

SSC0958 – Blockchain e Criptomoedas

Apresentação do Curso

Prof. Jó Ueyama

Agosto/2025

Sejam bem-vindos!

- **SSC0958 – Blockchain e Criptomoedas**
- **Curso Híbrido Multi-Instituto/Multicampi**
- **Terça 19:00 às 20:40 e 21:00 às 22:40**

O que eu acredito

I hear, I forget.
I see, I remember.
I DO, I UNDERSTAND.

– *Confucius (551 BC – 479 BC)*

Learn by Doing

Learn by DOING vs Learn by watching



Fonte da imagem: Google Images

Aula de Hoje

- Apresentação da disciplina
- Conceitos de Distributed Ledger Technologies (DLTs)
- Conteúdo programático
 - Metodologia
 - Formas de condução;
 - Avaliação
- bibliografia

Conteúdo Detalhado de Hoje

- Apresentação do professor
- Objetivos da disciplina de sistemas distribuídos
- Alguns esclarecimentos
- Metodologia
- Avaliação de aprendizado
- Regras de funcionamento
- Plano de Ensino
- Perguntas?

Apresentação do professor

- Professor Titular, 2019
 - ICMC/USP, Brasil
- Livre-docência, 2013
 - ICMC/USP, Brasil
- PhD em Ciência da Computação, 2006
 - Lancaster University - UK
- Pos-doc em Ciência da Computação, 2007
 - University of Kent at Canterbury - UK
- Pos-doc em Ciência da Computação, 2008
 - UNICAMP – Campinas SP
- Estágio de Pesquisa, 2016
 - University of Southern California, EUA



Prof. Titular ICMC

ICMC USP
SÃO CARLOS

GRADUAÇÃO PÓS-GRADUAÇÃO PESQUISA CULTURA E EXTENSÃO

Institucional ▾ Pessoas Parcerias Contato

Principal

Veja também

[Alunos de Graduação](#)

[Alunos de Pós-Graduação](#)

[Aposentados](#)

[Docentes](#)

[Egressos](#)

[Funcionários Técnicos-
Administrativos](#)

[Pós-Doutorandos](#)

[Sênior](#)

Pessoas



Docente:
Jo Ueyama

Professor Titular - SSC

Titular (MS6) - RDIDP

PhD em Ciência da Computação (U. of Lancaster, Inglaterra, 2006)

 Email:
joueyama@usp.br

 ResearcherID: F-7677-2011

 Sala: 3-126

 Telefone: +55 16 3373-6718

 Página Pessoal: www.icmc.usp.br/pessoas/

 [Curriculum Lattes](#)

 [Grupos CNPq](#)

Coordenador de Área - FAPESP

FAPESP
FUNDAÇÃO DE AMPARO À PESQUISA
DO ESTADO DE SÃO PAULO

Índice ▾
Buscar

Página inicial » Financiamento à pesquisa » Coordenações

Jó Ueyama

Coordenação de Área - Pesquisa para Inovação PPI 1

É professor titular do Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo (ICMC/USP) e bolsista de Produtividade de Desenvolvimento Tecnológico e Extensão Inovadora do CNPq, Nível 1D.

Tem os títulos de Bacharel em Ciência da Computação da Universidade Federal do Pará (UFPA), Mestre em Ciência da Computação na Universidade Estadual de Campinas (UNICAMP), PhD em Ciência da Computação na Lancaster University, Reino Unido. Foi pesquisador associado na University of Kent at Canterbury, Reino Unido (2006-2007) e pesquisador visitante na University of Southern California, Estados Unidos (2015-2016).

Foi desenvolvedor de sistemas por dez anos na Assembleia Legislativa do Pará (ingresso por concurso público), tendo sido gerente de desenvolvimento por dois anos na mesma repartição pública.

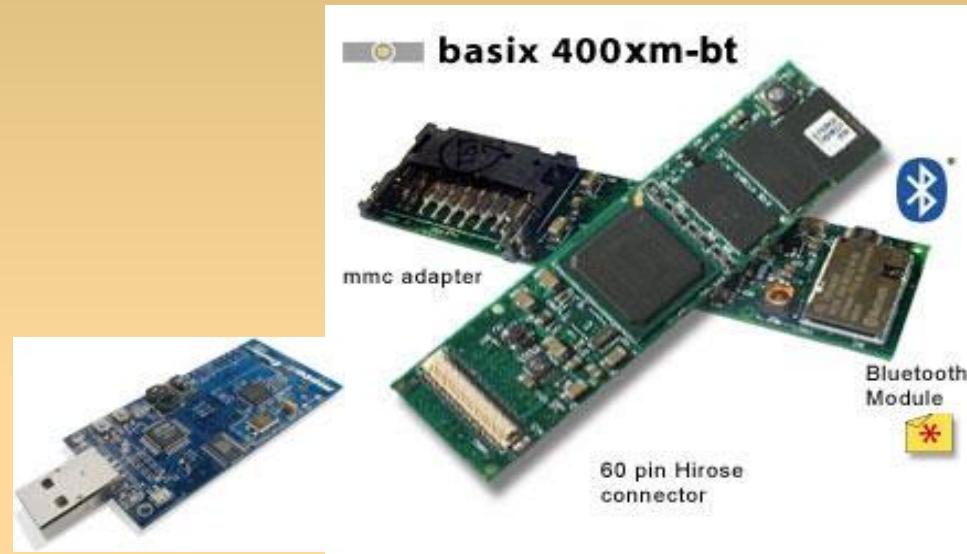
No ICMC/USP, foi o presidente da Comissão das Relações Internacionais (CRInt) por dois mandatos (2016-2020). Foi indicado pelo Departamento de Sistemas de Computação para o Prêmio USP Trajetória pela Inovação 2a. edição.

No ensino, ministrou aulas on-line (com mais de 150 mil visualizações) que servem de material didático para Institutos de Ensino Superior (IES) do Brasil e de países que falam português como língua nativa (p.ex., Angola). Co-coordenador do curso de MBA em Segurança de Dados que encontra-se em fase de submissão na USP.

É autor de cerca de 150 artigos em eventos e periódicos. Depositou três pedidos de patentes e dois registros de software. Realiza pesquisa em áreas multidisciplinares aplicando a inteligência computacional em meio-ambiente, saúde e segurança de dados.



Áreas de atuação



- Redes de Computadores (Internet das Coisas)
- Sistemas Distribuídos (Blockchain)

Objetivos da Disciplina

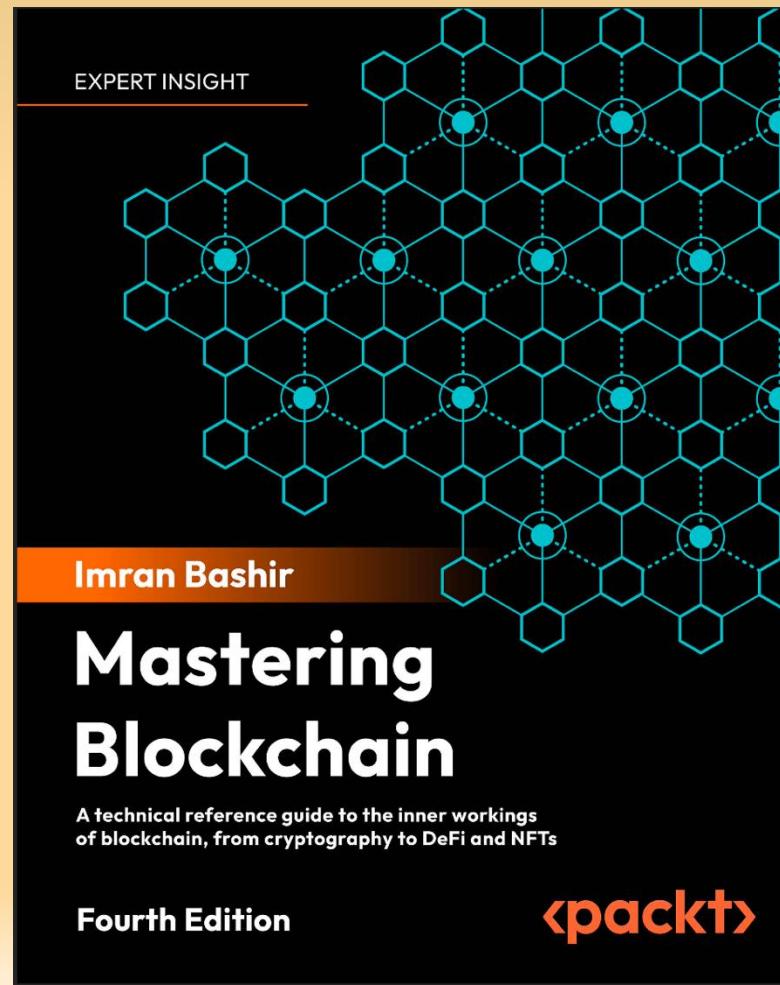
- Apresentar os conceitos de DLTs, incluindo:
 - Arquiteturas existentes;
 - Modelos e implementações
- Criptomoedas
 - Implementações
 - Uso das criptomoedas

Objetivos da Disciplina

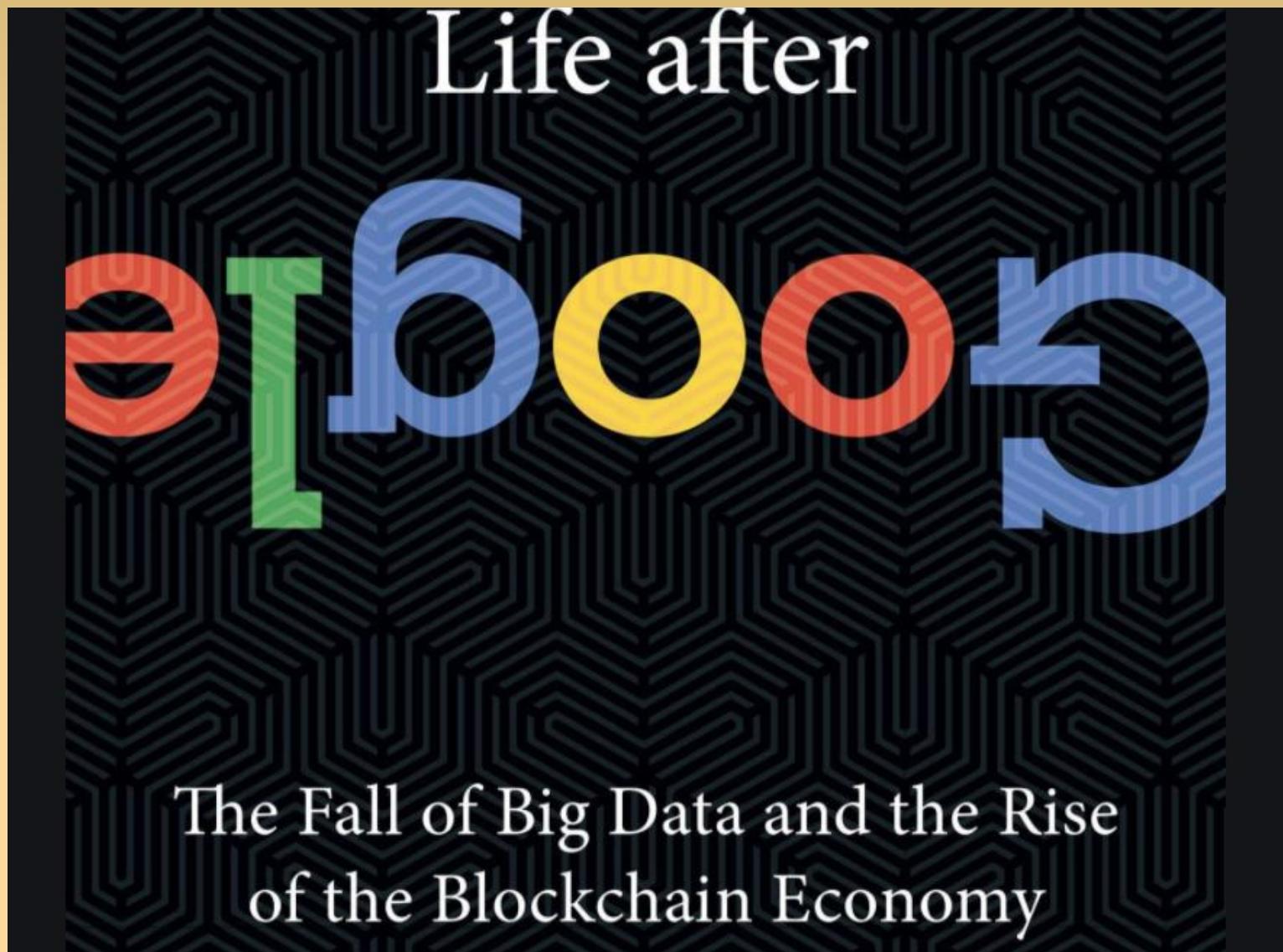
- *Learn by doing*
 - Seminários tecendo assuntos sobre DLTs
 - Implementações em GOL, JS e Solidity de contratos inteligentes

Bibliografia Básica

1. Dois livros
2. Artigos e Papers em Bibliotecas Digitais



Um livro interessante



Pré-requisitos

- Programação C e/ou Java;
- Disciplinas:
 - Sistemas Operacionais;
 - Arquitetura de Computadores;
 - Redes de Computadores.
 - Segurança de computadores

Metodologia (1)

- Exposição em aula pelo docente dos temas do curso
 - Link no Moodle
- Apresentação de Seminários e Projeto
 - Gravadas pelos alunos e submetidas no Moodle

Metodologia (2)

- Atendimento de dúvidas dos alunos pelo professor:
 - Depois das aulas
 - Horário: quarta das 18:00 às 19:00
 - Caso não possa nesse dia/horário, o atendimento poderá ser agendado por consulta via email
 - Não há atendimento em véspera de avaliações

Alguns esclarecimentos

- O cronograma pode sofrer alterações para ajustar com o andamento das aulas
- É você quem faz o curso

Comparative Analysis of Smart Contract Generation Using Large Language Models

Hiago Vinícius Benedito dos Santos¹, Raissa Rosa dos Santos Januario¹,
Ravelly Carvalho Zanatta¹, Saulo Neves Matos^{1,2}, Jó Ueyama¹

¹Instituto de Ciências Matemáticas e de Computação
Universidade de São Paulo (USP) – São Carlos, SP – Brasil

²School of Computing and Communications, Lancaster University,
Lancaster, United Kingdom

{hiagovini, raissa.rosa, ravellyzanatta, saulo.matos}@usp.br

joueyama@icmc.usp.br

Abstract. In recent years, blockchain technology has established itself as an effective, secure, and transparent data storage solution. In this context, smart contracts play a fundamental role by enabling the automated execution of agreements without intermediaries. With the advancement of language models, the opportunity to automatically generate these contracts has emerged, raising concerns about their reliability and potential vulnerabilities. This article proposes a comparative analysis of the available language models for developing smart contracts using Ethereum Virtual Machine's contracts as a case study. Experiments were made using various Large language models using different metrics to evaluate the susceptibility to vulnerabilities and computational cost. After comparing various models, ChatGPT appears to be the most suitable for generating smart contracts due to its higher compilation rate and, consequently, a larger sample size, despite detecting more vulnerabilities.

Avaliação

- Apresentação de seminários sobre DLTs
(Avaliação I)
- Desenvolvimento e apresentação de um projeto
(Avaliação II)

Avaliação - Seminários

- Seminários a serem apresentados pelos alunos sobre os artigos e temas a serem designados a cada aluno
- Critérios:
 - Apresentação
 - Domínio do assunto abordado
 - Aprofundamento do tema tratado
 - Clareza
- Os seminários correspondem a 40% da média final

Avaliação - Projeto

- Um projeto a ser desenvolvido durante o curso com uma apresentação:
 - Apresentação final com os resultados obtidos com o projeto
 - Exemplo: seminário sobre o Ethereum e contratos inteligentes
 - Exemplo: projeto sobre um sistema de votação com o Ethereum
 - É melhor que o projeto esteja conectado ao seminário
- Corresponde a 60% da média final

Sugestões de tema

1. Aplicações com blockchain
2. Ataques na blockchain
3. Qual a criptomoeda me tornará milionário?
4. Contratos inteligentes e IA no blockchain
5. DAO é futuro?
6. Non-Fungible Token (NFT)
7. Redes sociais baseados na blockchain
8. Descentralized Finance (DeFi)
9. Hyperledger
10. Metaverso e criptomoedas

Sugestões de tema

1. Qual a sua startup com blockchain?
2. Inteligência artificial em blockchain
3. Internet das coisas com blockchain
4. Privacidade em blockchain
5. Segurança da blockchain
6. Segurança de redes com blockchain
7. Redes de blockchain públicas e privadas
8. Redes de computadores robustas com blockchain
9. Tendermint
10. Proof of History e Solana

Avaliação (3)

- A média final (MF) é calculada da seguinte forma:

$$MF = 0,4 * M_{seminários} + 0,6 * M_{Projeto}$$

- Aprovação:

- Se $MF \geq 5$

Conteúdo programático

1. Introdução a Blockchain
2. Plataformas de Blockchain
3. Protocolos de Consenso
4. Contratos Inteligentes
5. Aplicações Descentralizadas (DApps)
6. NFTs, DeFis

Aulas no semestre (30 aulas)

Calendário de Agosto a Novembro de 2025

August 2025

Seg	Ter	Qua	Qui	Sex	Sáb	Dom	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
				1	2	3	1	2	3	4	5	6	7
4	5	6	7	8	9	10	8	9	10	11	12	13	14
11	12	13	14	15	16	17	15	16	17	18	19	20	21
18	19	20	21	22	23	24	22	23	24	25	26	27	28
25	26	27	28	29	30	31	29	30					

October 2025

Seg	Ter	Qua	Qui	Sex	Sáb	Dom	Seg	Ter	Qua	Qui	Sex	Sáb	Dom
		1	2	3	4	5						1	2
6	7	8	9	10	11	12	3	4	5	6	7	8	9
13	14	15	16	17	18	19	10	11	12	13	14	15	16
20	21	22	23	24	25	26	17	18	19	20	21	22	23
27	28	29	30	31			24	25	26	27	28	29	30

Proposta de datas

- 30/09: Seminário
- 18/11: Apresentação do Projeto
- 25/11: SUB

É importante salientar que estas datas poderão sofrer mudanças

Nas próximas aulas

- Definição do(a):
 - Tema do seminário
 - Escopo a ser apresentado
 - Inovação a ser tratada

Perguntas?