Sommaire blockchain

Introduction
- Généralités
- Le concept de vérité
- Comment se positionnent les entreprises
- La blockchain est une alternative à certaines architectures applicatives existantes pour éviter un contrôle centralisé ou fédéré

Un peu d'histoire
- Le role central d'Ethereum
- L'aventure bitcoin

Les technologies sous-jacentes
- Echange peer-to-peer et protocole Gossip
- Cryptographie et clés
- Les célèbres généraux byzantins
- Calcul de hash
- Arbre de Merkle et registres infalsifiables
- Signature électronique
- Gestion de fichiers distribuée : IPFS…
- Les bases mathématiques : on n'est pas obligé de tout connaître

Les principes fondamentaux de la blockchain
- Les types de blockchain : publique, privée (autorisée) ou hybride (fédérée)
- Un modèle à 4 niveaux
- Les architectures distribuées (DLT : Distributed Ledgers Technology) : Bitcoin, Ethereum, Hyperledger, Tendermint…
- Les protocoles de distribution de registres
- Les architectures centralisées
- Les architectures semi-centralisées
- Mise à jour de la vérité : les consensus, minage, différents types de preuves

La recherche de consensus : une brique essentielle dans le montage blockchain
- Les grandes familles de preuves d'autorité
- La preuve de travail (Bitcoin : « proof of work »)
- Preuve d'enjeu (« proof of stake ») : Ethereum
- Comparaison entre preuves de travail et preuves d'enjeux
- Preuve d'enjeu déléguée

Le survol des monnaies cryptographiques
- Un monde nouveau : ne pas confondre monnaie avec spéculation
- Bitcoin
- Ethereum
- Bumo
- Les stablecoins
- Libra de Facebook
- L'interopérabilité des blockchains

Exemple de la mécanique Bitcoin
- L'architecture globale
- Les transactions élémentaires
- La constitution des blocs

- Le choix du mineur et la technique du challenge

Architectures applicatives distribuées

- DApps : fonctionnement
- Les solutions pour mettre en œuvre une DApp
- Les bases distribuées : modes actif-actif
- Des exemples concrets

Développement interne

- Un métier très prometteur
- API et plates-formes dédiées
  - NOW/Nodes
  - Coinbase
  - Bitcore
  - Factom Alpha
  - Web3.js Ethereum API
  - Infura Ethereum API
  - Nomics
  - Chainpoint
  - ICObench Data API
  - Colu
  - Gem
  - BlockCypher
  - ChromaWay
  - Rootstock Open Source

L’exemple du développement concret d’une place de données boursière

Les applications concrètes de la blockchain

- La prudence est de mise : la blockchain est un moyen, pas un but
- Gestion de possession, de titularité, d'appartenance, de propriété cadastrale
- Données financières et levées de fonds ICO (« Initial Coin Offerings »)
- Formation : gestion des CV et diplômes
- Science des données
- Assurances
- Traçage de données agricoles et autres (santé, finance)
- Immobilier (« real estate »)
- Le domaine très prometteur du partage des données de santé
- Le vote électronique
- La distribution des identités : une proposition LeMarson
- Les noms de domaines gérés par les usagers

La dématérialisation et les « smart contracts »

- Principes de la dématérialisation et mise en œuvre des « smart contracts »
- Le rôle central d'Ethereum
- Langages de programmation
  - Langages qui décrivent les règles de gestion applicables à une Blockchain spécifique
  - Langages qui génèrent un code exécutable sur une autre Blockchain (« transpiler »).
- Zoom sur Solidity (Ethereum)
- L'extension du concept à des domaines non financiers : un potentiel d'idées quasi-infini.

La blockchain dans le Cloud (BaaS : Blockchain as a Service)

Les NFT (actifs non fongibles)

DeFi : finances décentralisées

- Les motivations de DeFi
- Architecture de mise en oeuvre

Web3 : la synthèse

Organismes de supervision et standards

Aspects juridiques

Les problèmes techniques à résoudre

- Gestion de la performance et capacité à monter en charge
- Solutions orientées performances : Tangle (DAG), Aerum Blockchain, Zilliqa, Ethereum Scaling Solutions, Stellar
- Sécurité
  - Des imperfections incontournables
  - Attaque à 51%
  - Attaque dite de relecture
  - Des exemples d'attaques : Sybil, Eclipse, Finney Hack, Vector Attack 76 (bitcoin), Erebus
- Consommation électrique (Bitcoin)
- Protection des données
- Le risque de prise de contrôle des opérations par une organisation politique ou commerciale

La parole à l'opposition

Ne pas ignorer les problèmes latents : techniques, juridiques, cohérence internationale

Le futur

- La recherche
- Les premiers processeurs dédiés
- Des alternatives : Hashgraph…

Avant de se quitter