Instituto de Computação

GT-Padlock

Garantindo Privacidade e Proteção de Dados Pessoais Usando Aprendizado e Desaprendendo de Máquina em cima de uma Solução de Blockchain de Camada 2

Antonio "Guto" Rocha
arocha@ic.uff.br

Instituto de Computação

GT-Padlock

Equipe: UFF+UFES

Rodolfo Villaça, Arthur Vianna, João Paulo Gonçalves, Rayan Lima, Marcos Paulo Mendes, Thiago Arruda, Adriano Busson, Vicente Ferran e Victor Teles

Antonio "Guto" Rocha

arocha@ic.uff.br

Instituto de Computação

Antes de eu começar ....

Antonio "Guto" Rocha
arocha@ic.uff.br


Instituto de
Computação
uff


67 Professores
~ 2000 estudantes

Universidade Federal Fluminense

Pós-Graduação em

Computação

MESTRADO E DOUTORADO

EXCELÊNCIA EM PESQUISA

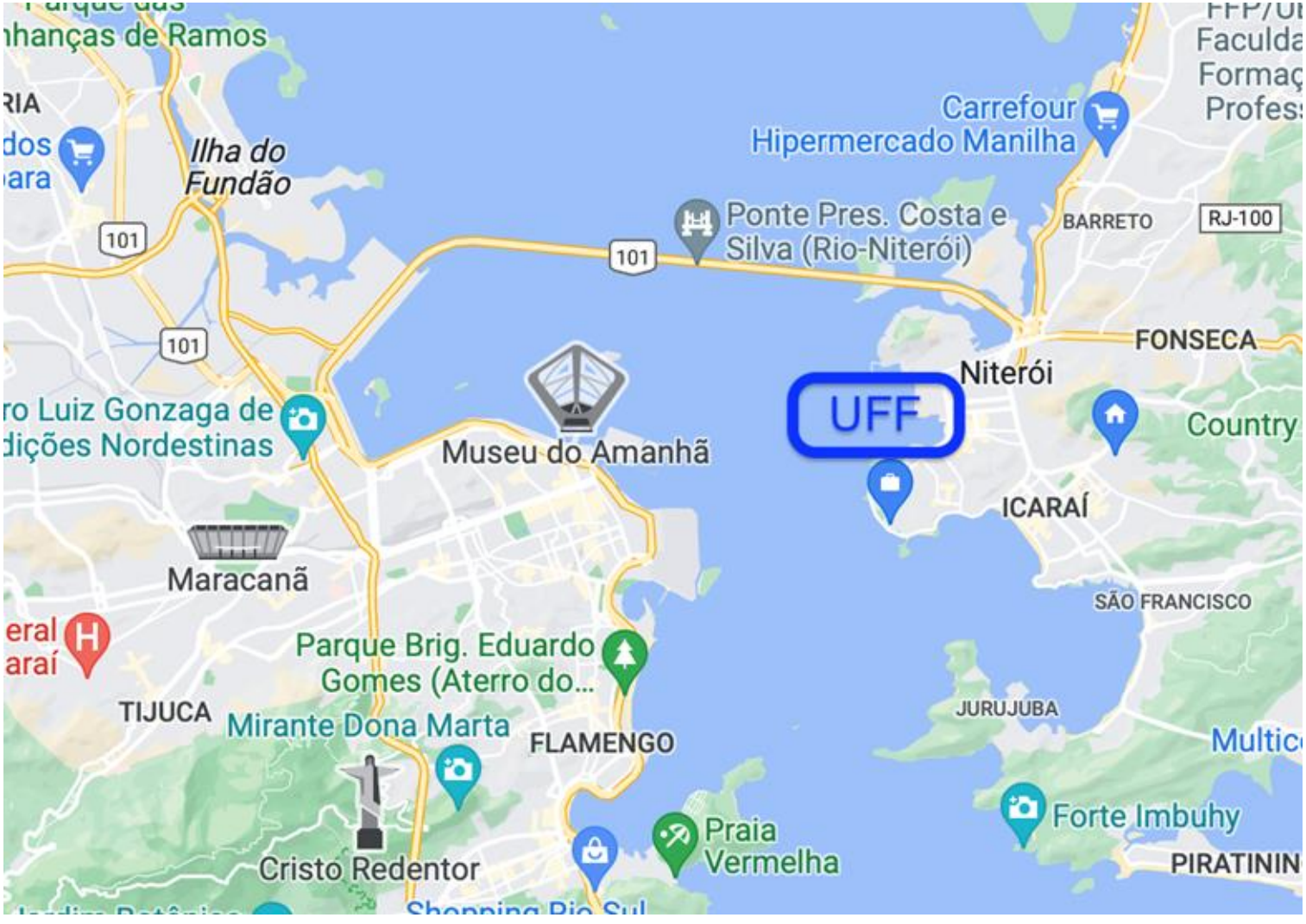
Instituto de Computação

ic.uff.br

CAPES

CONCEITO 7

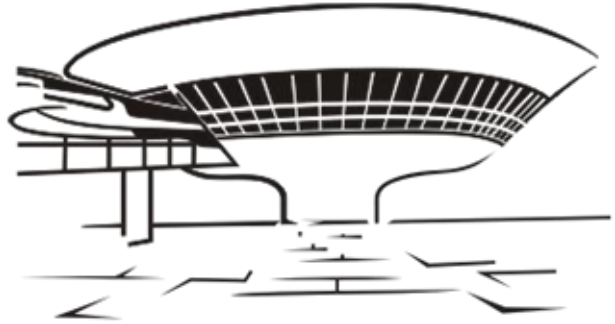
★ ★ ★ ★ ★ ★ ★


Carrefour Hipermercado Manilha
Ponte Pres. Costa e Silva (Rio-Niterói)
BARRETO
RJ-100
Ilha do Fundão
101
101
101
FONSECA
Niterói
UFF
Country
ro Luiz Gonzaga de dições Nordestinas
Museu do Amanhã
ICARAÍ
Maracanã
SÃO FRANCISCO
Parque Brig. Eduardo Gomes (Aterro do...
TIJUCA
Mirante Dona Marta
FLAMENGO
JURUJUBA
Forte Imbuhy
Praia Vermelha
Cristo Redentor
PIRATININ

NITERÓI

500k população

6° IDH no Brasil
1° no estado do RJ




Ótima Infraestrutura


Venham nos visitar!

Instituto de Computação

Agora, vamos falar do que mais interessa ….

Antonio "Guto" Rocha
arocha@ic.uff.br

Instituto de Computação

Agora, vamos falar do que mais interessa ….

GT-Padlock!

Antonio "Guto" Rocha
arocha@ic.uff.br

Dilema do Mundo Moderno!

Compartilhar ou não usar o serviço?

Dilema do Mundo Moderno!

Compartilhar ou não usar o serviço?

- Fornecer dados pessoais x serviços online
- Ameaça a privacidade das informações

Dilema do Mundo Moderno!

Compartilhar dados ou não usar o serviço?

- Fornecer dados pessoais x serviços online
- Ameaça a privacidade das informações
- Regulamentações ajudam a lidar com o problema
  - LGPDs e o "direito a ser esquecido"

Mas, o que significa “esquecer os dados”?

Mas, o que significa “esquecer os dados”?

- Regulamentações que visam a privacidade dos dados

1. Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia
   - O artigo 17 define o “direito a ser esquecido”, aplicada sempre que os dados pessoais são processados, o que inclui o seu recolhimento, transformação, consulta ou eliminação, dentro ou fora da União Europeia (UE), bastando que os dados digam a respeito a um residente da UE [Veale et al. 2018].
2. Lei de Privacidade do Consumidor da Califórnia (CCPA)
   - Estabelece que os usuários devem ter o direito de apagar os seus dados e informações relacionadas para proteger a sua privacidade.

Mas, o que significa “esquecer os dados”?

3. Lei Geral de Proteção de Dados (LGPD)
   - Edição da Lei 13.709/2018
   - Coloca o indivíduo como protagonista das relações jurídicas que envolvam o tratamento de dados
   - Elege como fundamento em seu art. 2º, II, a “autodeterminação informativa”, que confere a pessoa o direito de escolher quais dados serão usados, bem como os limites e o prazo de sua utilização.

Mas, o que significa “esquecer os dados”?

Mas, o que significa “esquecer os dados”?

Qual a efetividade do simples apagamento?

Mas, o que significa “esquecer os dados”? Qual a efetividade do simples apagamento?

- Os dados são utilizados para o treinamento de modelos de aprendizado de máquinas.
- A eliminação dos dados de um usuário podem ser suficientes para impedir que influenciem a formação de modelos futuros, mas não elimina a influência dos dados nos modelos existentes.

Mas, o que significa “esquecer os dados”? Qual a efetividade do simples apagamento?

- Segurança em IA
  - Os modelos de IA são vulneráveis a ataques
    - ✓ Envenenamento de modelos
    - ✓ Manipulação do modelo treinado
    - ✓ Vazamento de Informação de Treinamento

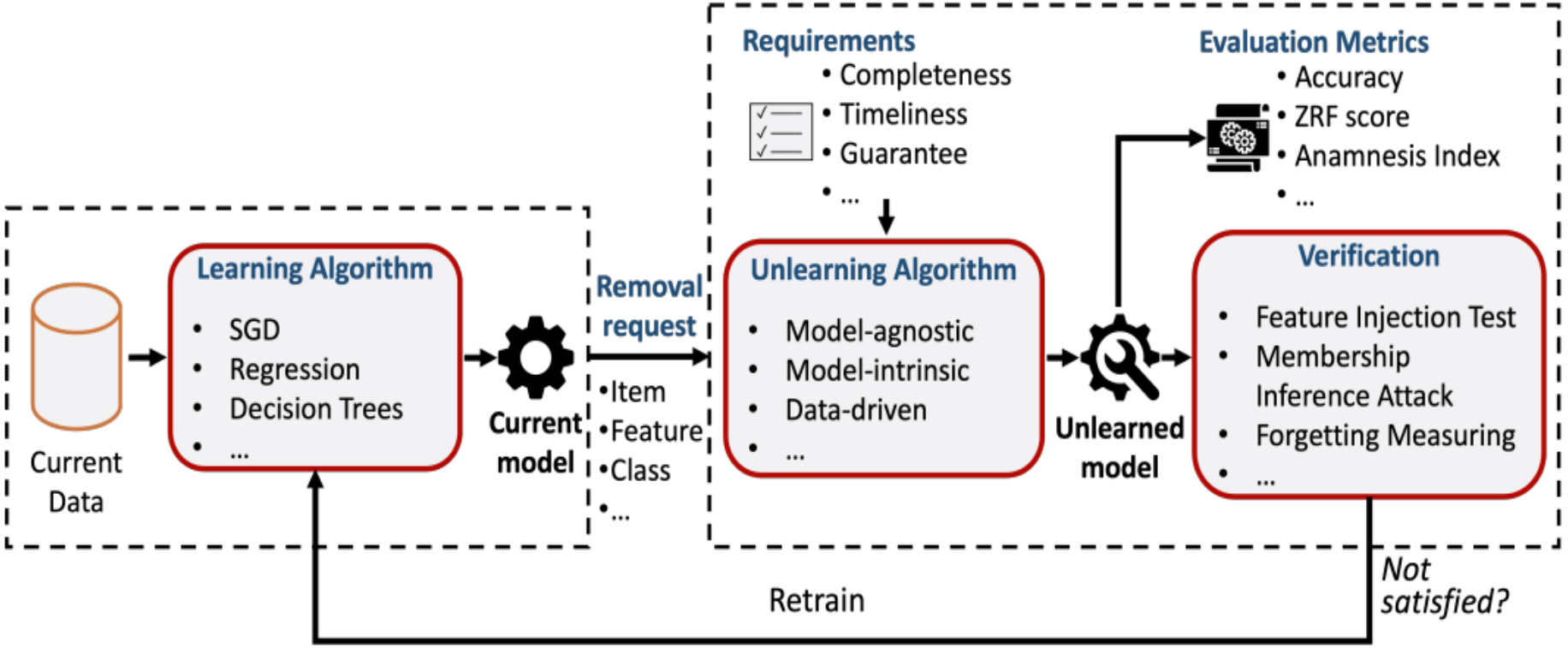
Como fazer para lidar conciliar o "esquecimento dos dados" vs Treinamento de Modelos?

- Solução ingênua:
  - Retreinar os modelos a cada remoção?
    - ✓ Alto custo computacional

Eis que surge o conceito Desaprendizado de Máquina (DM)!

- Do termo em inglês, Machine Unlearning (MU).
- Processo de remover seletivamente a influência de dados específicos nos modelos treinados

Workflow do processo de DM



Perguntas fundamentais do projeto GT-Padlock:

Perguntas fundamentais do projeto GT-Padlock:

P1: Como garantir que modelos de Inteligência Artificial (IA) treinados com dados revogados estejam em conformidade com a LGPD?

Perguntas fundamentais do projeto GT-Padlock:

P1: Como garantir que modelos de Inteligência Artificial (IA) treinados com dados revogados estejam em conformidade com a LGPD?

Usando algoritmos de Desaprendizado de Máquina!

Perguntas fundamentais do projeto GT-Padlock:

P1: Como garantir que modelos de Inteligência Artificial (IA) treinados com dados revogados estejam em conformidade com a LGPD?

P2: Como garantir que os algoritmos AM utilizados sejam, de fato, os declarados pela empresa, com base nos dados do usuário?

Perguntas fundamentais do projeto GT-Padlock:

P1: Como garantir que modelos de Inteligência Artificial (IA) treinados com dados revogados estejam em conformidade com a LGPD?

P2: Como garantir que os algoritmos AM utilizados sejam, de fato, os declarados pela empresa, com base nos dados do usuário?

Perguntas fundamentais do projeto GT-Padlock:

P1: Como garantir que modelos de Inteligência Artificial (IA) treinados com dados revogados estejam em conformidade com a LGPD?

P2: Como garantir que os algoritmos AM utilizados sejam, de fato, os declarados pela empresa, com base nos dados do usuário?

Fazendo o controle em uma Blockchain!

GT-Padlock: Objetivos

Garantindo Privacidade e Proteção de Dados Pessoais Usando Aprendizado e Desaprendendo de Máquina em cima de uma Solução de Blockchain de Camada 2

GT-Padlock: Objetivos

Garantindo Privacidade e Proteção de Dados Pessoais Usando Aprendizado e Desaprendendo de Máquina em cima de uma Solução de Blockchain de Camada 2

(i) o desenvolvimento de uma interface (API) de integração ao projeto Iliada de uma das principais soluções de Blockchain de camada 2 existentes, a Cartesi;

GT-Padlock: Objetivos

Garantindo Privacidade e Proteção de Dados Pessoais Usando Aprendizado e Desaprendendo de Máquina em cima de uma Solução de Blockchain de Camada 2

(i) o desenvolvimento de uma interface (API) de integração ao projeto Iliada de uma das principais soluções de Blockchain de camada 2 existentes, a Cartesi;

(ii) a implementações de algoritmos de DM dentro de máquinas Cartesi, que são executados na forma de contratos inteligentes de camada 2, à partir de chamadas da Blockchain principal do projeto Iliada;

GT-Padlock: Objetivos

Garantindo Privacidade e Proteção de Dados Pessoais Usando Aprendizado e Desaprendendo de Máquina em cima de uma Solução de Blockchain de Camada 2

(i) o desenvolvimento de uma interface (API) de integração ao projeto Iliada de uma das principais soluções de Blockchain de camada 2 existentes, a Cartesi;

(ii) a implementações de algoritmos de DM dentro de máquinas Cartesi, que são executados na forma de contratos inteligentes de camada 2, à partir de chamadas da Blockchain principal do projeto Iliada;

(iii) o desenvolvimento de uma Prova de Conceito (PoC) de DApp que faz uso do arcabouço como solução para o uso de modelos de AM, com a garantia de conformidade com as leis de proteção de dados, com a remoção dos dados e esquecimento por parte dos modelos, de forma confiável através da segurança da Blockchain e de forma escalável com a execução em camada 2

NitBus, NitBike ...

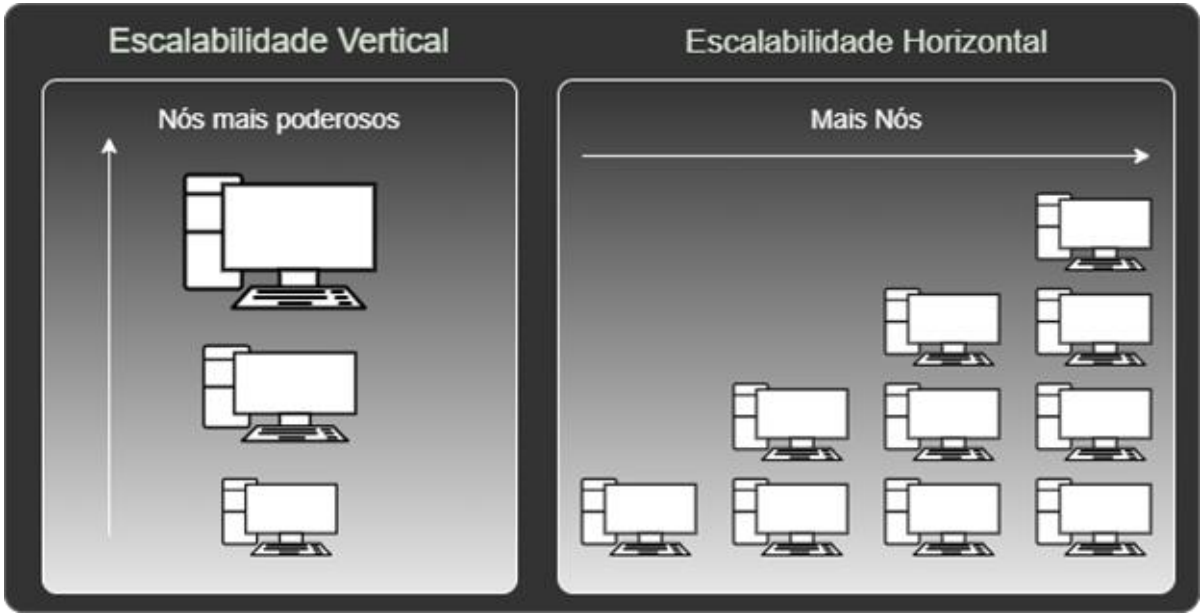
Já ouviu falar em Rollups?

Já ouviu falar em Rollups?
E na Cartesi?

Problema de Escalabilidade na Blockchain

Escalabilidade: Diz respeito à capacidade de um sistema crescer, tendo como intenção atender mais usuários ou adicionar mais funcionalidades. Sendo assim, um sistema é dito escalável quando o seu desempenho aumenta proporcionalmente com o seu poder computacional.

Tipos de Escalabilidade



Soluções de Escalabilidade na Blockchain

- Tratando-se de Blockchain e performance, devemos olhar basicamente três pontos principais:
  - a quantidade de blocos que cada nó armazena;
  - o algoritmo de consenso;
  - o tamanho dos blocos da cadeia.

Como resolver o problema de escalabilidade?

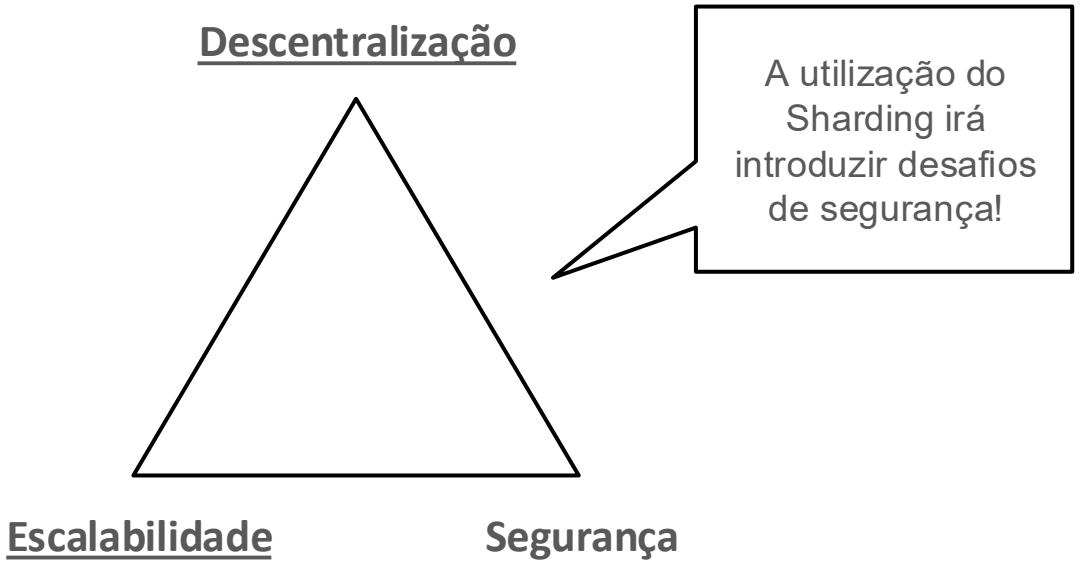
Como resolver o problema de escalabilidade?

- Sharding
- Rollups

Sharding

- A técnica consiste na fragmentação ou divisão horizontal de bancos de banco de dados, permitindo que processem mais transações por segundo.
- O sharding divide o sistema em partições menores, conhecidas como “shards”. Cada fragmento (shard) é composto por seus próprios dados, tornando-o distinto e independente quando comparado a outros fragmentos.

Sharding


Descentralização
A utilização do Sharding irá introduzir desafios de segurança!
Escalabilidade
Segurança

Soluções Off-Chain

- As soluções de layer-2 são um conjunto de técnicas com objetivo de aumentar a velocidade e vazão das transações.
- Essas técnicas reduzem o gas das transações que seria um grande empecilho para o surgimento de aplicações integradas à Blockchain.

Rollups

- A técnica de Rollups consiste em acumular as transações em lotes antes de adicioná-los à Blockchain.
  - Processadas fora da rede principal, compactadas em um lote e adicionadas à Blockchain.
- Os dados processados fora da rede principal devem ser verificados antes de serem adicionados para preservar a confiabilidade.
  - A forma de verificar os dados gerou duas categorias para a técnica de Rollups:
    - Optimistic Rollups
    - Zero Knowledge Rollups

Cartesi

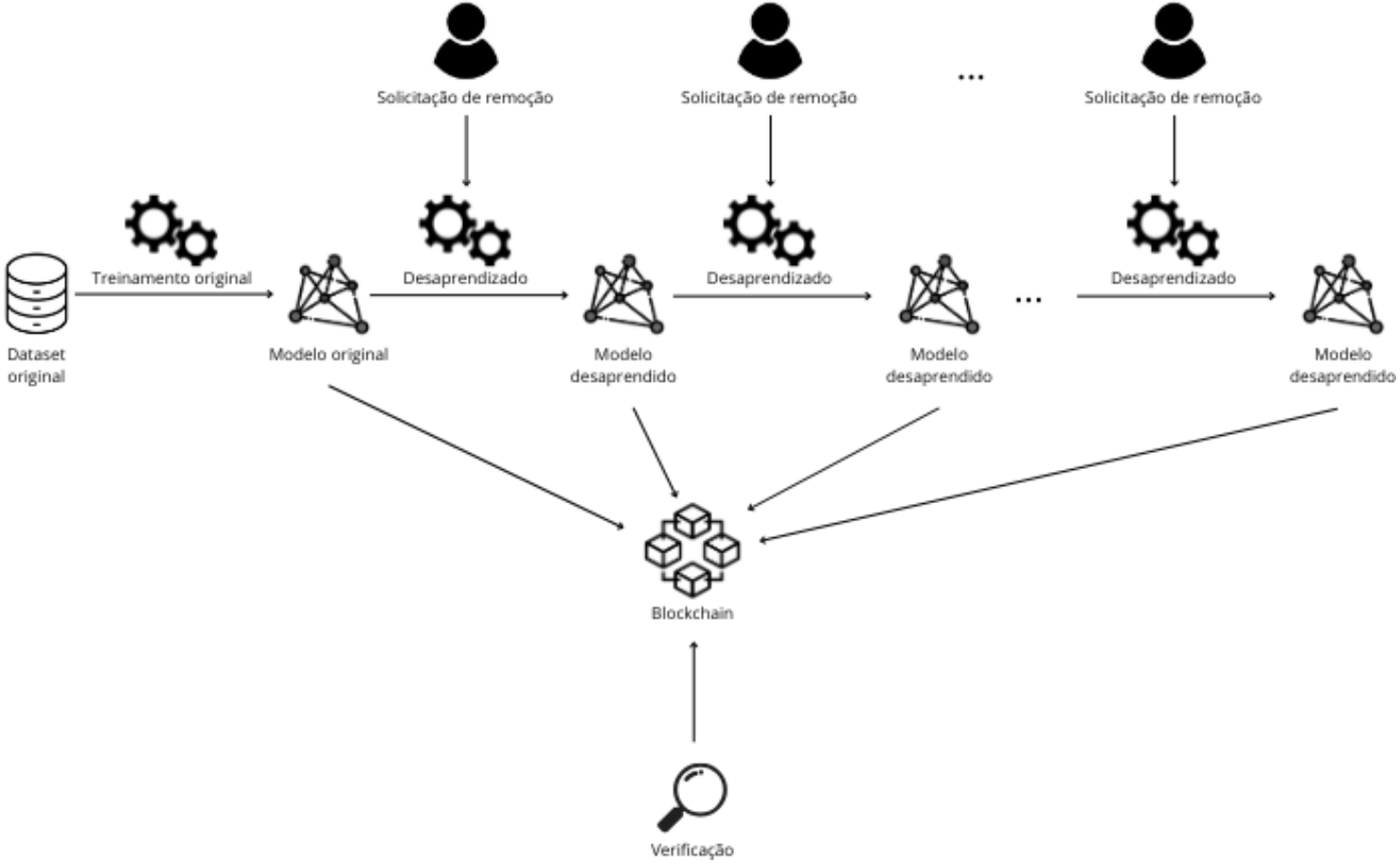
Cartesi

- A Cartesi é uma plataforma de layer-2 para o desenvolvimento de aplicações descentralizadas.
  - Ela permite que DApps sejam desenvolvidos utilizando linguagens de programação convencionais (oferece um SO Linux acoplado a uma infraestrutura Blockchain).

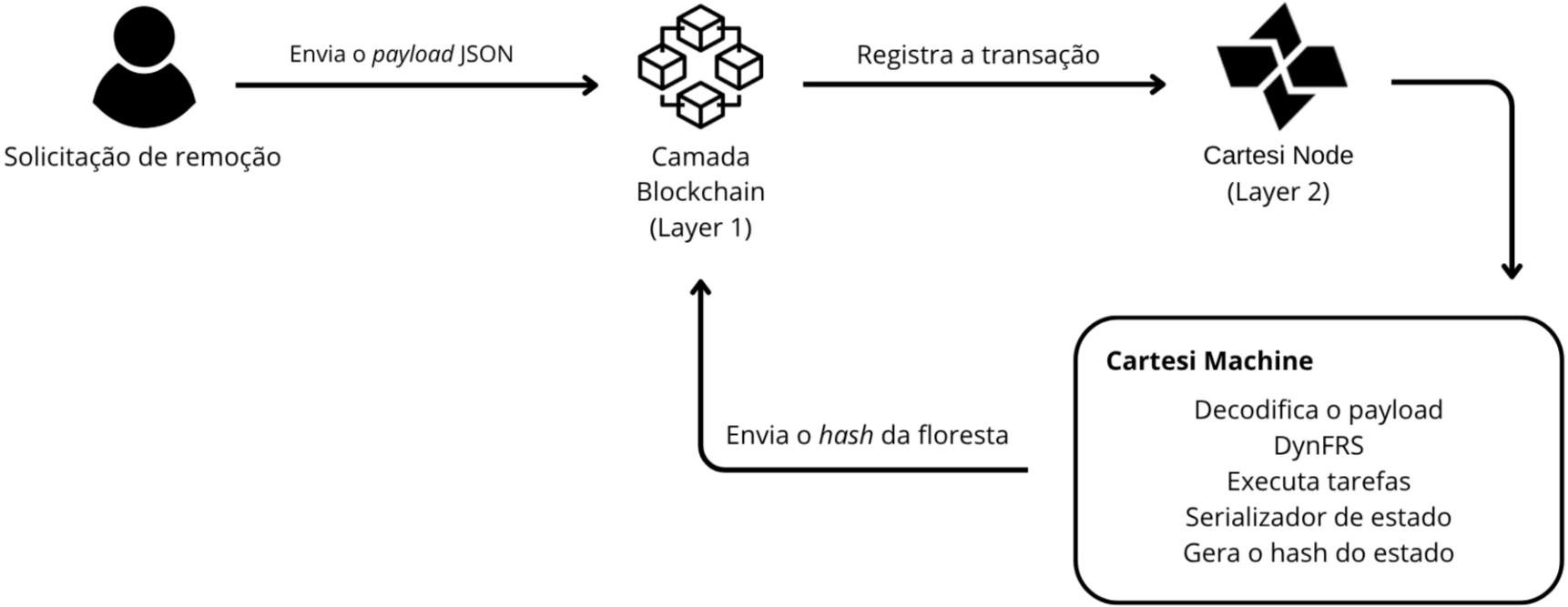
- Na Cartesi, tem-se duas tecnologias principais:
  - **Cartesi Machine**, uma máquina virtual que permite computação verificável usando um sistema operacional Linux.
  - **Cartesi Rollups**, que fornece uma estrutura geral para criação de DApps com a combinação da Cartesi Machine com Optimistic Rollups.

E como a proposta Padlock se alinha com a Cartesi?

Solução Padlock



Solução Padlock



Avaliação da Solução Padlock

- Para avaliar a estabilidade do modelo de DM (DynFRS serializado) integrado à blockchain, conduzimos análises experimentais focados na degradação da acurácia e do AUROC (Area Under the Receiver Operating Characteristic Curve)

Dataset	Cénario 1 (6 Rodadas Sucessivas)		Cenário 2 (Remoção Única Consolidada)	
	Acurácia Final	AUROC Final	Acurácia	AUROC
Adult	0,8668	0,9150	0,8644	0,9137
Bank	0,9139	0,9446	0,9130	0,9427
Heart	0,7304	0,7907	0,7199	0,7791
Vaccine	0,7956	0,8716	0,7954	0,8693
Diabetes	0,6444	0,6998	0,6447	0,7008
NoShow	0,7935	0,7309	0,7805	0,7127

Avaliação da Solução Padlock

- Solicitação de remoção enviada à Cartesi Machine

Avaliação da Solução Padlock

- Execução determinística e auditoria via notices: à esquerda, o log do nó validador detalha o tempo de processamento e a geração do hash do modelo; à direita, a recuperação do notice via script de consulta, expondo o payload que será passível de prova e verificação em Layer-1 após a finalização do estado.

GT-Padlock: Considerações Finais

É possível garantindo privacidade e proteção de dados usando DM e Blockchain

O GT apresentou Padlock, com as seguintes contribuições:

(i) o desenvolvimento de uma interface (API) de integração ao projeto e a Cartesi;

(ii) a implementações de algoritmos de DM dentro de máquinas Cartesi

(iii) o desenvolvimento de uma Prova de Conceito (PoC) de DApp que faz uso do arcabouço como solução para garantia de conformidade com as leis de proteção de dados

NitBus, NitBike ...

Instituto de Computação

Obrigado!
?? & /**/

Antonio "Guto" Rocha
arocha@ic.uff.br