LIBRA

Blockchain ou pas ?

Références:
https://libra.org/fr-FR/white-paper/
https://developers.libra.org/docs/assets/papers/the-libra-blockchain.pdf
https://developers.libra.org/docs/assets/papers/libra-consensus-state-machine-replication-in-the-libra-blockchain.pdf

Objectifs de Facebook?

Beaucoup de bons sentiments:

- Nous sommes convaincus que davantage de personnes devraient avoir accès à des services financiers et à des capitaux bon marché.
- Nous sommes convaincus que chacun dispose du droit inhérent de contrôler le fruit de son travail légal.
- Nous sommes convaincus qu'une circulation monétaire mondiale, libre et instantanée créera d'immenses opportunités économiques et commerciales dans le monde entier.
- Nous sommes convaincus que la confiance du public pour des formes de gouvernance décentralisées va graduellement se renforcer.
- Nous sommes convaincus qu'une devise mondiale et une infrastructure financière doivent être conçues et régies comme un bien public.
- Nous sommes convaincus que le développement de l'inclusion financière, le soutien des intervenants éthiques et la défense continue de l'intégrité de l'écosystème relèvent de notre responsabilité commune

Ce qui se dit:

- Facebook veut promouvoir le B2C avec création de PME mondialisées: elles auront des besoins :
  - Publicité → revenus pour Facebook
  - Moyens de paiement → LIBRA

Plus concrètement:

- développement d'une devise et d'une infrastructure financière mondiale simple, au service de milliards de personnes
- réserve d'actifs conçue pour lui offrir une valeur intrinsèque : « **stable coin** »
- L'association Libra est une organisation indépendante à but non lucratif basée à Genève
- Ambitions
  - traiter un flux important de transactions: 1000T/s (VISA: 2000; 20 pour bitcoin)
  - Aussi bien sur le NET qu'en face à face
  - Mention du µpaiement, et du ticketing

Partenariat?

- **Paiements :** Mastercard, Mercado Pago, PayPal, PayU (branche fintech de Nasper), Stripe, Visa
- **Technologies et marketplaces** : Booking Holdings, eBay, Facebook/Calibra, Farfetch, Lyft, Spotify AB, Uber Technologies, Inc.
- **Télécommunications** : Iliad, Vodafone Group
- **Blockchain** : Anchorage, Bison Trails, Coinbase Inc., Xapo Holdings Limited
- **Capital-risque** : Andreessen Horowitz, Breakthrough Initiatives, Ribbit Capital, Thrive Capital, Union Square Ventures
- **Organisations à but non lucratif, organisations multilatérales et institutions universitaires** : Creative Destruction Lab, Kiva, Mercy Corps, Women's World Banking

Une centaine de membres d'ici son lancement prévu pour le premier semestre 2020.

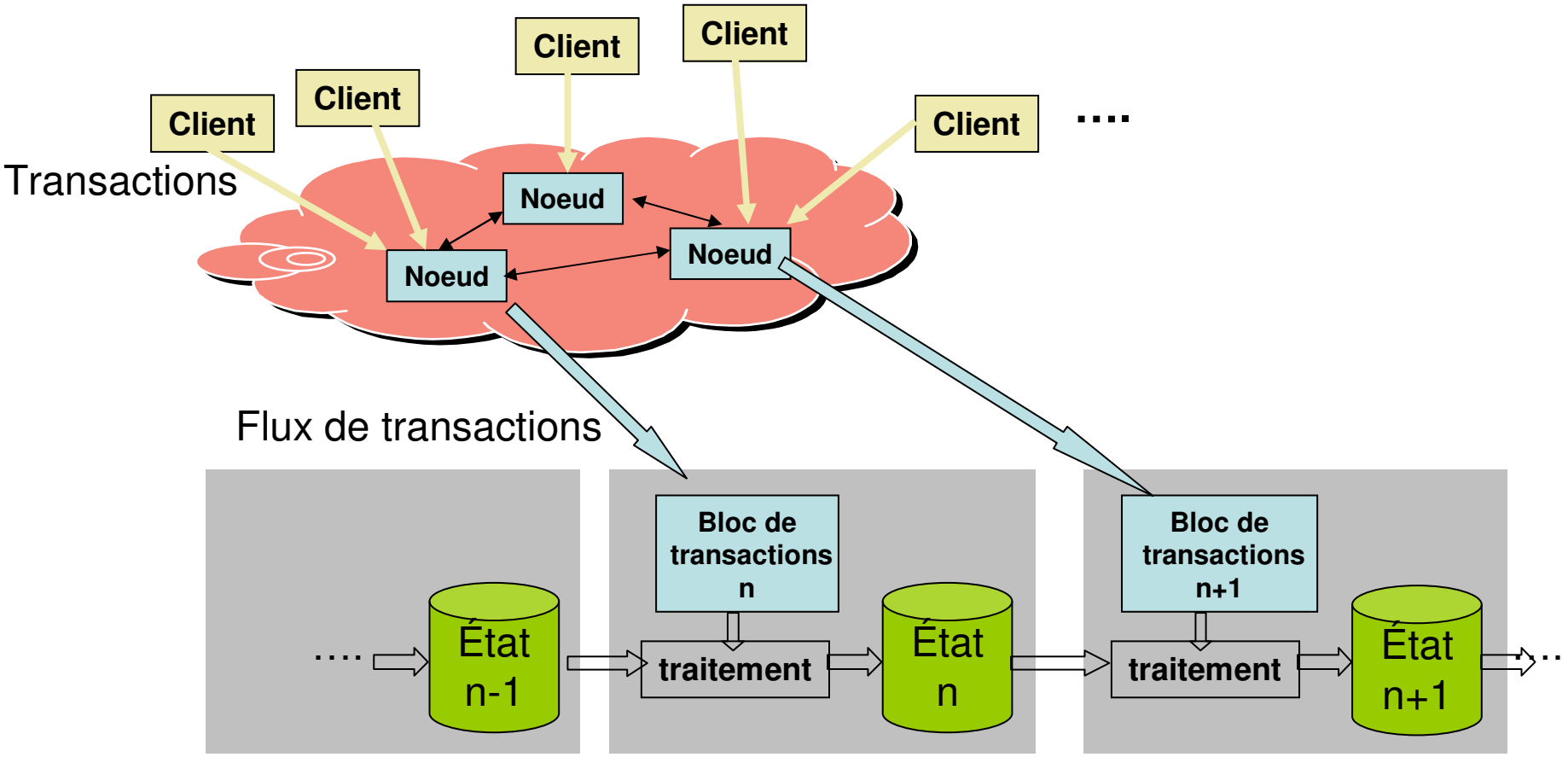
Facebook ne sera qu'un membre parmi d'autres et son rôle dans la gouvernance de l'association sera égal à celui de ses homologues.

Beaucoup de défections!!!

LIBRA: club fermé ou système ouvert?

- Traitements partagés entre les partenaires et leurs noeuds
  - Au départ: agrément par les partenaires
  - Futur à 5 ans: “permissionless”
    - Comme par ex Bitcoin
      - Mais Bitcoin est-il vraiment ouvert?
      - Miner utilement nécessite des investissements énormes
    - Donc version plus complexe des protocoles Libra
      - Mais sans doute moins consommatrice de puissance que Bitcoin: voir la suite

Cryptomonnaies: modèle général



+ tolérance aux fautes , intentionnelles ou pas : consensus

Mots clés LIBRA

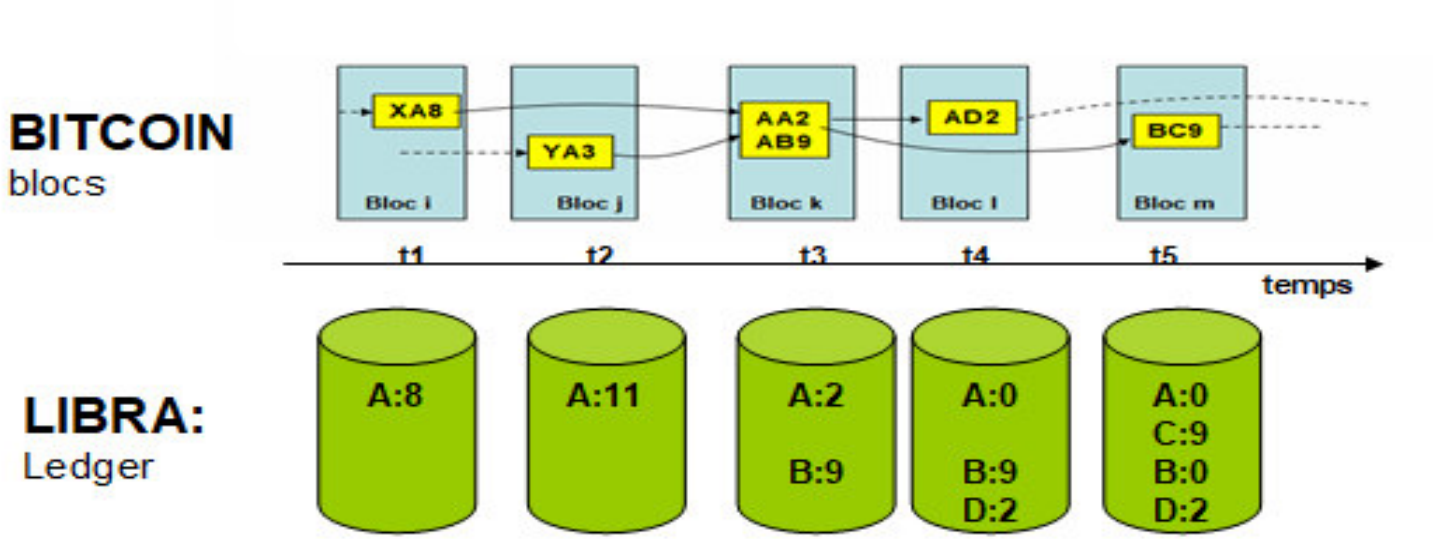
- **Client :** **1 milliard**
  effectue des transactions Libra avec d'autres clients (payeur ou payé).
  - Un ou plusieurs Comptes:
    - Chacum a sa bi-clé
    - Son Id= hash de la clé pub.
  - Donc anonymat de type pseudonyme(s)

- **Nœuds** :N serveurs, appelés nœuds, **100**
  - chargés du traitement des transactions.
  - Chaque nœud a une bi clé; chaque nœud connait la clé publique des autres nœuds
- **Leader** **1 par round**
  - Un seul nœud est leader /round: processus de choix aléatoire et consensuel
- **Valideur:** N-1 nœuds **99**
  - valide un nouvel état du grand livre (ledger)
- **Round** **10''**
  - Période de traitement des transactions, entre deux validations
- **Epoque:** plusieurs années
  - Période durant laquelle il n'y a pas de changement chez les nœuds

Mots clés LIBRA

- **Etat**
  - **Libra est orienté « état » contrairement à Bitcoin orienté « Bloc », Etherum orienté bloc+état**
- **Transaction** : « smart contract » avec un langage « MOVE »
  - Très typé:
    - Ex: Une donnée solde ne peut faire l'objet de copie et m à j que très contraintes
  - Un cas particulier : le paiement
    - Notation: (B,C,5) : B paye 5 à C, B et C étant les identifiants du compte utilisé par le payeur et le payé.
- **Blockchain:**
  - Pas de blocs de transactions avec chainage et POW
  - Approche totalement différente de Bitcoin!

Structure de données Libra



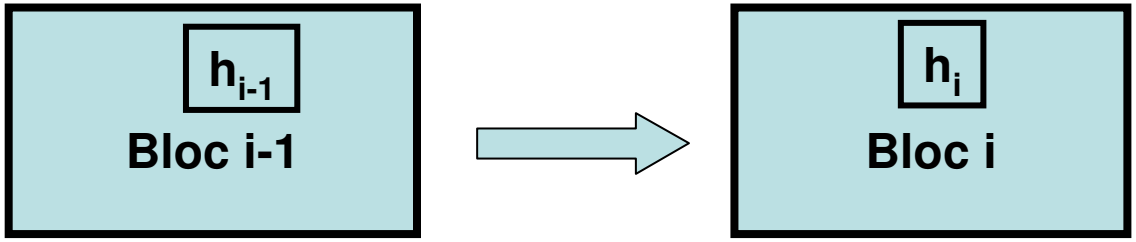
Avantage:

- **Rapidité/facilité du traitement des transactions**
  - **Réponse immédiate à YA3; dans bitcoin, il faut balayer TOUS les blocs précédents pour voir si Y a bien >3, (**ou truster son serveur)
- **Volume de données: état+historique restreint << historique complet**

Rappel Bitcoin 1

***POW**: Proof of work: trouver n (128 bits) tel que:*

hi= hash(hi-1 , bloc courant, n, …) a z bits PF à 0



z=70 actuellement
Difficulté: calcul de 2^{70}~10^{21}=mille milliards de milliards de hash

Consensus Bitcoin: principe:
un groupe malveillant qui a < ½ hash-power du réseau peut créer sa propre chaîne de blocs: fork → 2 chaînes concurrentes
Mais la plus longue chaîne sera celle du groupe honnête!
→ consensus sur la plus longue chaîne

Rappel Bitcoin 2

Création de Bitcoin: liée au POW

- **Le noeud gagnant insère dans le bloc une transaction de 12,5 BC;**
  (Confirmée 100 blocs plus loin)
- **Ce montant est divisé par 2 tous les 5 ans**
- **Total: 21 M BC**

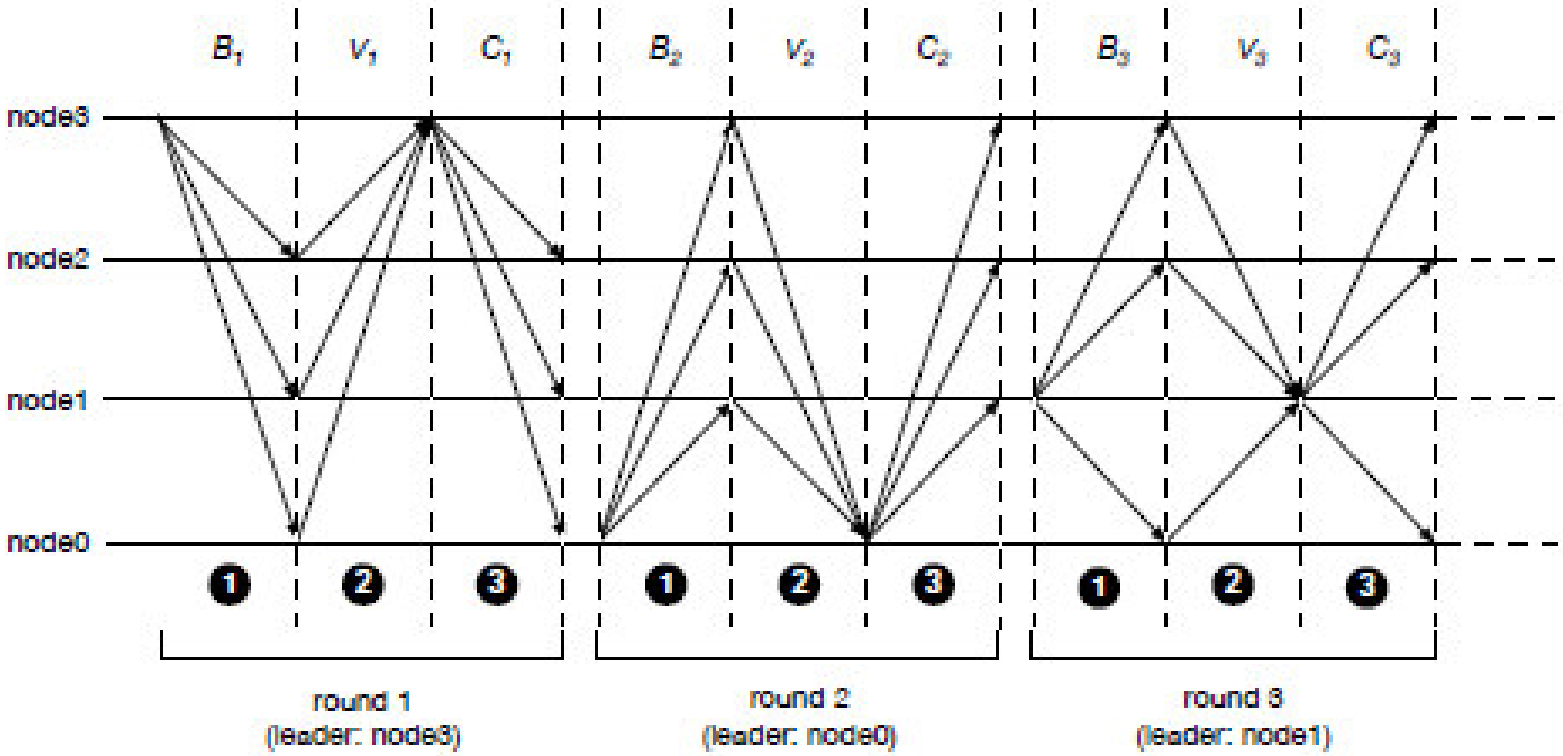
Bitcoin=15% de la consommation Française: aberrant!

Etherum

- Mélange des approches « bloc » et « état »: un nœud fait:
  - Choix Transactionsdu pool→bloc de transactions
  - Établit un état courant local
    - à partir de l'état consensus +bloc de transactions
    - Calcule Hash (merkle tree) du nouvel état
    - Ce hash est incorporé dans le POW
  - POW
  - Il gagne ou pas
- Si il gagne, son état courant devient l'état courant général
- Approche plus efficace que Bitcoin pour la vérification des transactions (double dépenses); mais conserve le POW, dispandieux en puissance de calcul

Principe du consensus Libra

B: block V: vote C: commit



- **Bi: le leader choisit les transactions à traiter du round I, puis les traite et publie hash du nouvel état**
- **Vi: les valideurs (dont le leader) vérifient les traitements du leader: nouvel état, et signent si concordance**
- **Ci: établissement du consensus: vote (vérif de toutes les signatures) et choix leader suivant**

Traitement des transactions

- Le client envoie cette transaction chez un ou plusieurs noeuds
- Cette transaction est répercutée en P2P aux autres noeuds
- Un pool de transactions se constitue

Leader

B

Exemple: Transaction (B,C,9) lors du round r
Ses données: (~bitcoin)

- Id B, P_B , Id C
- horodatage
- Sig_B (montant=9, round=r,IdB, IdC)

- choisit un bloc de n transactions à traiter dans ce pool
- envoie le bloc aux valideurs
- vérifie les transactions du bloc ;
  (sig, solde>montant+commission)
- met à jour état r → état r+1
- envoi le hash de état r+1 aux valideurs

Traitement des transactions

Valideurs

C

- Exécutent les transactions du bloc, mettent à jour etat r → état r+1 : cf arbre de Merkel
- Calculent hash de l'état r+1
- cf arbre de Merkel
- Vérifient hash identique à celui du leader
- Signent si concordance et renvoi au leader

Consensus

V

Si quorum atteint:

- L'état r+1 est scellé: signatures agrégées du quorum: QC
- un nouveau leader est déterminé à partir du sceau
- Le processus recommence pour round r+1→r+2

Scellement du nouvel état

- Un quorum de valideurs doit donner son accord
- Ex: si 100 noeuds, quorum=67
- Sceau de l' état r+1 : *signature agrégée* du leader et des 67 valideurs du hash de l'état r+1
- Ce sceau est appelé ***quorum certificate*** dans les docs Libra
- Calculs énormes pour le hash!
- Mais très limités grâce aux "Merkel Tree"
- Donc 2 techniques essentielles :
  - Merkel tree
  - Signature agrégée

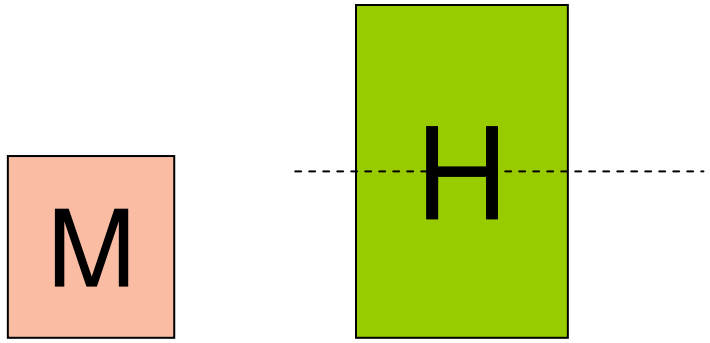
Argumentation sur la sécurité du procédé

- **Problème classique de systèmes distribués : BFT "Byzantine Fault Tolerance"**
- **Hypothèse:**
  - **N noeuds**
  - **< F fautifs, mais ne peuvent changer d'identité***
  - **H=N-F honnêtes, qui ne votent pas 2 fois**

    *** l'utilisation de signature électronique garantit ceci**
- **Besoin d'un protocole avec Q votes garantissant**

1. **Consensus établi avec des noeuds honnêtes** **Q>F**
2. **Consensus unique** **Q>F+E(H/2)**
3. **Consensus impossible (les M se taisent)** **Q<= H**

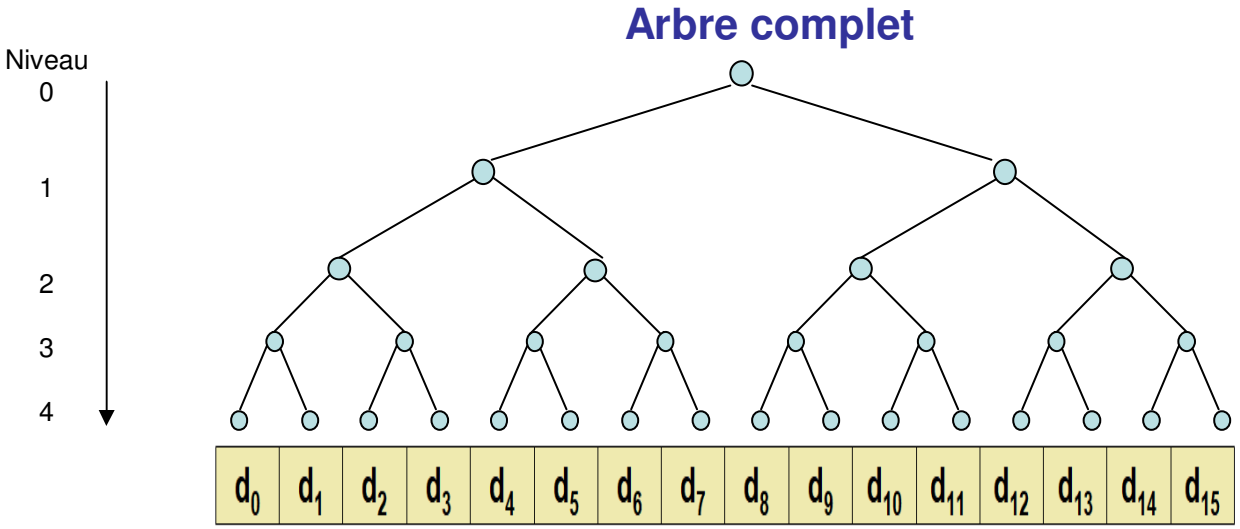
⇒ N>3F



Avec N=100, F=33, H=67

Q=67 convient

Arbre de Merkel : structure



11110
1110,(1)
110,(2)
10,(3)
0,(4)

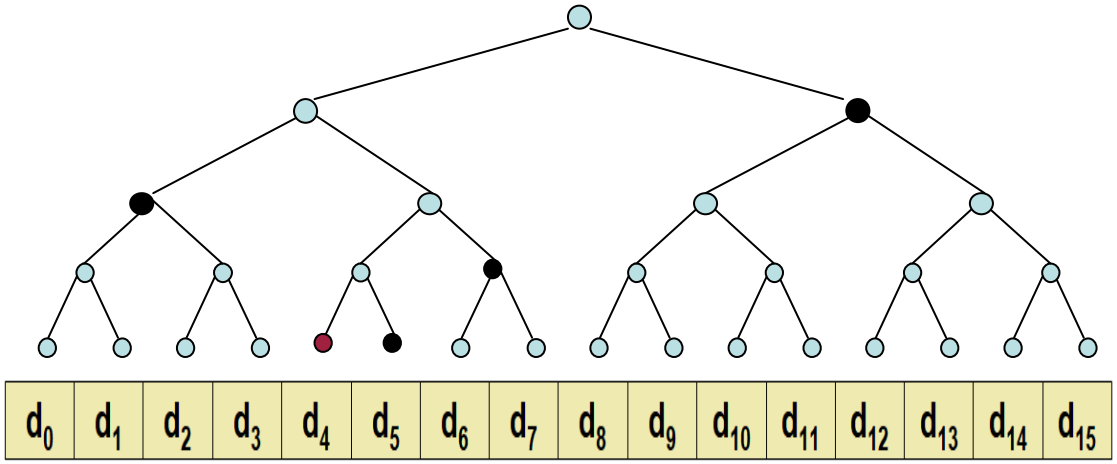
Chaque noeud contient un hash de 32 octets

- H(di) feuilles de l'arbre
- H(fils G , fils D) en remontant jusqu'à la racine
- Le hash de la racine est un hash de l'ensemble des di

Sceau (quorum certificate):
signature de h(round r, h(root)) par Quorum (sous forme agrégée)

Arbre de Merkel : lecture

Lecture et authentification d'un di par un client



Exemple: client U veut lire et authentifier d4

il suffit que U obtienne
- **d4**
- **Tous les oncles jusqu'à la racine : noeuds noirs**
- **le quorum certificate**

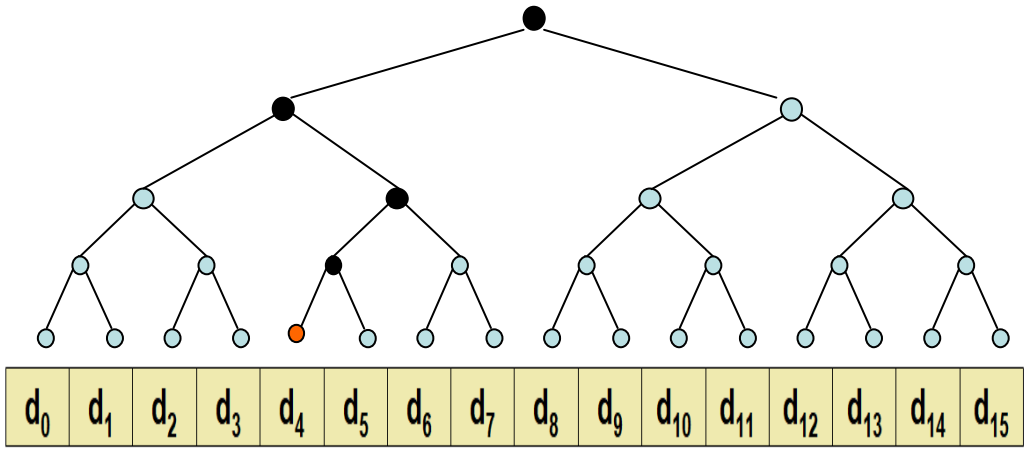
U peut alors en utilisant la relation
h(père)=h(fils G, fils D)
recalculer le hash de la racine , puis vérifier le quorum certificate

Sans cette organisation, en utilisant un fichier plat {di} il aurait fallu transmettre tous les 16 di; cette opération peut être faite dans un wallet

Arbre de Merkel : mise à jour

Mise à jour de l'arbre par un noeud:

Dans Libra, di est un compte et une transaction de paiement implique une mise à jour du compte du payeur et de celui du payé



Mise à jour de d4 → d4'

Mettre à jour noeud 4 (rouge) : h(d4)→h(d4') Puis mise à jour père, grand père,…jusqu'à la racine avec la relation h(père)=h(fils G, fils D) Donc seulement 5 hash à calculer et mettre à jour

Cette opération concerne les Nœuds
Un paiement nécessite 2 fois cette opération

Arbre de Merkel : exemple réaliste

- 1 milliard de comptes (donc de di) de 1ko en moyenne: 1To ; $H=SHA_{256}$
- Arbre de 31 niveaux: Volume arbre: 2.10^9(32 octets hash, 8 index…)=80Go

Lecture et authentification d'un di

U doit seulement calculer 31 hash et vérifier les signatures

Avec un fichier plat {di} il aurait fallu transmettre tout le fichier et calculer~ 1 milliard de hashs

Mise à jour état pour m transactions

pour mettre à jour m transactions il faut calculer et mettre à jour moins de 31.m.2 noeuds

Une organisation à plat nécessiterait le calcul de 1 milliard de hash!

Arbre de Merkel : conclusion

Avec Bitcoin 20 T/sec

Supposons que Libra ait à traiter 1000 T/s avec un milliard de comptes

Les noeuds doivent calculer <64000 hash/s

Un INTEL i7 calcule 10^6 hash en moins de 1 seconde!

Même si les noeuds ont bien d'autres tâches que les calculs de hash, on voit que LIBRA est peu consommateur de puissance de calcul, à la différence de BITCOIN!

Remarque: Historique des transactions:

1. Les noeuds peuvent fonctionner avec seulement l'état courant
2. Mais il peut être intéressant pour les clients d'avoir un historique de transactions, limité
3. Liberté de choix des noeuds

Conclusion

	LIBRA	BITCOIN
Ouverture	***Permission*** **: Club fermé** **Pas de vraie autorité** **Tolère membres malhonnêtes**	***Permissionless*** **Illusoire sans Millions de $ de serveurs / miners**
Architecture	**État des comptes=balance des comptes**	**Block chain = journal des transactions**
Scalabilité	**Bonne**	**Mauvaise et conflictuelle**
Coût invetissement **+fonctionnement**	**-Faible car leader désigné par vote, droits de vote non basés sur « CPU power »**	**-Elevé car course à la "hash power" pour gagner des bitcoins ou des commissions** **-Consommation électrique**
Performances/coût d'infrastructure	**Semble bon 1000 T/s et 1 milliards de comptes**	**Actuellement 10T/s malgré des usines de mining**
Utilisation	**Paiement FtoF ou NET** **Confirmation ~10''/2 ?**	**Paiement essentiellement NET** **Confirmation 10' inadaptée au F2F**
Stabilité unité monétaire	**Oui : gérée comme une banque centrale**	**Non: spéculation**
Anonymat	**Pseudo**	**Pseudo**

LIBRA n'est pas une blockchain (au sens Bitcoin) : Libra, c'est mieux!!!!