Introduction

Abdelkader Ouared

abdelkader.ouared@univ-tiaret.dz

 @ouared

My roadmap..

Bonjour !

Je m'appelle **Abdelkader OUARED**

Maître de conférences HDR

Blockchain

Blockchain = The Trust Machine

« Vers la disparition de certains métiers » (Mme de Silguy, sur *Blockchain, la nouvelle révolution numérique*).

Influence du numérique dans la redéfinition de professions judiciaires et juridiques

A propos du module

- **Chapitre 1: Introduction**
  - Définition
  - La naissance de la Blockchain
  - Les inconvénients des systèmes de transactions existants Blockchain et digitalisation : Pourquoi la Blockchain est-elle appropriée pour les entreprises ?
  - Bâtir la confiance avec la Blockchain
- **Chapitre 2: Architectures et technologies Blockchain**
  - Fonctionnement
  - Caractéristiques
  - Types
  - Structure de données
  - Protocoles
  - La technologie du grand livre distribué (DLT)
- **Chapitre 3 : Contrats intelligents (smarts contracts)**
- **Chapitre 4 : Etapes pour le développement d'une application Blockchain**
- **Chapitre 5 : Utilisation de la blockchain**
  - Services financiers (Administration publique, Assurance, banques, Gestion de la chaîne logistique)
  - Santé (Dossiers médicaux personnels, Accords préalables de paiement)
  - Internet des objets (IoT)

Contenu de la matière

Intitulé du Master : Intelligence Artificielle et Digitalisation

Semestre *:* 3

Intitulé de l’UE : UF132

Intitulé de la matière : Blockchain

Crédits : 4

Coefficients : 3

Horaire du cours

Cours Théorique

14h – 15h30 (dimanche pour les cours et discussions)

TP

??h – ??h?? (?? pour la pratique et les discussions)

Mode d'évaluation

Mini projets (sous forme de TP), examen final

Logistique: contenu du cours

Site Web du cours: https://moodle.univ-tiaret.dz/

Devoirs et projets sur GitHub : https://github.com/ouared14

Communication: Instructions du personnel par courrier électronique
Les étudiants peuvent publier sur le forum Moodle et GitHub

Objectifs de l’enseignement

Le cours vise à présenter les technologies des **chaînes de blocs (blockchains)** et des registres distribués (DLT) en mettant l'accent sur leur **application** dans les domaines du **Bitcoin** et de **l'Internet des objets (IoT).** Il éclairera tous les principes derrière cette technologie ("Transactions", "Consensus décentralisé", "Blockchain", "Minage", "Preuve de travail", etc.) et discutera comment elle a commencé à révolutionner le monde par sa combinaison avec le domaine de l'IoT.

Des cas d'utilisation réels seront discutés et présentés pour mettre en avant les principaux avantages et bénéfices que les DLT peuvent apporter dans divers domaines.

Enfin, quelques leçons pratiques vous permettront de comprendre concrètement comment il est possible d'intégrer la technologie blockchain dans des scénarios IoT et de vous fournir tous les outils et compétences nécessaires pour opérer de manière autonome avec les DLT présentées.

Connaissances préalables recommandées

Systèmes informatiques et concurrence

Notions de base de l'organisation des systèmes d'exploitation, des threads, de la gestion de la mémoire, des systèmes de fichiers, de l'ordonnancement, des réseaux, etc.

Bonnes compétences en programmation

Systèmes distribués – utile

Cryptographie – utile

Probabilité – utile

Prérequis

Have you ever heard about Bitcoins?

- Yes, I know what they are
- Yes, I know something but not sure about what they are
- Yes, but I still don't what they are
- Are you kidding me :D (never heard)?

Have you ever heard about Blockchains?

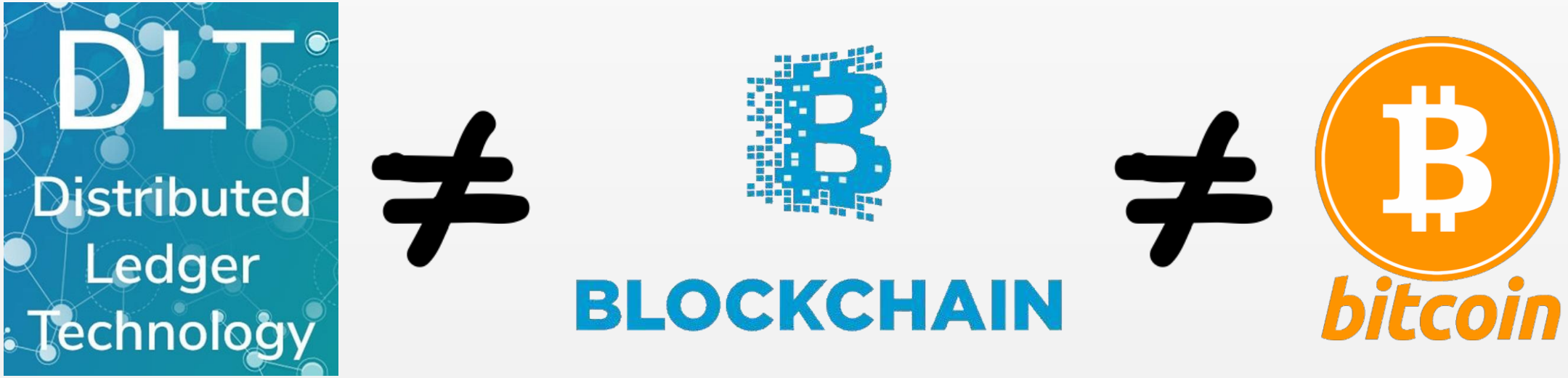
- Yes, I know what they are
- Yes, I know something but not sure about what they are
- Yes, but I still don't what they are
- Are you kidding me :D (never heard)?

Have you ever heard about DLT (Distributed Ledger Technologies)?

- Yes, I know what they are
- Yes, I know something but not sure about what they are
- Yes, but I still don't what they are
- Are you kidding me :D (never heard)?

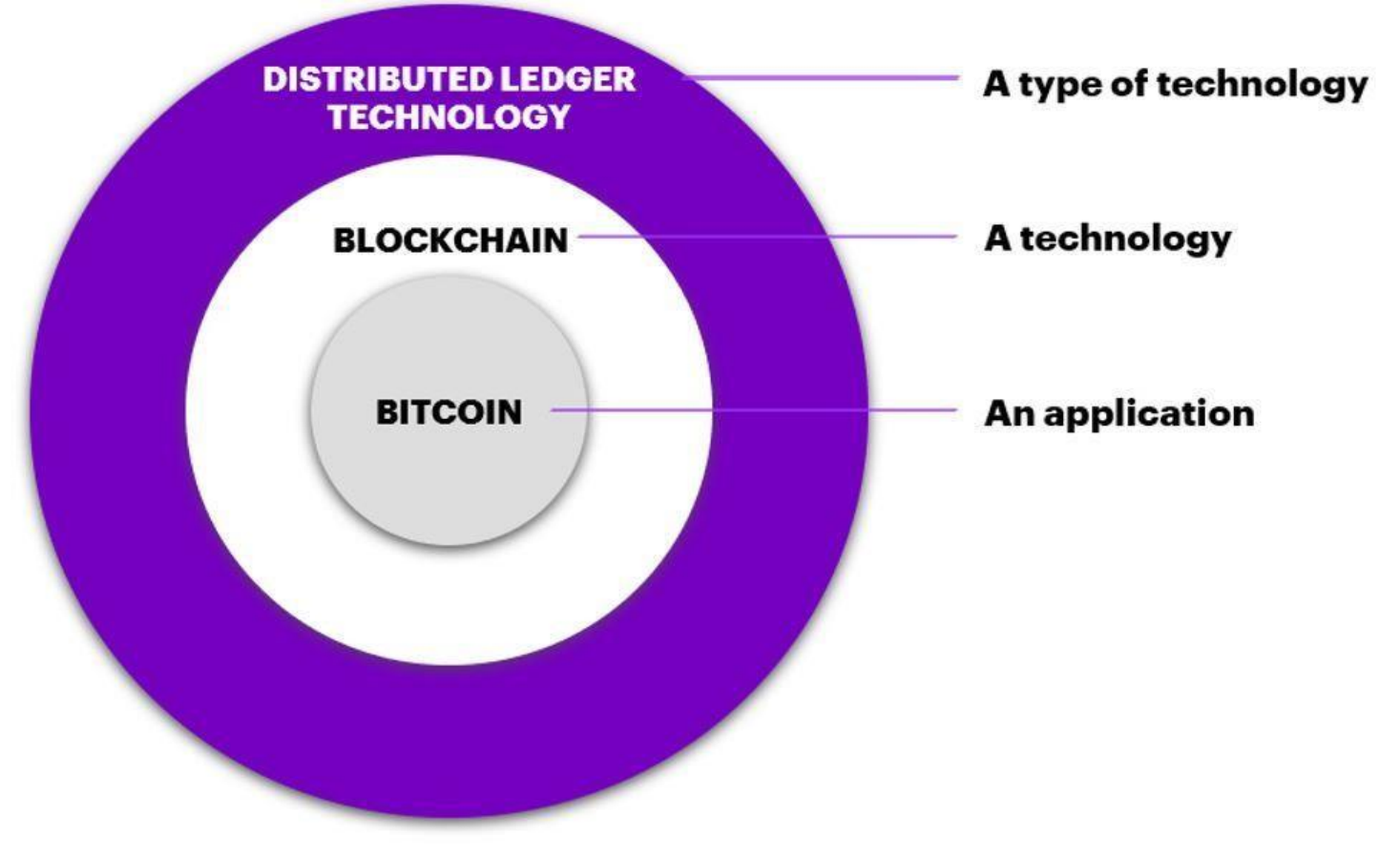
Concepts fondamentaux

DLT vs Blockchain vs bitcoin…



Concepts fondamentaux

DLT vs Blockchain vs bitcoin…



Source: https://www.accenture.com/nl-en/blogs/insights/redefining-blockchain-more-than-a-technology

Comment nous sommes arrivés ?

Évolution de la confiance (**Trust**)

PHASE 1

TRIBAL TRUST

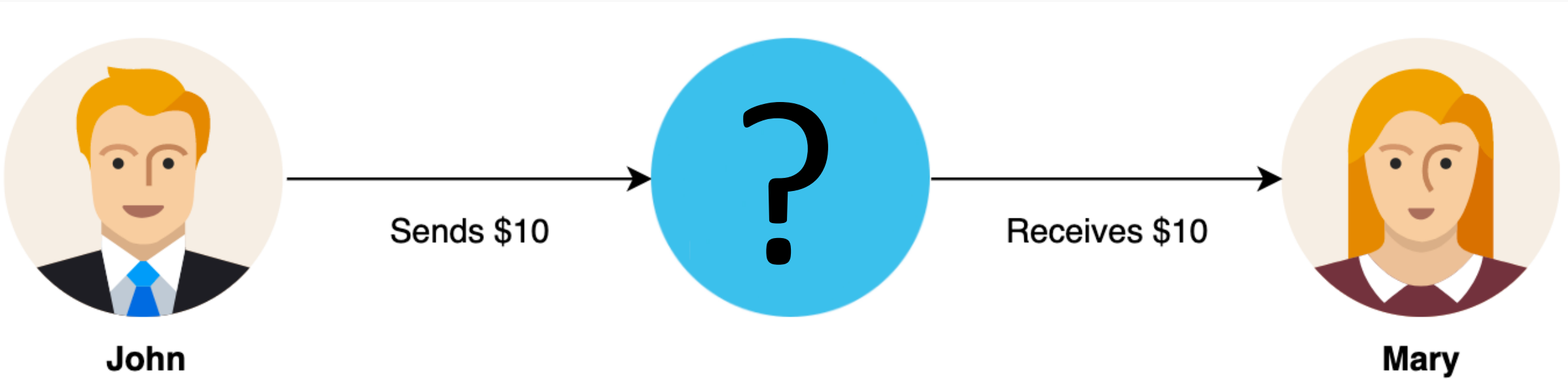
PHASE 2

INSTITUTIONAL TRUST

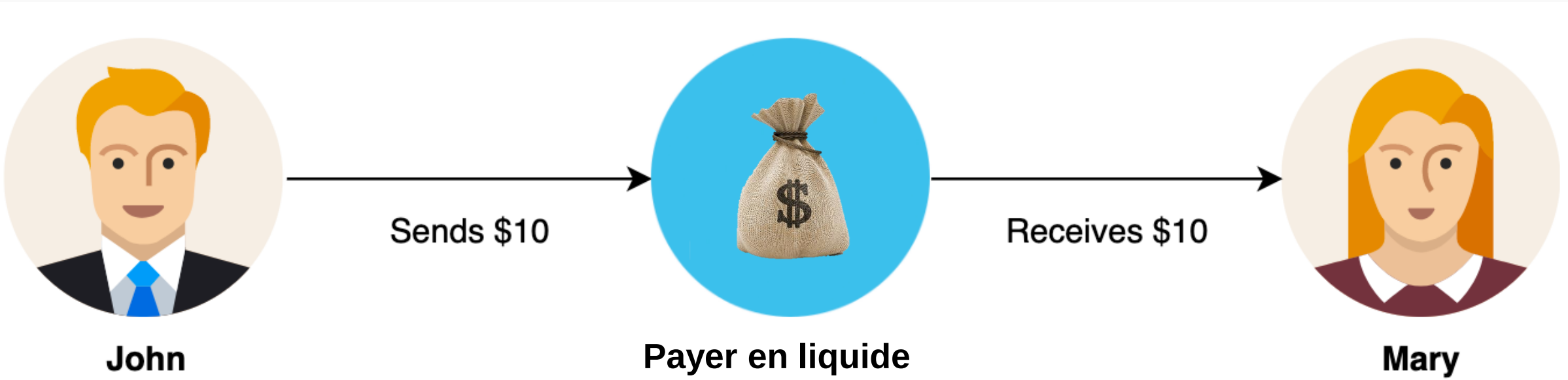
PHASE 3

DISTRIBUTED TRUST

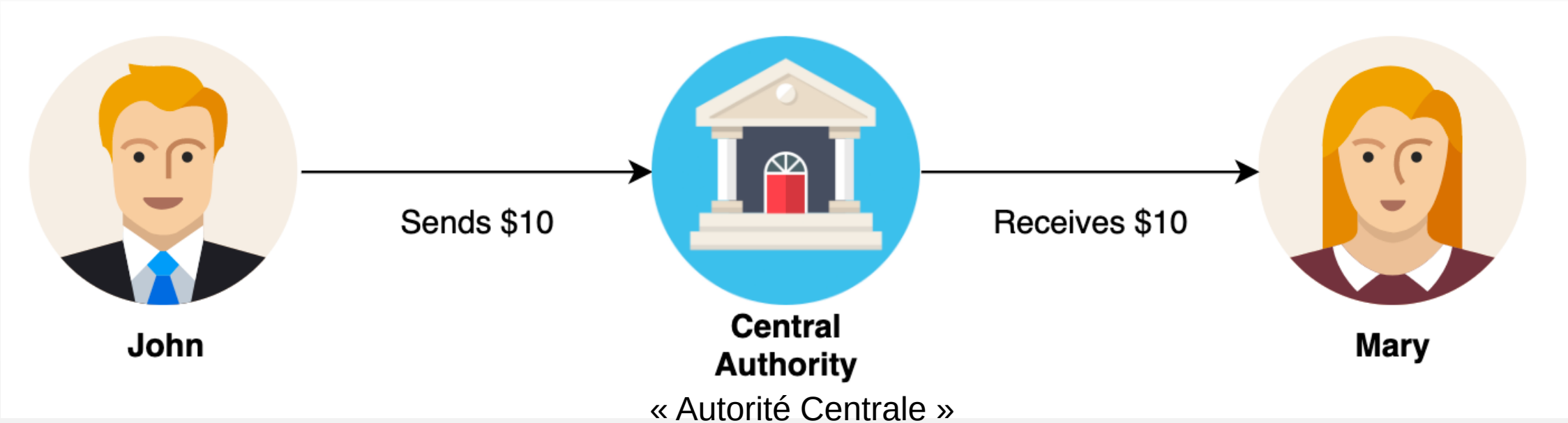
Évolution de la confiance (**Trust**)



Évolution de la confiance (**Trust**)



Évolution de la confiance (**Trust**)



« Autorité Centrale »

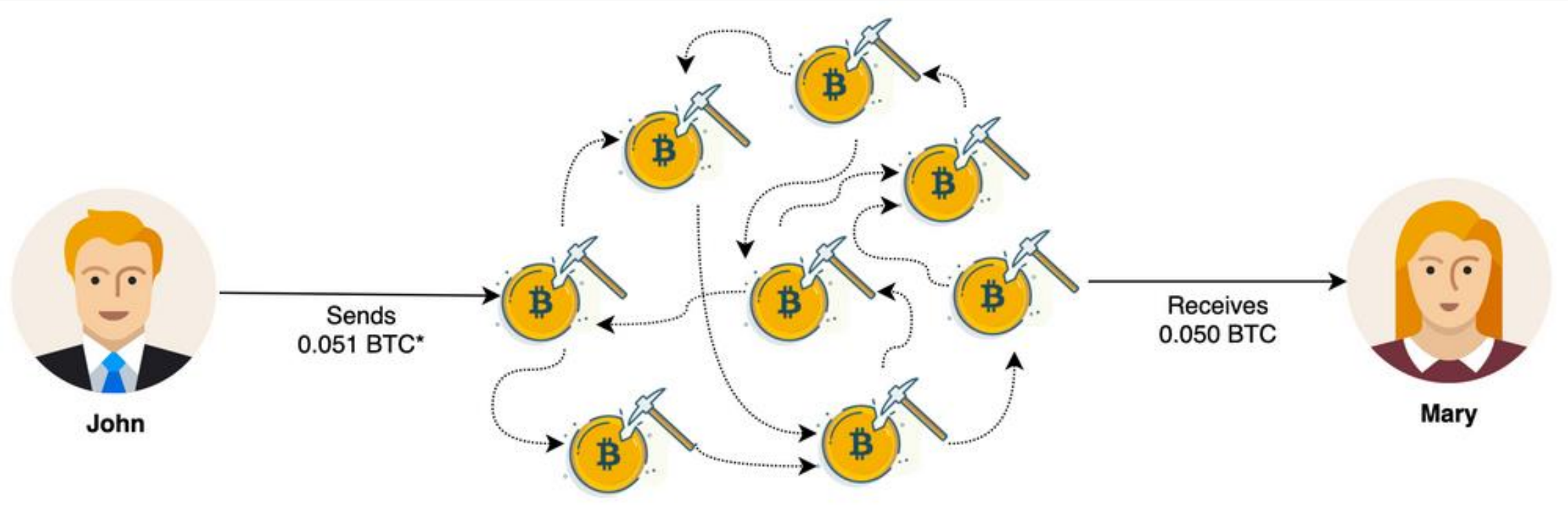
Évolution de la confiance (**Trust**)

Deux problèmes :

- Comment créer un identifiant unique sans autorité centrale ?
- Comment s'assurer que les transactions ont été légitimement émises depuis un compte ?

Évolution de la confiance (**Trust**)

Human success is based on flexible cooperation in large numbers. This requires **trust**



C’est quoi un **Grand Livre** (LEDGER??)

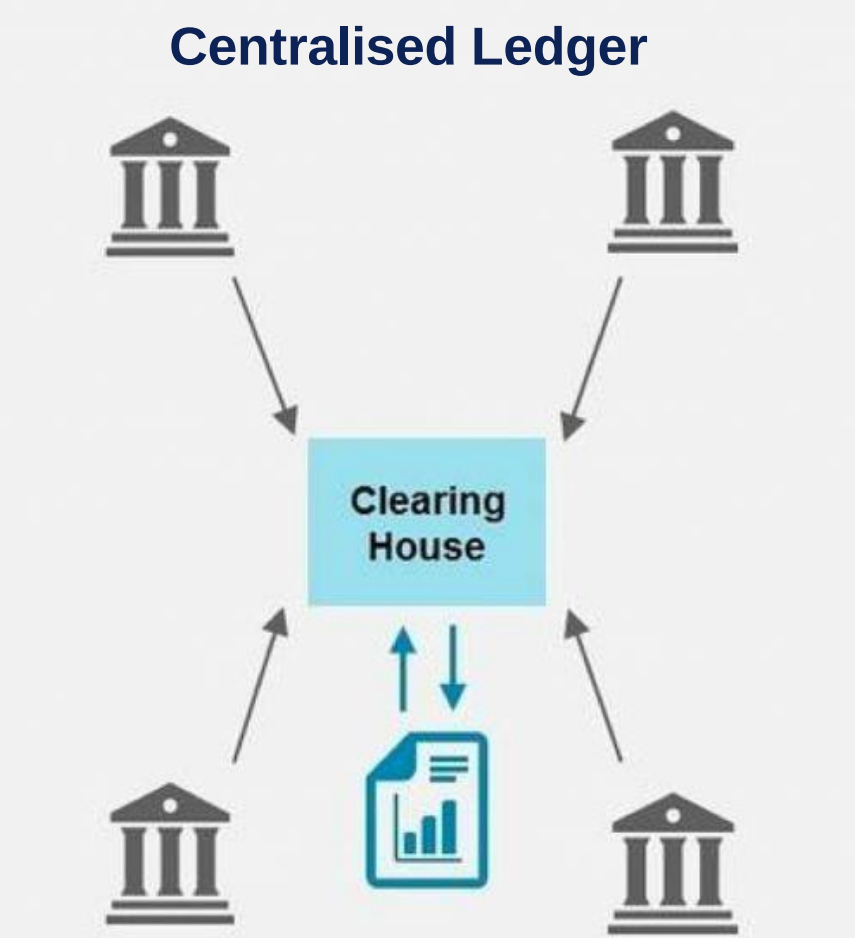
Date	Description	Credit	Debit	Balance
2/20/2011	Alice to Bob	-$10		$90
2/20/2011	Bob from Alice		+$10	$10
3/20/2011	Bob to Eve	-$5		$5

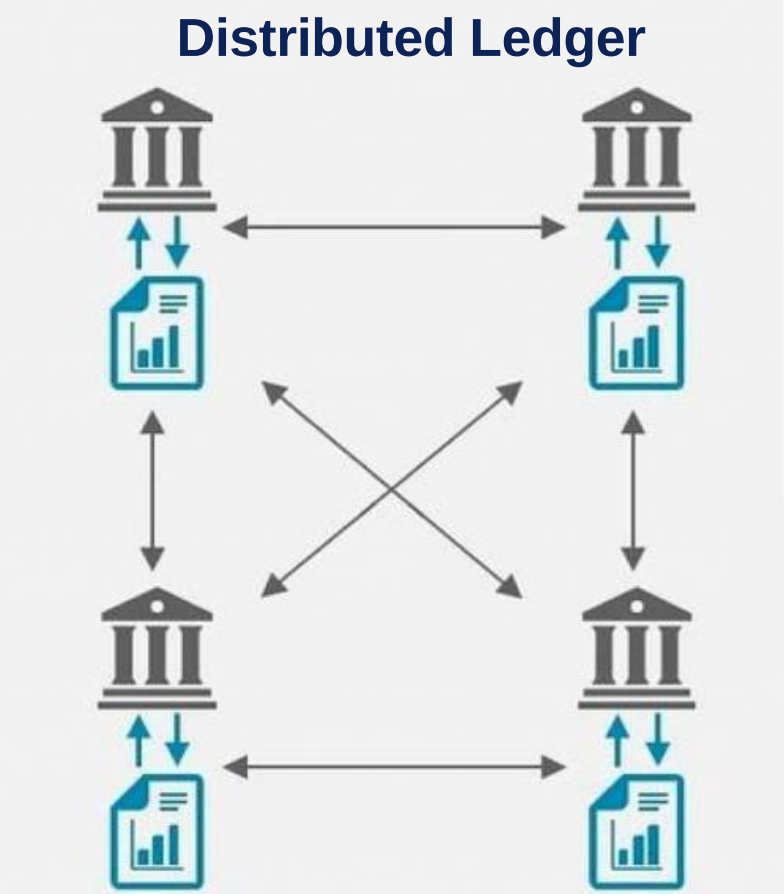
Not a very new thing !

Early 19th-century German ledger

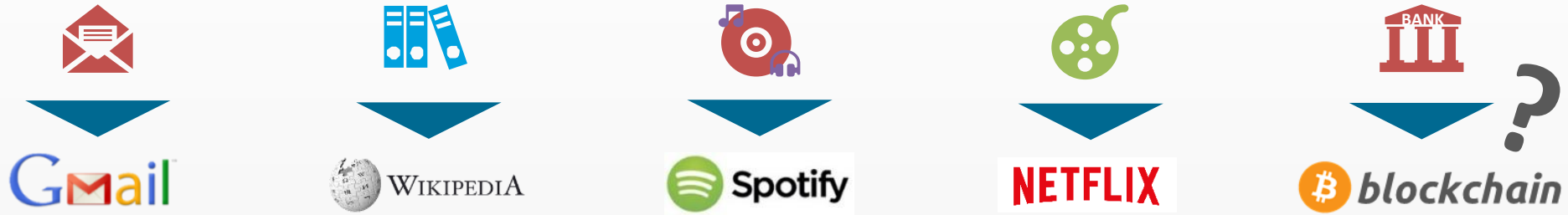
L’idée principale: Distribution et la Réplication

La technologie des registres distribués (DLT)





L'économie de l'information



- Les données sont transférées à coût marginal nul.
- Pourquoi payer des frais pour déplacer des octets représentant de la richesse ?
- Pourquoi seulement de 9h à 16h, du Dimanche au Jeudi, avec un délai de règlement de deux jours ?

Qui (et quand) offrira à l'humanité un réseau de paiement P2P mondial ***instantané*** et ***gratuit*** ?

QU'EST-CE QU'UNE BLOCKCHAIN ?

A blockchain is
one of the possible implementations
of a distributed ledger

where transactions are stored
in a series of ***cryptography-linked blocks***

La Naissance des Blockchain

Stuart Haber and Scott Stornetta

How to time-stamp a digital document

Early 1990

How our timestamping mechanism was used in Bitcoin

A Peer-to-Peer Cache System for Bitcoin.

Year 2008

Satoshi Nakamoto

The co-inventors of the early blockchains.

Objective: Implement a system wherein document timestamps could not be tampered with

Invention of BlockChain

First bitcoin transactions
Reusable Proofs of Work

Dev. Hal Finney

Dr. Vitalik Buterin

Year 2014

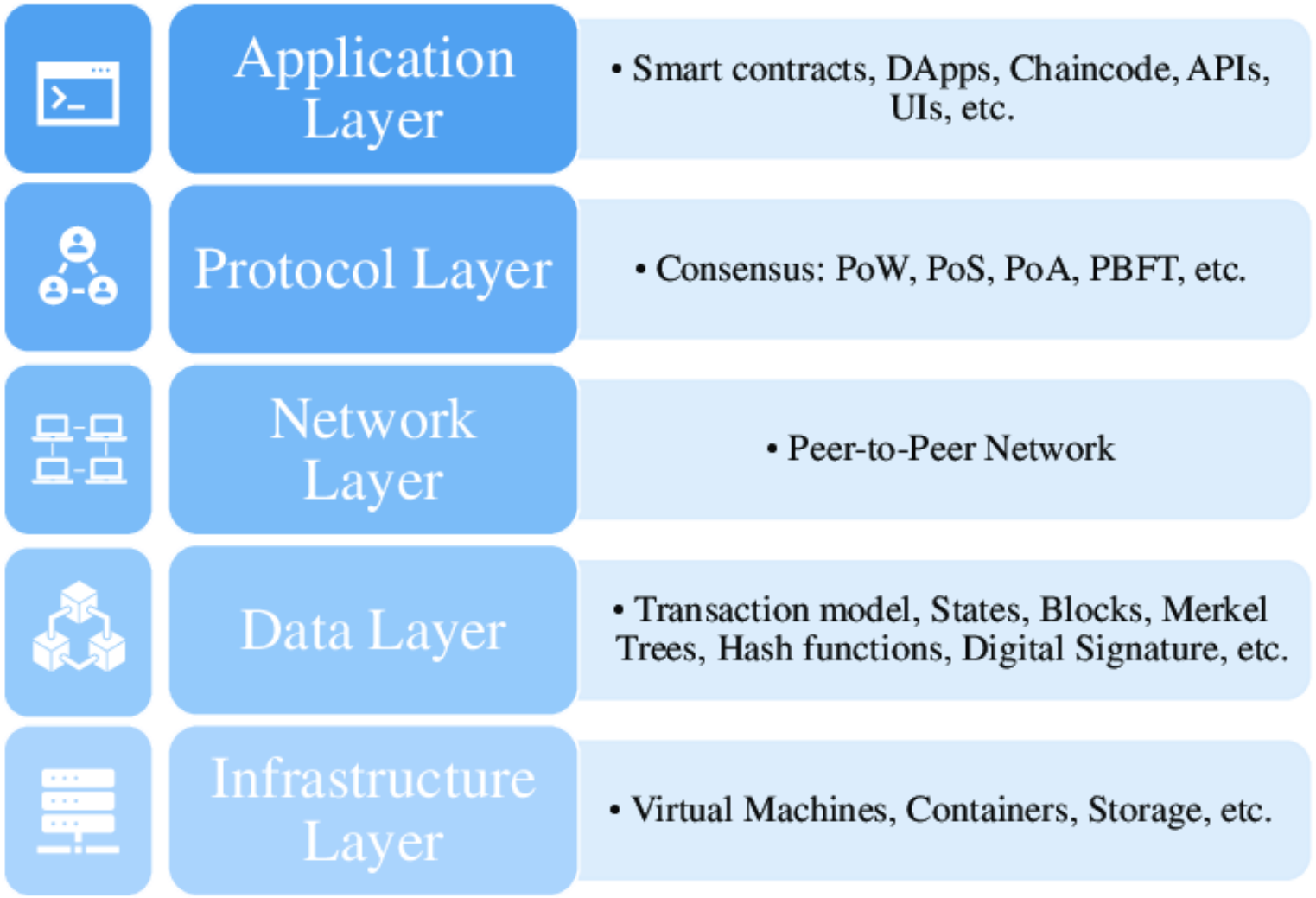
Ethereum white paper: a next generation smart contract & decentralized application platform.

Gavin Wood, Charles Hoskinson, Anthony Di Iorio

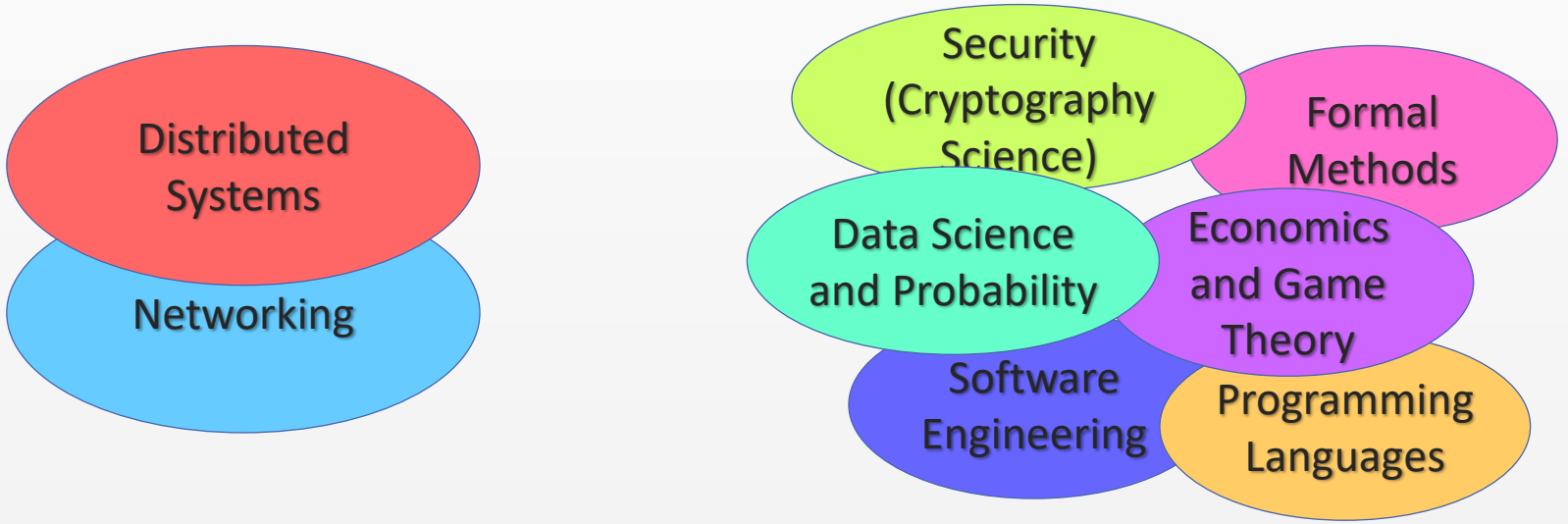
The idea of Ethereum >> Let's BUILD

Year 2015

Blockchain Layer



Blockchain est un carrefour entre plusieurs disciplines..



C’est quoi le Bitcoin

Le Bitcoin est une monnaie numérique qui fonctionne de manière décentralisée. Cela signifie qu'aucune institution centrale, comme une banque ou un gouvernement, ne contrôle son émission ni ses transactions.

- **Transactions directes et anonymes:** Les utilisateurs peuvent envoyer et recevoir des bitcoins directement entre eux, sans passer par un intermédiaire. Ce système de paiement peer-to-peer garantit un certain anonymat, bien que les transactions soient enregistrées sur une blockchain publique.
- **Pas de forme physique, pas de valeur intrinsèque:** Le Bitcoin n'existe pas sous forme physique (comme un billet ou une pièce). Sa valeur est entièrement déterminée par l'offre et la demande sur les marchés.
- **Une technologie sous-jacente :** la blockchain : Le Bitcoin repose sur une technologie appelée blockchain, un registre numérique décentralisé et sécurisé qui enregistre toutes les transactions. Cette technologie est également utilisée par d'autres cryptomonnaies.

C’est quoi le Bitcoin

Monnaie numérique décentralisée

Aucun gouvernement ni aucune organisation ne la soutiennent

Pas besoin de tiers de confiance

Transactions peer-to-peer instantanées

Sécurité cryptographique

Incitations économiques synergiques

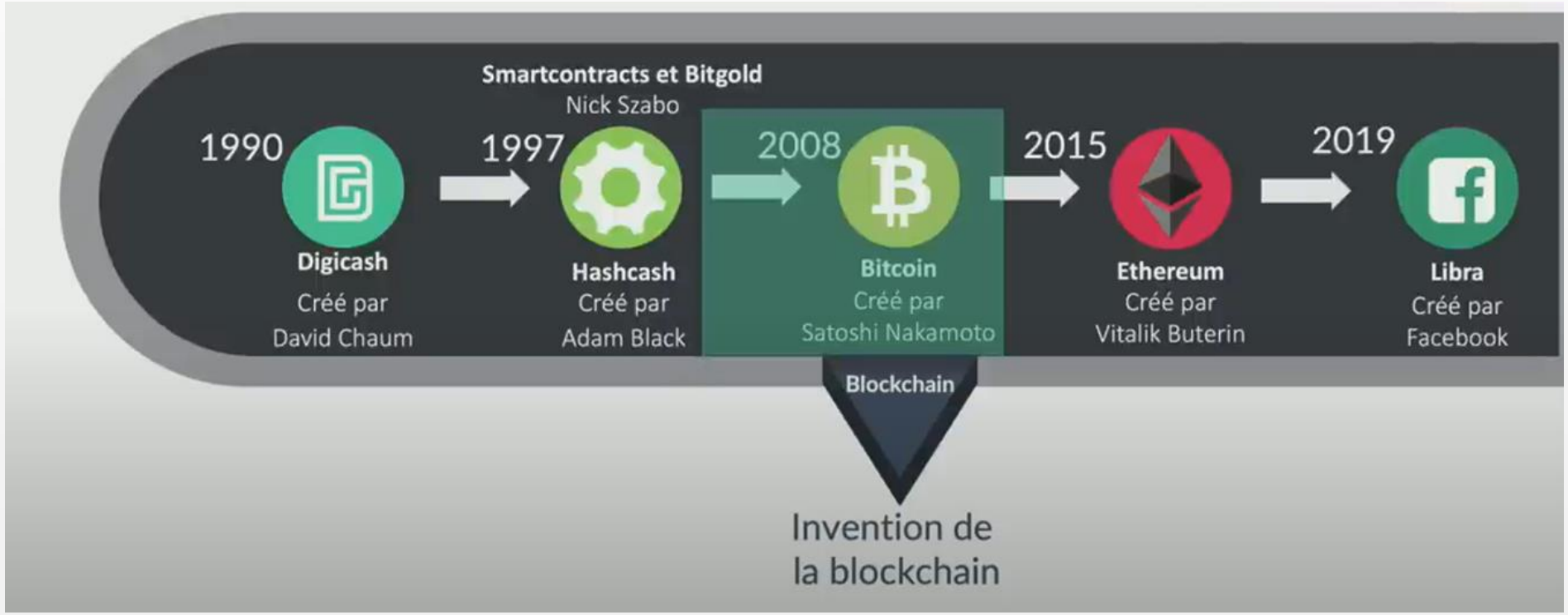
Services bancaires efficaces à faible coût pour tous et partout

https://bitcoin.org/en/faq

http://www.coindesk.com/information/

La Naissance des Blockchain

De Digicash à Libre



QUELQUES CRYPTO-MONNAIES CÉLÈBRES

Bitcoin

• Dash

Litecoin

•Dogecoin

Ether

Ripple

Quelle est la différence entre la Blockchain et les bases de données traditionnelles ? (SQL/NoSQL)

Properties	Database	Blockchain
Operations	Can perform CRUD Operations	Can Insert & View Data
Owner	Entity is the Owner	No-one Owns the Data
Edit Access	Administrator Can Edit Data	Editing Data is not possible
Replication	Data available on at Admin	Data available in All the peers
Consensus	No Consensus, anyone can enter the data	Peers will confirm the outcome of the Transactions
Verification	Only admin can access the data	Anyone can verify the transactions

Langage de programmation

Connaissance de HTML5/CSS3, Javascript

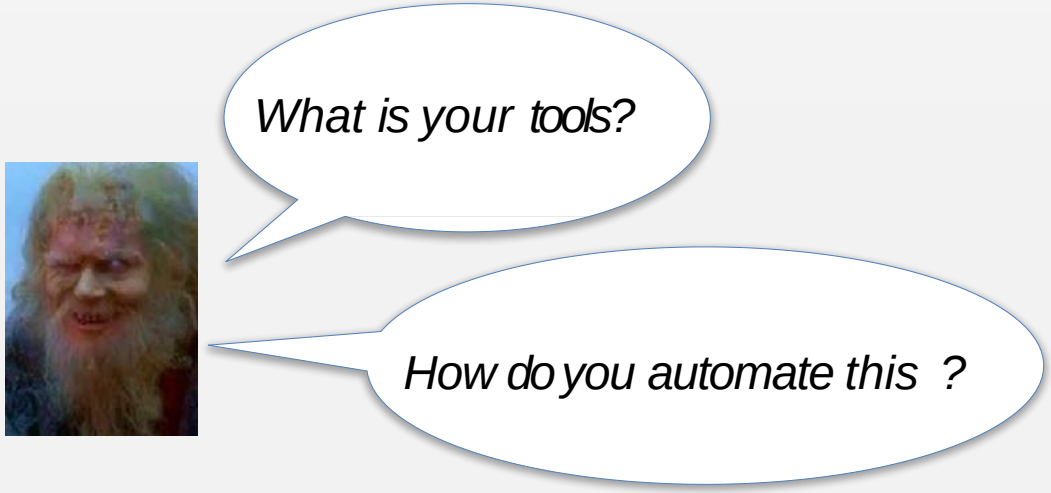
MEAN Stack : Mongo Js, Express Js, Angular Js, Node JS

Programmation Python

Programmation Go

REST (e.g. Libra, Parity) libra parity

Solidity



Références (Useful materiaL)

- *BOOK Andreas M. Antonopoulos. 2014. Mastering Bitcoin: Unlocking Digital Crypto Currencies (1st. ed.). O'Reilly Media, Inc. Opensource book, Published on Github : https://github.com/bitcoinbook/bitcoinbook*
- *BOOK Imran Bashir. 2020. "Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps , cryptocurrencies, Ethereum, and more". 3rd Edition. Packt Publishing Limited*
- *BOOK Chapter Shubhani Aggarwal, Neeraj Kumar, "Chapter Seven Basics of blockchain", Editor(s): Shubhani Aggarwal, Neeraj Kumar, Pethuru Raj, Advances in Computers, Elsevier, Volume 121, 2021, Pages 129 146, ISSN 0065 2458, ISBN 9780128219911, https://doi.org/10.1016/bs.adcom.2020.08.007*
- *Fran Casino, Thomas K. Dasaklis , Constantinos Patsakis , "A systematic literature review of blockchain based applications: Current status, classification and open issues", Telematics and Informatics, Volume 36, 2019, Pages 55 81, ISSN 07365853, https://doi.org/10.1016/j.tele.2018.11.006*
- *T. M. Fernández Caramés and P. Fraga Lamas, "A Review on the Use of Blockchain for the Internet of Things," in IEEE Access, vol. 6, pp. 32979 33001, 2018, doi : 10.1109/ACCESS.*
- *J. Brogan, I. Baskaran, N. Ramachandran, "Authenticating Health Activity Data Using Distributed Ledger Technologies", Computational and Structural Biotechnology Journal, Vol. 16, 2018, Pages 257 266, doi: 10.1016/j.csbj.2018.06.004*
- *A. Rashid and M. J. Siddique, "Smart Contracts Integration between Blockchain and Internet of Things: Opportunities and Challenges," 2019 2nd International Conference on Advancements in Computational Sciences (ICACS), Lahore, Pakistan, 2019, pp. 1 9, doi : 10.23919/ICACS.*
- *Teng, S.Y., Touš , M., Leong, W.D., How, B.S., Lam, H.L., Máša , V., "Recent advances on industrial data driven energy savings: Digital twins and infrastructures" (2021) Renewable and Sustainable Energy Reviews, 135, art. no. 110208, DOI: 10.1016/j.rser.2020.110208*

Questions ?!!