de ativos de hardware é grande e fundamental para a operação do sistema.

c) **Concessionária**: os servidores de dados concentram as informações em seus bancos de dados próprios e os disponibilizam internamente segundo as diretrizes de tecnologia de informação da concessionária de energia. Estes servidores, existentes hoje nos processos de telemedição, demandam de aplicações desenhadas para a comunicação com os mineradores Blockchain e respectiva coleta de dados dos mesmos. Com os dados já coletados, o centro de controle poderá endereçar os dados aos clientes finais adequados (i.e., operação, faturamento, manutenção, etc.).

5.3.7 Compartilhamento de Serviços

Uma das grandes vantagens do Blockchain e a capacidade de criptografia de dados que pode ser usada de diversas maneiras conforme já exemplificado neste documento. No SCMI, através da criptografia é possível a convivência de diversas concessionárias de serviços de energia em uma mesma região ou macrorregiões compartilhando o mesmo serviço de Blockchain aplicado. Os elementos mineradores serão programados para identificar isentamente qual concessionária possui os direitos sobre qual pacote de dados (blocos). Essa metodologia possibilitará mais uma

redução substancial de gastos com infraestrutura já que todos os elementos mineradores serão compartilhados entre as empresas.

Na Figura 5-21 são ilustrados todos os elementos necessários para a rede do SCMI com a informação de quais elementos são ou não passíveis de compartilhamento entre as comercializadoras de energia.

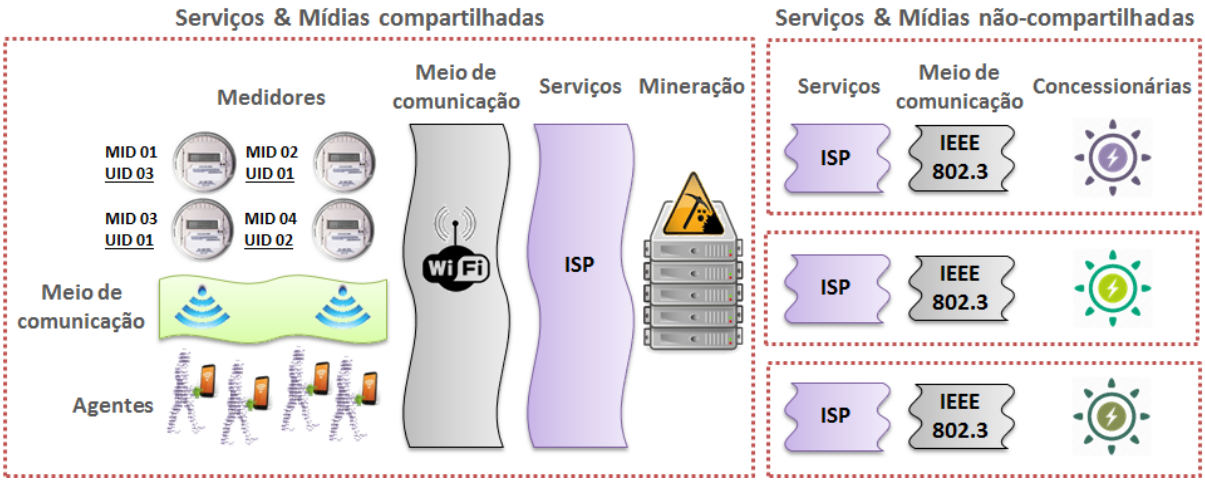


Figura 5-21: Compartilhamento do SCMI entre Concessionárias

Basicamente, todos os elementos fora das instalações das concessionárias podem ser compartilhados. O crescimento do mercado de serviços de armazenamento, processamento e gerenciamento de dados de forma remota vem crescendo a cada ano e se tornou uma realidade nos mercados de tecnologia da informação. A terceirização destes serviços se apresenta como uma mudança de paradigma na área de energia que ainda se conserva resistente às mudanças mais significativas na gestão da informação.

Capítulo 6

Simulações e Resultados

6.1 INTRODUÇÃO

Este capítulo apresenta os resultados obtidos para diferentes situações testadas através de um simulador desenvolvido para promover uma prova de conceito referente ao SCMI proposto. Para tal, foram criados módulos de simulação no intuito de evidenciar em cada etapa do processo a viabilidade da metodologia proposta.

6.2 O SIMULADOR

O simulador desenvolvido nesta Tese apoia-se nos softwares do fabricante MathWorks®, nomeadamente Matlab™ e Simulink, sendo este último usado como ferramenta de visualização gráfica.

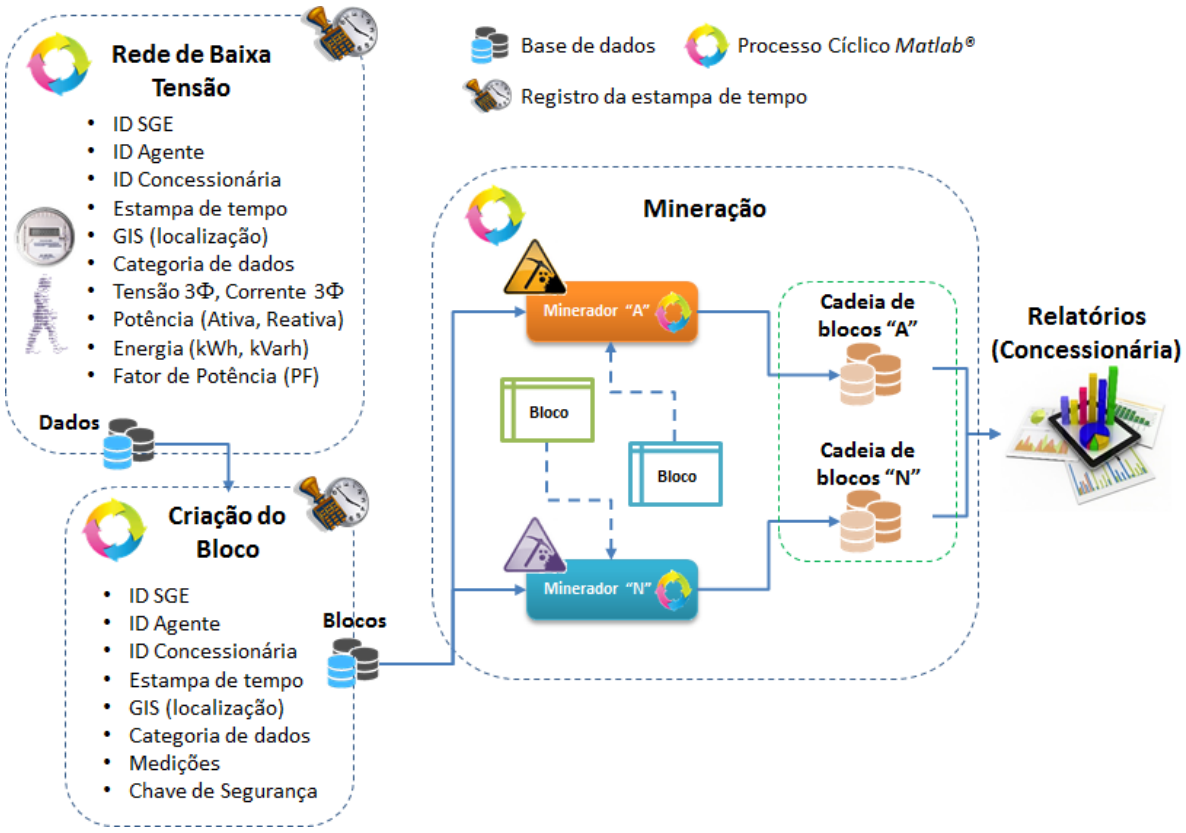


Figura 6-1: Módulos do Simulador

Os principais módulos do simulador estão ilustrados na Figura 6-1 e compreendem: módulo simulador da rede de baixa tensão, seguido pelo gerador de blocos de dados, pelo módulo de mineração e, finalmente, o módulo de relatório que simula a concessionária. Com este simulador é possível avaliar inicialmente o desempenho da metodologia proposta sobre tempos de processamento de blocos e a identificação de fraudes. Para tal, os algoritmos foram implementados para se garantir a gama de funcionalidades necessárias para avaliar o processo de mineração e a segurança para os blocos de dados em uma rede que utilize a tecnologia Blockchain.

6.2.1 Módulo de Rede de Baixa Tensão

O primeiro módulo de simulação destina-se à geração de valores de medição de grandezas elétricas tais como: energia elétrica consumida pelos clientes e subestações secundárias (postos de transformação); potências trifásicas ativas e reativas, fator de potência; tensões e correntes trifásicas.

O simulador desenvolvido contém uma interface amigável que permite modelar diferentes tipos de sistemas de distribuição de energia elétrica tomando por base a experiência obtida na pesquisa relatada em (ZANGHI, BROWN DO COUTTO FILHO e DE SOUZA, 2011). A sua biblioteca de elementos da área elétrica (i.e., geradores, disjuntores, cargas, etc.) foi baseada em blocos básicos “*Simscape Power Systems*”, muito difundidos na área científica. A interface gráfica permite ao usuário configurar um sistema de distribuição através de arquivos tipo “csv” e definir parâmetros referentes a dimensão e topologia do sistema. O simulador identifica erros de consistência entre aquilo que foi desenhado graficamente no Simulink e respectivamente o que foi configurado via arquivos com colunas divididas “csv”, sendo bastante robusto neste sentido.

De forma escalonável e dependendo exclusivamente da capacidade computacional do ambiente em que será executado, o simulador suporta quaisquer redes elétricas, independentemente do seu porte ou nível de tensão apresentando como característica uma grande facilidade para seu uso e configuração. Com o módulo de rede desenvolvido é possível acrescentar elementos compatíveis com a biblioteca de sistemas de potência utilizada, bem como apresentar e testar algumas situações operacionais típicas. Algumas funcionalidades são:

- Representação trifásica de um sistema de distribuição;
- Modelagem de redes de diversos portes, como as que cobrem ruas, bairros, ilhas, e até grandes áreas urbanas;
- Adição de modelos de microgeração, tais como, centrais térmicas, solares, eólicas, dentre outras;
- Adição de modelos de sistemas de armazenamento de energia;
- Geração de faltas utilizando modelos para simular curtos-circuitos, sobrecargas, faltas de alta impedância ou outras faltas disponíveis na biblioteca do Simulink;
- Introdução de elementos para provocar perturbações no sistema, tais como, usuários invasores, i.e., aqueles não previstos na rede que consomem energia clandestinamente;
- Adição de chaves/disjuntores que podem ser comandados, alterando a topologia da rede sem que seja necessário redesenhá-la;
- Alocação de medidores (SGEs) com tabela dinâmica de carga configurável, sendo disponibilizadas para o sistema as medições de valores de corrente, tensão, potência ativa/reativa e energia consumida (acumulador) e fator de potência;

Na Figura 6-2 é ilustrada uma parte da rede elétrica de distribuição utilizada para compor os circuitos desenhados no Simulador do SCMI. Elementos especiais de medição de corrente e tensão trifásicos foram criados, assim como cada elemento SGE que simula um medidor de energia completo com medidas de corrente (magnitudes e ângulos), tensão (magnitudes e ângulos), potência ativa/reativa, energia ativa/reativa e fator de potência. Estas medidas são fornecidas a cada varredura do sistema e ficam disponíveis para os agentes do SCMI coletarem, quando estiverem na proximidade de um SGE.

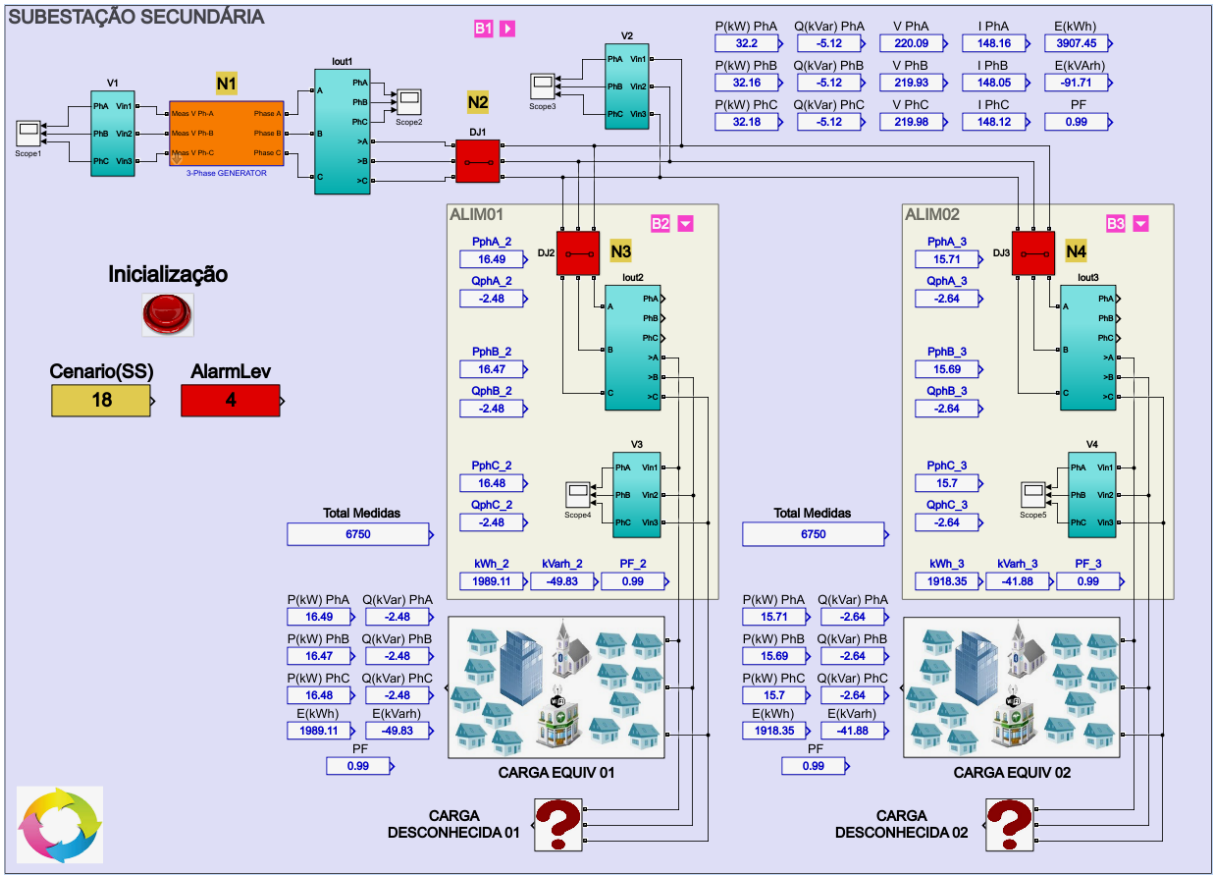


Figura 6-2: Módulo de Rede de distribuição de energia elétrica

Elementos tipo disjuntor ou chaves (i.e., “DJ1”, “DJ2” e “DJ3”) foram criados para proporcionar versatilidade, caso o usuário queira mudar a topologia da rede sem precisar redesenhar novamente o sistema no Simulink. Com estes elementos, podem ser ligados e desligados circuitos e simular assim uma perda de fonte geradora.

O fluxograma simplificado apresentado na Figura 6-3 a seguir mostra como funciona o encadeamento de funções internas. O módulo de simulação de rede começa antes dos demais módulos para que as medidas já estejam disponíveis na primeira varredura do simulador, com isso, o SCMI pode processar a criação dos blocos e enviá-los para a mineração. Desta forma, o simulador é capaz de processar dados da rede elétrica de distribuição de forma independente dos módulos referentes ao Blockchain (criação de blocos e mineração), o que se assemelha ao mundo real.

Através deste módulo, é possível alterar os valores de medição, inserindo erros sobre os valores calculados no fluxo de potência através das telas de controle que serão detalhadas no item f). Esta funcionalidade oferece a possibilidade de simulações de fraudes nos medidores de energia, erros de medida no instrumento e perdas de comunicação com o medidor.

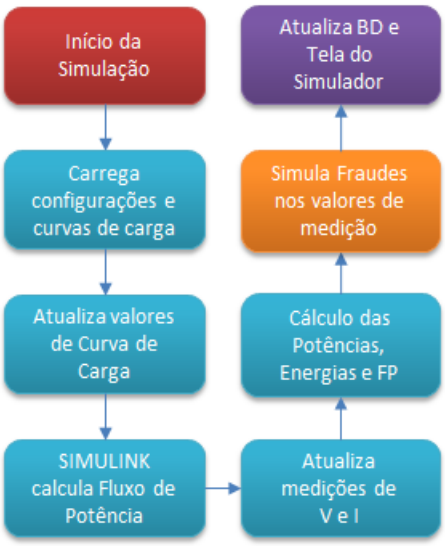


Figura 6-3: Fluxograma do módulo simulador da Rede

Diversos elementos (blocos) de simulação foram criados a partir da biblioteca padrão do Simulink. As alterações tiveram como objetivo tornar o módulo de rede mais versátil e configurável, atendendo às necessidades variadas de simulação. Os elementos criados são explicados em detalhes a seguir.

a) Subestação Secundária

A subestação secundária criada no Simulink, conforme ilustra na Figura 6-4, compõe-se basicamente de gerador, medidores e disjuntor de saída. O gerador simula a entrada de tensão na SS, que no caso real se apresenta em média tensão, mas no caso da simulação, pode ser configurada com valores de baixa tensão. Caso seja necessário simular o abaixamento de média para baixa tensão, o transformador de potência pode ser acrescentado a fim de simular eletricamente um posto de transformação.

O disjuntor de saída da subestação (“DJ1”), alimenta a barra de baixa tensão que liga os circuitos alimentadores de distribuição local. Cada um dos alimentadores supre a demanda de suas respectivas cargas.

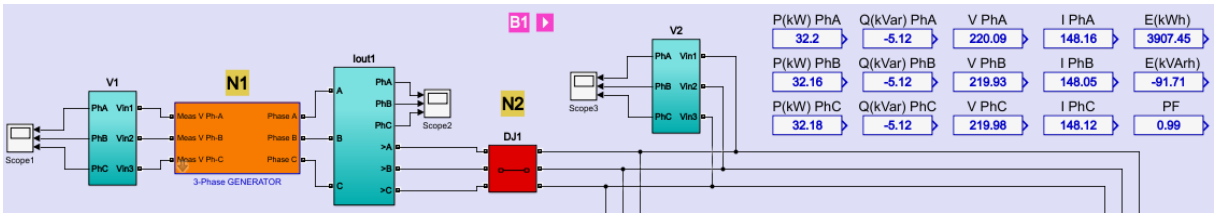


Figura 6-4: Subestação secundária

Os dados do gerador trifásico podem ser facilmente alterados, atuando-se em suas fases de maneira independente, a partir da tela de configuração ilustrada na Figura 6-5 (item “C”). Todos os valores de tensão por fase (Va, Vb e Vc), ângulos por fase, valor de frequência fundamental da rede e potência ativa de produção, podem ser editados pelo usuário. Este bloco foi construído de maneira simples e didática para facilitar a simulação de condições adversas.

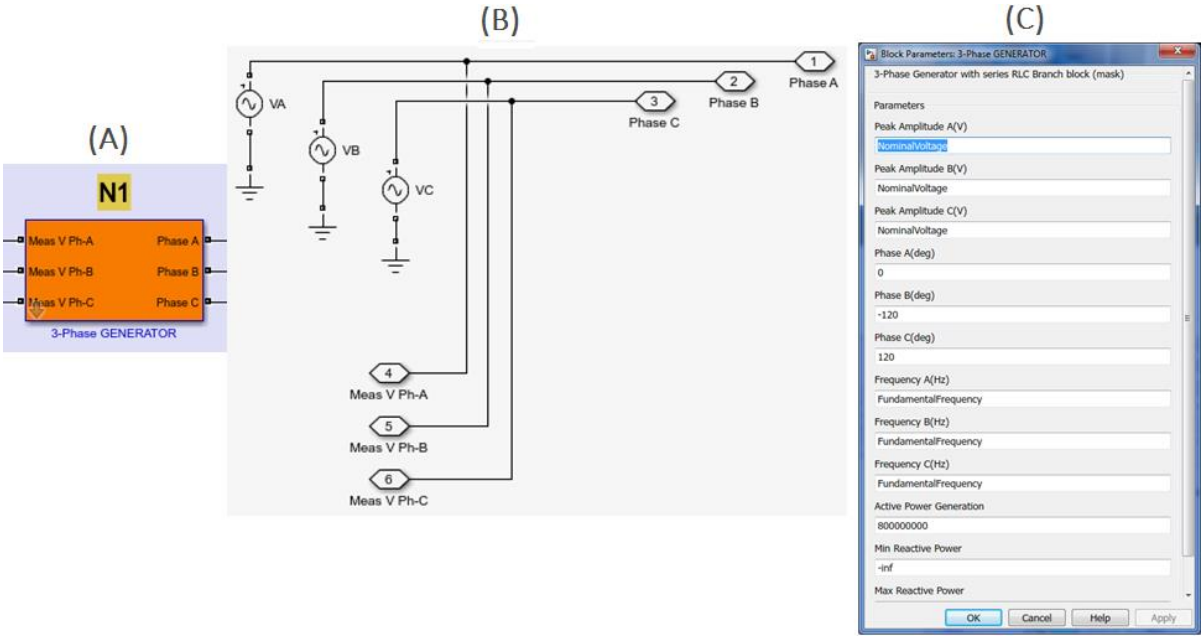


Figura 6-5: Gerador (A), diagrama de blocos (B) e tela de parâmetros (C)

b) Alimentadores

A saída do alimentador suporta todas as cargas necessárias para a simulação, desde que o gerador (Figura 6-5) possua a potência ativa máxima configurada suficiente para suportar o somatório de todas as cargas de todos os alimentadores. O número de alimentadores criados no simulador depende exclusivamente da capacidade computacional da estação de trabalho, já que o sistema é totalmente modular e configurável pelo usuário.

Nos alimentadores (Figura 6-6) são instalados elementos de disjuntor (“DJ”), medidores de corrente (“Iout”) e medidores de tensão (“V”). Com isso, é possível simular medições provenientes de uma UTR para análise de consistências entre as medições coletadas dos clientes (cargas) e o correspondente valor medido no alimentador.

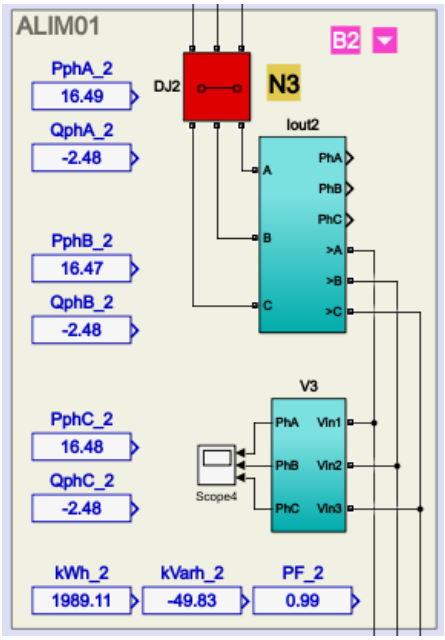


Figura 6-6: Alimentador

c) Medidores de Energia e Cargas associadas

Os medidores (SGE) estão agrupados em um único objeto que suporta quantos SGEs o usuário desejar. Os valores das curvas de carga de cada um dos SGEs criados são somados. O valor total é correspondente a demanda configurada na carga equivalente (Figura 6-7 – A) e compõe a carga total no alimentador respectivo. Todos os valores de medição são expostos em tela (Figura 6-7 – B).

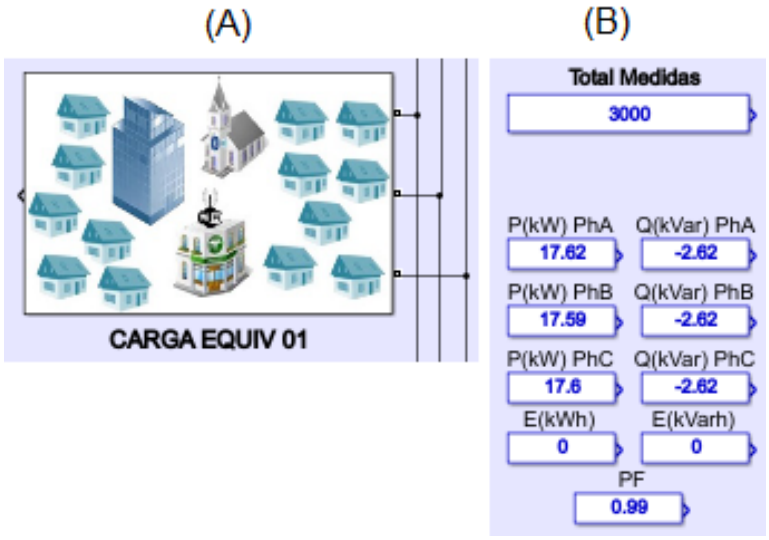


Figura 6-7: Dados de Medição (A) do grupo de SGEs (B)

Todas as medições são realizadas por fase (Va, Vb, Vc, Ia, Ib e Ic) de acordo com os resultados do fluxo de potência fornecidos pelo Simulink. Os resultados desta

medição são diretamente dependentes da carga associada denominada de “LOAD_SGExx”, já que o Simulink calcula o fluxo de potência a cada varredura de simulação. Os valores de tensão e corrente aferidos são utilizados para o cálculo das potências, fator de potência e energias consumidas pela carga. A realização deste cálculo pelo algoritmo desenvolvido no Matlab™, gera versatilidade para o tratamento das medições, possibilitando a simulação de erros de telemedição, como será visto nas próximas seções.

Todas as medidas coletadas são gravadas com a devida estampa de tempo e registro de localização da origem, sendo a latitude e longitude representadas aqui pelas coordenadas “x” e “y” dos elementos medidores de energia alocados pelo usuário na tela do simulador (Simulink).

Para os cálculos das potências ativas e reativas, são utilizadas as equações 6.1 e 6.2 onde são utilizadas as medições de corrente e tensão:

$$P_{carga} = real[(V_{carga}) \times conj(I_{carga})] \quad (6.1)$$

$$Q_{carga} = imag[(V_{carga}) \times conj(I_{carga})] \quad (6.2)$$

Sendo:

'V_{carga}' a tensão no ponto de entrega na carga;

'I_{carga}' a corrente no ponto de entrega na carga;

Referente às cargas criadas no simulador de rede de baixa tensão, foram criados 2 tipos de cargas: residenciais e comerciais. Cada tipo possui um perfil específico de demanda que é utilizado no simulador, mais especificamente no objeto de carga acoplado no medidor inteligente.

Figura 6-8: Perfil de carga residencial

As cargas podem ser alteradas manualmente em termos de potência ativa e/ou reativa, mas podem também ser alimentadas por valores pré-determinados em uma curva de carga de 24 horas. Valores típicos de demanda residencial (Figura 6-8) e comercial (Figura 6-9) foram utilizados com inspiração no exposto em (JARDINI, TAHAN, *et al.*, 2000).

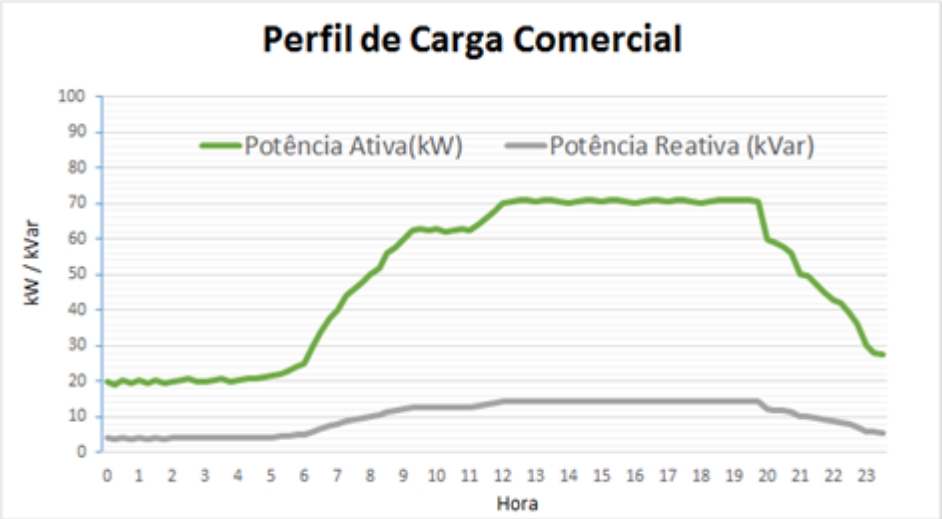


Figura 6-9: Perfil de carga comercial

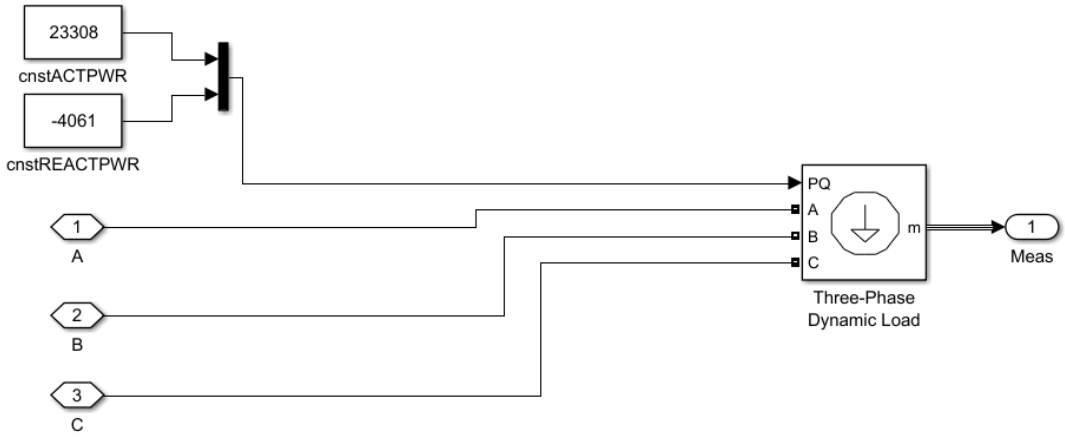


Figura 6-10: Diagrama de blocos do grupo de SGEs

A alteração dos valores de carga pode simular uma mudança de comportamento de consumo do cliente, assim como o aumento de consumo de potência reativa e consequente diminuição de fator de potência. O elemento de carga e seu respectivo diagrama de blocos internos estão representados na Figura 6-10, onde os elementos “cnstACTPWR” e “cnstREACTPWR” são os respectivos valores de usuário para a Potência Ativa e Reativa.

d) Objetos de Medição

Os elementos de medidor de tensão (Figura 6-11) e de corrente (Figura 6-12) além de sua função de medição possuem também a funcionalidade de simulação de erros de medição. Os seguintes erros podem ser simulados: discrepância de valores de amplitude entre fases em qualquer valor percentual desejado; valores nulos para grandezas elétricas de qualquer fase; valores que não se alteram (conhecidos como “valores congelados”). Com isso, é possível simular uma série de situações frequentemente encontradas, tais como, erros de telemedição, e também testar funções especializadas, e.g. localização de faltas e estimação de estado.

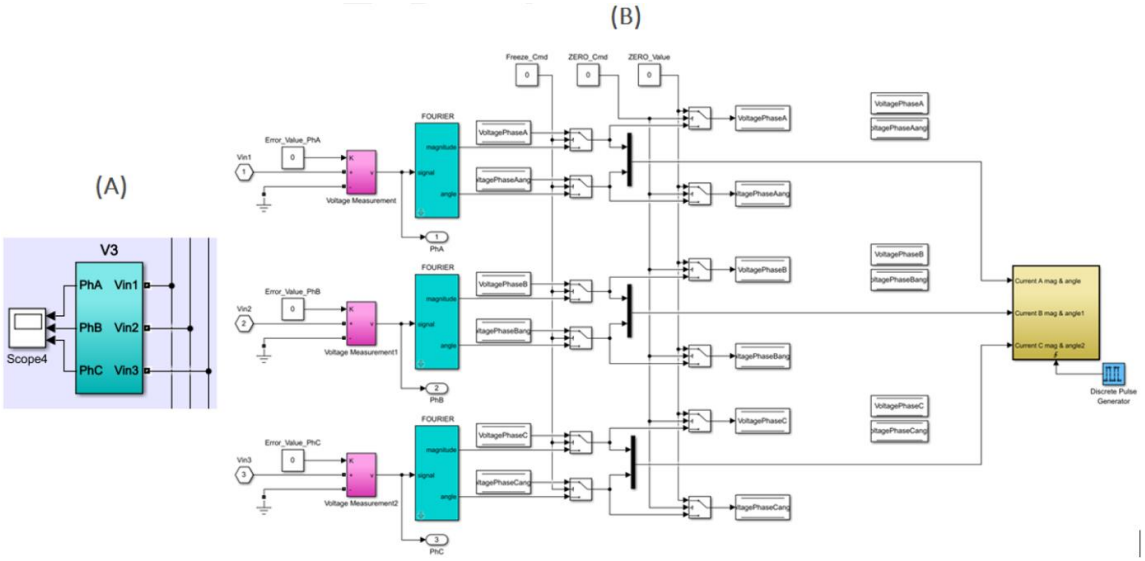


Figura 6-11: Medidor de tensão (A) e seu diagrama de blocos (B)

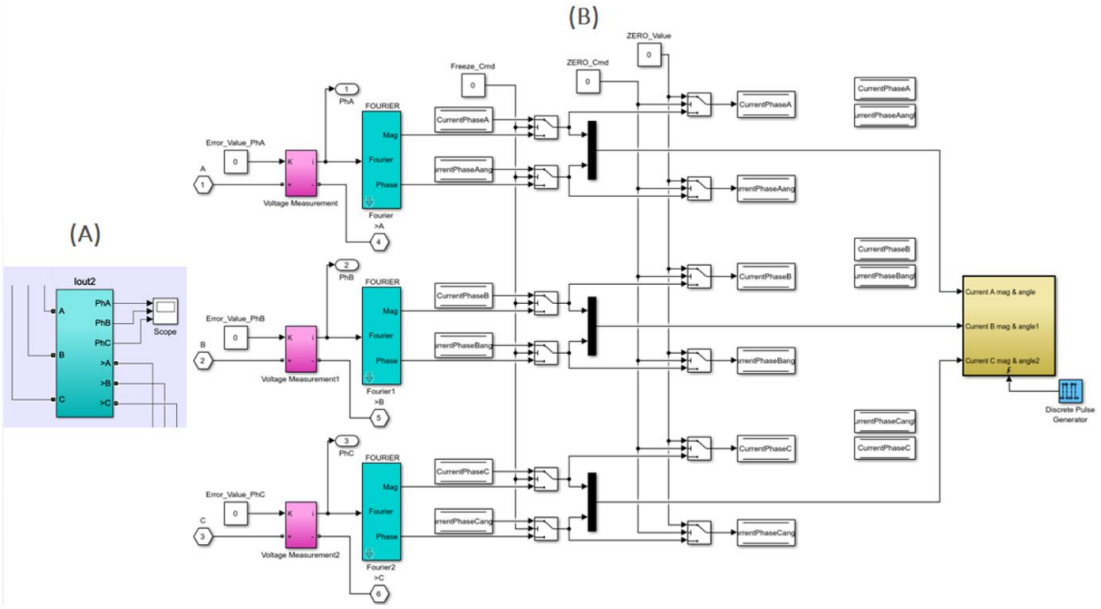


Figura 6-12: Medidor de Corrente (A) e seu diagrama de blocos (B)

e) Equipamentos de Manobra

A fim de caracterizar uma mudança topológica do sistema, foram criados os equipamentos de manobra (disjuntor) comandados pelo usuário graficamente. Conforme ilustrado na Figura 6-13, o comando é atribuído a cada fase, possibilitando a simulação de uma falha que seja a atuação discrepante entre fases.

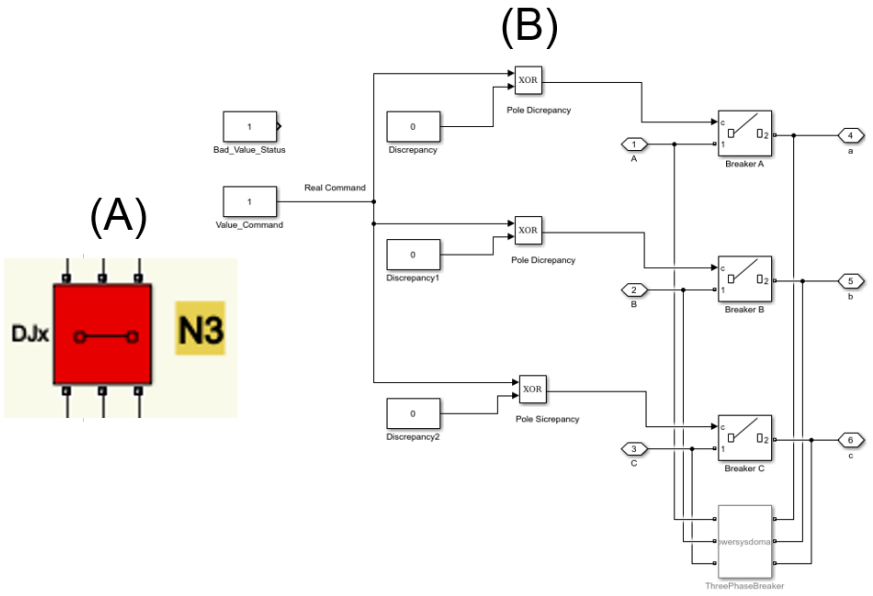


Figura 6-13: Disjuntor (parte A) e seu diagrama de blocos (parte B)

O objeto possibilita o modo "*Bad Data*" que significa forçar valores de estado não verdadeiros a fim de simular erros de telemedição e inconsistências topológicas. Esta função não é utilizada neste trabalho, mas pode ser configurada para aplicações futuras.

f) Telas de Controle

O simulador é composto de três telas de comando conforme ilustrado na Figura 6-14, sendo a tela "A" referente ao comando do disjuntor, a tela "B" referente à simulação de falhas no medidor de tensão e a tela "C", o mesmo para o medidor de corrente. Conforme ilustrado na Figura 6-14, os botões de simulação de erros de telemedição e as caixas de texto (e.g. "Error PhA (%)") para indicação de erros de medição estão disponíveis ao usuário a qualquer tempo durante a simulação.

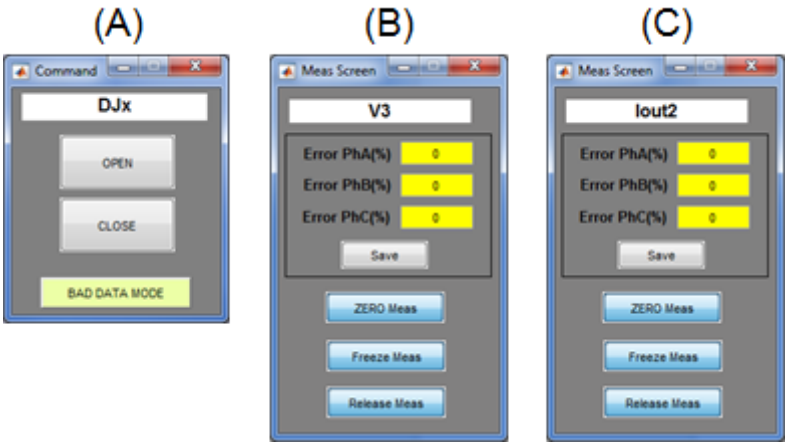


Figura 6-14: Telas de controle do disjuntor (A), medidor de tensão (B) e corrente (C)

Abaixo segue uma descrição detalhada do significado de cada botão nas telas de comando dos medidores:

- Botão "***SAVE***" – Todos os valores (negativos ou positivos) inseridos nas caixas de texto em amarelo são salvos como os valores de erro (percentual) introduzidos pelo usuário do simulador.
- Botão *"**ZERO** Meas*" – Este botão gera valores iguais a ZERO para todas as fases (tensão ou corrente) simulando falha de aquisição de dados.
- Botão *"**Freeze Meas***" – Este botão congela as medições a partir do último valor gerado pelo simulador. Com isso, perdas de comunicação com medidores ou falhas do sistema digital podem ser simuladas.
- Botão "***Release Meas***" – Retira o medidor da situação de falha, exceto quando ainda há valores diferentes de ZERO nas caixas de texto amarelas.

Os valores de corrente e tensão levam em consideração os resultados do cálculo do fluxo de potência e os valores de erros introduzidos pelo usuário. Para uma simulação de telemedição de corrente menor do que a que realmente circulou na rede, o usuário deverá inserir um valor negativo percentual (e.g. -10%). Com isso, o novo valor simulado será apresentado como resultado do medidor de corrente, e será propagado no bloco de medição que por sua vez será transportado no sistema Blockchain. As equações 6.3 e 6.4 abaixo apresentam como são calculados os valores de corrente e tensão com erros simulados.

$$I_{medido} = I_{pf} \times (1 + \ Error\ Ph_n) \tag{6.3}$$

$$V_{medido} = V_{pf} \times (1 + \ Error\ Ph_n) \tag{6.4}$$

Sendo:

"V_{medido}" o valor de tensão fornecida pelo medidor;

"I_{medido}" o valor de corrente fornecida pelo medidor;

"V_{pf}" o valor de tensão calculado no fluxo de potência do Simulink;

"I_{pf}" o valor de corrente calculado no fluxo de potência do Simulink;

"$Error\ Ph_n$" é o erro criado pelo usuário.

6.2.2 Módulo de Criação de Blocos de Dados

Este módulo de simulação age como um Agente ou SGE e é responsável pela organização e empacotamento dos dados de medição, informações de localização, estampa de tempo da origem da medição e identificação dos medidores, agentes e concessionária provenientes do módulo de simulação de rede (Seção 6.2.1). Estes dados são inseridos na estrutura do bloco (Seção 5.3.2) que será enviado para o processo de mineração que será detalhado na Seção a seguir.

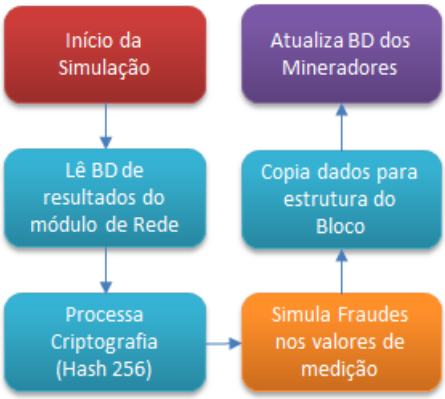


Figura 6-15: Fluxograma do módulo de criação dos blocos

O fluxograma simplificado apresentado na Figura 6-15 abaixo, ilustra como são encadeadas as funções internas do módulo. Os valores lidos do banco de dados atualizado pelo módulo de rede de baixa tensão (Seção 6.2.1) são utilizados para a criação da chave de segurança com a função hash criptografada ("sha256"). Após a esta etapa, o bloco é criado a partir da estrutura padrão, utilizando-se dos dados coletados do banco de dados mais a chave de segurança.

Este módulo permite que alterações de valores das medições sejam criadas a fim de simular fraudes inseridas no próprio software utilizado pelo Agente de medição ou nos pacotes de dados enviados pelo Agente para os mineradores. Os valores podem ser alterados antes da criação do bloco, mas depois da criação do código hash

criptografado. Com isso, haverá a possibilidade de comparação posterior, no processo de mineração, dos valores de medição enviados com o respectivo hash criado, apontando eventuais discordâncias entre os valores.

A estrutura de pastas e arquivos utilizadas neste módulo se encontra descrita no Apêndice B na Tabela B.1.

6.2.3 Módulo de Mineração

O módulo de simulação do processo de mineração é o cerne de todo o simulador e onde se encontra a maior complexidade computacional. Foram criados códigos em Matlab™ para modelar o processo de mineração desde a recepção de novos blocos no banco de dados até a criação dos encadeamentos de blocos com destino aos clientes finais do processo (módulo de relatórios).

Conforme descrito na Seção 5.3.3, o processo de mineração é composto de funções de verificação cruzada entre os mineradores pertencentes ao sistema. Cada bloco de entrada é testado quanto ao seu valor de hash de origem (análise de segurança), sua consistência no conteúdo dos dados (análise semântica) e sua aderência às regras contratuais do comercializador de energia (análise contratual). Todo este processo tem como objetivo a conquista do nível de consenso desejado (totalidade ou maioria).

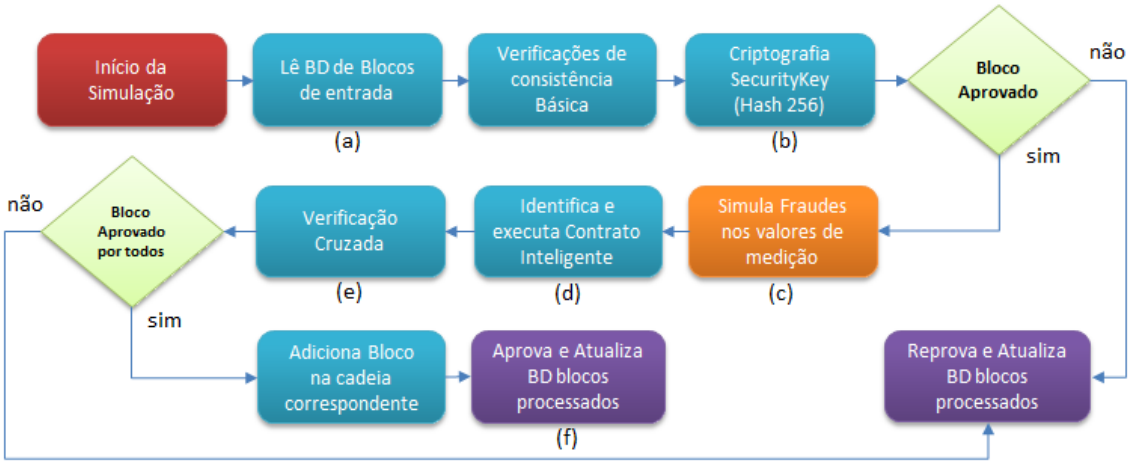


Figura 6-16: Fluxograma do módulo de mineração.

Todos os blocos que forem processados pela primeira vez, são recebidos diretamente de Agentes ou dos SGEs. Blocos que não se encontram no banco de dados de blocos pendentes e que sejam originários de outros mineradores serão rejeitados. Este procedimento garante maior robustez ao processo, uma vez que

blocos passíveis de fraude provenientes de um ou mais mineradores não serão processados pelo demais mineradores do sistema.

Este módulo, se divide em três partes complementares conforme ilustrado na Figura 6-16. O fluxograma simplificado do módulo minerador implementado, contempla etapas cujos fluxogramas correspondentes foram detalhados na Seção 5.3.

A seguir são detalhados alguns pontos importantes do fluxograma utilizado:

a) O Banco de Dados de entrada armazena os blocos de dados criados no módulo de simulação anterior. São armazenados blocos novos e blocos provenientes dos demais mineradores. Cada bloco possui um campo interno indicador de aprovação do bloco, onde estão armazenadas as informações do ID do minerador e a estampa de tempo do momento de finalização da validação. A não existência de registros de aprovação ou reprovação denota que o bloco é novo e veio da origem;

b) Após o bloco ter passado pela fase de verificações básicas já detalhadas no fluxograma de mineração na Seção 5.3, o *SecurityKey* é calculado conforme a função descrita na equação (5.1). O anagrama gerado é comparado com a chave de segurança de origem do bloco. Caso os valores sejam exatamente iguais, quer dizer que os valores usados como base para a geração do hash criptografado são os mesmos;

c) Nesta etapa, fraudes podem ser simuladas, alterando o valor de medições originais do bloco. Nos casos de teste de cenários de fraudes, os quais serão apresentados no próximo capítulo, valores menores de contagem de Energia Ativa são registrados no bloco de origem. O minerador fraudado, cria uma nova chave de segurança de origem para tentar manter a consistência dos dados com o valor do hash criptografado;

d) É acionado o contrato inteligente respectivo à concessionária de destino do bloco. Todas as verificações contratuais e semânticas são realizadas. O bloco não pode mais ser reprovado nesta fase, mas pode receber indicadores de que todas as verificações tiveram sucesso, ou que há restrições que precisam ser avaliadas pela concessionária. Para isso, este módulo de simulação se utiliza de um campo interno denominado “SC_Flag”, que se trata de um indicador

hexadecimal com 4 caracteres contendo no total 2 bytes (16 bits) de dados, sendo: SC_Flag = XXYY, onde os valores possíveis transitam entre 00 e FF. Os valores de “XX” podem ser iguais à: Hexadecimal “01” e Binário “00000001” (que indica um bloco de medidas) e Hexadecimal “11” e Binário “00010001” (que indica um bloco de medidas e alarmes). Para os dois caracteres “YY” a Tabela 6-1 detalha cada valor correspondente ao resultado da verificação semântica e contratual:

Tabela 6-1: Lista de indicadores da análise

Valor Hexa	Valor Binário	Descrição
00	00000000	Não verificado
01	00000001	Aprovado SEM restrições
02	00000010	Discrepância entre fases
03	00000011	Detecção do valor de tensão zero
04	00000100	Detecção do valor de corrente zero
05	00000101	Discrepância de potência medida
06	00000110	Energia acima do perfil sazonal
07	00000111	Potência excedente à contratada
08	00001000	Interrupção do suprimento de energia

O bloco é retornado para o processo já com o indicador de resultados do contrato inteligente, partindo assim para a próxima etapa.

e) Após ter sido avaliado pelo minerador, o bloco é enviado aos demais mineradores do sistema a fim de se realizar a verificação cruzada. O bloco é marcado com o seu status de aprovação (aprovado ou reprovado) e o instante final da validação é registrado. Essas informações são enviadas dentro do bloco de dados até os demais mineradores. Ao receber o mesmo bloco de outros mineradores, é verificado o status de aprovação de cada um dos mineradores.

f) Caso todos tenham aprovado o bloco, ou seja, o consenso tenha sido alcançado, o mesmo é marcado como aprovado, caso contrário, o bloco é reprovado e guardado no banco de dados de blocos processados.

O módulo de mineração registra todas as fases do processo e cada bloco possui as estampas de tempo dos momentos de recepção do bloco e o momento da aprovação ou reprovação do mesmo. O registro de cada etapa do processo propiciou ilustrar os exemplos de casos estudados, auxiliando nas provas de conceito do processo de mineração. A estrutura de pastas e arquivos utilizadas neste módulo se encontra descrita no Apêndice B na Tabela B.1.

6.2.4 Módulo de Relatórios

Este módulo, codificado no Matlab™, apenas coleta os dados da Base de Dados de blocos processados e cria arquivos de relatórios para registro de resultados das simulações. Todos os dados simulados e calculados nos módulos do simulador são gravados em arquivos texto com divisão de colunas por vírgula tipo ".csv", propiciando uma grande facilidade de manipulação conforme indica a Tabela C-1 apresentada no Apêndice C.

6.3 RESULTADOS OBTIDOS

Durante o processo de simulação, todas as etapas fundamentais do SCMI, com a utilização da tecnologia Blockchain, foram testadas conforme descrito a seguir.

Conforme descrito na Seção 6.2, as medições elétricas foram geradas tendo como base uma rede de baixa tensão. Os valores gerados foram utilizados na criação dos blocos de dados, processados pelo módulo de mineração. Todo este ciclo de processamento produziu uma massa de dados que foi utilizada para os relatórios finais de análise de resultados.

O simulador produziu basicamente dois grupos de resultados. O primeiro grupo de resultados é referente a uma sequência de acontecimentos. Todos os passos foram registrados a fim de se acompanhar a resposta do sistema para as situações simuladas.

Estas simulações tiveram como objetivo, a validação dos algoritmos utilizados quanto à acuracidade e resiliência dos algoritmos propostos. A sequência lógica prevista foi comprovada nos testes e serviu de subsídio para a produção dos resultados ilustrativos, nomeadamente referente à:

- Processamento normal dos blocos;

- Atraso de blocos;
- Corrupção de blocos, de mineradores e de medidores inteligentes;
- Perda de blocos de dados.

O segundo grupo de resultados é numérico e foi obtido tomando como base os registros de estampa de tempo de cada parte do processo de simulação. Desde a criação dos blocos de dados até a formação da cadeia de dados final, todos os tempos dispendidos foram aferidos com precisão de milissegundos.

O objetivo destas simulações foi validar os algoritmos utilizados quanto à performance de processamento dos algoritmos testados e a capacidade de processamento de blocos. Os resultados numéricos encontrados foram preliminares e visaram aferir a ordem de grandeza dos tempos de processamento totais dos blocos, em um ambiente de simulação laboratorial. Os testes realizados neste grupo aferiram os seguintes itens:

- Desempenho dos Mineradores - blocos de medição e comando;
- Cenários de avalanche de blocos de medição - tempo e capacidade de processamento de blocos e capacidade de clusters.

6.3.1 Plataforma de testes

Os testes aqui registrados foram realizados em uma estação de trabalho Windows de performance regular, cujos dados técnicos de hardware e software constam da Tabela 6-2.

Tabela 6-2: Plataforma de testes

Hardware	**Descrição**
CPU	Intel® Core™ i7-2600 CPU 3.4GHz
Memória RAM	32 GB
Hard Drive	1 TB
Performance	Windows Experience Index 5,4
Software	**Descrição**
Sistema Operacional	Windows 7 Professional SP1 de 64 bits
IDE para os códigos e para as GUIs	Matlab 2016a c/ Simulink

6.3.2 Resultados Ilustrativos (Blockchain)

O SCMI proposto foi projetado para ser seguro (evitando a propagação de fraudes) e resiliente a problemas de comunicação ou invasões cibernéticas pontuais.

Diversos cenários foram criados simulando a ocorrência de fraudes e problemas sistêmicos nos pontos críticos do processo de telemedição. O sistema foi composto por três mineradores (“A”, “B” e “C”) e um bloco sendo simulado por vez, visto que o foco do teste era validar o sequenciamento lógico do algoritmo implementado e analisar seus resultados.

Processamento Normal do Bloco

O primeiro cenário simulado trata de um fluxo de trabalho normal, em que um bloco é gerado, proveniente de um medidor de energia, e é gravado no banco de dados de entrada (“Tempo 0”) conforme ilustrado na Figura 6-17. Este bloco, que pode ser de medição ou de comando, se apresenta como um bloco íntegro e de origem comprovada. Por ser um bloco que provém diretamente de sua fonte de medição, de um Agente ou um bloco de comando enviado pela concessionária, em todas as hipóteses tal bloco se torna pendente em cada um dos mineradores, onde a chave de segurança é verificada.

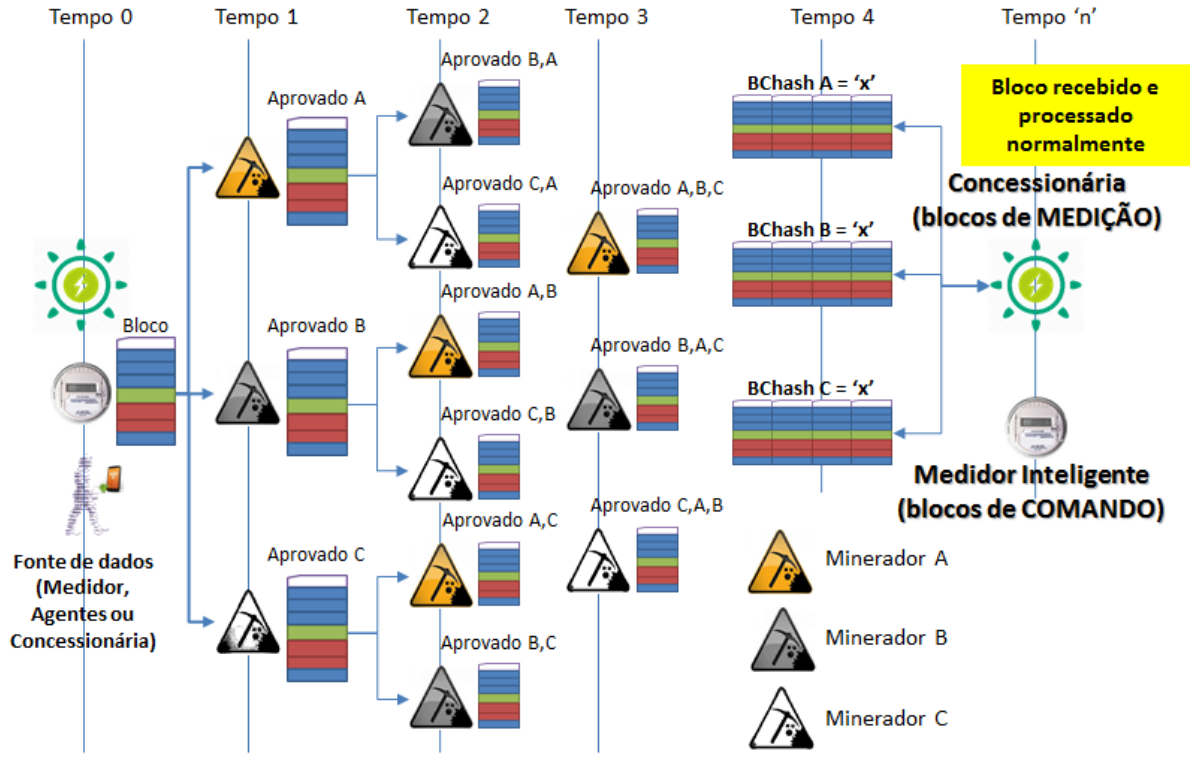


Figura 6-17: Tráfego normal de um bloco.

Cada minerador verifica e valida o bloco (“Tempo 1”), enviando-o para os demais mineradores no processo de verificação cruzada. Os mineradores recebem o bloco já com o status de aprovação atualizado (“Tempo 2”) e concluem a verificação

cruzada completando a validação por todos os mineradores (“Tempo 3”). A cadeia de blocos é testada em cada um dos mineradores, onde o BChash é gerado e comparado com os demais mineradores (“Tempo 4”). Após validado o BChash, o bloco é então inserido na cadeia de blocos e disponibilizado no banco de dados de blocos processados.

Bloco com atraso

O segundo cenário simulado e ilustrado na Figura 6-18 está relacionado à ocorrência de um atraso de comunicação entre a fonte de criação do bloco (medição ou comando) e o minerador “C”. Devido ao atraso gerado, o bloco é entregue ao minerador “C” somente após ser processado pelos mineradores “A” e “B”. Como o bloco já foi validado pelos mineradores “A” e “B”, os mesmos realizam sua fase de verificação cruzada, enviando o bloco aos demais. O minerador “C” recebe o bloco enviado pelos mineradores “A” e “B”. Nesse caso, “C” identifica o bloco como um bloco que não é de origem, ou seja, não foi enviado por um SGE ou um Agente. O bloco é então ignorado pois ele não se encontra na sua BD de blocos de entrada e ainda não foi processado por “C”, ou seja, não aparece na BD de blocos pendentes.

Finalmente o bloco é enviado pela fonte ao minerador “C” que o identifica como bloco válido, o aprova e o envia para “A” e “B”, os quais já aprovaram o bloco. O processo termina com sucesso, mas com um tempo total maior de conclusão, devido ao atraso ocorrido no recebimento do bloco pelo minerador “C”. As três cadeias de blocos foram atualizadas com o mesmo BChash e estão prontos para serem coletados pela concessionária. A simulação foi repetida com um atraso maior, e o resultado foi o mesmo, alterando somente o tempo total de conclusão do processo, que por consequência, foi maior. Este teste mostra a resiliência do sistema quanto a falhas de comunicação de dados entre qualquer fonte de dados (SGE, Agentes ou concessionária) e a nuvem de serviços Blockchain. Caso o Minerador “C” não recebesse o bloco, o mesmo não seria aprovado e não ficaria disponível à concessionária. Dispositivos de verificação de erros de comunicação podem ser desenvolvidos nos mineradores para que casos repetitivos possam ser identificados e corrigidos.

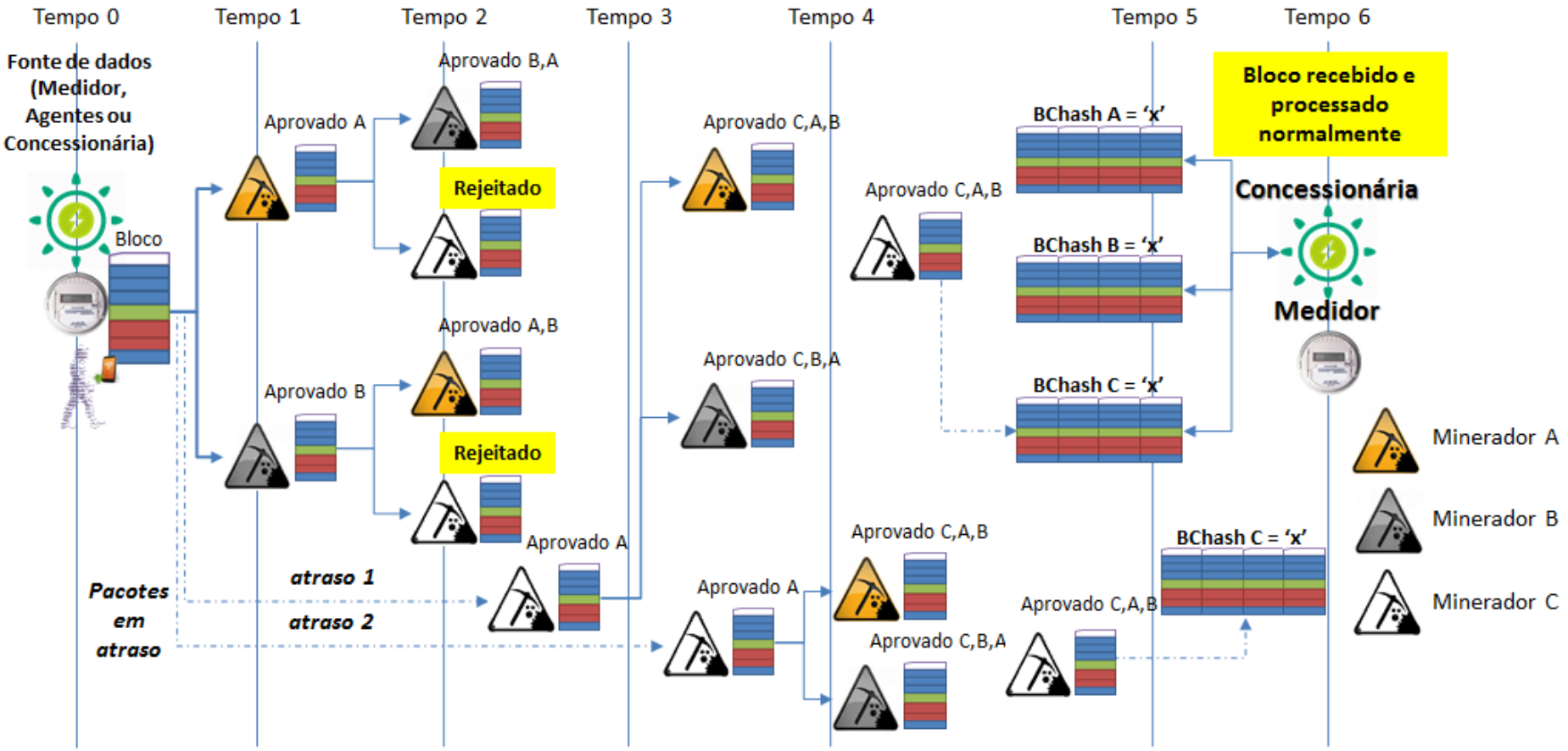


Figura 6-18: Cenário com atraso de envio do bloco.

Bloco corrompido

Neste cenário, o bloco se encontra corrompido, ou seja, entre o processo de envio do bloco de dados pelo Agente ou diretamente pelo próprio SGE (“Tempo 1”) até a chegada ao BD de blocos de entrada dos mineradores. Este caso simula uma invasão na rede de dados onde as informações de medições foram manipuladas no pacote de dados transmitidos, porém, o hash criptografado gerado pelo SGE (fonte dos dados) não foi alterado. Esta simulação é realizada alterando-se os valores de medição no módulo de criação de blocos da Seção 6.2.2.

Conforme ilustrado na Figura 6-19, na linha de “Tempo 2”, o bloco é verificado e logo na validação básica de segurança, é identificado que o *SecurityKey* gerado pelo “sha256” não é exatamente igual ao anagrama da chave de segurança de origem. Com isso, o bloco é descartado imediatamente e reprovado pelos mineradores. Como a reprovação foi concluída antes da verificação cruzada, o tempo de processamento do Blockchain é poupado.

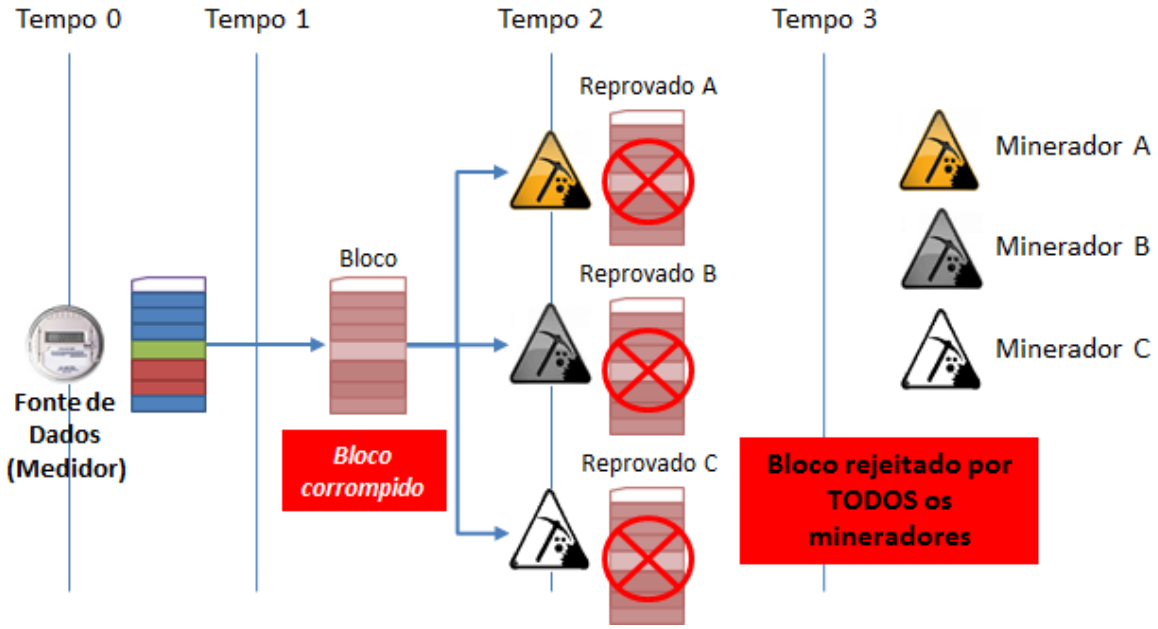


Figura 6-19: Cenário de Bloco corrompido.

Minerador corrompido

O quarto cenário, ilustrado na Figura 6-20, representa uma invasão cibernética no minerador “B” ou uma corrupção do código de mineração. É uma situação um tanto inusitada por ser bastante custosa do ponto de visto técnico, porém possível de

ocorrer. Nesta simulação foram manipulados valores de Energia Ativa e de Corrente nas fases presentes no campo de dados de medição.

No minerador “B” (“Tempo 1”), a chave de segurança é recalculada com os valores corrompidos, gerando um novo anagrama hash na chave de segurança, tentando compatibilizar o hash criptografado com os valores de medição alterados. O minerador corrompido tenta então disseminar o bloco fraudado entre os outros mineradores através do processo de verificação cruzada.

Ainda no “Tempo 1”, os mineradores “A” e “C”, recebem o bloco da origem e o validam normalmente. Eles por sua vez, enviam o bloco ao minerador “B” (“Tempo 2”) que “reconhece” a fraude, mas o valida mesmo assim.

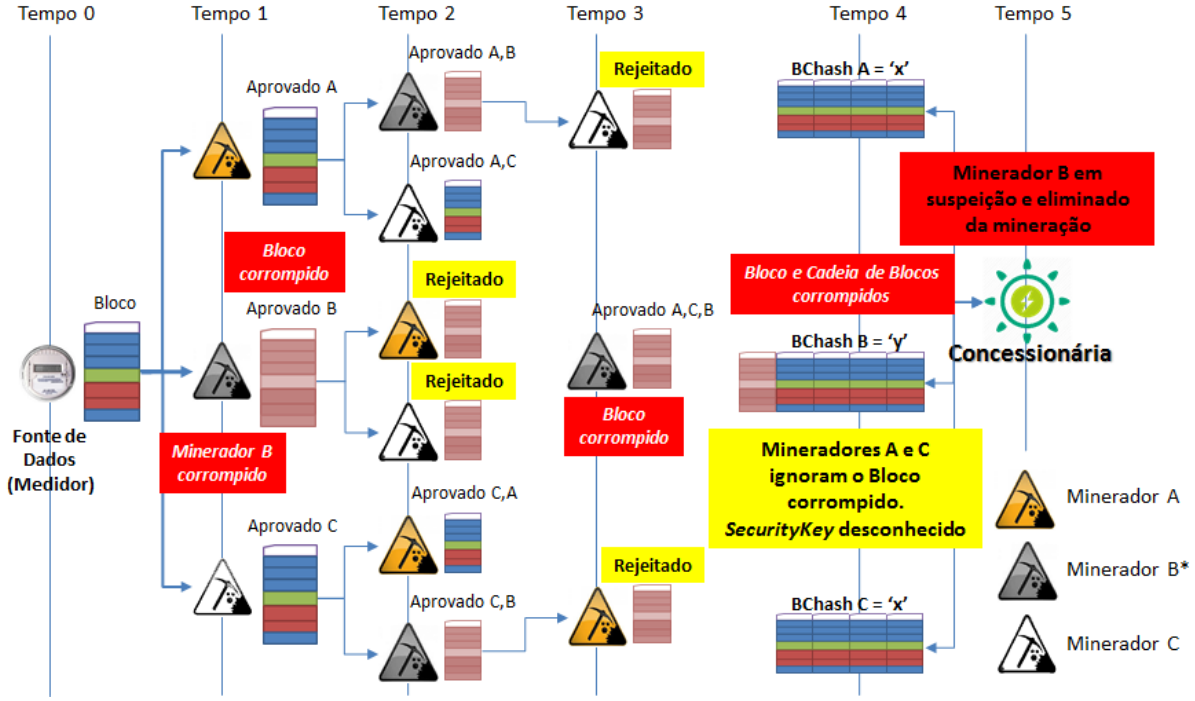


Figura 6-20: Cenário de Minerador corrompido (medição ou comando).

Quando “A” e “C” recebem o bloco corrompido de “B”, o bloco é rejeitado (“Tempo 2”). Isso ocorre devido a chave de segurança ser desconhecida dentre os blocos registrados no BD de entrada e no BD de blocos pendentes em “A” e “C”. Com isso, o bloco é interpretado em “A” e “C” como inválido e é reprovado sumariamente.

Devido às diferenças nas chaves de segurança dos blocos provenientes de “B” e da origem, o resultado desta simulação mostra que não houve consenso na aprovação do bloco e a fraude não foi propagada (“Tempo 3”).

O minerador corrompido “B” ignora a reprovação dos demais mineradores e insere o bloco na cadeia de blocos (“Tempo 4”), assumindo um BChash diferente dos

demais. Esta situação provoca um alarme de inconsistência perigosa, causando a eliminação deste minerador do processo de mineração. Este teste é válido tanto para blocos de comando quanto para blocos de medição, visto que as verificações de segurança atingem os dois tipos de bloco igualmente. A criptografia no caso dos blocos de comando, contempla o campo “Valor” ao invés do campo “Dados” dos blocos de medição.

Minerador e Bloco corrompidos

Neste quinto cenário, ilustrado na Figura 6-21, uma fraude é simulada no minerador “B” e no campo “Dados” referente aos dados de medição. O bloco é manipulado no módulo de criação do bloco (“Tempo 0”), ou seja, a simulação reproduz uma fraude realizada pelo Agente de medição.

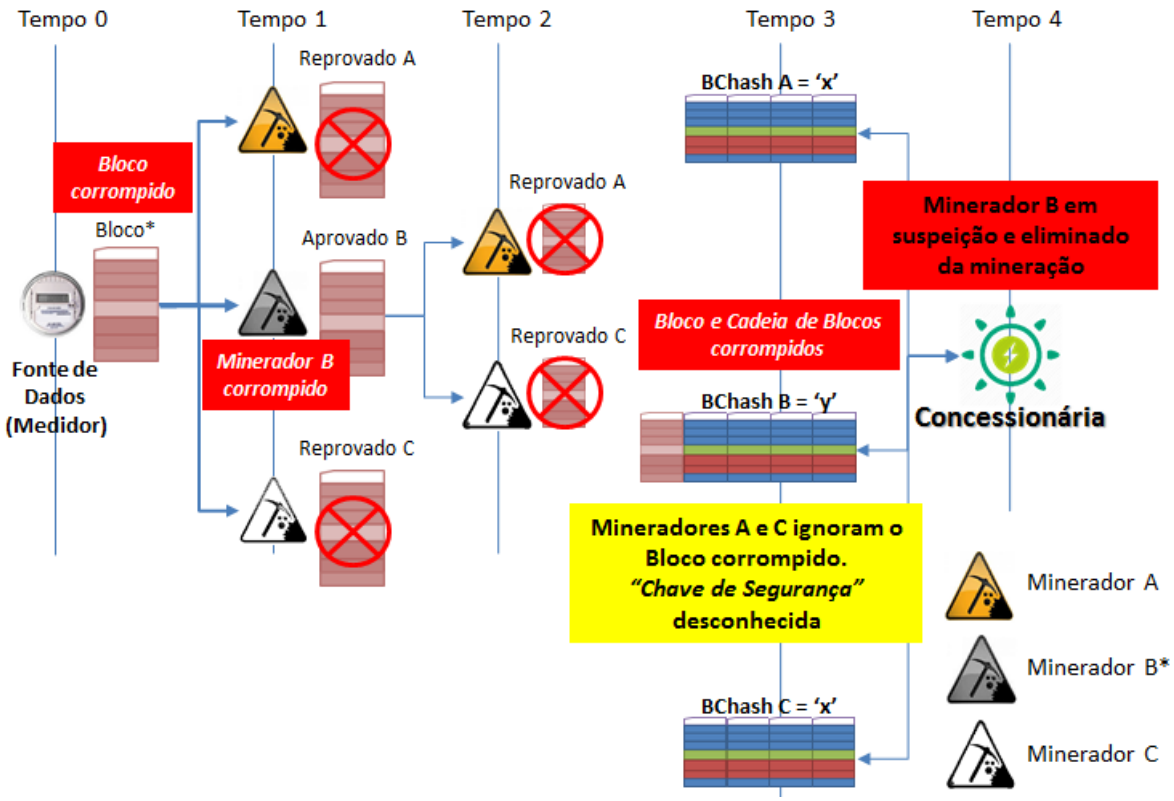


Figura 6-21: Cenário com Minerador e bloco corrompidos (medição ou comando).

Essa fraude altera os valores de medição do pacote de dados sem qualquer alteração na chave de segurança que foi gerada pelo próprio dispositivo de medição inteligente. Ao chegar no BD de entrada, lido pelos mineradores (“Tempo 1”), o bloco é processado e a verificação de sua chave de segurança é realizada. Os mineradores “A” e “C” rejeitam o bloco por este não passar no teste do hash criptografado (“Tempo

2”), visto que a função “sha256” aplicada aos valores de medição gera um anagrama diferente do anagrama da chave de segurança da origem.

O minerador “B” cria uma nova chave de segurança, gerando um anagrama compatível com as medições alteradas e tenta propagar o bloco para os demais mineradores através da verificação cruzada. Porém, os mineradores “A” e “C” rejeitam o bloco pelo fato da chave de segurança ser desconhecida. Em seguida, o bloco corrompido por “B” é descartado por “A” e “C” e não é propagado para a cadeia de blocos.

O minerador corrompido “B” ignora a reprovação dos demais mineradores e insere o bloco na cadeia de blocos (“Tempo 3”), assumindo um BChash diferente dos demais. Esta situação provoca um alarme de inconsistência perigosa causando a eliminação deste minerador do processo de mineração.

Este teste é válido tanto para blocos de comando quanto para blocos de medição, visto que as verificações de segurança atingem os dois tipos de bloco igualmente. A criptografia no caso dos blocos de comando, contempla o campo “Valor” ao invés do campo “Dados” dos blocos de medição.

Dispositivo de medição corrompido

O sexto caso de simulação produz uma fraude no próprio dispositivo de medição. A fraude no medidor significa que os valores de energia são adulterados direta ou indiretamente a fim de registrar valores menores do que os realmente consumidos pelo cliente final.

Há várias técnicas de fraude de medidores de energia na literatura e nos registros das concessionárias (DE FARIA, ONO FONSECA, *et al.*, 2014). Essas fraudes podem ser aplicadas em medidores eletrônicos ou eletromecânicos. No caso dos medidores inteligentes digitais, as fraudes são realizadas usualmente nos elementos de medição (transformadores de corrente e tensão) e nas invasões das redes de dados (BAIG, AL AMOUDY e SALAH, 2015) com a captura de pacotes e manipulação das informações de medição. A alteração do software do medidor se torna extremamente complicada, visto que o *firmware* do medidor, que é o software programado de fábrica, não pode ser acessado em seu código fonte.

Caso o medidor inteligente (SGE) possua capacidade de criptografar a chave de segurança, somente uma alteração no *firmware* do medidor poderia gerar uma fraude nos campos de dados tratados internamente nos módulos de conversão

analógico digitais ou no processamento digital de sinais (DSP). Este tipo de fraude seria mais complicada de se identificar, porém ela é pouco viável tecnicamente. Excetuando este caso de fraude descrito, a criptografia na origem da medição age nos demais casos, impossibilitando que dados manipulados sejam propagados no Blockchain, conforme visto nos exemplos anteriores desta seção.

Este caso de simulação (Figura 6-22) foi subdividido em dois casos que devem levar aos mesmos resultados. No primeiro caso simulado, o medidor inteligente foi totalmente corrompido e seu código fonte alterado a tal ponto que o campo de dados de medição na memória interna do medidor já não representa os valores reais lidos dos transformadores de corrente (TC) e de tensão (TP) dos medidores. Com isso, os valores calculados de potência e energia terão uma base de informação com correntes menores do que as verdadeiramente consumidas. O processo de criptografia usará os valores manipulados internamente gerando anagramas matematicamente coerentes. Conforme explicado anteriormente nesta seção, esta é uma situação de difícil viabilidade, mas que também pode ser tratada mesmo assim pelo sistema proposto.

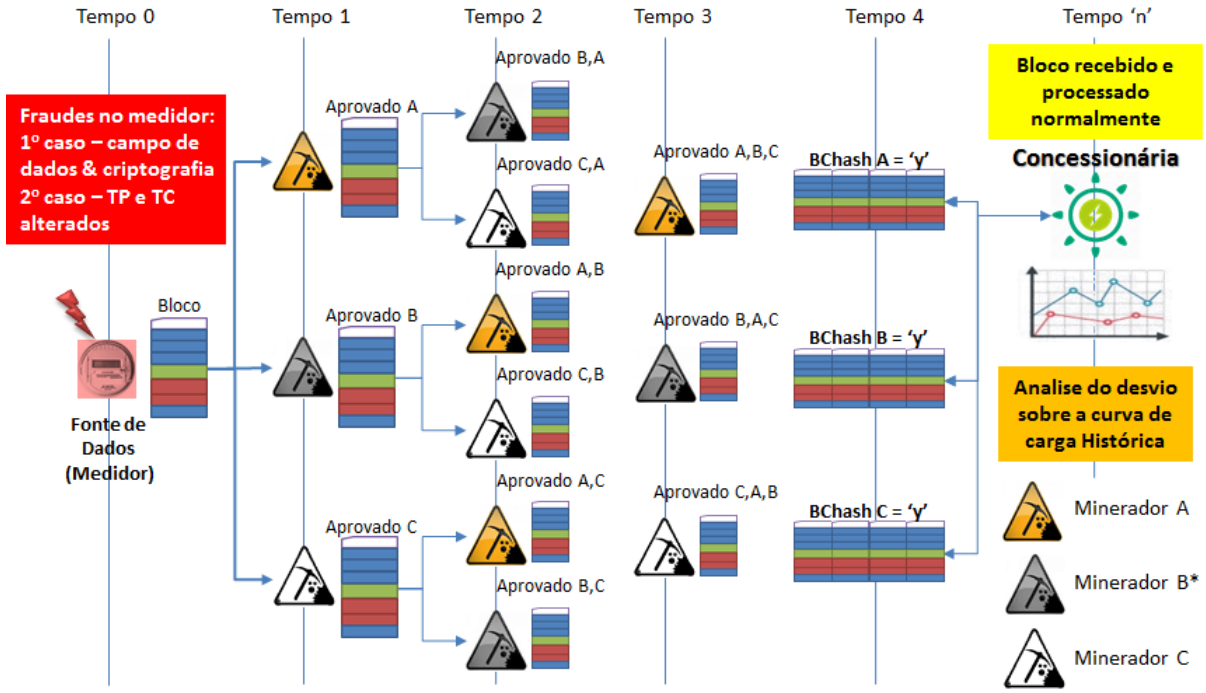


Figura 6-22: Cenário com medidor corrompido (blocos de medição).

O bloco com medidas alteradas passa pelo processo de verificação de segurança ("Tempo 1") como se fosse um bloco válido, já que o valor do anagrama

do hash criptografado calculado na mineração (*SecurityKey*) é exatamente igual à chave de segurança de origem.

Antes de se continuar a análise do andamento do processo de mineração nota-se que, no segundo caso, a alteração física nos sensores de corrente e/ou tensão, gera medidas com valor de correntes menores a fim de gerar um valor menor de energia consumida. Ao gerar o hash criptografado utilizando-se dos dados de medição lidos dos sensores (TP e TC), o medidor inteligente gera uma chave de segurança coerente com os valores fisicamente lidos. Por esta razão, o campo “Dados” do bloco possui exatamente os valores lidos dos sensores físicos adulterados.

Ainda no processo de mineração (“Tempo 2”), o contrato inteligente é acionado e as verificações semânticas e contratuais são realizadas. Neste ponto, o sistema de mineração Blockchain proposto atua mais uma vez no combate às fraudes, mesmo as mais difíceis. Isto ocorre na verificação semântica, pois nesta fase (Seção 5.2.2) é realizada a análise do valor da carga medida. A verificação é realizada utilizando como base a discrepância máxima permitida de medição de carga (*MALMdis*) explicitada na equação (5.6). Nesta verificação é utilizada uma base de dados histórica de demanda típica do cliente naquela mesma janela de tempo, ou na falta de dados históricos, o valor típico de carga de um cliente da mesma categoria, e.g. residencial tipo “A”, tipo “C”, ou qualquer classificação específica da concessionária.

Caso o valor de *MALMdis* seja excedido, o minerador irá gerar o alarme e anexar esta informação no campo “*Data*” de medidas e alarmes. Conforme listado na Tabela 6-1 o alarme será de “Carga abaixo do perfil sazonal”. Como a medição de demanda manipulada tende a ser menor do que o valor esperado, o contrato inteligente indicará uma não conformidade em todos os blocos do medidor, gerando uma situação de suspeição técnica do medidor ou de fraude do cliente. A concessionária receberá a mensagem de não conformidade para todos os blocos do medidor, alertando a manutenção e gerando uma verificação *in loco* até a troca do medidor para nova avaliação.

Este processamento distribuído de verificações de consistências, retira do SCADA da concessionária uma carga de processamento consideravelmente grande, visto que o DMS/ADMS observa um sistema muitas vezes maior do que o *cluster* o qual o minerador está responsável.

Finalizando o processo de mineração, ainda na Figura 6-22, a verificação cruzada é realizada com sucesso (“Tempo 2”) e finalmente o bloco é aprovado com

restrições por todos (“Tempo 3”). A cadeia de blocos é atualizada com os valores de BChash exatamente iguais.

A Figura 6-23 ilustra um exemplo de perfil de carga esperada (em P.U.) comparada com a carga medida, considerado como “real” (em P.U.). A carga “real” se apresenta abaixo do esperado e sua diferença percentual pode variar no tempo de acordo com o valor da demanda.

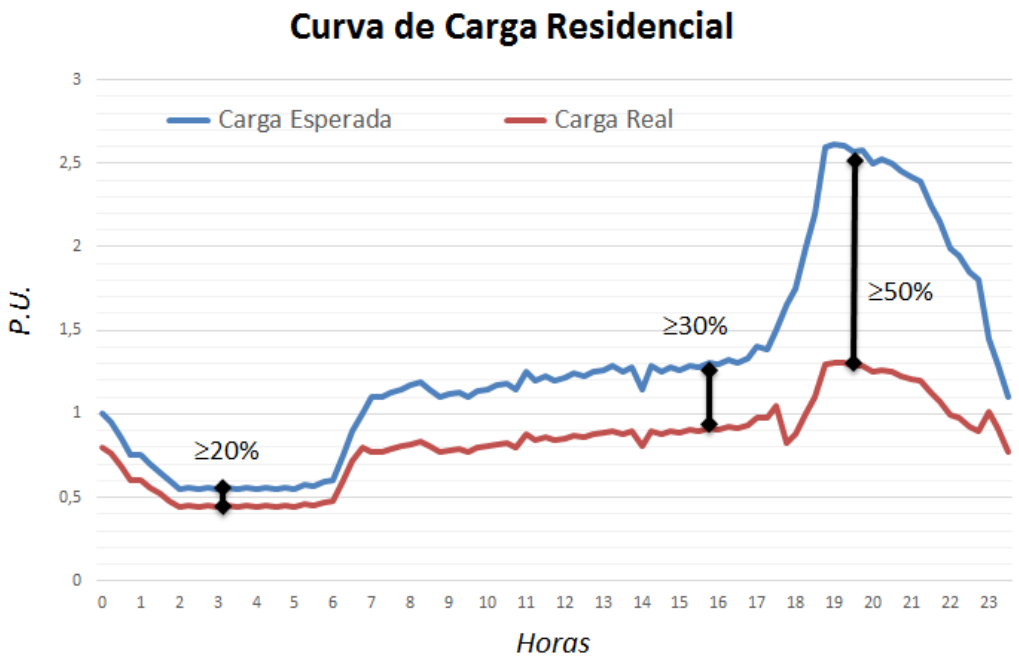


Figura 6-23: Comparação com valores medidos e esperados.

Perda de Blocos de dados

Neste caso será avaliada a resiliência do sistema proposto a condições de perda de bloco de dados. Na primeira tentativa de envio, um dos mineradores não recebe um novo bloco de dados (de medição ou comando) que, em um cenário real, poderia ocorrer hipoteticamente devido a falhas na comunicação de dados entre a fonte e este minerador.

Conforme ilustrado na Figura 6-24, o bloco é encaminhado normalmente para os mineradores “A” e “B”, mas não vai para o minerador “C”. O bloco é processado por “A” e “B”, que executam a mineração normalmente no “Tempo 1” e efetuam as verificações cruzadas no “Tempo 2’”. Os dois mineradores aprovam o bloco, mas não recebem a aprovação do minerador “C”. Este rejeita o bloco, uma vez que o mesmo não se encontra no seu banco de dados de entrada nem no de blocos pendentes de

aprovação. Sendo assim, o minerador “C” descarta o bloco, enquanto os mineradores “A” e “B” o armazenam como bloco pendente de aprovações.

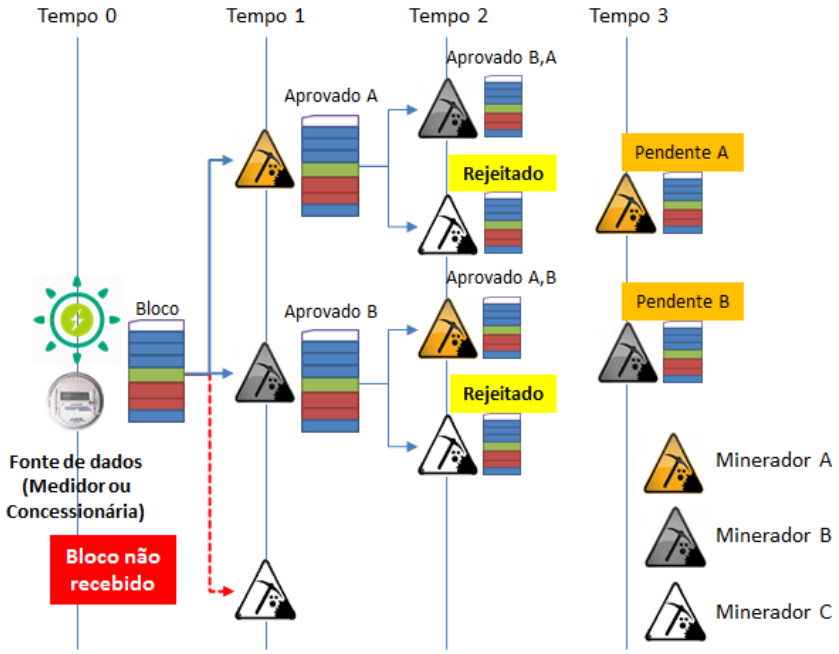


Figura 6-24: 1ª tentativa de entrega do bloco ao minerador “C” (medição ou comando)

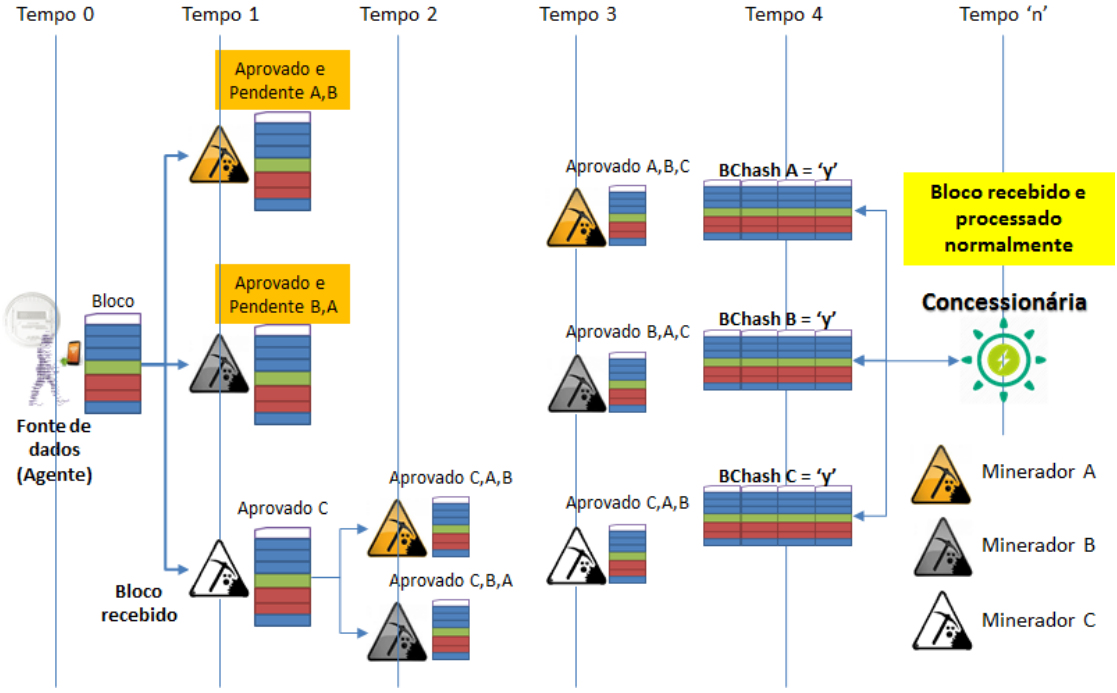


Figura 6-25: 2ª tentativa de entrega do bloco ao minerador “C” (medição)

Conforme ilustrado na Figura 6-25, uma segunda tentativa é realizada no caso de blocos de medição. Neste caso, um Agente colaborativo de medição envia o bloco de medição do mesmo medidor com o mesmo conteúdo, consequentemente, com a

mesma chave segurança. Isso é possível se os dados coletados do medidor foram efetuados antes de uma nova atualização de medição, que pode ocorrer em minutos ou segundos, dependendo da tecnologia do medidor inteligente.

O bloco é então recebido por todos os 3 mineradores que o processam normalmente. Os mineradores “A” e “B” já processaram um bloco com a mesma chave de segurança. Este bloco se encontra na base de dados de blocos pendentes de cada um deles. O minerador “C” processa o bloco pela primeira vez e o envia aos demais mineradores para a verificação cruzada (“Tempo 2”). Os mineradores “A” e “B” não precisam minerar novamente o bloco mas, identificam que a aprovação de “C” ainda está pendente. Por isso, enviam novamente o bloco para “C”, que por sua vez, também envia o bloco para os mineradores “A” e “B”. O bloco é recebido em “C” já marcado com todas as respectivas aprovações. Com isso, em “Tempo 3” o bloco já está completamente aprovado e segue para a sua cadeia de blocos respectiva para ser coletado pela concessionária.

Este teste ilustra como a redundância na coleta de dados dos medidores pode ajudar substancialmente na disponibilidade do sistema, fazendo com que medidas não se percam no curto prazo ou, pelo menos, tenham estatisticamente menos chance de serem perdidas.

No caso de blocos de comando, a segunda tentativa não conta com Agentes colaborativos, mas sim com novas tentativas da própria concessionária.

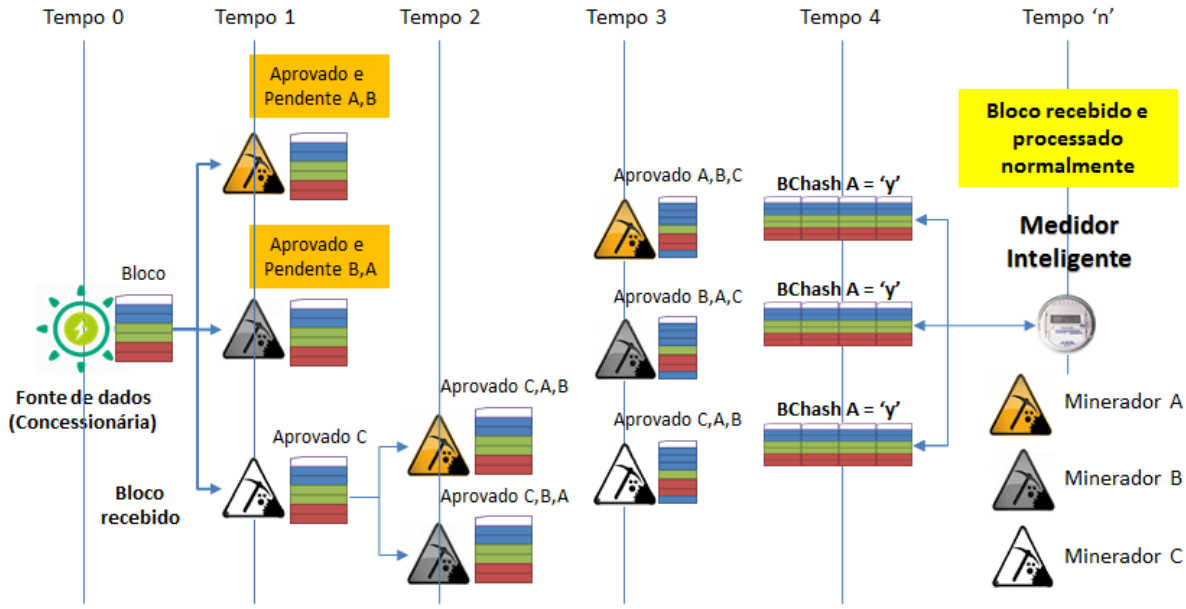


Figura 6-26: 2ª tentativa de entrega do bloco ao minerador “C” (comando)

Conforme ilustrado na Figura 6-26, o bloco segue o mesmo processo bem-sucedido do bloco de medição ilustrado na Figura 6-25, caso sua validade não tenha sido expirada. Lembrando que, para todo bloco de comando, há um campo chamado “Validade” contendo uma estampa de tempo referente à validade de emissão do comando. A análise semântica deste tipo de bloco verifica se validade da emissão do comando está ou não expirada baseado na estampa de tempo do momento atual.

Na Figura 6-27, o teste foi realizado com a validade de comando expirada. Com isso, o bloco, que já havia sido aprovado pelos mineradores “A” e “B” na primeira tentativa, agora será reprovado pelo minerador “C”, pois este efetuará o processo de verificação semântica e reprovará o bloco. Esta reprovação será propagada para os demais mineradores (“Tempo 2”) que atualizarão seus respectivos bancos de dados, reprovando também o bloco pela falta de consenso de aprovação. Assim, finalmente o processa termina no “Tempo 3” com a reprovação do bloco por todos os mineradores.

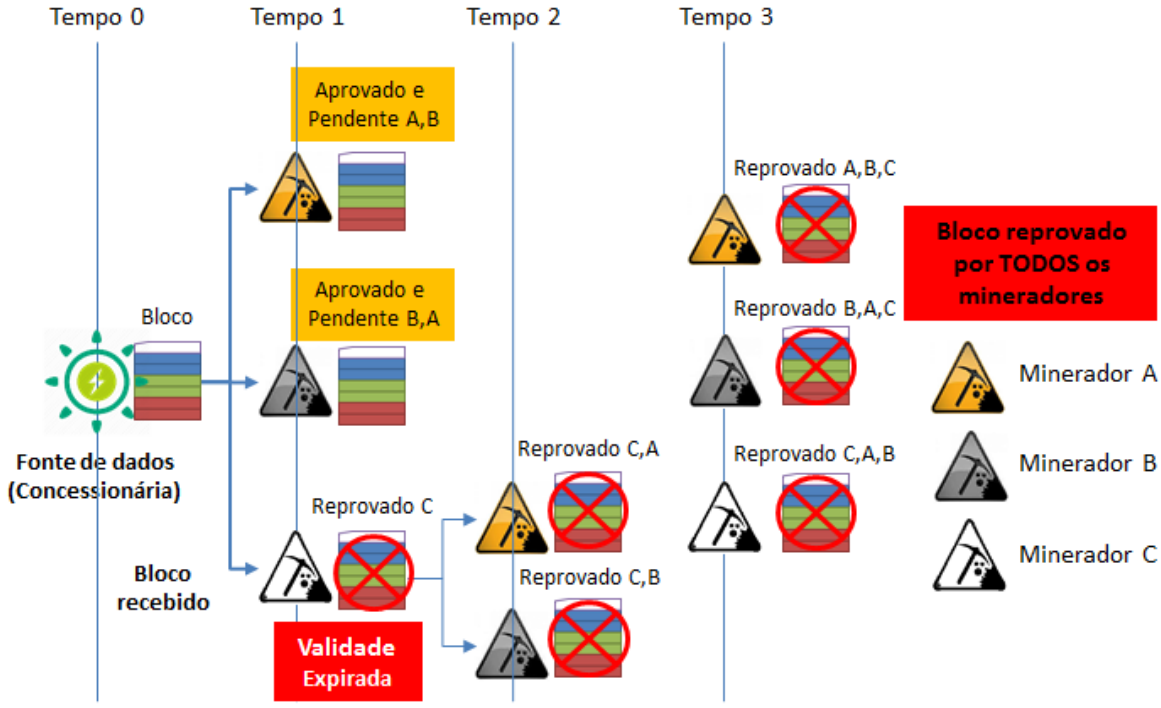


Figura 6-27: 2ª tentativa de entrega do bloco ao minerador “C” (comando expirado)

Simulação de Perda Não-Técnica

O simulador da rede de baixa tensão foi utilizado para promover uma validação do contrato inteligente dos blocos de medição referente especificamente à verificação semântica utilizando uma situação real de perda não técnica. Inspirado nas propostas

de trabalhos futuros exemplificados no Capítulo 7, o teste consistiu na criação de uma carga desconhecida e ilegal na rede de BT a fim de se identificar a capacidade do SCMI de tratar esta anomalia localmente e de forma célere.

A simulação de cargas desconhecidas pode ser realizada com o acréscimo de cargas no simulador de rede de BT sem que seja declarado no arquivo de configuração. Esse procedimento provoca a geração de valores maiores de demanda no alimentador, pois haverá mais uma carga na rede. Não há medição associada a esta carga desconhecida, pois não há um SGE associado na configuração. Com isso, o SCMI não coleta esta medição e consequentemente, não há bloco para ser enviado ao Blockchain relativo à estas medidas.

Na Figura 6-28 (A) são ilustrados os objetos das cargas conhecidas (“CARGA EQUIV 01”) e desconhecidas (“CARGA DESCONHECIDA 01”) e o diagrama de blocos do objeto da carga desconhecida (Figura 6-28 (B)) que propicia uma mudança dinâmica de carga no tempo.

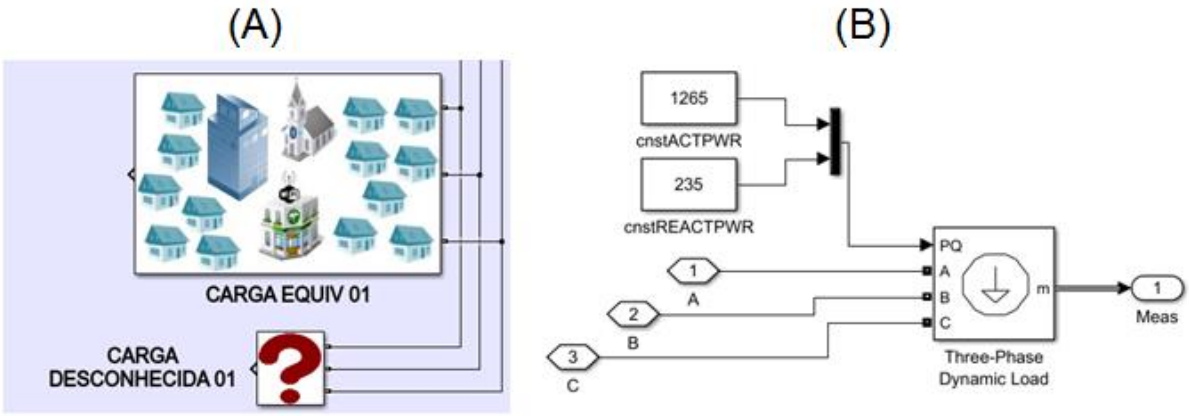


Figura 6-28: Cargas (A) e seu diagrama de blocos (B).

As medições que não estão sendo consideradas apontam para duas curvas de carga distintas coletadas do cluster segundo informações do simulador do SCMI. A primeira corresponde ao somatório de todas as curvas de carga medidas dos clientes (SGEs) e a segunda foi medida diretamente da UTR da subestação secundária.

Conforme ilustrado na Figura 6-29, embora as duas curvas de carga sejam bem próximas, elas apresentam diferenças devidas à potência ativa não contabilizada (equação (6.1)), que pode estar sendo furtada da concessionária, no caso com origem em perdas não-técnicas por furto de energia.

$$L_{tl} = P_{UTR} - \sum_{x=1}^{n} P_{SGE(x)} - P_{tec} \quad (6.1)$$

Onde L_{tl} é a Perda de Potência total do Cluster (kW), P_{UTR} é a Potência total lida pela Unidade Terminal Remota ou qualquer outro IED responsável pela Medição do cluster em questão, "n" é o número de elementos inteligentes de medidas instalados no cluster e $P_{SGE(x)}$ é a Potência do elemento inteligente de medida "x". A parcela P_{tec} referesse à perdas técnicas de cabeamento e instalações, que neste caso são iguais à ZERO.

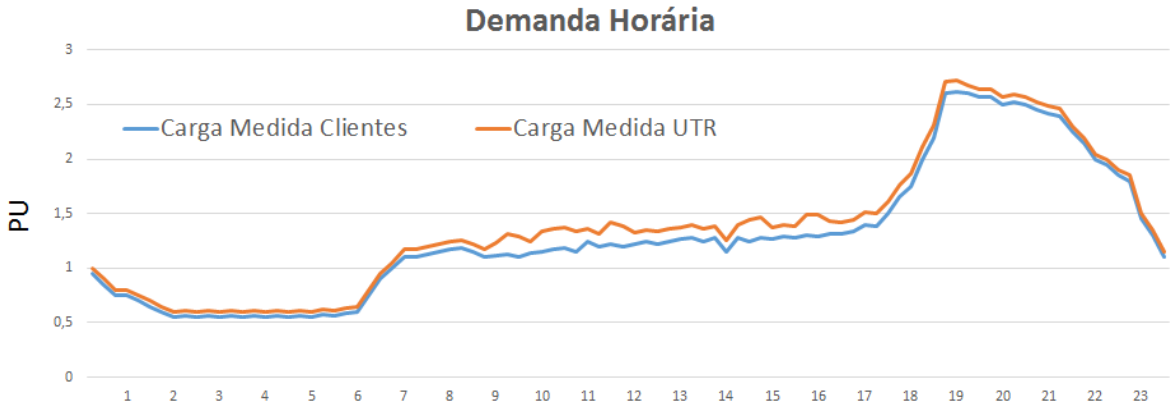


Figura 6-29: Curvas de demanda (potência ativa) do ∑Clientes e UTR do alimentador.

Conforme ilustrado na Figura 6-30, a curva da diferença das demandas apresenta um perfil atual de demanda desconhecida e traz à luz o perfil das cargas que estão sendo utilizadas ilegalmente, fazendo com que seja identificável se o perfil é de uso comercial ou residencial, ajudando na identificação da fonte da perda.

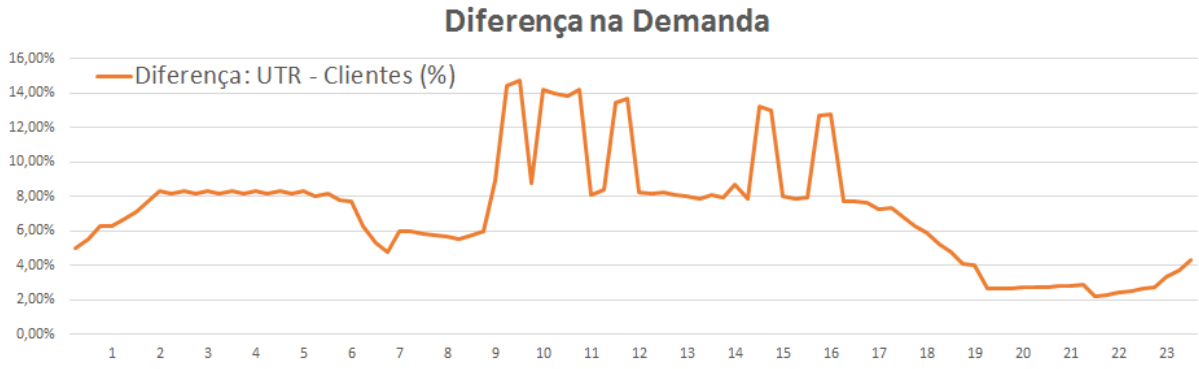


Figura 6-30: Diferença percentual entre demandas (UTR - ∑Clientes)

Na Figura 6-31 é exemplificado um dos blocos de dados do Blockchain correspondentes a medições realizadas pela UTR neste caso de simulação. O conteúdo de cada campo é apresentado, assim como o anagrama hash criptografado correspondente à chave de segurança. A Figura 6-32 ilustra um bloco de medição de um dos medidores envolvidos no teste que perfazem um total de 25 medidores.

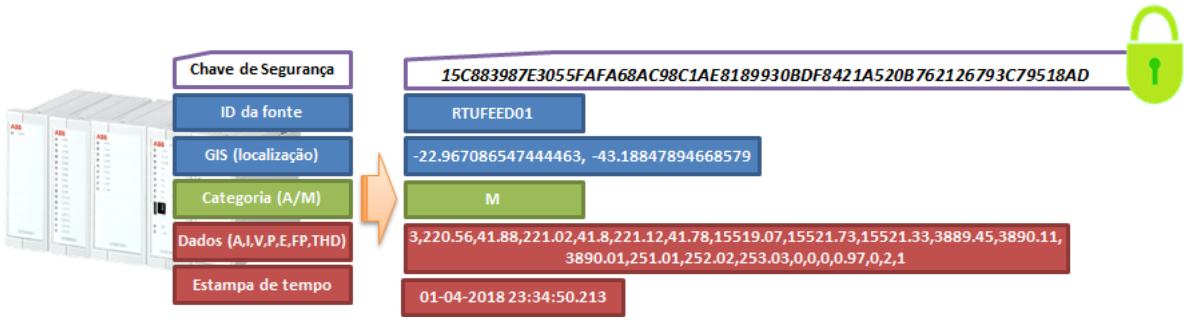


Figura 6-31: Bloco de dados da UTR da Subestação.

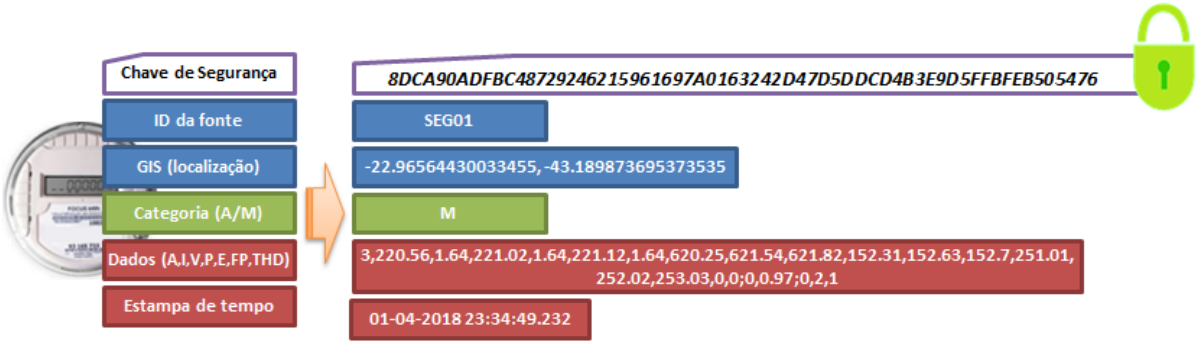


Figura 6-32: Bloco de dados de um medidor inteligente da rede.

6.3.3 Resultados Numéricos

Em cidades de médio ou grande porte, as subestações secundárias típicas de distribuição em baixa tensão podem atender de dezenas a centenas de clientes residenciais e comerciais. As modernas redes AMI enviam as leituras de medições elétricas diretamente pelos dispositivos de medição inteligentes. No caso do SCMI, além do envio direto das medições pelos medidores, ainda se tem a ação dos Agentes de medição, os quais tendem a gerar um alto grau de redundância de informações de um mesmo medidor. Estas medições, conforme já detalhado neste trabalho, são enviadas para a nuvem de serviços Blockchain.

Os testes apresentados nesta seção, impuseram um número previsível de dados de medição aos cenários de avalanche simulados, face às possibilidades do mundo real. Os cenários de avalanche de dados são compostos de um gande número de blocos sendo entregues aos mineradores ao mesmo tempo. Algumas métricas foram utilizadas para avaliar o desempenho do algoritmo de mineração, tendo em vista diferentes cargas de blocos nos BD de entrada.

Cada bloco criado possuiu sua própria chave de segurança e, consequentemente, foi processado como uma informação exclusiva. Com isso, foi

garantido que todos os blocos processados eram diferentes e únicos. Não foram criados blocos redundantes, pois estes seriam descartados no processo inicial de verificação básico do algoritmo de mineração. A ideia foi avaliar os casos de sucesso onde os blocos são íntegros e com medições válidas, transitando em todas as fases do algoritmo. Em termos de performance, os testes representam o pior caso, ou seja, o processamento completo do bloco sem descartes no meio da mineração.

Desempenho dos Mineradores

Os testes de desempenho foram realizados para os blocos de medição e para os blocos de comando separadamente, visto que cada tipo de bloco possui um tempo de processamento diferente, devido às verificações semânticas nos contratos inteligentes. Os resultados dos testes levaram em consideração duas situações distintas de acordo com o tipo do bloco, conforme descrito a seguir.

a) Testes de desempenho nos blocos de Medição

Para os blocos de medição, foram testados o tempo de processamento mínimo, médio e máximo de um único bloco da base de dados de entrada, tomando em consideração cinco cenários de mineração contendo respectivamente: 3, 5, 7, 9 e 11 mineradores no processo. Cada cenário contemplou quatro cargas diferentes de blocos, respectivamente com 100, 1.000, 5.000 e 10.000 blocos na BD de entrada do minerador. O bloco testado foi o primeiro bloco da lista e o teste foi repetido 12 vezes, sendo os tempos de processamento apresentados na Figura 6-33.

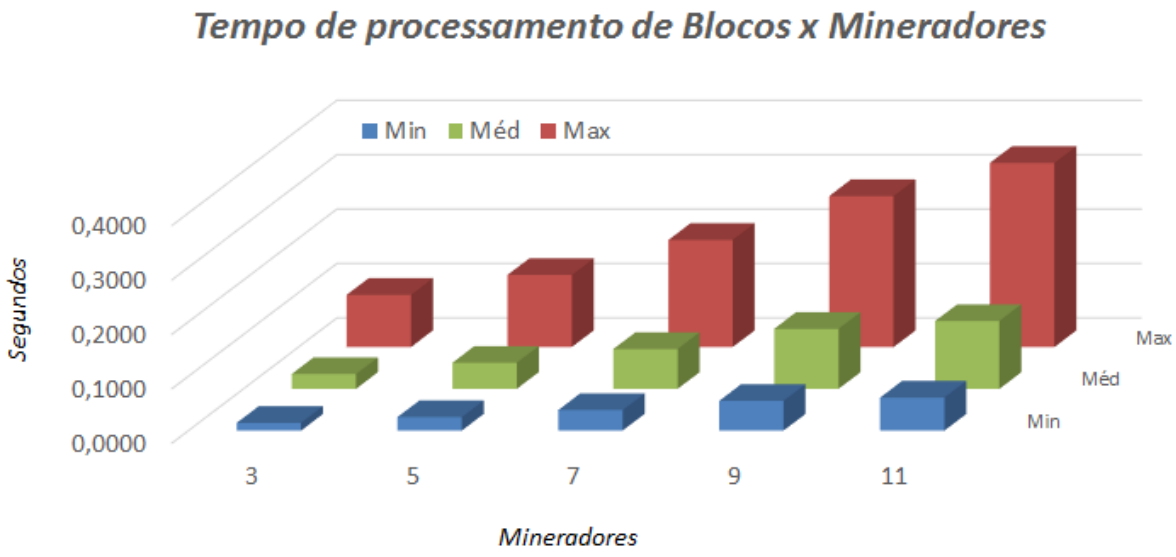


Figura 6-33: Processamento de blocos de medição por grupo de mineradores.

Para o cálculo dos tempos apresentados, foram utilizados registros de estampa de tempo em alguns pontos do processo. O tempo de transmissão de dados entre a fonte do bloco (Agente/SGE) e os mineradores não foi considerado porque a análise de desempenho foi focada somente no algoritmo do minerador. O meio físico de comunicação entre os elementos de campo (Agente/SGE) e o Blockchain não faz parte das análises e propostas deste trabalho, apesar de ter sido exemplificada no Capítulo 4.

Conforme mostra a equação (6.2), o tempo total de processamento de bloco "Tt" é composto pelo tempo de acesso à base de dados de entrada "Tdb", o tempo de verificação cruzada de mineração "Tc", o tempo de processamento do contrato inteligente "Tsc" e pelo tempo de atualização da cadeia de blocos "Tbc":

$$\mathrm{Tt} = \mathrm{Tdb} + \mathrm{Tc} + \mathrm{Tsc} + \mathrm{Tbc} \tag{6.2}$$

Vale ressaltar que o tempo "Tdb" é totalmente dependente da estratégia de implementação da base de dados e do tipo de base de dados utilizada (i.e., SQL, Oracle, MySQL, etc.). Os testes descritos neste capítulo foram realizados com acesso direto à memória para a gravação e leitura de dados, não utilizando base de dados física baseada em arquivos. Alguns fabricantes de banco de dados utilizam a técnica de espelhamento da BD na memória, ou seja, a técnica usada nos testes não se desvia tecnicamente de uma implementação real de banco de dados.

Conforme mostrado na Tabela 6-3, os valores detalhados de tempo estão divididos em: tempo mínimo aferido no cenário de 100 blocos, tempo máximo aferido no cenário de 10 mil blocos e tempo médio aferido contanto com todos os quatro cenários de avalanche de blocos.

Tabela 6-3: Mineradores x tempo de processamento do bloco de medição (seg)

Mineradores	Mínimo (100bl)	Máximo (10kbl)	Médio (todos)
3	0.0143	0.0960	0.0271
5	0.0249	0.1326	0.0480
7	0.0378	0.1969	0.0732
9	0.0546	0.2776	0.1103
11	0.0606	0.3386	0.1246

Devido ao algoritmo de verificação cruzada, o tempo de processamento é diretamente afetado pelo aumento no número de mineradores devido à ordem do algoritmo ser O (n^2). Nesta etapa, todos os mineradores enviam os blocos aprovados

internamente para serem aprovados pelos demais mineradores. Por este motivo se observa um aumento nos tempos de processamento do bloco com o aumento de número de mineradores.

Intuitivamente, seria razoável pensar que um aumento no número de mineradores aumentaria a segurança do processo de telemedição e a sua resiliência em relação às tentativas de fraudes. No entanto, o SCMI proposto foi desenvolvido de tal forma que a segurança do sistema não depende diretamente do número de mineradores empregados no Blockchain. A confiabilidade do sistema pode ser garantida mesmo que apenas três mineradores estejam disponíveis, o que gera um substancial ganho de performance, conforme visto nos dados apresentados. Embora uma invasão cibernética total seja mais fácil de ocorrer com apenas três mineradores em vez de um sistema com onze mineradores, o custo-benefício e as reais condições de ameaças de fraude devem ser analisadas para se tomar uma decisão ótima sobre o número de mineradores a serem empregados.

b) Testes de desempenho nos blocos de Comando

Os testes referentes aos blocos de comando, foram desenvolvidos para um cenário com 100 blocos na base de dados de entrada. Para a mesma carga de blocos, foram testados os mesmos grupos de mineradores usados para os blocos de medição (3, 5, 7, 9 e 11).

Os blocos de comando são prioritários em relação aos blocos de medição e possuem sua base de dados de entrada distinta. Os 100 blocos criados para os testes simulam um cenário exigente, além das expectativas no que tange à redes de baixa tensão. Como o processamento dos blocos de comando demanda muito pouco tempo de processamento, os testes foram repetidos 30 vezes. O mesmo teste foi realizado para cada um dos grupos de mineradores a fim de se coletar valores representativos, minimizando o efeito das oscilações momentâneas da performance da plataforma de testes. A Figura 6-34 ilustra os valores encontrados do total de tempo de processamento de todos os blocos de comando no melhor caso, baseado nos valores mínimos, nos piores casos, baseados nos valores máximos e no caso médio. Os valores de base seguem listados na Tabela 6-4 para o cenário de 100 blocos de comando.

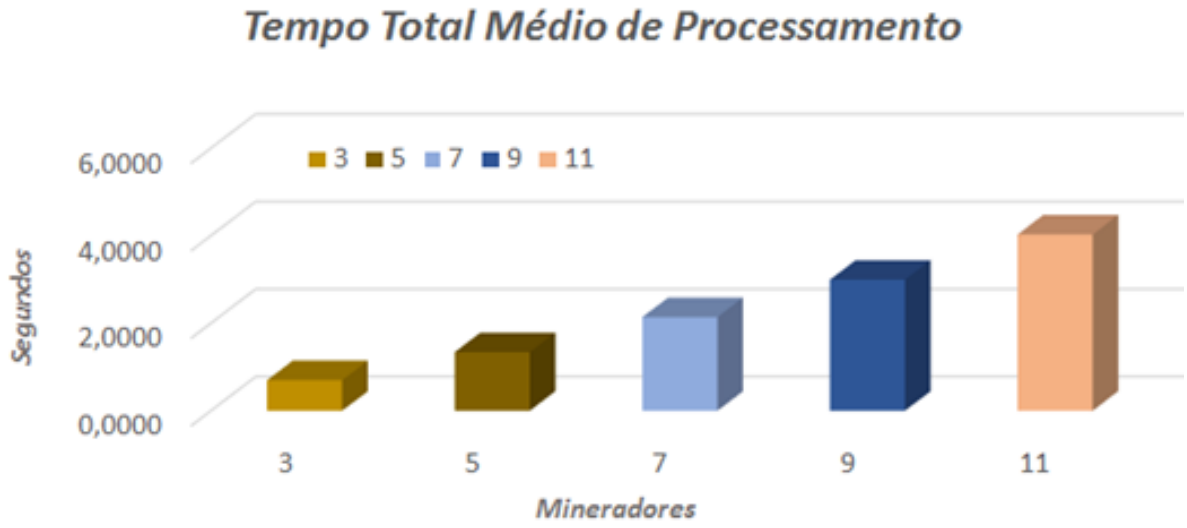


Figura 6-34: Processamento de 100 blocos de comando por grupo de mineradores.

Tabela 6-4: Mineradores x tempo de processamento de 100 blocos de comando (seg)

Mineradores	Mínimo	Máximo	Médio
3	0,6020	2,7710	0,6996
5	1,1769	2,6943	1,3392
7	1,8235	3,1239	2,1399
9	2,3245	3,9456	2,9960
11	2,7542	7,5204	4,0283

Calculando cada um dos valores totais de processamento do Blockchain do pior caso referente ao uso de 11 mineradores (equações (6.3), (6.4) e (6.5)), nota-se que em no máximo 7,5 segundos todos os 100 comandos já estariam processados e prontos para serem emitidos aos medidores inteligentes.

$$\mathrm{Tbcmin} = 0{,}0275 * 100 = 2{,}754s \tag{6.3}$$

$$\mathrm{Tbcmax} = 0{,}0752 * 100 = 7{,}520s \tag{6.4}$$

$$\mathrm{Tbcmed} = 0{,}0402 * 100 = 4{,}028s \tag{6.5}$$

Imaginando as etapas envolvidas no ciclo de telecontrole, a equação (6.6) indica cada um dos elementos temporais que devem ser levados em consideração para o cálculo do tempo total de execução de comandos remotos.

$$\mathrm{Tt} = \mathrm{T1} + \mathrm{Tbc} + \mathrm{T2} + \mathrm{Tm} + \mathrm{Tsw} \tag{6.6}$$

Onde temos "T1" é o tempo de comunicação de dados entre a concessionária até o sistema Blockchain, "Tbc" é o tempo de processamento total do Blockchain, "Tm"

é o tempo de processamento da requisição de comando pelo medidor inteligente e "Tsw" é o tempo de chavemento do elemento de corte de fornecimento, instalado dentro do medidor.

Cenários de avalanche de dados de medição

Conforme informado na Seção anterior, os testes foram realizados levando-se em consideração quatro cenários de avalanche de dados e cinco conjuntos de mineradores. A avalanche de dados significa que uma massa de blocos é emitida ao mesmo tempo para o banco de dados de entrada, o que altera o tempo total de acesso a cada informação, dependendo da quantidade de blocos.

A disponibilidade de diferentes quantidades de mineradores (3, 5, 7, 9 e 11) foi considerada nas simulações. Os cenários de avalanche consideraram 100, 1.000, 5.000 e 10.000 blocos para cada um dos cinco conjuntos de mineradores. Os blocos foram enviados pelo módulo de criação de blocos (Seção 6.2.2), que representa dispositivos de medição inteligentes e/ou qualquer outro agente que coleta dados com um dispositivo móvel. Esse volume de blocos reflete um cenário da vida real em que várias leituras são obtidas em uma única área de uma subestação secundária ou posto de transformação (MT/BT) que cobre clientes residenciais e comerciais.

Uma câmara ou posto de transformação que possui capacidade típica de 500kVA (LIGHT, 2018) poderia suportar facilmente 200 clientes residenciais. Assumindo que cada cliente possuí um medidor inteligente conectado diretamente à rede *Internet* de comunicação e envie os blocos de medição à nuvem de serviços Blockchain, tem-se 200 blocos a serem processados a cada 15 min, o que corresponde a um período típico de integração de dados de energia. Somando-se a isto uma quantidade aleatória de Agentes no alcance de comunicação com estes medidores, pode-se ter alguns milhares de blocos a cada ciclo de 15 minutos.

a) Tempos de Processamento

O resultado levantado neste relatório leva em consideração o processamento de todos os blocos nos diferentes cenários apresentados. Os valores aferidos e mostrados na Figura 6-35 e na Tabela 6-5, refletem os tempos médios, entre todos os blocos processados, para cada um dos cenários de avalanche e de grupo de mineradores.

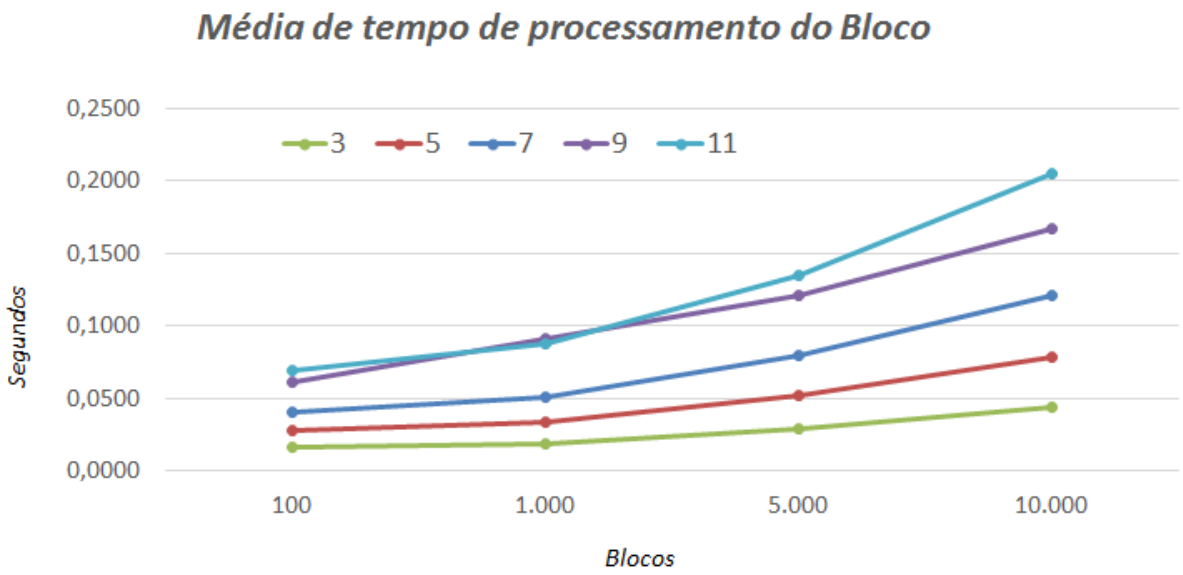


Figura 6-35: Tempo médio por cenário.

Conforme descrito na Tabela 6-5, no caso da avalanche de 10 mil blocos, o tempo médio encontrado para processar um bloco foi de 0,2052 segundos, considerando um grupo de 11 mineradores inseridos no sistema e realizando as verificações cruzadas entre si.

Tabela 6-5: Cenários de avalanche x tempo médio de processamento do bloco (seg)

Número de Blocos	3	5	7	9	11
100	0.0162	0.0276	0.0403	0.0617	0.0695
1,000	0.0186	0.0333	0.0514	0.0907	0.0881
5,000	0.0296	0.0519	0.0797	0.1216	0.1354
10,000	0.0440	0.0790	0.1214	0.1671	0.2052

Nesse caso, o tempo esperado de entrega “Td” do último bloco presente na BD de entrada do Blockchain seria:

$$\mathrm{Td} = 0{,}2052 * 10.000 = 2.052\,s \sim 34\,min \quad (6.7)$$

Por outro lado, ao considerar o mesmo cenário de 10 mil blocos em avalanche com 3 mineradores no sistema, o tempo esperado para a entrega do último bloco presente na BD de entrada do Blockchain seria:

$$\mathrm{Td} = 0{,}0440 * 10.000 = 440\,\mathrm{s} \rightarrow 7{,}3\,min \quad (6.8)$$

Através dos valores encontrados na Tabela 6-5 e na equação (6.7), pode-se inferir que um bloco, no pior caso, demoraria cerca de 34 minutos para ser liberado

pelo Blockchain a fim de ser utilizado pela concessionária. Como se terá medições de energia atualizadas apenas a cada 15 minutos, o faturamento teria apenas uma única medida ainda em atraso. Assim, como os procedimentos de faturamento de energia são mensais, esta demora na entrega não afetaria este setor da concessionária. No que diz respeito à manutenção, os alarmes que por ventura venham a ser gerados nos medidores, só motivariam uma ação da manutenção depois da sua entrega (34 min). O mesmo ocorreria com o uso dos dados pelo setor de operação, que veria alterações nos últimos dados de medição depois de 34 min.

Analisando-se o resultado da equação (6.8), o tempo máximo de 7,3 minutos atenderia perfeitamente a área de faturamento e manutenção, o que não seria compatível apenas com o ambiente de operação em tempo real, o que é um ponto discutível e analisado nos comentários localizados no fim deste capítulo.

Uma segunda análise foi realizada no caso da avalanche de apenas 100 blocos por vez. O tempo médio de processamento foi de 0,0695 segundos considerando-se um grupo de 11 mineradores inseridos no sistema e realizando-se as verificações cruzadas entre si.

Nesse caso, o tempo esperado de entrega "Td" do último bloco presente na BD de entrada do Blockchain seria:

$$\mathrm{Td} = 0{,}0695 * 10.000 = 695{,}00\,\mathrm{s} \sim 11{,}58\,min \tag{6.9}$$

Por outro lado, ao se considerar o mesmo cenário de 100 blocos por vez em avalanche com 3 mineradores no sistema, o tempo esperado para a entrega do último bloco presente na BD de entrada do Blockchain seria:

$$\mathrm{Td} = 0{,}0162 * 10.000 = 162{,}00\,\mathrm{s} \sim 2{,}7\,min \tag{6.10}$$

Os valores encontrados em (6.9) e (6.10) indicam que um bloco, no pior caso, demoraria cerca de 11,58 minutos para ser liberado pelo Blockchain a fim de ser utilizado pela concessionária. A área de faturamento não teria nenhum bloco de medição de Energia em atraso e a manutenção teria um retorno de possíveis alarmes em tempos razoáveis para os padrões atuais de manutenção corretiva.

b) Capacidade de Processamento de Blocos

Com um alto nível de engajamento dos usuários, consequentemente alcançando uma grande quantidade de Agentes ativos de medição atuando diariamente, o SCMI pode ter que tratar grandes quantidades de dados. Assim, se faz necessária uma métrica que represente a quantidade de blocos possíveis para cada cenário de mineração.

Levando-se em consideração uma linha temporal, foram realizadas análises com dois tipos de cenários de cargas de avalanche. A carga mínima de 100 blocos e a máxima com 10 mil blocos por ciclo. Cada ciclo termina quando todos os blocos da avalanche foram processados, gerando uma nova avalanche e assim ocorrendo sucessivamente. O objetivo foi aferir o número de blocos que podem ser processados pelo simulador SCMI para os cenários informados. No melhor cenário, com 100 blocos na avalanche apresentado na Figura 6-36, considerando uma janela de tempo de 15 minutos, o SCMI simulado processou quase 13.000 blocos com 11 mineradores e mais de 55.000 blocos com 3 mineradores.

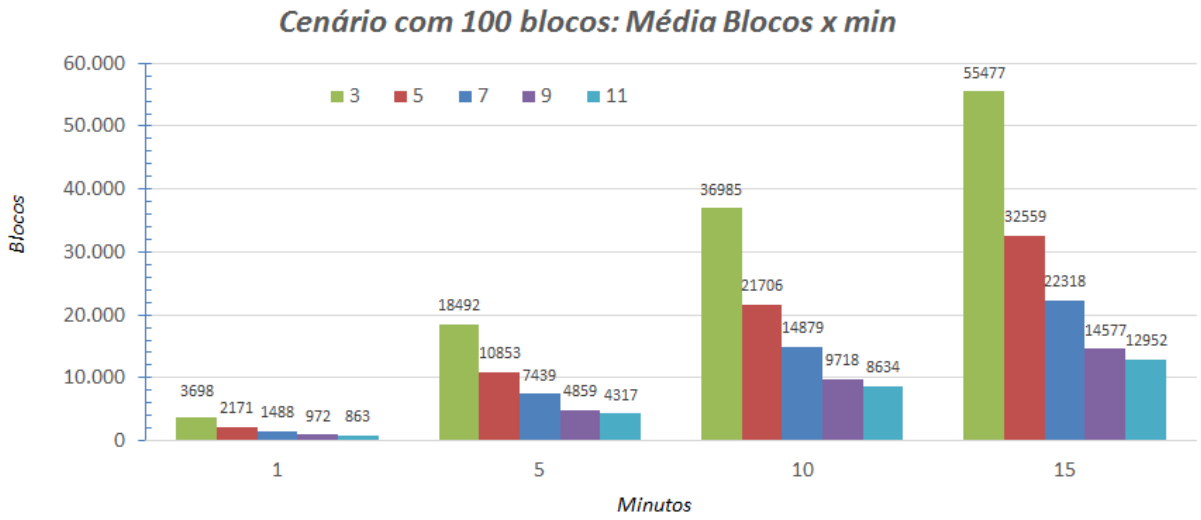


Figura 6-36: Média de tempo com cenário de 100 blocos.

Considerando-se hipoteticamente a presença de 200 medidores e dividindo-se os números de blocos processados pelo número de medidores, obtém-se aproximadamente 65 (com 11 mineradores) até 275 (com 3 mineradores) blocos de medidas para um mesmo medidor no intervalo de 15 minutos. Tais números apresentam uma distribuição equitativa entre os medidores. Se cada medidor for inteligente e com capacidade de distribuir seus dados direto à nuvem de serviços Blockchain, obter uma medição por minuto de cada medidor significaria 15 blocos

neste intervalo de tempo. Neste caso, sobrariam de 50 até 260 blocos para serem coletados por Agentes que tenderão a possuir uma distribuição não homogênea de coleta para cada medidor, visto sua característica aleatória. A partir desta análise, infere-se que as medições de energia teriam a possibilidade de estar sobre-garantidas neste tipo de cenário. Caso a atualização de medidas provenientes de um dado medidor ocorra em um curto período (alguns segundos), as informações de outras medidas elétricas tais como tensão, corrente e potências poderiam ser disponibilizadas de maneira dinâmica ao sistema SCADA ADMS/DMS.

O pior cenário em termos de resultados está ilustrado na Figura 6-37. Neste caso os dados analisados são referentes aos testes de avalanche de 10 mil blocos ao mesmo tempo, considerando-se a mesma janela de tempo de 15 minutos. Os resultados da simulação apontam para mais de 4.300 blocos quando se tem 11 mineradores e mais de 20.000 blocos com 3 mineradores. Realizando-se a mesma análise de blocos por medidor, temos o equivalente a 21 até 100 blocos de medidas para um mesmo medidor no intervalo de 15 minutos com uma distribuição homogênea de blocos por medidor.

Com 15 blocos de medição (um a cada minuto) sendo enviado por cada medidor inteligente, teremos de 6 até 85 blocos de medição que poderiam ser coletados por Agentes de medição. Neste caso mais extremo, estariam garantidas as medições de energia e se teria atualizações de medidas de corrente, tensão, potências e eventuais alarmes a cada 1 minuto, no máximo, garantidas pelos medidores.

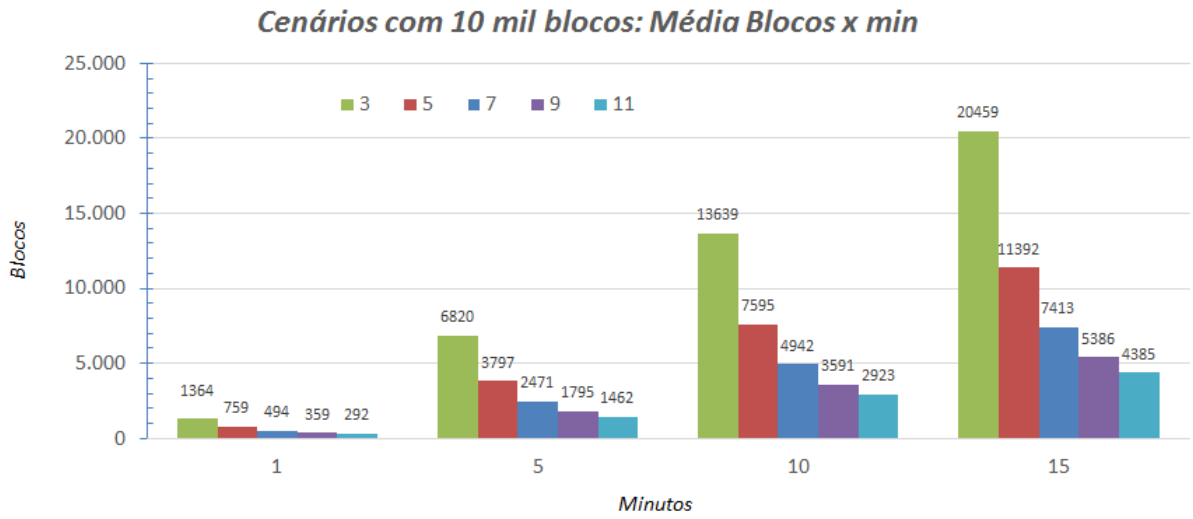


Figura 6-37: Média de tempo com cenário de 10 mil blocos.

c) Avaliação da capacidade dos clusters

Os resultados até agora apresentados mostram que o número de blocos de medição possíveis por medidor se encontra em um patamar interessante no que tange a cobertura de ação do sistema. Para se calcular quantos *clusters* poderiam ser cobertos pela mineração Blockchain proposta, alguns dados foram analisados e outros estimados:

- Quantidade de medidores por Cluster: $QM_{cl} = 1.000\ medidores$
- Quantidade mínima de blocos de medição desejada por medidor a cada 15 minutos (distribuição homogênea): $Qbl = 15\ blocos\ de\ medição$

Tomando como base um sistema de mineração com 5 mineradores, os resultados mostram $QB_{M5} = 32.559$ blocos passíveis de serem processados em situação de avalanche de 100 blocos por vez. Ao se aplicarem os valores especificados acima, os seguintes resultados mostrados em (6.11) são obtidos:

$$Qcl = \frac{\frac{QB_{M5}}{Qbl}}{QM_{cl}} = \frac{\frac{32.559}{15}}{1.000} = 2{,}17 \approx 2\ \text{clusters} \qquad (6.11)$$

O resultado apresentado (2 clusters) significaria um total de 2.000 medidores sendo atendidos por um único grupo de mineração.

Comentários

Importante ressaltar que os resultados obtidos para os quatro cenários de avalanche foram aferidos em simulações realizadas utilizando uma plataforma desenvolvida em Matlab™ com uma estação de trabalho convencional e sem performance computacional significativa.

O desempenho do SCMI em tais condições não poderia ser considerado bom o suficiente para ser usado na operação em tempo real. No entanto, na operação de sistemas SCADA ADMS aplicados a redes de baixa tensão não se faz necessário o processamento em tempo real de medidas de energia consumida dos clientes. Quando as tensões, correntes e potências são supervisionadas nos medidores inteligentes, os SCADAs contam com redes de medidores com capacidade de aquisição em períodos menores. Partindo da premissa que um medidor inteligente teria tecnologia para enviar as medições diretamente para o sistema Blockchain, teria-se monitoramento garantido de todas as grandezas disponíveis nos períodos de amostragem respectivos à cada medidor.

Nota-se que os tempos médios encontrados de processamento de blocos encontrados nos cenários testados são quase todos abaixo de 200 milissegundos. Com isto, pode-se prever um aumento significativo de desempenho do algoritmo de mineração proposto caso sejam utilizados os poderosos recursos computacionais compatíveis nas unidades de hardware dedicadas à mineração, já citadas neste trabalho. Os resultados obtidos dão indicação da factibilidade do uso da mineração Blockchain considerando-se os padrões atuais de telemedição em redes de distribuição.

A robustez do sistema pode ser melhorada com a colaboração de mais agentes, reduzindo-se a possibilidade de perda de leituras. Estratégias de recompensa podem ser criadas para motivar os agentes a participarem da rede colaborativa (CAMARINHA-MATOS, 2016), tornando-se agentes ativos de leitura por meio de seus dispositivos móveis. Essa ação pode aumentar o número de medições coletadas e a qualidade da supervisão do sistema.

Capítulo 7

Conclusão e Trabalhos Futuros

Inegavelmente, o uso da energia elétrica constitui um dos alicerces para a conquista de grandes avanços da sociedade moderna, sendo em grande medida impulsionadora da descoberta de novas tecnologias e processos inovadores. Nesta linha, várias pesquisas vêm sendo conduzidas de modo a encontrar meios de aperfeiçoar sua eficiente distribuição e supervisão. O desenvolvimento das chamadas redes elétricas inteligentes cumpre este papel, uma vez que busca eficiência econômica e energética, de modo confiável, se valendo de tecnologias digitais avançadas. Esta nova geração de redes elétricas monitoram e gerenciam o transporte de eletricidade com informações bidirecionais entre o sistema de fornecimento de energia e o usuário final.

Em uma rede elétrica dita inteligente, dados da medição do consumo energético trafegam por redes de comunicação digital até o armazenamento em bancos de dados para tarifação e diversos estudos. A construção de um sistema de medição inteligente é amplamente reconhecida como o primeiro passo para o estabelecimento de redes inteligentes.

Inovadoras ideias em um mercado conservador tal como o de energia elétrica devem se estruturar através de propostas convenientemente descritas, para que venham a ser implementadas, validadas e adotadas. As contribuições diversas ao se propor um sistema colaborativo de medição inteligente com base na tecnologia Blockchain destinado a um sistema de distribuição de energia elétrica moderno são a seguir sintetizadas.

Como benefícios aos consumidores, espera-se: melhoria nos serviços das concessionárias com a participação ativa dos consumidores (agentes colaborativos); identificação e envio direto à concessionária de possíveis erros de medição nos seus próprios medidores; premiações por participação na cadeia de suprimento-consumo de energia (descontos de tarifa, crédito em criptomoedas, crédito de dados de telefonia, premiações por cobertura, etc.).

Figura 7-1: Contribuições do SCMI

Em relação às concessionárias, vislumbra-se uma série de vantagens provenientes do sistema colaborativo de medição inteligente proposto, das quais algumas são ilustradas esquematicamente na Figura 7-1 e listadas a seguir:

- Cobertura de telemedição em áreas sem infraestrutura de comunicação da concessionária;
- Localização de falta com alta precisão geográfica com base nos dados da telemedição dos agentes colaborativos;
- Identificação de ilhamentos e autossuficiência energética em microredes;
- Subsídios para análise de perdas e perturbações em certos locais da rede;
- Apoio aos serviços de manutenção para atender automaticamente a emergências do sistema;
- Apoio aos sistemas de reconfiguração automática da rede elétrica;

- Melhoria na automação dos sistemas de distribuição com o aumento da capacidade de monitoramento;
- Análise de perfil de carga gerando informações para os programas de resposta da demanda;
- Auxílio para a função estimação de estado em termos da disponibilidade de medições;
- Diminuição dos custos de referentes aos sistemas de telecomunicação para a distribuição de dados de medições de grandezas elétricas.

Como está desenhado, o sistema de medição inteligente proposto reduz significativamente os custos de instalação de uma rede elétrica inteligente, bem como permite a modernização de uma rede existente, por não demandar nenhuma instalação de infraestrutura de telecomunicações entre o consumidor/prosumidor e a concessionária. Para a adequação de um sistema avançado de medição existente ao sistema proposto com base na tecnologia Blockchain, são necessários investimentos tais como: interfaces de comunicação wi-fi, Bluetooth/BLE ou equivalente para os dispositivos de medição; aplicativos para dispositivos móveis; servidores de mineração de dados Blockchain e adequações de software nos Centros de Controle.

As tecnologias de medição remota utilizadas nas redes elétricas inteligentes atuais não são capazes de corresponder às gradativas exigências do setor elétrico para a distribuição de energia. O sistema de medição baseado na tecnologia Blockchain proposto se constitui em uma alternativa promissora, de acordo com os resultados obtidos com a prova de conceito realizada no Capítulo 6. Tais resultados evidenciam que os algoritmos do sistema proposto possuem características desejadas de segurança, resiliência e flexibilidade, e que também alcançam desempenho compatível para a realização de manutenção na rede elétrica, de cobrança de energia, etc. Os testes realizados mostram uma capacidade considerável do sistema proposto para o processamento de blocos de dados, se apresentando como uma solução robusta de telemedição inteligente em redes de pequeno e médio porte de baixa tensão.

Considerando o que foi apresentado nesta Tese sobre a concepção, implementação e benefícios da tecnologia Blockchain para a transmissão de dados em sistemas de energia, pode-se depreender, de forma sintética, que há soluções computacionalmente factíveis e atraentes em termos tecnológicos/financeiros, para problemas importantes e atuais, tais como aqueles que envolvem: telemedição

massiva e distribuída, envolvendo altos investimentos de infraestrutura de telecomunicações; modernização de sistemas que apresentam alto custo de migração tecnológica; implantação de modelos de mercado multiagentes convivendo em uma mesma região e compartilhando os mesmos serviços essenciais de transporte de dados para a comercialização de energia; segurança de informações (sigilosas e privadas); faturamento de energia sem interferência humana.

Destaca-se também que a estimação de estado (GOMEZ-EXPOSITO, ABUR, *et al.*, 2011) tem sido vista como uma importante função dos sistemas de gerenciamento da distribuição. Valores de medidas estimadas são usados como dados de entrada para outras funções (e.g., análise de contingências e otimização operativa). Entretanto, o uso desta ferramenta muitas vezes esbarra na falta de observabilidade da rede, ou seja, sofre pela escassez de medições provenientes das áreas supervisionadas. O sistema proposto pode contribuir para a estimação de estado distribuída (PAU, PATTI, *et al.*, 2016) e para a criação de uma estimação de estado móvel, como será mencionado na proposta para trabalhos futuros.

Os sistemas de distribuição de baixa tensão possuem características que por vezes podem dificultar a identificação de pequenas anomalias até problemas mais graves. Tal dificuldade pode residir na identificação da causa ou na determinação do local da falha. Um destes problemas são as denominadas faltas de alta impedância. Com o sistema proposto, o monitoramento detalhado de todos os usuários instalados e o registro da sua localização geográfica facilitam a identificação de faltas na rede monitorada.

Outro grande desafio na distribuição de energia em baixa tensão é a identificação da origem de perdas e desvios na qualidade de energia, tendo em vista a capilaridade deste tipo de rede e os aspectos de natureza social que o fornecimento de energia está atrelado. O sistema proposto SCMI poderia auxiliar na análise local de perdas com a identificação de perdas não-técnicas e técnicas utilizando sua cobertura de medição mesmo em áreas de difícil acesso.

TRABALHOS FUTUROS

Considerando que esta Tese trata de tema bastante atual que experimenta a fase de desenvolvimento inicial, torna-se apropriado imaginar que haja um caminho longo a percorrer até que as redes elétricas modernas venham de fato a se tornar

capazes de dotar as companhias de energia elétrica de plena visibilidade e amplo controle sobre seus ativos e serviços. As redes elétricas inteligentes devem também estar capacitadas a superar por si mesmas de certas anomalias a que estiverem expostas. Por fim, e não menos importante, tais redes devem viabilizar que seus usuários possam se engajar em tarefas de gestão do próprio consumo/produção de energia. Assim sendo, em continuação ao presente trabalho de pesquisa são apresentados a seguir alguns tópicos que merecem destaque, a saber: estimação de estado, faltas de alta impedância, análise de perdas e qualidade de energia.

Estimação de Estado

O sistema de medição proposto pode contribuir para a concepção de um processo de estimação de estado móvel (EEM), como ilustrado na Figura 7-2.

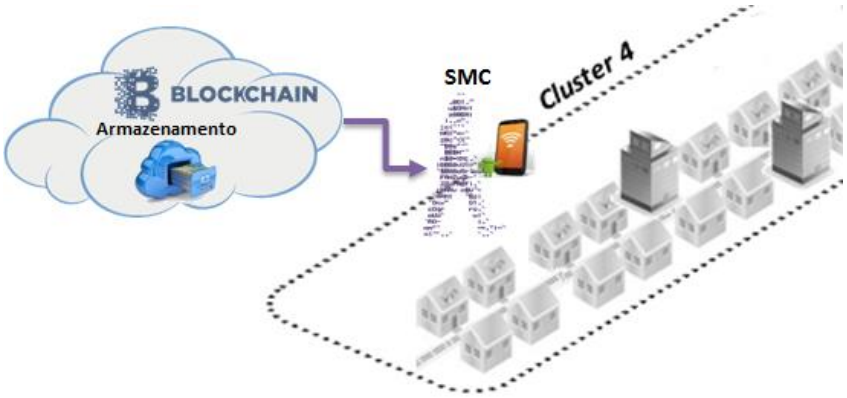


Figura 7-2: Estimação de Estado Móvel

Já foi descrito anteriormente nesta Tese a importância do agente tipo SMC e suas funções especiais. Uma destas funções poderia ser sua colaboração na estimação de medidas, de forma local, a partir de um conjunto de dados disponíveis e de acesso permitido a tal agente. O SMC poderia possuir acesso a uma cadeia de blocos, a fim de obter medidas registradas em respectivo cluster, armazenadas por mineradores. O uso de dados históricos como pseudomedidas para complementar o conjunto de medidas de uma rede de transmissão consta em diversos estudos, tais como nos que utilizam o método FASE (*Forecasting-Aided State Estimation*), na referência (BROWN DO COUTTO FILHO e DE SOUZA, 2009).

Pode-se aplicar a Estimação de Estado sobre diversos pequenos conjuntos de medidas, tomadas em determinadas áreas (clusters), como ilustra a Figura 7-3.

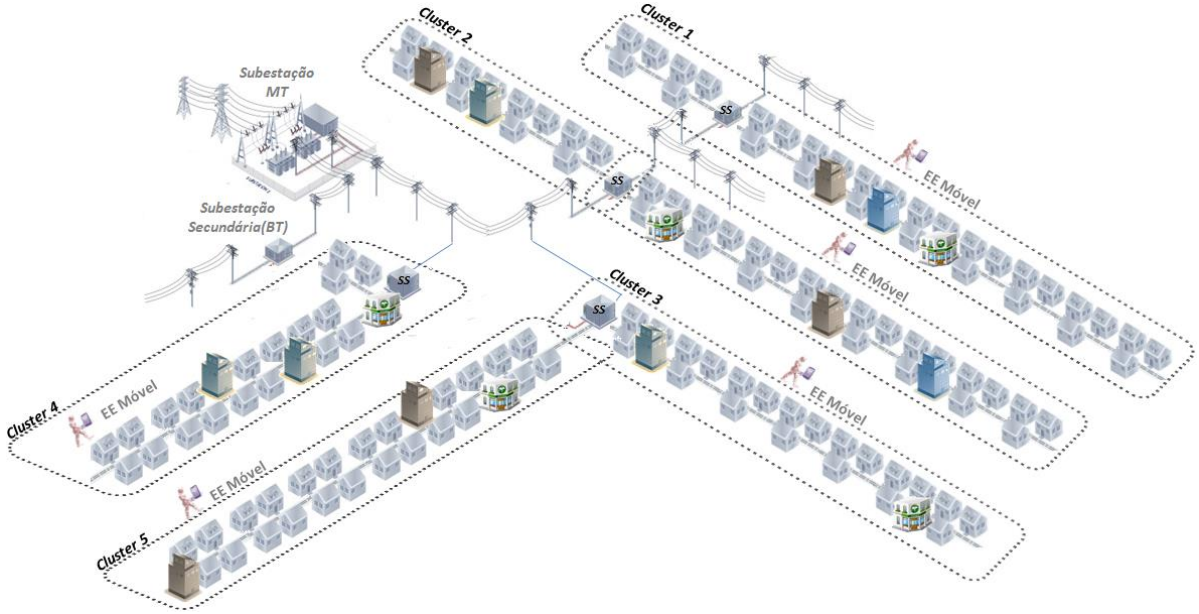


Figura 7-3: Estimação de Estado Móvel e distribuída em Clusters

O crescimento de redes de baixa tensão com micro-geração vem ocorrendo e a estimação de estado em tais redes torna-se necessária (WAERESCH, BRANDALIK, *et al.*, 2015), levando-se em consideração o uso dos medidores inteligentes como fonte de dados para este processo (ABDEL-MAJEED e BRAUN, 2012).

Faltas de Alta Impedância

Este tipo de falta, descrito amplamente na literatura (TENGDIN, 1989), se caracteriza pelo contato de um condutor com uma superfície qualquer de alta impedância, disto decorrendo uma corrente de defeito insuficiente para sensibilizar qualquer sistema de proteção de sobrecorrente instalado na rede, fazendo com que o ponto de falta seja interpretado como o de mais uma carga no sistema. Entretanto, este não é uma carga cadastrada, tampouco possui medidor associado e por consequência não é observável pelo DMS.

Tais ocorrências são comuns em linhas aéreas de média tensão, por causa da ruptura de cabos ou pelo movimento destes submetidos a condições climáticas adversas que provocam o contato deles com as outras superfícies.

Poucos fabricantes de dispositivos de proteção de alimentadores conseguem atuar com sucesso quando ocorre este tipo de falta, pela conhecida complexidade do problema. Usualmente, faz-se uma análise da variação de energia e da corrente no momento da falta, o que permite que algumas “assinaturas” da falta de alta impedância

já possam ser identificadas. Análises dos harmônicos nas zonas de falta também estão cada vez mais usuais como visto em (ZAMANAN e SYKULSKI, 2014) e (SOHEILI, SADEH, *et al.*, 2016) onde uma análise mais detalhada da corrente através da transformada de Fourier, possibilita o reconhecimento de padrões de harmônicos para as faltas simuladas.

Apesar de comumente observadas em linhas de média tensão, estas faltas podem ocorrer também em ramais e entroncamentos de baixa tensão, e segundo as análises encontradas em (KAWADY, TAALAB e ELGEZIRY, 2009), os comportamentos de tensão e corrente são extremamente semelhantes, possuindo similar “assinatura” de falta. Em (HOU, 2009) uma bateria de testes de campo foi realizada com faltas de rompimento de cabos e contato forçado em árvores, pneus e superfície de areia, a fim de registrar não só o comportamento local da corrente, mas também o observado da subestação.

Como referido anteriormente, os agentes participantes do sistema de medição proposto nesta Tese estão constantemente coletando dados (corrente e tensão), caso estas estejam disponíveis nos SGEs, e ainda contam com as informações de localização geográfica das medidas. Caso a falta de alta impedância corresponder à queda de um condutor de fase que toca o solo, pode-se traçar um caminho que levará a uma análise simples de como o sistema de medição proposto pode auxiliar na identificação desta falta, isto porque haverá uma discordância de valores de tensão e ângulo entre as fases nos circuitos de BT e um acréscimo na corrente consumida pelo circuito de MT.

Com auxílio de um algoritmo especializado durante a fase de mineração, o sistema de medição proposto pode verificar se mais de um SGE no mesmo cluster sentiu o mesmo efeito nas tensões, ângulos e correntes (Figura 7-4). Em caso positivo, uma discordância entre fases sistêmica é identificada no cluster e o DMS recebe este alarme juntamente com a equipe de manutenção. Em caso negativo, ou seja, somente alguns SGEs mediram o evento, o defeito tem 100% de chance de estar localizado dentro do cluster. Para isso, não precisa estar prevista nenhuma instalação de IED de proteção específico contra faltas deste tipo, sendo necessária apenas uma análise dos dados de medição já disponíveis no banco de dados do SCMI.

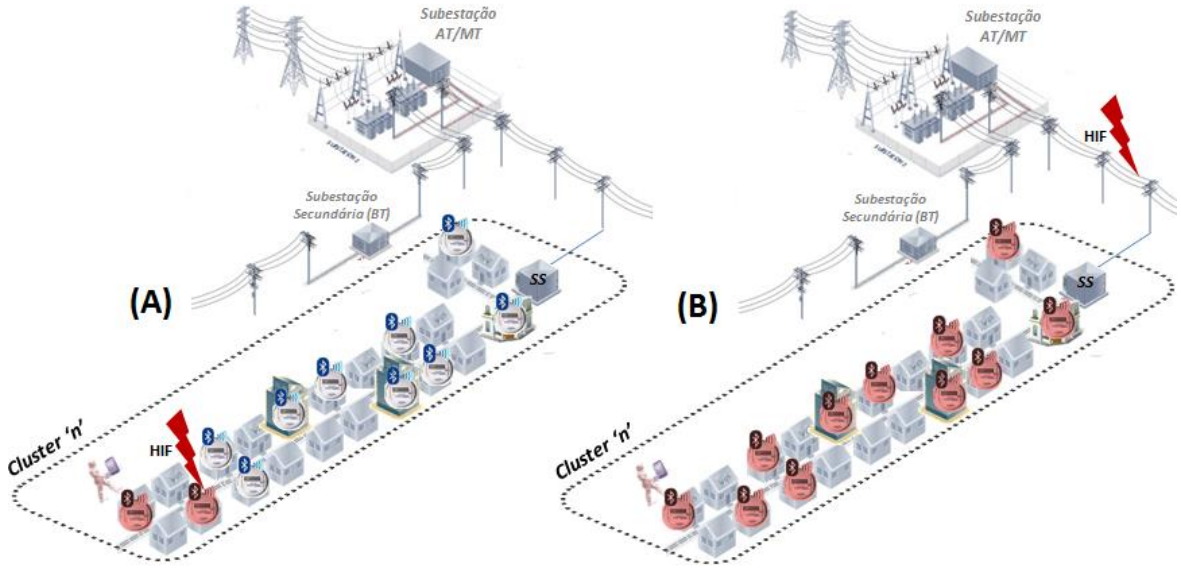


Figura 7-4: Faltas de Alta impedância em BT e MT

Análise de Perdas e Desvios de Qualidade de Energia

As perdas na rede podem ser classificadas como técnicas e não técnicas, ANEEL (http://www2.aneel.gov.br/area.cfm?idArea=801&idPerfil=4). As perdas técnicas correspondem à transformação de energia elétrica em térmica nos condutores (efeito joule), perdas nos núcleos dos transformadores, perdas dielétricas, etc. Quanto às perdas não técnicas, estas correspondem a todas as demais perdas associadas à distribuição de energia elétrica, tais como: furtos de energia, erros de medição, erros no processo de faturamento, etc.

Para se ter uma ideia da magnitude destas perdas no sistema de distribuição de energia elétrica no Brasil, em 2015 (17/04/2015), apuradas todas as perdas do sistema, chegou-se aos seguintes valores, consideradas todas as 63 concessionárias de distribuição existentes naquele ano: R$ 3,78 bilhões em perdas não técnicas e R$ 5,9 bilhões em perdas técnicas.

As perdas técnicas são geralmente mensuráveis pelas especificações e ensaios laboratoriais dos elementos da rede (e.g.: transformadores, cabos, chaves, conectores, etc.), mas contém também componentes variáveis que são diretamente ligados ao tempo de uso, à aplicação e ao ambiente em estão expostos. De certa forma, este tipo de perda é controlável pela concessionária e requer estratégias concretas para sua minimização, ligadas à manutenção preventiva, preditiva e até troca de componentes.

As perdas não técnicas são atualmente um problema crítico para algumas concessionárias, nomeadamente aquelas que têm áreas de concessão com problemas sociais crônicos, envolvendo um número excessivo de furtos de energia, ligações ilegais, adulterações de medidores, etc. A intervenção de um funcionário de manutenção se faz muitas vezes extremamente perigosa e indesejada nestas áreas críticas, o que acarreta uma incapacidade da concessionária de identificar tais problemas. O tempo gasto na identificação de uma fraude pode inviabilizar a ação corretiva, visto que o técnico deve adentrar na área de risco e investigar possíveis focos com alta probabilidade de perdas, efetuando medições e avaliações visuais, o que demanda tempo e concentração, que é deveras complicado sob circunstâncias de grande insegurança.

A título de ilustração, as perdas por fraudes na Espanha (MONEDERO, BISCARRI, *et al.*, 2012) atinge 30%. Em uma análise via mineração de dados históricos da concessionária Endesa juntamente com a análise desvios de consumo de energia e reconhecimento de padrões, foi possível identificar possíveis fontes de fraude, onde o cliente diminuiu seu padrão de consumo. Este tipo de método comparativo também verificado em (COMA-PUIG, CARMONA, *et al.*, 2016) percebe tanto a mudança quantitativa quanto temporal do comportamento de consumo do cliente, identificando se o fraudador é do tipo perene ou sazonal. Apesar de se apresentar como um método complementarmente interessante, se aplica somente nos casos de mudança de comportamento do consumidor, que é apenas um dos sintomas de perdas não técnicas. O que se vê em áreas deste tipo de ocorrência é comumente o consumo estável mínimo (e.g. iluminação, tomadas de uso geral) e o furto de energia para os consumos mais significativos, sejam eles residenciais (e.g., ar condicionado) ou de pequenos estabelecimentos comerciais (e.g., freezers, fritadeiras elétricas, ar condicionado, etc.), o que não gera individualmente uma mudança de comportamento de consumo computada no medidor legalmente instalado, mas sim um mudança coletiva de consumo na área identificada com um acréscimo de carga desconhecida.

Caso haja comportamento suspeito de um cliente no que tange ao decréscimo abrupto, crescente e sistemático do consumo, valendo-se do método do coeficiente de correlação de Pearson (MONEDERO, BISCARRI, *et al.*, 2012) e (COMA-PUIG, CARMONA, *et al.*, 2016), o SCMI proposto pode automaticamente atribuir alarmes que identifiquem o medidor com um grau de confiança abaixo do usual. Este procedimento forneceria mais uma indicação de suspeição que contribuiria para a

identificação da fonte da fraude. No fluxograma da Figura 7-5 ilustra-se o método aqui proposto, onde as curvas de carga são analisadas em cada um dos medidores do cluster a fim de se identificar fraudes ou até mesmo problemas técnicos nos medidores do sistema.

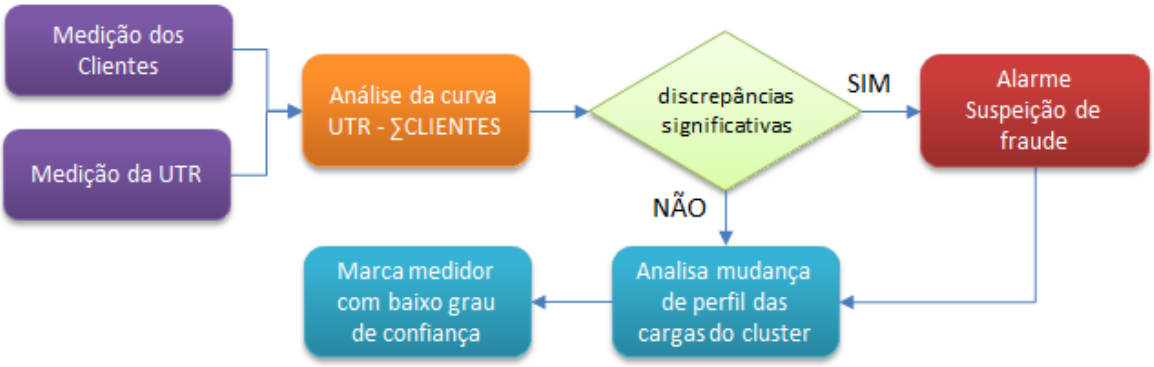


Figura 7-5: Fluxograma simplificado de busca por fraude

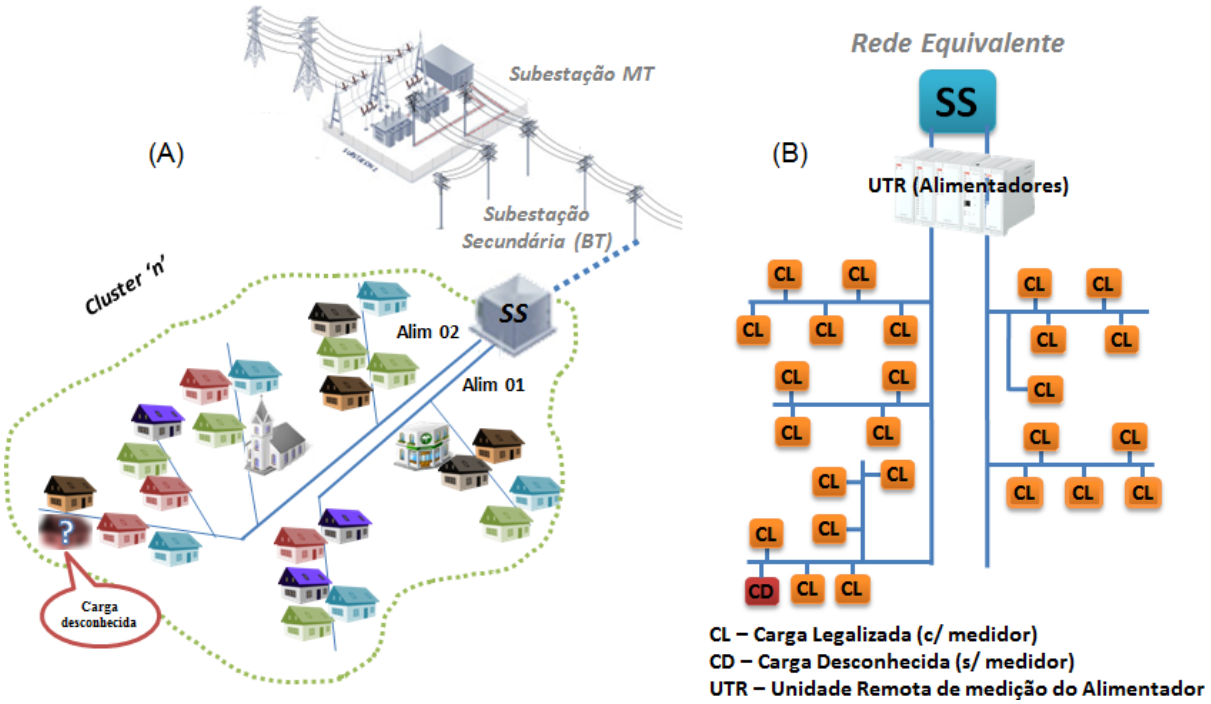


Figura 7-6: Exemplo de uma zona crítica com carga desconhecida

O problema de perdas não técnicas pode também ser tratado no SCMI conforme ilustrado na Figura 7-6. Nela apresenta-se um exemplo de cluster representando uma região crítica com furtos de energia, onde as ruas e construções algumas vezes são irregulares e sem qualquer planejamento, não havendo por vezes sequer um endereço formal (e.g.: número da casa e nome de rua).

Ainda na Figura 7-6, há uma carga extra não conhecida, sendo identificada através da simples comparação entre a potência total do circuito (medida pela UTR

da subestação) e o somatório das medições de Potências Ativas (P) provenientes dos medidores inteligentes instalados. Este tipo de medição de confronto entre clientes e UTRs é realizado atualmente por algumas concessionárias, mas só ajuda a identificar perdas em uma determinada região, muito tempo depois do início dos eventos e quando as perdas são significativamente altas. O SCMI poderia auxiliar nesta busca da fraude de maneira mais eficaz e refinada, pois recebe e processa os dados de medição de consumo histórico do cluster e de todos os medidores pertencentes a ele. A análise, realizada localmente, trabalha com valores de desvio de consumo por vezes sutis e a quantidade de elementos a serem testados é bem reduzida em relação ao que se apresenta nos ADMS. Estes sistemas de gerenciamento recebem informações de milhares/milhões de medidores todos os dias, inviabilizando computacionalmente análises pormenorizadas em cada um deles a fim de identificar perdas na rede de BT.

REFERÊNCIAS

ABB INC. **Silicon Valley Power: Multi-use network for power and water AMI + free Wi-Fi**. [S.l.]. 2012.

ABDEL-MAJEED, A.; BRAUN, M. **Low voltage system state estimation using smart meters**. 2012 47th International Universities Power Engineering Conference (UPEC). [S.l.]: IEEE. 2012. p. 1-6.

ABDULLA, G. **The deployment of advanced metering infrastructure**. 2015 First Workshop on Smart Grid and Renewable Energy (SGRE). [S.l.]: IEEE. 2015. p. 1-3.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES - ANATEL. Ferramenta de monitoramento da cobertura móvel celular, 2015. Disponivel em: <http://gatewaysiec.anatel.gov.br/mobileanatel>.

ALAM, M. T.; LI, H.; PATIDAR, A. **Bitcoin for smart trading in smart grid**. The 21st IEEE International Workshop on Local and Metropolitan Area Networks. [S.l.]: IEEE. 2015. p. 1-2.

ANATEL. TELEFONIA MÓVEL - ACESSOS. **ANATEL - Agência Nacional de Telecomunicações**, 2018. Disponivel em: <www.anatel.gov.br/dados/acessos-telefonia-movel>.

APARECIDO PELEGRINI, M.; VALE, Z. A. Redes Elétricas Inteligentes: Diálogo Setorial Brasil-União Europeia (2014). **Ministério do planejamento, Orçamento e Gestão**, Brasilia, 1, 2014. 204.

ARRIGONI, C. et al. **Smart Distribution Management System:** Evolution of MV grids supervision & control systems. 2016 AEIT International Annual Conference (AEIT). [S.l.]: IEEE. 2016. p. 1-6.

BACH, L. M.; MIHALJEVIC, B.; ZAGAR, M. **Comparative analysis of blockchain consensus algorithms**. 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). [S.l.]: IEEE. 2018. p. 1545-1550.

BAEK, J. et al. A Secure Cloud Computing Based Framework for Big Data Information Management of Smart Grid. **IEEE Transactions on Cloud Computing**, v. 3, n. 2, p. 233-244, 1 abr. 2015. ISSN 10.1109/TCC.2014.2359460.

BAIG, Z. A.; AL AMOUDY, A.; SALAH, K. **Detection of compromised smart meters in the Advanced Metering Infrastructure**. 2015 IEEE 8th GCC Conference & Exhibition. [S.l.]: IEEE. 2015. p. 1-6.

BEDFORD TAYLOR, M. The Evolution of Bitcoin Hardware. **Computer**, v. 50, n. 9, p. 58-66, 2017. ISSN 10.1109/MC.2017.3571056.

BERGER, L. T.; SCHWAGER, A.; ESCUDERO-GARZÁS, J. J. Power Line Communications for Smart Grid Applications. **Journal of Electrical and Computer Engineering**, v. 2013, p. 1-16, 2013. ISSN 10.1155/2013/712376.

BISWAS, K.; MUTHUKKUMARASAMY, V. **Securing Smart Cities Using Blockchain Technology**. 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS). [S.l.]: IEEE. 2016. p. 1392-1393.

BLUETOOTH SIG PROPRIETARY. **BLUETOOTH:** Master Table of Contents & Compliance Requirements. [S.l.]: [s.n.], v. 0, 2014.

BOJKOVIC, Z.; BAKMAZ, B. **Smart Grid Communications Architecture:** A Survey and Challenges. [S.l.]: [s.n.]. ISBN 9781618040848.

BREUER, H. A Microgrid Grows in Brooklyn. **Pictures of the Future: The Magazine for Research and Innovation**, New York, New York, USA, fev. 2018.

BRONZI, W. et al. **Bluetooth low energy for inter-vehicular communications**. 2014 IEEE Vehicular Networking Conference (VNC). [S.l.]: IEEE. 2014. p. 215-221.

BROWN DO COUTTO FILHO, M.; DE SOUZA, J. C. S. Forecasting-Aided State Estimation—Part I: Panorama. **IEEE Transactions on Power Systems**, v. 24, n. 4, p. 1667-1677, nov. 2009. ISSN 10.1109/TPWRS.2009.2030295.

BROWN DO COUTTO FILHO, M.; DE SOUZA, J. C. S.; FREUND, R. S. Forecasting-Aided State Estimation—Part II: Implementation. **IEEE Transactions on Power Systems**, v. 24, n. 4, p. 1678-1685, nov. 2009. ISSN 10.1109/TPWRS.2009.2030297.

CAMARINHA-MATOS, L. M. Collaborative smart grids – A survey on trends. **Renewable and Sustainable Energy Reviews**, v. 65, p. 283-294, nov. 2016. ISSN 10.2753/JEC1086-4415160403.

CHARLY, A.; REDDY, J.; ASHOK, S. **Development of inbuilt Energy Management Controller for Smart meter**. 2014 IEEE International Conference on

Advanced Communications, Control and Computing Technologies. [S.l.]: IEEE. 2014. p. 371-375.

CHERNYI, A. I. MOBILITY REPORT: ON THE PULSE OF THE NETWORKED SOCIETY. **Automatic Documentation and Mathematical Linguistics**, 2015. ISSN 10.3103/S0005105510050031.

CHRISTIDIS, K.; DEVETSIKIOTIS, M. Blockchains and Smart Contracts for the Internet of Things. **IEEE Access**, v. 4, p. 2292-2303, 2016. ISSN 10.1109/ACCESS.2016.2566339.

CLARIZIA, F. et al. **Smart meter systems for smart grid management**. 2016 IEEE International Instrumentation and Measurement Technology Conference Proceedings. [S.l.]: IEEE. 2016. p. 1-6.

COMA-PUIG, B. et al. **Fraud Detection in Energy Consumption:** A Supervised Approach. 2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA). [S.l.]: IEEE. 2016. p. 120-129.

COURTOIS, N. T.; GRAJEK, M.; NAIK, R. Optimizing SHA256 in Bitcoin Mining. In: COURTOIS, N. T.; GRAJEK, M.; NAIK, R. **Communications in Computer and Information Science**. [S.l.]: [s.n.], v. 448 CCIS, 2014. p. 131-144. ISBN 10.1007/978-3-662-44893-9_12.

CROSBY, M.; PATTANAYAK, P.; VERMA, S. **BlockChain Technology:** Beyond Bitcoin. Berlin, Boston: De Gruyter, 2016. ISBN 10.1515/9783110488951.

DE FARIA, R. A. et al. **Collusion and Fraud Detection on Electronic Energy Meters - A Use Case of Forensics Investigation Procedures**. 2014 IEEE Security and Privacy Workshops. [S.l.]: IEEE. 2014. p. 65-68.

DIMITRIOU, T.; KARAME, G. **Privacy-friendly tasking and trading of energy in smart grids**. Proceedings of the 28th Annual ACM Symposium on Applied Computing - SAC '13. New York, New York, USA: ACM Press. 2013. p. 652.

DORRI, A. et al. **Blockchain for IoT security and privacy:** The case study of a smart home. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). [S.l.]: IEEE. 2017. p. 618-623.

ECONOMIST, T. Blockchain: The next big thing. **The Economist**, jul. 2016.

ELGENEDY, M. A.; MASSOUD, A. M.; AHMED, S. **Smart grid self-healing:** Functions, applications, and developments. 2015 First Workshop on Smart Grid and Renewable Energy (SGRE). [S.l.]: IEEE. 2015. p. 1-6.

EL-SAYED, M.; GAGEN, P. **Mobile Data explosion and planning of heterogeneous networks**. 2012 15th International Telecommunications Network Strategy and Planning Symposium (NETWORKS). [S.l.]: IEEE. 2012. p. 1-6.

EVANS, D. **The Internet of Things:** How the Next Evolution of the Internet Is Changing Everything. [S.l.]: Cisco Internet Business Solutions Group (IBSG), v. 0, 2011.

EYAL, I.; SIRER, E. G. Majority is not enough. **Communications of the ACM**, v. 61, n. 7, p. 95-102, 25 jun. 2018. ISSN arXiv:1311.0243v5.

FAN, Z. et al. Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities. **IEEE Communications Surveys & Tutorials**, v. 15, n. 1, p. 21-38, 2013. ISSN 1112.3516v1.

FENG TIAN. **An agri-food supply chain traceability system for China based on RFID & blockchain technology**. 2016 13th International Conference on Service Systems and Service Management (ICSSSM). [S.l.]: IEEE. 2016. p. 1-6.

FERREIRA, L. R. et al. **Solução do problema de self-healing para redes de distribuição radiais através de otimização via algoritmo genético**. XI Simpósio Brasileiro de Automação Inteligente (SBAI). Fortaleza: [s.n.]. 2013.

FINSTER, S.; BAUMGART, I. **Elderberry:** A peer-to-peer, privacy-aware smart metering protocol. 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). [S.l.]: IEEE. 2013. p. 37-42.

GAI, K. et al. Privacy-Preserving Energy Trading Using Consortium Blockchain in Smart Grid. **IEEE Transactions on Industrial Informatics**, v. 15, n. 6, p. 3548-3558, jun. 2019. ISSN 10.1109/TII.2019.2893433.

GALLI, S.; SCAGLIONE, A. Power Line Communications and the Smart Grid, n. November, 2010. ISSN 10.1109/SMARTGRID.2010.5622060.

GANGALE, F.; MENGOLINI, A.; ONYEJI, I. Consumer engagement: An insight from smart grid projects in Europe. **Energy Policy**, v. 60, p. 621-628, set. 2013. ISSN 10.1016/j.enpol.2013.05.031.

GHATIKAR, G. INTERNET OF THINGS AND SMART GRID STANDARDIZATION. In: GHATIKAR, G. **Internet of Things and Data Analytics Handbook**. Hoboken, NJ, USA: John Wiley & Sons, Inc., 2016. p. 495-512. ISBN 10.1002/9781119173601.ch30.

GOHIL, A.; MODI, H.; PATEL, S. K. **5G technology of mobile communication:** A survey. 2013 International Conference on Intelligent Systems and Signal Processing (ISSP). [S.l.]: IEEE. 2013. p. 288-292.

GOMEZ-EXPOSITO, A. et al. A Multilevel State Estimation Paradigm for Smart Grids. **Proceedings of the IEEE**, v. 99, n. 6, p. 952-976, jun. 2011. ISSN 10.1109/JPROC.2011.2107490.

GRACKOVA, L.; OLEINIKOVA, I.; KLAVS, G. **Electric vehicles in the concept of smart cities**. 2015 IEEE 5th International Conference on Power Engineering, Energy and Electrical Drives (POWERENG). [S.l.]: IEEE. 2015. p. 543-547.

GUNGOR, V. C. et al. Smart Grid Technologies: Communication Technologies and Standards. **IEEE Transactions on Industrial Informatics**, v. 7, n. 4, p. 529-539, nov. 2011. ISSN 10.1109/TII.2011.2166794.

GUPTA, R.; GUPTA, R. **ABC of Internet of Things:** Advancements, benefits, challenges, enablers and facilities of IoT. 2016 Symposium on Colossal Data Analysis and Networking (CDAN). [S.l.]: IEEE. 2016. p. 1-5.

HAIDER, H. T.; SEE, O. H.; ELMENREICH, W. A review of residential demand response of smart grid. **Renewable and Sustainable Energy Reviews**, v. 59, p. 166-178, jun. 2016. ISSN 10.1016/j.rser.2016.01.016.

HOU, D. **High-Impedance Fault Detection — Field Tests and Dependability Analysis**. 36th Annual Western Protective Relay Conference. Spokane: 36th Annual Western Protective Relay Conference. 2009. p. 1-10.

IBGE - INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **Domicílios particulares permanentes, por existência de energia elétrica, segundo as Grandes Regiões e as Unidades da Federação**. [S.l.]. 2010.

INTANAGONWIWAT, C.; GOVINDAN, R.; ESTRIN, D. **Direct diffusion:** a scalable and robust communication paradigm for sensor networks. Proceedings of the 6th annual international conference on Mobile computing and networking - MobiCom '00. New York, New York, USA: ACM Press. 2000. p. 56-67.

INTANAGONWIWAT, C.; GOVINDAN, R.; ESTRIN, D. **Directed diffusion**. Proceedings of the 6th annual international conference on Mobile computing and networking - MobiCom '00. New York, New York, USA: ACM Press. 2000. p. 56-67.

IRIA, J. P.; SOARES, F. J.; MATOS, M. A. **Trading small prosumers flexibility in the day-ahead energy market**. 2017 IEEE Power & Energy Society General Meeting. [S.l.]: IEEE. 2017. p. 1-5.

JARDINI, J. A. et al. **Daily Load Profiles for Residential, Commercial and Industrial Low Voltage Consumers**. [S.l.], p. 375-380. 2000. (10.1109/61.847276).

JAYACHANDRAN, P. The difference between public and private blockchain. **Blockchain Pulse:** IBM Blockchain Blog, 2017. Disponivel em: <https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/>.

JIXUAN ZHENG; GAO, D. W.; LI LIN. **Smart Meters in Smart Grid:** An Overview. 2013 IEEE Green Technologies Conference (GreenTech). [S.l.]: IEEE. 2013. p. 57-64.

KAWADY, T. A.; TAALAB, A. E.-M. I.; ELGEZIRY, M. Z. **Experimental investigation of high impedance faults in low voltage distribution networks**. 2009 IEEE Power & Energy Society General Meeting. [S.l.]: IEEE. 2009. p. 1-6.

KELLY, J. Smart Grid Network to use LTE. **Ericsson AB**, Stockholm, 2011. 48-213.

KIM, G.; PARK, J.; RYOU, J. **A Study on Utilization of Blockchain for Electricity Trading in Microgrid**. 2018 IEEE International Conference on Big Data and Smart Computing (BigComp). [S.l.]: IEEE. 2018. p. 743-746.

KIM, S. et al. **Flush:** a reliable bulk transport protocol for multihop wireless networks. Proceedings of the 5th international conference on Embedded networked sensor systems - SenSys '07. New York, New York, USA: ACM Press. 2007. p. 351.

KRZYSZTOF BILLEWICZ. Smart Meters and Under-Frequency Load Shedding. **Journal of Energy and Power Engineering**, v. 9, n. 10, p. 905-911, 28 out. 2015. ISSN 10.17265/1934-8975/2015.10.009.

LEIDING, B.; MEMARMOSHREFI, P.; HOGREFE, D. **Self-managed and blockchain-based vehicular ad-hoc networks**. Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing Adjunct - UbiComp '16. New York, New York, USA: ACM Press. 2016. p. 137-140.

LIGHT. ESPECIFICAÇÃO PARA PROJETO E CONSTRUÇÃO DE DISTRIBUIÇÃO SUBTERRÂNEA, 2018.

LIN, C. M.; CHEN, M. T. **Design and implementation of a smart home energy saving system with active loading feature identification and power management**. 2017 IEEE 3rd International Future Energy Electronics Conference and ECCE Asia (IFEEC 2017 - ECCE Asia). [S.l.]: IEEE. 2017. p. 739-742.

M. ANNASWAMY, A.; AMIN, M. IEEE Vision for Smart Grid Controls: 2030 and Beyond. **IEEE Vision for Smart Grid Controls: 2030 and Beyond**, p. 1-168, 2013. ISSN 10.1109/IEEESTD.2013.6577608.

MACKENSEN, E.; LAI, M.; WENDT, T. M. **Bluetooth Low Energy (BLE) based wireless sensors**. 2012 IEEE Sensors. [S.l.]: IEEE. 2012. p. 1-4.

MALANDRA, F.; SANSO, B. **Performance analysis of large scale RF-mesh networks for smart cities and IoT**. 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm). [S.l.]: IEEE. 2017. p. 13-18.

MANTUANO FILHO, S. et al. **Sistemas De Medição Fasorial Princípios E Aplicações**. VIII Seminário Técnico de Proteção e Controle. Rio de Janeiro: [s.n.]. 2005.

MARINAKIS, Y. D.; WALSH, S. T.; HARMS, R. **Internet of Things Technology Diffusion Forecasts**. 2017 Portland International Conference on Management of Engineering and Technology (PICMET). [S.l.]: IEEE. 2017. p. 1-5.

MAYER-SCHÖNBERGER, V.; CUKIER, K. Big Data: A Revolution That Will Transform How We Live, Work, and Think. **American Journal of Epidemiology**, v. 179, n. 9, p. 1143-1144, 1 maio 2014. ISSN 10.1093/aje/kwu085.

MENGELKAMP, E. et al. A blockchain-based smart grid: towards sustainable local energy markets. **Computer Science - Research and Development**, v. 33, n. 1-2, p. 207-214, 22 fev. 2018. ISSN 10.1007/s00450-017-0360-9.

MONEDERO, I. et al. Detection of frauds and other non-technical losses in a power utility using Pearson coefficient, Bayesian networks and decision trees. **International Journal of Electrical Power & Energy Systems**, v. 34, n. 1, p. 90-98, jan. 2012. ISSN 10.1016/j.ijepes.2011.09.009.

MULLER, J. et al. **African Utility Market Intelligence Report:** Conference and Industry Insights. Cape Town: African Utility Week. 2015.

NAZEH, M. et al. A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention. **J Comp Sci Appl Inform Technol.**, p. 1-7, 2018.

PAU, M. et al. **Low voltage system state estimation based on smart metering infrastructure**. 2016 IEEE International Workshop on Applied Measurements for Power Systems (AMPS). [S.l.]: IEEE. 2016. p. 1-6.

PECK, M. E. Blockchains: How they work and why they'll change the world. **IEEE Spectrum**, v. 54, n. 10, p. 26-35, out. 2017. ISSN 10.1109/MSPEC.2017.8048836.

PEREIRA, P. P. et al. **Enabling Cloud Connectivity for Mobile Internet of Things Applications**. 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering. [S.l.]: IEEE. 2013. p. 518-526.

POP, C. et al. Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids. **Sensors**, v. 18, n. 2, p. 162, 9 jan. 2018. ISSN 10.3390/s18010162.

RAYCHAUDHURI, D.; MANDAYAM, N. B. Frontiers of Wireless and Mobile Communications. **Proceedings of the IEEE**, v. 100, n. 4, p. 824-840, abr. 2012. ISSN arXiv:1011.1669v3.

RAZA, S. et al. **Bluetooth smart:** An enabling technology for the Internet of Things. 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). [S.l.]: IEEE. 2015. p. 155-162.

ROMERO, D.; MOLINA, A. Collaborative networked organisations and customer communities: value co-creation and co-innovation in the networking era. **Production Planning & Control**, v. 22, n. 5-6, p. 447-472, 31 jul. 2011. ISSN 10.1080/09537287.2010.536619.

ROTONDO, R. **Mesh networks: Delivering IP-Based seamless Mobility in Municipal and Ad Hoc Wireless Networks**. Motorola’s Mesh networks product Group. [S.l.]. 2006.

RUSCHEL, C. S. et al. **Recursos Energéticos Distribuídos: Impactos no Planejamento Energético**. EPE - Empresa de Pesquisa Energética. Rio de Janeiro, p. 1-11. 2018.

RUTKIN, A. Blockchain-based microgrid gives power to consumers in New York. **DAILY NEWS**, 2 mar. 2016.

SCHWARTZ, D.; YOUNGS, N.; BRITTO, A. **The Ripple Protocol Consensus Algorithm**. Ripple Labs, Inc. San Francisco, CA, USA. 2014. (1802.07242).

SHERRINGTON, S.; DICKS, D. Smart Grid Technology Investment : Forecasts for 2010-2030, n. February, p. 6, 2011. ISSN 9780956280367.

SIKORSKI, J. J.; HAUGHTON, J.; KRAFT, M. Blockchain technology in the chemical industry: Machine-to-machine electricity market. **Applied Energy**, v. 195, p. 234-246, jun. 2017. ISSN 10.1016/j.apenergy.2017.03.039.

SMERTNIK, H. Mobile For Development Utilities: Mobile for smart energy solutions Senegal. **GSMA**, n. November, 2014.

SOHEILI, A. et al. **A new high impedance fault detection scheme:** Fourier based approach. 2016 IEEE International Conference on Power System Technology (POWERCON). [S.l.]: IEEE. 2016. p. 1-6.

SORIN, E.; BOBO, L.; PINSON, P. Consensus-Based Approach to Peer-to-Peer Electricity Markets With Product Differentiation. **IEEE Transactions on Power Systems**, v. 34, n. 2, p. 994-1004, mar. 2019. ISSN 10.1109/TPWRS.2018.2872880.

SZABO, N. Formalizing and Securing Relationships on Public Networks. **First Monday**, v. 2, n. 9, p. 9-13, 1 set. 1997. ISSN 10.5210/fm.v2i9.548.

TENGDIN, J. Detection of Downed Conductors on utility distribution System. **IEEE PES Tutorial course 90EH0310--3-PWR**, 1989.

THOLOMIER, D.; KANG, H.; CVOROVIC, B. **Phasor measurement units:** Functionality and applications. 2009 IEEE Power Systems Conference. [S.l.]: IEEE. 2009. p. 1-12.

TIAN, F. An agri-food supply chain traceability system for China based on RFID & blockchain technology. **2016 13th International Conference on Service Systems and Service Management (ICSSSM)**, p. 1-6, 2016. ISSN 10.1109/ICSSSM.2016.7538424.

TREFKE, J. et al. **Smart Grid Architecture Model use case management in a large European Smart Grid project**. IEEE PES ISGT Europe 2013. [S.l.]: IEEE. 2013. p. 1-5.

WAERESCH, D. et al. **State estimation in lowvoltage grids based on smart meter data and photovoltaic-feed-in-forecast**. 23rd International Conference on Electricity Distribution. Lyon: [s.n.]. 2015. p. 15-18.

WANG, W.; XU, Y.; KHANNA, M. A survey on the communication architectures in smart grid. **Computer Networks**, v. 55, n. 15, p. 3604-3629, out. 2011. ISSN 10.1016/j.comnet.2011.07.010.

XU, Y. et al. A Blockchain-Based Nonrepudiation Network Computing Service Scheme for Industrial IoT. **IEEE Transactions on Industrial Informatics**, v. 15, n. 6, p. 3632-3641, jun. 2019. ISSN 10.1109/TII.2019.2897133.

YAN, Y. et al. A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges. **IEEE Communications Surveys & Tutorials**, v. 15, n. 1, p. 5-20, 2013. ISSN 10.1109/SURV.2012.021312.00034.

ZAMANAN, N.; SYKULSKI, J. **The evolution of high impedance fault modeling**. 2014 16th International Conference on Harmonics and Quality of Power (ICHQP). [S.l.]: IEEE. 2014. p. 77-81.

ZANGHI, E.; BROWN DO COUTTO FILHO, M.; DE SOUZA, J. C. S. **TRATAMENTO TRIFÁSICO DA ESTIMAÇÃO DE ESTADO EM SUBESTAÇÕES**. IX Simpase - Simpósio de Automação e Sistemas Elétricos. Curitiba: [s.n.]. 2011. p. 8.

ZHENG, Z. et al. **An Overview of Blockchain Technology:** Architecture, Consensus, and Future Trends. 2017 IEEE International Congress on Big Data (BigData Congress). [S.l.]: IEEE. 2017. p. 557-564.

APÊNDICE A – DADOS DAS SIMULAÇÕES

A.1 CURVAS DE CARGA TÍPICAS

Tabela A-1: Valores da curva de carga (Watts) residencial.

Hour	P	QL	QC
00:00	200	0	0
00:15	190	0	0
00:30	170	0	0
00:45	150	0	0
01:00	150	0	0
01:15	140	0	0
01:30	130	0	0
01:45	120	0	0
02:00	110	0	0
02:15	112	0	0
02:30	110	0	0
02:45	112	0	0
03:00	110	0	0
03:15	112	0	0
03:30	110	0	0
03:45	112	0	0
04:00	110	0	0
04:00	112	0	0
04:15	110	0	0
04:30	112	0	0
05:45	110	0	0
05:00	115	0	0
05:15	113	0	0
05:30	118	0	0
06:45	120	0	0
06:00	150	0	0
06:15	180	0	0

Hour	P	QL	QC
06:45	200	0	0
07:00	220	0	0
07:15	220	0	0
07:45	225	0	0
07:00	230	0	0
08:15	234	0	0
08:30	238	0	0
08:45	230	0	0
09:00	220	0	0
09:15	224	0	0
09:30	225	0	0
09:45	220	0	0
09:00	228	0	0
10:15	230	0	0
10:30	234	0	0
10:45	237	0	0
10:00	229	0	0
11:15	250	0	0
11:30	240	0	0
11:30	245	0	0
11:45	240	0	0
12:00	244	0	0
12:15	248	0	0
12:30	245	0	0
12:45	250	0	0
13:00	253	0	0
13:15	257	0	0

Hour	P	QL	QC
13:30	250	0	0
13:45	255	0	0
14:45	230	0	0
14:00	257	0	0
14:30	250	0	0
14:00	255	0	0
15:15	253	0	0
15:30	258	0	0
15:45	256	0	0
15:00	261	0	0
16:15	259	0	0
16:30	264	0	0
16:45	262	0	0
16:00	267	0	0
17:15	280	0	0
17:30	278	0	0
17:45	300	0	0
17:00	330	0	0
18:15	350	0	0
18:30	400	0	0
18:45	440	0	0
18:00	520	0	0
19:15	523	0	0
19:30	521	0	0
19:45	514	0	0
19:00	515	0	0
20:15	500	0	0
20:30	505	0	0
20:45	500	0	0
20:00	490	0	0
21:15	483	0	0
21:30	478	0	0

Hour	P	QL	QC
21:45	450	0	0
21:00	430	0	0
22:15	398	0	0
22:30	390	0	0
22:45	370	0	0
22:00	360	0	0
23:15	290	0	0
23:30	260	0	0
23:45	220	0	0

Tabela A-2: Valores da curva de carga (Watts) comercial.

Hour	P	QL	QC
00:00	20000	4061	0
00:15	19000	3858	0
00:30	20500	4163	0
00:45	19500	3960	0
01:00	20500	4163	0
01:15	19500	3960	0
01:30	20500	4163	0
01:45	19500	3960	0
02:00	20000	4061	0
02:15	20500	4163	0
02:30	20600	4183	0
02:45	20000	4061	0
03:00	20000	4061	0
03:15	20500	4163	0
03:30	20600	4183	0
03:45	20000	4061	0
04:00	20500	4163	0
04:00	20600	4183	0
04:15	20800	4224	0
04:30	21000	4264	0
05:45	21500	4366	0
05:00	22000	4467	0
05:15	23000	4670	0
05:30	24000	4873	0
06:45	25000	5076	0
06:00	30000	6092	0
06:15	34000	6904	0
06:45	38000	7716	0
07:00	40000	8122	0
07:15	44000	8935	0

Hour	P	QL	QC
07:45	46000	9341	0
07:00	48000	9747	0
08:15	50000	10153	0
08:30	52000	10559	0
08:45	56000	11371	0
08:00	58000	11777	0
09:15	60000	12184	0
09:30	62600	12711	0
09:45	63000	12793	0
09:00	62600	12711	0
10:15	63000	12793	0
10:30	62000	12590	0
10:45	62600	12711	0
10:00	63000	12793	0
11:15	62600	12711	0
11:30	64000	12996	0
11:30	66000	13402	0
11:45	68000	13808	0
12:00	70000	14214	0
12:15	70500	14316	0
12:30	71000	14417	0
12:45	70800	14377	0
13:00	70500	14316	0
13:15	71000	14417	0
13:30	70800	14377	0
13:45	70500	14316	0
14:45	70000	14214	0
14:00	70500	14316	0
14:30	71000	14417	0
14:00	70800	14377	0

Hour	P	QL	QC
15:15	70500	14316	0
15:30	71000	14417	0
15:45	70800	14377	0
15:00	70500	14316	0
16:15	70000	14214	0
16:30	70500	14316	0
16:45	71000	14417	0
16:00	70800	14377	0
17:15	70500	14316	0
17:30	71000	14417	0
17:45	70800	14377	0
17:00	70500	14316	0
18:15	70000	14214	0
18:30	70500	14316	0
18:45	71000	14417	0
18:00	70800	14377	0
19:15	71000	14417	0
19:30	71000	14417	0
19:45	70800	14377	0
19:00	70500	14316	0
20:15	60000	12184	0
20:30	59000	11980	0
20:45	58000	11777	0
20:00	56000	11371	0
21:15	50000	10153	0
21:30	49500	10051	0
21:45	47000	9544	0
21:00	45000	9138	0
22:15	43000	8732	0
22:30	42000	8528	0
22:45	39000	7919	0
22:00	36000	7310	0

Hour	P	QL	QC
23:15	30000	6092	0
23:30	28000	5686	0
23:45	27500	5584	0

A.2 DADOS DE CONFIGURAÇÃO DA GUI

Tabela A-3: Dados dos ramos da subestação secundária

Number	Type	Name	FromNode	ToNode
1	1	SUBSTATION	1	2
2	3	FEEDER1	2	3
3	3	FEEDER2	2	4

Tabela A-4: Dados dos equipamentos de corte por alimentador

Name	BranchNumber
DJ1	1
DJ2	2
DJ3	3

Tabela A-5: Exemplo de Configuração dos SGEs

Feeder	ClusterID	Name	Type	Branch Number	AutoClient	Utility ID
1	1	SGE1	2	2	1	1
1	1	SGE2	2	2	1	1
2	2	SGE3	2	2	1	2
2	2	SGE4	2	2	1	3

APÊNDICE B – ESTRUTURA DE PASTAS DO PROJETO

Todos os arquivos do projeto dos módulos do simulador do SCMI se encontram na seguinte estrutura de pastas da Tabela B.1:

Tabela B-1: Estrutura de Pastas e Arquivos

Pastas	Arquivos	Descrição
SCMI BlockchainMain\	Power_Models_revXX.mdl	Biblioteca de objetos.
	Modelo_SCMI_TESE_revXX.mdl	Modelo da subestação.
SCMI BlockchainMain \ CfgFiles	BranchMatrix.csv	Arquivos de Configuração.
	EquipMatrix.csv	
	MinerList.csv	
	NodeMatrix.csv	
	SGEMatrix.csv	
	SGEOwners.csv	
	SICMatrix.csv	
SCMI BlockchainMain \ DataFiles	LoadProfile'N'.csv	Arquivos de tipos de perfil de carga.
SCMI BlockchainMain \ Functions	Lock_Model.m	Código do Módulo de Rede de BT.
	LogFilefcn.m	
	ParentBlockName.m	
	ProcessMeasData.m	
	SS_Main.m	
	SS_Processing.m	
	SS_PowerCalculation.m	
	SGE_SystemInitialization.m	Código do Módulo Criador de Blocos de dados.
	SGE_Processing.m	
	SGE_PowerCalculation.m	
	Block.m	
	Miners_SystemInitialization.m	Código do Módulo de Mineração e Relatórios.
	Miners_Processing.m	
	Mining_Miners.m	

Pastas	Arquivos	Descrição
	VC_”N”.m	
SCMI BlockchainMain \ Log	DD-mmm-AAA - LogFile.txt	Arquivo de "Log" do dia.
SCMI BlockchainMain \ Screens	CommandScreen (xx.fig e xx.m)	Arquivos das Telas Pop-Up de comando de equipamento, Medidores e log de Alarmes.
	LogScreen (xx.fig e xx.m)	
	MetterScreen (xx.fig e xx.m)	

APÊNDICE C – DADOS DOS TESTES DE AVALANCHE

Os valores apresentados na Tabela C-1 são referentes aos resultados parciais aferidos nos testes de avalanche que contemplaram cenários com variação do número de mineradores e de blocos de dados. Os valores foram utilizados na composição dos gráficos ilustrados na Seção 6.3.

Tabela C-1: Relatório parcial de testes de avalanche

Time Stamp	Num Of Miners	iMiner	Num Blocks	Num Pendings	Num Meas	Meas MinCT	Meas MaxCT	Meas AvgCT
18:24:30.018	3	1	100	100	300	0,017102	0,02171	0,017732
18:24:30.028	3	2	100	100	300	0,017465	0,019526	0,018164
18:24:30.050	3	3	100	100	300	0,017351	0,018971	0,017805
18:24:35.265	3	1	100	100	600	0,014668	0,017649	0,015734
18:24:35.275	3	2	100	100	600	0,014984	0,019721	0,016153
18:24:35.295	3	3	100	100	600	0,014555	0,017266	0,015408
18:24:40.285	3	1	100	100	900	0,014258	0,017145	0,014666
18:24:40.295	3	2	100	100	900	0,01442	0,017734	0,015503
18:24:40.315	3	3	100	100	900	0,014392	0,01617	0,014842
18:25:46.260	3	1	1000	1000	3900	0,018552	0,032332	0,020119
18:25:46.270	3	2	1000	1000	3900	0,0189	0,037565	0,020103
18:25:46.290	3	3	1000	1000	3900	0,019193	0,034791	0,021015
18:26:44.287	3	1	1000	1000	6900	0,016112	0,031022	0,017503
18:26:44.307	3	2	1000	1000	6900	0,016439	0,032804	0,017797
18:26:44.317	3	3	1000	1000	6900	0,01672	0,033633	0,017965
18:27:42.099	3	1	1000	1000	9900	0,016173	0,021422	0,016923
18:27:42.119	3	2	1000	1000	9900	0,016624	0,023116	0,017875
18:27:42.139	3	3	1000	1000	9900	0,016815	0,031147	0,018313
18:36:02.672	3	1	5000	5000	24900	0,027189	0,051254	0,032366
18:36:02.692	3	2	5000	5000	24900	0,026059	0,067592	0,031314
18:36:02.702	3	3	5000	5000	24900	0,02752	0,04686	0,031384
18:43:39.228	3	1	5000	5000	39900	0,02641	0,043351	0,028881
18:43:39.248	3	2	5000	5000	39900	0,02633	0,043115	0,028847
18:43:39.278	3	3	5000	5000	39900	0,026439	0,045468	0,028655
18:51:09.285	3	1	5000	5000	54900	0,026551	0,041111	0,028506
18:51:09.305	3	2	5000	5000	54900	0,026077	0,042024	0,028
18:51:09.315	3	3	5000	5000	54900	0,026693	0,041341	0,028531
19:15:29.003	3	1	10000	10000	84900	0,037146	0,079609	0,047486
19:15:29.023	3	2	10000	10000	84900	0,036815	0,09123	0,046274
19:15:29.043	3	3	10000	10000	84900	0,038687	0,072829	0,046923
19:37:21.283	3	1	10000	10000	114900	0,037125	0,054539	0,039765
19:37:21.303	3	2	10000	10000	114900	0,040167	0,058201	0,042661
19:37:21.323	3	3	10000	10000	114900	0,040502	0,096014	0,043698

Time Stamp	Num Of Miners	iMiner	Num Blocks	Num Pendings	Num Meas	Meas MinCT	Meas MaxCT	Meas AvgCT
19:59:43.546	3	1	10000	10000	144900	0,038568	0,072859	0,041358
19:59:43.566	3	2	10000	10000	144900	0,040536	0,071236	0,042874
19:59:43.586	3	3	10000	10000	144900	0,041906	0,055547	0,044881
19:59:59.085	5	1	100	100	145400	0,027906	0,033354	0,02899
19:59:59.095	5	2	100	100	145400	0,028471	0,033027	0,029331
19:59:59.115	5	3	100	100	145400	0,028123	0,030957	0,028929
19:59:59.125	5	4	100	100	500	0,028225	0,030264	0,028827
19:59:59.145	5	5	100	100	500	0,028039	0,030794	0,028706
20:00:13.956	5	1	100	100	145900	0,03052	0,034246	0,031083
20:00:13.966	5	2	100	100	145900	0,026427	0,033062	0,028882
20:00:13.986	5	3	100	100	145900	0,025195	0,029547	0,02606
20:00:13.996	5	4	100	100	1000	0,024888	0,028179	0,025759
20:00:14.016	5	5	100	100	1000	0,026847	0,029274	0,027595
20:00:27.919	5	1	100	100	146400	0,025182	0,027827	0,025752
20:00:27.939	5	2	100	100	146400	0,025205	0,028604	0,026125
20:00:27.949	5	3	100	100	146400	0,025318	0,027418	0,025883
20:00:27.969	5	4	100	100	1500	0,025357	0,03074	0,026726
20:00:27.989	5	5	100	100	1500	0,025233	0,028508	0,025984
20:03:32.962	5	1	1000	1000	151400	0,031631	0,037187	0,032913
20:03:32.972	5	2	1000	1000	151400	0,033628	0,039282	0,035072
20:03:32.992	5	3	1000	1000	151400	0,034877	0,044236	0,036131
20:03:33.002	5	4	1000	1000	6500	0,034608	0,04678	0,036381
20:03:33.022	5	5	1000	1000	6500	0,03427	0,057291	0,035848
20:06:23.536	5	1	1000	1000	156400	0,030242	0,036854	0,031265
20:06:23.566	5	2	1000	1000	156400	0,031429	0,038384	0,032286
20:06:23.576	5	3	1000	1000	156400	0,031672	0,039951	0,032619
20:06:23.596	5	4	1000	1000	11500	0,032002	0,039605	0,032995
20:06:23.626	5	5	1000	1000	11500	0,031684	0,039089	0,03269
20:09:13.879	5	1	1000	1000	161400	0,030136	0,035527	0,031093
20:09:13.899	5	2	1000	1000	161400	0,031331	0,042186	0,032184
20:09:13.909	5	3	1000	1000	161400	0,031782	0,037841	0,032764
20:09:13.929	5	4	1000	1000	16500	0,031687	0,041189	0,032626
20:09:13.959	5	5	1000	1000	16500	0,032055	0,038376	0,032929
20:32:18.352	5	1	5000	5000	186400	0,050166	0,070463	0,054401
20:32:18.362	5	2	5000	5000	186400	0,048978	0,068239	0,052647
20:32:18.382	5	3	5000	5000	186400	0,048434	0,064664	0,052594
20:32:18.402	5	4	5000	5000	41500	0,04838	0,062581	0,052247
20:32:18.432	5	5	5000	5000	41500	0,051142	0,072782	0,055589
20:54:17.151	5	1	5000	5000	211400	0,049485	0,060721	0,051106
20:54:17.171	5	2	5000	5000	211400	0,048364	0,070909	0,049992
20:54:17.191	5	3	5000	5000	211400	0,048012	0,086045	0,04968
20:54:17.201	5	4	5000	5000	66500	0,049499	0,07337	0,051226

Time Stamp	Num Of Miners	iMiner	Num Blocks	Num Pendings	Num Meas	Meas MinCT	Meas MaxCT	Meas AvgCT
20:54:17.238	5	5	5000	5000	66500	0,050259	0,065767	0,052299
21:16:30.603	5	1	5000	5000	236400	0,050724	0,072241	0,052887
21:16:30.623	5	2	5000	5000	236400	0,04909	0,065364	0,050962
21:16:30.643	5	3	5000	5000	236400	0,048313	0,071221	0,049925
21:16:30.653	5	4	5000	5000	91500	0,048916	0,060717	0,050726
21:16:30.693	5	5	5000	5000	91500	0,051303	0,071396	0,052751
22:25:33.553	5	1	10000	10000	286400	0,07178	0,1204	0,082258
22:25:33.573	5	2	10000	10000	286400	0,071461	0,10504	0,080035
22:25:33.593	5	3	10000	10000	286400	0,068309	0,098278	0,077612
22:25:33.613	5	4	10000	10000	141500	0,066923	0,10419	0,076393
22:25:33.643	5	5	10000	10000	141500	0,07829	0,12015	0,087577
23:31:55.718	5	1	10000	10000	336400	0,073228	0,13256	0,078213
23:31:55.728	5	2	10000	10000	336400	0,070654	0,10611	0,074683
23:31:55.748	5	3	10000	10000	336400	0,068993	0,097911	0,073444
23:31:55.768	5	4	10000	10000	191500	0,073818	0,10423	0,077704
23:31:55.798	5	5	10000	10000	191500	0,080285	0,11231	0,083781
00:39:13.198	5	1	10000	10000	386400	0,074524	0,10039	0,079261
00:39:13.218	5	2	10000	10000	386400	0,071612	0,10976	0,075949
00:39:13.238	5	3	10000	10000	386400	0,069534	0,092908	0,074325
00:39:13.258	5	4	10000	10000	241500	0,073695	0,090371	0,077999
00:39:13.278	5	5	10000	10000	241500	0,082459	0,1172	0,085786
00:39:44.176	7	1	100	100	387100	0,038859	0,043238	0,040384
00:39:44.196	7	2	100	100	387100	0,039655	0,043266	0,04109
00:39:44.216	7	3	100	100	387100	0,040397	0,045753	0,041896
00:39:44.236	7	4	100	100	242200	0,040193	0,044293	0,041742
00:39:44.256	7	5	100	100	242200	0,040576	0,046545	0,042262
00:39:44.266	7	6	100	100	700	0,040857	0,044131	0,042246
00:39:44.286	7	7	100	100	700	0,041426	0,048973	0,043214
00:40:13.310	7	1	100	100	387800	0,037803	0,040849	0,038926
00:40:13.330	7	2	100	100	387800	0,037908	0,044965	0,039827
00:40:13.340	7	3	100	100	387800	0,038111	0,041938	0,039262
00:40:13.360	7	4	100	100	242900	0,038659	0,043165	0,039787
00:40:13.380	7	5	100	100	242900	0,038145	0,04199	0,039327
00:40:13.390	7	6	100	100	1400	0,03866	0,04276	0,039905
00:40:13.410	7	7	100	100	1400	0,038592	0,041694	0,039736
00:40:42.487	7	1	100	100	388500	0,037786	0,041421	0,038919
00:40:42.503	7	2	100	100	388500	0,038073	0,046269	0,039912
00:40:42.513	7	3	100	100	388500	0,038347	0,041403	0,039452
00:40:42.533	7	4	100	100	243600	0,038493	0,042372	0,039481
00:40:42.543	7	5	100	100	243600	0,038164	0,04701	0,040139
00:40:42.563	7	6	100	100	2100	0,038089	0,041824	0,039348
00:40:42.573	7	7	100	100	2100	0,038571	0,044003	0,039985

Time Stamp	Num Of Miners	iMiner	Num Blocks	Num Pendings	Num Meas	Meas MinCT	Meas MaxCT	Meas AvgCT
00:47:03.566	7	1	1000	1000	395500	0,047	0,059753	0,050167
00:47:03.596	7	2	1000	1000	395500	0,04863	0,057466	0,050783
00:47:03.616	7	3	1000	1000	395500	0,050154	0,059597	0,052383
00:47:03.626	7	4	1000	1000	250600	0,050161	0,058256	0,052517
00:47:03.656	7	5	1000	1000	250600	0,051295	0,058772	0,053343
00:47:03.676	7	6	1000	1000	9100	0,050991	0,059081	0,053124
00:47:03.696	7	7	1000	1000	9100	0,053158	0,059803	0,054959
00:53:12.491	7	1	1000	1000	402500	0,049808	0,05821	0,051864
00:53:12.509	7	2	1000	1000	402500	0,049081	0,056827	0,050761
00:53:12.525	7	3	1000	1000	402500	0,048129	0,056125	0,049799
00:53:12.545	7	4	1000	1000	257600	0,04933	0,058732	0,051476
00:53:12.565	7	5	1000	1000	257600	0,047836	0,057821	0,049453
00:53:12.595	7	6	1000	1000	16100	0,047875	0,055665	0,049568
00:53:12.605	7	7	1000	1000	16100	0,049734	0,060248	0,05205
00:59:23.013	7	1	1000	1000	409500	0,049342	0,059327	0,050916
00:59:23.033	7	2	1000	1000	409500	0,048688	0,057066	0,050769
00:59:23.053	7	3	1000	1000	409500	0,049016	0,058019	0,050886
00:59:23.063	7	4	1000	1000	264600	0,048827	0,058947	0,050663
00:59:23.093	7	5	1000	1000	264600	0,048816	0,057093	0,050699
00:59:23.123	7	6	1000	1000	23100	0,049161	0,056863	0,050917
00:59:23.143	7	7	1000	1000	23100	0,049771	0,057924	0,051754
01:47:45.366	7	1	5000	5000	444500	0,075289	0,097579	0,080701
01:47:45.384	7	2	5000	5000	444500	0,074173	0,093577	0,079881
01:47:45.402	7	3	5000	5000	444500	0,073451	0,092945	0,078355
01:47:45.418	7	4	5000	5000	299600	0,074429	0,095574	0,080173
01:47:45.449	7	5	5000	5000	299600	0,073858	0,12044	0,079377
01:47:45.476	7	6	5000	5000	58100	0,073745	0,094603	0,078697
01:47:45.494	7	7	5000	5000	58100	0,082555	0,10064	0,088019
02:35:17.304	7	1	5000	5000	479500	0,076973	0,092143	0,079969
02:35:17.314	7	2	5000	5000	479500	0,075181	0,092203	0,078082
02:35:17.334	7	3	5000	5000	479500	0,073867	0,086258	0,076287
02:35:17.354	7	4	5000	5000	334600	0,074263	0,087354	0,077008
02:35:17.364	7	5	5000	5000	334600	0,075055	0,09221	0,077987
02:35:17.384	7	6	5000	5000	93100	0,07757	0,092385	0,08038
02:35:17.404	7	7	5000	5000	93100	0,081947	0,11442	0,085288
03:22:43.912	7	1	5000	5000	514500	0,078392	0,095932	0,081599
03:22:43.932	7	2	5000	5000	514500	0,0765	0,091931	0,07924
03:22:43.952	7	3	5000	5000	514500	0,074673	0,087953	0,077095
03:22:43.962	7	4	5000	5000	369600	0,073958	0,091844	0,076654
03:22:43.992	7	5	5000	5000	369600	0,074574	0,092033	0,077195
03:22:44.012	7	6	5000	5000	128100	0,075907	0,096737	0,078821
03:22:44.032	7	7	5000	5000	128100	0,080545	0,097432	0,083386

Time Stamp	Num Of Miners	iMiner	Num Blocks	Num Pendings	Num Meas	Meas MinCT	Meas MaxCT	Meas AvgCT
05:48:10.260	7	1	10000	10000	584500	0,1078	0,19691	0,12166
05:48:10.270	7	2	10000	10000	584500	0,11088	0,14568	0,12216
05:48:10.290	7	3	10000	10000	584500	0,10768	0,1516	0,11984
05:48:10.310	7	4	10000	10000	439600	0,10789	0,1537	0,11948
05:48:10.340	7	5	10000	10000	439600	0,10675	0,1496	0,11779
05:48:10.370	7	6	10000	10000	198100	0,10456	0,14463	0,11542
05:48:10.380	7	7	10000	10000	198100	0,12705	0,17463	0,13893
08:10:46.961	7	1	10000	10000	654500	0,11095	0,13562	0,11753
08:10:46.991	7	2	10000	10000	654500	0,10743	0,15541	0,11389
08:10:47.001	7	3	10000	10000	654500	0,10728	0,13683	0,11347
08:10:47.022	7	4	10000	10000	509600	0,10995	0,13357	0,11604
08:10:47.062	7	5	10000	10000	509600	0,11044	0,13624	0,11636
08:10:47.072	7	6	10000	10000	268100	0,11722	0,16828	0,12297
08:10:47.092	7	7	10000	10000	268100	0,13295	0,15462	0,13807
10:36:22.584	7	1	10000	10000	724500	0,11446	0,16289	0,12077
10:36:22.602	7	2	10000	10000	724500	0,10987	0,13425	0,1159
10:36:22.620	7	3	10000	10000	724500	0,10866	0,13727	0,11424
10:36:22.639	7	4	10000	10000	579600	0,10887	0,15572	0,11486
10:36:22.658	7	5	10000	10000	579600	0,10736	0,15361	0,11477
10:36:22.676	7	6	10000	10000	338100	0,11865	0,18192	0,12864
10:36:22.695	7	7	10000	10000	338100	0,13756	0,19156	0,14682
10:37:20.752	9	1	100	100	725400	0,054641	0,0637	0,057685
10:37:20.770	9	2	100	100	725400	0,057191	0,061856	0,058632
10:37:20.786	9	3	100	100	725400	0,059309	0,06618	0,061456
10:37:20.801	9	4	100	100	580500	0,060854	0,069187	0,063388
10:37:20.817	9	5	100	100	580500	0,060949	0,068583	0,063769
10:37:20.833	9	6	100	100	339000	0,060409	0,070387	0,06266
10:37:20.849	9	7	100	100	339000	0,059732	0,069003	0,062519
10:37:20.864	9	8	100	100	900	0,060885	0,068071	0,063088
10:37:20.879	9	9	100	100	900	0,060737	0,070387	0,062925
10:38:17.873	9	1	100	100	726300	0,057314	0,065778	0,060663
10:38:17.893	9	2	100	100	726300	0,056468	0,065724	0,059228
10:38:17.910	9	3	100	100	726300	0,056492	0,065128	0,059407
10:38:17.938	9	4	100	100	581400	0,056445	0,064138	0,059204
10:38:17.955	9	5	100	100	581400	0,057821	0,06558	0,060938
10:38:17.974	9	6	100	100	339900	0,058785	0,065574	0,061172
10:38:17.990	9	7	100	100	339900	0,060179	0,074265	0,063535
10:38:18.006	9	8	100	100	1800	0,061386	0,069917	0,063921
10:38:18.022	9	9	100	100	1800	0,058802	0,064812	0,061064
10:39:16.254	9	1	100	100	727200	0,057233	0,063546	0,059275
10:39:16.272	9	2	100	100	727200	0,056935	0,06427	0,059202
10:39:16.292	9	3	100	100	727200	0,056869	0,066324	0,05923

Time Stamp	Num Of Miners	iMiner	Num Blocks	Num Pendings	Num Meas	Meas MinCT	Meas MaxCT	Meas AvgCT
10:39:16.311	9	4	100	100	582300	0,0565	0,069463	0,059728
10:39:16.331	9	5	100	100	582300	0,057889	0,065167	0,060115
10:39:16.348	9	6	100	100	340800	0,057911	0,070197	0,060668
10:39:16.364	9	7	100	100	340800	0,059104	0,073573	0,063344
10:39:16.381	9	8	100	100	2700	0,063896	0,080033	0,070128
10:39:16.398	9	9	100	100	2700	0,062776	0,080948	0,07008
10:51:55.787	9	1	1000	1000	736200	0,063173	0,075692	0,067102
10:51:55.815	9	2	1000	1000	736200	0,06729	0,080512	0,070891
10:51:55.839	9	3	1000	1000	736200	0,069589	0,094307	0,07579
10:51:55.906	9	4	1000	1000	591300	0,073293	0,089239	0,077886
10:51:55.924	9	5	1000	1000	591300	0,074078	0,098435	0,079035
10:51:55.944	9	6	1000	1000	349800	0,081115	0,11492	0,087726
10:51:55.962	9	7	1000	1000	349800	0,081707	0,14561	0,095015
10:51:55.980	9	8	1000	1000	11700	0,080597	0,10401	0,088488
10:51:55.998	9	9	1000	1000	11700	0,081497	0,10596	0,089269
11:06:56.378	9	1	1000	1000	745200	0,088936	0,10989	0,095882
11:06:56.397	9	2	1000	1000	745200	0,091646	0,12382	0,097997
11:06:56.414	9	3	1000	1000	745200	0,090682	0,1124	0,097174
11:06:56.432	9	4	1000	1000	600300	0,088928	0,11485	0,097858
11:06:56.449	9	5	1000	1000	600300	0,08902	0,11785	0,095201
11:06:56.466	9	6	1000	1000	358800	0,088791	0,10417	0,093963
11:06:56.483	9	7	1000	1000	358800	0,090268	0,12164	0,099069
11:06:56.500	9	8	1000	1000	20700	0,091132	0,13106	0,10002
11:06:56.518	9	9	1000	1000	20700	0,092467	0,1136	0,098568
11:21:21.808	9	1	1000	1000	754200	0,083089	0,12633	0,095276
11:21:21.827	9	2	1000	1000	754200	0,07918	0,13213	0,091107
11:21:21.852	9	3	1000	1000	754200	0,081276	0,16234	0,09873
11:21:21.868	9	4	1000	1000	609300	0,080251	0,12729	0,092385
11:21:21.884	9	5	1000	1000	609300	0,079393	0,13414	0,090973
11:21:21.902	9	6	1000	1000	367800	0,082466	0,13212	0,09734
11:21:21.918	9	7	1000	1000	367800	0,086265	0,14289	0,10218
11:21:21.934	9	8	1000	1000	29700	0,076682	0,1223	0,083769
11:21:21.951	9	9	1000	1000	29700	0,080231	0,12004	0,089204
12:54:10.166	9	1	5000	5000	799200	0,10871	0,19288	0,12353
12:54:10.183	9	2	5000	5000	799200	0,108	0,16116	0,12303
12:54:10.200	9	3	5000	5000	799200	0,11054	0,17716	0,12577
12:54:10.236	9	4	5000	5000	654300	0,10897	0,15039	0,12224
12:54:10.263	9	5	5000	5000	654300	0,10759	0,15949	0,11879
12:54:10.282	9	6	5000	5000	412800	0,10825	0,1569	0,11646
12:54:10.302	9	7	5000	5000	412800	0,10982	0,15596	0,11808
12:54:10.320	9	8	5000	5000	74700	0,10828	0,13178	0,11591
12:54:10.338	9	9	5000	5000	74700	0,11739	0,14007	0,12471

Time Stamp	Num Of Miners	iMiner	Num Blocks	Num Pendings	Num Meas	Meas MinCT	Meas MaxCT	Meas AvgCT
14:26:34.715	9	1	5000	5000	844200	0,10809	0,12673	0,11172
14:26:34.734	9	2	5000	5000	844200	0,10794	0,15628	0,11641
14:26:34.752	9	3	5000	5000	844200	0,11068	0,14923	0,11788
14:26:34.769	9	4	5000	5000	699300	0,10919	0,15169	0,11753
14:26:34.808	9	5	5000	5000	699300	0,11072	0,15647	0,11932
14:26:34.825	9	6	5000	5000	457800	0,10861	0,14477	0,11711
14:26:34.843	9	7	5000	5000	457800	0,11151	0,14567	0,11935
14:26:34.863	9	8	5000	5000	119700	0,11485	0,16552	0,1253
14:26:34.880	9	9	5000	5000	119700	0,12739	0,19105	0,14034
16:01:01.752	9	1	5000	5000	889200	0,1178	0,16788	0,12828
16:01:01.771	9	2	5000	5000	889200	0,11417	0,16539	0,12188
16:01:01.790	9	3	5000	5000	889200	0,11334	0,15793	0,12054
16:01:01.807	9	4	5000	5000	744300	0,11149	0,18598	0,12081
16:01:01.849	9	5	5000	5000	744300	0,11396	0,16412	0,12388
16:01:01.866	9	6	5000	5000	502800	0,10951	0,15195	0,11557
16:01:01.884	9	7	5000	5000	502800	0,11123	0,15557	0,1201
16:01:01.902	9	8	5000	5000	164700	0,11321	0,16811	0,12059
16:01:01.921	9	9	5000	5000	164700	0,12866	0,21502	0,13692
20:42:19.958	9	1	10000	10000	979200	0,15503	0,21857	0,17584
20:42:19.976	9	2	10000	10000	979200	0,15929	0,23107	0,18175
20:42:19.996	9	3	10000	10000	979200	0,16393	0,23363	0,18661
20:42:20.019	9	4	10000	10000	834300	0,16137	0,21864	0,1784
20:42:20.039	9	5	10000	10000	834300	0,15618	0,21417	0,17428
20:42:20.066	9	6	10000	10000	592800	0,16035	0,22453	0,17798
20:42:20.085	9	7	10000	10000	592800	0,16036	0,23875	0,18196
20:42:20.105	9	8	10000	10000	254700	0,1632	0,22096	0,18426
20:42:20.125	9	9	10000	10000	254700	0,1935	0,27758	0,21725
00:45:45.150	9	1	10000	10000	1069200	0,15286	0,19216	0,16133
00:45:45.170	9	2	10000	10000	1069200	0,14668	0,18582	0,15216
00:45:45.190	9	3	10000	10000	1069200	0,14713	0,17312	0,15392
00:45:45.210	9	4	10000	10000	924300	0,14633	0,19213	0,15423
00:45:45.230	9	5	10000	10000	924300	0,15029	0,17628	0,15582
00:45:45.250	9	6	10000	10000	682800	0,14514	0,17708	0,15269
00:45:45.270	9	7	10000	10000	682800	0,14431	0,19533	0,14969
00:45:45.290	9	8	10000	10000	344700	0,15697	0,18272	0,16215
00:45:45.300	9	9	10000	10000	344700	0,18352	0,23699	0,19204
04:46:33.270	9	1	10000	10000	1159200	0,15316	0,18491	0,15984
04:46:33.300	9	2	10000	10000	1159200	0,14656	0,18533	0,15187
04:46:33.310	9	3	10000	10000	1159200	0,14816	0,16827	0,15413
04:46:33.330	9	4	10000	10000	1014300	0,14492	0,19489	0,15201
04:46:33.360	9	5	10000	10000	1014300	0,14725	0,17174	0,15217
04:46:33.380	9	6	10000	10000	772800	0,14301	0,16342	0,14996

Time Stamp	Num Of Miners	iMiner	Num Blocks	Num Pendings	Num Meas	Meas MinCT	Meas MaxCT	Meas AvgCT
04:46:33.400	9	7	10000	10000	772800	0,14203	0,19221	0,14766
04:46:33.410	9	8	10000	10000	434700	0,15413	0,17596	0,15868
04:46:33.430	9	9	10000	10000	434700	0,17983	0,27006	0,19303
04:47:52.927	11	1	100	100	1160300	0,060649	0,065835	0,061666
04:47:52.947	11	2	100	100	1160300	0,063565	0,067912	0,064602
04:47:52.967	11	3	100	100	1160300	0,064555	0,068436	0,065921
04:47:53.007	11	4	100	100	1015400	0,066315	0,069885	0,067282
04:47:53.027	11	5	100	100	1015400	0,075827	0,084947	0,078552
04:47:53.037	11	6	100	100	773900	0,068876	0,074328	0,070093
04:47:53.057	11	7	100	100	773900	0,069576	0,072851	0,070722
04:47:53.077	11	8	100	100	435800	0,069738	0,073323	0,070796
04:47:53.087	11	9	100	100	435800	0,070485	0,074929	0,071394
04:47:53.107	11	10	100	100	1100	0,07103	0,075212	0,072063
04:47:53.127	11	11	100	100	1100	0,071131	0,077455	0,07243
04:49:11.829	11	1	100	100	1161400	0,067845	0,073951	0,069574
04:49:11.849	11	2	100	100	1161400	0,06805	0,07689	0,069567
04:49:11.869	11	3	100	100	1161400	0,067644	0,072142	0,068674
04:49:11.889	11	4	100	100	1016500	0,067958	0,076087	0,069921
04:49:11.929	11	5	100	100	1016500	0,067782	0,073885	0,069606
04:49:11.949	11	6	100	100	775000	0,068188	0,072859	0,069211
04:49:11.959	11	7	100	100	775000	0,068152	0,072388	0,069176
04:49:11.979	11	8	100	100	436900	0,068486	0,074719	0,069543
04:49:11.999	11	9	100	100	436900	0,068111	0,07372	0,069062
04:49:12.009	11	10	100	100	2200	0,06825	0,073116	0,069273
04:49:12.029	11	11	100	100	2200	0,068991	0,072276	0,069941
04:50:30.823	11	1	100	100	1162500	0,068756	0,07316	0,070418
04:50:30.843	11	2	100	100	1162500	0,068181	0,075348	0,069994
04:50:30.863	11	3	100	100	1162500	0,067999	0,071093	0,069054
04:50:30.873	11	4	100	100	1017600	0,068453	0,071452	0,069263
04:50:30.903	11	5	100	100	1017600	0,06813	0,071648	0,06917
04:50:30.923	11	6	100	100	776100	0,068288	0,072303	0,069171
04:50:30.943	11	7	100	100	776100	0,068359	0,071347	0,06946
04:50:30.953	11	8	100	100	438000	0,068164	0,071834	0,069233
04:50:30.973	11	9	100	100	438000	0,068181	0,072448	0,069506
04:50:30.983	11	10	100	100	3300	0,068342	0,072584	0,069271
04:50:31.003	11	11	100	100	3300	0,068525	0,072333	0,069552
05:06:54.168	11	1	1000	1000	1173500	0,076504	0,083448	0,078096
05:06:54.188	11	2	1000	1000	1173500	0,079851	0,086225	0,081517
05:06:54.208	11	3	1000	1000	1173500	0,081969	0,088404	0,083414
05:06:54.228	11	4	1000	1000	1028600	0,083736	0,093236	0,085961
05:06:54.248	11	5	1000	1000	1028600	0,085642	0,093696	0,087608
05:06:54.268	11	6	1000	1000	787100	0,085637	0,092882	0,087164

Time Stamp	Num Of Miners	iMiner	Num Blocks	Num Pendings	Num Meas	Meas MinCT	Meas MaxCT	Meas AvgCT
05:06:54.288	11	7	1000	1000	787100	0,087794	0,094367	0,089311
05:06:54.298	11	8	1000	1000	449000	0,088169	0,094859	0,089698
05:06:54.318	11	9	1000	1000	449000	0,089177	0,10088	0,09122
05:06:54.328	11	10	1000	1000	14300	0,089091	0,094826	0,09083
05:06:54.348	11	11	1000	1000	14300	0,091428	0,10109	0,093185
05:23:33.622	11	1	1000	1000	1184500	0,086616	0,095352	0,088095
05:23:33.642	11	2	1000	1000	1184500	0,087423	0,093484	0,088939
05:23:33.662	11	3	1000	1000	1184500	0,087108	0,094562	0,088386
05:23:33.672	11	4	1000	1000	1039600	0,086633	0,095927	0,0892
05:23:33.712	11	5	1000	1000	1039600	0,086426	0,095857	0,087674
05:23:33.722	11	6	1000	1000	798100	0,087446	0,093209	0,088696
05:23:33.732	11	7	1000	1000	798100	0,086104	0,093305	0,088072
05:23:33.752	11	8	1000	1000	460000	0,087004	0,095407	0,088453
05:23:33.762	11	9	1000	1000	460000	0,086596	0,094114	0,087853
05:23:33.782	11	10	1000	1000	25300	0,086649	0,09314	0,088013
05:23:33.792	11	11	1000	1000	25300	0,089424	0,09653	0,090968
05:40:14.859	11	1	1000	1000	1195500	0,086578	0,091524	0,087861
05:40:14.879	11	2	1000	1000	1195500	0,087112	0,092877	0,088899
05:40:14.899	11	3	1000	1000	1195500	0,088008	0,097662	0,089457
05:40:14.919	11	4	1000	1000	1050600	0,08572	0,0918	0,087036
05:40:14.959	11	5	1000	1000	1050600	0,086664	0,092772	0,087999
05:40:14.969	11	6	1000	1000	809100	0,087149	0,097555	0,089004
05:40:14.989	11	7	1000	1000	809100	0,086771	0,13181	0,088818
05:40:14.999	11	8	1000	1000	471000	0,087686	0,094093	0,088944
05:40:15.019	11	9	1000	1000	471000	0,086653	0,09694	0,087935
05:40:15.029	11	10	1000	1000	36300	0,086353	0,097896	0,088619
05:40:15.039	11	11	1000	1000	36300	0,090033	0,10233	0,091635
07:45:38.886	11	1	5000	5000	1250500	0,12165	0,14192	0,12735
07:45:38.916	11	2	5000	5000	1250500	0,12681	0,14616	0,13226
07:45:38.926	11	3	5000	5000	1250500	0,12805	0,14402	0,1326
07:45:38.946	11	4	5000	5000	1105600	0,12883	0,14583	0,13395
07:45:38.976	11	5	5000	5000	1105600	0,12661	0,17632	0,1321
07:45:38.986	11	6	5000	5000	864100	0,12564	0,14441	0,13045
07:45:38.996	11	7	5000	5000	864100	0,12699	0,14306	0,13248
07:45:39.016	11	8	5000	5000	526000	0,12797	0,15106	0,13317
07:45:39.026	11	9	5000	5000	526000	0,12788	0,14319	0,13278
07:45:39.046	11	10	5000	5000	91300	0,13004	0,14525	0,13562
07:45:39.056	11	11	5000	5000	91300	0,14698	0,19459	0,1533
09:52:36.934	11	1	5000	5000	1305500	0,13355	0,14751	0,1369
09:52:36.954	11	2	5000	5000	1305500	0,13242	0,14765	0,13548
09:52:36.964	11	3	5000	5000	1305500	0,13192	0,14836	0,13473
09:52:36.984	11	4	5000	5000	1160600	0,1305	0,1683	0,13438

Time Stamp	Num Of Miners	iMiner	Num Blocks	Num Pendings	Num Meas	Meas MinCT	Meas MaxCT	Meas AvgCT
09:52:36.994	11	5	5000	5000	1160600	0,12986	0,14582	0,13284
09:52:37.014	11	6	5000	5000	919100	0,1284	0,14236	0,13092
09:52:37.024	11	7	5000	5000	919100	0,12993	0,14681	0,13332
09:52:37.034	11	8	5000	5000	581000	0,12902	0,14273	0,13166
09:52:37.054	11	9	5000	5000	581000	0,12988	0,14396	0,13277
09:52:37.064	11	10	5000	5000	146300	0,13491	0,17875	0,13825
09:52:37.084	11	11	5000	5000	146300	0,14961	0,16863	0,15395
11:59:40.906	11	1	5000	5000	1360500	0,13534	0,15429	0,13899
11:59:40.926	11	2	5000	5000	1360500	0,13435	0,14676	0,13695
11:59:40.946	11	3	5000	5000	1360500	0,13283	0,14499	0,13558
11:59:40.966	11	4	5000	5000	1215600	0,13222	0,17996	0,13579
11:59:40.986	11	5	5000	5000	1215600	0,13036	0,14465	0,13288
11:59:41.006	11	6	5000	5000	974100	0,12855	0,14309	0,13141
11:59:41.016	11	7	5000	5000	974100	0,12895	0,14297	0,13195
11:59:41.036	11	8	5000	5000	636000	0,12852	0,14208	0,1314
11:59:41.046	11	9	5000	5000	636000	0,12887	0,16186	0,13202
11:59:41.066	11	10	5000	5000	201300	0,13294	0,14916	0,13619
11:59:41.076	11	11	5000	5000	201300	0,14873	0,16556	0,15322
18:35:15.971	11	1	10000	10000	1470500	0,18801	0,27632	0,21087
18:35:15.991	11	2	10000	10000	1470500	0,21315	0,33856	0,241
18:35:16.011	11	3	10000	10000	1470500	0,19893	0,29208	0,2232
18:35:16.021	11	4	10000	10000	1325600	0,19651	0,27848	0,22143
18:35:16.051	11	5	10000	10000	1325600	0,19145	0,31298	0,21461
18:35:16.071	11	6	10000	10000	1084100	0,18299	0,21848	0,19509
18:35:16.091	11	7	10000	10000	1084100	0,18384	0,22642	0,19573
18:35:16.111	11	8	10000	10000	746000	0,18889	0,22715	0,20208
18:35:16.131	11	9	10000	10000	746000	0,18849	0,2232	0,20157
18:35:16.151	11	10	10000	10000	311300	0,18922	0,21963	0,20128
18:35:16.171	11	11	10000	10000	311300	0,21483	0,24989	0,23138
00:51:42.300	11	1	10000	10000	1580500	0,19825	0,22476	0,20449
00:51:42.330	11	2	10000	10000	1580500	0,19215	0,21266	0,1988
00:51:42.340	11	3	10000	10000	1580500	0,18869	0,21588	0,19566
00:51:42.360	11	4	10000	10000	1435600	0,18807	0,21191	0,19441
00:51:42.390	11	5	10000	10000	1435600	0,18686	0,21119	0,1947
00:51:42.410	11	6	10000	10000	1194100	0,19251	0,22163	0,19858
00:51:42.430	11	7	10000	10000	1194100	0,18862	0,20764	0,19445
00:51:42.440	11	8	10000	10000	856000	0,19139	0,21821	0,20084
00:51:42.460	11	9	10000	10000	856000	0,19258	0,21257	0,19765
00:51:42.480	11	10	10000	10000	421300	0,2058	0,22733	0,21142
00:51:42.490	11	11	10000	10000	421300	0,22363	0,24923	0,234
07:05:36.722	11	1	10000	10000	1690500	0,19721	0,22364	0,20576
07:05:36.742	11	2	10000	10000	1690500	0,19522	0,22725	0,20093

Time Stamp	Num Of Miners	iMiner	Num Blocks	Num Pendings	Num Meas	Meas MinCT	Meas MaxCT	Meas AvgCT
07:05:36.762	11	3	10000	10000	1690500	0,1915	0,21645	0,19768
07:05:36.772	11	4	10000	10000	1545600	0,18818	0,21099	0,19635
07:05:36.802	11	5	10000	10000	1545600	0,18625	0,25995	0,19356
07:05:36.822	11	6	10000	10000	1304100	0,18679	0,20951	0,19307
07:05:36.842	11	7	10000	10000	1304100	0,18609	0,20773	0,19242
07:05:36.862	11	8	10000	10000	966000	0,18595	0,21652	0,19669
07:05:36.872	11	9	10000	10000	966000	0,18667	0,21045	0,19375
07:05:36.882	11	10	10000	10000	531300	0,19929	0,22238	0,20657
07:05:36.902	11	11	10000	10000	531300	0,22268	0,25095	0,23307