Université Constantine 2
جامعة قسنطينة 2

Algorithmes distribués avancés (ALDA)

– Cours 5 et 6 –

Chapitre 3 : Technologie Blockchain et consensus distribués

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

Université Constantine 2
جامعة قسنطينة 2

Algorithmes distribués avancés (ALDA)

– Cours 5 et 6 –

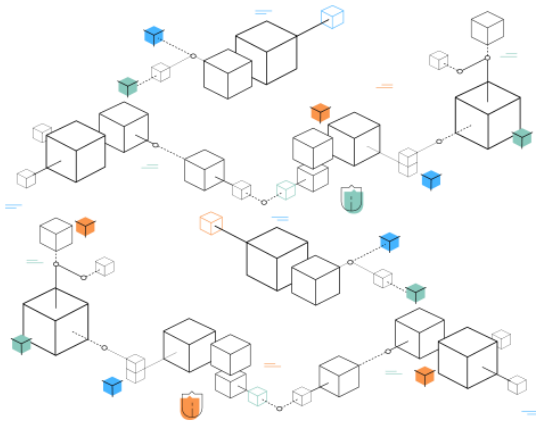
Chapitre 3 : Technologie Blockchain et consensus distribués

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

Etudiants concernés

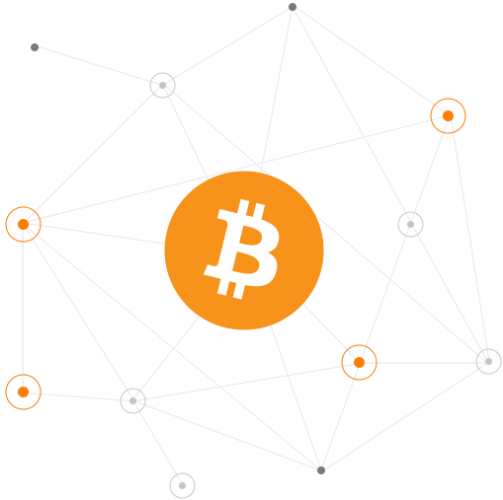
Faculté/Institut	Département	Niveau	Spécialité
Nouvelles technologies	IFA	Master 2	RSD

- Blockchain
- Bitcoin
- Smart-contracts
- Blockchain semi-publique et privée



Blockchain

(Chaine de blocs)



Bitcoin

Contexte

- Dans un contexte de **crise économique** (2008-2009), de **scandales financiers** et monétaires, de **perte de confiance** en les institutions bancaires,
  - Un groupe de hackers a crée une **crypto-monnaie** émise par un système peer-to-peer et indépendant de tout système de contrôle centralisé
  - C'est ainsi que **Satoshi Nakamato** pose les principes fondateurs de Bitcoin en 2008, en publiant « **Bitcoin: A Peer-to-Peer Electronic Cash System** »
  - L'idée est devenue une réalité après le développement du **logiciel open-source** du bitcoin en 2009

Problématique

Problématique

- Comment résoudre le problème cryptographique du **double paiement** (ou problème des **généraux Byzantins**) ?
- Comment deux utilisateurs peuvent s'échanger des biens (monnaies, …), **sans passer par un tiers de confiance** ?
- Comment garantir une monnaie **sans autorité centrale** ?

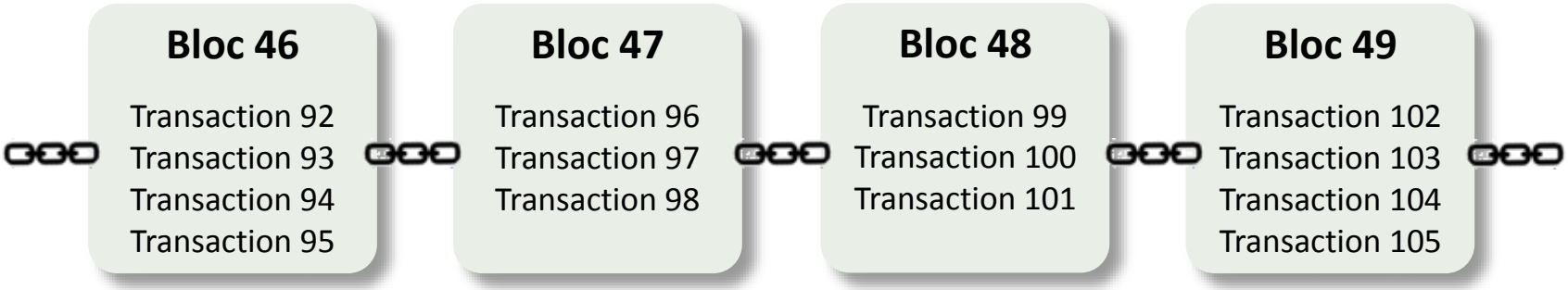
Consensus distribué et sécurisé

Solution : **Naissance du Bitcoin**

- **Bitcoin** est une crypto-monnaie supportée par une technologie décentralisée appelée la **Blockchain (la chaine de blocs)**
  - Echange **peer-to-peer** des transactions → **Désintermédiation** (Sans passer par des banques)
  - Stockage des transactions dans **un registre complet**
  - **Vérification décentralisée** des transactions à tout moment
- La blockchain est présentée comme une révolution impactant les mondes **industriel**, **économique** et **citoyen**

Blockchain (Chaine de bloc)

- Une technologie de **stockage** et de **transmission** d'informations sans **organe de contrôle**
  - Les informations envoyées par les utilisateurs et les liens internes à la base sont **groupés en blocs** et **vérifiés à intervalles** de temps **réguliers**
  - Les blocs sont sécurisés contre la falsification ou la modification par des **techniques cryptographiques**,
  - Les blocs sont liés entre eux, formant une **chaîne de blocs**, qui est vue comme une **BD distribuée** et **sécurisé** de toutes les transactions effectuées depuis le démarrage du système réparti.



Blockchain

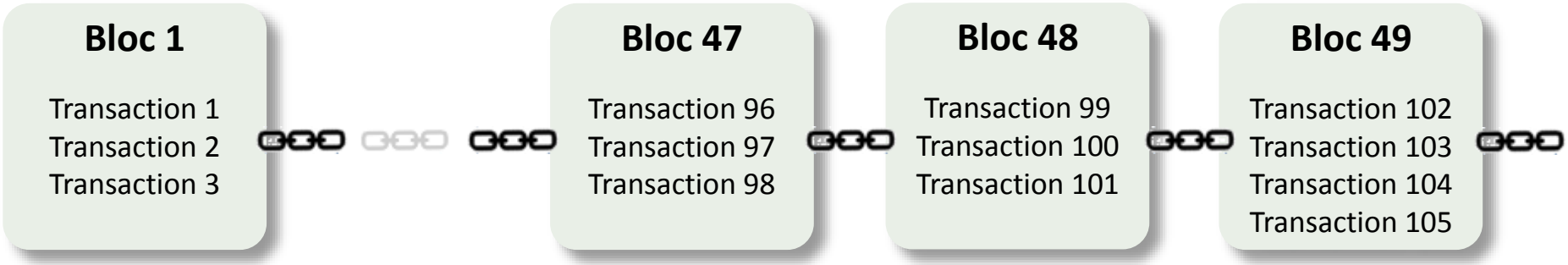
Historique

- La première étude sur les **chaînes de blocs** cryptographiquement **sécurisées** a été décrite en **1991** (par Bayer, Haber et Stornetta)
  - Les documents horodatés ne pourraient pas être falsifiés ou antidatés
- En **1992**, ils ont incorporé le concept d'**arbre de Merkle** pour améliorer l'efficacité du système
  - Plusieurs documents sont assemblés en un seul bloc
- En **2008**, la **1ère chaîne de blocs** a été conceptualisée (par Satoshi Nakamoto)
  - La blockchain du Bitcoin a été implémentée (**3 Janvier 2009 à 18h15 UTC**) où elle sert de **registre publique** à toutes les transactions sur le réseau
  - Le 1er bloc est appelé **bloc de genèse**. La 1er transaction bitcoin est une transaction unique de paiement de **50 nouveaux bitcoins** à son créateur
- **Actuellement (oct 2018)**, la Blockchain du Bitcoin enregistre **547 416 blocs** avec environ 150 blocs/jour comportant en moy. 1700 transactions chacun (Lien)
  - **+1000 crypto-monnaies sur le marché :** Litecoin (2011), Ethereum (2015), Zcash (2016), Bitcoin Cash (2017), …

Blockchain - Implémentation

Monnaie virtuelle - Bitcoin

- Bitcoin est une crypto-monnaie dédié aux paiements électroniques peer-to-peer, fonctionnelle depuis 2009
- La Blockchain du Bitcoin permet de stocker **des données des transactions** depuis la création du **Bitcoin**, qui sont :
  - **Pérennes** (durent très longtemps)
  - **Infalsifiables** (non modifiables, ni supprimables)
  - **Distribués** (sur plusieurs nœuds)

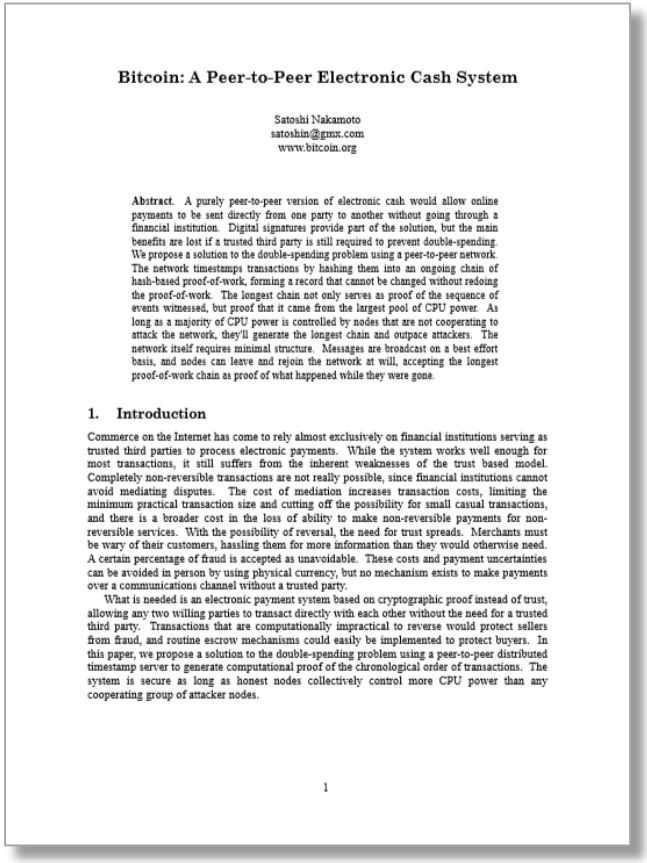


Bitcoin

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 :

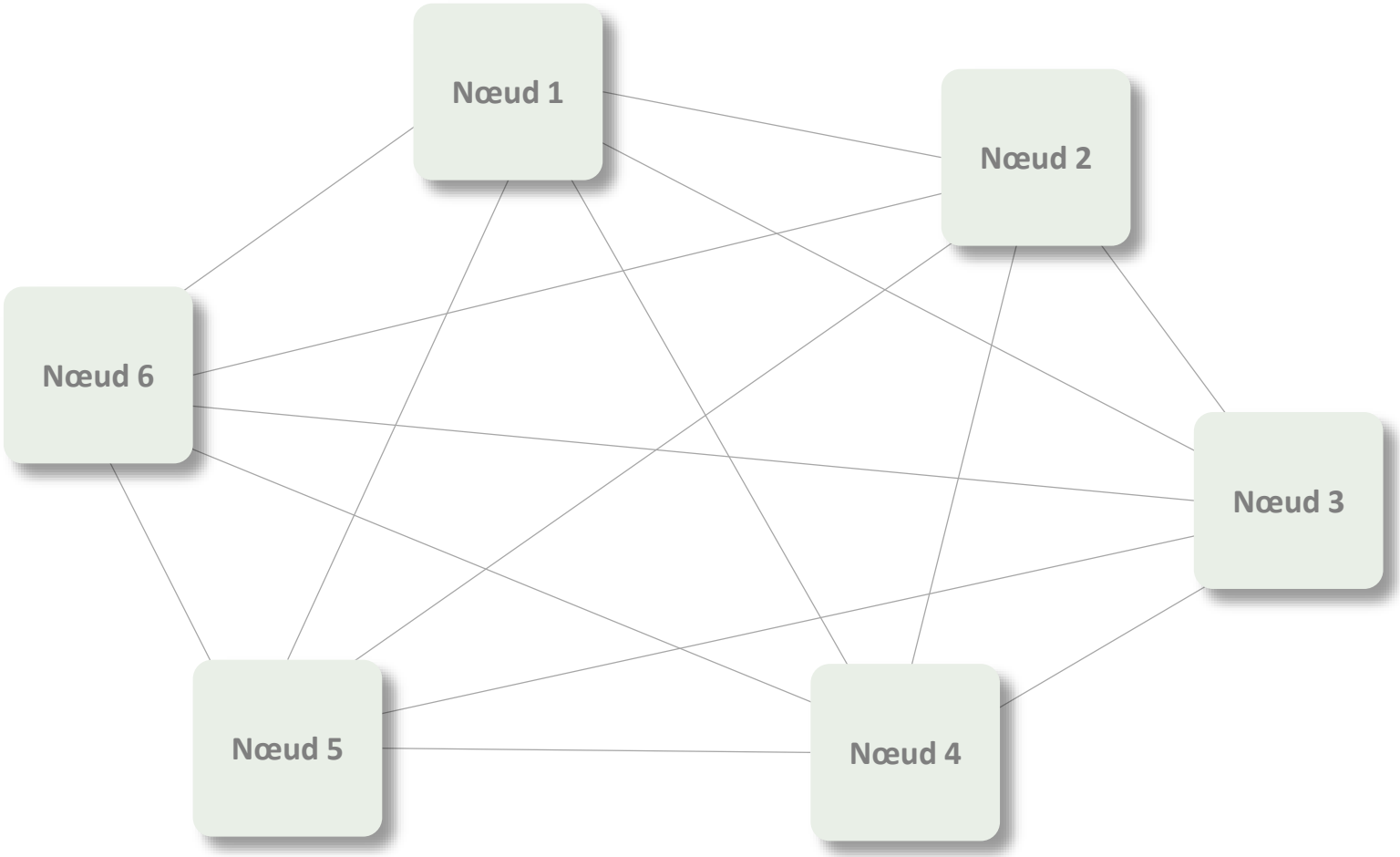
- https://bitcoin.org/bitcoin.pdf

Mots clés :

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

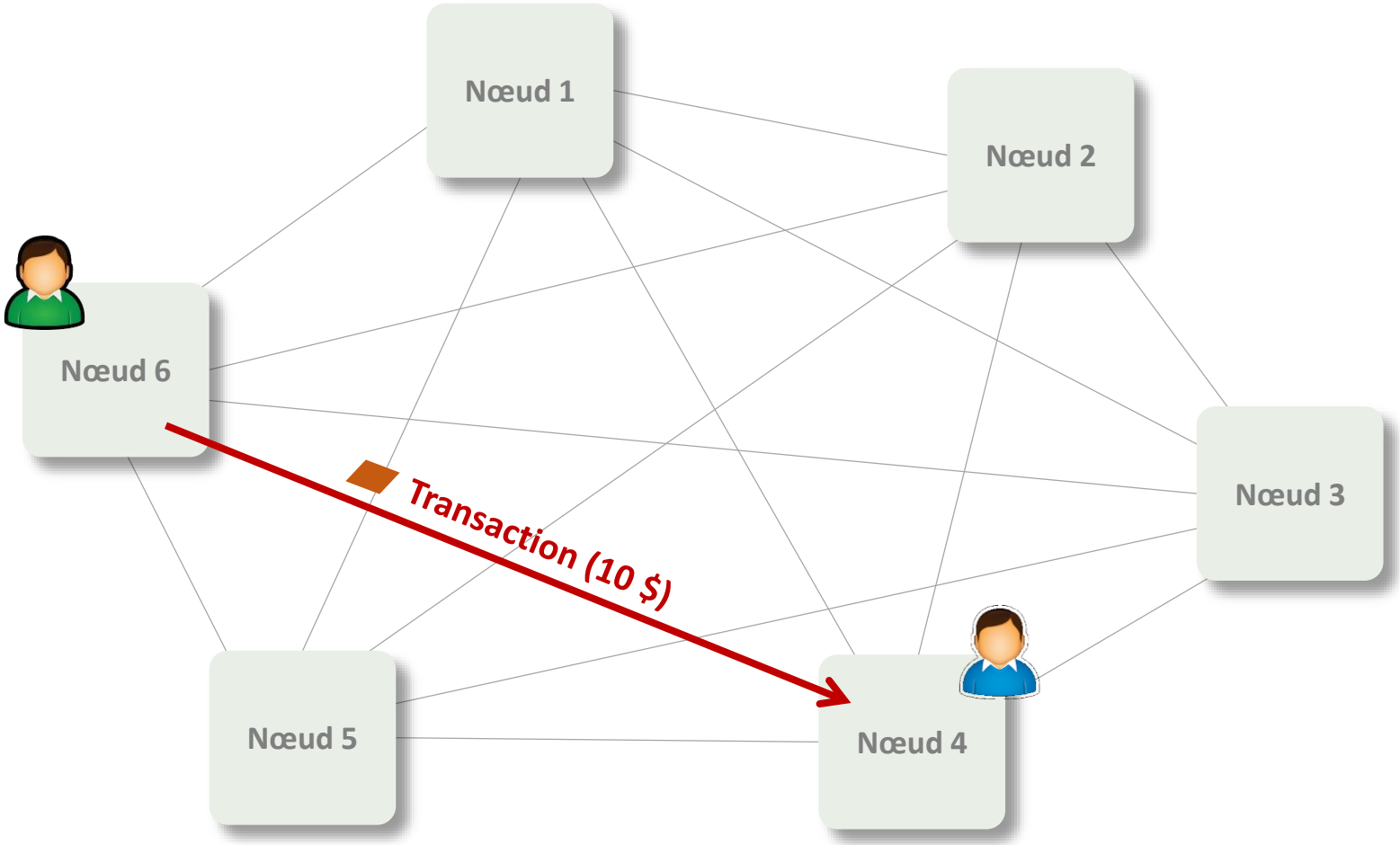
Bitcoin

Principe de fonctionnement



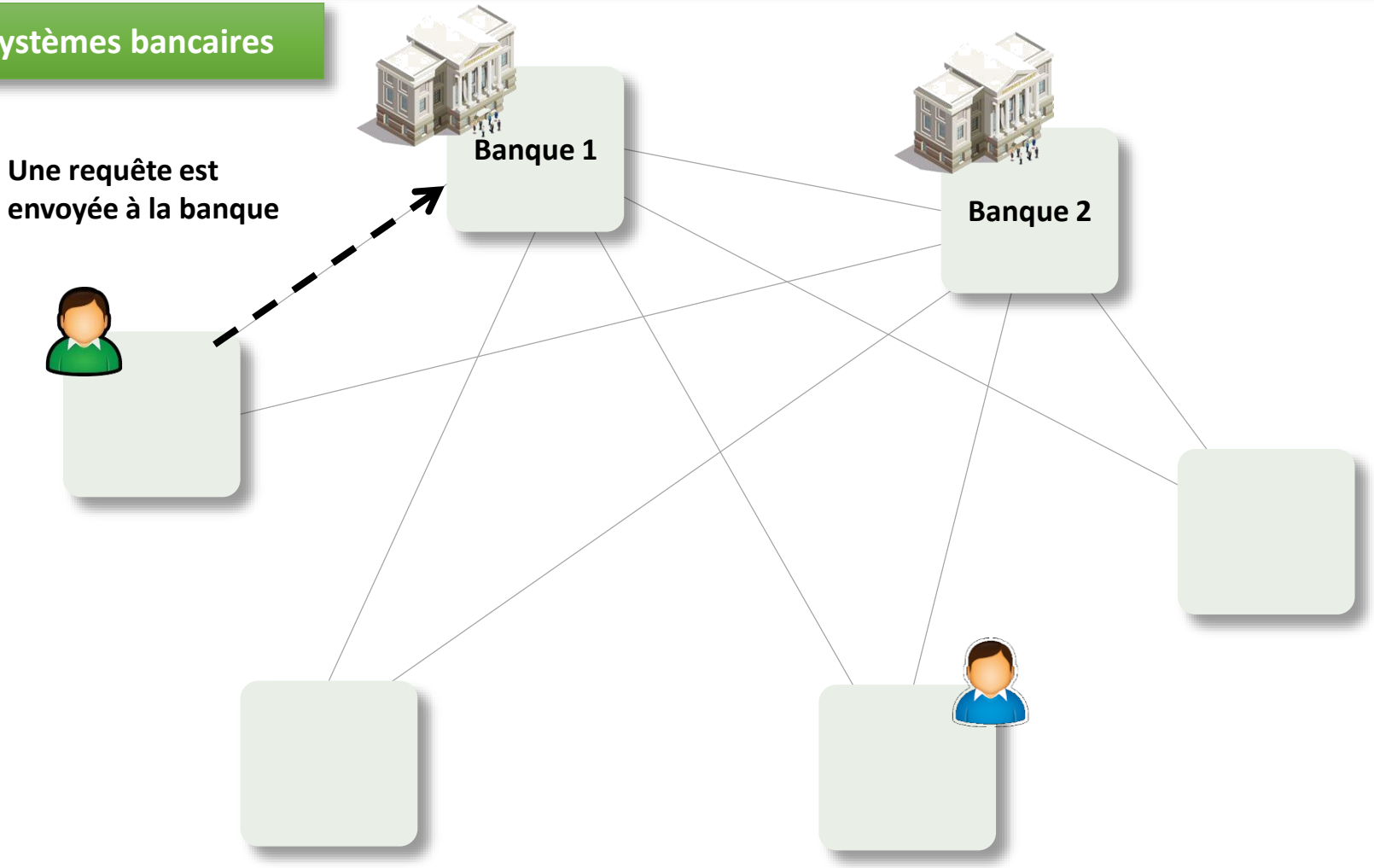
Bitcoin

Principe de fonctionnement



Principe de fonctionnement

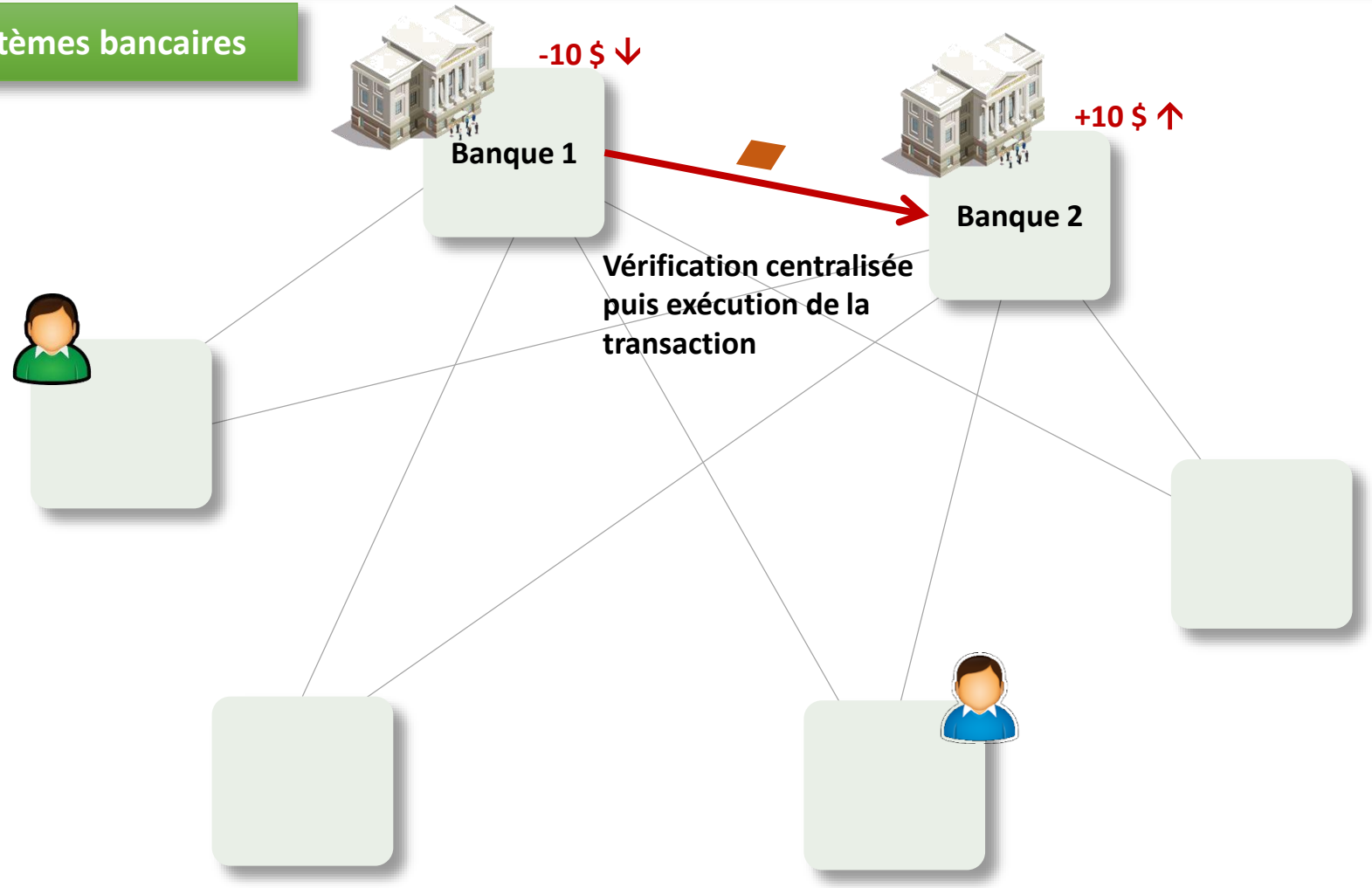
Systèmes bancaires



Bitcoin

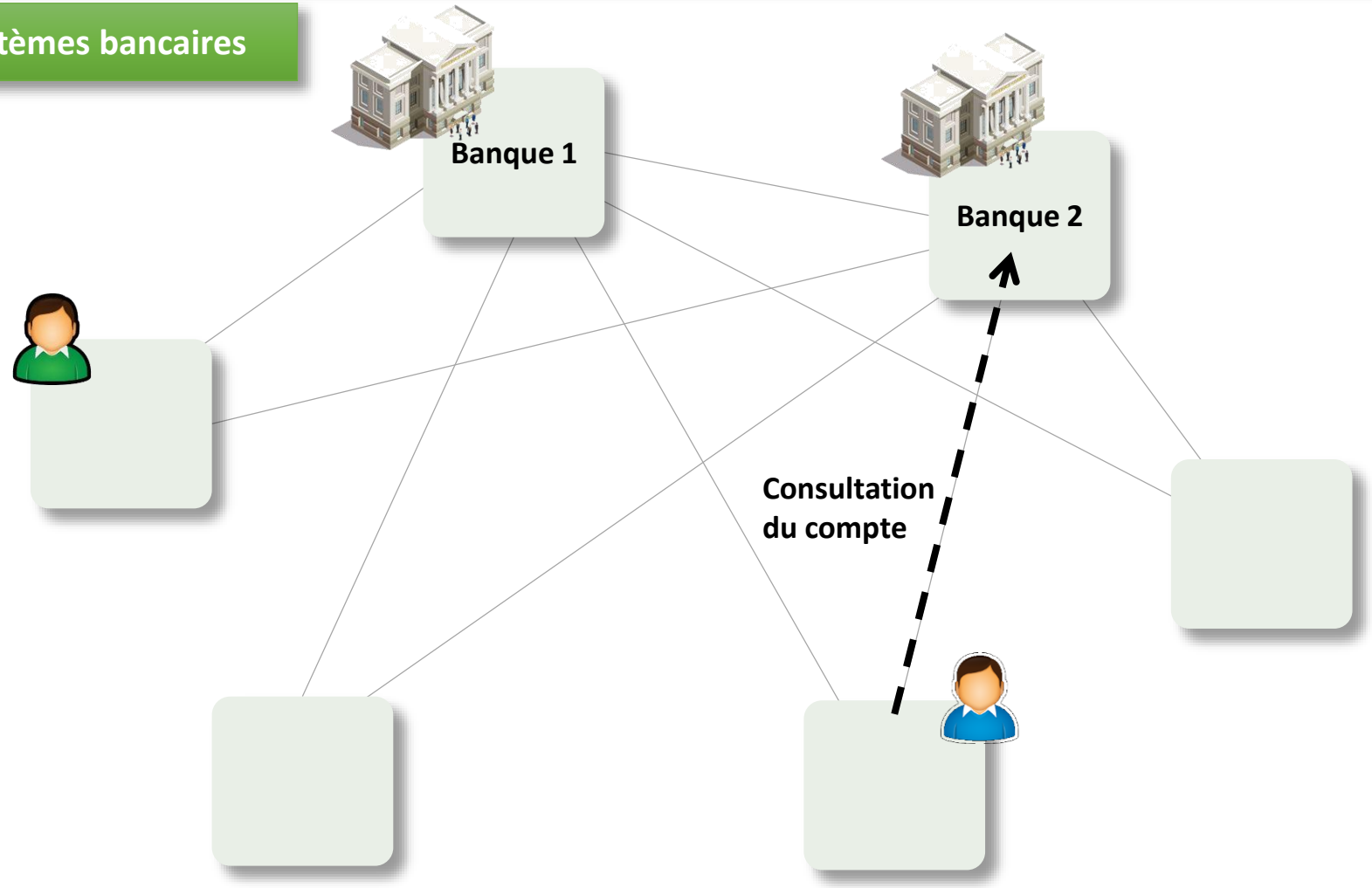
Principe de fonctionnement

Systèmes bancaires



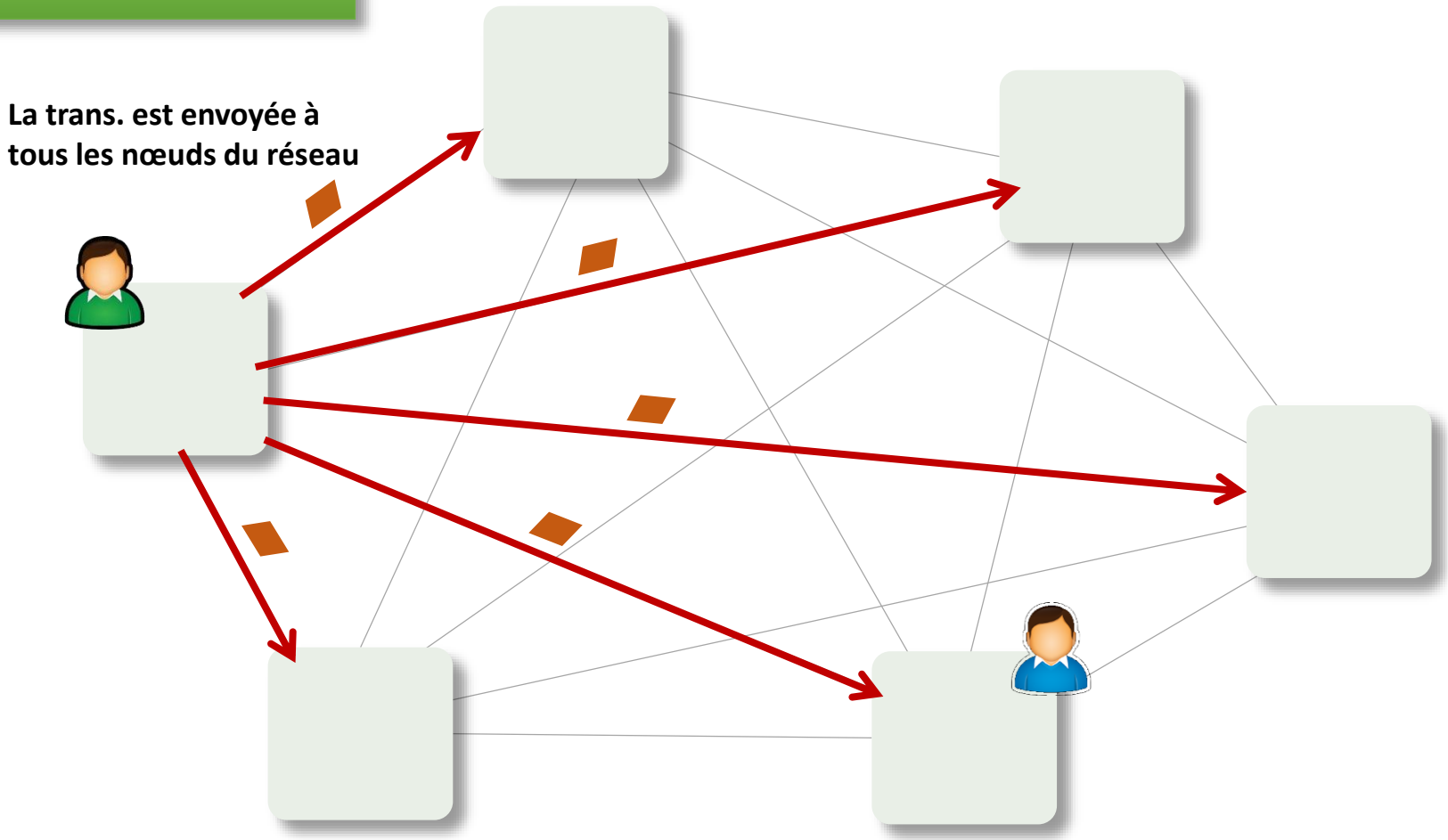
Principe de fonctionnement

Systèmes bancaires



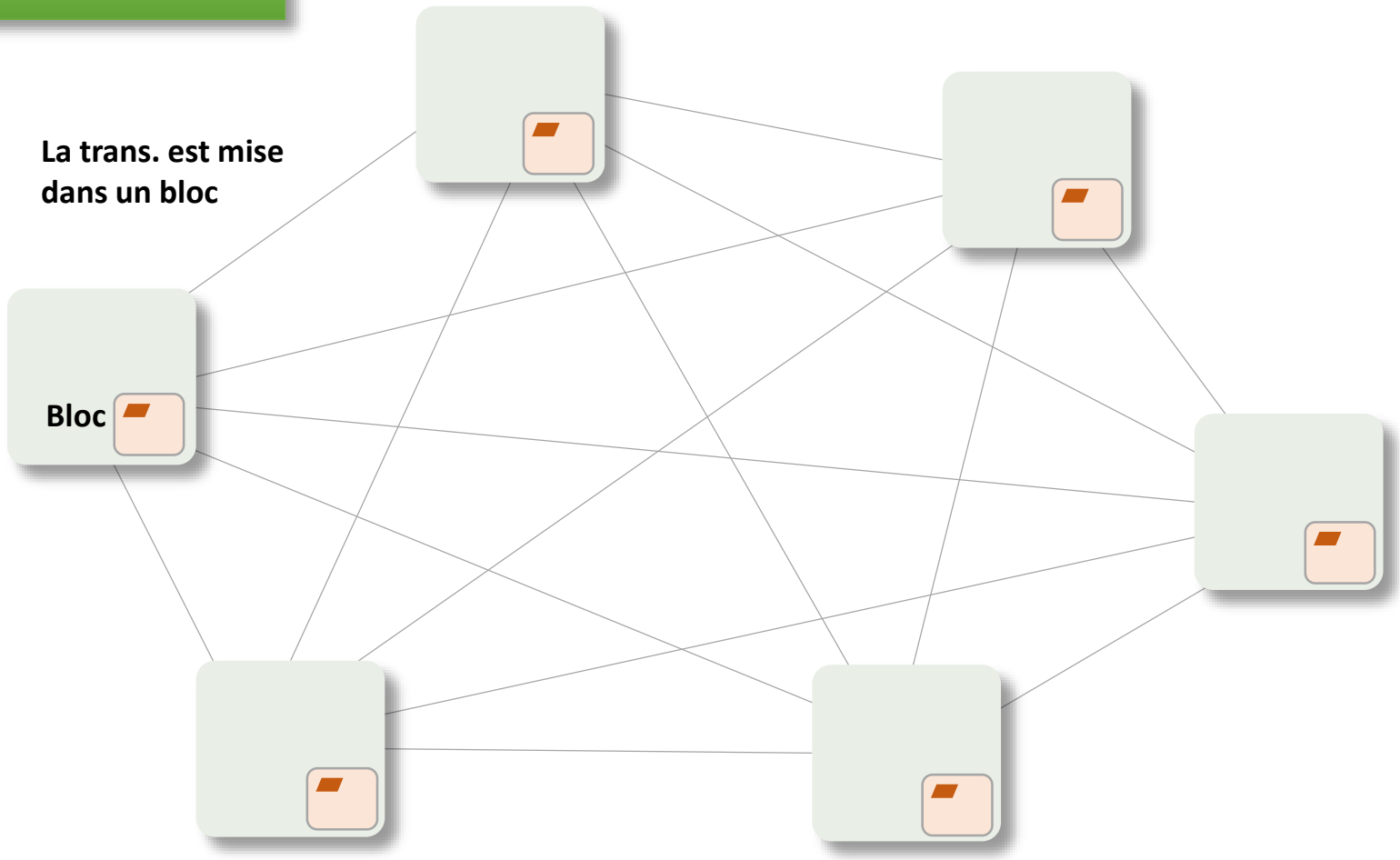
Principe de fonctionnement

Blockchain



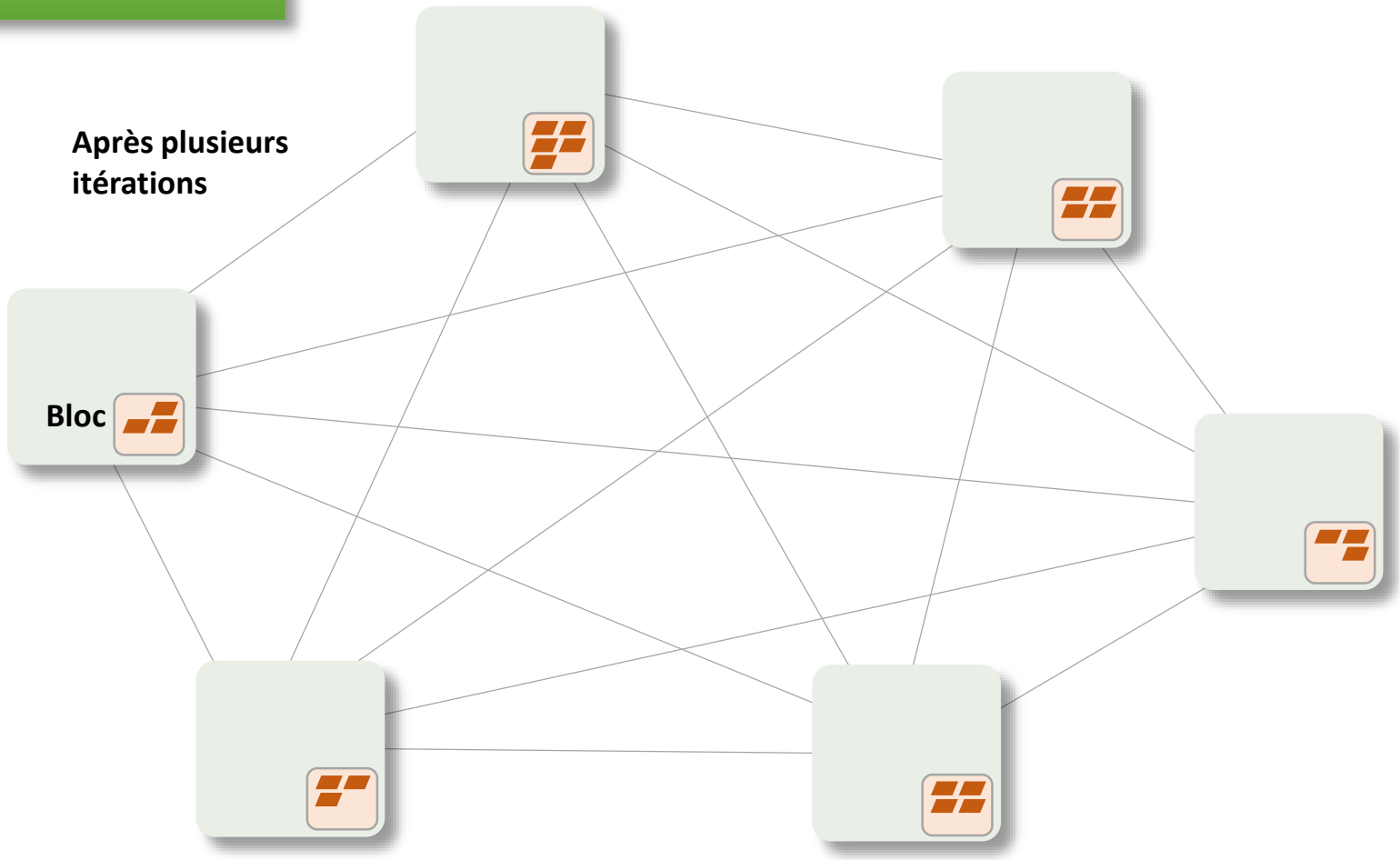
Principe de fonctionnement

Blockchain



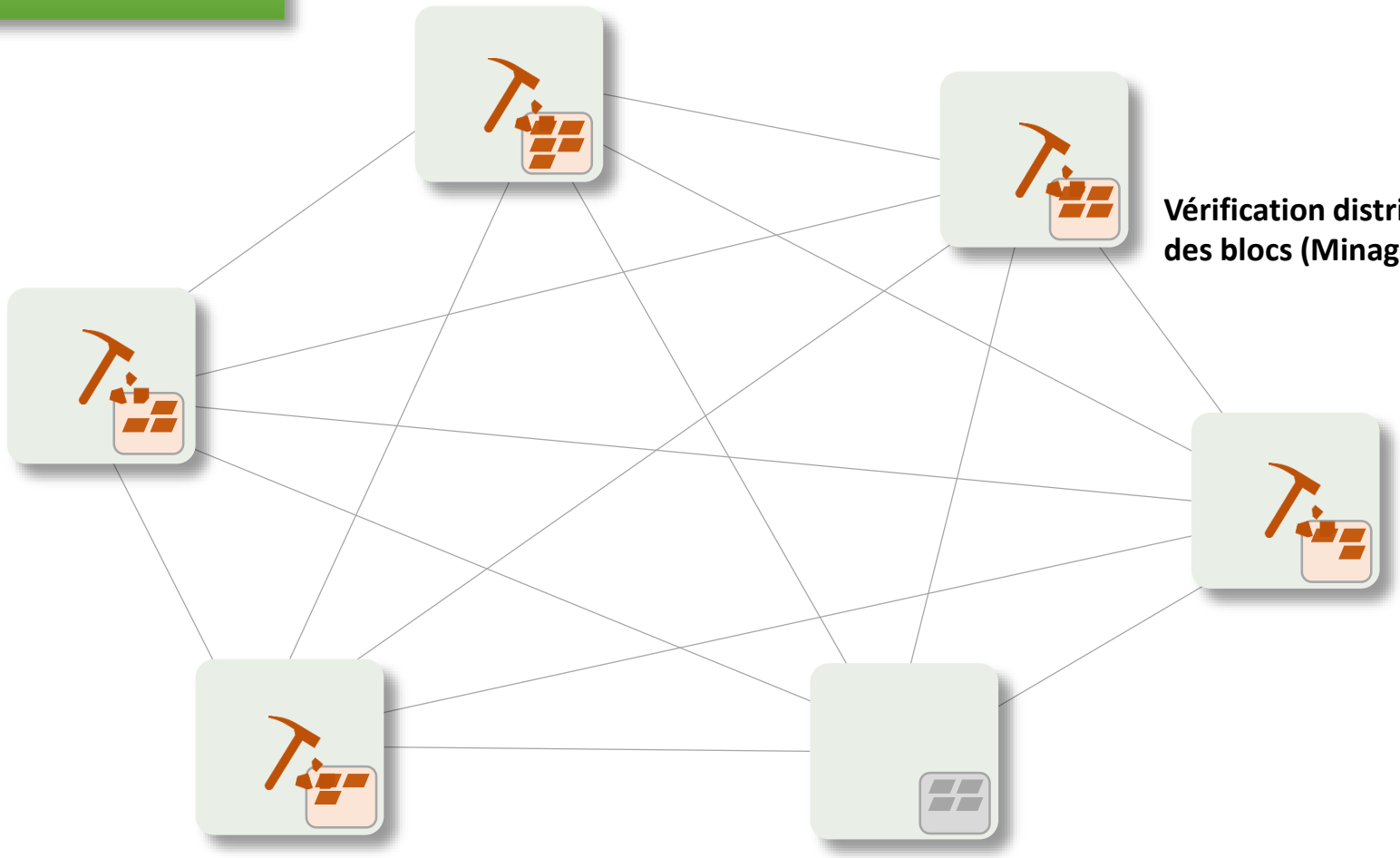
Principe de fonctionnement

Blockchain



Principe de fonctionnement

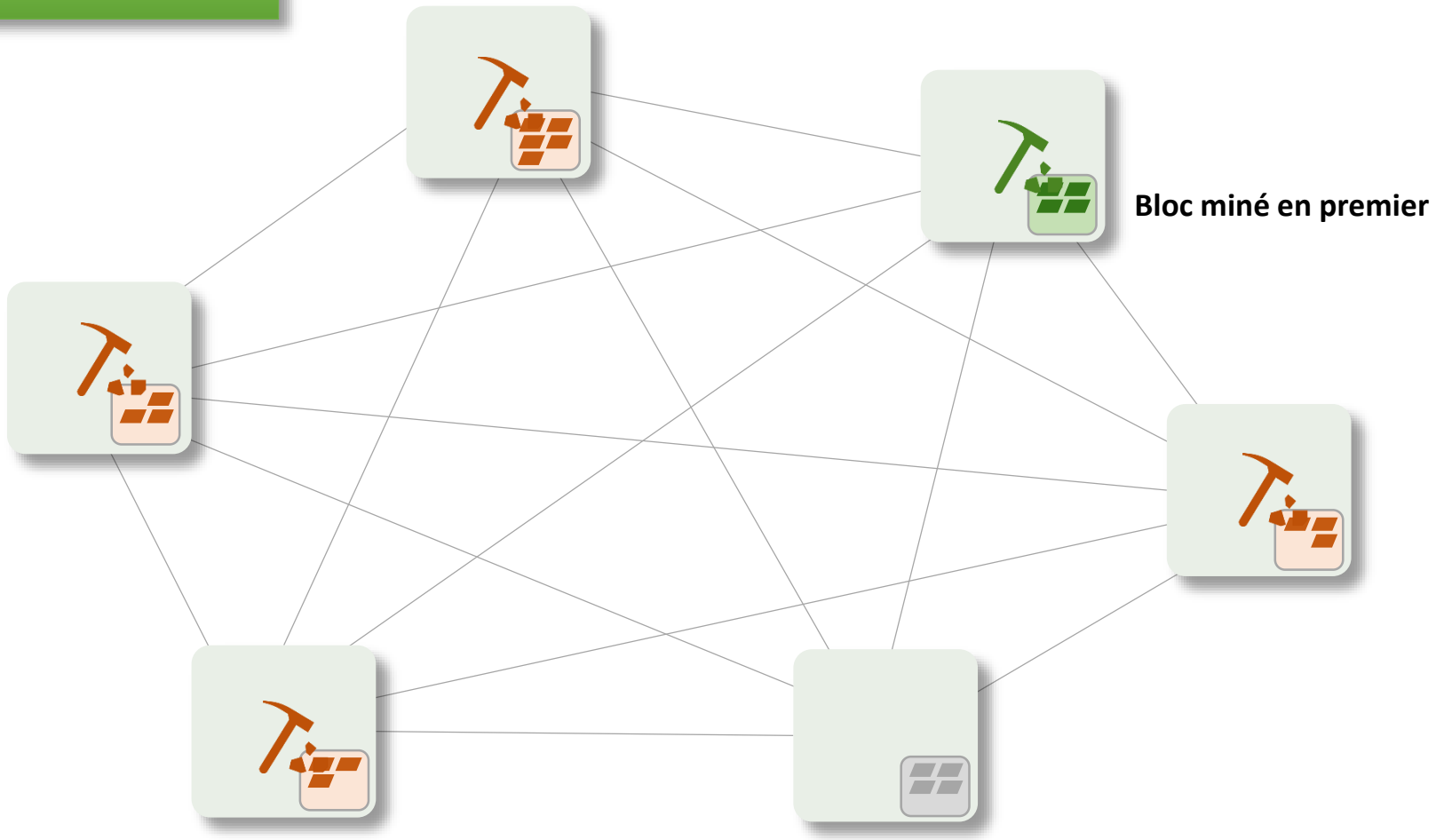
Blockchain



Vérification distribuée des blocs (Minage)

Principe de fonctionnement

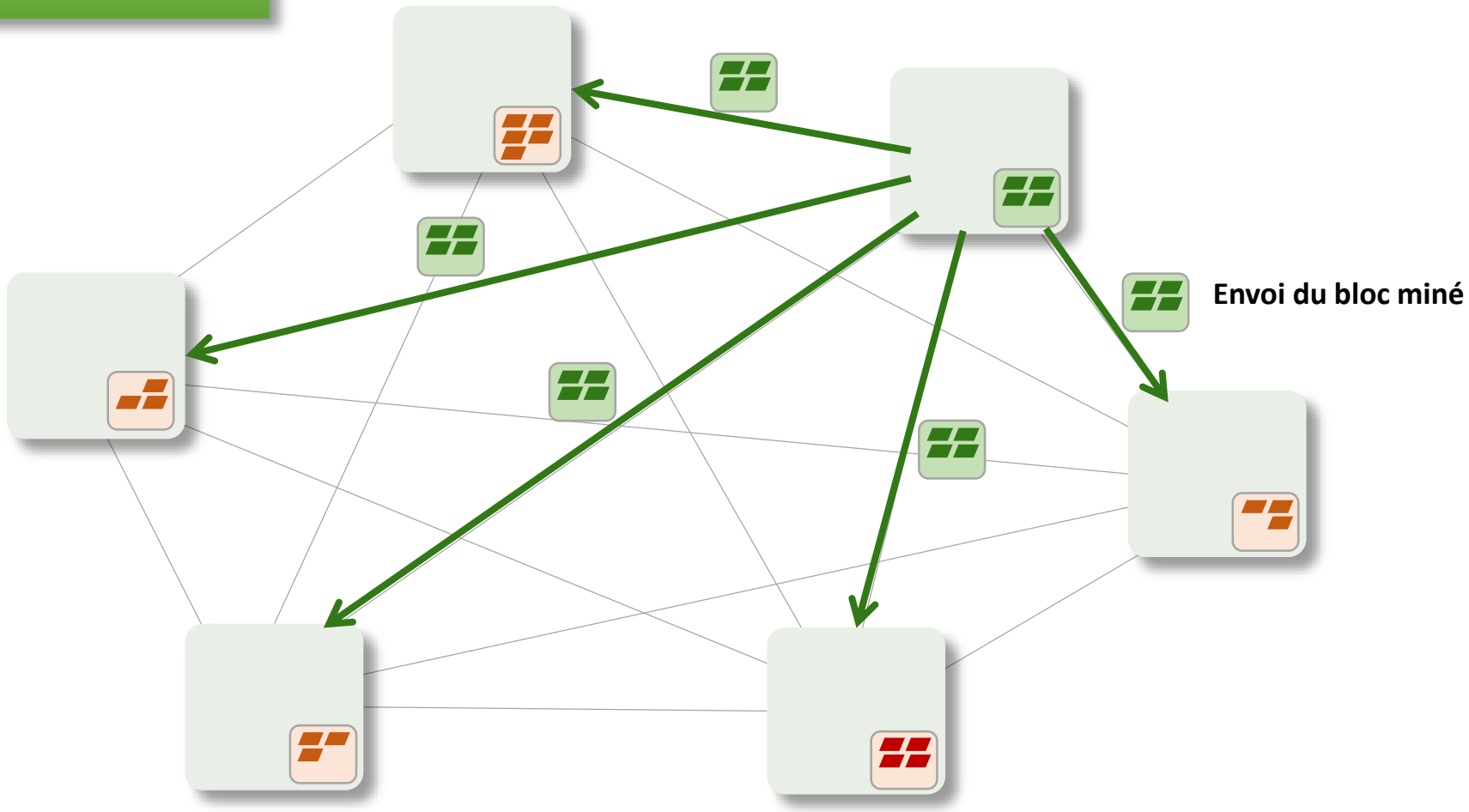
Blockchain



Bitcoin

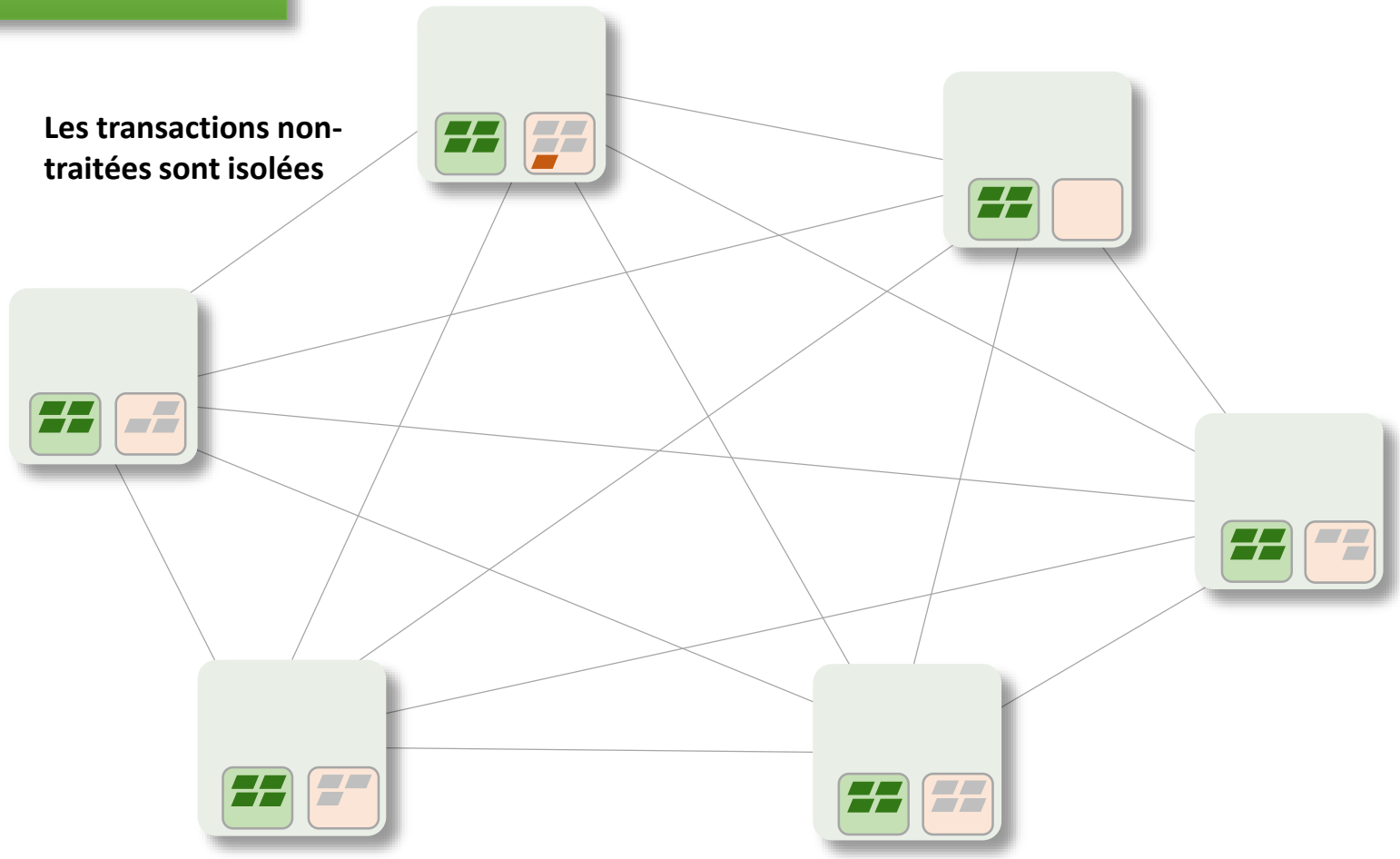
Principe de fonctionnement

Blockchain



Principe de fonctionnement

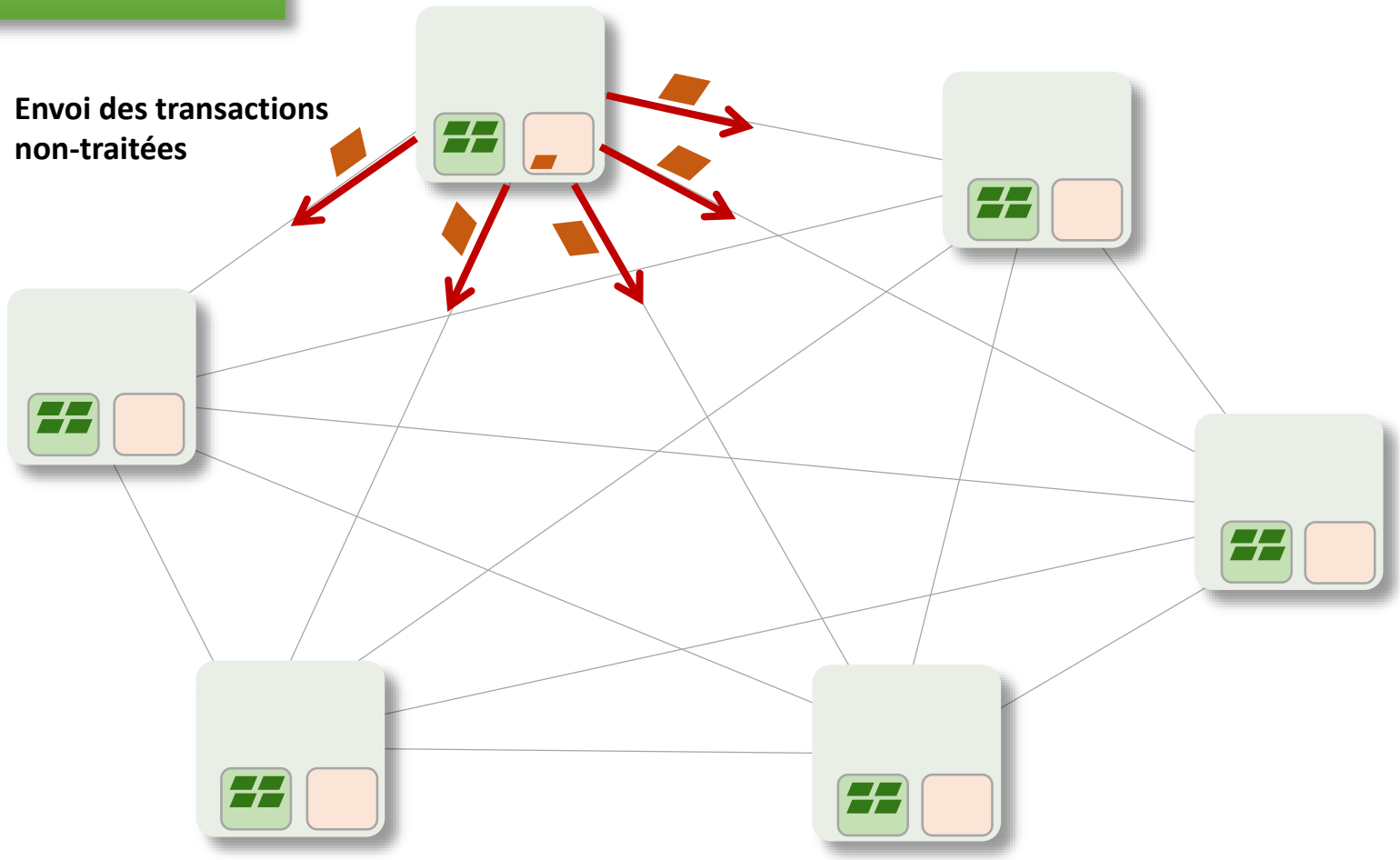
Blockchain



Bitcoin

Principe de fonctionnement

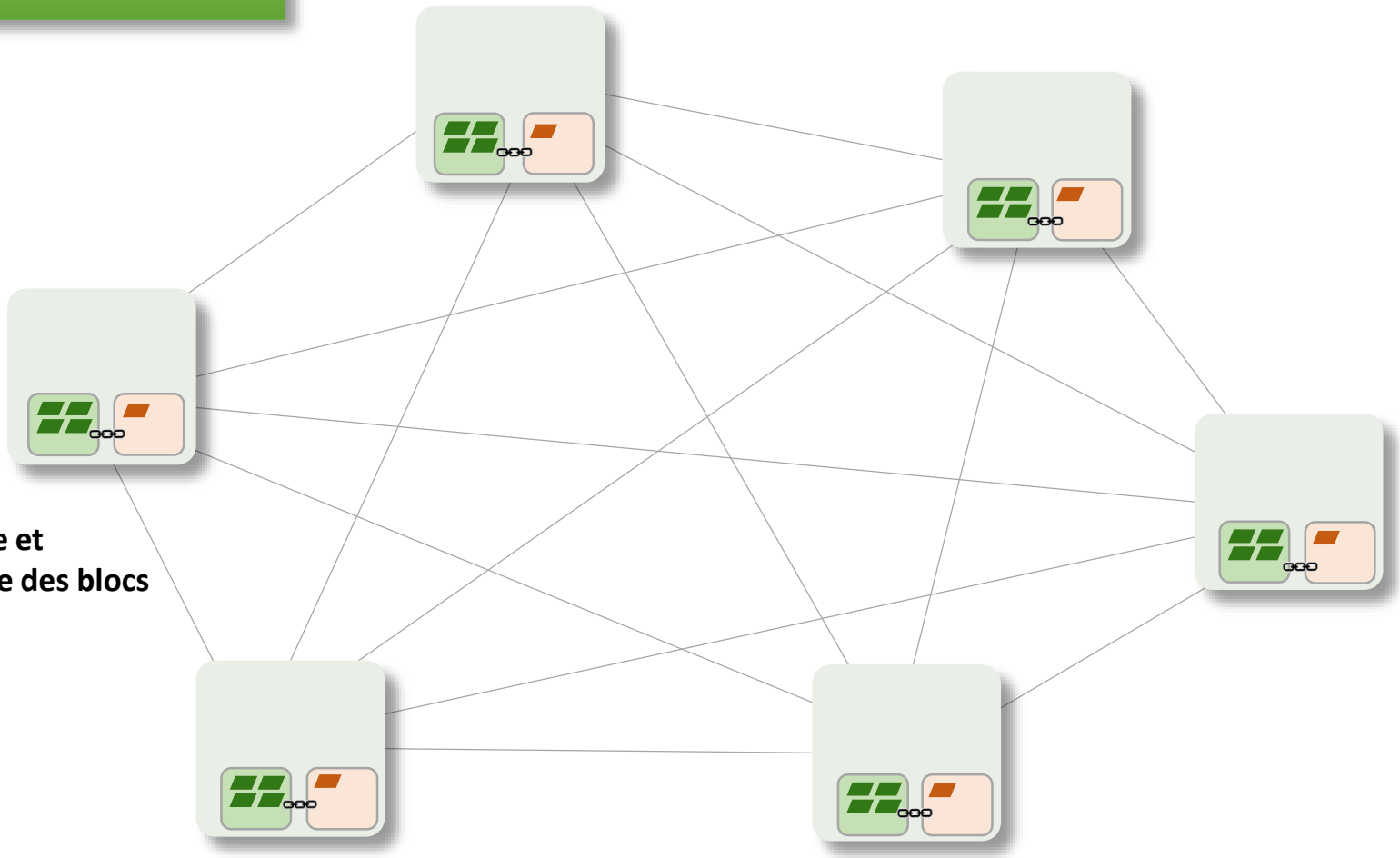
Blockchain



Bitcoin

Principe de fonctionnement

Blockchain



Hachage et chainage des blocs

Propriétés de la Blockchain

Désintermédiation :

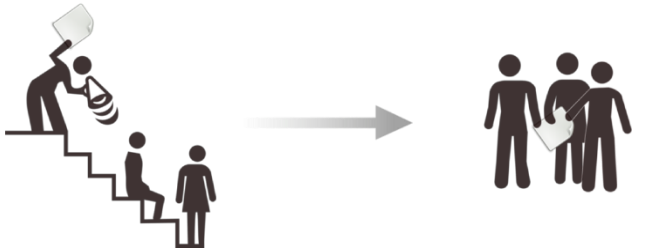
- Pas d'autorité centrale
- Données partagées dans tous les nœuds du réseau
- Architecture décentralisée

Autonomie :

- Blocs horodatés (time-stamped) et hachés
- Émission de crypto-monnaies (ex: Bitcoin)

Sécurité :

- Blocs chainés cryptographiquement
- Minage et preuve de travail
- Protection cryptographique



Centralisé Décentralisé