Université Constantine 2
جامعة قسنطينة 2

Algorithmes distribués avancés (ALDA)

– TP –

Implémentation de la Blockchain

Dr. BOUKHARROU R.
Faculté des nouvelles technologies
radja.boukharrou@univ-constantine2.dz

Université Constantine 2
جامعة قسنطينة 2

Algorithmes distribués avancés (ALDA)

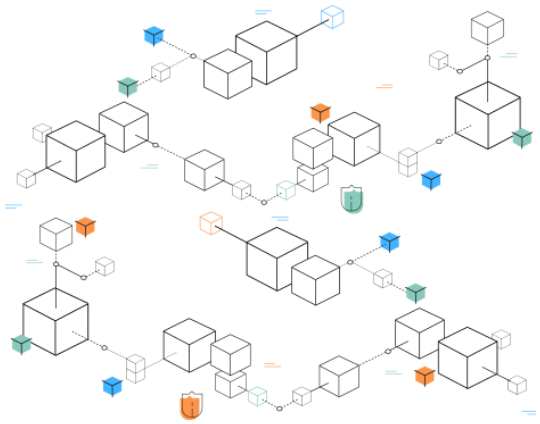
– TP –

Implémentation de la Blockchain

Dr. BOUKHARROU R.
Faculté des nouvelles technologies
radja.boukharrou@univ-constantine2.dz

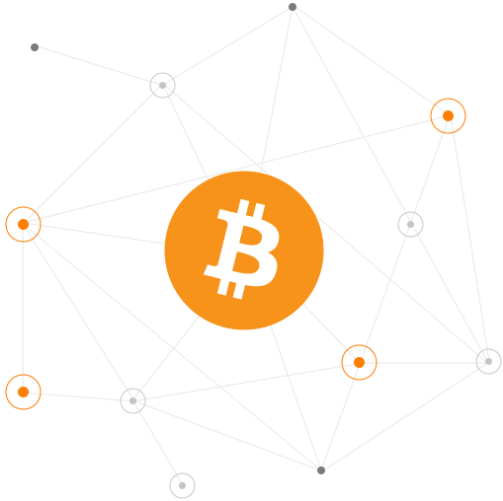
Etudiants concernés

Faculté/Institut	Département	Niveau	Spécialité
Nouvelles technologies	IFA	Master 2	RSD



Blockchain

(Chaine de blocs)



Bitcoin

Etapes du TP

- **TP1** Préparation de la plateforme JADE
- **TP2** Nœuds du réseau Blockchain en JADE
- **TP3** Structure des transactions, des blocs et de la blockchain
- **TP4** Hachage des données
- **TP5** Transfert des données
- **TP6** Preuve de travail et minage
- **Mini-projet**

TP1

Préparation de la plateforme JADE

TP1 : Préparation de la plateforme JADE

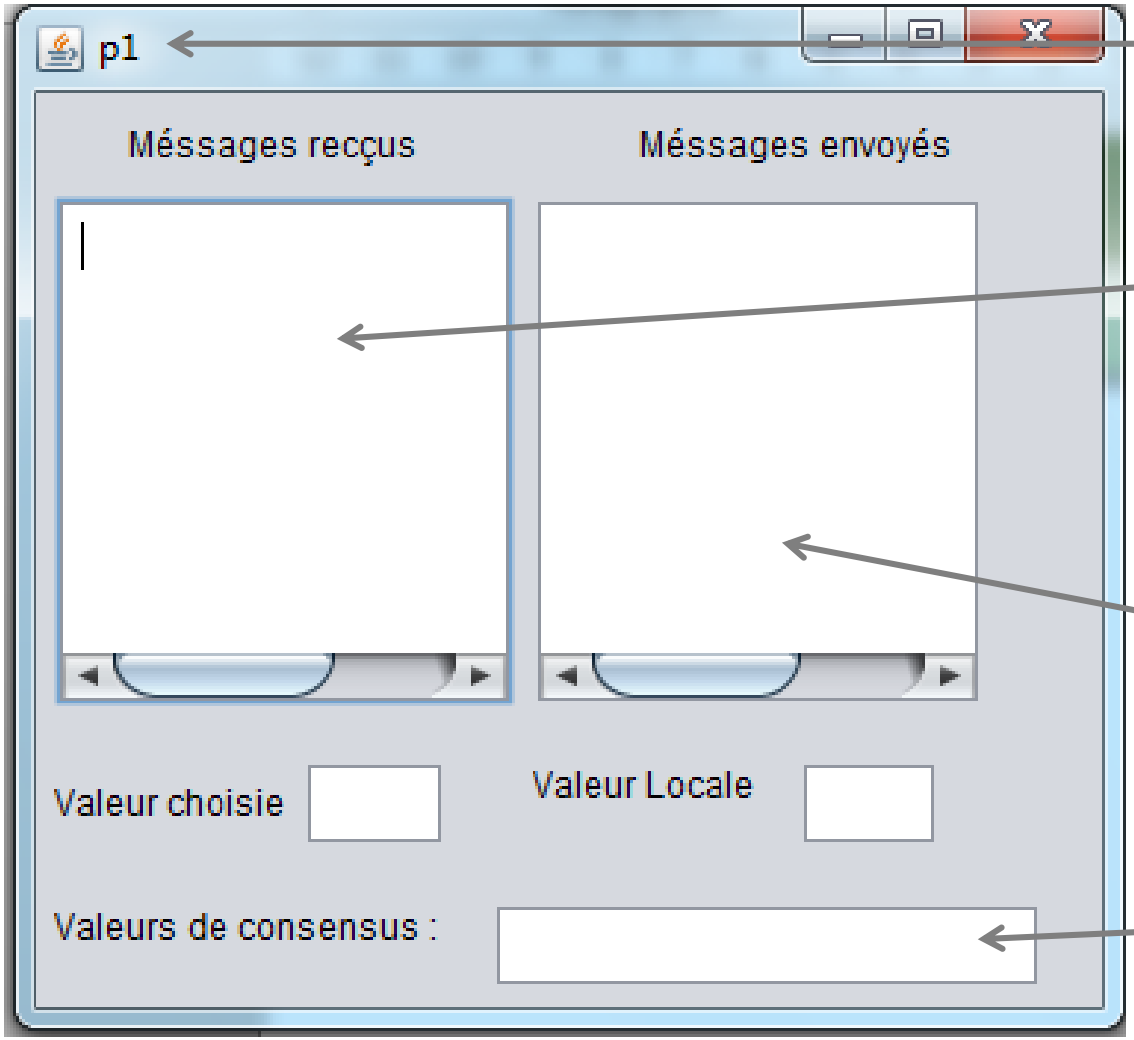
Etape 1 : Installer la plateforme Jade

1. Créer un projet **`TpAlda01`**
2. Ajouter la dépendance vers la bibliothèque de JADE
   - Mettre le ficher « **`jade.jar`** » dans le dossier « **`./libs/`** »

NB :**Vous pouvez consulter TP1 et TP2 du Module ALDI – Master 1 RSD**

TP1 : Préparation de la plateforme JADE

Etape 2 : Implémenter l'interface graphique (1/2)



Nom du processus

Espace réservé à l'affichage des messages reçus (valeurs proposées)

Espace réservé à l'affichage des messages délivrés par le processus **P1** (sa valeur locale)

Liste des valeurs d'accord (en ordre)

TP1 : Préparation de la plateforme JADE

Etape 2 : Implémenter l'interface graphique (2/2)

L'interface graphique est associée à chaque processus (elle sera utilisée dans les prochains TPs)

Travail demandé : Dans le projet **`TpAlda01`** :

1. Créer l'interface graphique de la forme déjà présentée, nommée **`Fenetre`**
2. implémenter le processus **`P1`** en utilisant l'interface **`Fenetre`**

Processus.java

```
public class Processus extends Agent{
  Fenetre f;

  public void setup(){
    System.out.println("Je suis l'agent : "+getLocalName());
    f = new Fenetre(getLocalName());
  }
```

3. Exécuter le programme en utilisant la commande :

```
-cp jade.boot P1: Processus
```

TP1 : Préparation de la plateforme JADE

Etape 3 : Implémenter un protocole de consensus (1/3)

Objectif :

- Implémentation d'un protocole de consensus qui s'agit d'**une fonction de calcule commune** à l'ensemble de processus, dont le contexte est le suivant

Hypothèses :

- **Environnement :** sans faute
- **Système :** synchrone ou asynchrone
- **Communication (canal) :** fiable, pas de perte ni duplication du messages
- **Initiation :** soit un processus initiateur
- **Processus :**
  - Le groupe de processus est fermé et statique
  - Tous les processus sont correct
  - Tout processus peut communiquer avec tous les autres processus

TP1 : Préparation de la plateforme JADE

Etape 3 : Implémenter un protocole de consensus (2/3)

Comportement d'un processus Pi

à la réception d'une valeur j du processus P_j

```
Consensus ← true
if val_Pj == j
   Envoyer (val_locale)
   Attendre la réception de (n-1) valeurs;
   Appliquer la fonction commune : val_choisie == min(v1,v2, …, vn)
   Afficher le résultat (val_choisie)
   Consensus ← false
```

à l'envoi de valocal à tous les processus

```
Envoyer val_locale à tous les processus (n proccesus)
Calculer val_locale : val_locale ← val_locale + random
```

TP1 : Préparation de la plateforme JADE

Etape 3 : Implémenter un protocole de consensus (3/3)

Variables locales d'un processus pi

- **groupe_P** : liste des identifiants des processus et leurs valeurs
- **val_choisie** : valeur choisie parés l'application du protocole de consensus
- **val_locale** : valeur locale proposée par le processus **Pi**

Pour lancer processus

```
-cp jade.boot P1:Processus(P1,P2,P3,1); P2:Processus(P1,P2,P3,2),
              P3:Processus(P1,P2,P3,3)
```

TP2

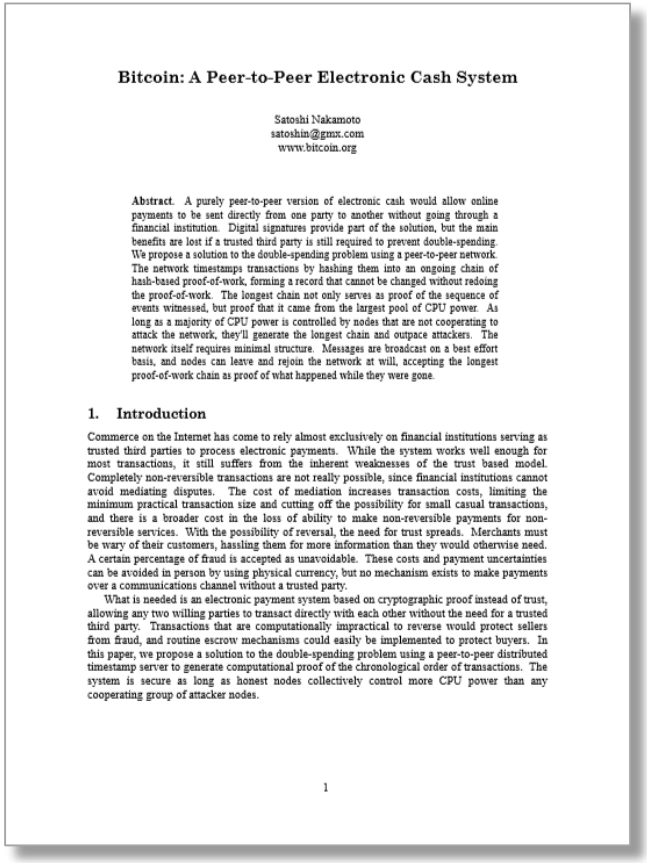
Nœuds du réseau Blockchain en JADE

Bitcoin

White paper

Bitcoin: A Peer-to-Peer Electronic Cash System (2009)

Cité 229 fois



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

1

Auteurs :

- Satoshi Nakamoto (Unknown affiliation)

Lien :

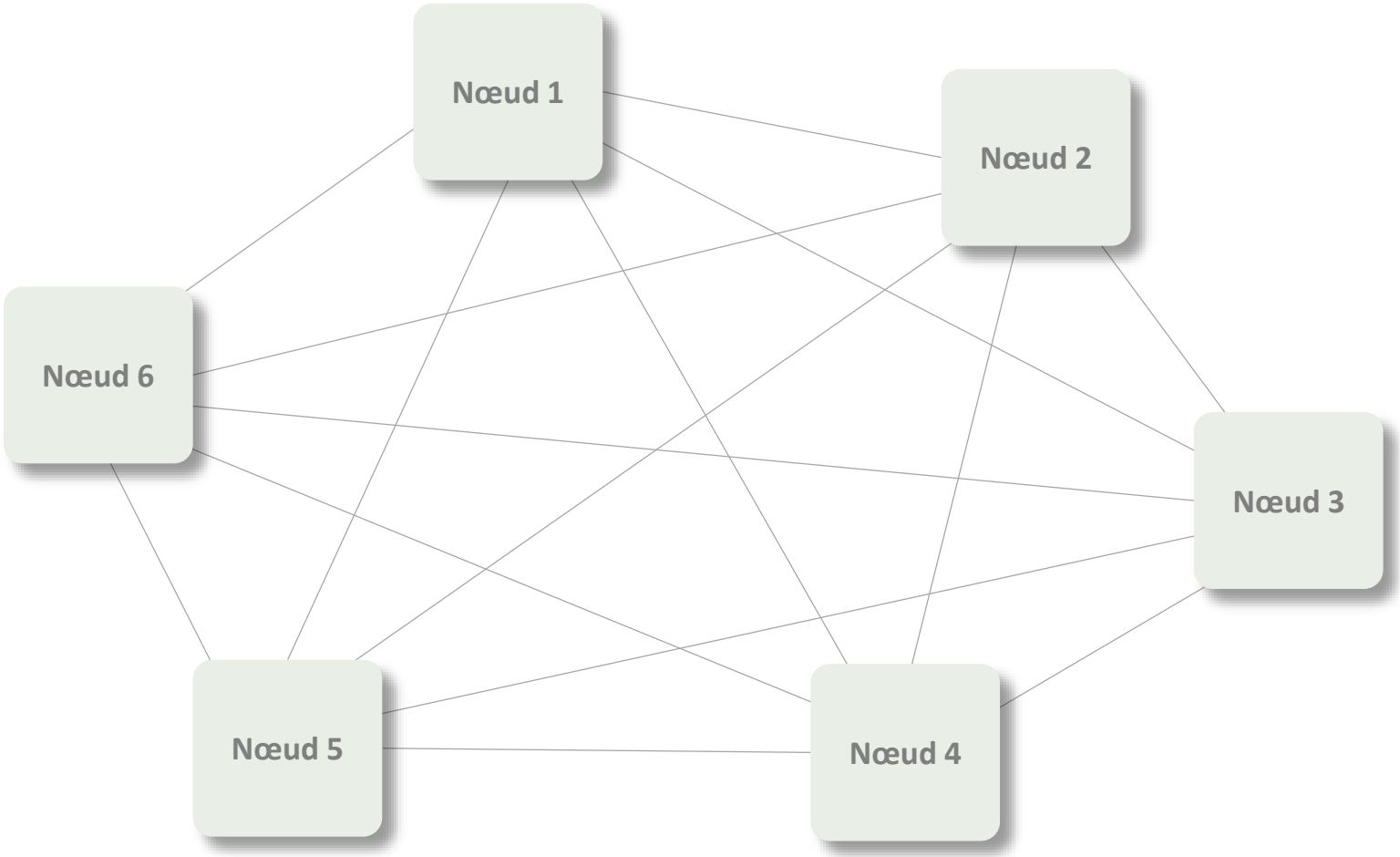
- https://bitcoin.org/bitcoin.pdf

Mots clés :

Transactions ◆ Blockchain ◆ peer-to-peer ◆ Monnaie électronique ◆ Cryptographie ◆ Consensus distribué

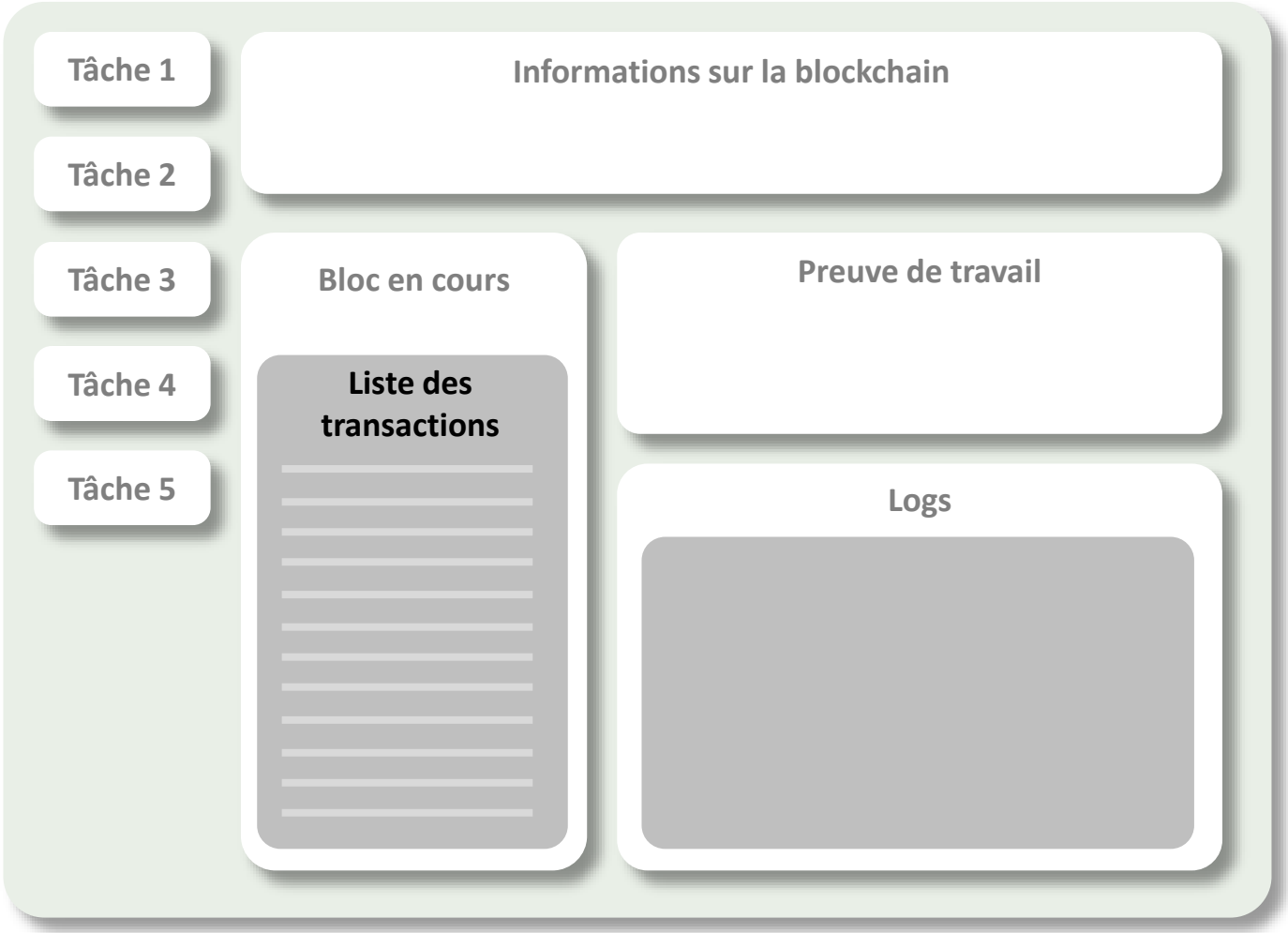
TP2 : Nœuds du réseau Blockchain en JADE

Architecture



TP2 : Nœuds du réseau Blockchain en JADE

Interface graphique d'un nœud



TP2 : Nœuds du réseau Blockchain en JADE

Tâches d'un nœud

Tâches possibles :

- **Créer une transaction**
- **Envoyer une transaction**
- **Créer un bloc**
- **Envoyer un bloc**
- **Miner un bloc**
- **Vérifier une transaction**
- **Hacher un bloc**
- **…**

TP3

Structure des transactions, des blocs et de la blockchain