



Blockchain & Decentralized Applications

Ahmed Zinedine



2

Objectifs

- ▶ Avoir une compréhension et une connaissance pratique de la technologie émergente de la blockchain.
- ▶ penser à des modèles d'application innovants, en tirant parti de la technologie blockchain.
- ▶ Comprendre les contrats intelligents, une idée centrale et un modèle de calcul de la blockchain qui permet l'automatisation, l'autonomie, l'évolutivité et la transparence.
- ▶ Concevoir et programmer des contrats intelligents et des applications décentralisées.



Sommaire

- 1. Introduction**
- 2. Bitcoin**
- 3. Ethereum**
- 4. Smart Contracts**
- 5. Decentralized Applications (dApps)**
- 6. Blockchain Platforms**



4

Documentation

- ▶ Toute la documentation nécessaire sera publiée sur la plateforme Moodle de la FSDM et sur la plateforme Google Classroom



5

Introduction

1

Dans ce chapitre vous allez voir:

- ▶ Un peu d'Historique
- ▶ Qu'est ce que une blockchain
- ▶ Objectifs de la blockchain
- ▶ Comment ça marche ?:
 - ▶ Structure (transactions, blocs, blockchain)
 - ▶ Réseau (création, validation, et propagation des transactions et blocs)
 - ▶ Consensus : minage, Forks,...



Un peu d'Historique

- ▶ La Blockchain est une technologie émergente qui a gagné beaucoup de terrain et d'attention durant toute cette dernière décennie.
- ▶ Certains disent qu'il s'agit de la plus grande innovation depuis l'invention de l'internet.
- ▶ D'autres affirme que cette technologie va certainement bouleverser beaucoup d'aspects de notre vie quotidienne ainsi que beaucoup des industries actuelles
- ▶ Elle va révolutionner les méthodes de transfert des actifs et les modes de conduire les affaires et bien beaucoup d'autres chose.

Un peu d'Historique

- ▶ Un jour de 2008, Satoshi Nakamoto a publié un papier intitulé « Bitcoin : A Peer-to-Peer Electronic Cash System ».
- ▶ Dans ce papier, Nakamoto a décrit le concept d'un **système de paiement** qui va permettre de procéder, d'une manière **cryptographiquement sécurisée**, à des **transactions** directes **pair à pair**, entre des **parties inconnues** les uns aux autres.
- ▶ Le même système crée une « **monnaie virtuelle** » qui s'appelle **Bitcoin** et qui n'a besoin d'aucune autorité centrale pour la frapper ou la gérer.
- ▶ Quelque mois après, la première implémentation opérationnelle du système est mise en place.
- ▶ Le **3 janvier 2009**, la première transaction bitcoin a été créée déclarant une nouvelle ère complètement **bouleversante et révolutionnaire**. C'est l'ère de la Blockchain.



Un peu d'Historique

Préliminaires et précurseurs de Bitcoin

- ▶ Histoire de la monnaie et des banques
- ▶ Les progrès en **cryptographie** et en **systèmes détribués**
- ▶ Les travaux de David Chaum (anonymat sur Internet)
- ▶ **Cypherpunks** et **Crypto-anarchistes**
- ▶ Recherches sur la crypto-monnaie
 - ▶ **eCash** de David Chaum (1982)
 - ▶ **b-money** de Wei Dai (1998)
 - ▶ **bitGold** de Nick Szabo (1998)



Un peu d'Historique

Préliminaires et précurseurs de Bitcoin

- ▶ Autres pièces existantes réutilisées dans Bitcoin:
 - ▶ **Timestamping** : Travaux de Stuart Haber & W. Scott Stornetta (1991-1993-1997)
 - ▶ **HashCash** : de Adam Back (1997-2002)
 - ▶ **RPoW** : de Hal Finney (2004)



Un peu d'Historique

Et enfin Satoshi Nakamoto a mis le tous ensemble et a créé **Bitcoin**.

1. un système de monnaie numérique fonctionnant en continu
2. un modèle de technologie d'application décentralisée autonome appelé **blockchain**.

Les spécialistes ont vite réalisé le potentiel énorme de cette technologie et ont remarqué qu'elle peut facilement s'étendre à d'autre champs d'application au-delà de la crypto-monnaie et des paiements.



Qu'est que une Blockchain ?

Quand on dit Blockchain, on fait d'habitude référence à trois aspects sous-jacents :

1. Un réseau de nœuds **Pear-to-Pear**. Les nœuds du réseau sont sensés échanger des **transactions** et entretenir les opérations du réseau.
2. Un registre **décentralisé** sous forme de **blocs enchaînés**. Ces blocs contiennent les transactions valides circulées par les nœuds du réseau.
3. Un protocole (=ensemble de règles) codé sous forme de logiciel. Ce protocole précise les différentes activités du réseau; par exemple : comment créer, valider, et propager les transactions et les blocs, comment arriver au consensus en cas de conflit ...etc...



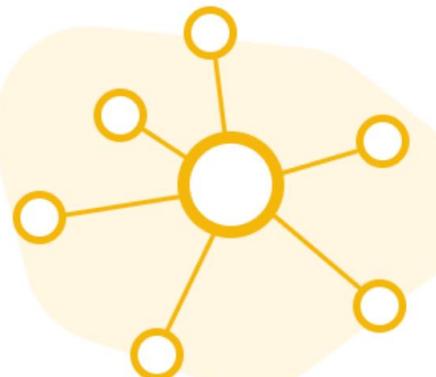
Objectifs de la Blockchain

Permettre des **transactions sécurisées**:

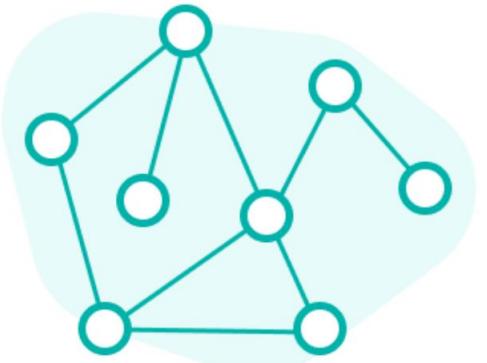
- ▶ **De pair à pair** (donc dans un réseau **décentralisé**, sans entités intermédiaires)
 - ▶ **Sans confiance** mutuelle entre les pairs
-
- ▶ C'est le **protocole de la blockchain** qui va créer une **confiance collective prouvable et garantie**.
 - ▶ Ce protocole assure le **consensus** sur la validité des transactions, des blocs et de la chaîne de blocs entière.
 - ▶ Les transactions sont enregistrées dans un **registre distribué immuable et pérenne**.

Centralized vs Decentralized

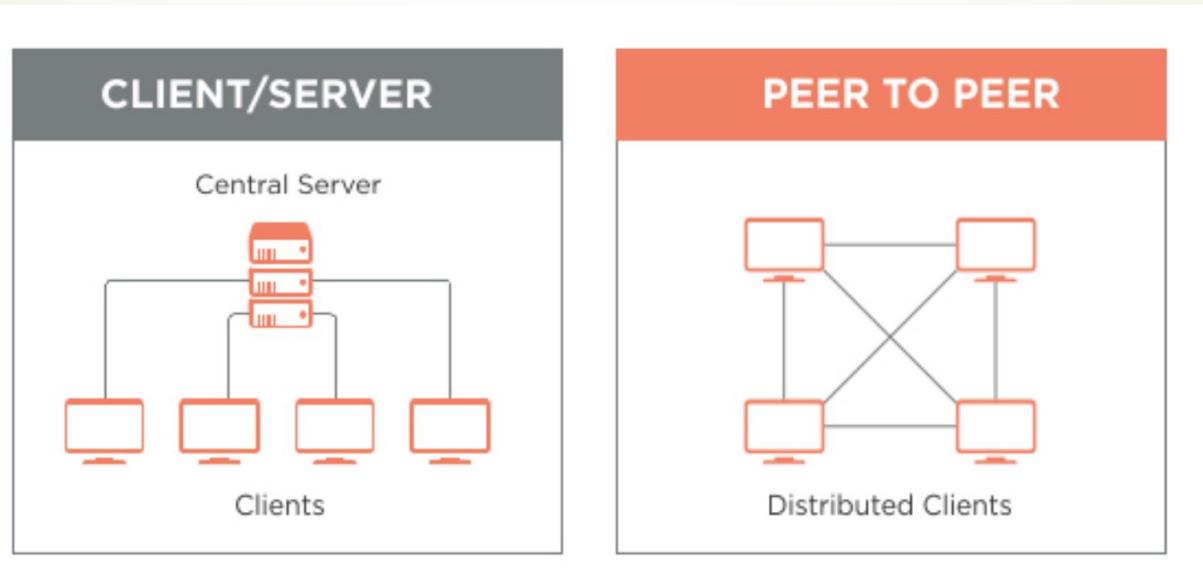
Centralized



Decentralized



Client/Server vs Peer to Peer



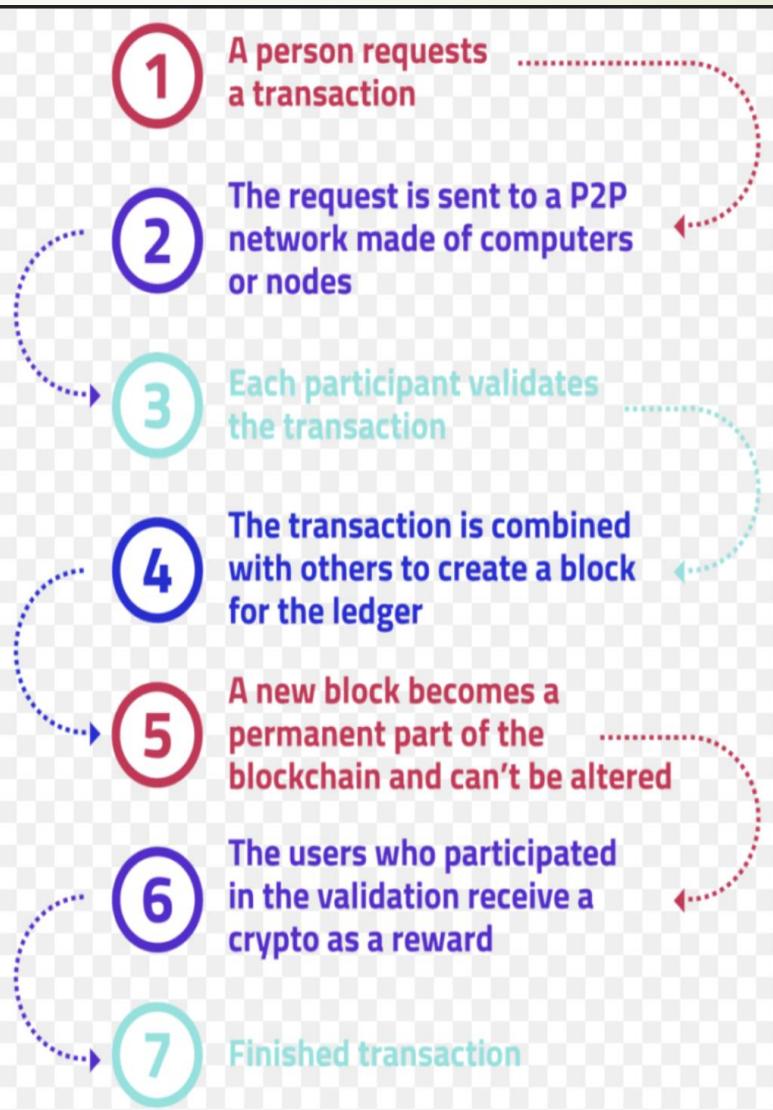


Comment ça fonctionne ?

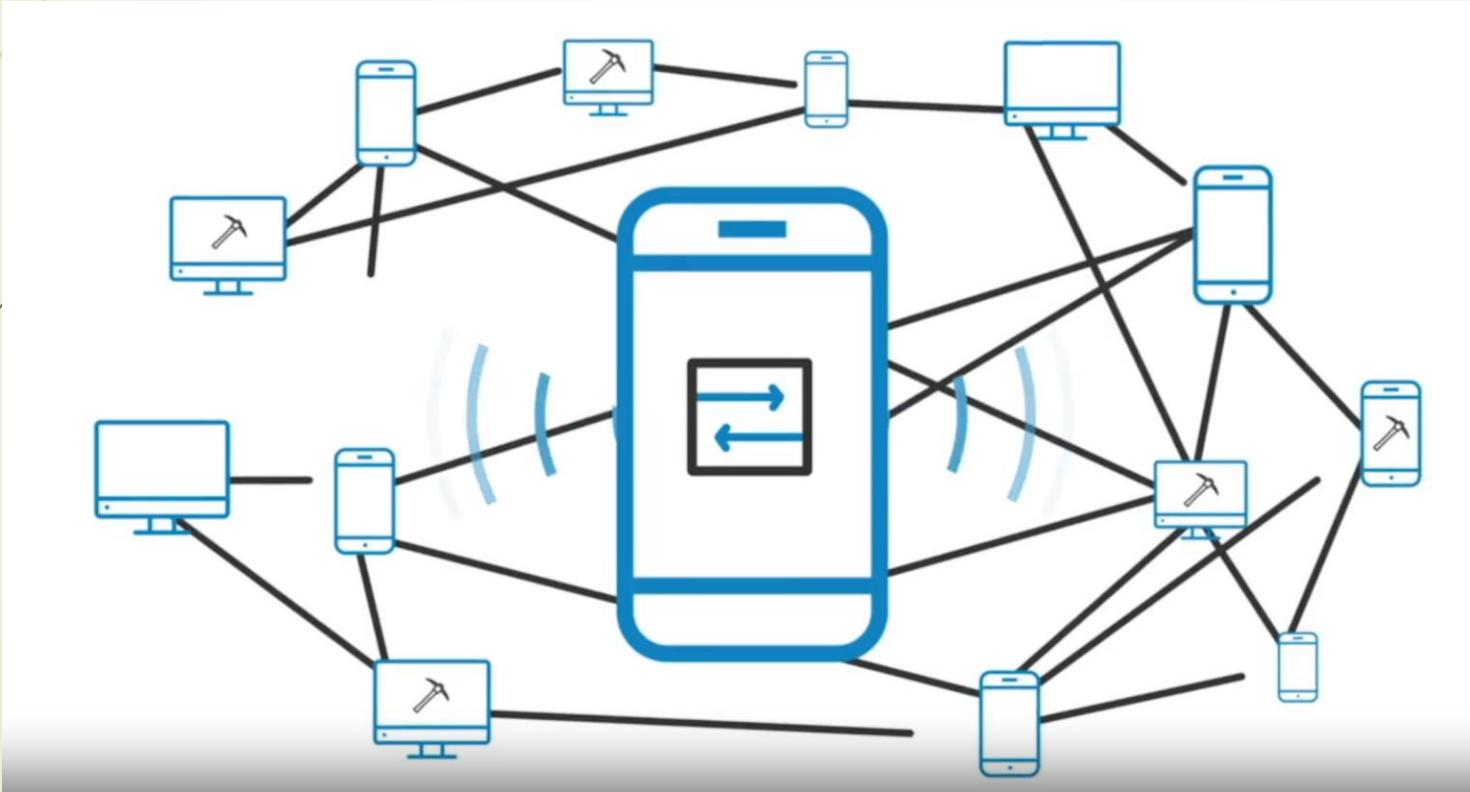
- ▶ Structures:
 - ▶ Transactions
 - ▶ Blocs
 - ▶ Registre (Chaine de blocs)
- ▶ Opérations du réseau:
 - ▶ Création, propagation et validation des transactions
 - ▶ Minage, propagation et validation des blocs
 - ▶ Maintien du registre
- ▶ Consensus

Comment ça fonctionne ?

Cycle de vie d'une transaction :



Diffusion d'une transaction

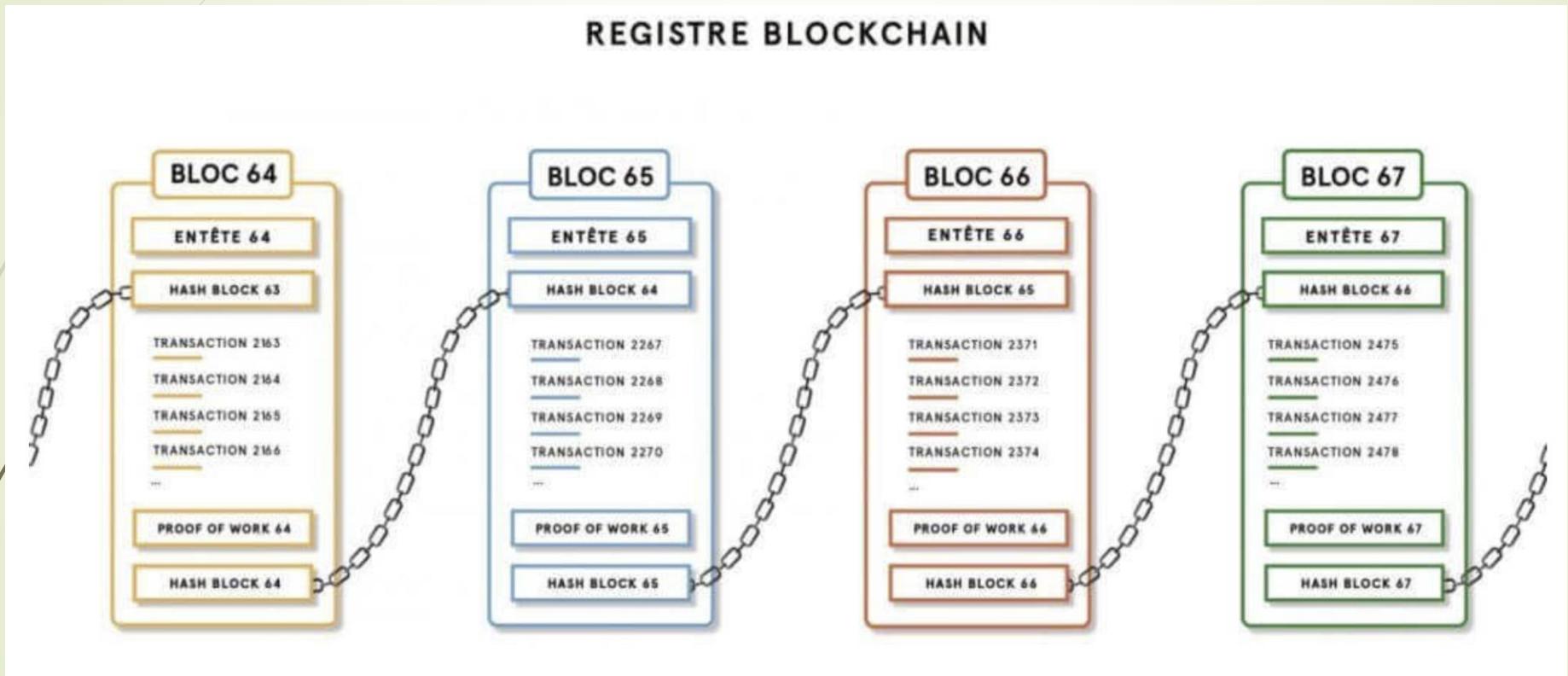


Les blocs

Un bloc regroupe plusieurs transactions:

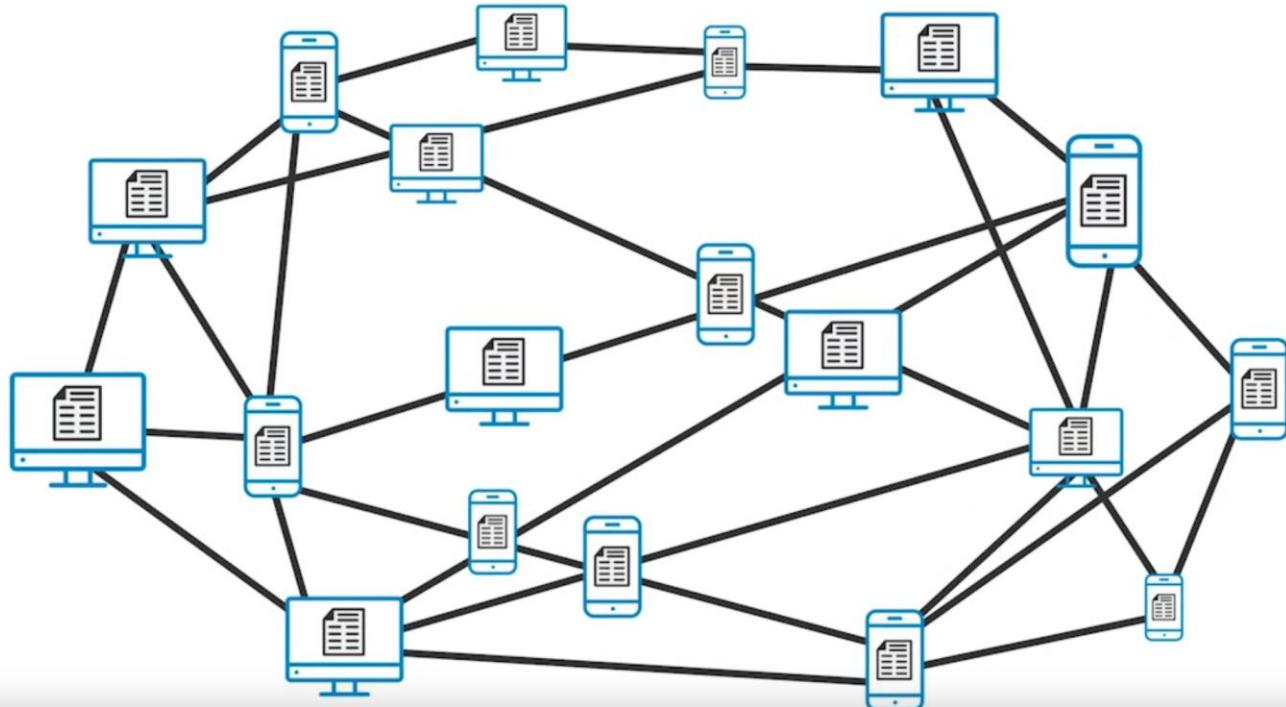


Chaîne de blocs immuables

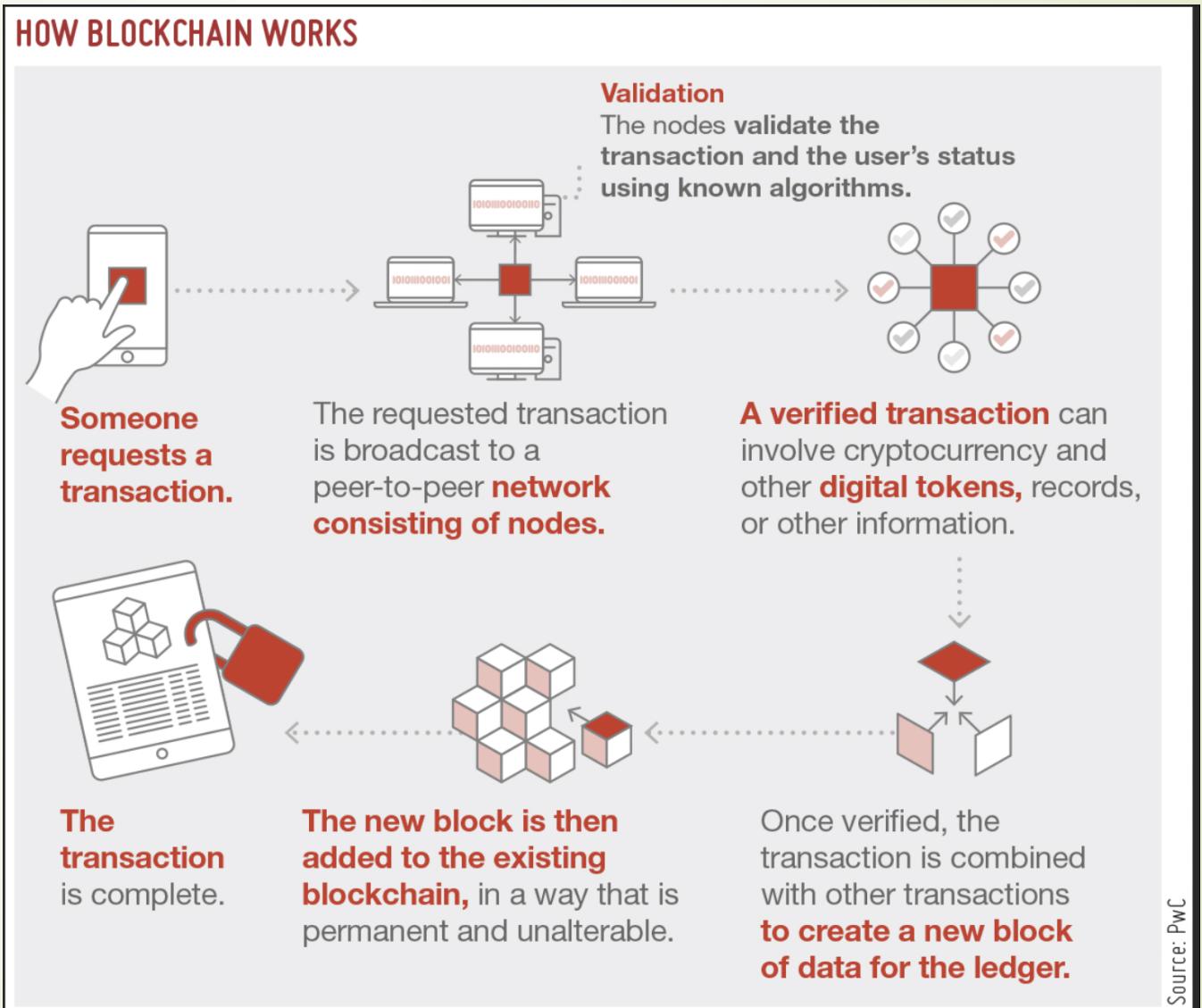


Registre décentralisé

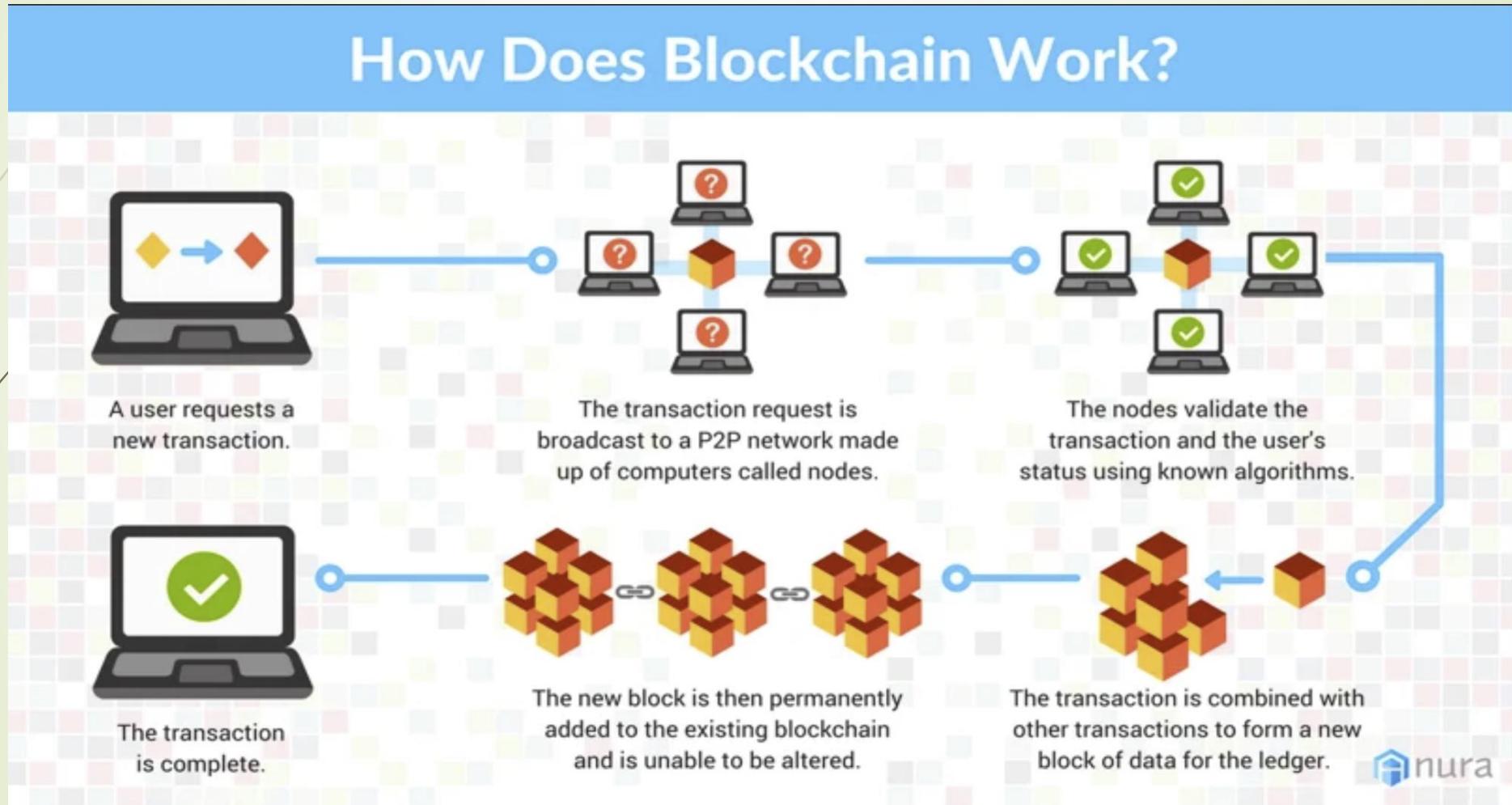
Chaque nœud du réseau garde sa propre copie du registre:



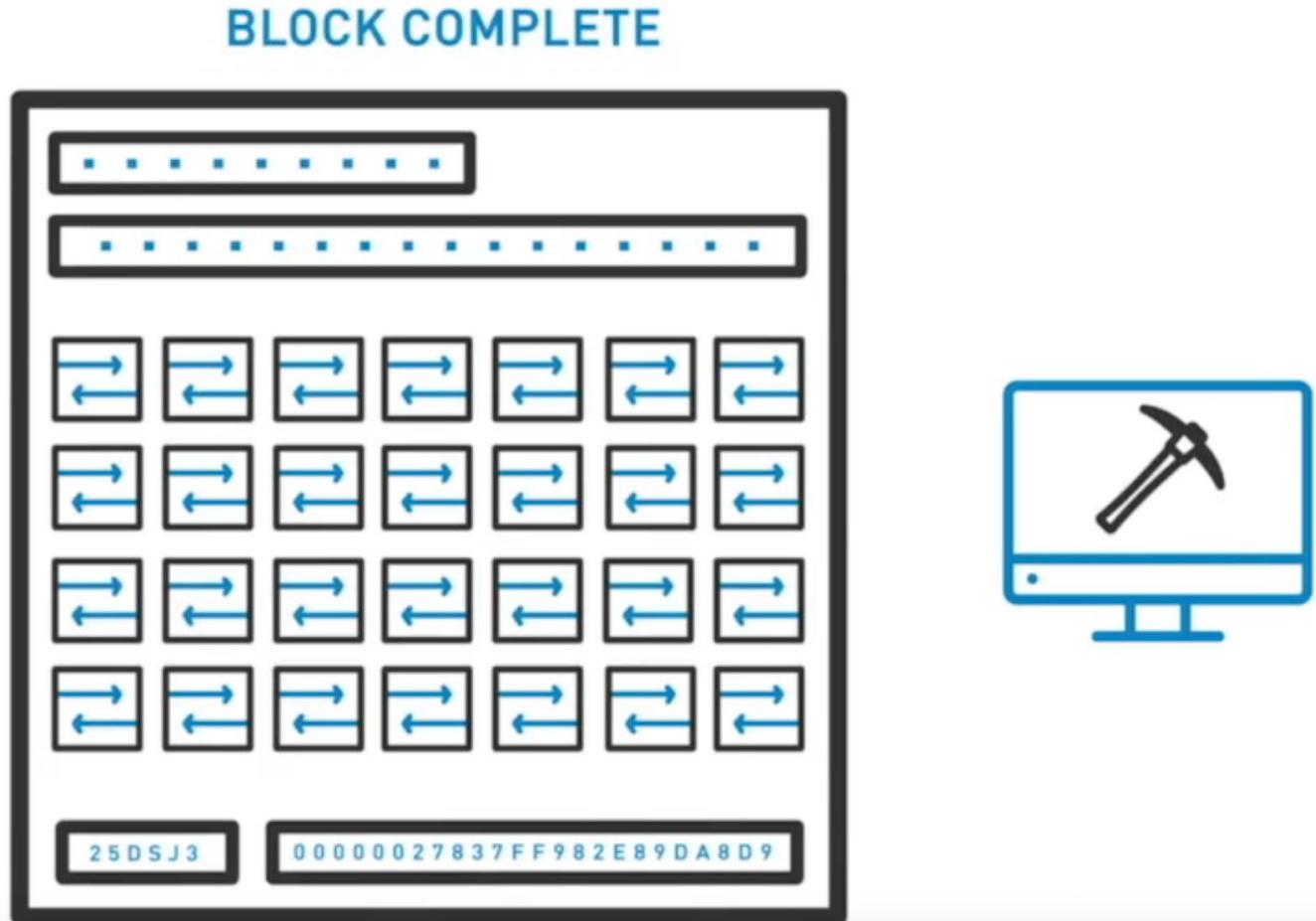
Comment ça fonctionne ?



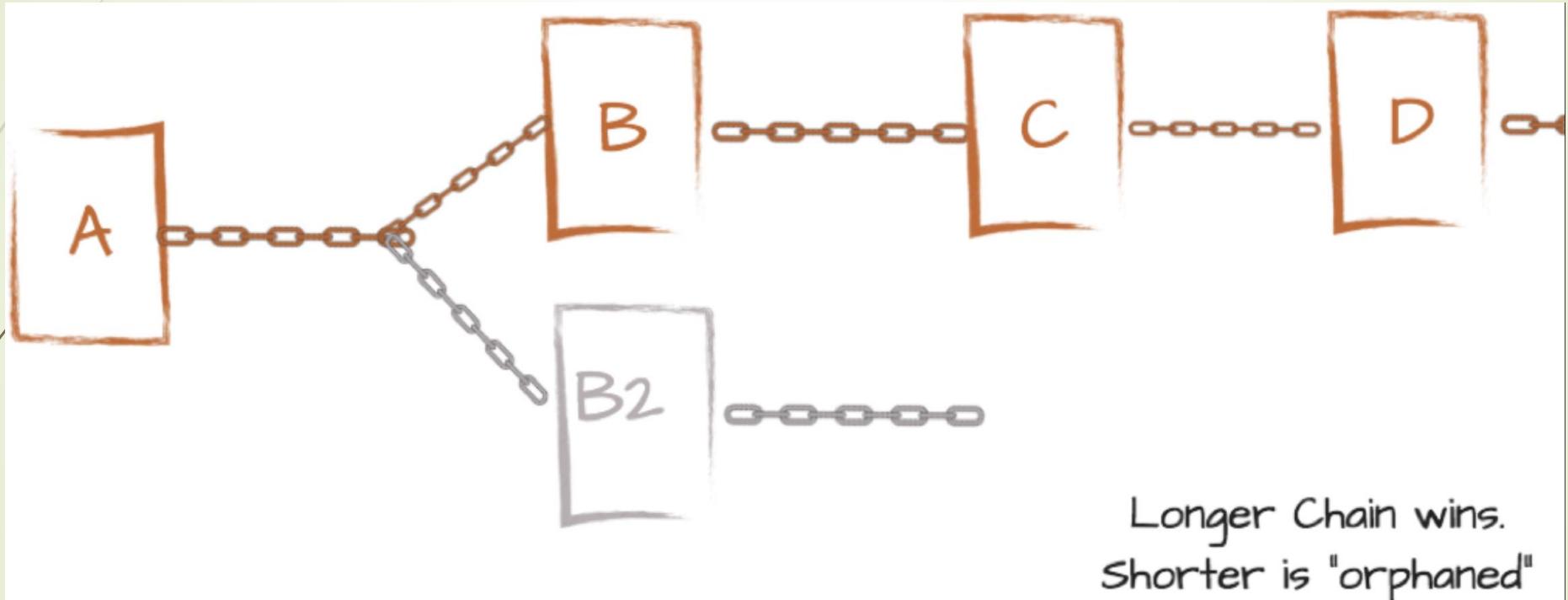
Comment ça fonctionne ?



Consensus: Minage d'un bloc



Consensus: Forks





25

Démo:

[Blockchain Demo \(andersbrownworth.com\)](http://andersbrownworth.com)

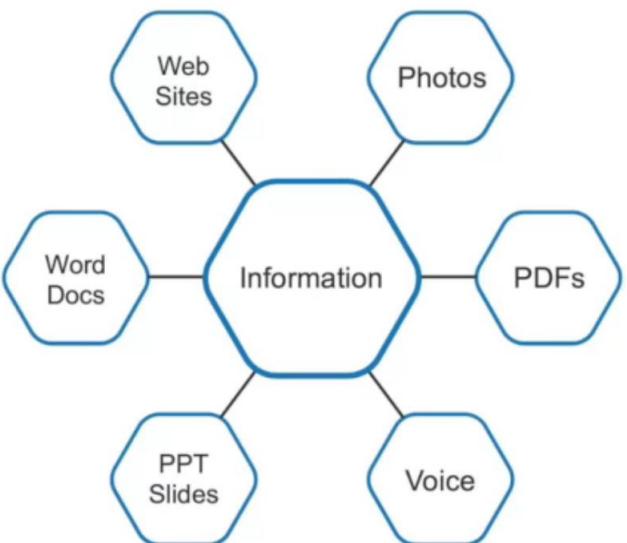


Au-delà de Bitcoin

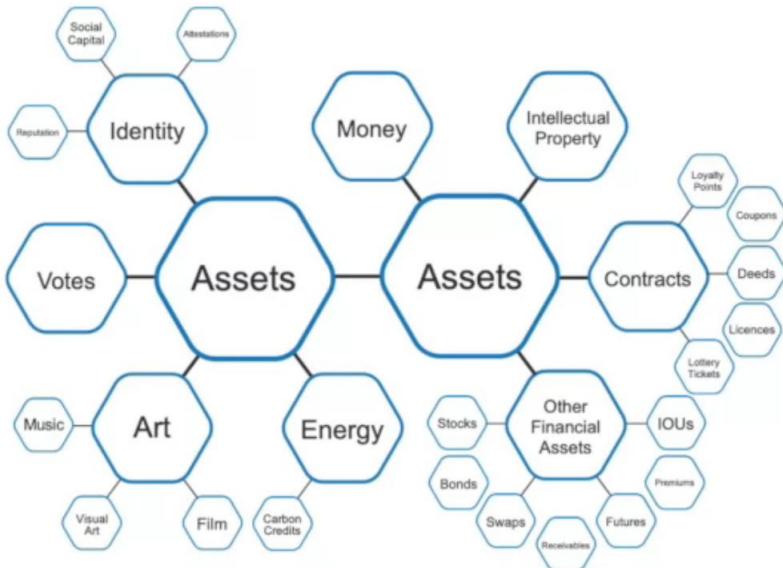
- ▶ Ethereum
- ▶ Smart Contract
- ▶ D'autres application
 - ▶ Tokens
 - ▶ NFT,
 - ▶ DAOs
 - ▶ Autres Application
- ▶ Web3

Web 3

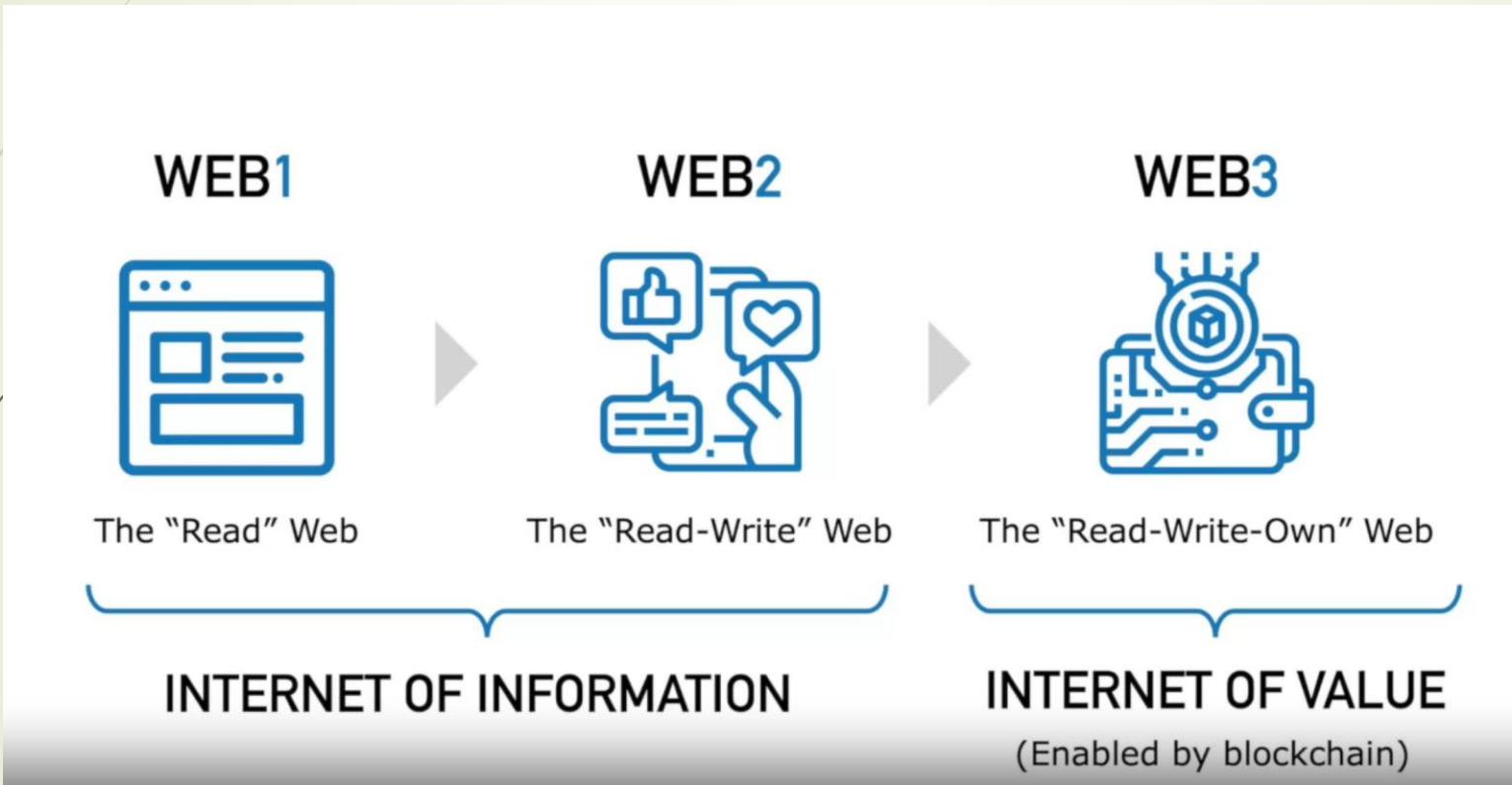
INTERNET OF INFORMATION



INTERNET OF VALUE



Web 3



Bitcoin



2

Dans ce chapitre vous allez voir:

- ▶ Introduction
- ▶ Le réseau Bitcoin
(Pair à pair, les différentes fonctions, Types de nœuds, Réseau Bitcoin Etendu)
- ▶ Comment joindre le réseau
(logiciel à installer selon la fonction voulue, Bitcoin core, Wallets,...)
- ▶ Structures
(Transactions, Blocs, BlockChain)
- ▶ Opérations
(Mining, Consensus,...)
- ▶ Sécurité
(Public Key Cryptography, Clés et Adresses, Attaques et Précautions,...)
- ▶ Application



Introduction

- ▶ Bitcoin est un ensemble de concepts et de technologies qui constituent la base d'un écosystème de **monnaie numérique**.
- ▶ Bitcoin comprend quatre innovations clés réunies dans une combinaison unique et puissante:
 - ▶ • Un réseau peer-to-peer décentralisé (le protocole Bitcoin)
 - ▶ • Un registre public des transactions (la blockchain)
 - ▶ • Un ensemble de règles pour la validation indépendante des transactions et l'émission de devises (règles de consensus)
 - ▶ • Un mécanisme pour parvenir à un consensus décentralisé mondial sur la blockchain valide (algorithme Proof-of-Work)



Introduction

- ▶ Des unités monétaires appelées **bitcoin** sont utilisées pour **stocker et transmettre de la valeur** entre les participants du réseau Bitcoin.
- ▶ Les utilisateurs peuvent **transférer** des bitcoins sur le réseau pour **acheter et vendre des biens, envoyer de l'argent** à des personnes ou à des organisations ou **accorder du crédit**.
- ▶ Le Bitcoin peut être **acheté, vendu et échangé** contre d'autres devises sur des bourses de devises spécialisées.
- ▶ Dans un certain sens, le bitcoin est la forme d'argent parfaite pour Internet car il est **rapide, sécurisé et sans frontières**.



Introduction

- ▶ Contrairement aux monnaies traditionnelles, le bitcoin est entièrement virtuel.
 - ▶ Il n'existe pas de pièces physiques.
 - ▶ Les pièces sont implicites dans des transactions qui transfèrent de la valeur de l'expéditeur au destinataire.
- ▶ Les utilisateurs possèdent des clés qui leur permettent de prouver la propriété de bitcoin sur le réseau Bitcoin.
- ▶ Avec ces clés, ils peuvent signer des transactions pour débloquer la valeur et la dépenser en la transférant à un nouveau propriétaire.
- ▶ Les clés sont souvent stockées dans un portefeuille numérique sur l'ordinateur ou le smartphone de chaque utilisateur.
- ▶ La possession de la clé permettant de signer une transaction est la seule condition préalable pour dépenser du bitcoin, mettant entièrement le contrôle entre les mains de chaque utilisateur.



Introduction

- ▶ les unités de bitcoin, sont créées via un processus appelé « minage »,
 - ▶ consiste à rivaliser pour résoudre un problème mathématique lors du traitement des transactions Bitcoin.
- ▶ Tout participant au réseau Bitcoin peut fonctionner comme un mineur, utilisant la puissance de traitement de son ordinateur pour vérifier et enregistrer les transactions.
- ▶ Toutes les 10 minutes, en moyenne, un mineur de Bitcoin peut valider les transactions des 10 dernières minutes et est récompensé par des nouveaux bitcoins.
- ▶ Essentiellement, le minage de bitcoin décentralise les fonctions d'émission de devises et remplace le besoin de toute banque centrale.

Introduction

- ▶ Le protocole Bitcoin comprend des algorithmes qui régulent la fonction minage:
 - ▶ La difficulté du problème est ajustée dynamiquement de sorte qu'on puisse créer un bloc toutes les 10 minutes en moyenne (quel que soit le nombre de mineurs).
 - ▶ Le protocole réduit également de moitié le taux de création de nouveaux bitcoins tous les 210000 blocs (environ 4 ans).
 - ▶ Il limite le nombre total de bitcoins qui seront créés à un total fixe ($\sim=21$ millions de pièces).
- ▶ Le résultat est que le nombre de bitcoins en circulation suit de près une courbe facilement prévisible qui approche les 21 millions d'ici 2140.
- ▶ En raison de la diminution du taux d'émission du Bitcoin, sur le long terme, la monnaie Bitcoin est déflationniste.
- ▶ De plus, le bitcoin ne peut pas être gonflé en « imprimant » de la nouvelle monnaie au-delà du taux d'émission attendu.



Introduction

- ▶ Bitcoin est aussi le nom du protocole, d'un réseau peer-to-peer et d'une innovation informatique distribuée.
- ▶ La monnaie bitcoin n'est en réalité que la première application de cette invention.
- ▶ Bitcoin représente l'aboutissement de décennies de recherche en cryptographie et en systèmes distribués.



Introduction

- Bitcoin comprend quatre innovations clés réunies dans une combinaison unique et puissante:
 - • Un réseau peer-to-peer décentralisé (le protocole Bitcoin)
 - • Un registre public des transactions (la blockchain)
 - • Un ensemble de règles pour la validation indépendante des transactions et l'émission de devises (règles de consensus)
 - • Un mécanisme pour parvenir à un consensus décentralisé mondial sur la blockchain valide (algorithme Proof-of-Work)



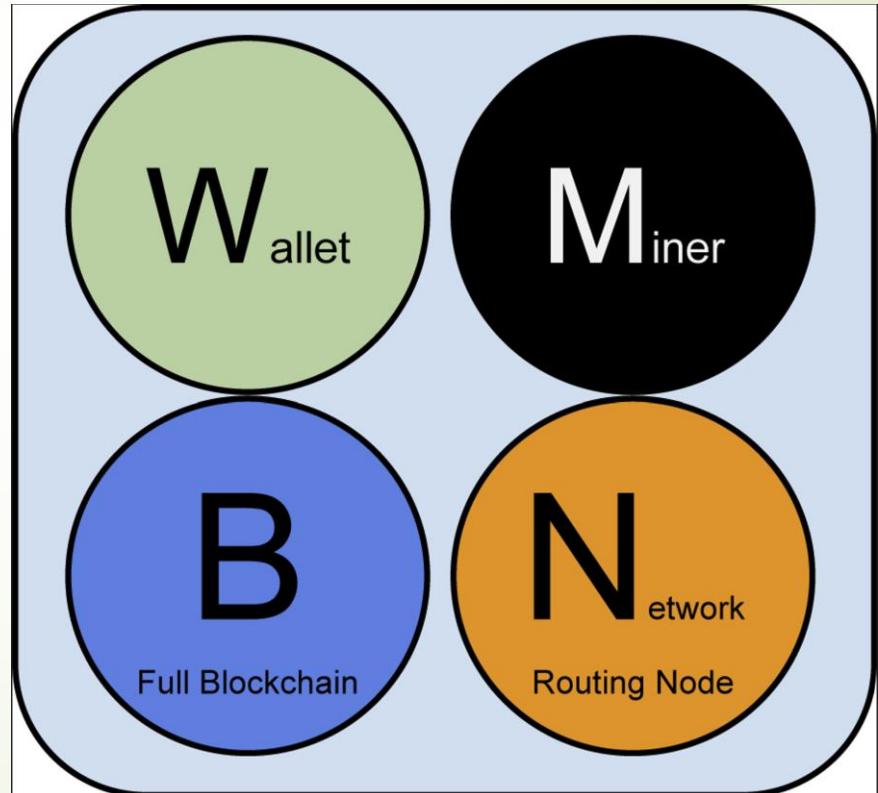
Le réseau Bitcoin

- ▶ Le réseau bitcoin est constitué de milliers de nœuds, qui sont tous des pairs, sans nœuds « spéciaux ».
- ▶ Le réseau est décentralisé, donc sans nœud central.

Le réseau Bitcoin

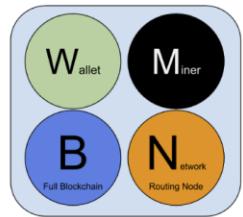
► On peut distinguer quatre fonctions assurées par les nœuds du réseau:

- Le routage
- Les fonctions de portefeuille
- Le minage
- Le registre



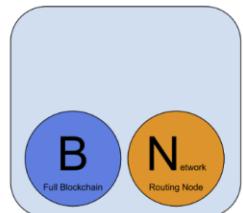
Le réseau Bitcoin

► Les différents types de nœuds:



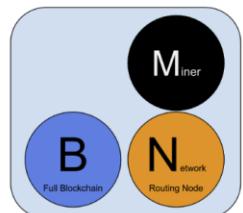
Reference Client (Bitcoin Core)

Contains a Wallet, Miner, full Blockchain database, and Network routing node on the bitcoin P2P network.



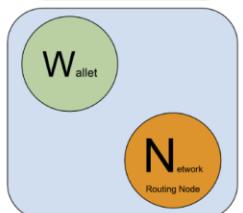
Full Block Chain Node

Contains a full Blockchain database, and Network routing node on the bitcoin P2P network.



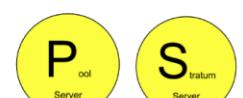
Solo Miner

Contains a mining function with a full copy of the blockchain and a bitcoin P2P network routing node.



Lightweight (SPV) wallet

Contains a Wallet and a Network node on the bitcoin P2P protocol, without a blockchain.



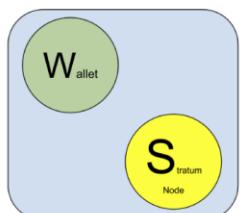
Pool Protocol Servers

Gateway routers connecting the bitcoin P2P network to nodes running other protocols such as pool mining nodes or Stratum nodes.



Mining Nodes

Contain a mining function, without a blockchain, with the Stratum protocol node (S) or other pool (P) mining protocol node.

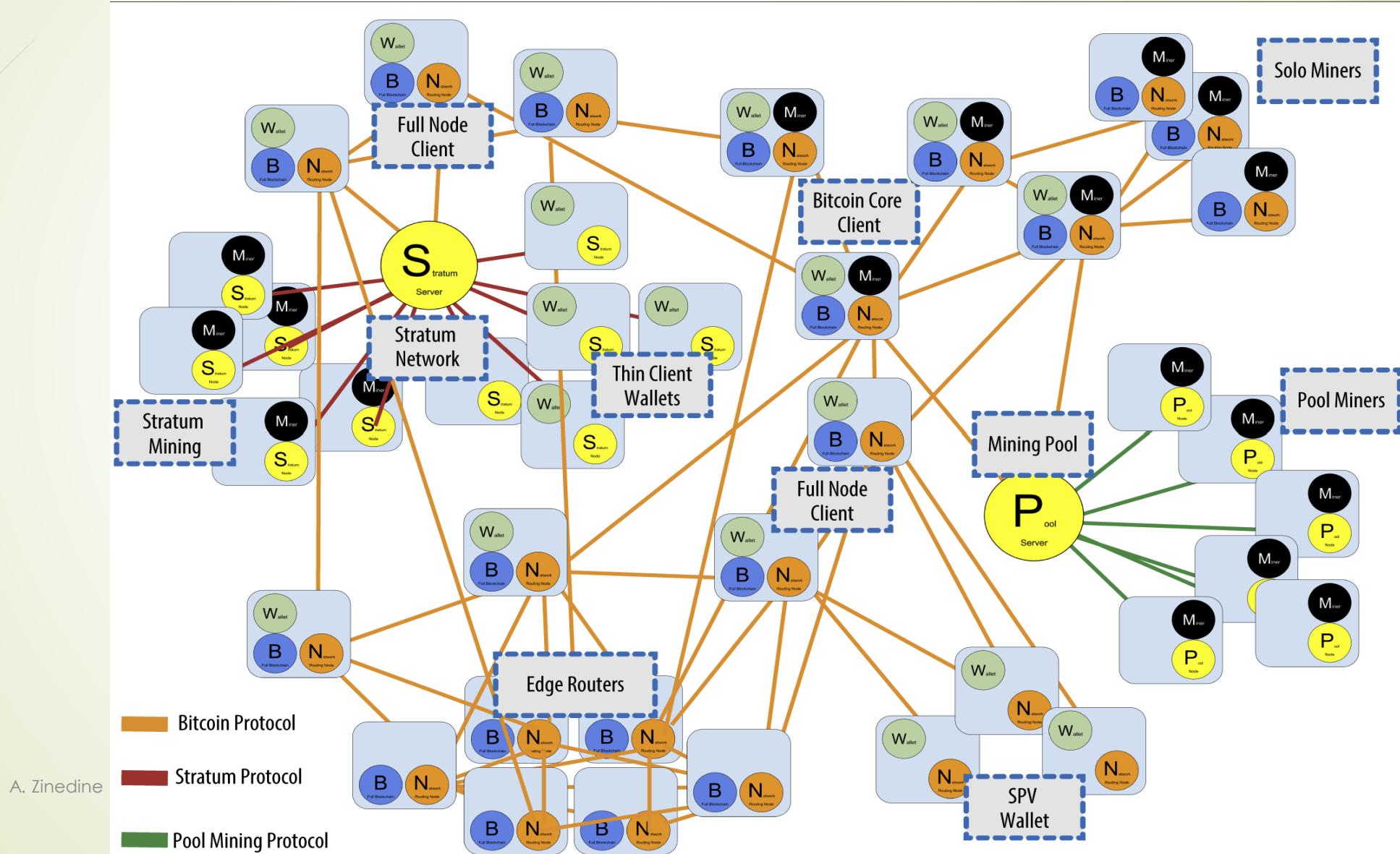


Lightweight (SPV) Stratum wallet

Contains a Wallet and a Network node on the Stratum protocol, without a blockchain.



Le réseau Bitcoin étendu



Comment joindre le réseau

- ▶ Le réseau Bitcoin est public :
 - ▶ tout le monde peut joindre et quitter le réseau à volonté
 - ▶ Aucune autorisation ou inscription ni requise
 - ▶ Il suffit seulement d'installer le logiciel adéquat selon le rôle désirée
- ▶ Le logiciel de référence : Bitcoin Core.



Comment joindre le réseau

- ▶ Le réseau Bitcoin est public :
 - ▶ tout le monde peut joindre et quitter le réseau à volonté
 - ▶ Aucune autorisation ou inscription ni requise
 - ▶ Il suffit seulement d'installer le logiciel adéquat selon le rôle désiré (lightweight, full node, ou miner)
- ▶ Le logiciel de référence: **Bitcoin Core** (www.bitcoin.org)
 - ▶ Contient toutes les composante
 - ▶ Il y a d'autres alternatives (l'essentiel c'est d'implémenter correctement le protocole)



Transactions

- ▶ Les transactions sont les structures de bases de bitcoin
- ▶ La fonction principale du réseau c'est de créer, propager, valider, confirmer et stocker les transactions.
- ▶ Pour créer des transactions, il suffit d'installer un portefeuille (Wallet).
- ▶ Premier Exemple d'une Transaction :
 - ▶ Voir Chapitre 1 du livre de **Mastering Bitcoin**



Transactions

- ▶ Premier Exemple d'une Transaction :
 - ▶ Voir Chapitre 1 du livre de **Mastering Bitcoin**

- ▶ Installer Wallet
 - (mnemonic phrase, Clé Privé, Clé Public, Adresse).
- ▶ Acheter bitcoin
- ▶ Acheter une tasse de café avec bitcoin
- ▶ Consulter la transaction sur **BlockChain Explorer**



45

Transactions

Alice's Wallet:

The image shows a mobile application interface for a Bitcoin wallet. On the left, the screen displays "Alice" with "0 BTC" and a large blue button labeled "Buy Bitcoin". Below this is a section titled "Transactions" with the placeholder text "Your transactions will appear here." At the bottom are buttons for "Receive" and "Send". A large black arrow points from this screen to the right. On the right, a "Receive" screen is shown with a QR code, the address "1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK", and buttons for "Receive with amount" and "Share".

Alice

0 BTC

Transactions

Your transactions will appear here.

Buy Bitcoin

Receive

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK

Receive with amount

Share

Send

Receive



Transactions

Joe sends 0,10 BTC to Alice's address:

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK

X Send ...

0.10 BTC
\$10.00

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7... Scan

Alice

Fee 0 sat/byte

Next

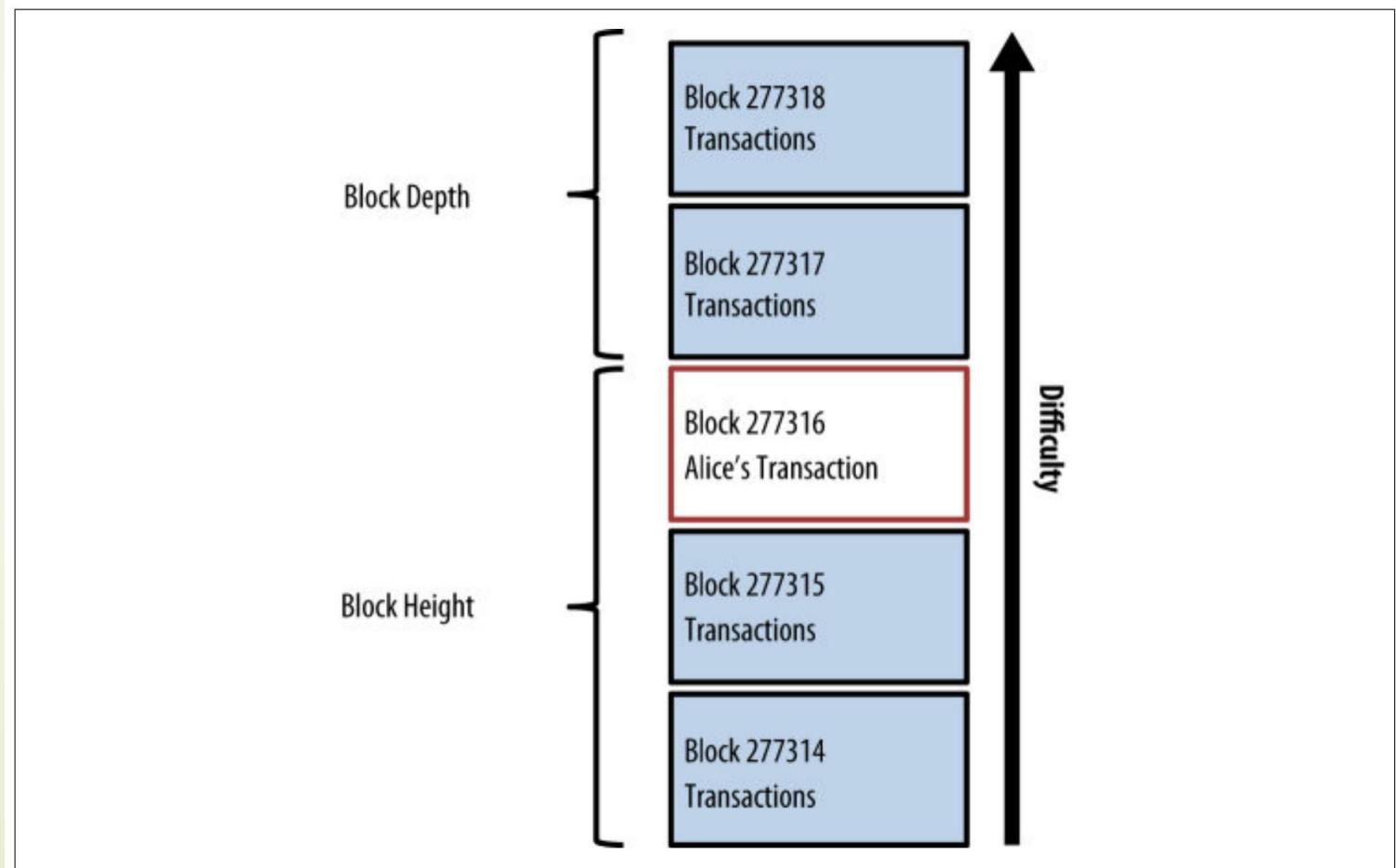


Transactions

- ▶ Diffusion de la transaction par Joe
- ▶ Validation et Propagation de la transaction par tous les nœuds
- ▶ Ajout de la transaction à un bloc par un mineur, et validation de ce Bloc.
- ▶ Tout bloc supplémentaire ajoute une **confirmation** de plus à la transaction en la rendant plus sûre.

Transactions

- ▶ Tout bloc supplémentaire ajoute une confirmation de plus à la transaction en la rendant plus sûre.





Transactions

- ▶ Structure d'une transaction
 - ▶ Inputs
 - ▶ Outputs
 - ▶ Frais
- ▶ La notion de Unspent Transaction Outputs (**UTXO**)
- ▶ L'enchainement des transactions
- ▶ Exemple d'illustration:
 - ▶ Alice achète une tasse de café de chez Bob avec bitcoin
(Voir l'exemple sur le Chapitre 2 du livre **Mastering Bitcoin**)

Transactions

Transaction as Double-Entry Bookkeeping

Inputs	Value	Outputs	Value
Input 1	0.10 BTC	Output 1	0.10 BTC
Input 2	0.20 BTC	Output 2	0.20 BTC
Input 3	0.10 BTC	Output 3	0.20 BTC
Input 4	0.15 BTC		

Total Inputs:

0.55 BTC

Total Outputs:

0.50 BTC

$$\begin{array}{rcl} \text{Inputs} & 0.55 \text{ BTC} \\ \text{Outputs} & 0.50 \text{ BTC} \\ \hline \text{Difference} & 0.05 \text{ BTC} \text{ (implied transaction fee)} \end{array}$$

Transactions

Transaction 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18

INPUTS From
 From (previous transactions Joe has received):
 Joe 0.1000 BTC

OUTPUTS To
 Output #0 Alice's Address 0.1000 BTC (spent)
 Transaction Fees: 0.0000 BTC

Transaction 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fb8a57286c345c2f2

INPUTS From
 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18 : 0
 Alice 0.1000 BTC

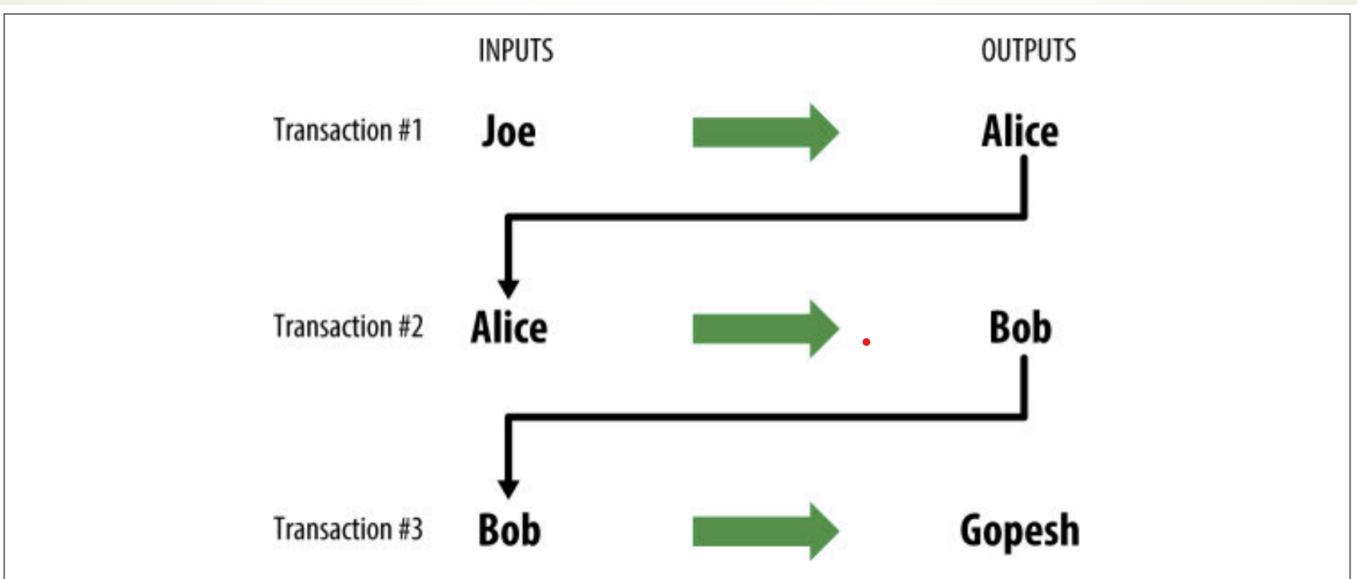
OUTPUTS To
 Output #0 Bob's Address 0.0150 BTC (spent)
 Output #1 Alice's Address (change) 0.0845 BTC (unspent)
 Transaction Fees: 0.0005 BTC

Transaction 2bbac8bb3a57a2363407ac8c16a67015ed2e88a4388af58cf90299e0744d3de4

INPUTS From
 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fb8a57286c345c2f2 : 0
 Bob 0.0150 BTC

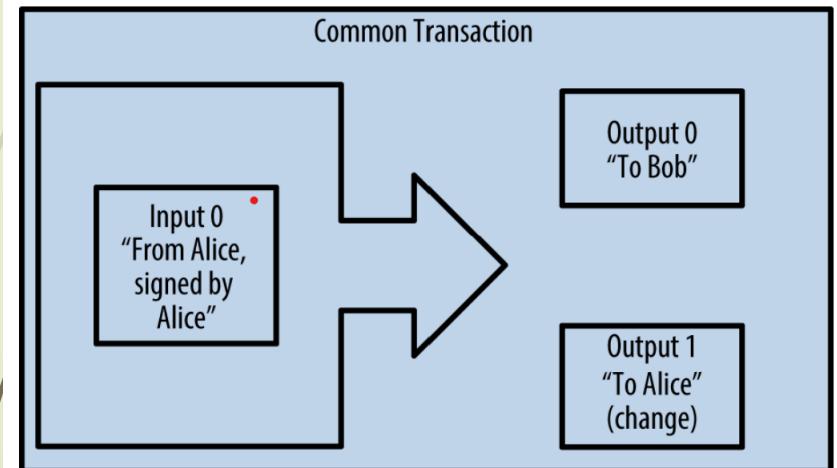
OUTPUTS To
 Output #0 Gopesh's Address 0.0100 BTC (unspent)
 Output #1 Bob's Address (change) 0.0045 BTC (unspent)
 Transaction Fees: 0.0005 BTC

Transactions

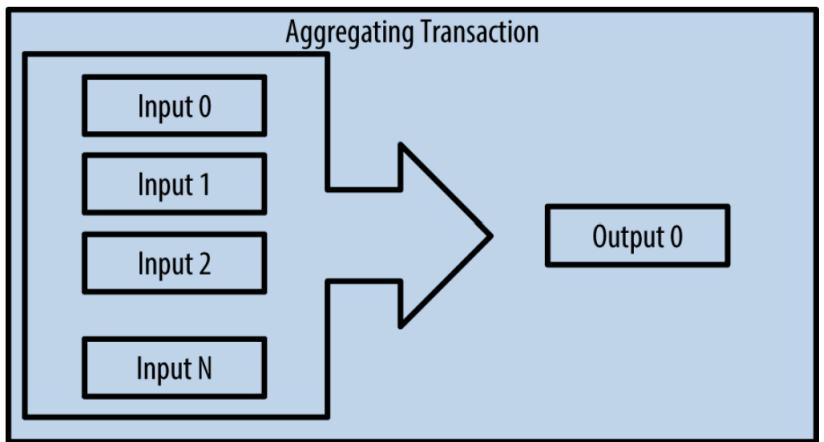


Formes communes d'une transaction

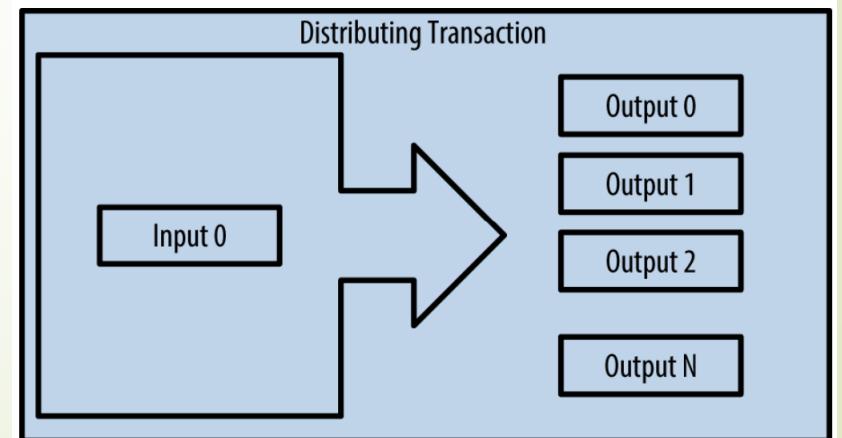
1:



2:



3:





Transactions

- ▶ Consulter la transaction de Alice à Bob sur un Blockchain Explorer:

<https://www.blockchain.com/btc/tx/0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fb8a57286c345c2f2>

Transaction View information about a bitcoin transaction

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fb8a57286c345c2f2

Inputs	Outputs
1CdId9KFAaatwczBwBttQcwXYCpvK8h7FK (0.1 BTC - Unspent)	 1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA (Unspent) 0.015 BTC 1CdId9KFAaatwczBwBttQcwXYCpvK8h7FK (Unspent) 0.0845 BTC

97 Confirmations **0.0995 BTC**

Summary		Inputs and Outputs	
Size	258 (bytes)	Total Input	0.1 BTC
Received Time	2013-12-27 23:03:05	Total Output	0.0995 BTC
Included In Blocks	277316 (2013-12-27 23:11:54 +9 minutes)	Fees	0.0005 BTC
		Estimated BTC Transacted	0.015 BTC

Transactions

► Alice's raw transaction

```
{  
  "version": 1,  
  "locktime": 0,  
  "vin": [  
    {  
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",  
      "vout": 0,  
      "scriptSig" : "3045022100884d142d86652a3f47ba4746ec719bbfb040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac96f  
      "sequence": 4294967295  
    }  
  ],  
  "vout": [  
    {  
      "value": 0.01500000,  
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"  
    },  
    {  
      "value": 0.08450000,  
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeea53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",  
    }  
  ]  
}
```

Transactions

- ▶ Alice's transaction serialized and presented in hexadecimal notation

```
0100000001186f9f998a5aa6f048e51dd8419a14d8a0f1a8a2836dd73  
4d2804fe65fa35779000000008b483045022100884d142d86652a3f47  
ba4746ec719bbfb0d040a570b1deccbb6498c75c4ae24cb02204b9f039  
ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e3813  
01410484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade84  
16ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc1  
7b4a10fa336a8d752adfffffff0260e31600000000001976a914ab6  
8025513c3dbd2f7b92a94e0581f5d50f654e788acd0ef800000000000  
1976a9147f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a888ac 00000000
```