Blockchain

Sylvain Conchon

Laboratoire Méthodes Formelles

Université Paris-Saclay, CNRS, ENS Paris-Saclay

sylvain.conchon@universite-paris-saclay.fr

Contenu du cours

- Introduction
- Couche P2P
- Bitcoin
  - Modèle UTXO
  - Langage Script
  - Clients légers, Arbres de Merkle, Lightning Network
- Tezos
  - Introduction à Tezos, CLI
  - Smart contracts
  - Michelson
  - SmartPy

Évaluation

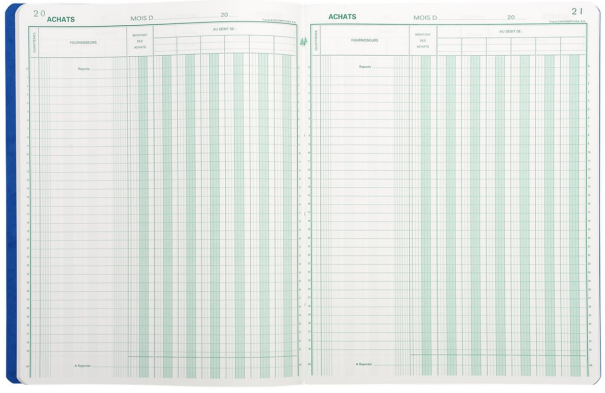
- Exercices de programmation de smart-contracts.
- Mini-projet (À faire par groupe de 4 maximum) :

  Programmation d'une mini blockchain du type Bitcoin + une démo

INTRODUCTION

Qu’est-ce qu’une Blockchain ?

Une blockchain est comme un grand livre de comptes



Chaque page de ce livre correspond à un bloc où sont enregistrées des transactions (d’argent ou autre)

Dans le monde des blockchains, ce livre de comptes est appelé un registre (*ledger* en anglais).

Registre distribué

Une blockchain est un système distribué formé de nœuds qui s'entendent sur le contenu d'un registre.

La particularité de la blockchain est que ce registre n'est pas stocké sur un serveur centralisé, mais il est partagé (ou recopié) sur un grand nombre d'ordinateurs à travers le monde entier qui sont tous interconnectés.

On parle de registre distribué (*distributed ledger* en anglais), sans aucun organe central de contrôle.

L'intérêt d'une structure distribuée est une très grande résistance aux pannes (des serveurs) et aux attaques de sécurité.

Transactions

Le registre distribué contient entre autres des transactions.

Chaque transaction implique deux “clients”, celui à l’origine de la transaction et le bénéficiaire, ainsi qu’un montant.

Les nœuds du système s’accordent donc à la fois sur quelles transactions inclure dans le registre, mais également l’ordre dans lequel ces transactions doivent apparaître.

Faire les comptes

À partir de ces transactions contenues dans tous les blocs, on tient à jour les comptes...

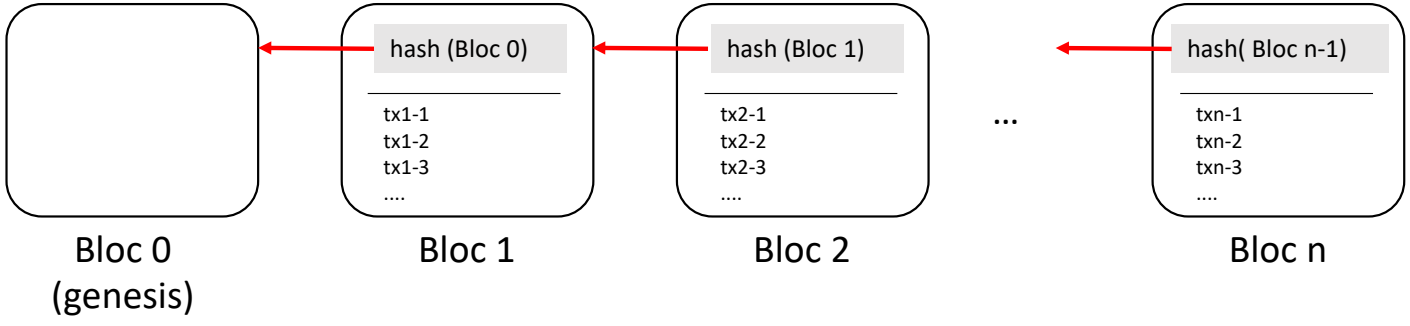
Comptes bancaires

Client	Montant
#1	100 Ƀ
#2	20 Ƀ
#3	50 Ƀ
⋮	⋮

Chaînes de blocs

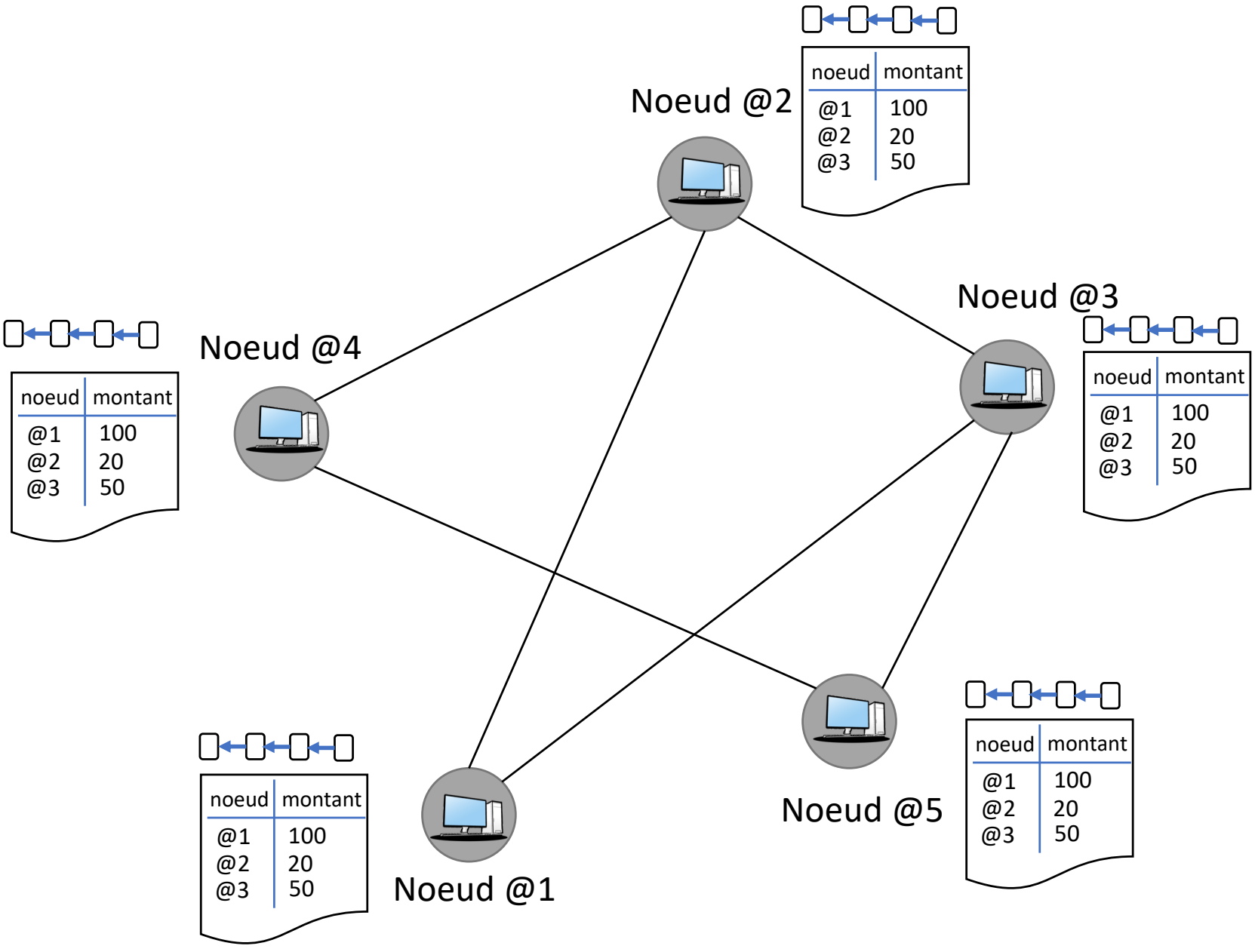
Le registre est stocké dans une structure de données de type append-only qui contient des blocs de transactions.

Cette structure est similaire à une liste chaînée. Chaque bloc n contient un “pointeur” vers le bloc $n-1$ représenté par la valeur de hash du bloc précédent. Le premier bloc est nommé genesis.



Les nœuds d’une blockchain s’accordent donc sur les blocs à inclure dans le registre.

Architecture décentralisée



Quelques problèmes sous-jacents à une blockchain

Comment s'assurer qu'un bloc ne va pas être supprimé de la chaîne ? (c'est-à-dire qu'une page du registre ne soit supprimée)

Comment vérifier l'intégrité d'un bloc ? C'est-à-dire que personne ne peut modifier le contenu des transactions ou en ajouter, en supprimer ?

Comment faire pour que toutes les machines aient la même version du registre ?

Comment faire pour être sûr qu'une personne ne dépense pas plus qu'elle n'a d'argent ?

Comment s'assurer qu'une personne ne dépense pas l'argent d'une autre ?

Etc.

Quelques problèmes sous-jacents à une blockchain

Comment s'assurer qu'un bloc ne va pas être supprimé de la chaîne ? (c'est-à-dire qu'une page du registre ne soit supprimée)

Comment vérifier l'intégrité d'un bloc ? C'est-à-dire que personne ne peut modifier le contenu des transactions ou en ajouter, en supprimer ?

Comment faire pour que toutes les machines aient la même version du registre ? $\Rightarrow$ **Le problème du consensus distribué**

Comment faire pour être sûr qu'une personne ne dépense pas plus qu'elle n'a d'argent ?

Comment s'assurer qu'une personne ne dépense pas l'argent d'une autre ?

Etc.

Consensus distribués dans les Blockchains

Il existe de nombreuses solutions au problème du consensus distribué dans les blockchains.

Cette diversité est principalement liée aux hypothèses faites sur la couche réseau sous-jacente à la blockchain, ainsi qu'aux pannes envisagées.

Afin de comprendre les solutions proposées dans certaines blockchains actuelles, ce cours présente les définitions, résultats et algorithmes fondamentaux liés au problème du consensus distribué.

La technologie Blockchain

Pour résoudre ces problèmes, l'implémentation d'une blockchain repose (entre autre) sur :

- une architecture de réseau pair-à-pair (P2P)
- un protocole de consensus distribué
- des primitives cryptographiques