



Matheus Rodrigues de Oliveira Leal

**ARTIIMoR: Serviço de alta disponibilidade,
confiabilidade e transparência para registros
imutáveis e irrevogáveis de dados de
mobilidade**

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre pelo Programa de Pós-graduação em Informática, do Departamento de Informática da PUC-Rio.

Orientador : Prof. Markus Endler

Co-orientador: Dra. Flávia Pisani

Rio de Janeiro
Agosto de 2023



Matheus Rodrigues de Oliveira Leal

**ARTIIMoR: Serviço de alta disponibilidade,
confiabilidade e transparência para registros
imutáveis e irrevogáveis de dados de
mobilidade**

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre pelo Programa de Pós-graduação em Informática da PUC-Rio. Aprovada pela Comissão Examinadora abaixo: Aprovada pela Comissão Examinadora abaixo:

Prof. Markus Endler

Orientador

Departamento de Informática – PUC-Rio

Dra. Flávia Pisani

UNICAMP

Prof. Sergio Lifschitz

Departamento de Informática – PUC-Rio

Prof. Arlindo Flavio da Conceição

UNIFESP

Rio de Janeiro, 29 de Agosto de 2023

Todos os direitos reservados. A reprodução, total ou parcial do trabalho, é proibida sem a autorização da universidade, do autor e do orientador.

Matheus Rodrigues de Oliveira Leal

Formado em engenharia de computação pela Pontifícia Universidade Católica do Rio de Janeiro.

Ficha Catalográfica

Rodrigues de Oliveira Leal, Matheus

ARTIIMoR: Serviço de alta disponibilidade, confiabilidade e transparência para registros imutáveis e irrevogáveis de dados de mobilidade / Matheus Rodrigues de Oliveira Leal; orientador: Markus Endler; co-orientador: Flávia Pisani. – 2023.

63 f: il. color. ; 30 cm

Dissertação (mestrado) - Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Informática, 2023.

Inclui bibliografia

1. Informática – Teses. 2. Sistemas Distribuídos. 3. Internet das Coisas Móveis. 4. Blockchain. I. Endler, Markus. II. Pisani, Flávia. III. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Informática. IV. Título.

CDD: 004

Aos meus pais, pelo seu apoio
e incentivo.

Agradecimentos

Aos meus orientadores Professor Markus Endler e Flávia Pisani pelo estímulo e parceria para realizar este trabalho.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Resumo

Rodrigues de Oliveira Leal, Matheus; Endler, Markus; Pisani, Flávia. **ARTIIMoR: Serviço de alta disponibilidade, confiabilidade e transparência para registros imutáveis e irrevogáveis de dados de mobilidade.** Rio de Janeiro, 2023. 63p. Dissertação de Mestrado – Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro.

Um sistema de rastreamento que armazena dados de alto volume, tais como indicadores de mobilidade, status de agentes e cargas, é de interesse tanto para empresas quanto para consumidores. Um sistema como esse permite verificar informações, como os locais visitados em um shopping center, a duração das estadias dos funcionários em determinadas partes de um prédio de escritórios ou fábrica, se um ônibus parou em cada ponto de ônibus em uma rota, a rota do entregador ou se uma equipe de seguranças está executando a ronda especificada em um bairro. Esta dissertação tem como objetivo investigar a eficiência de identificar a posição atual de uma entidade móvel e propor uma solução para transmitir, adicionar e recuperar informações como estas. A solução proposta é um framework chamado ARTIIMoR, que armazena dados de maneira segura, imutável e transparente usando um sistema de *Distributed Ledger Technology* (DLT) multicamadas. Três camadas de DLT são utilizadas para armazenar informações de localização em diferentes níveis de abstração e agregação. O sistema visa permitir que empresas e consumidores registrem informações de posição e movimento com confiabilidade, escalabilidade e rastreabilidade.

Palavras-chave

Sistemas Distribuídos; Internet das Coisas Móveis; Blockchain.

Abstract

Rodrigues de Oliveira Leal, Matheus; Endler, Markus (Advisor); Pisani, Flávia (Co-Advisor). **ARTIIMoR: Available, Reliable, Transparent, Immutable, and Irrevocable service for Mobility Records.** Rio de Janeiro, 2023. 63p. Dissertação de Mestrado – Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro.

A tracking system capable of storing high volume data, such as mobility indicators, agent and cargo statuses, is of interest to both companies and consumers. Such a system enables the checking of information, such as the locations visited in a shopping center, the duration of employees' stays in certain parts of an office building or factory, whether a bus stopped at each bus stop on a route, the route of a delivery driver, or whether a security team is performing the specified patrol in a neighborhood. This dissertation aims to investigate the efficiency of identifying the current position of a mobile entity and propose a solution for transmitting, adding, and retrieving information like this. The proposed solution is a framework called ARTIIMoR, which stores data securely, immutably, and transparently using a multilayer Distributed Ledger Technology (DLT) system. Three layers of DLT are used to store location information at different levels of abstraction and aggregation. The system aims to allow companies and consumers to record position and movement information with reliability, scalability, and traceability.

Keywords

Distributed computing; Internet of Mobile Things; Blockchain.

Sumário

1	Introdução	15
2	Conceitos Fundamentais e Tecnologias	18
2.1	ContextNet	18
2.2	Complex Event Processing	20
2.3	Distributed Ledger Technology (DLT)	21
2.3.1	Mecanismo de Consenso	21
2.3.2	IOTA	22
2.3.3	Contratos Inteligentes	23
2.3.4	Blockchain	24
3	Trabalho Relacionado	28
4	Arquitetura do Framework	33
4.1	Localização de Entidade Móvel com ContextNet	33
4.2	Modelo de Rede DLT Multicamada	34
4.3	Checkpoints	36
4.4	Fluxo de Inserção de Dados	37
4.5	Modelo de Busca de Dados	39
4.6	Privacidade	40
4.7	Garantindo a Precisão dos Dados Armazenados	41
5	Aplicações	42
5.1	Entrega de Alimentos	42
5.2	Carsharing	43
5.3	Coleta de Lixo	44
5.4	Cadeia de Suprimentos	45
6	Resultados	47
6.1	Experimentos de Desempenho de Inserção	48
6.2	Experimentos do Modelo de Inserção	50
6.3	Experimentos de Desempenho de Consulta	52
7	Conclusão	54
8	Referências bibliográficas	56

Lista de figuras

Figura 2.1	Arquitetura de software e protocolos do núcleo do ContextNet e nos M-Hubs.	19
Figura 2.2	Diagram of a Mobile Event Processing Agent service	20
Figura 4.1	Exemplo de arquitetura DLT multicamada.	35
Figura 4.2	Diagrama detalhado de inserção.	38
Figura 6.1	Comparação entre número de mensagens e tempo de inserção.	49
Figura 6.2	Comparação entre número de mensagens e tempo de inserção após ajustar o modelo de inserção do Ethereum.	49
Figura 6.3	Comparação do modelo de inserção entre Geofences e Tamanho Fixo.	51
Figura 6.4	Comparação entre mensagens e tempo de consulta.	53

Lista de tabelas

Tabela 2.1	Tipos de Blockchain.	26
Tabela 2.2	Diferenças entre Ethereum, Hyperledger Fabric e IOTA.	27
Tabela 3.1	Comparação de soluções similares com ARTIIMoR.	31
Tabela 5.1	Caso de uso do ARTIIMoR.	46

Lista de algoritmos

Lista de Códigos

Lista de Abreviaturas

ARTIIMoR – *Available reliable transparent immutable and irrevocable service for Mobility Record*

BLE – *Bluetooth Low Energy*

CEP – *Complex Event Processing*

DApps – *Decentralized Applications*

DAG – *Directed Acyclic Graph*

DLT – *Distributed Ledger Technology*

ETH – *Ether*

GLMP – *Generic Ledger Middleman Process*

GPS – *Global Positioning System*

IoT – *Internet of Things*

IoMT – *Internet of Mobile Things*

LBS – *Location Based Service*

LSP – *Ledger Scheduler Process*

MOP – *Mobility Observer Process*

M-Hub – *Mobile-Hub*

UID – *User identifier*

*Everything not saved will be lost. –Nintendo
“Quit Screen” message*

T. Michael Martin, *The End Game*.

1

Introdução

O movimento de produtos, itens de suprimento e funcionários pode revelar muito sobre a operação diária de uma empresa. Em muitas indústrias, as informações sobre padrões de mobilidade e a localização exata e o tempo de permanência de entidades móveis são inestimáveis. Isso pode ser usado para verificar a adequação dos fluxos de trabalho e dos serviços de mobilidade, além de servir como base para otimizar as operações comerciais (ZHAO et al., 2016). A utilidade desses dados é ainda maior para empresas e plataformas modernas, como entrega de alimentos, logística, aluguel de bicicletas e compartilhamento de viagens.

O negócio de entrega de refeições de restaurantes aos clientes está mudando rapidamente, à medida que novas plataformas online competem por clientes em todo o mundo. No modelo tradicional de entrega, os clientes fazem pedidos em um restaurante local e esperam que o restaurante traga a comida até a porta deles (LI; MIROSA; BREMER, 2020). Isso pode dificultar o rastreamento de itens ou agentes individuais ao longo da cadeia de suprimentos. No entanto, plataformas digitais como DoorDash, GrubHub e UberEats estão reformulando o mercado de entrega, oferecendo acesso a vários restaurantes por meio de um único portal online.

Neste mercado competitivo, não ter uma rastreabilidade adequada dos produtos enviados pela cadeia significa perder informações valiosas que poderiam ser usadas para economizar recursos e aumentar a receita (STADTLER, 2005). Um sistema que permite que empresas e consumidores registrem dados em grande escala, como indicadores de mobilidade e o status de agentes e produtos, e consultem essas informações em vários níveis de detalhe, pode ser um ativo valioso para a rastreabilidade. Um sistema desse tipo pode ajudar entregadores, proprietários de restaurantes e clientes a garantir que a melhor rota possível tenha sido usada, considerando a qualidade do serviço de entrega necessário, as condições de tráfego e veículo e as características dos itens entregues.

Um sistema capaz de registrar um grande volume de dados, como indicadores de mobilidade, o status de agentes e cargas, e permitir que empresas e consumidores verifiquem essas informações em diferentes níveis de detalhe, é um ativo valioso (GIANNOTTI; PEDRESCHI, 2008). Esse sistema escalável pode ajudar motoristas de entrega, proprietários de restaurantes e clientes a garantir que eles usem a melhor rota possível com base na qualidade

do serviço de entrega necessário, nas condições de tráfego e veículo e nas características dos itens entregues (SUHARTANTO et al., 2018). Ele também pode melhorar o transporte de produtos sensíveis ao ambiente ou frágeis, como frutas, flores, animais ou medicamentos, adicionando informações relevantes aos pontos de dados geográficos, como temperatura, umidade, luminosidade, leituras do acelerômetro, nome do condutor ou qualquer outra informação de contexto/status orientada ao transporte.

Além disso, caso ocorra um incidente, por exemplo, um produto perecível não chega dentro da janela de tempo esperada, é essencial ter um registro confiável e não modificável do histórico de transporte que possa ser auditado para identificar o problema e resolver disputas legais associadas (LEAL; PISANI; ENDLER, 2019). Através da transparência e imutabilidade, as Distributed Ledger Technologies (DLTs) (RAUCHS et al., 2018) garantem que não haja manipulação, distorção ou fraude nos registros, o que pode aumentar a confiança entre empresas e clientes.

Esta dissertação foca na necessidade de um serviço confiável, escalável e rastreável para registros de mobilidade. A solução proposta é um framework chamado ARTIIMoR (LEAL; PISANI; ENDLER, 2022), que significa **A**vailable, **R**eliable, **T**ransparent, **I**mmutable e **I**rrevocable service for **M**obility **R**ecords. Esta dissertação tem como objetivo coletar dados de entidades móveis por meio de geolocalização e sensores embutidos, e armazená-los de forma segura, imutável e transparente.

O principal desafio nesse cenário é a alta frequência de geração de dados versus a maior latência de consolidação de dados em DLTs. Nossa solução aborda esse problema utilizando um sistema DLT de várias camadas como serviço principal do middleware ContextNet (ENDLER; SILVA, 2018). Como a confiabilidade desse sistema é fundamental, os registros de mobilidade não podem ser alterados ou removidos em nenhum nível de armazenamento. Portanto, DLT é utilizado em cada camada desse sistema de armazenamento.

Cada novo bloco em um Blockchain é criado com base na precisão compartilhada do bloco anterior (NOFER et al., 2017), ou seja, para cometer fraude, um hacker precisaria invadir e editar os dados de todos os blocos anteriores. Além disso, contratos inteligentes desenvolvidos via Blockchain são uma forma segura de automatizar acordos legais no processo logístico. Eles podem monitorar cada etapa do processo e verificar as regras estabelecidas no código que garantirão o cumprimento de cada contrato até o final. O framework apresentado nesta dissertação permite que proprietários e consumidores compartilhem carros com segurança. A ARTIIMoR implementou uma funcionalidade baseada em contratos inteligentes para controlar o acesso a informações

pessoais. O sistema de autorização permite que os gerentes visualizem dados de várias pessoas, mas apenas o operador da entidade móvel pode controlar as configurações de permissão. Isso permitirá que os motoristas comprovem a posição do carro, onde e por quanto tempo o carro foi conduzido.

Esta dissertação está dividida em vários capítulos, cada um abordando um aspecto específico do framework. O Capítulo 3 fornece uma revisão aprofundada de trabalhos relevantes. Este capítulo serve como base para esta dissertação, permitindo-nos identificar lacunas no estado da arte atual e os desafios que devemos superar. O Capítulo 4 apresenta o framework DLT de várias camadas para armazenar registros de mobilidade. Este capítulo descreve os detalhes técnicos e explica como a ARTIIMoR aborda os desafios identificados no capítulo anterior, fornecendo um serviço confiável, escalável e rastreável para registros de mobilidade. O Capítulo 5 demonstra os potenciais usos do nosso serviço em vários domínios, como transporte, logística e saúde. O capítulo também explica como a utilização desse framework pode melhorar a eficiência e a transparência em cada um desses domínios mencionados, destacando seus benefícios associados.

O Capítulo 6 discute os resultados experimentais do framework, apresentando a avaliação de desempenho e destacando suas forças e fraquezas. Nossos experimentos visam investigar os principais conceitos da ARTIIMoR examinando a eficiência de identificar a posição atual de uma entidade móvel e transmitir, adicionar e recuperar informações da DLT de várias camadas. O Capítulo 7 fornece observações conclusivas e possibilidades para trabalhos futuros, resumindo as principais contribuições do projeto e o impacto potencial do framework na indústria. Esta dissertação também identifica desafios que precisam ser abordados em pesquisas futuras para melhorar a escalabilidade e a usabilidade do framework. No geral, este estudo fornece uma análise abrangente e demonstra o potencial do framework DLT de várias camadas para armazenar registros de mobilidade.

2

Conceitos Fundamentais e Tecnologias

Para tornar essa dissertação clara e abrangente, é importante definir termos-chave como Tecnologia de Livro Razão Distribuído, Blockchain, Contratos Inteligentes, Processamento de Eventos Complexos e Contexto de Rede. Isso ajudará os leitores a entender melhor esses conceitos importantes e como eles se relacionam com a construção de um serviço confiável, escalável e rastreável para registros de mobilidade.

2.1

ContextNet

ContextNet (ENDLER; SILVA, 2018) é uma plataforma distribuída escalável de middleware em nuvem-móvel-edge, composta por duas partes principais: o **Core**, um conjunto extensível de microserviços baseados em nuvem, como uma infraestrutura de comunicação peer-to-peer escalável de publicação/assinatura; e o **Mobile-Hub** (ou simplesmente M-Hub) (TALAVERA et al., 2015), um framework de microserviço extensível para dispositivos Android (por exemplo, telefones e sistemas de baixo custo em um chip (SoCs)) que serve como um hub de conectividade para dispositivos IoT. Em sua versão atual, o M-Hub fornece conectividade à Internet para qualquer dispositivo Bluetooth Low Energy (BLE) dentro de seu alcance de comunicação e suporta o Processamento de Eventos Complexos (CEP) (LUCKHAM, 2001) como meio de processamento local em dispositivos edge. Além disso, permite a descoberta, configuração e registro de qualquer beacon BLE (iBeacon/Eddystone) usando a web ou um dispositivo móvel remoto.

Os beacons BLE enviam periodicamente anúncios para dispositivos inteligentes próximos, como o M-Hub, para serem detectados por meio de varreduras sem fio. Esses dispositivos, então, mapeiam os identificadores do beacon para um nome ou coordenada significativa. Para converter esses valores em coordenadas do mundo real, cada beacon precisa ser atribuído a um nome de localização simbólico ou coordenada física, normalmente armazenado em um banco de dados externo baseado em nuvem. Como os beacons BLE são pequenos e leves (JEON et al., 2018), eles podem ser incorporados em pulseiras, crachás de identificação ou pequenas etiquetas que podem ser anexadas a qualquer tipo de equipamento, móvel ou não, móveis, paredes ou tetos.

Para o estudo, decidiu-se detectar beacons móveis configurando M-Hubs em áreas externas de interesse. Esses M-Hubs são executados em pequenos

SoCs com interfaces BLE e Wi-Fi e são montados em paredes ou tetos. Todos os M-Hubs possuem uma lista branca de IDs de beacon que serão considerados, enquanto outros (por exemplo, dispositivos BLE emitindo anúncios de beacon para emparelhamento) serão simplesmente ignorados. Um beacon BLE geralmente tem um alcance de 10 a 50 metros (KUMAR et al., 2016), mas é ajustado para atender às necessidades de nossa aplicação por meio da configuração de sua potência de transmissão. Por fim, o serviço de detecção de proximidade do ContextNet também realiza a desambiguação do sinal do beacon com base na intensidade do sinal de frequência de rádio (RF) sempre que um beacon é detectado por mais de um M-Hub. Dessa forma, é possível construir entradas de `found()` e `lost()` no registro de mobilidade.

Para detectar beacons móveis em áreas externas de interesse, este estudo instalou M-Hubs equipados com pequenos SoCs que possuem interfaces BLE e Wi-Fi (RASHINKAR; PATERSON; SINGH, 2007). Esses M-Hubs podem ser montados em paredes ou tetos e possuem uma lista branca de IDs de beacon que eles reconhecerão. Quaisquer outros beacons (como dispositivos BLE que emitem anúncios de beacon para emparelhamento) serão ignorados. Para atender às necessidades da aplicação, a potência de transmissão do beacon BLE é ajustada, que normalmente tem um alcance de 10 a 50 metros.

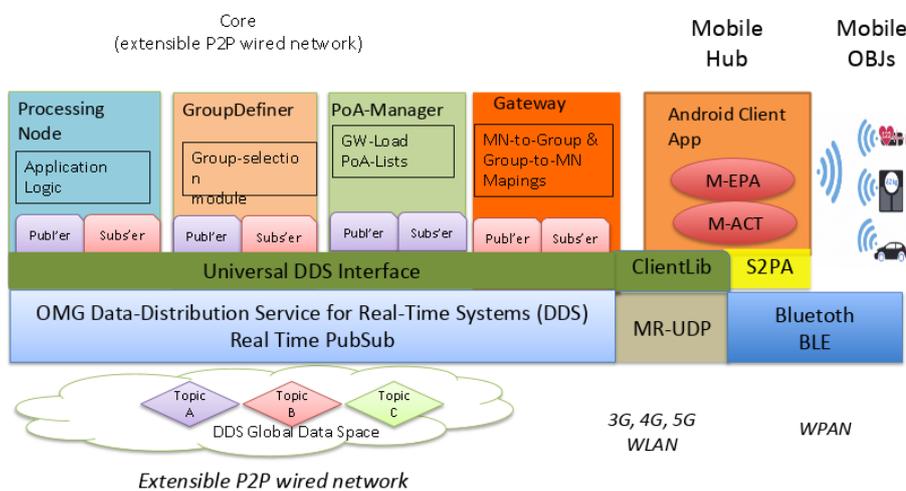


Figura 2.1: Arquitetura de software e protocolos do núcleo do ContextNet e nos M-Hubs.

Conforme apresentado na Figura 2.1 (ENDLER; SILVA, 2018), o ContextNet também permite o posicionamento de entidades móveis por meio de geolocalizações e cercas geográficas. Para isso, o serviço GroupDefiner do Core (VASCONCELOS; SILVA; ENDLER, 2014) foi utilizado para definir uma cerca geográfica como um polígono convexo de coordenadas (lat, long). O sistema então verifica a qual polígono registrado cada georreferência recebida

periodicamente dos M-Hubs (por exemplo, GPS ou posição da rede celular) pertence.

2.2 Complex Event Processing

Para melhorar a efetividade e precisão da detecção de presença usando beacons, é importante comparar, filtrar, corrigir e resumir os sinais dos beacons imediatamente após a leitura. Isso deve ser feito pelos hubs, em vez de um serviço central na nuvem. O Mobile-Hub da ContextNet inclui um mecanismo de eventos complexos ESPER completo (TALAVERA; ENDLER; COLCHER, 2016) que pode processar consultas contínuas na forma de regras EPL sobre o fluxo de sinais de beacon que chegam.

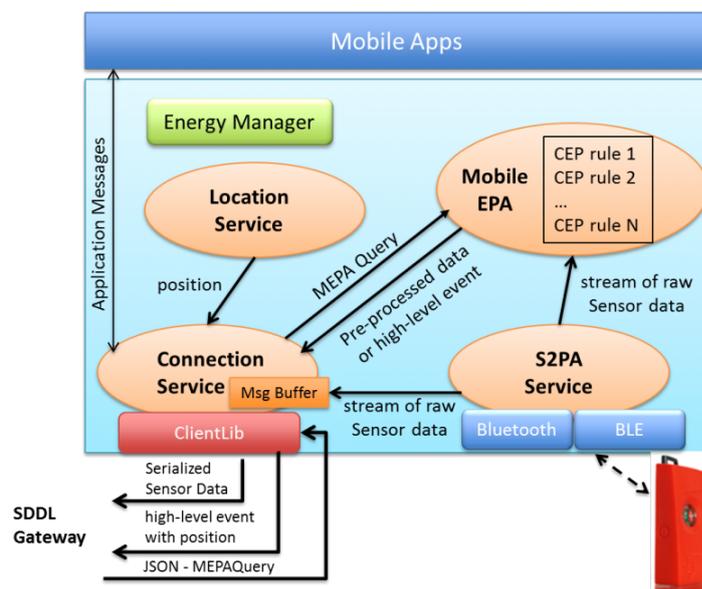


Figura 2.2: Diagram of a Mobile Event Processing Agent service

Conforme apresentado na Figura 2.2 (TALAVERA; ENDLER; COLCHER, 2016), tais consultas contínuas normalmente definem uma janela de observação deslizante de eventos sobre a qual os padrões nas regras são verificados. Por exemplo, uma regra pode ser definida para determinar que se apenas um anúncio com intensidade de sinal de até -100dB é recebido de um beacon B1 dentro de uma janela de 15 segundos, então esse beacon saiu da proximidade do M-Hub. Também usando regras de CEP, qualquer M-Hub, como H1, é capaz de mapear uma sequência de confirmações subsequentes da proximidade de um beacon em eventos iniciais `found(H1, B1)` e `lost(H1, B1)`, que são então enviados para o serviço no Core.

2.3

Distributed Ledger Technology (DLT)

Uma Distributed Ledger Technology (IOINI; PAHL, 2018) é um banco de dados composto por vários dispositivos conectados (nós) em uma rede descentralizada, onde os registros de eventos são armazenados com um carimbo de data/hora e uma assinatura digital. O objetivo é estabelecer confiança e segurança por meio do acordo entre vários nós sobre os registros armazenados.

A principal vantagem desse padrão de processamento distribuído é a falta de uma autoridade central, que constituiria um único ponto de falha. Quando uma transação de atualização do registro é transmitida para a rede, cada nó distribuído processa independentemente uma nova transação de atualização e, em seguida, todos os nós de trabalho coletivamente usam um algoritmo de consenso para determinar a cópia correta do registro atualizado (SUNYAEV; SUNYAEV, 2020). Uma vez que um consenso tenha sido determinado, todos os outros nós se atualizam com a cópia atualizada mais recente e correta do registro.

2.3.1

Mecanismo de Consenso

Um grande problema na computação distribuída e em sistemas multia-gentes é garantir a confiabilidade do sistema ao lidar com processos com falhas. Isso frequentemente requer a coordenação de processos para alcançar consenso ou acordo sobre um valor de dados específico necessário para a computação. Aplicações de consenso incluem determinar a ordem e o conteúdo das transações de banco de dados, replicação de máquina de estados e transmissões atômicas. Aplicações do mundo real que dependem de consenso incluem computação em nuvem, redes inteligentes de energia, controle de VANTs e muito mais. No escopo desta dissertação, um mecanismo de consenso é um protocolo que faz com que todos os nós de uma rede DLT concordem com um único conjunto de dados. Eles servem como padrões de verificação pelos quais cada transação é aprovada. Existem vários tipos de algoritmos de mecanismos de consenso, cada um operando com princípios diferentes. Um validador verifica novas transações e as adiciona à cadeia. Isso envolve verificar se as transações são válidas de acordo com as regras da rede e garantir que o remetente tenha fundos suficientes para concluir a transação.

Antes de enviar uma transação para seus pares (MARIJAN; LAL, 2022), um nó não apenas a assina, mas também confirma sua integridade e autenticidade. Identificadores exclusivos anexados a mensagens e protocolos criptográficos trabalham juntos para garantir segurança. Isso facilita a manutenção da

integridade geral da rede e garante que todas as transações sejam legítimas. Um hash de transação único é criado e, utilizando um algoritmo de verificação, qualquer usuário pode validar uma transação usando esse valor de hash (LI; PALANISAMY, 2020). Quando os destinatários tentam validar a transação usando a assinatura digital, eles poderão saber se ela foi comprometida ou corrompida porque o valor do hash será diferente.

No mundo da Distributed Ledger Technology e Blockchain, existem dois mecanismos amplamente usados. O Proof of Work (PoW) é um mecanismo de consenso popular, amplamente usado na tecnologia Blockchain. Ele é baseado no conceito de mineração. Quando um usuário faz uma transação na rede, ele deve resolver um quebra-cabeça matemático complexo para validar a transação (GERVAIS et al., 2016). Uma vez que o quebra-cabeça seja resolvido, a transação é adicionada ao registro distribuído e o usuário é recompensado com uma certa quantidade de criptomoeda (LIU; CAMP, 2006). Essa recompensa incentiva os usuários a continuarem validando transações e contribuindo para a rede.

Outro mecanismo famoso é o Proof of Stake (PoS) (SALEH, 2020), que é uma classe de mecanismos de consenso que funcionam selecionando validadores proporcionalmente à quantidade de ativos na criptomoeda associada. Isso é feito para evitar o custo computacional de esquemas PoW. Além desses dois mecanismos de consenso famosos, estão sendo criados múltiplos outros (YU; LIU; WANG, 2018) com a mesma ideia de garantir a segurança da rede e promover a descentralização.

2.3.2

IOTA

IOTA (POPOV; LU, 2019) é uma DLT que surgiu para aplicações de IoT. Uma das principais diferenças dessa Distributed Ledger Technology é que ela não usa blocos sequenciais como no Blockchain, em vez disso, cada nó do gráfico é uma transação. Para que uma nova transação seja realizada, seu remetente deve aprovar e verificar duas transações anteriores, ou seja, os validadores são os usuários que enviam ativos e precisam garantir que as transações aprovadas não estejam em conflito.

A tecnologia intimamente associada ao IOTA é chamada de Tangle, que é um Grafo Acíclico Direcionado (DAG) (BENČIĆ; ŽARKO, 2018). Em teoria, o Tangle torna o IOTA mais escalável e seguro à medida que a rede se expande. Seu design interconectado elimina a necessidade de verificação completa do registro. Em vez disso, todas as partes verificam simultaneamente as transações, reduzindo o esforço e o tempo necessários para a execução. O

procedimento de verificação do Tangle também evita gastos duplos, garantindo que as transações não sejam processadas mais de uma vez. No entanto, esse mecanismo de defesa é insuficiente contra ataques em larga escala. Se um atacante obtiver a maioria do poder de hash da rede, ele pode manipular o processo de consenso, potencialmente levando à divisão da rede e gastos duplos. Para mitigar esse risco, o IOTA introduziu a função "Coordenador".

Outra vantagem da tecnologia Tangle é o baixo custo de operação. Para criptomoedas baseadas em Blockchain, como o Bitcoin, uma taxa de transação é cobrada para todas as transações na rede. Não há taxas de transação, pois o sistema do Tangle para armazenar e processar transações não requer mineradores. Isso pode ser extremamente benéfico para sistemas de IoT que criam grandes quantidades de dados.

2.3.3

Contratos Inteligentes

Contratos inteligentes (CLACK; BAKSHI; BRAINE, 2016) são contratos autoexecutáveis com os termos do acordo entre as partes sendo diretamente escritos em linhas de código. O código e os acordos nele contidos existem em uma rede descentralizada, que distribui as informações para todos os participantes da rede. Essa tecnologia fornece os benefícios de um contrato tradicional, mas com a segurança e a transparência adicionais da DLT. O código é à prova de adulteração (GALLERSDÖRFER; MATTHES, 2019), pois é armazenado em vários nós na rede, proporcionando um alto nível de segurança. Além disso, a transparência da DLT permite que todas as partes envolvidas no contrato visualizem os termos do acordo (WANG et al., 2018), o que promove confiança e responsabilidade.

Os contratos inteligentes também têm o potencial de reduzir a necessidade de intermediários, como advogados ou corretores. Isso pode economizar tempo e dinheiro, além de reduzir o risco de fraude e erros (ZOU et al., 2021). O uso de contratos inteligentes está se tornando cada vez mais popular em setores como imóveis, gerenciamento da cadeia de suprimentos e finanças. No entanto, também existem alguns desafios associados aos contratos inteligentes. Um dos principais desafios é que a tecnologia ainda é relativamente nova e existem poucos padrões estabelecidos ou melhores práticas para criar e implementar contratos inteligentes (CAPOCASALE; PERBOLI, 2022). Isso pode tornar o processo de desenvolvimento mais difícil e demorado.

2.3.4

Blockchain

Blockchain é um tipo de Distributed Ledger Technology que facilita o acompanhamento de ativos e o registro de transações. Ele tem um conceito mais amplo, mesmo que tenha sido usado como o livro público para algumas criptomoedas, como o Bitcoin (NAKAMOTO, 2008). Uma rede Blockchain pode rastrear pedidos, pagamentos, contas, produção e muito mais (ZHENG et al., 2017). O nome Blockchain vem da forma como ele armazena os dados de transação em blocos vinculados que formam uma cadeia. Conforme o número de transações aumenta, a cadeia cresce em tamanho. Cada bloco registra e verifica o horário e a ordem das transações, que são então anexadas ao Blockchain dentro de uma rede específica governada por regras acordadas pelos participantes. Devido à sua resistência à adulteração, essa cadeia é segura. Os dados inseridos no Blockchain não podem ser alterados ou removidos depois de serem armazenados lá.

2.3.4.1

A Estrutura do Blockchain

Em geral, todos os participantes da rede têm acesso ao registro distribuído e seu registro imutável de transações. Com esse registro compartilhado, as transações são registradas apenas uma vez, eliminando a duplicação de esforço que é típica das redes de negócios tradicionais (WANG et al., 2019). Essa rede pode incluir nós de todo o mundo, cada um trazendo sua própria perspectiva e experiência única para a mesa. Uma vez que essa rede é estabelecida, os nós podem começar a executar transações.

Os blocos são estruturas de dados dentro do Blockchain que registram permanentemente os dados das transações. Um bloco armazena uma parte ou todas as transações mais recentes que aguardam validação pela rede. Assim que os dados são validados, o bloco é fechado e um novo bloco é criado para que novas transações sejam inseridas e validadas. Esses blocos são conectados por meio de criptografia. Em geral, cada bloco contém um hash criptográfico do bloco anterior, um carimbo de data/hora e dados da transação (ZHANG; XUE; LIU, 2019). O hash do bloco anterior vincula os blocos juntos e impede que qualquer bloco seja alterado ou que um bloco seja inserido entre dois blocos existentes.

A natureza descentralizada da tecnologia Blockchain é um de seus benefícios mais importantes. Isso significa que nenhuma entidade única tem controle sobre os dados, ao contrário de sistemas tradicionais em que uma autoridade central supervisiona as transações. Como não há um único ponto

de falha, é mais difícil para hackers assumirem o sistema, aumentando a segurança (IQBAL; MATULEVIČIUS, 2019). Além disso, ao envolver vários nós nesse processo, o Blockchain se torna mais resiliente e menos suscetível a ataques ou adulterações. Isso ocorre porque qualquer tentativa de adulterar o Blockchain precisaria ser replicada em todos os nós da rede (STEPHEN; ALEX, 2018), tornando muito mais difícil de ter sucesso. Um sistema de referência dentro e entre blocos significa que qualquer tentativa de adulteração quebraria as conexões dentro da cadeia e seria detectada.

2.3.4.2

Classificação do Blockchain

A tecnologia Blockchain já está sendo utilizada em várias indústrias, incluindo finanças, saúde e gerenciamento da cadeia de suprimentos (ZILE; STRAZDINA, 2018). Ela tem o potencial de revolucionar a forma como as transações são conduzidas e verificadas online, tornando-se uma solução promissora para o futuro. Existem várias variedades de Blockchains, cada uma com características e capacidades únicas (ANDERSON et al., 2016).

Blockchains sem permissão, também conhecidos como *trustless* ou públicos, são redes abertas disponíveis para todos. Eles permitem a participação no processo de consenso, que é usado para validar transações e dados. Esse tipo de DLT é completamente descentralizado, o que significa que qualquer pessoa pode participar da rede e acessar os dados armazenados nela. O Bitcoin, a primeira criptomoeda do mundo, é um exemplo primordial de um Blockchain sem permissão.

No caso dos Blockchains públicas, é essencial projetar mecanismos de incentivo que encorajem os nós a compartilhar ativamente e de forma confiável informações na rede, ao mesmo tempo em que isolam e desconectam nós não confiáveis (HUANG et al., 2019). Isso é alcançado por meio de um sistema de recompensas que motiva os nós a contribuir para a rede (IRRESBERGER; JOHN; SALEH, 2020). O mecanismo de incentivo desempenha um papel fundamental nas redes de Blockchain públicas, pois garante o engajamento e a sustentabilidade da rede.

Outro tipo é o Blockchain com permissão (SOLTANI et al., 2022), também conhecido como privado. Como o nome sugere, esse tipo de Blockchain não está aberto ao público. Em vez disso, é mantido por uma única organização ou grupo de organizações (GEYER et al., 2019). Blockchains privados são frequentemente usados para soluções empresariais, pois fornecem um ambiente mais controlado para armazenar e compartilhar dados.

Em contraste com os Blockchains públicas, as transações em um Block-

chain privado são verificadas por um grupo selecionado de participantes (GUEGAN, 2017). Os Blockchains com permissão são tipicamente utilizados por agências governamentais, instituições financeiras e outras organizações que exigem um alto nível de segurança e privacidade de dados (SHAHAAB et al., 2019). Os participantes em um Blockchain com permissão devem estar autorizados a acessar a rede.

Por fim, existem os Blockchains híbridos (VESTERGAARD; BOBOSHA; LANGFELDT, 2021). Como o nome sugere, esse tipo combina as características de Blockchains públicas e privadas. Os híbridos são comumente usados em indústrias que precisam tanto de transparência quanto de privacidade, como saúde e gerenciamento da cadeia de suprimentos.

Tabela 2.1: Tipos de Blockchain.

Com base no acesso ao Blockchain	Com base no acesso aos Dados do Blockchain
Sem permissão: Qualquer um pode participar	Pública: Todos que acessam podem modificar
Com permissão: Apenas usuários aprovados	Privado: Apenas usuários específicos podem escrever/modificar

2.3.4.3

Hyperledger Fabric

Hyperledger (ELROM, 2019) é um projeto guarda-chuva de Blockchains de código aberto e ferramentas relacionadas, estabelecido pela Linux Foundation em 2015. Ele cresceu e se tornou um dos projetos Blockchain mais influentes do mundo, com muitas empresas contribuindo para o desenvolvimento colaborativo de livros-razão distribuídos baseados em Blockchain.

O objetivo do projeto é promover a colaboração entre diferentes setores através do desenvolvimento de Blockchains e livros-razão distribuídos, focados em melhorar seu desempenho e confiabilidade para suportar transações comerciais globais por grandes empresas tecnológicas, financeiras e de cadeia de suprimentos.

O projeto integra protocolos e padrões abertos independentes em uma estrutura para módulos específicos de uso, incluindo Blockchains com seus próprios algoritmos de consenso e armazenamento, e serviços para identidade, controle de acesso e contratos inteligentes. Hyperledger Fabric (ANDROULAKI et al., 2018) é uma plataforma de Blockchain com permissão usada para executar contratos inteligentes e focada na implantação de aplicativos distribuídos. Sua modularidade o torna flexível e adaptável a uma ampla gama de casos de

uso, não está vinculado a nenhum Blockchain ou criptomoeda específica, e é configurável para funcionar com vários mecanismos de consenso.

Hyperledger Fabric enfatiza fortemente a segurança e privacidade, garantindo que as transações sejam seguras e que informações sensíveis sejam mantidas confidenciais. Ele usa a Practical Byzantine Fault Tolerance (CASTRO; LISKOV, 2002) para algoritmos de consenso, o que é crucial em ambientes empresariais onde a privacidade dos dados é uma preocupação importante. Seu foco na interoperabilidade o torna compatível com outras plataformas Blockchain, facilitando a integração por desenvolvedores em sistemas existentes. Isso também significa que ele tem o potencial de ser usado em uma ampla variedade de setores, desde finanças até saúde e gerenciamento da cadeia de suprimentos.

2.3.4.4

Ethereum

A Blockchain do Ethereum (BUTERIN et al., 2014) é uma plataforma descentralizada de Blockchain de código aberto que permite aos desenvolvedores construir aplicativos descentralizados (DApps) e contratos inteligentes. Uma das principais características do Ethereum é sua capacidade de criar contratos inteligentes, que são programas de computador que executam automaticamente os termos de um contrato quando certas condições são cumpridas (MOHANTY; MOHANTY, 2018).

O Ethereum também introduziu o conceito de tokens, que são um tipo de ativo digital que pode ser criado no Ethereum. Os tokens podem representar qualquer coisa, desde um ativo do mundo real, como ouro ou imóveis, até um ativo digital, como um item de jogo de vídeo ou um token de mídia social. A rede Ethereum é alimentada pelo ether (ETH), que é a criptomoeda nativa da Blockchain do Ethereum (BOUOYOUR; SELMI, 2017). O ETH é usado para pagar taxas de transação e incentivar os mineradores a processar transações e manter a rede.

Tabela 2.2: Diferenças entre Ethereum, Hyperledger Fabric e IOTA.

Tipo	Acesso	Rede	Consenso
IOTA	Qualquer pessoa	Descentralizada	Tangle
Ethereum	Qualquer pessoa	Descentralizada	Processo de Mineração
Hyperledger	Por convite	Parcialmente centralizada	Método acordado pelos participantes

3

Trabalho Relacionado

Entre os muitos usos e aplicações da Distributed Ledger Technology (DLT), um deles é a capacidade de registrar informações de posição e movimento com confiabilidade, escalabilidade e rastreabilidade. Nesse contexto, a *confiabilidade* é um fator importante a ser considerado. Isso significa que, uma vez que uma posição visitada é registrada, ela não pode ser excluída ou modificada. Isso é importante não apenas para garantir um registro preciso, mas também para manter a confiança entre os usuários. A *escalabilidade* também é crucial para que um aplicativo possa lidar com muitas entidades móveis. Isso significa que o sistema pode crescer conforme necessário, sem comprometer o desempenho ou a qualidade. Também significa que o sistema pode lidar com muitos indicadores de mobilidade e com o status de agentes e mercadorias sem problemas. Por fim, a implementação de medidas de *rastreabilidade* ajuda a garantir a segurança dos produtos, bem como identificar possíveis problemas ou áreas de melhoria em tempo real. Também nos permite fornecer transparência aos clientes e partes interessadas, o que pode ajudar a construir confiança e credibilidade em um negócio.

Poucos estudos foram realizados em sistemas semelhantes que estão de alguma forma relacionados ao que propomos nesta dissertação. Nos parágrafos a seguir, resumiremos esses estudos e os compararemos ao nosso sistema para demonstrar as vantagens e benefícios únicos que nossa abordagem oferece.

A prova de localização é uma questão importante. Usuários enganosos podem fornecer informações falsas de localização em aplicativos sensíveis à localização para receber ilegalmente um serviço ou vantagem. Nosouhiab et al. (NOSOUHI et al., 2020) propõem uma solução baseada em Blockchain para criação e verificação de prova de localização (Tabela 3.1 referência A). Ao contrário do ARTIIMoR, o usuário transmite uma localização para os dispositivos vizinhos por meio de uma conexão Bluetooth. Os dispositivos vizinhos, então, autenticam o usuário solicitante por meio de um mecanismo de incentivo. Um registro de transação é criado e transmitido por uma rede peer-to-peer. Os verificadores usam a localização assim que ela é validada.

Neste estudo, eles desenvolvem um sistema descentralizado para geração e verificação de prova de localização usando as propriedades especiais da tecnologia Blockchain. Na abordagem sugerida, um usuário (denominado provedor), que requer uma prova de localização, transmite uma solicitação para os dispositivos próximos usando uma interface de comunicação de curto alcance,

como Bluetooth. Os dispositivos vizinhos que optam por responder (denominados testemunhas) começam a confirmar a pessoa que fez a solicitação. As confirmações criptográficas dos usuários em relação aos seus dados de localização podem ser armazenadas para proteger sua privacidade em relação aos seus paradeiros.

Seus testes revelaram que os tempos de resposta são significativamente mais rápidos quando nenhum procedimento de distância é usado. Embora promissor, essa abordagem não é a mais adequada para validar a posição em cenários de instâncias dinâmicas, pois os nós são móveis e podem ficar indisponíveis para seus vizinhos. Sua solução não fornece um mecanismo para resolver esse problema. Os próximos passos de nossa pesquisa estão diretamente relacionados a essas falhas de conectividade com entidades móveis.

Outra proposta (Tabela 3.1 referência B) consiste em um sistema distribuído descentralizado que coleta e transfere dados para o BigchainDB (TIAN, 2017), não necessariamente relacionados à mobilidade. Diferente de nossa abordagem, Tian usa apenas um Blockchain privado. Assim, apenas os membros do Blockchain podem adicionar, atualizar e verificar as informações. O sistema é governado por um conjunto de regras escritas em código e também armazenadas no BigchainDB. Essas regras definem como os usuários interagem com o sistema e como os dados são compartilhados entre eles.

ARTIIMoR possui um sistema de informações públicas e privadas que garante a segurança dos dados enquanto mantém a transparência. Em vez de usar apenas uma DLT, nosso projeto pretende conectar muitas redes de Distributed Ledger Technology e garantir que o sistema possa se comunicar tanto com redes DLT públicas quanto privadas. ARTIIMoR requer apenas um pequeno conjunto de características das DLTs escolhidas, portanto, ter uma solução genérica é vantajoso, pois o framework não precisa ficar restrito a uma Distributed Ledger Technology específica.

Swagatika et al. (Tabela 3.1 referência C) também propõem um modelo de Blockchain hierárquico em vários níveis para resolver possíveis problemas de escalabilidade (SAHOO et al., 2019). Cada nível mantém várias redes locais de Blockchain, onde cada uma registra atividades transacionais locais. Visões parciais são mantidas nos Blockchains no próximo nível da hierarquia. Isso torna o sistema suficientemente escalável, reduzindo as atividades em uma única rede. Essas visões também facilitam o controle do acesso a diferentes grupos de pessoas ou processos de acordo com seus direitos de acesso. Existem muitas situações em que os detalhes exatos dos dados podem não ser necessários.

Nesse modelo genérico, o número de níveis hierárquicos pode ser facilmente variado de acordo com as necessidades do aplicativo. Diferente do mo-

delo hierárquico proposto por Swagatika et al., nosso modelo tem foco no armazenamento de dados de mobilidade. Cada nova camada em nosso modelo está diretamente relacionada a uma estrutura de dados que um cliente deseja consultar no futuro. Portanto, o mecanismo de identificação e consolidação para a próxima camada está relacionado ao movimento dessa entidade.

De acordo com Ahmad et al. (Tabela 3.1 referência D), trilhas de auditoria baseadas em Blockchain fornecem um registro de eventos do sistema impulsionado por consenso que auxilia na criação de procedência em sistemas corporativos (AHMAD et al., 2019). Seu BlockTrail é uma nova arquitetura de Blockchain que pode corrigir problemas atuais, mantendo segurança e procedência. Eles dividem os sistemas de Blockchain legados em camadas de hierarquias co-dependentes, semelhante ao nosso conceito, reduzindo a complexidade de tempo e espaço e aumentando o rendimento. Transações envolvendo um grupo de organizações dentro de uma cidade são processadas e armazenadas separadamente das outras.

Um único razão para registro pode ser ineficiente e caro devido ao volume de transações criadas por esses aplicativos e às restrições de rendimento dos Blockchains atuais. Diante disso, eles acreditam que há uma necessidade crítica de uma nova arquitetura que possa resolver os problemas atuais sem sacrificar segurança e procedência. Assim, como uma solução escalável e eficaz para aplicativos de auditoria, o BlockTrail divide os sistemas de Blockchain existentes em camadas de hierarquias interconectadas, o que reduz a complexidade de tempo e espaço e aumenta o rendimento.

Eles apresentaram um protótipo baseado em Blockchain que utiliza o protocolo Practical Byzantine Fault Tolerance (PBFT), que é uma técnica de consenso possível para circunstâncias envolvendo Blockchains de consórcio em que é necessária um alto grau de consistência. No entanto, isso resulta em alto consumo de energia, baixa eficiência e baixa escalabilidade.

Seus testes revelaram que o BlockTrail é mais eficiente e tem uma pegada de armazenamento menor do que os Blockchains tradicionais. No entanto, diferente de nosso trabalho, eles não utilizam uma função de hash para produzir um hash do registro de dados a ser armazenado. Sua solução pode criar problemas de armazenamento em um curto período de tempo, devido ao volume de novos dados produzidos pelos serviços de IoT.

Brambilla, Amoretti e Zanichelli propõem uma abordagem para produzir um sistema de prova de localização (Tabela 3.1 referência E), que são certificados digitais que atestam a presença de alguém em uma área geográfica específica (BRAMBILLA; AMORETTI; ZANICHELLI, 2016). Os autores identificaram que as abordagens de verificação centralizada propostas no passado

não são satisfatórias, pois podem representar um alto risco para a privacidade do usuário.

Seu artigo ilustra um esquema completamente descentralizado baseado em Blockchain que garante a integridade da localização e preserva a privacidade do usuário. ARTIIMoR também compartilha a ideia de um sistema baseado em Blockchain para comprovar a localização de uma entidade. No entanto, ARTIIMoR não inclui e compartilha uma cadeia com os dados entre os nós, uma vez que o framework usa uma rede pública independente com as conexões do M-Hub.

Além disso, Brambilla, Amoretti e Zanichelli consideram uma rede peer-to-peer de Serviços Baseados em Localização (LBS) com nós móveis conectados à Internet e capazes de interagir com nós vizinhos por meio de comunicação Bluetooth de curto alcance. Em seu artigo, eles definem dois papéis para os nós na rede: provador e testemunha. Um provador é um nó que deseja coletar provas de localização de seus vizinhos, enquanto uma testemunha é um nó que forneceu prova de localização ao provador. Cada nó é descrito por um identificador único, sua chave pública e pode assinar digitalmente informações com a chave privada de seu identificador.

Tabela 3.1: Comparação de soluções similares com ARTIIMoR.

Solução	Confiável	Escalável	Rastreável
A	Compartilhado em uma rede local	Armazena todos os dados em uma rede local	Consulta na rede local
B	BigchainDB	Escala linearmente	Consulta no BigchainDB
C	Arquitetura de Blockchain com várias camadas	Armazena todos os dados em um Blockchain	Consulta no Blockchain
D	Arquitetura de Blockchain com várias camadas	Armazena todos os dados em um Blockchain	Consulta no Blockchain
E	Vulnerável a violações	Comunicação de curto alcance	Mesma informação em toda a rede
ARTIIMoR	Arquitetura de várias DLTs	Armazena hash de tamanho fixo	Identificador entre as camadas

Manter dados precisos é crucial para o uso efetivo e eficiente das informações. Dados imprecisos podem levar a erros e inconsistências, afetando a qualidade geral do trabalho. Priorizar o armazenamento confiável de dados pode evitar erros custosos e aumentar a produtividade. Para garantir que os dados sejam confiáveis, é necessário implementar medidas rigorosas de con-

trole de qualidade. A precisão dos dados armazenados é um aspecto crucial que merece uma elaboração mais detalhada nesta dissertação.

Pinho et al. se baseia na oportunidade de explorar as capacidades de visão computacional para melhorar a geolocalização, especialmente em ambientes urbanos muito densos, situações em que os sensores GPS perdem precisão (PINHO; CARVALHO; CARREIRA, 2015). Usando esse conhecimento no desenvolvimento de um protótipo de aplicativo capaz de resolver um problema existente em veículos de transporte: a falta de boa visão que um passageiro de transporte público tem para a paisagem exterior e a falta de acesso personalizado a informações sobre os pontos de interesse nessa paisagem.

Com essa abordagem, seria possível para um dispositivo conhecer sua posição relativa, mesmo em locais onde as informações do GPS não estão disponíveis, corrigindo alguns problemas conhecidos, como o posicionamento dentro de "desfiladeiros urbanos", onde as informações do GPS ficam indisponíveis por momentos, deixando os softwares de geolocalização sem pistas sobre sua posição

4

Arquitetura do Framework

Esta seção discutirá os detalhes do ARTIIMoR. O framework é uma combinação dos conceitos M-Hub da ContextNet e DLT, trabalhando juntos para armazenar de forma segura as interações entre objetos inteligentes. Utilizando o poder dessas duas tecnologias, o ARTIIMoR tem como objetivo fornecer um serviço confiável, escalonável e rastreável para registros de mobilidade. Para alcançar esse objetivo, o sistema foi cuidadosamente projetado para ser robusto e eficiente. Algoritmos avançados foram implementados para garantir o armazenamento seguro de dados e fácil acessibilidade, mantendo as informações do usuário privadas e preservando sua integridade.

4.1

Localização de Entidade Móvel com ContextNet

Esta dissertação é baseada no ContextNet (ENDLER; SILVA, 2018), um middleware distribuído cloud-mobile-edge composto por duas camadas principais: o **Core**, um conjunto extensível de microservices baseados em nuvem, como uma infraestrutura de comunicação peer-to-peer escalável e baseada em publicação/assinatura; e o **Mobile-Hub** (ou M-Hub) (TALAVERA et al., 2015), um framework de microservices extensível para dispositivos Android (como smartphones e sistemas em um chip (SoCs) de baixo custo).

O M-Hub é um dispositivo de borda que serve como um hub/repetidor de conectividade para dispositivos IoT de baixa potência próximos. Sua versão atual fornece conectividade à Internet para qualquer dispositivo Bluetooth Low Energy (BLE) dentro de seu alcance de comunicação. Ele também permite a descoberta, configuração e registro de qualquer beacon BLE usando a web ou um dispositivo móvel remoto.

Esses beacons BLE podem ser usados para detectar a presença de entidades móveis. Para melhorar a eficácia e a precisão desse processo, é importante comparar, filtrar, corrigir e resumir os sinais dos beacons. Para isso, o M-Hub suporta Complex Event Processing (LUCKHAM, 2001) por meio de uma ESPER Complex Event engine (TALAVERA; ENDLER; COLCHER, 2016) que pode processar consultas contínuas na forma de regras EPL sobre o fluxo de sinais de beacons que chegam.

Por fim, o ContextNet também suporta o posicionamento dessas entidades móveis usando geolocalizações, como Sistema de Posicionamento Global

(GPS) ou a posição da rede celular, e geocercas, polígonos convexos de coordenadas (lat, long) usados para mapear regiões de interesse.

4.2

Modelo de Rede DLT Multicamada

No mundo atual, onde o uso da tecnologia é generalizado, muitas indústrias estão aproveitando os benefícios da coleta de dados. No entanto, com o grande número de entidades monitoradas em cenários como entrega de alimentos ou aluguel de bicicletas, o processo de armazenar e gerenciar todos os dados coletados se torna um grande desafio em termos de escalabilidade. Isso ocorre porque a quantidade de dados gerados em um curto período de tempo pode ser esmagadora, e os métodos tradicionais de gerenciamento de dados podem não ser suficientes para lidar com isso. Em resumo, o desafio de armazenar e gerenciar dados é um desafio que requer inovação contínua e adaptação para acompanhar as necessidades em constante evolução da indústria. Trabalhos anteriores (LEAL; PISANI; ENDLER, 2021) apresentaram uma solução que armazena todas as informações de um período de interesse. Para obter insights desses dados, seria necessário acessar todos os registros e processar suas informações para agregá-las.

Além disso, a solução anterior não seria eficaz em grande escala devido à alta frequência de novas informações adicionadas ao DLT. Para resolver isso, o ARTIIMoR propõe melhorar o desempenho da implementação anterior utilizando uma arquitetura DLT multicamada. Este novo framework armazena um hash de tamanho fixo das entidades móveis, o que garante a precisão dos dados sem comprometer o desempenho do sistema, enquanto os dados reais são armazenados em um banco de dados.

O ARTIIMoR não impõe um tipo específico de banco de dados. O objetivo do framework é definir uma interface que possa ser usada tanto com bancos de dados relacionais quanto não relacionais (LI; GAI, 2021). Essa interface consiste em duas funções para os agentes do framework inserirem e removerem registros de mobilidade. Ao implementar o framework em um serviço, é importante escolher um modelo de armazenamento que melhor se adeque aos dados sendo armazenados. No entanto, recomendamos o uso de um banco de dados não relacional para serviços que requerem uma grande quantidade de dados, pois geralmente apresentam desempenho mais rápido do que os bancos de dados relacionais (UMA; SHRADDHA, 2010). Isso ocorre porque uma consulta não precisa acessar várias tabelas para fornecer uma resposta. Como a lógica dos relacionamentos dos dados está nas camadas, esse modelo pode ser o mais adequado para o framework.

O ARTIIMoR utiliza apenas os valores de hash para verificar a integridade dos dados quando necessário para evitar atrasos desnecessários. Embora um DLT específico possa fornecer maiores benefícios ao sistema, este framework não tem como objetivo definir um DLT específico a ser usado. É amplamente aceito que o sistema pode deixar de funcionar se uma rede específica for utilizada (SCHULTE et al., 2019). O objetivo principal é garantir que redes públicas e privadas possam se comunicar de forma eficaz com o sistema. O ARTIIMoR fornece apenas os requisitos essenciais para isso. A Figura 4.1 ilustra um exemplo de como essa arquitetura pode ser utilizada para armazenar dados de um sistema de entrega de alimentos, que registra a localização de todos os motoristas de entrega a cada minuto.

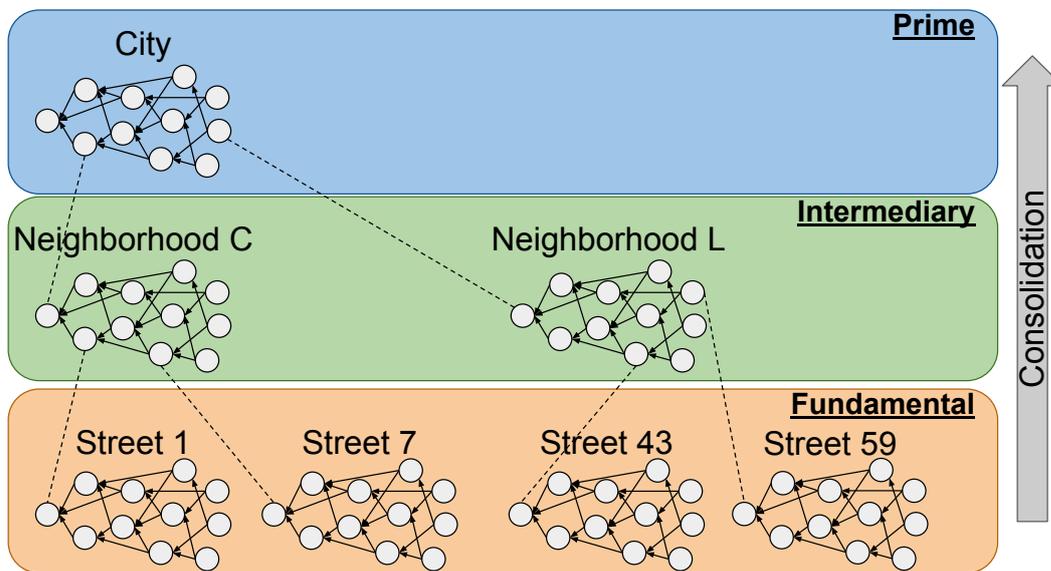


Figura 4.1: Exemplo de arquitetura DLT multicamada.

A primeira camada de DLT, conhecida como camada Fundamental, recebe hashes de todos os dados coletados. O ARTIIMoR consolida as informações periodicamente com base em um parâmetro específico, como o tempo (por exemplo, diariamente), o tamanho de uma região (por exemplo, uma rua) ou o número de nós (por exemplo, a cada 100 nós), entre outros. O ARTIIMoR, em seguida, armazena o hash desses dados consolidados na camada Intermediária, facilitando a validação da precisão dos dados agregados em consultas futuras. Por fim, o ARTIIMoR consolida os dados mais uma vez (por exemplo, mensalmente, por bairro ou a cada 10.000 nós). O hash desse resultado final é mantido em um único DLT na camada Prime, permitindo novamente uma rápida validação da precisão.

Nesse cenário, o ARTIIMoR pode armazenar as coordenadas geográficas da rua atual de cada motorista nos DLTs da camada Fundamental. A cada hora, ele pode consolidar esses dados para determinar o número de entregas

feitas em cada rua. O ARTIIMoR pode então armazenar o hash resultante no DLT da camada Intermediária correspondente ao bairro onde essa rua está localizada. Dessa forma, é possível verificar rapidamente se um número incomum de entregas em um local específico é devido a um aumento inesperado na demanda ou a um ataque de terceiros. No final do dia, o ARTIIMoR pode consolidar o número de entregas em cada bairro e armazenar o hash resultante no DLT da camada Prime. Esse hash pode então ser usado para certificar a precisão das estatísticas de uso mensais apresentadas a investidores e ao público.

Além disso, sempre que o ARTIIMoR adicionar nós aos DLTs nas camadas Intermediária ou Prime, é possível incluir referências ao DLT na camada inferior que contém os dados consolidados. Dessa forma, o ARTIIMoR terá um caminho que permite ao usuário acessar o hash das informações mais detalhadas, se assim o desejar. Como a confiabilidade é um dos principais aspectos desse sistema, os hashes não podem ser alterados ou removidos em nenhum nível de armazenamento. Devido a isso, esse framework precisa usar DLTs em cada camada do sistema de armazenamento.

4.3

Checkpoints

Como esta dissertação se concentra em agentes móveis dentro de um sistema em grande escala, pode não ser necessário ou viável registrar informações relacionadas a cada pequeno movimento. Além disso, coletar dados em intervalos regulares pode resultar em numerosos registros correspondentes à mesma posição devido ao congestionamento do tráfego.

Os checkpoints são locais com beacons BLE que podem representar uma região ou um local específico, dependendo do número de checkpoints na área. Quanto maior o número de pontos, mais específico cada um se torna. Nesse cenário, o ARTIIMoR pode determinar a posição do agente comparando sua localização geográfica (ou seja, suas coordenadas de GPS) com os limites da cerca geográfica formada pelos beacons. Usando essa abordagem, o ARTIIMoR pode monitorar o movimento dessas entidades móveis sempre que houver uma mudança significativa na posição. Por exemplo, esse framework pode especificar intervalos (por exemplo, 1, 5, 10 km) e armazenar as informações apenas quando uma entidade móvel se move de um intervalo para outro.

Do ponto de vista da estrutura de dados, cada ponto de verificação inclui um objeto que representa um registro de mobilidade. Este objeto possui uma estrutura consistente em todas as camadas e contém todas as informações necessárias para identificação, posicionamento, gerenciamento de acesso e

muito mais. Uma informação importante é o ID único atribuído a cada objeto, que é crucial para identificação e gerenciamento fácil. Além disso, há uma referência que auxilia nas permissões de acesso, garantindo que apenas clientes autorizados possam acessar os dados.

Além disso, o objeto também contém um subobjeto que armazena informações geográficas sobre a posição. Isso inclui dados importantes, como a localização precisa, a duração e as métricas ambientais. Além disso, há um argumento para representar a referência que conecta esses dados a um segmento ou trajeto específico. Essa referência é essencial para vincular facilmente o ponto de verificação a uma viagem ou rota específica. Em resumo, essa estrutura de objeto é crucial para garantir uma jornada segura e organizada, permitindo que o ARTIIMoR gerencie efetivamente os dados.

Usando nossa arquitetura multicamada, o ARTIIMoR pode armazenar hashes de checkpoints na camada Fundamental. Podemos então agrupar checkpoints para formar um segmento que representa o movimento entre os checkpoints A e B e armazenar o hash dessas informações consolidadas na camada Intermediária. Por sua vez, um ou mais segmentos formam uma trajetória, que representa o caminho completo de viagem do agente, e tem seu hash armazenado na camada Prime.

4.4

Fluxo de Inserção de Dados

Para compreender totalmente essa arquitetura de DLT em várias camadas, é necessário analisar de perto o sistema de inserção. Ele consiste em três processos: o Ledger Scheduler Process (LSP), o Mobility Observer Process (MOP) e o Generic Ledger Middleman Process (GLMP). Cada processo é crucial para manter a rastreabilidade e a segurança do sistema.

O M-Hub é responsável por identificar os beacons e estabelecer a posição da entidade móvel por meio de um filtro. Quando o M-Hub entra no sistema, ele realiza um handshake com o MOP. O Mobility Observer Process é projetado para monitorar a mobilidade das entidades. Esse processo é especialmente importante para observar todas as entidades e definir os segmentos em que estão. Sempre que o MOP identifica que o checkpoint está em uma nova região, ele envia um `idSegment` e um `idTrack` para o M-Hub. Em seguida, criamos uma estrutura composta pelo checkpoint, um timestamp, um `idTrack` e um `idSegment` e a enviamos para o LSP. O Ledger Scheduler Process é responsável por gerenciar a ordem em que as transações são processadas e registradas no razão. Ele recebe as transações recebidas e é responsável por enfileirar os hashes dos checkpoints das entidades móveis. Periodicamente, agregamos

esses checkpoints e enviamos o hash dos dados combinados para a camada Intermediária. No final de uma trilha, o ARTIIMoR agrega todos os dados correspondentes à camada Intermediária e armazena o hash respectivo na camada Prime.

Cada vez que o MOP cria um novo `idSegment`, ele envia o identificador antigo para o GLMP. O Generic Ledger Middleman Process atua como uma ponte entre o LSP e o MOP, garantindo que todas as transações sejam registradas e validadas corretamente. Esse processo é responsável por recuperar os checkpoints correspondentes à camada Fundamental e compilá-los em um segmento para a camada Intermediária. O MOP também envia o `idTrack` no final do caminho de uma entidade móvel. O GLMP é novamente responsável por recuperar os segmentos correspondentes à camada Intermediária e compilá-los em uma trilha para a camada Prime.

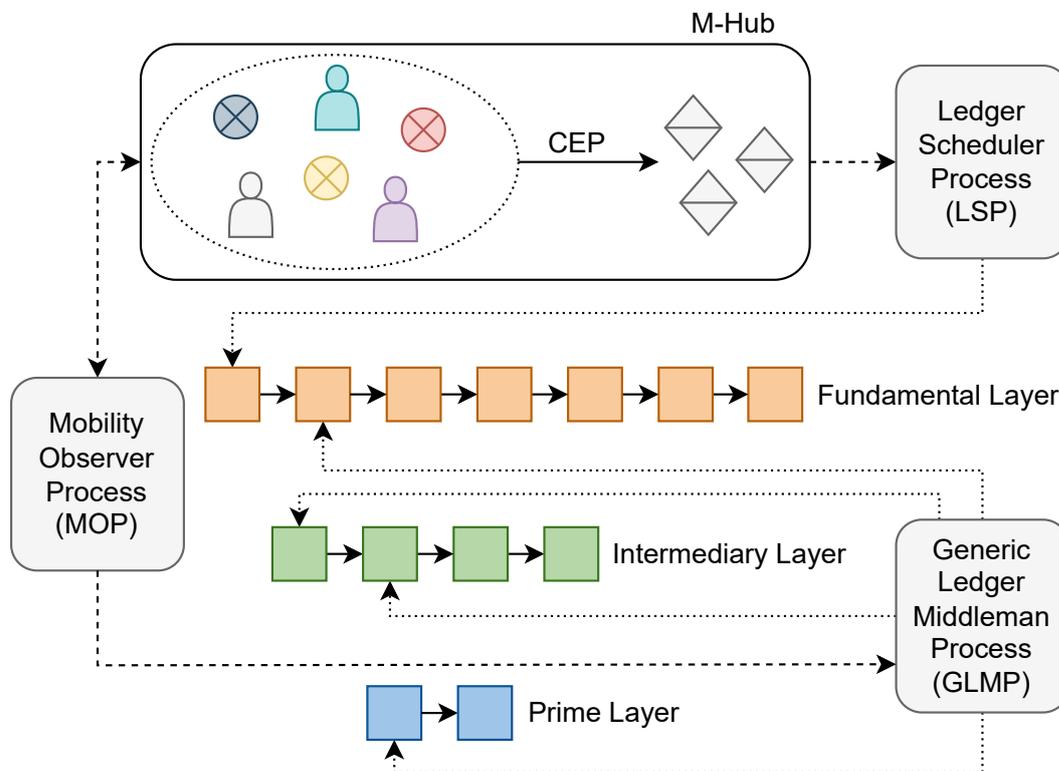


Figura 4.2: Diagrama detalhado de inserção.

O diagrama representado na Figura 4.2 é uma representação do complexo processo de inserção e de como ele se interrelaciona com nossos serviços. É importante reconhecer que o processo de inserção pode ser multifacetado e há inúmeros aspectos a serem considerados. Por exemplo, a natureza dos dados a serem inseridos, a magnitude dos dados e as camadas envolvidas podem afetar o desempenho do processo de inserção. No entanto, o diagrama nos fornece

uma visualização clara dos detalhes intrincados do processo, ajudando-nos a entender e otimizá-lo melhor.

4.5

Modelo de Busca de Dados

Como nosso sistema possui várias camadas, ele permite a busca de informações de acordo com o nível de abstração que o usuário requer. Para consultas mais gerais, eles podem pesquisar na camada Prime, enquanto para consultas detalhadas específicas, eles podem pesquisar na camada Fundamental.

Imagine uma empresa com vários armazéns (com produtos valiosos) espalhados por um grande pátio que contratou uma empresa de segurança para fazer rondas noturnas no campus. Nessas patrulhas, os seguranças precisam percorrer um caminho específico e visitar "checkpoints" específicos, que são registrados por meio do ARTIIMoR.

Devido ao tamanho grande do campus da empresa, eles só percebem o roubo (discreto) de um dos armazéns e o furto de muitos produtos caros muitos dias depois, e uma investigação sobre o que aconteceu começa. O detetive consulta a camada Prime para determinar se houve algum atraso nas rondas das noites anteriores e se todos os checkpoints foram visitados. Como resultado, eles identificam que três dias antes, as rondas das 3h e das 5h tiveram atrasos incomuns. A correspondência dos registros com seus hashes permite que o detetive valide rapidamente sua veracidade e prossiga com a investigação.

Em seguida, o detetive verifica mais detalhadamente os segmentos das rondas que se referem especificamente à localização do armazém onde ocorreu o roubo (essa informação corresponde à camada Intermediária). Eles percebem que esses segmentos contêm uma falta de conformidade com a qualidade de serviço de segurança estabelecida. Novamente, o detetive pode confiar na confiabilidade dos registros comparando-os com o hash imutável.

Por fim, eles analisam os detalhes de cada um dos segmentos (que correspondem à camada Fundamental). Eles descobrem que o segurança passou muito cedo no checkpoint das 3h, muito rápido no checkpoint das 4h (compensando depois com um atraso maior em outro checkpoint) e demorou muito para passar no checkpoint das 5h. O detetive agora pode usar essas evidências sólidas para interrogar o segurança.

Por meio dessa investigação, suportada pelos registros irrevogáveis do ARTIIMoR, o detetive foi capaz de concluir que o segurança da empresa de segurança não cumpriu as especificações do contrato e, assim, acabou facilitando a ação dos ladrões. Caso o detetive não pudesse verificar rapidamente a veracidade dos dados em cada nível, ele poderia ter seguido informações in-

corretas que teriam direcionado a investigação em uma direção completamente errada, desperdiçando tempo valioso.

4.6 Privacidade

O ARTIIMoR possui um sistema de informações público e privado para garantir a proteção de dados sem interferir em sua transparência. A transparência é um conceito fundamental para esse framework. No entanto, às vezes, a transparência dos dados não é desejável devido a preocupações com a privacidade. Por exemplo, o General Data Protection Regulation (GDPR) na Europa garante a todos o direito de revogar seu consentimento a qualquer momento e acessar ou excluir permanentemente todas as informações que eles concordaram previamente em compartilhar (LI; YU; HE, 2019). Isso levanta a questão de como isso se alinha com o registro permanente do Blockchain. O ARTIIMoR não foi criado para excluir dados armazenados. Uma vez que os dados foram adicionados ao banco de dados do framework, eles não podem ser removidos ou alterados.

Todos os dados têm uma relação com a entidade que os gerou, permitindo-nos controlar quem pode e quem não pode acessá-los. Como sua intenção é coletar dados tanto da localização geográfica quanto dos sensores incorporados, o framework possui informações em diferentes níveis de sensibilidade. É crucial proteger a identidade do usuário para evitar qualquer exposição potencial de informações sensíveis. Para abordar essa preocupação, o GLMP implementou um recurso que controla cuidadosamente o acesso aos dados. As informações menos sensíveis são exibidas para todos, mas as informações pessoais só podem ser visualizadas pelo emissor ou por um cliente autorizado. Esse recurso é baseado em um contrato inteligente, que fornece uma camada extra de proteção aos dados de seus usuários.

Além disso, o ARTIIMoR aprimora ainda mais as medidas de segurança controlando o acesso por meio do uso de IDs de dispositivos pessoais para identificar e armazenar entidades móveis. Quando a consulta é feita, o ARTIIMoR verifica se o cliente tem permissão ou é responsável pelos dados gerados. Esse sistema de autorização permite que um gerente visualize os dados de várias pessoas. Vinculamos o UID do gerente ao UID da entidade para que eles possam acessar as informações. O operador da entidade móvel define essas configurações de permissão e é o único que pode controlá-las.

4.7

Garantindo a Precisão dos Dados Armazenados

Quando se trata de armazenar dados, a precisão pode ser difícil de manter. No entanto, é importante encontrar uma solução que mantenha os dados armazenados confiáveis. Dados imprecisos podem gerar erros e inconsistências, o que pode afetar a qualidade geral do trabalho. Para garantir que as informações sejam usadas de maneira eficaz e eficiente, é crucial priorizar a precisão dos dados armazenados. Uma solução que garanta dados confiáveis evitará erros custosos e aumentará a produtividade. Com os avanços tecnológicos ao longo dos anos, surgiram novas tecnologias de geolocalização e as existentes se tornaram mais precisas, acessíveis e portáteis.

Hoje é possível encontrar sistemas de navegação GPS mais baratos e muito mais precisos e rápidos do que há uma década (DUNCAN; BADLAND; MUMMERY, 2009). Nosso objetivo é demonstrar que a localização geográfica pode ser mais precisa com a ajuda de outro sistema de localização, que adiciona valor às coordenadas lidas do sistema de posicionamento global, reduzindo o erro por meio de uma identificação de entidades móveis em quadros capturados. Ao combinar a conexão do checkpoint BLE com as informações do GPS, pode ser possível obter respostas mais conclusivas sobre a proximidade de uma posição bem conhecida, bem como detectar se o sistema já passou por essa posição ou não.

Sempre que a entidade móvel passa por um checkpoint, ela recebe a localização desse ponto e coleta sua geolocalização por meio de seu GPS interno. Antes de enviar as informações adiante, ela verifica e confirma sua localização. Se um dos sistemas falhar, ele usa o único método de localização geográfica identificado. Se ambos falharem, ele usa um modelo de tentativa até um tempo limite pré-definido. Com essa abordagem, um dispositivo pode conhecer sua posição relativa, mesmo em locais onde as informações do GPS não estão disponíveis, resolvendo problemas como o posicionamento dentro de desfiladeiros urbanos, onde as informações do GPS estão indisponíveis, deixando o software de geolocalização sem nenhuma informação sobre sua posição.

Essa abordagem melhora a confiabilidade dos dados, mas não resolve completamente os problemas de ordenação causados pela latência. Para garantir a consistência dos dados e a ordenação por nível, deve-se considerar a implementação de uma capacidade de Oracle para o Generic Ledger Middleman Process. O GLMP precisaria fazer uma suposição educada com base nos pontos que possui da camada mais baixa sempre que agrupa dados para uma camada superior.

5 Aplicações

Desenvolver um serviço confiável, escalável e rastreável para registros de mobilidade pode revolucionar várias indústrias. Por exemplo, os motoristas de entrega podem se beneficiar dessa tecnologia ao encontrar a melhor rota possível com base em fatores como qualidade do serviço de entrega, tráfego e condições do veículo e características dos itens entregues. Isso pode levar a tempos de entrega mais rápidos e maior satisfação do cliente. Da mesma forma, os proprietários de restaurantes também podem se beneficiar desse serviço ao garantir que as entregas de alimentos sejam feitas no prazo e nas melhores condições possíveis.

Além disso, o transporte de produtos sensíveis ao ambiente ou frágeis, como frutas, flores, animais ou medicamentos, pode ser vastamente melhorado adicionando informações relevantes aos pontos de dados geográficos. Essas informações podem incluir temperatura, umidade, luminosidade, leituras de acelerômetro, nome do condutor ou qualquer outra informação relevante de contexto/estado orientada para o transporte. Ao fornecer essas informações, os riscos de deterioração ou danos a esses produtos sensíveis podem ser drasticamente reduzidos, aumentando assim a eficiência geral e garantindo a satisfação do cliente. Em resumo, as possibilidades das ideias do ARTIIMoR são vastas e podem beneficiar grandemente várias indústrias.

5.1 Entrega de Alimentos

O negócio de entrega de refeições em restaurantes em casa está passando por mudanças rápidas, já que novas plataformas online correm para conquistar clientes em todo o mundo. O modelo tradicional de entrega continua sendo o mais comum (CHEN; HU; WANG, 2022). Nesse sistema, o consumidor faz um pedido no restaurante local e aguarda o restaurante levar a comida até a porta. No entanto, o surgimento da tecnologia digital está moldando o mercado, oferecendo acesso a vários restaurantes por meio de um único portal online. Empresas como DoorDash, GrubHub e UberEats são os três principais serviços de entrega de alimentos em restaurantes. Nesse mercado competitivo, conveniência e transparência podem definir os próximos grandes jogadores (CHAI; YAT, 2019). Com isso em mente, o ARTIIMoR permitirá que os jogadores e consumidores avaliem e verifiquem as condições de uso e os recursos do veículo. Isso permitirá que os motoristas provem que as melhores

rotas foram escolhidas, dadas as condições do veículo e sua carga.

Essas mudanças podem ajudar a melhorar o processo de entrega de alimentos. Embora atualmente existam aplicativos que auxiliam nessa tarefa, ainda é difícil acompanhar e ter um histórico preciso do caminho percorrido durante uma entrega (YEO; GOH; REZAEI, 2017). Além disso, a falta de informações detalhadas pode levar a atrasos na entrega, o que pode prejudicar tanto o motorista quanto o cliente.

Com as mudanças propostas, será possível ter um rastreamento mais preciso das entregas por meio de tecnologia avançada e sistemas de gerenciamento de entrega mais eficientes. Isso permitirá que os motoristas tenham acesso a informações detalhadas sobre o caminho percorrido, bem como os horários e locais de entrega. Além disso, será possível monitorar e avaliar o desempenho dos motoristas, o que pode ajudar a identificar áreas que precisam de melhorias e melhorar a eficiência geral do processo de entrega.

Essas mudanças também podem ajudar a melhorar a experiência do cliente, pois eles terão acesso a informações mais precisas e atualizadas sobre o status da entrega. Isso pode ajudar a reduzir atrasos, melhorar a satisfação do cliente e aumentar a fidelidade à marca. Em resumo, as mudanças propostas têm o potencial de transformar positivamente o setor de entrega de alimentos, tornando-o mais eficiente, seguro e confiável para todas as partes envolvidas.

5.2 Carsharing

O compartilhamento de carros se tornou um modo popular de transporte na Europa e está se espalhando para outras partes do mundo também (KATZEV, 2003). Na verdade, é uma forma conveniente e acessível de desfrutar de todos os benefícios de um veículo sem as complicações de possuir um. Os serviços de compartilhamento e aluguel de carros oferecem uma variedade de opções para os usuários, como retirada e devolução em locais diferentes ou no mesmo local. Hoje em dia, existem vários aplicativos que atuam como intermediários entre proprietários de carros e locatários, facilitando o cadastro e o registro de ambas as partes.

Uma das maiores vantagens do compartilhamento de carros é que ele é um sistema de transporte sustentável e uma alternativa ecológica (BARDHI; ECKHARDT, 2012). No entanto, é importante observar que o sucesso desse sistema depende da disponibilidade e qualidade do transporte público. Se o transporte público oferecer qualidades básicas, como conforto, segurança e abrangência, então o compartilhamento de carros pode ser uma solução eficaz e conveniente para os usuários.

Com isso em mente, o ARTIIMoR cria uma plataforma segura para proprietários de carros e consumidores compartilharem carros. Nossa infraestrutura permite que os motoristas provem que o carro está em boas condições e fornece informações sobre onde e por quanto tempo o carro foi conduzido. Além disso, nossos sistemas ajudam a criar uma comunidade de compartilhadores de carros comprometidos com a sustentabilidade e a redução da pegada de carbono.

5.3 Coleta de Lixo

Nas últimas décadas, houve um aumento no foco em alcançar metas específicas de reciclagem para resíduos domiciliares municipais (MOON, 1984). Alcançar esses objetivos pode ser uma tarefa complexa e desafiadora, pois há muitos fatores diferentes a serem considerados, como métodos de coleta, métodos de separação e a escolha entre sistemas de logística descentralizados ou centralizados.

Um dos maiores desafios na organização da melhor maneira de distribuir o sistema de coleta é lidar com a alta taxa de fraude que geralmente está associada a esse serviço (BOEHM; WEISER, 1988). Isso ocorre porque as informações de rota geralmente são relatadas por motoristas ou funcionários que ficam em pontos específicos, o que pode levar a imprecisões e inconsistências.

Uma solução potencial para esse problema é o uso do ARTIIMoR nos processos logísticos de coleta de lixo. Essa tecnologia pode ser usada para rastrear o movimento das várias entidades envolvidas no processo de coleta de resíduos, garantindo que a jornada e o tempo consumido durante as coletas individuais e todo o processo como um todo sejam precisos e corretos. Ao fornecer dados mais precisos sobre as rotas definidas, o ARTIIMoR pode ajudar a melhorar a eficiência da coleta de resíduos e identificar possíveis atrasos devido à ineficiência do trabalhador.

Além disso, ao fornecer aos clientes mais informações sobre a frequência da coleta e permitir que eles relatem quaisquer problemas com sua coleta, o ARTIIMoR pode ajudar a melhorar a satisfação geral do cliente e garantir que o lixo seja coletado de maneira pontual e eficiente. Por meio do sistema de 3 camadas, o ARTIIMoR tem a capacidade de agrupar e gerenciar eficientemente as diferentes rotas que o sistema de Coleta de Lixo possui dentro de bairros e ruas.

A arquitetura de 3 camadas do ARTIIMoR permite que os sistemas logísticos tenham uma arquitetura mais robusta e segura, sendo que cada camada é responsável por uma função específica e há a possibilidade de ter

mais de uma DLT em cada camada, garantindo assim a disponibilidade e confiabilidade do sistema. Em geral, o uso do ARTIIMoR na logística de coleta de lixo tem o potencial de melhorar significativamente a precisão e a eficiência do processo de gerenciamento de resíduos.

5.4

Cadeia de Suprimentos

Quando se trata de sistemas de Cadeia de Suprimentos, um dos desafios mais relevantes para alcançar eficiência operacional não está apenas relacionado à obtenção de dados em tempo real (STADTLER, 2014), mas também ao gerenciamento eficiente de entregas. Esse gerenciamento envolve um conjunto de processos complexos e interdependentes que, se não forem bem gerenciados, podem prejudicar a satisfação do cliente e as métricas do negócio. Nesse tipo de serviço, é comum enfrentar problemas relacionados à entrega fora do horário combinado com o entregador, o que pode gerar insatisfação para o cliente e até afetar sua fidelidade à marca. Portanto, é essencial que as empresas de Cadeia de Suprimentos estejam preparadas para lidar com essas situações e tenham processos bem definidos para gerenciar as entregas.

Além disso, os entregadores muitas vezes marcam a entrega como concluída ou como tentativa de entrega, mesmo que não tenham efetivamente realizado a entrega (TERZI; CAVALIERI, 2004). Esse tipo de situação pode gerar inconsistências nos dados e tornar o processo menos confiável. Para evitar esse tipo de problema, é importante que as empresas de Cadeia de Suprimentos implementem mecanismos de controle e auditoria para garantir que as entregas sejam feitas conforme o planejado e que os dados gerados sejam confiáveis e consistentes.

O ARTIIMoR tem a capacidade de lidar com um grande volume de dados e usuários, mantendo sempre alto desempenho e excelente qualidade de serviço. A arquitetura de 3 camadas fornece uma infraestrutura mais robusta e segura. Além disso, pode aprimorar o transporte de produtos sensíveis ao ambiente ou frágeis, como frutas, flores, animais ou medicamentos, incluindo informações pertinentes aos pontos de dados geográficos. Essas informações podem consistir em temperatura, umidade, luminosidade, leituras de acelerômetro, nome do condutor ou qualquer outra informação de contexto/estado orientada para o transporte.

Tabela 5.1: Caso de uso do ARTIIMoR.

Caso de Uso	Confiável	Escalável	Rastreável
Entrega de Alimentos	Validação de dados	Monitorar motoristas	Rastreamento por meio de Pontos de Verificação
Carsharing	Ambiente à prova de violações	Gerenciar usuários	Recuperar informações detalhadas
Coleta de Lixo	Precisão de localização por meio de Pontos de Verificação	Rastrear o movimento de várias entidades	Cada camada tem um objetivo específico
Cadeia de Suprimentos	Coletar vários sensores	Lidar com um grande volume de dados	Cada camada tem um objetivo específico

6

Resultados

Os experimentos descritos nesta seção têm como objetivo validar os conceitos apresentados nesta proposta, observando a eficiência de identificar a localização de uma entidade e enviar, adicionar e recuperar as informações armazenadas invioláveis. Os resultados reportados representam o tempo médio de transação de 30 execuções para cada DLT selecionada. Utilizamos o ContextNet versão 2.7 para a comunicação entre as entidades móveis e os checkpoints.

Ethereum (BUTERIN et al., 2014) é uma plataforma para criar aplicativos descentralizados usando contratos inteligentes em Solidity. Utilizamos o Ethereum Testnet para experimentar com novo código e soluções, sem nos preocuparmos com a quantidade de ETH que gastaríamos. Para usar o Testnet, criamos uma carteira e obtivemos tokens gratuitos para enviar um contrato inteligente em Solidity que adicionou novos dados e armazenou as informações. Com essa estrutura, enviamos dados de localização de forma assíncrona para a Blockchain.

IOTA (POPOV; LU, 2019) é uma DLT para aplicações IoT. Ele utiliza um DAG chamado Tangle em vez de blocos sequenciais. Para realizar uma transação, seu remetente deve aprovar e verificar duas transações anteriores. Os validadores são usuários que enviam ativos e precisam garantir que as transações aprovadas não estejam em conflito. Em nossos experimentos, enviamos informações para o IOTA Testnet oficial usando o SDK Java oficial.

Hyperledger Fabric (ANDROULAKI et al., 2018) é uma estrutura modular de Blockchain para desenvolver produtos, soluções e aplicativos baseados em Blockchain para empresas privadas. Implementamos uma rede de teste usando imagens e exemplos do Docker fornecidos no repositório fabric-samples, incluindo duas organizações de pares e uma organização de ordenação. Testamos nossos contratos inteligentes e aplicativos executando os nós da rede de teste em uma máquina local.

As implementações de exemplo desta estrutura armazenadas no GitHub foram usadas como base para esses experimentos: LSP (LEAL, 2022b), MOP (LEAL, 2022d) (LEAL, 2022c) e GLMP (LEAL, 2022a). É importante observar que esses repositórios não são uma representação exata do código utilizado durante o estudo. Foram feitos ajustes para adaptá-los aos dados de mobilidade e permitir a execução em um ambiente virtual usando contêineres Docker (POTDAR et al., 2020). Além disso, foram feitas melhorias adicionais

para otimizar o desempenho e a escalabilidade do sistema, garantindo que ele possa lidar com grandes volumes de dados de forma eficiente. Para armazenar os dados, utilizamos um banco de dados PostgreSQL (DRAKE; WORSLEY, 2002) também executado em um ambiente virtual usando contêineres Docker. Temos três tabelas, cada uma representando uma camada, e as colunas dessas tabelas representam o objeto definido para o checkpoint.

6.1

Experimentos de Desempenho de Inserção

As características de um sistema baseado em DLT podem melhorar a segurança e a transparência de soluções descentralizadas. Em vez de adotar uma única DLT, este projeto visa integrar várias redes de DLT e garantir que o sistema possa interagir com redes de DLT públicas e privadas. Ainda assim, há um conjunto mínimo de atributos que as DLTs empregadas precisam ter: alta disponibilidade, uma baixa taxa de hash (OZISIK; BISSIAS; LEVINE, 2017) e permitir a criação de um sistema de controle de acesso para os dados armazenados.

Considerando que as DLTs podem apresentar problemas de escalabilidade em termos de throughput, latência e capacidade quando confrontadas com grandes quantidades de dados em um ambiente de negócios real, decidimos estudar a latência de uma transação que insere um novo registro em três DLTs diferentes: Ethereum, IOTA e Hyperledger Fabric. Nesse primeiro experimento, utilizamos uma rede local de 280 megabits. Variamos o período de espera na fila que retém os hashes antes de enviá-los para a DLT, começando com dez mensagens e aumentando a quantidade para 1000 mensagens.

A partir do gráfico da Figura 6.1, podemos ver que enquanto o tempo médio de transação do IOTA e do Fabric cresce aproximadamente linearmente com o número de mensagens (ajustes lineares com inclinações de 0,96 e 0,84, respectivamente, $R^2 > 0,95$), o do Ethereum permaneceu aproximadamente constante (ajuste linear com inclinação de 0,04, $R^2 > 0,95$).

Em um estudo inicial sobre Blockchain multilayer (LEAL; PISANI; ENDLER, 2022), realizamos um teste na rede Ethereum com inserção assíncrona. A Figura 6.1 mostra um resultado quase constante (ajuste linear com inclinação de 0,04, $R^2 > 0,95$) para todas as quantidades de mensagens. Isso proporciona uma vantagem significativa ao acelerar o processo de envio de dados. No entanto, essa abordagem não garante que os dados tenham sido armazenados e que não encontraríamos problemas de ordem. Um bloco de mensagem pode levar mais tempo do que seu sucessor. Portanto, a confirmação de armazenamento é necessária para garantir que os dados tenham sido armazenados e

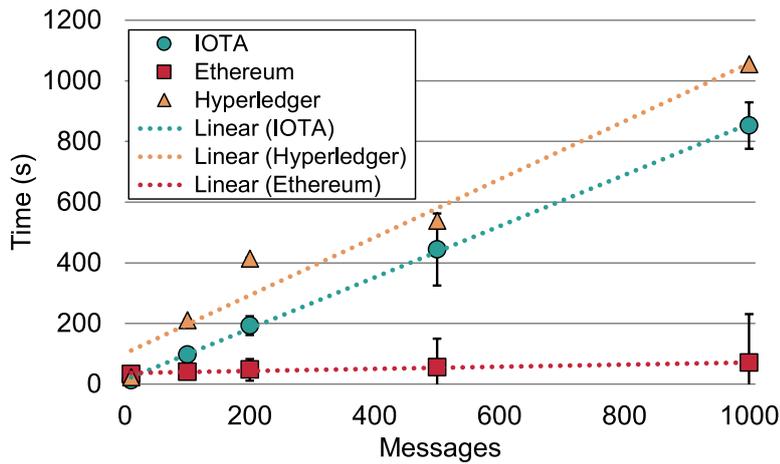


Figura 6.1: Comparação entre número de mensagens e tempo de inserção.

possam ser recuperados na ordem correta posteriormente, se necessário.

Para garantir a confiabilidade dos resultados, criamos um modelo de espera para a confirmação do envio, que consiste em aguardar a confirmação do armazenamento dos dados antes de prosseguir para o próximo envio. Isso nos permitiu comparar as redes Ethereum sob a mesma perspectiva: envio ordenado com confirmação de armazenamento. Dessa forma, pudemos validar a ordem dos dados e garantir a integridade dos resultados. A partir do gráfico da Figura 6.2, podemos ver que o tempo médio de transação de todas as redes cresce aproximadamente linearmente com o número de mensagens.

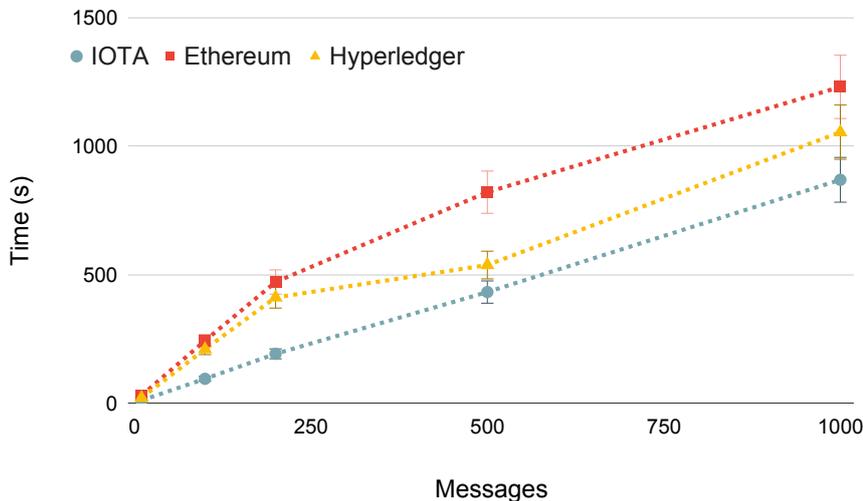


Figura 6.2: Comparação entre número de mensagens e tempo de inserção após ajustar o modelo de inserção do Ethereum.

Esses resultados verificam que todas as DLTs observadas têm operações de inserção eficientes e são adequadas para as ideias do ARTIIMoR, com resultados de tempo de inserção diferentes dependendo das características da

rede. Variar a frequência das transações permite que as redes enviem grandes quantidades de mensagens em grupo sem degradar o tempo de transação.

Além disso, é importante destacar que o uso de várias DLTs é uma das principais vantagens da estrutura. Por meio do modelo de interface, podemos garantir a compatibilidade com várias Distributed Ledger Technology. Como resultado, podemos dizer que o modelo é altamente genérico e não possui um forte vínculo com um ledger específico. Vale ressaltar que esse recurso aumenta a usabilidade do sistema, uma vez que diferentes DLTs atendem a diferentes requisitos de desempenho e segurança. Além disso, várias DLTs podem ser usadas dentro da mesma hierarquia, combinando suas características específicas para alcançar a solução mais eficiente. Portanto, a capacidade de integrar várias Distributed Ledger Technology é uma vantagem que a estrutura oferece e a diferencia na implementação das funções necessárias de forma mais eficiente e flexível.

Com base em nossos testes de desempenho de inserção, pode parecer que o IOTA é a abordagem mais adequada para casos com muitas mensagens concorrentes. No entanto, outros fatores além do desempenho devem ser considerados ao escolher as DLTs para nossa arquitetura multilayer, como o custo. Cada transação no Ethereum, por exemplo, precisa de "ether" para ser realizada, o que pode se tornar bastante caro. Além disso, há uma preocupação com a energia. À medida que a capacidade de processamento atinge novos patamares, isso também leva a um maior consumo de energia. O efeito dessas redes no meio ambiente deve ser levado em consideração, uma vez que desejamos que nossos sistemas sejam energeticamente eficientes e sustentáveis no mundo real. Portanto, nos experimentos seguintes, utilizamos o segundo melhor resultado e solução mais eficiente em termos de energia (IOTA, 2021), a rede IOTA.

6.2

Experimentos do Modelo de Inserção

No nosso segundo experimento, decidimos examinar alguns possíveis modelos de inserção. Definimos os dois modelos mais comuns: Tamanho Fixo e Geofences. Na primeira abordagem, o MOP contabiliza o número de pontos de verificação e só cria um segmento quando atinge um tamanho pré-definido. Acreditamos que isso pode ser útil em percursos longos onde a rota não tem desvios sutis. O segundo modelo usa barreiras geográficas predefinidas para criar os segmentos. O MOP segue o movimento e compara as Geofences definidas com as posições anteriores e atuais. Ao atravessar uma cerca, o sinal é enviado para o GLMP para criar um novo segmento. Acreditamos que este

é um modelo apropriado para cenários onde a região geográfica tem uma forte relação com as consultas futuras.

Para gerar o gráfico da Figura 6.3, calculamos o tempo de inserção de cada camada combinando o próprio tempo de inserção com o tempo gasto consultando os dados na camada inferior para gerar um novo registro agregado para a camada superior. Utilizamos 100 mensagens por transação e comparamos o desempenho de armazenar todos os dados nas DLTs (Dados Completos) com o desempenho de armazenar apenas o seu hash (Hash).

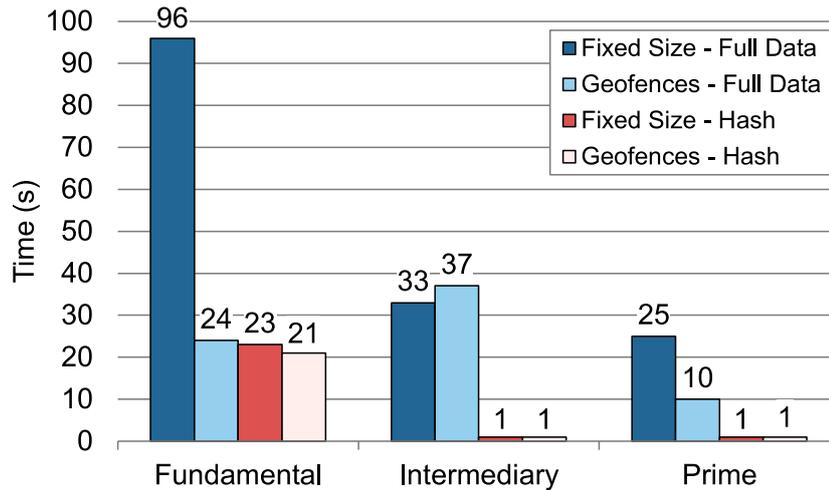


Figura 6.3: Comparação do modelo de inserção entre Geofences e Tamanho Fixo.

Como podemos ver, no caso dos Dados Completos, o modelo de Tamanho Fixo apresenta uma diminuição no tempo da camada mais baixa para a camada mais alta. Por outro lado, o tempo para Geofences não diminui à medida que se move para níveis hierárquicos superiores. O aumento no tempo para a Camada Intermediária de Geofences pode estar relacionado a uma discrepância no tempo de consulta.

A função hash utilizada nos testes de Hash mapeia nossos dados de tamanho variável para itens de dados de tamanho fixo pequeno, tornando o pacote carregado menor e mais fácil de armazenar. Isso resultou em tempos de transmissão 83% mais curtos e 70% mais curtos do que os Dados Completos nas abordagens de Geofences e Tamanho Fixo, respectivamente. A consulta e a compilação dos dados também se tornaram mais rápidas com essa solução. Além disso, o desempenho de propagar as informações da camada Fundamental para a camada Prime também foi melhor. Assim, o modelo Hash é mais eficiente do que os Dados Completos, pois envia partes menores de dados para a rede e permite a comparação mais fácil de valores.

Após validar as vantagens do modelo Hash, também decidimos medir o esforço no envio e encapsulamento das informações. Comparamos o processo de consolidação de mensagens em um único hash com diferentes quantidades de mensagens. Executamos testes com 10, 100, 200, 500 e 1000 mensagens e observamos que o aumento no tempo de processamento teve um crescimento suave de 1,16s para 1,68s. Como o hash tem um tamanho padrão, podemos assumir que esse aumento se deve ao processo de consolidação e, portanto, essa implementação pode consolidar grandes quantidades de dados.

6.3 Experimentos de Desempenho de Consulta

No nosso terceiro experimento, simulamos o desempenho de consulta em cada uma das três camadas. Para facilitar a comparação de um sistema multinível, utilizamos a DLT IOTA em todas as camadas.

Suponhamos que queiramos coletar as informações de mobilidade de um motorista de transporte compartilhado. Grandes empresas desse setor têm restrições quanto ao número de horas trabalhadas por dia. Por exemplo, uma delas sugere que se faça uma pausa após passar 12 horas trabalhando (UBER, 2022).

Se um motorista trabalha o tempo máximo todos os dias em uma semana, e nosso sistema coleta os dados de mobilidade dessa pessoa a cada minuto, isso geraria 5040 mensagens. Para simplificar, suponhamos que um novo segmento seja criado a cada hora e uma nova trajetória seja gerada ao final de cada dia. Isso geraria 168 segmentos e 7 trajetórias em uma semana. Então, poderíamos realizar uma consulta em cada camada para identificar a posição mais recente dessa pessoa. O gráfico na Figura 6.4 ilustra o desempenho desse tipo de consulta nos casos em que todos os dados são armazenados nas DLTs (Dados Completos) ou apenas o hash é armazenado (Hash).

No caso dos Dados Completos, o tempo de resposta na Camada Prime com 7 nós é 12,3 vezes mais rápido do que o tempo de resposta na Camada Fundamental com 5040 nós. No entanto, para a implementação do Hash, a diferença entre os tempos de consulta na Prime e na Fundamental é apenas de 1,9 vezes. Esse pequeno ganho de desempenho pode ser explicado pelo fato de que o Hash apresenta tempos de consulta muito mais rápidos devido ao mapeamento dos dados de tamanho variável para dados de tamanho fixo pequeno (a variação nos resultados está principalmente relacionada ao tempo de reversão do hash). Vemos que os tempos de consulta do Hash ficam abaixo de 1,5s mesmo para 200.000 mensagens (5,16 vezes mais rápido do que os Dados Completos).

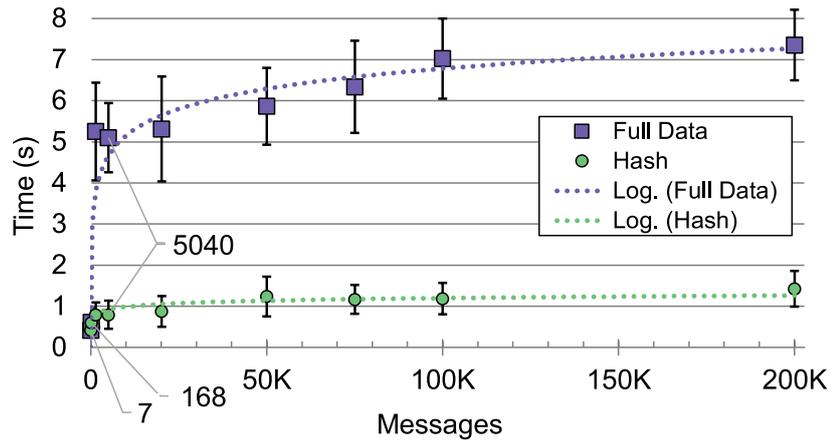


Figura 6.4: Comparação entre mensagens e tempo de consulta.

Por fim, quando aumentamos o número de mensagens além de 1000, observamos que a diferença no tempo de consulta entre as camadas começa a diminuir, mesmo para os Dados Completos, pois os valores de tempo de consulta têm uma tendência de crescimento logarítmico ($R^2 > 0,89$). Esse comportamento logarítmico pode ser atribuído à implementação do IOTA como um DAG, o que torna as buscas mais rápidas do que as DLTs implementadas como uma Blockchain. Ainda assim, mesmo nesses cenários, a arquitetura multinível das DLTs melhoraria a resposta das consultas fornecendo informações consolidadas.

7

Conclusão

Esta dissertação discute a necessidade de um serviço confiável, escalável e rastreável para registros de mobilidade. A ARTIIMoR apresenta uma estrutura para implementá-lo usando um sistema DLT de várias camadas como um serviço central do middleware ContextNet, aproveitando suas capacidades de Processamento de Eventos Complexos na borda (ou seja, os M-Hubs) e na nuvem (ou seja, o Núcleo).

O desempenho desse tipo de serviço é essencial para a viabilidade de aplicativos de rastreamento de mobilidade do mundo real em ambientes externos, onde grandes quantidades de dados são coletados com alta frequência. Portanto, os experimentos avaliam a eficiência de tarefas como armazenamento e recuperação de informações invioláveis. Destacamos que, embora armazenar dados em um DLT tenha o potencial de alta latência, existem maneiras de evitar interrupções de tempo de transação no fluxo de novos dados, como mantê-los em um sistema DLT de várias camadas.

Nossos resultados mostram que é possível utilizar o DLT IOTA para obter tempos rápidos de inserção e consulta em um sistema de três camadas, onde a camada mais baixa (Fundamental) armazena hashes de todos os dados coletados e as camadas superiores (Intermediária e Prime) armazenam hashes calculados a partir de informações cada vez mais consolidadas. Um DLT específico pode beneficiar mais o sistema, no entanto, o projeto não está interessado em definir um específico para ser usado. Acreditamos que o sistema pode parar de funcionar no futuro se uma rede for definida para ser usada. O objetivo é garantir que tanto redes públicas quanto privadas possam se comunicar com o sistema. Testar várias situações com diferentes DLTs é interessante. Utilizaremos as Blockchains previamente estudadas (Ethereum, IOTA, Hyperledger) para a análise subsequente em cada uma das camadas.

A fila configurável na Camada Fundamental do ARTIIMoR permite o gerenciamento do atraso da mensagem antes do envio. Em um ambiente onde o acesso à Internet é escasso, esse sistema pode ter um impacto negativo no atraso geral do envio de mensagens (e registro de dados), pois as mensagens podem ficar retidas. Até agora, o framework assume que todos os nós móveis estão disponíveis durante todo o período. Sabemos que no mundo real é improvável que essas entidades estejam conectadas. Focar em analisar soluções onde falhas são possíveis cria um grande desafio de causalidade. Nesse caso, o processo de armazenamento e até mesmo o envio entre mensagens será afetado,

uma vez que a ordem das informações é fundamental para consultas futuras. Estudaremos possíveis soluções para detectar falhas nesse processo.

Para detectar a proximidade de uma posição conhecida e se o agente móvel já passou por essa posição, a ARTIIMoR combina conexões de pontos de verificação BLE com informações de GPS. A entidade móvel recebe a localização de cada ponto de verificação e coleta sua geolocalização via GPS. A localização é validada cruzando antes de ser enviada. Se um sistema falhar, assume o outro. Se ambos falharem, ele tenta novamente até um tempo limite. Essa abordagem permite que um dispositivo conheça sua posição relativa, mesmo onde o GPS não está disponível, resolvendo problemas como posicionamento dentro de Canyons Urbanos. No entanto, isso não resolve problemas de latência que causam problemas de ordenação. Para resolver isso, uma capacidade de Oracle para o GLMP deve ser desenvolvida. Isso garante consistência de dados e classificação nível por nível, fazendo suposições educadas com base em pontos da camada mais baixa.

A estrutura ARTIIMoR garante proteção e transparência de dados, mas a natureza permanente do Blockchain levanta preocupações com privacidade. A estrutura implementa uma funcionalidade baseada em contratos inteligentes para controlar o acesso a informações pessoais e aprimora as medidas de segurança usando IDs de dispositivo pessoais. Embora eficiente em cenários básicos de permissão, melhorias devem ser consideradas para estudos futuros. Com o aumento da sofisticação dos ataques cibernéticos, estudos aprofundados são cruciais para garantir a segurança de sistemas e dados críticos.

Ao analisar cada segmento da Camada Fundamental, a ARTIIMoR tem como objetivo aprofundar-se nos detalhes. Ao realizar simulações, será possível testar não apenas a inserção e consulta de dados armazenados, mas também verificar a consistência dos dados em uma escala maior. Através desta dissertação, esperamos obter uma melhor compreensão de como os componentes da Camada Fundamental interagem entre si e como podemos otimizá-los para melhor desempenho. Em última análise, nosso objetivo é fornecer uma plataforma que possa apoiar o crescimento e a evolução dos negócios de nossos clientes, ao mesmo tempo em que garante a segurança e privacidade de seus dados.

Referências bibliográficas

AHMAD, A. et al. Blocktrail: A scalable multichain solution for blockchain-based audit trails. In: **ICC 2019 - 2019 IEEE International Conference on Communications (ICC)**. [s.n.], 2019. p. 1–6. Disponível em: <<https://ieeexplore.ieee.org/document/8761448>>.

ANDERSON, L. et al. **New kids on the block: an analysis of modern blockchains**. 2016. Accessed: 2016-07-04. Disponível em: <<http://arxiv.org/pdf/1606.06530.pdf>>.

ANDROULAKI, E. et al. Hyperledger fabric: A distributed operating system for permissioned blockchains. In: **EuroSys**. [s.n.], 2018. ISBN 9781450355841. Disponível em: <<https://dl.acm.org/doi/10.1145/3190508.3190538>>.

BARDHI, F.; ECKHARDT, G. M. Access-based consumption: The case of car sharing. **Journal of consumer research**, Oxford University Press, v. 39, n. 4, p. 881–898, 2012. Disponível em: <<https://academic.oup.com/jcr/article/39/4/881/1798309>>.

BENČIĆ, F. M.; ŽARKO, I. P. Distributed ledger technology: Blockchain compared to directed acyclic graph. In: **2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)**. [s.n.], 2018. p. 1569–1570. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8416434>>.

BOEHM, H.-J.; WEISER, M. Garbage collection in an uncooperative environment. **Software: Practice and Experience**, Wiley Online Library, v. 18, n. 9, p. 807–820, 1988. Disponível em: <<https://dl.acm.org/doi/10.1145/512429.512449>>.

BOUOYOUR, J.; SELMI, R. Ether: Bitcoin's competitor or ally? **arXiv preprint arXiv:1707.07977**, 2017. Disponível em: <https://www.researchgate.net/publication/318635518_Ether_Bitcoin's_competitor_or_ally>.

BRAMBILLA, G.; AMORETTI, M.; ZANICHELLI, F. Using Block Chain for Peer-to-Peer Proof-of-Location. **arXiv preprint arXiv:1607.00174**, Jul. 2016. Disponível em: <<https://arxiv.org/pdf/1607.00174.pdf>>.

BUTERIN, V. et al. **A Next-Generation Smart Contract and Decentralized Application Platform**. 2014. Accessed: May 01, 2022. Disponível em: <<https://ethereum.org/whitepaper>>.

CAPOCASALE, V.; PERBOLI, G. Standardizing smart contracts. **IEEE Access**, IEEE, v. 10, p. 91203–91212, 2022. Disponível em: <<https://ieeexplore.ieee.org/document/9869650>>.

CASTRO, M.; LISKOV, B. Practical byzantine fault tolerance and proactive recovery. **ACM Trans. Comput. Syst.**, Association for Computing Machinery, New York, NY, USA, v. 20, n. 4, p. 398–461, nov 2002. ISSN 0734-2071. Disponível em: <<https://doi.org/10.1145/571637.571640>>.

- CHAI, L. T.; YAT, D. N. C. Online food delivery services: Making food delivery the new normal. **Journal of Marketing advances and Practices**, v. 1, n. 1, p. 62–77, 2019. Disponível em: <https://www.researchgate.net/publication/334050513_Online_Food_Delivery_Services_Making_Food_Delivery_the_New_Normal>.
- CHEN, M.; HU, M.; WANG, J. Food delivery service and restaurant: Friend or foe? **Management Science**, v. 68, n. 9, p. 6539–6551, 2022. Disponível em: <<https://doi.org/10.1287/mnsc.2021.4245>>.
- CLACK, C. D.; BAKSHI, V. A.; BRAINE, L. **Smart Contract Templates: foundations, design landscape and research directions**. 2016. Accessed: 2017-01-10. Disponível em: <<https://arxiv.org/pdf/1608.00771v2.pdf>>.
- DRAKE, J. D.; WORSLEY, J. C. **Practical PostgreSQL**. [S.l.]: "O'Reilly Media, Inc.", 2002.
- DUNCAN, M. J.; BADLAND, H. M.; MUMMERY, W. K. Applying gps to enhance understanding of transport-related physical activity. **Journal of Science and Medicine in Sport**, Elsevier, v. 12, n. 5, p. 549–556, 2009. Disponível em: <<https://www.sciencedirect.com/science/article/abs/pii/S1440244008002107>>.
- ELROM, E. Hyperledger. In: _____. **The Blockchain Developer: A Practical Guide for Designing, Implementing, Publishing, Testing, and Securing Distributed Blockchain-based Projects**. Berkeley, CA: Apress, 2019. p. 299–348. ISBN 978-1-4842-4847-8. Disponível em: <https://doi.org/10.1007/978-1-4842-4847-8_8>.
- ENDLER, M.; SILVA, F. S. E. Past, present and future of the contextnet iomt middleware. **Open J. Internet Things**, v. 4, p. 7–23, 2018. Disponível em: <<https://api.semanticscholar.org/CorpusID:51689202>>.
- GALLERSDÖRFER, U.; MATTHES, F. Tamper-proof volume tracking in supply chains with smart contracts. In: SPRINGER. **Euro-Par 2018: Parallel Processing Workshops: Euro-Par 2018 International Workshops, Turin, Italy, August 27-28, 2018, Revised Selected Papers 24**. 2019. p. 367–378. Disponível em: <https://link.springer.com/chapter/10.1007/978-3-030-10549-5_29>.
- GERVAIS, A. et al. On the security and performance of proof of work blockchains. In: **Proceedings of the 2016 ACM SIGSAC conference on computer and communications security**. [s.n.], 2016. p. 3–16. Disponível em: <<https://dl.acm.org/doi/10.1145/2976749.2978341>>.
- GEYER, F. et al. Performance perspective on private distributed ledger technologies for industrial networks. In: IEEE. **2019 International Conference on Networked Systems (NetSys)**. 2019. p. 1–8. Disponível em: <<https://ieeexplore.ieee.org/document/8854512>>.
- GIANNOTTI, F.; PEDRESCHI, D. Mobility, data mining and privacy - geographic knowledge discovery. In: **Mobility, Data Mining and Privacy**. [s.n.], 2008. Disponível em: <<https://api.semanticscholar.org/CorpusID:1145948>>.

GUEGAN, D. Public Blockchain versus Private blockchain. abr. 2017. Documents de travail du Centre d'Economie de la Sorbonne 2017.20 - ISSN : 1955-611X. Disponível em: <<https://shs.hal.science/halshs-01524440>>.

HUANG, J. et al. Survey on blockchain incentive mechanism. In: **ICPCSEE**. [s.n.], 2019. Disponível em: <<https://api.semanticscholar.org/CorpusID:203470296>>.

IOINI, N. E.; PAHL, C. A review of distributed ledger technologies. In: **OTM Conferences**. [s.n.], 2018. Disponível em: <<https://api.semanticscholar.org/CorpusID:53014631>>.

IOTA. **Energy Benchmarks for the IOTA Network**. 2021. Accessed: May 01, 2022. Disponível em: <<https://blog.iota.org/internal-energy-benchmarks-for-iota/>>.

IQBAL, M.; MATULEVIČIUS, R. Comparison of blockchain-based solutions to mitigate data tampering security risk. In: SPRINGER. **Business Process Management: Blockchain and Central and Eastern Europe Forum: BPM 2019 Blockchain and CEE Forum, Vienna, Austria, September 1–6, 2019, Proceedings 17**. 2019. p. 13–28. Disponível em: <https://link.springer.com/chapter/10.1007/978-3-030-30429-4_2>.

IRRESBERGER, F.; JOHN, K.; SALEH, F. The public blockchain ecosystem: An empirical analysis. **Other Information Systems & eBusiness eJournal**, 2020. Disponível em: <<https://api.semanticscholar.org/CorpusID:213138568>>.

JEON, K. E. et al. Ble beacons for internet of things applications: Survey, challenges, and opportunities. **IEEE Internet of Things Journal**, IEEE, v. 5, n. 2, p. 811–828, 2018. Disponível em: <<https://ieeexplore.ieee.org/document/8242361>>.

KATZEV, R. Car sharing: A new approach to urban transportation problems. **Analyses of social issues and public policy**, Wiley Online Library, v. 3, n. 1, p. 65–86, 2003. Disponível em: <<https://doi.org/10.1111/j.1530-2415.2003.00015.x>>.

KUMAR, B. A. et al. A bluetooth low energy based beacon system for smart short range surveillance. In: IEEE. **2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)**. 2016. p. 1181–1184. Disponível em: <<https://ieeexplore.ieee.org/document/7808018>>.

LEAL, M. **Atlas**. [S.l.]: GitHub, 2022. <https://github.com/matheusroleal/atlas>.

LEAL, M. **Blockchain Scheduler**. [S.l.]: GitHub, 2022. <https://github.com/matheusroleal/blockchain-scheduler>.

LEAL, M. **Kelpie API**. [S.l.]: GitHub, 2022. <https://github.com/kelpie-tracker/kelpie-api>.

LEAL, M. **Kelpie Processing Node**. [S.l.]: GitHub, 2022. <https://github.com/kelpie-tracker/kelpie-processing-node>.

LEAL, M.; PISANI, F.; ENDLER, M. Inviolable presence registration of mobile entities in the contextnet middleware (short paper). In: **2019 9th Latin-American Symposium on Dependable Computing (LADC)**. [s.n.], 2019. p. 1–4. Disponível em: <<https://ieeexplore.ieee.org/document/8995684>>.

LEAL, M.; PISANI, F.; ENDLER, M. A blockchain-based service for inviolable presence registration of mobile entities. **JBCS**, v. 27, p. 1:1–1:15, 2021. ISSN 1678-4804. Disponível em: <<https://journal-bcs.springeropen.com/articles/10.1186/s13173-021-00104-y>>.

LEAL, M.; PISANI, F.; ENDLER, M. A multilayer distributed ledger technology architecture for immutable registry of mobility and location information. In: **2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain)**. [s.n.], 2022. p. 1–6. Disponível em: <<https://ieeexplore.ieee.org/document/10087097>>.

LI, C.; MIROSA, M.; BREMER, P. Review of online food delivery platforms and their impacts on sustainability. **Sustainability**, v. 12, n. 14, 2020. ISSN 2071-1050. Disponível em: <<https://www.mdpi.com/2071-1050/12/14/5528>>.

LI, C.; PALANISAMY, B. Comparison of decentralization in dpos and pow blockchains. In: SPRINGER. **Blockchain–ICBC 2020: Third International Conference, Held as Part of the Services Conference Federation, SCF 2020, Honolulu, HI, USA, September 18-20, 2020, Proceedings 3**. 2020. p. 18–32. Disponível em: <<https://arxiv.org/abs/2002.02082>>.

LI, H.; YU, L.; HE, W. **The impact of GDPR on global technology development**. Taylor & Francis, 2019. 1–6 p. Disponível em: <<https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1569186>>.

LI, J.; GAI, R. Survey of performance comparison based on non relational database. In: **2021 IEEE 23rd Int Conf on High Performance Computing Communications; 7th Int Conf on Data Science Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud Big Data Systems Application (HPCC/DSS/SmartCity/DependSys)**. [s.n.], 2021. p. 2278–2282. Disponível em: <<https://ieeexplore.ieee.org/document/9781213>>.

LIU, D.; CAMP, L. J. Proof of work can work. In: CITESEER. **WEIS**. 2006. Disponível em: <https://www.researchgate.net/publication/228929310_Proof_of_work_can_work>.

LUCKHAM, D. C. **The Power of Events: An Introduction to Complex Event Processing in Distributed Enterprise Systems**. Addison-Wesley Longman Publishing Co., Inc., 2001. ISBN 0201727897. Disponível em: <https://www.researchgate.net/publication/221343017_Luckham_DC_The_Power_of_Events_An_Introduction_to_Complex_Event_Processing_in_Distributed_Enterprise_Systems_Addison-Wesley_Longman>.

MARIJAN, D.; LAL, C. Blockchain verification and validation: Techniques, challenges, and research directions. **Computer Science Review**, Elsevier, v. 45, p. 100492, 2022. Disponível em: <<https://www.sciencedirect.com/science/article/abs/pii/S1574013722000314>>.

- MOHANTY, D.; MOHANTY, D. Ethereum use cases. In: **Ethereum for Architects and Developers: With Case Studies and Code Samples in Solidity**. Springer, 2018. p. 203–243. Disponível em: <<https://link.springer.com/book/10.1007/978-1-4842-4075-5>>.
- MOON, D. A. Garbage collection in a large lisp system. In: **Proceedings of the 1984 ACM Symposium on LISP and Functional Programming**. [s.n.], 1984. p. 235–246. Disponível em: <<https://dl.acm.org/doi/pdf/10.1145/800055.802040>>.
- NAKAMOTO, S. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008. Accessed: 2015-07-01. Disponível em: <<https://bitcoin.org/bitcoin.pdf>>.
- NOFER, M. et al. Blockchain. **Business & Information Systems Engineering**, Springer, v. 59, p. 183–187, 2017. Disponível em: <<https://www.springer.com/journal/12599>>.
- NOSOUHI, M. et al. Blockchain for secure location verification. **JPDC**, v. 136, p. 40–51, 2020. Disponível em: <<https://www.sciencedirect.com/science/article/abs/pii/S074373151930320X>>.
- OZISIK, A. P.; BISSIAS, G.; LEVINE, B. N. Estimation of miner hash rates and consensus on blockchains (draft). **CoRR**, abs/1707.00082, 2017. Disponível em: <<http://arxiv.org/abs/1707.00082>>.
- PINHO, F.; CARVALHO, A.; CARREIRA, R. Improving geolocation by combining gps with image analysis. In: _____. **Geoinformatics for Intelligent Transportation**. Cham: Springer International Publishing, 2015. p. 213–225. ISBN 978-3-319-11463-7. Disponível em: <https://doi.org/10.1007/978-3-319-11463-7_15>.
- POPOV, S.; LU, Q. IOTA: feeless and free. **IEEE Blockchain Technical Briefs**, 2019. Disponível em: <<https://blockchain.ieee.org/technicalbriefs/january-2019/iota-feeless-and-free>>.
- POTDAR, A. M. et al. Performance evaluation of docker container and virtual machine. **Procedia Computer Science**, v. 171, p. 1419–1428, 2020. ISSN 1877-0509. Third International Conference on Computing and Network Communications (CoCoNet'19). Disponível em: <<https://www.sciencedirect.com/science/article/pii/S1877050920311315>>.
- RASHINKAR, P.; PATERSON, P.; SINGH, L. **System-on-a-chip Verification: Methodology and Techniques**. Springer Science & Business Media, 2007. Disponível em: <<https://link.springer.com/book/10.1007/b116428>>.
- RAUCHS, M. et al. Distributed ledger technology systems: A conceptual framework. **Available at SSRN 3230013**, 2018. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3230013>.
- SAHOO, S. et al. A hierarchical and abstraction-based blockchain model. **Appl. Sci.**, v. 9, n. 11, 2019. ISSN 2076-3417. Disponível em: <<https://www.mdpi.com/2076-3417/9/11/2343>>.

SALEH, F. Blockchain without Waste: Proof-of-Stake. **The Review of Financial Studies**, v. 34, n. 3, p. 1156–1190, 07 2020. ISSN 0893-9454. Disponível em: <<https://doi.org/10.1093/rfs/hhaa075>>.

SCHULTE, S. et al. Towards blockchain interoperability. In: SPRINGER. **Business Process Management: Blockchain and Central and Eastern Europe Forum: BPM 2019 Blockchain and CEE Forum, Vienna, Austria, September 1–6, 2019, Proceedings 17**. 2019. p. 3–10. Disponível em: <https://link.springer.com/chapter/10.1007/978-3-030-30429-4_1>.

SHAHAAB, A. et al. Applicability and appropriateness of distributed ledgers consensus protocols in public and private sectors: A systematic review. **IEEE access**, IEEE, v. 7, p. 43622–43636, 2019. Disponível em: <<https://ieeexplore.ieee.org/document/8672572>>.

SOLTANI, R. et al. Distributed ledger technologies and their applications: A review. **Applied Sciences**, v. 12, n. 15, 2022. ISSN 2076-3417. Disponível em: <<https://www.mdpi.com/2076-3417/12/15/7898>>.

STADTLER, H. Supply chain management and advanced planning—basics, overview and challenges. **European Journal of Operational Research**, v. 163, n. 3, p. 575–588, 2005. ISSN 0377-2217. Supply Chain Management and Advanced Planning. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S0377221704001183>>.

STADTLER, H. Supply chain management: An overview. **Supply chain management and advanced planning: Concepts, models, software, and case studies**, Springer, p. 3–28, 2014. Disponível em: <https://link.springer.com/chapter/10.1007/978-3-540-74512-9_2>.

STEPHEN, R.; ALEX, A. A review on blockchain security. In: IOP PUBLISHING. **IOP conference series: materials science and engineering**. 2018. v. 396, n. 1, p. 012030. Disponível em: <https://www.researchgate.net/publication/327298944_A_Review_on_BlockChain_Security>.

SUHARTANTO, D. et al. Loyalty toward online food delivery service: the role of e-service quality and food quality. **Journal of Foodservice Business Research**, v. 22, p. 81 – 97, 2018. Disponível em: <<https://api.semanticscholar.org/CorpusID:158502509>>.

SUNYAEV, A.; SUNYAEV, A. Distributed ledger technology. In: **Internet computing: Principles of distributed systems and emerging internet-based technologies**. Springer, 2020. p. 265–299. Disponível em: <<https://link.springer.com/book/10.1007/978-3-030-34957-8>>.

TALAVERA, L. E.; ENDLER, M.; COLCHER, S. An energy-aware iot gateway, with continuous processing of sensor data. In: **Proc. SBRC**. [s.n.], 2016. Disponível em: <<https://www-di.inf.puc-rio.br/~endler/paperlinks/SBRC-Talavera-2016.pdf>>.

TALAVERA, L. E. et al. The mobile hub concept: Enabling applications for the internet of mobile things. In: **PerCom Workshops**. [s.n.], 2015. p. 123–128. Disponível em: <<https://ieeexplore.ieee.org/document/7134005>>.

- TERZI, S.; CAVALIERI, S. Simulation in the supply chain context: a survey. **Computers in industry**, Elsevier, v. 53, n. 1, p. 3–16, 2004. Disponível em: <<https://www.sciencedirect.com/science/article/abs/pii/S0166361503001040>>.
- TIAN, F. A supply chain traceability system for food safety based on HACCP, blockchain & internet of things. In: **ICSSSM**. [s.n.], 2017. p. 1–6. Disponível em: <<https://ieeexplore.ieee.org/document/7996119>>.
- UBER. **Introducing a new feature: Driving Hours Limit**. 2022. Accessed: May 01, 2022. Disponível em: <<https://www.uber.com/blog/driving-hours-limit>>.
- UMA, B.; SHRADDHA, J. Moving towards non-relational databases. **International Journal of Computer Applications**, v. 1, 02 2010. Disponível em: <https://www.researchgate.net/publication/43763817_Moving_Towards_Non-Relational_Databases>.
- VASCONCELOS, R. O.; SILVA, L. D. N.; ENDLER, M. Towards Efficient Group Management and Communication for Large-Scale Mobile Applications. In: **PER-COM Workshops**. [s.n.], 2014. p. 551–556. Disponível em: <<https://ieeexplore.ieee.org/document/6815266>>.
- VESTERGAARD, C.; BOBOSHA, H. A.; LANGFELDT, K. Distributed ledger technology: beyond the hype. **Blockchain for International Security: The Potential of Distributed Ledger Technology for Nonproliferation and Export Controls**, Springer, p. 7–22, 2021. Disponível em: <https://link.springer.com/chapter/10.1007/978-3-030-86240-4_2>.
- WANG, S. et al. An overview of smart contract: architecture, applications, and future trends. In: IEEE. **2018 IEEE Intelligent Vehicles Symposium (IV)**. 2018. p. 108–113. Disponível em: <<https://ieeexplore.ieee.org/document/8500488>>.
- WANG, W. et al. A survey on consensus mechanisms and mining strategy management in blockchain networks. **Ieee Access**, IEEE, v. 7, p. 22328–22370, 2019. Disponível em: <<https://ieeexplore.ieee.org/document/8629877>>.
- YEO, V. C. S.; GOH, S.-K.; REZAEI, S. Consumer experiences, attitude and behavioral intention toward online food delivery (ofd) services. **Journal of Retailing and Consumer Services**, v. 35, p. 150–162, 2017. ISSN 0969-6989. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S0969698916302855>>.
- YU, Z.; LIU, X.; WANG, G. A survey of consensus and incentive mechanism in blockchain derived from p2p. **2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)**, p. 1010–1015, 2018. Disponível em: <<https://api.semanticscholar.org/CorpusID:67865468>>.
- ZHANG, R.; XUE, R.; LIU, L. Security and privacy on blockchain. **ACM Computing Surveys (CSUR)**, v. 52, p. 1 – 34, 2019. Disponível em: <<https://api.semanticscholar.org/CorpusID:81980629>>.
- ZHAO, K. et al. Urban human mobility data mining: An overview. **2016 IEEE International Conference on Big Data (Big Data)**, p. 1911–1920, 2016. Disponível em: <<https://api.semanticscholar.org/CorpusID:5864808>>.

ZHENG, Z. et al. An overview of blockchain technology: Architecture, consensus, and future trends. **2017 IEEE International Congress on Big Data (BigData Congress)**, p. 557–564, 2017. Disponível em: <<https://api.semanticscholar.org/CorpusID:29591273>>.

ZILE, K.; STRAZDINA, R. Blockchain use cases and their feasibility. **Applied Computer Systems**, v. 23, p. 12 – 20, 2018. Disponível em: <<https://api.semanticscholar.org/CorpusID:67351626>>.

ZOU, W. et al. Smart contract development: Challenges and opportunities. **IEEE Transactions on Software Engineering**, v. 47, p. 2084–2106, 2021. Disponível em: <<https://api.semanticscholar.org/CorpusID:204087135>>.