

Perspectives on Distributed Computing, Networks and Blockchain

Fabíola Greve

Distributed Computing

Leobino Sampaio

Networks

**Computer Science Department
Federal University of Bahia (UFBA)**

Salvador de Bahia

- Founded in 1549 as the 1st capital of Brazil
- About 3 million people
- 3rd largest city in the country, largest in Northeast
- Cuisine, music, architecture





www.ufba.br



- 70 years
- One of the most prestigious in Brazil (top 15)
- 3 thousand professors
- 40 th. undergraduate students
- 6 th. graduate



www.dcc.ufba.br Computer Science Department





Computer Science Department

- 45 professors
- Undergraduate courses in Computer Science, Information Systems
 - ◆ 1.250 undergraduate students
- Graduate programs in Computer Science and Mechatronics
 - 400 graduate students
- Fabíola Greve's currently work
 - Gaudi distributed computing group (gaudi.dcc.ufba.br)
 - Part-time administration: Information Tech advisor to the president of the university
 - Semester 1: Distributed Computing course
 - Semester 2: Blockchain course

Blockchain

Tutorials, Talks, Panels



6 a 10 de Maio



[CERTIFICADOS](#)

[O EVENTO ▾](#)

[CHAMADAS ▾](#)

[PROGRAMA ▾](#)

[CONTATO](#)



MINICURSO 5 (MC-5)

[CERTIFICADOS](#)

[INSCRIÇÕES](#)

[O EVENTO ▾](#)

[COMITÊS ▾](#)

[ANAIS](#)

[TRILHA PRINCIPAL ▾](#)

[MINICURSOS ▾](#)

[CHAMADA DE MINICURSOS](#)

[MINICURSOS ACEITOS](#)

Blockchain e a Revolução do Consenso sob Demanda

Horário: 10/05/2018 (Quinta-feira) – 14:00 às 18:00

Autores: Fabíola Greve (UFBA), Leobino Sampaio (UFBA), Jauberth Abijaüde (UESC), Antônio Coutinho (UEFS), Italo Valcy (UFBA) e Sílvio Queiroz (UFBA)

Apresentadores: Fabíola Greve e Leobino Sampaio

Resumo: Blockchain é uma tecnologia emergente que oferece suporte distribuído confiável para realização de transações com compartilhamento de dados entre participantes que não necessariamente têm confiança entre si e que estão dispersos

Blockchain

Tutorials, Talks, Panels



XXXIX
Congresso da Sociedade Brasileira de Computação
14 a 18 de Julho | Centro de Convenções da Amazônia | Belém - PA

Realizado por:



Certificados

Eventos ▾

Informações ▾

MINICURSO JAI #3

38° Jornada de Atualização em Informática (JAI)

[PÁGINA INICIAL](#)

[ANAIS DE EVENTOS](#)

[CERTIFICADOS](#)

[EVENTOS BASE](#)

[49° SECOMU](#)

[38° JAI](#)

[CHAMADA](#)

[PROGRAMAÇÃO](#)

Correntes de Blocos: Algoritmos de Consenso e Implementação na Plataforma Hyperledger Fabric

A corrente de blocos (blockchain) é uma tecnologia disruptiva que deve revolucionar o nosso modo de viver, trabalhar e negociar. A corrente de blocos é considerada a tecnologia que vai revolucionar a Internet, provendo uma camada de confiança distribuída. Assim como a Internet permite hoje a transferência de arquivos, a tecnologia de corrente de blocos permitirá a Internet de Valores, na qual é possível a transferência sem intermediários de ativos, tais como dinheiro, ações, propriedade intelectual, votos, etc. A corrente de blocos em sua essência é uma simples estrutura de dados imutável que armazena registros de transações e

Inova
Desenbahia

INNOVATION DAY

PALESTRA

A REVOLUÇÃO BLOCKCHAIN

O QUE É? COMO IRÁ TRANSFORMAR AS DIVERSAS RELAÇÕES?

28/06 (QUINTA-FEIRA)
ESPAÇO CRIATIVO - ÀS 10H

PALESTRANTE



FABÍOLA GREVE

PROFESSORA DO DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO –UFBA
DOUTORA EM CIÊNCIA DA COMPUTAÇÃO PELA UNIVERSITÉ RENNES
E PÓS-DOUTORA NA PARIS-SORBONNES UNIVERSITÉS

Desenbahia
Agência de Fomento do
Estado da Bahia S.A.

BAHIA
GOVERNO DO ESTADO

26 de Julho de 2018 | Das 10:30 às 12h | NO HUB Salvador

2º SEMINÁRIO
SALVADOR
CIDADE INOVADORA
Empreendedorismo de Impacto Social



Fabíola Greve

É pesquisadora e professora do Departamento de Ciência da Computação da Universidade Federal da Bahia, doutora em Ciência da Computação e pós-doutora pela Paris-Sorbonnes Universités. Coordena o grupo de computação distribuída GAUDI, onde lidera pesquisas nacionais e internacionais em sistemas e algoritmos distribuídos, tolerância a falhas, computação em nuvem, névoa e blockchain.



Parceiro:



Apoio:



Apoio Institucional:



Realização:



PRIMEIRA CAPITAL DO BRASIL

Serviço Brasileiro de Apoio às
Médias e Pequenas Empresas

Blockchain

First academic Workshop



6 a 10 de Maio



[CERTIFICADOS](#) [O EVENTO](#) [CHAMADAS](#) [PROGRAMA](#) [CONTATO](#)



WBLOCKCHAIN – WORKSHOP EM “BLOCKCHAIN: TEORIA, TECNOLOGIAS E APLICAÇÕES”

ORGANIZAÇÃO



Fabíola Greve (UFBA)

Coordenadora do WBlockchain

E-mail: [fabiola\[at\]ufba.br](mailto:fabiola@ufba.br)



**Eduardo Alchieri
(UnB)**

Coordenador do WBlockchain



**Alysso Bessani
(Universidade de
Lisboa)**

Coordenador do WBlockchain

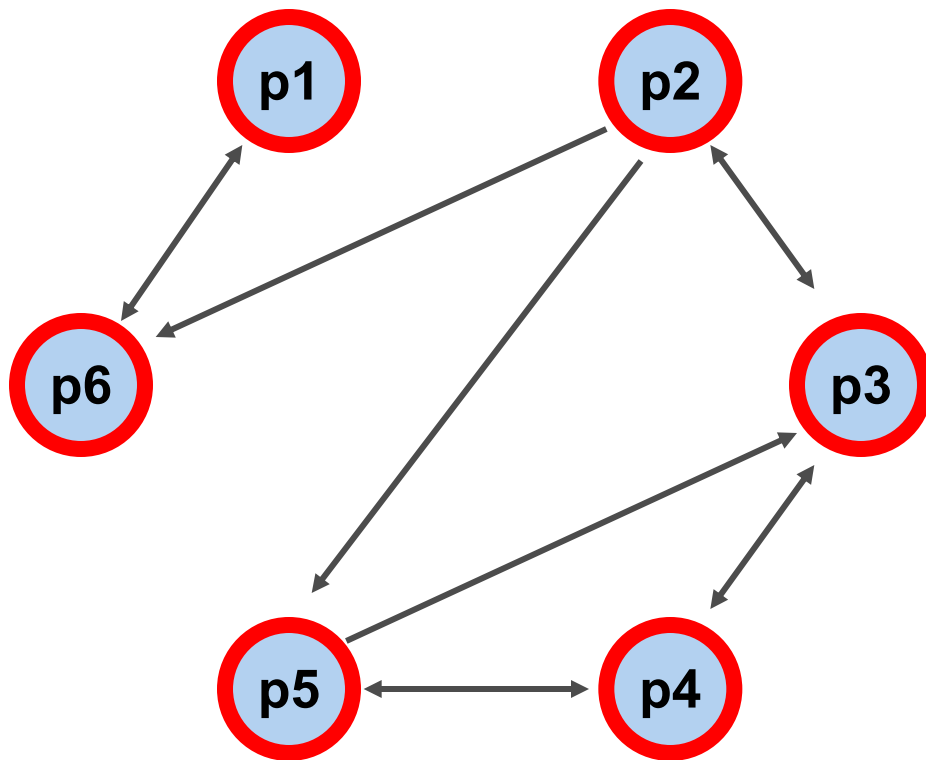
Research Lines

1. Consensus and Fault Tolerant Algorithms
 2. Fog Computing
 3. IoT Applications
 4. Networks
- PhD and Master students, with some other DCC colleagues
 - Cooperation with international/national universities, brazilian public institutions and industry

Conditions for the Solvability of Fault-Tolerant Agreement in Unknown Networks

Fabíola Greve (UFBA, Bahia)
Sébastien Tixeuil (LIP6, Paris)
Alysson Bessani (U. Lisboa)
Eduardo Alchieri (UnB, Brasília)

Dynamic Context – Unknown Networks



- Π and n, f are unknown
- Partial Knowledge
 - ◆ p_i knows $\Pi_i \subseteq \Pi$
 - ◆ p_i can send a message only to processes in Π_i
- Communication Graph is dynamic
- Knowledge Graph is not complete

Consensus in Unknown Networks

- CUP (Consensus with Unknown Participants)
 - ◆ Classical Consensus + No Global Knowledge about Π and n
 - ◆ Fail-free environment
- FT-CUP (Fault-Tolerant CUP)
 - Fail-prone environment
- BFT-CUP (Byzantine Fault-Tolerant CUP)

Abstractions to Solve CUP, FT-CUP and BFT-CUP

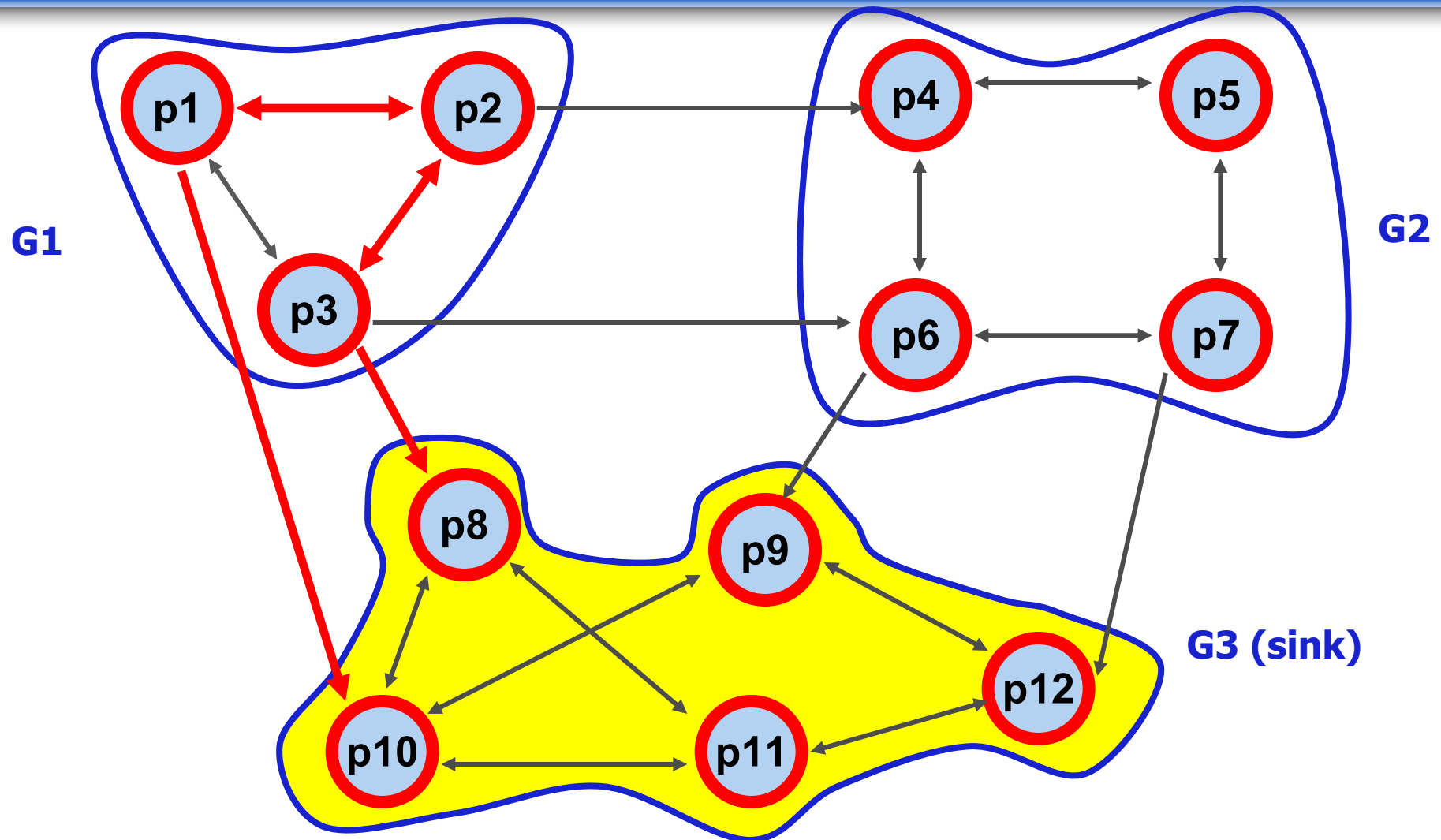
- Synchrony Conditions
 - ◆ Leader Oracles [Lamport, 98]
 - Eventual Leadership Property
 - ◆ Unreliable Failure-Detectors [Chandra and Toueg, 96]
 - Hints about failures
- Knowledge Connectivity Conditions
 - ◆ Participant Detectors [Cavin, Sasson and Schiper, 04]
 - Hints about participants

Participant Detectors (PD)

- Distributed Oracles
- Partial information about processes in the system
 - ◆ Information Accuracy
 - No mistakes about participation
 - ◆ Information Inclusion
 - Information is non-decreasing over time
- Enriches the system with a « knowledge connectivity graph » G
- The graph properties establish « participant detectors classes »

k-One Sink Reducibility PD (k-OSR)

G : sink k -connected, $\geq k$ paths



Conditions to Solve FT-CUP (fault-prone scenario)

[Greve and Tixeuil, DSN 07, PODC:WRAS 10]

Minimal Synchrony \rightarrow Strongest Connectivity

- ◆ k -OSR (k-one sink reducibility)
- ◆ Unreliable Failure Detector: $\diamond S$ or Ω
are necessary and sufficient to FT-CUP,
when n is unknown but f is known
- Uniform FT-CUP is possible!
 - ◆ Reduction to re-use classical indulgent consensus

FT-CUP Byzantine Failures, Shared-Memory

[Khouri, Greve, Tixeuil, SRDS 2013]

Consensus with Unknown Participants for
Shared Memory

[Alchieri, Bessani, Greve, Fraga, TDSC 2016]

Connectivity Requirements for Solving
Byzantine Consensus with Unknown
Participant (BFT-CUP)

Solving BFT-CUP

- Same participant detector necessary to solve FT-CUP: k -OSR PD
- Same level of synchrony necessary to solve FT-CUP: failure, leader oracles
- But BFT-CUP requires authenticated channels & more connectivity than FT-CUP
 - BFT-CUP ($k \geq 2f+1$), FT-CUP ($k \geq f+1$)

Perspective: BFT-CUP for Blockchains

Alysson Bessani (U. Lisboa) and Eduardo Alchieri (UnB)

- ◆ Hyperledger Fabric Project with BFT-SMaRt [DSN 14, DSN 18, DSN 2019 Carter award Thesis]
- Necessary and Sufficient conditions (synchrony and knowledge connectivity) are useful for blockchains?
- How to adapt BFT-CUP algorithms to permissioned blockchains?
- Challenge BFT reconfiguration => Churn/committee management
- Participant detectors are a way to define dynamic BFT committees?


Failure and Leader Detectors for Dynamic Systems

- Most detectors assume
 - Global knowledge about the membership, fully communication connectivity, reliable communication
- Additionally, **they are Time-Based**
 - Requiring that eventually some bound on the message transmission will permanently hold
- These assumptions are not well appropriate to the new scenario of dynamic systems

The Time-Free Approach to Failure Detection and Leader Election

- Propose a Model and Identify sufficient assumptions able to implement the properties of a new class of FDs suitable for mobile networks with unknown membership.
 - TVG (*Time Varying Graphs*), global membership is unknown (n , f), communication is fair-lossy
- The class of eventually strong FDs with unknown membership (namely, \blacklozenge SM)
 - Adapts the properties of the \blacklozenge S class to a dynamic system with an unknown membership.

The Time-Free Approach to Failure Detection and Leader Election

- FD Algorithm that implements  SM
 - Tolerates mobility, dynamic membership
 - Uses local information about the membership
 - Uses QUERY-RESPONSE pattern to exchange messages between local nodes
 - Based on the reception of sufficient Q-R messages from the neighborhood a node is able to suspect or revoke a suspicion
 - The suspicion information is piggybacked and eventually propagated to the whole network

The Time-Free Approach to Failure Detection and Leader Election

[Pierre Sens (LIP6, Paris), Luciana Arantes (LIP6, Paris)]

- An Unreliable Failure Detector for Unknown and Mobile Networks [The Computer Journal 2012, Euro-Par LNCS 2011, Handbook on Mobility 2011, OPODIS 2008]
- What Model and What Conditions to Implement Unreliable Failure Detectors in Dynamic Networks ? [DISC TADDS 2011, DSN HotDep 2011]
- A Time-Free Byzantine Failure Detector for Dynamic Networks [EDCC 2012]
- Eventual Leader Election in Shared-Memory Dynamic Systems [AINA 2018]

Fog Computing

Antônio Coutinho (UFBA, PhD candidate)

Josué Junior(UFBA, Master candidate)

Fabíola Greve (UFBA)

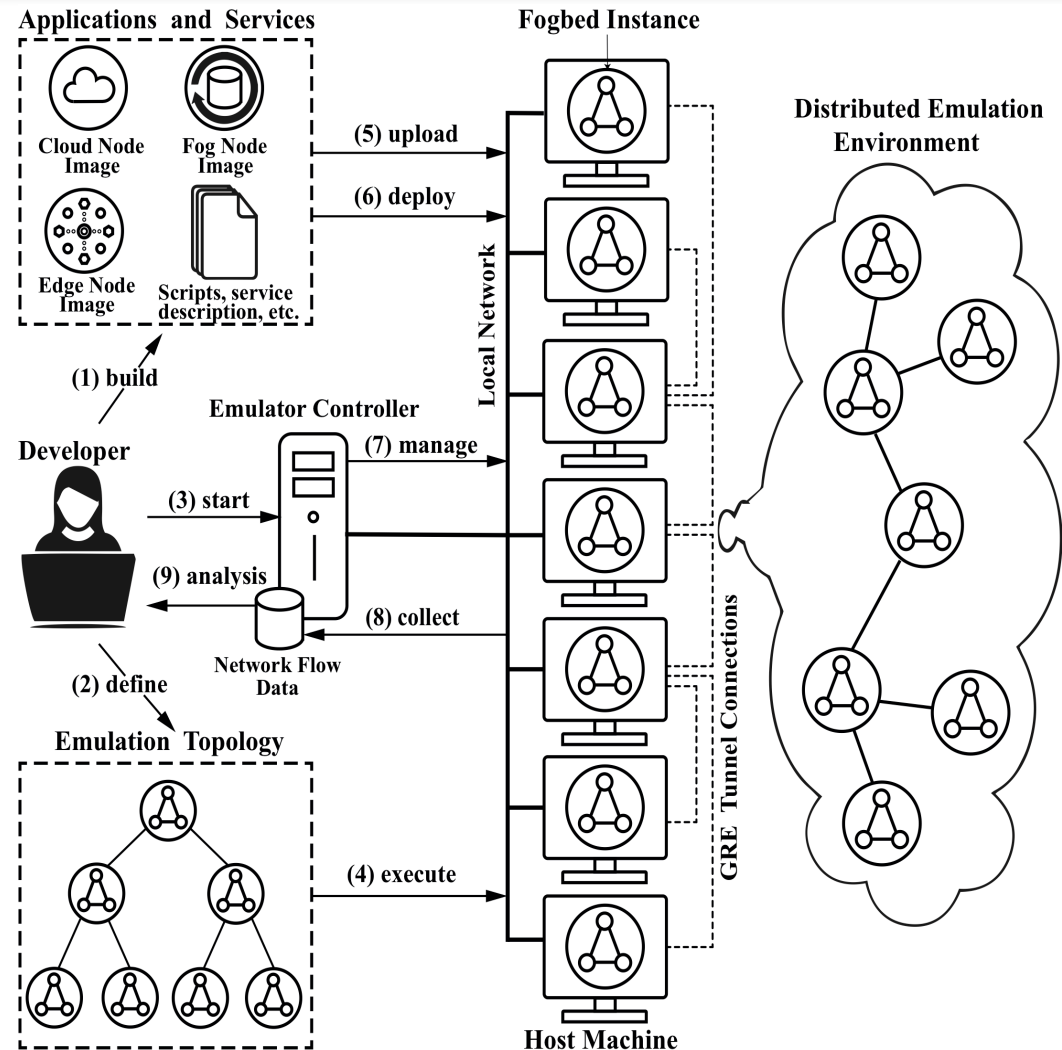
Cássio Prazeres (UFBA)

Fog Testbed Platform Motivation

- No readily available real world fog testbeds that can help researchers to design and verify fog solutions on a truly IoT scale
- To this purpose, net simulators and cloud middleware are adapted to allow the experimental evaluation of fog solutions in limited conditions

Fogbed: Scalable Prototyping Environment for Fog Computing

- A framework and toolset integration for rapid prototyping of fog components in virtualized environments.
- Using a desktop approach, Fogbed enables the deployment of fog nodes as software containers under different network configurations.
- Its design meets the requirements of low cost, flexible setup and compatibility with real world technologies.



Fog Computing

Some Results

- [Antônio Coutinho et al, ICC 2018]
Fogbed: A Rapid-Prototyping Emulation Environment for Fog Computing
- [Antônio Coutinho et al, ISCC 2018]
Scalable Fogbed for Fog Computing Emulation
- [Antônio Coutinho et al., Tutorial at SBRC 2016]
Computação em Névoa: Conceitos, Aplicações e Desafios

Chapter (PDF Available) · May 2016 *with* 3,650 Reads

In book: Minicursos / XXXIV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, Edition: XXXIV, Chapter: Computação em Névoa: Conceitos, Aplicações e Desafios, Publisher: Sociedade Brasileira de Computação, Editors: Frank Augusto Siqueira, Lau Cheuk Lung, Fabíola Gonçalves Pereira Greve, Allan Edgard Silva Freitas, pp.266-315

Perspectives: Fog Blockchain Architecture

- Most of works integrate blockchain into the Fog as a separate service
- Propose to redesign the Fog architecture with blockchains
 - Offering a Blockchain SLA support in the Fog architecture

IoT Applications

Jauberth Abijaude (UFBA, PhD candidate)

Alef Chaves (UFBA, Master candidate)

Hellan Viana (UFBA, Master candidate)

Fabíola Greve (UFBA)

IoT Applications

Some Results

- [Jaubert et al, ISCC 2018]
I2oTegrator – Multiservice middleware with IoT, Ontology and Blockchain support
- [Jaubert et al, SBSI 2018]
IoT Água – Intelligent system for water consumption management and planning

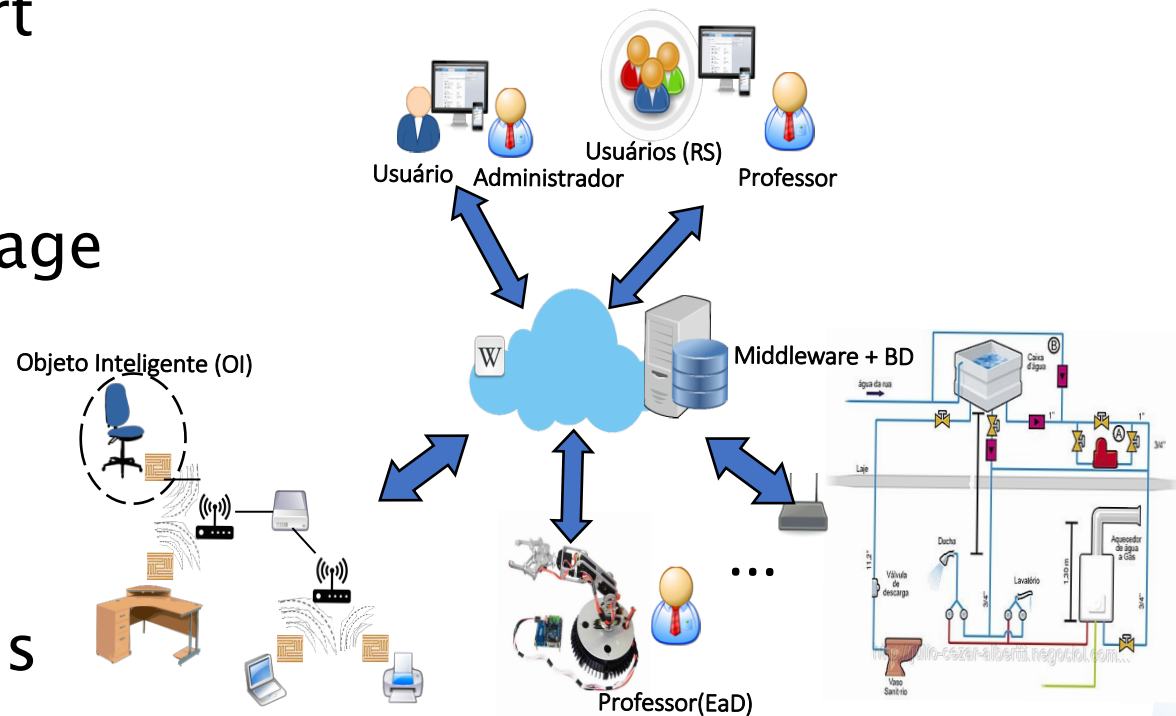
IoT Applications

Some Results

- [Jaubert et al, SBSI 2017]
I²oT Inventory – Autonomous asset inventory system
- [Jaubert et al, in Progress]
IoT Cocoa – IoT and blockchain support for gourmet cocoa production

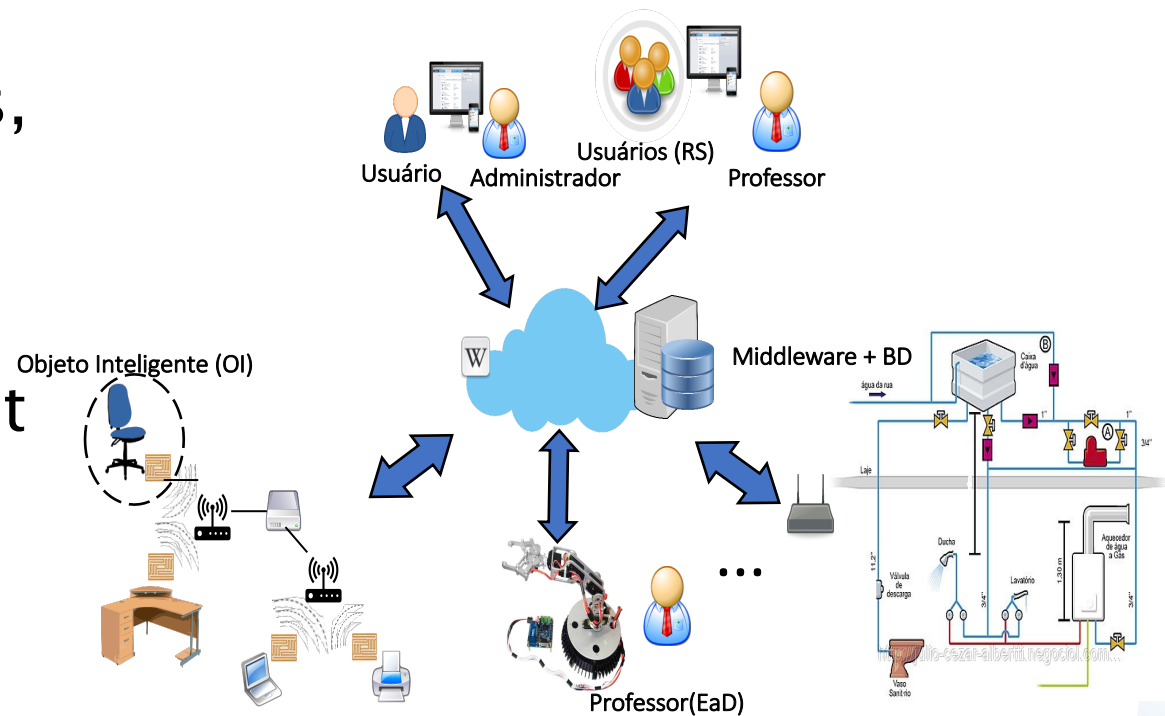
I²oTegrator – Multiservice middleware with IoT, Ontology

- A service-oriented middleware, with support for ontology, REST architectural style and communication by message exchange
- Solve the problem of uniform management of objects, including their tracking and autonomous monitoring



I²oTegrator + Blockchain

- Innovative features: take decisions, recognize situations, trigger alarms, send and receive information by exchanging messages with applications or client software
- **In construction** – Smart contacts creation, compilation and implementation, on-demand, integrated into a web system

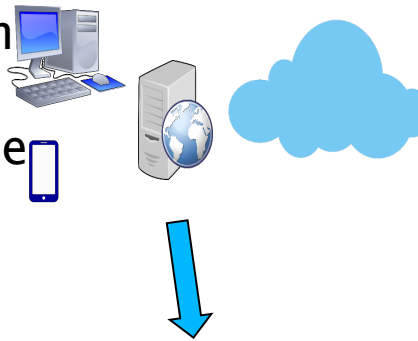


IoTÁgua – Intelligent system for water consumption management and planning

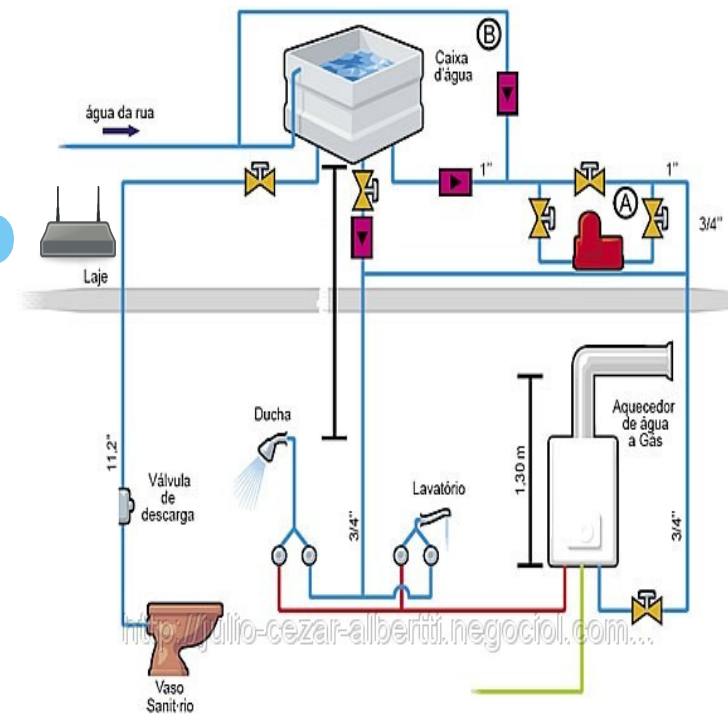
Intelligent water consumption monitoring system, associated to the construction of a database for analytical studies of stored values.

The interconnected Internet system which controls the water supply process in residential and corporate environments, monitors the individual consumption of water outlets, detects leakages, send alerts and creates consumption graphs

Thanks to a middleware able to manage sensors and trigger actions: checking the tank level, measuring the water flow, and handling solenoid valves

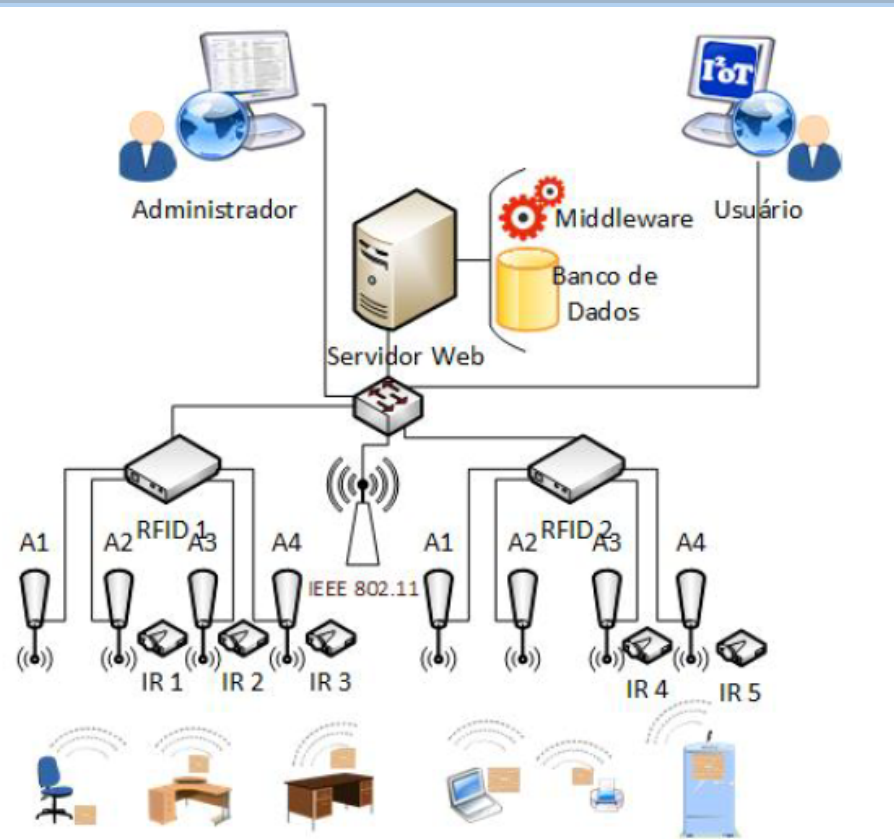


1	PRODUTO	PREÇO	DATA	USUÁRIO	ESTADO	VENDIDOR
2	Seguro de Vida	R\$ 200,00	15/02/2014	São Paulo	SP	Oceiro
3	Captação	R\$ 50,00	16/02/2014	Florianópolis	SC	Fernando
4	Seguro Auto	R\$ 100,00	15/12/2013	Corumbá	MT	Janelle
5	Seguro Auto	R\$ 200,00	15/07/2014	Rio de Janeiro	RJ	Samarita
6	Captação	R\$ 100,00	16/12/2013	Rio de Janeiro	RJ	Samarita
7	Previdência complementar	R\$ 1.000,00	07/12/2013	São Paulo	SP	Oceiro
8	Seguro de Vida	R\$ 500,00	28/02/2014	Rio de Janeiro	RJ	Samarita
9	Captação	R\$ 300,00	10/02/2014	Curitiba	PR	Isabelle
10	Previdência complementar	R\$ 600,00	12/12/2013	Curitiba	PR	Rodrigo
11	Previdência complementar	R\$ 100,00	25/02/2014	São Paulo	SP	Oceiro
12	Seguro de Vida	R\$ 200,00	12/02/2014	São Paulo	SP	Genésio
13	Seguro Auto	R\$ 100,00	12/02/2014	Porto Alegre	RS	Marcos
14	Seguro Auto	R\$ 200,00	28/07/2014	Florianópolis	SC	Fernando
15	Captação	R\$ 100,00	24/12/2013	Porto Alegre	RS	Roberto
16	Captação	R\$ 400,00	25/02/2014	São Paulo	SP	Genésio
17	Captação	R\$ 400,00	15/02/2014	Rio de Janeiro	RJ	Samarita
18	Seguro de Vida	R\$ 50,00	16/02/2014	São Paulo	SP	Oceiro
19	Previdência complementar	R\$ 600,00	16/02/2014	Curitiba	PR	Rodrigo
20	Previdência complementar	R\$ 500,00	16/02/2014	Porto Alegre	RS	Roberto
21	Seguro Auto	R\$ 600,00	12/12/2014	São Paulo	SP	Genésio



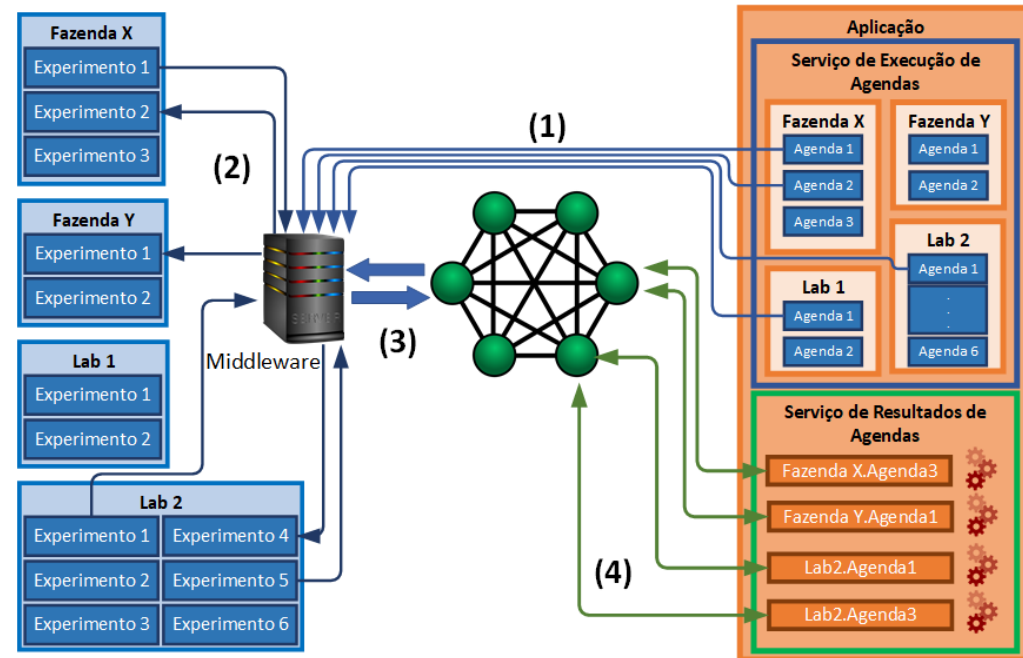
I²oT – Inventory IoT

- Middleware that allows the communication among smart objects (RFID) and the Web system, which operates as a social network.
- A platform able to perform the intelligent management and monitoring of the movement of goods within a institution in an automatic way, reducing the human labor time and keeping the information always updated.



IoT Cocoa – support for gourmet cocoa production

- The worldwide search for gourmet cacao has rekindled interest in production, whose fermentation and drying processes are the key.
- Develop a Web system for the control and monitoring of these events, based on IoT, blockchain and smart contracts to catalog valuable information of the process for improvement and future research.
- Proof of concept and performance evaluation done.



Thanks!



Fabíola Gonçalves Pereira Greve

Computer Science Department

Federal University of Bahia, Brazil

fabiola@ufba.br

<http://gaudi.dcc.ufba.br>

Salvador de Bahia



- In 1985 the Historic Centre of Salvador was made a [World Heritage Site](#) by [UNESCO](#)
- A center of [Afro-Brazilian](#) (*negro*) culture, due to slaves descendants