Cours Blockchain

Module 2

Module 2 : Constitution d'un blockchain

1

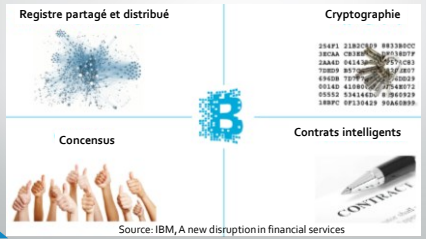
2

BLOCKCHAIN – Rappel

- La blockchain est une technologie de stockage et de transmission d'informations.
- C'est une technologie transparente, sécurisée, et fonctionnant sans organe central de contrôle.
- Dans la réalité, une blockchain constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création.
- Cette base de données est sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne

3

Les 4 Concepts fondamentaux

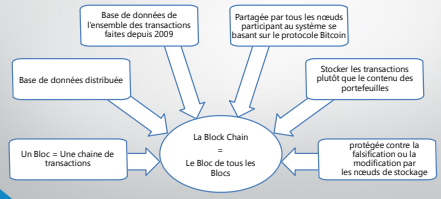


Source: IBM, A new disruption in financial services

4

BLOCKCHAIN : (CHAINE DE BLOCS)

- C'est quoi la Blockchain ?



5

5

BLOCKCHAIN : TRANSACTION

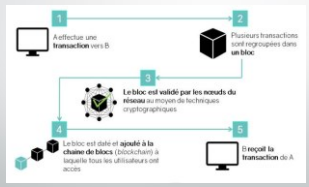
- C'est quoi une transaction?
  - Il s'agit du transfert de valeurs (actifs) entre portefeuilles
  - Incluse dans la Blockchain
  - Signée par la clé privée de l'émetteur
  - Les transactions sont diffusées dans le réseau, confirmées par un procédé appelé le minage

6

6

BLOCKCHAIN : TRANSACTION

- Cycle de vie d'une transaction

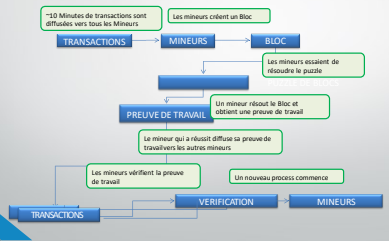


7

7

BLOCKCHAIN : (CHAINE DE BLOCS)

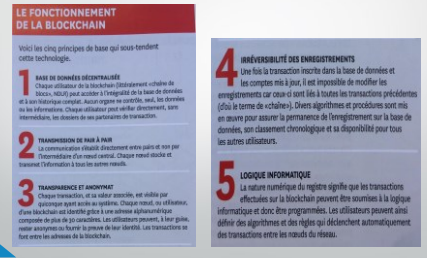
- Comment la Blockchain fonctionne



8

8

Résumé :
les 5 principes de base de la Blockchain



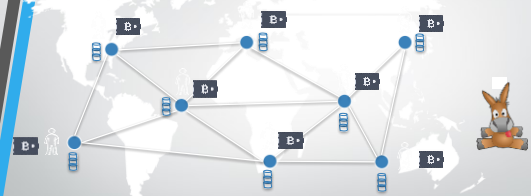
9

1. Le réseau
2. Le hashage
3. La base de données
4. Le nœud mineur
5. La transaction
6. Le Fork
7. La sécurité dans la blockchain
8. Inctenvites ?

10

11

Réseau Peer to peer



Chaque nœud du réseau contient une copie de la base de données Chaque utilisateur réalise des transactions via un nœud du réseau
Il effectue ses transactions à l'aide d'un portefeuille électronique

12

Le Réseau

- Les étapes mises en œuvre pour faire fonctionner le réseau sont les suivantes :
- Les nouvelles transactions sont diffusées à tous les nœuds.
- Chaque nœud regroupe les nouvelles transactions dans un bloc.
- Chaque nœud travaille à la résolution de la preuve de travail sur son bloc.
- Quand un nœud trouve une preuve de travail, il diffuse ce bloc à tous les nœuds.
- Les nœuds n'acceptent le bloc que si toutes les transactions qu'il contient sont valides et n'ont pas déjà été dépensées.
- Les nœuds expriment l'acceptation du bloc en travaillant sur un nouveau bloc dans la chaîne, ce nouveau bloc ayant comme empreinte précédente celle du bloc accepté.

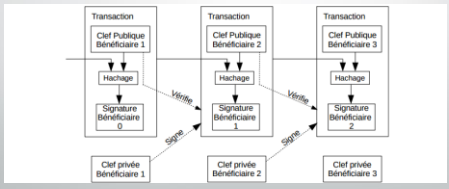
13

14

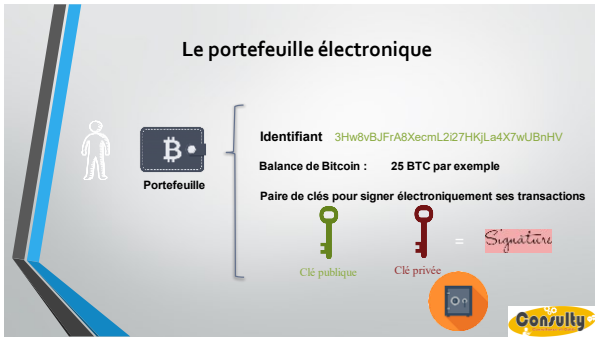
BLOCKCHAIN : TRANSACTION

15

Transaction



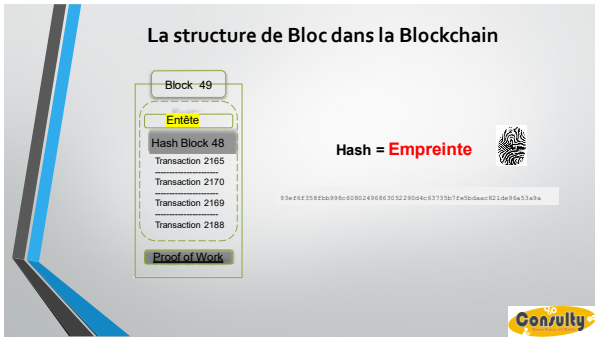
16


Le portefeuille électronique
Portefeuille
Identifiant 3Hw8vBJFrA8XecmL2i27HKjLa4X7wUBnHV
Balance de Bitcoin : 25 BTC par exemple
Paire de clés pour signer électroniquement ses transactions
Clé publique
Clé privée
Signature
Consulty

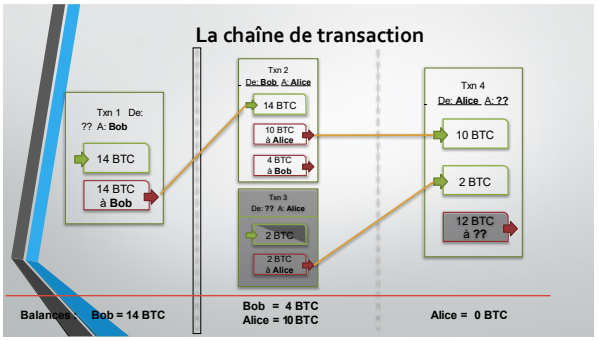
17


Principe de la signature éléctronique
Crypté avec la clé privée
Clé privée
François H.
Clé publique
Julie G.
Seule la clé publique peut décrypter le message crypté avec la clé privée
Cela permet d'identifier avec certitude l'auteur du message
Consulty

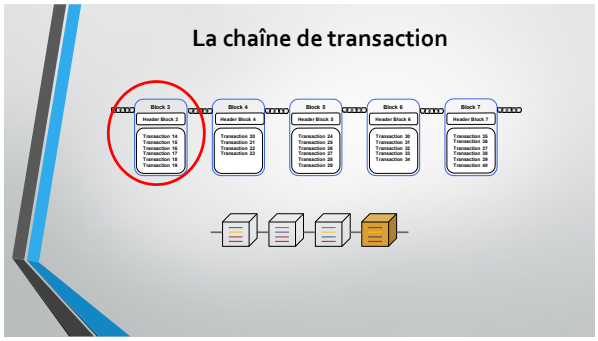
18


La structure de Bloc dans la Blockchain
Block 49
Entête
Hash Block 48
Transaction 2165
Transaction 2170
Transaction 2169
Transaction 2188
Proof of Work
Hash = Empreinte
Consulty

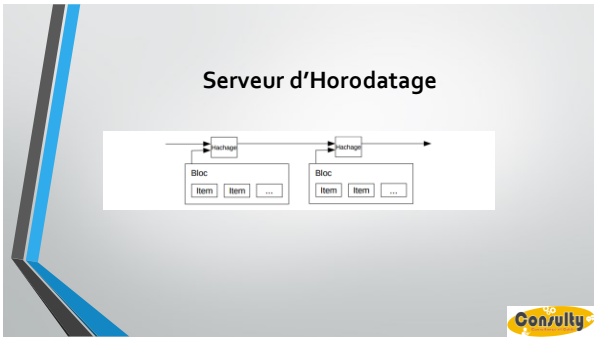
19


La chaîne de transaction
Txn 1 De: ?? A: Bob
14 BTC
14 BTC à Bob
Txn 2 De: Bob A: Alice
14 BTC
10 BTC à Alice
4 BTC à Bob
Txn 3 De: ?? A: Alice
2 BTC
2 BTC à Alice
Txn 4 De: Alice A: ??
10 BTC
2 BTC
12 BTC à ??
Balances
Bob = 14 BTC
Bob = 4 BTC
Alice = 10 BTC
Alice = 0 BTC

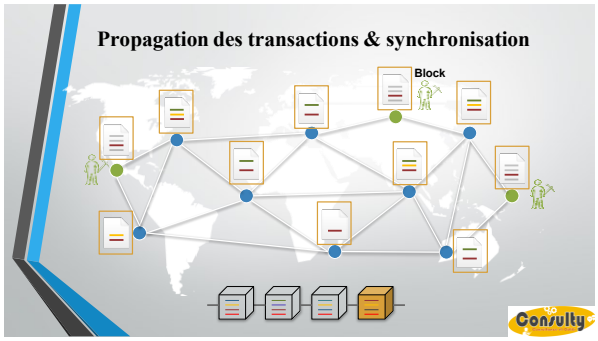
20


La chaîne de transaction

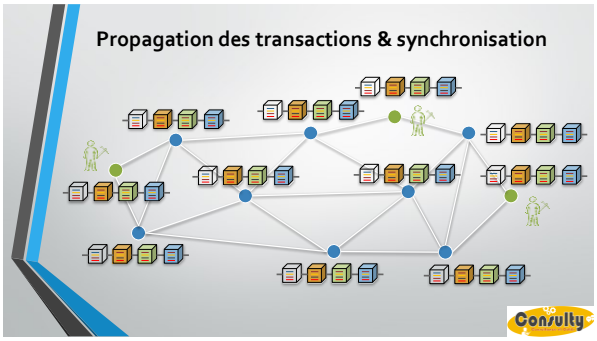
21


Serveur d'Horodatage
Hachage
Hachage
Bloc
Item
Item
...
Bloc
Item
Item
...
Consulty

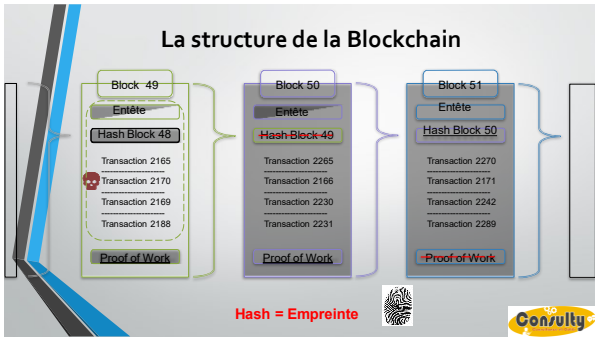
22


Propagation des transactions & synchronisation
Block
Consulty

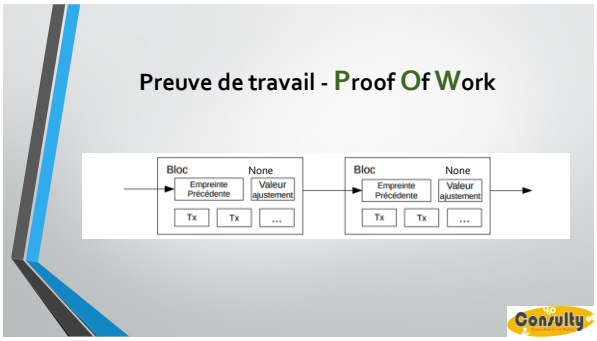
23


Propagation des transactions & synchronisation
Consulty

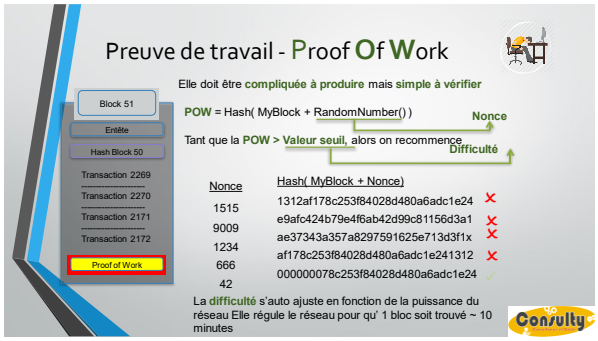
24


La structure de la Blockchain
Block 49
Entête
Hash Block 48
Transaction 2165
Transaction 2170
Transaction 2169
Transaction 2188
Proof of Work
Block 50
Entête
Hash Block 49
Transaction 2265
Transaction 2166
Transaction 2230
Transaction 2231
Proof of Work
Block 51
Entête
Hash Block 50
Transaction 2270
Transaction 2171
Transaction 2242
Transaction 2289
Proof of Work
Hash = Empreinte
Consulty

25


Preuve de travail - Proof Of Work
Bloc
Empreinte Précédente
None
Valeur ajustement
Tx
Tx
...
Bloc
Empreinte Précédente
None
Valeur ajustement
Tx
Tx
...
Consulty

26


Preuve de travail - Proof Of Work
Block 51
Entête
Hash Block 50
Transaction 2269
Transaction 2270
Transaction 2171
Transaction 2172
Proof of Work
Elle doit être compliquée à produire mais simple à vérifier
POW = Hash(MyBlock + RandomNumber())
Nonce
Tant que la POW > Valeur seuil, alors on recommence
Difficulté
Nonce
Hash(MyBlock + Nonce)
1515
1312af178c253f84028d480a6adc1e24
9009
e9afc424b79e4f6ab42d99c81156d3a1
1234
ae37343a357a8297591625e713d3f1x
666
af178c253f84028d480a6adc1e241312
42
000000078c253f84028d480a6adc1e24
La difficulté s'auto ajuste en fonction de la puissance du réseau Elle régule le réseau pour qu' 1 bloc soit trouvé ~ 10 minutes
Consulty

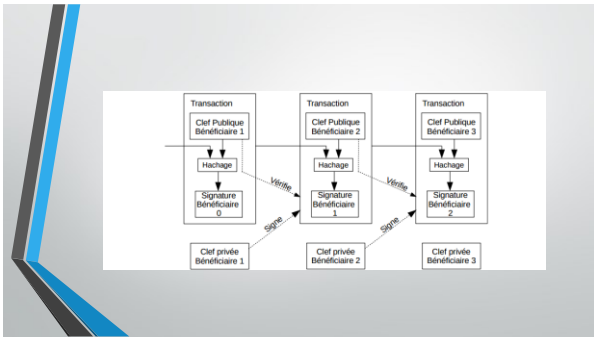
27


3 – LA HASHAGE

28


SHA-256
SHA256 (Secure Hash Algorithm)
un algorithme représentant une famille de fonctions de hachage (National Security Agency des États-Unis)
la suite logique d'autres algorithmes.
signature pour les fichiers de données
Pour plus d'informations : https://cryptostrategie.com/sha256-algorithme-bitcoin/
Consulty

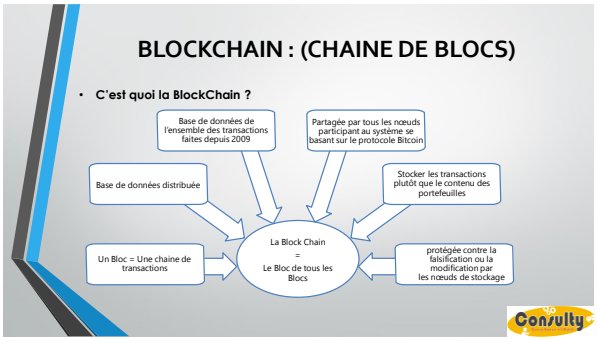
29


Transaction
Clef Publique Bénéficiaire 1
Hachage
Signature Bénéficiaire 0
Clef privée Bénéficiaire 1
Vérifie
Signe
Transaction
Clef Publique Bénéficiaire 2
Hachage
Signature Bénéficiaire 1
Clef privée Bénéficiaire 2
Vérifie
Signe
Transaction
Clef Publique Bénéficiaire 3
Hachage
Signature Bénéficiaire 2
Clef privée Bénéficiaire 3

30


4 - LA BASE DE DONNEES
(Ledger)

31


BLOCKCHAIN : (CHAINE DE BLOCS)
C'est quoi la BlockChain ?
Base de données de l'ensemble des transactions faites depuis 2009
Partagée par tous les noeuds participant au système se basant sur le protocole Bitcoin
Base de données distribuée
Stocker les transactions plutôt que le contenu des portefeuilles
Un Bloc = Une chaine de transactions
La Block Chain = Le Bloc de tous les Blocs
protégée contre la falsification ou la modification par les nœuds de stockage
Consulty

32

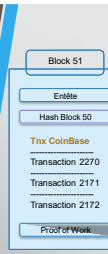
La Base de Données

Propriétés	Blockchain	Base de données traditionnelle
Opérations	Seulement des opérations d'insertion	Peut effectuer des opérations CRUD
Réplication	Réplication complète du bloc sur chaque pair	Maître esclave multi-maître
Consensus	La majorité des pairs s'accordent sur le résultat des transactions	Transactions distribuées (validation en 2 phases)
Invariants	Tout le monde peut valider les transactions sur le réseau	Contraintes d'intégrité

33

34

Le Minage



Le minage c'est le procédé par lequel les transactions Bitcoin sont propagées et sécurisées

Miner consiste à résoudre un problème mathématique en vue de produire une preuve de travail (Proof of Work).

Dès que la POW est produite, un nouveau Bloc est créé et le mineur est récompensé

C'est également par ce procédé que la monnaie se créée

La fièvre du bitcoin

35

BLOCKCHAIN : MINAGE

- **C'est quoi le minage?**
  - Vérifier la chaine de blocs
  - Mettre à disposition des ressources techniques au réseau « Bitcoin » et vérifier les transactions entre utilisateurs qui ont lieu partout dans le monde
  - Un logiciel installé sur les serveurs des Mineurs, permet de résoudre des problèmes mathématiques
  - Plus il y a de mineurs => Plus il y a de sécurité
- – https://bitcoin.fr/minage/

36

BLOCKCHAIN : MINAGE

- Que calculent les mineurs ?
  - effectuent des hashs cryptographiques (deux *SHA256* successifs) sur ce qu'on appelle un *entête de bloc*
  - Pour chaque nouveau hash, le logiciel de minage utilise un nombre aléatoire différent qu'on appelle le *nonce*

37

38

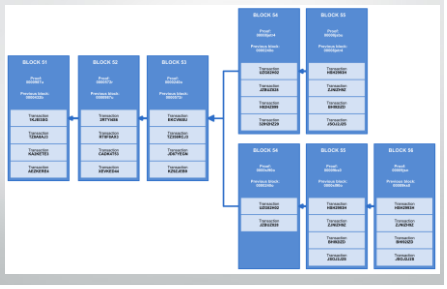
Terminologie Blockchain

- **Les forks, ou *bifurcations***
  - La creation d'une version alternative de la blockchain, en créant deux blocs simultanément à deux endroits différents du réseau. Cela crée deux blockchains parallèles, parmi lesquelles une sera gagnante sur l'autre
  - Quand-est ce que cela se produit t'il ?
    - Si deux blocs sont trouvés au même moment par deux mineurs différents
    - En cas d'incompatibilités entre les logiciels des noeuds des mineurs
    - En cas de désaccord sur les règles du protocole entre plusieurs noeuds

39

Terminologie Blockchain

- **Forks**



40

41

CLÉS PUBLIQUE / CLÉS PRIVÉE

- L'utilisation d'une paire **clés publique/clés privée** est un des principe sur lequel repose la **cryptographie asymétrique** (une méthode de chiffrement).
- Principes :
  1. Chaque utilisateur dispose d'une **clés publique** qu'il **diffuse** et d'une **clé privée** qu'il **garde**
  2. Un utilisateur A souhaite envoyer un message m à un utilisateur B
  3. L'utilisateur A chiffre le message m avec la clés publique de l'utilisateur B
  4. L'utilisateur B reçoit le message m chiffré avec sa clés publique B.
  5. L'utilisateur B est le seul à pouvoir déchiffrer le message m chiffré avec sa clé privée B

42

MÉCANISMES DE CONSENSUS

Les mécanismes de consensus sont utilisés pour s'assurer que tout les nœuds du réseau (paires) disposent des mêmes informations et que seules les transactions valides sont enregistrées dans les registres distribués. En d'autres termes, il s'agit de la manière de valider les blocs de la Blockchain

- **Proof of Work** (Preuve de travail ou PoW) constitue le processus de résoudre un défi informatique imposé par une Proof of Work est appelé **mining** (on parle de **mineurs**). Les mineurs doivent résoudre un problème informatique ayant une difficulté d (d est variable et évolue en fonction de la puissance de calcul du système) pour valider un block. La Proof of Work est utilisé par la Blockchain de Bitcoin
- **Proof of Stake** (Preuve d'enjeu ou de possession ou PoS) constitue le processus de résoudre un défi informatique imposé par une Proof of Stake est appelé **minting** (on parle de **forgeurs**). La Proof of Stake se base sur la probabilité qu'un nœud parvienne le prochain block de transactions à ajouter à la Blockchain est proportionnelle à la quantité de monnaie que possède ce nœud. Les forgeurs doivent résoudre un problème informatique pour valider un block.
- Il existe d'autres mécanismes de consensus comme le **Practical Byzantine Fault Tolerance** (**PBFT**) basé sur le problème des généraux byzantins (métaphore informatique) et le **Zero Knowledge Proof** (*un fournisseur de preuve* prouve mathématiquement à un *vérificateur* qu'une proposition est vraie sans toutefois révéler d'autres informations que la véracité de la proposition)

43

LE CONCEPT DE TOKENISATION

- Les *ledgers* (registres) de la plupart des blockchains reposent sur des assets digitaux appelés Tokens (jetons)
  - Dans la blockchain **Ripple**, les tokens sont nommés **XRP**
  - Dans la blockchain d'**Ethereum**, les tokens sont nommés **Ethers**
- Les Tokens servent deux objectifs principaux
  - Rémunérer les nœuds du réseaux lors du processus de minage et donc encourager la définition d'un consensus
  - Prévenir des SPAM et attaques de types *Deni de Services*

44

45

En récompense, le mineur reçoit un certains nombre de bitcoins (divisé par 2, tous les 4 ans environ - Le 12 mai 2020 cette récompense est passée à 6,25 bitcoins par bloc.-)

46