

**Nouveaux Mondes**

**Blockchain et Cryptocurrencies**

**Philippe DUCHEMIN**

**19 janvier 2018**

# INTRODUCTION

## APPROCHE MULTI AXES

- Monde Réel et Monde Numérique/Digital
- Les technologies de l'information - Fintech
- Approche Historique
- Impacts Finance et autres
- Enjeux économiques, éthiques, sociaux

# REVOLUTIONS

## RUPTURES TECHNOLOGIQUES

- Information Technology: cpu, database
- Système de paiement: Swift
- Internet/web
- Blockchain/Cryptodevises
- Smartcontracts

# LE MONDE EN CHANGEMENT

- NUMERISATION DE L'ECONOMIE : DEMAT
- DIGITALISATION DES PROCESS
- CONFIANCE ET PREUVE – **trust and proof**

## TRAITEMENT DE L'INFORMATION

- **Big Data**
- **Artificial Intelligence**
- **From Data Management to Event management**

# LE MONDE EN CHANGEMENT

TOUT DEVIENT DE INFORMATION

- IDENTITE
- PROPRIETE
- ECONOMIE

ET

DEMATERIALISATION

# IDENTITE

- Définition:
  - Individu: personne physique, personne morale, fonction dans l'entreprise
  - Animal, objet
  - Biorecognition, puce électronique
- Certificats:
  - Papiers d'identité, passeport
  - Permis de conduire
  - Diplômés et certificats d'aptitude
  - Autorisations
  - Certification physique : taille, poids,
  - Certification monétaire : revenus
  - Certification : nb d'enfants

## COMMENT IDENTIFIER

- un individu
  - Présence physique et empreinte biologique
  - Certificats « infalsifiables »: ID, passeport, ss, iban, siret, siren, LEI (Legal Entity Identification)
  - Identification: nom, adresse mail, téléphone
  - Support physique: « être en possession de »
  - « dans la tête »: code numérique ou password
- Un objet

# OBJETS

PROPRIETES = immatriculés

- Voitures – carte grise
- Terrains, maisons = cadastre
- Ressources naturelles: énergie, matériau, métaux, ...
- Animaux , végétaux, ...
- Personnages célèbres (décédés)
- Ordinateurs, smartphone, bagages (gps)

Attributs et certificats

- Objets/ certification (grues)
- Objets/conformité
- Animaux/vaccination



# ECONOMIE

- Support de valeur
  - Physiques: terrains, objets, vivant/non vivant
  - Immatériel: securities, marque, brevets, entreprises, media
  - Capital humain: expertise, consommateur
  - Monnaie fiduciaire et monnaie scripturale
  - Compte bancaire - compte de paiement (PSP2)
- Transactions = contrats
  - Achats / Ventes immédiats
  - Contrats avec durée: engagement

# ECONOMIE

- Valeur marginale nulle
  - Objets numériques = médias: musiques, photos, livres, films,....
- Valeur marginale infinie
  - La monnaie
  - Comment éviter la duplication
- Economie démonétisée
  - Troc
- Disparition de la monnaie fiduciaire (y compris divisionnaire)
- Disparition de la comptabilité...

# CONTRAT AVEC SIGNATURE

## COMMENT SIGNER UN CONTRAT BILATERAL

- Lieu physique de signature, document papier, 2 représentants
- Signature de 2 documents avec dates de signature
- Présences de témoins éventuels
- Document électronique
  - Non répudiation: ne peut être remis en cause
  - Signature électronique: fonction de « hashing » fournissant un code réduit représentant le document
  - Horodatage électronique: preuve temporelle
  - Tiers de Confiance

# ARCHIVAGE NUMERIQUE

## COMMENT ASSURER L'INTEGRITE D'UN DOCUMENT

- Lieu physique de conservation: coffre
- Altération lente
- Accès via copie conforme

## DOCUMENT ELECTRONIQUE

- Message = CONTENU + FORMAT
- Définition du contenu
- Le contenu reste, le format change
- Les outils de lecture
- Problème des documents signés
- Décryptage possible demain

# BOURSE DE VALEURS

## COMMENT ECHANGER DES VALEURS

### Bourse des valeurs - Exchange

- Lieu physique: Bourse de Paris (Palais Brongniart)
- Produits standardisés: Futures, Securities, Brent, once d'or, carcasse de porc, droit à polluer,...
- Membres d'un club: « agents de change »/ broker
- Serveurs informatiques et algorithme (prix d'ouverture)
- Membres d'un club: « agents de change »/ broker

POUR: financement et pricing

### LES INFRASTRUCTURES DE MARCHES : DTCC - EMIR

- CCH: Central Clearing Houses – CC: Central Counterparts – LCH- Global Custodian ....

# DEMATERIALIZATION

- Infrastructures de Monnaie: CB, SWIFT, PSP2
- Infrastructures de marché: Bourses (Organized Markets/listed products) et OTC, EMIR, netting
- Factures, web facturiers, API
- Crypto currency BTC ETH

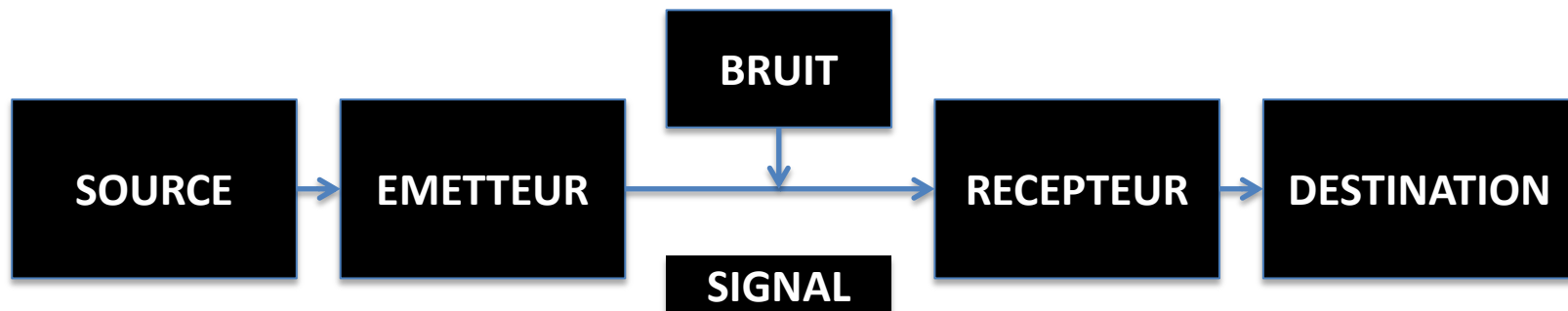
done ....next:

- Urssaf émetteur de feuilles de salaire
- Education: émetteur de diplômes et certificats
- Fisc: émetteur de factures, collecte de tva
- Disparition de la monnaie fiduciaire

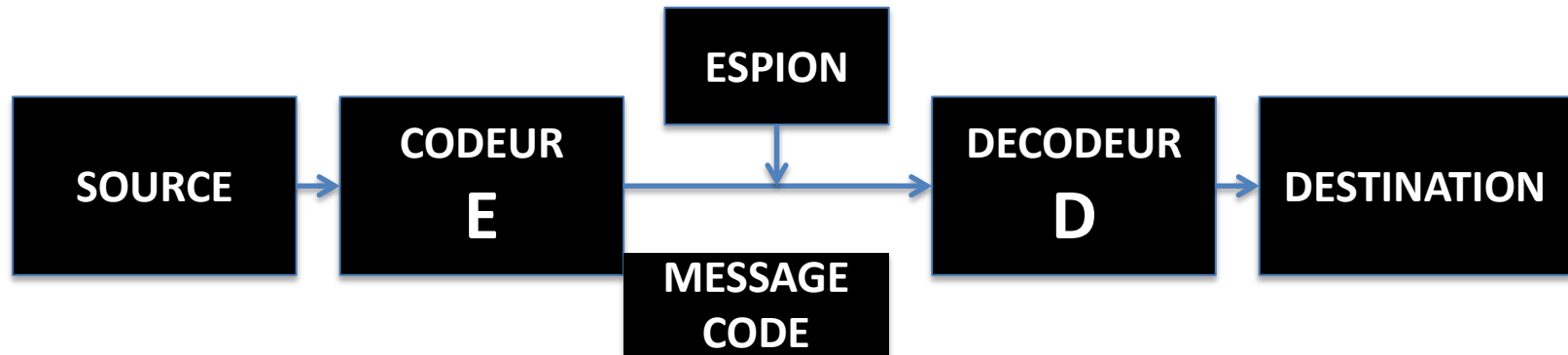
# THEORIE DE L'INFORMATION

1948: théorie de la communication de SHANNON

- Un émetteur et un récepteur = identités
- Lien physique = canal de communication
- Échangé de données: codage compression
- Correction d'erreurs – redondance
- Confidentialité: cryptographie



## COMMENT ECHANGER UN MESSAGE SECRET



2 méthodes:

- Codage avec une clé privée symétrique, qui sert au codage et au décodage.
- Codage asymétrique, avec clé publique et clé privée
  - 1976 - Diffie et Hellmann
  - 1978 - RSA: Rivest, Shamir et Adleman



# CRYPTOGRAPHIE et RSA

Le RSA (Rivest, Shamir, Adleman 1977) repose sur les:

## FONCTIONS A SENS UNIQUE (TRAPDOOR FUNCTION)

Et génération de 2 clés:

- Clé publique = adresse
- Clé privée = clé de la boîte aux lettres

Et aussi:

- AUTHENTIFICATION d'un utilisateur, Signature électronique
- INTEGRITE d'un document
- CONFIDENTIALITE

# ENIGMA – CODES ALLEMANDS

Geheime Kommandosache! Jede einzelne Tagesstiftel ist geheim. Mitteil. v. im Flugzeug verboten! Nr. 00190

## Luftwaffen-Maschinen-Schlüssel Nr. 649

**Achtung!** Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.

Monats- tag	Wellenlage			Ringstellung	Stellung der Verbindungen										Kenngruppen										
					an der Umkehrrolle				an Stecherbrett																
049	31	I	V	III	14	09	24					SZ	OT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ekb	rzg
049	30	IV	III	II	05	26	02					IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	kti	acw	zsi	wao
049	29	III	II	I	12	24	03	KM	AX	PZ	OO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioe	zen	ovw	wvd
049	28	II	III	V	06	08	16	DI	CN	BR	PV	CR	PV	AI	DK	OT	MQ	EU	BX	LP	GJ	lrb	cid	ude	rzh
049	27	III	I	IV	11	03	07	LT	EQ	HS	UW	DY	IN	BV	OR	AM	LO	PP	HT	EX	UW	woj	fbh	vet	uis
049	26	I	IV	V	17	22	19					VZ	AL	RT	KO	CG	EI	BJ	DU	PS	HP	xle	gbo	uev	rxm
049	25	IV	III	I	08	25	12					OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit
049	24	V	I	IV	05	18	14					TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl	rwl	vei	tlq
049	23	IV	II	I	24	12	04					QV	FR	AK	EO	DH	CJ	MZ	SX	GN	LT	ebn	rwm	udf	tlo
049	22	II	IV	V	01	09	21	IU	AS	DV	OL	FJ	ES	IM	RX	LV	AY	OU	BG	WZ	CN	jqc	acx	mwe	wve
049	21	I	V	II	13	05	19	PT	OX	EZ	CH	RU	HL	PY	OS	GZ	DM	AW	CE	TV	NX	jpw	del	mwf	wvf
049	20	III	IV	V	24	01	10	MR	KN	BQ	PW	DP	NO	QZ	AU	RY	SV	JL	GX	BE	TW	jqd	cef	nvo	ysh
049	19	V	III	I	17	25	20					OX	PR	PH	WY	DL	CM	AE	TZ	JS	GI	idf	fpz	jwg	tlg
049	18	IV	II	V	15	23	26					EJ	OY	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	gbw	vcj	rxn
049	17	I	IV	II	21	10	06					IR	KZ	LS	EM	OV	OY	QX	AP	JP	BU	mae	hzi	sog	ysi
049	16	V	II	III	08	16	13					HM	JO	DI	NR	BY	XZ	OS	PU	PQ	CT	tdp	dhb	rkb	uiv
049	15	II	IV	I	01	03	07					DS	HY	MR	QW	LX	AJ	BQ	CO	IP	NT	ldw	hzj	soh	wvg
049	14	IV	I	V	15	11	05	AI	BT	MV	HU	GM	JR	KS	IY	HZ	PL	AX	BT	CQ	NV	imz	noa	tjv	xtk
049	13	I	III	II	13	20	03	PW	EL	DG	KN	LY	AG	KM	BR	IQ	JU	HV	SW	ET	CX	zdy	rkf	tjw	xtl
049	12	V	I	IV	18	10	07	MU	BP	CY	RZ	KX	AN	JT	DG	IL	PW					zdy	rkf	tjw	xtl
049	11	II	IV	III	02	26	15	RZ	OQ	CP	SX	KN	UY	HR	PW	PM	BO	EZ	QT	DX	JV	zea	rjy	soi	wvh
049	10	III	V	IV	23	21	01					LR	IK	MS	QU	HW	PT	GO	VX	PZ	EN	lrc	zbx	vbm	rxo
049	9	V	I	III	16	04	08					QY	BS	LN	KT	AP	IU	DW	HO	RV	JZ	edj	eyr	vby	tih
049	8	IV	II	V	13	19	25					PI	NQ	SY	CU	BZ	AH	EL	TX	DO	KP	yiz	dha	ekc	tli
049	7	I	IV	II	09	03	22					UX	IZ	HN	BK	OQ	CP	FT	JY	MW	AR	lan	dgb	zsj	wbi
049	6	III	I	V	11	18	14	IL	AP	EU	HO	DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	lao	cft	zsk	wbj
049	5	V	II	IV	23	02	25	QT	WZ	KV	GM	MV	CL	OK	OQ	BI	FU	HS	PX	NW	EY	lju	cdr	iye	waj
049	4	II	IV	I	04	21	09					AC	BL	OZ	EK	QW	QP	SU	DH	JM	TX	lsb	zby	vcy	ujb
049	3	V	I	II	19	11	06	BF	NR	DX	CS	KR	MP	CN	BP	EH	DZ	IW	AV	GJ	LO	lap	owd	iwu	wak
049	2	IV	V	I	16	14	02					BN	HU	EG	PY	KQ	CP	OS	JW	AI	VZ	aqd	bdy	iyf	xtd
049	1	II	I	III	23	12	10					DP	BM	NZ	CK	OV	HQ	AP	UY	SW	JO	kgl	cdf	giq	wuv

# OBLIVIOUS TRANSFER PROTOCOL: OTP

- Le problème du millionnaire:
  - Alice possède 5 millions
  - Bob possède 7 millions

Comment savoir qui est le plus riche sans divulguer les richesses respectives
- Tirer à pile ou face au téléphone
  - Alice et Bob choisissent 2 nombres
  - Alice gagne si les deux nombres sont pairs
  - Alice envoie son nombre codé à Bob
  - Bob envoie son nombre non codé à Alice
  - et...

# OBLIVIOUS TRANSFER PROTOCOL

- Ou comment calculer des fonctions sur des données non identifiables
- Les applications sont énormes à l'ère du **Big Data**
  - Faire des statistiques sans connaître les participants
  - Statistiques financières sur les portefeuilles
  - Le vote en ligne

# PROOFS and COSTS

- Captcha :
- Proof of Work – cout cpu
- Proof of Knowledge - Zero Knowledge Proof
- Proof of Space – cout en mémoire
- Proof of Ownership –Proof of Stake – utilisé par Ethereum
- Proof of Bandwidth – collecter des tokens
- SFE: Secure Functions Evaluation

# Proof of Knowledge - PoK

Alice veut prouver à Bob qu'elle connaît X

1. Alice calcule  $Y = G^X$  et  $T = G^V$
2. Bob reçoit Y et T (il connaît G mais pas X et V)
3. Alice calcule  $R = V - C.X$
4. Bob reçoit R et connaît C
5. Bob vérifie  $T = G^R . Y^C = G^{V-CX} . G^{CX} = G^V$

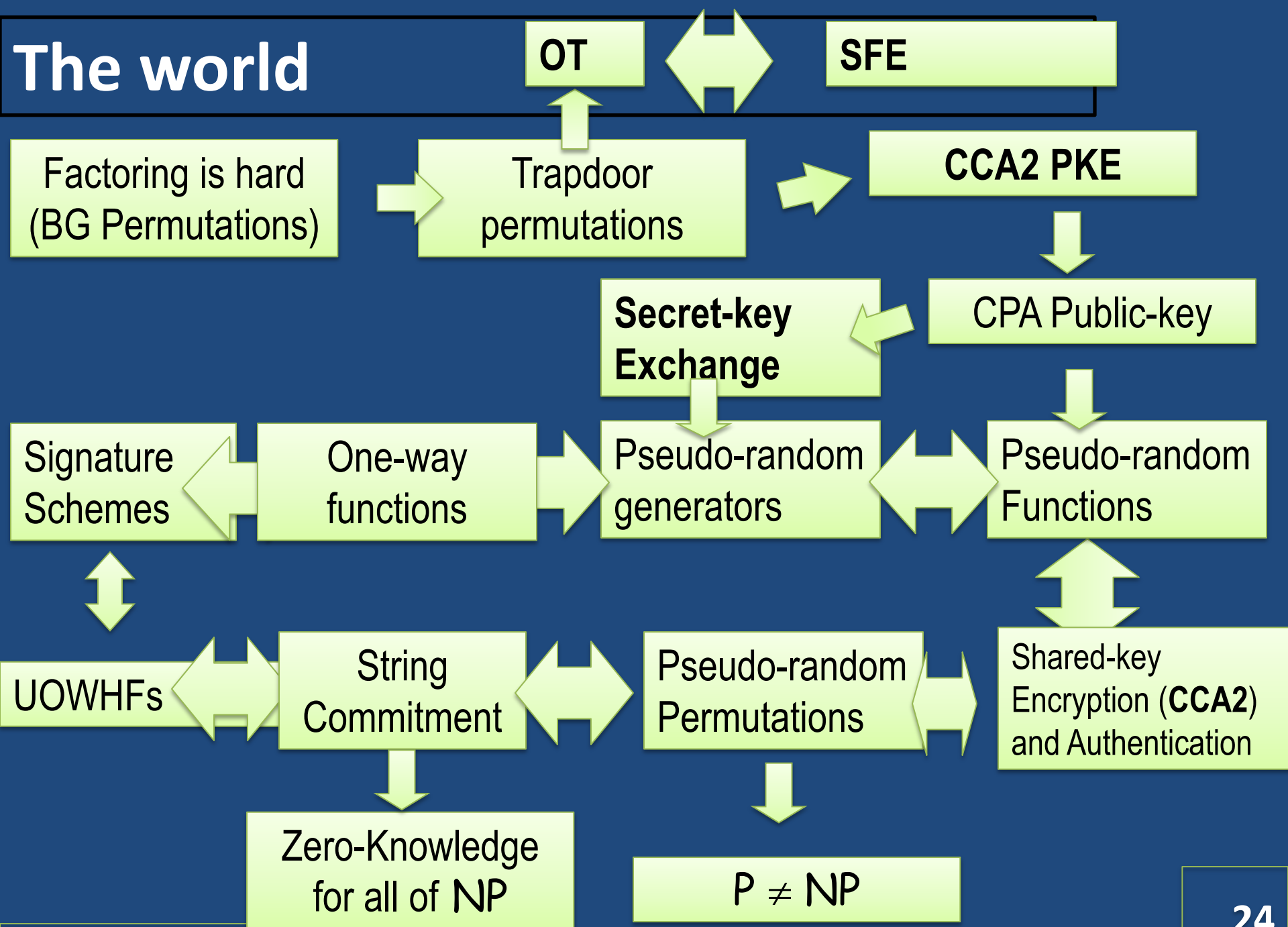
qui prouve que Alice connaît X et Bob n'a jamais eu connaissance de X

# Proof of Stake - PoS

Preuve d'enjeu ou comment sélectionner le valideurs:

- A partir des encours des participants (obligatoirement en possession de le devise)
- Parfois, pondération par la durée de possession des devises.
- Tirage au sort dans une loi uniforme
- Combinaison des deux pour identifier le 'gagnant'

# The world





# PRE-REQUIS DU BLOCKCHAIN

- 1976: **cyber block chaining**: DES
- 1977: RSA cryptographie asymétrique
- 1979: Merkle Tree pour la compression
- 1993: **Proof of Work** (PoW) – Cynthia Dwork et Mani Naor
- 1999: Horodatage sécurisé sans tiers de confiance
- 2000: P2P : **Peer To Peer** - Réseaux distribués : Napster et Gnutella

# Qu'est ce que la Blockchain ?

- Un **registre** où toutes les transactions, détenu et supervisé par tous les participants et contrôlées par aucun en particulier (non centralisé).
- Littéralement : une chaîne de blocs (de transactions).
- Un registre **séquentiel** de mouvements de valeurs. L'information de référence, contenue dans la blockchain, est copiée sur chacun des nœuds du réseau.
- La blockchain contient l'historique de l'ensemble des transactions réalisées depuis l'origine.

# BLOCKCHAIN

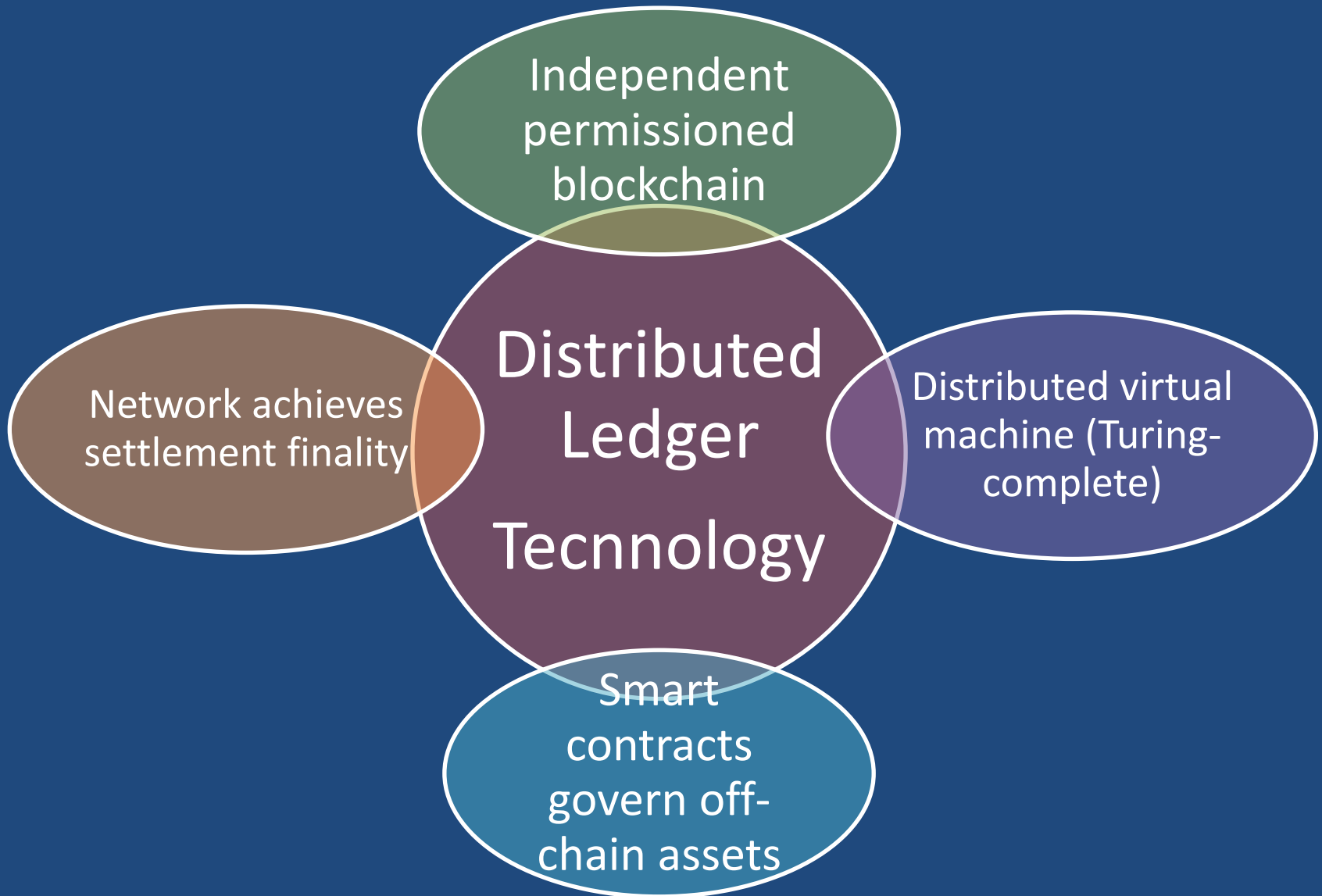
- La blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle.
- Une blockchain constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création.
- 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.



# BLOCKCHAIN

- Il existe des blockchains publiques, ouvertes à tous, et des blockchains privées, dont l'accès et l'utilisation sont limitées à un certain nombre d'acteurs.
- Une blockchain publique peut donc être assimilée à un grand livre comptable public, anonyme et infalsifiable.
- Comme l'écrit le mathématicien **Jean-Paul Delahaye**, il faut s'imaginer « un très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible. »

# Distributed Ledger Technology - DLT



# BLOCKCHAIN

- A **protocol** that supports a decentralized, pseudo-anonymous, peer-to-peer digital currency\*
- A **publicly** disclosed linked **ledger** of transactions stored in a blockchain
- A **reward** driven system for achieving **consensus** (mining) based on “Proofs of Work” for helping to secure the network
- A “scare token” economy with an eventual cap of about 21M bitcoins



- La première blockchain est apparue en 2008 avec la monnaie numérique bitcoin, développée par un inconnu se présentant sous le pseudonyme Satoshi Nakamoto. Elle en est l'architecture sous-jacente.
- Si blockchain et bitcoin ont été construits ensemble, aujourd'hui de nombreux acteurs (entreprises, gouvernements, etc) envisagent l'utilisation de la technologie blockchain pour d'autres cas que la monnaie numérique.



- Le bitcoin est une crypto-devise, sans organe centralisateur.
- La blockchain de bitcoin a été lancée le 3 Janvier 2009 par Satoshi Nakamoto.
- Le premier bloc est appelé bloc de genèse.
- La première transaction bitcoin enregistrée dans le premier bloc est une transaction unique de paiement de 50 nouveaux bitcoins à son créateur.





# Bitcoin: A Peer-to-Peer Electronic Cash System

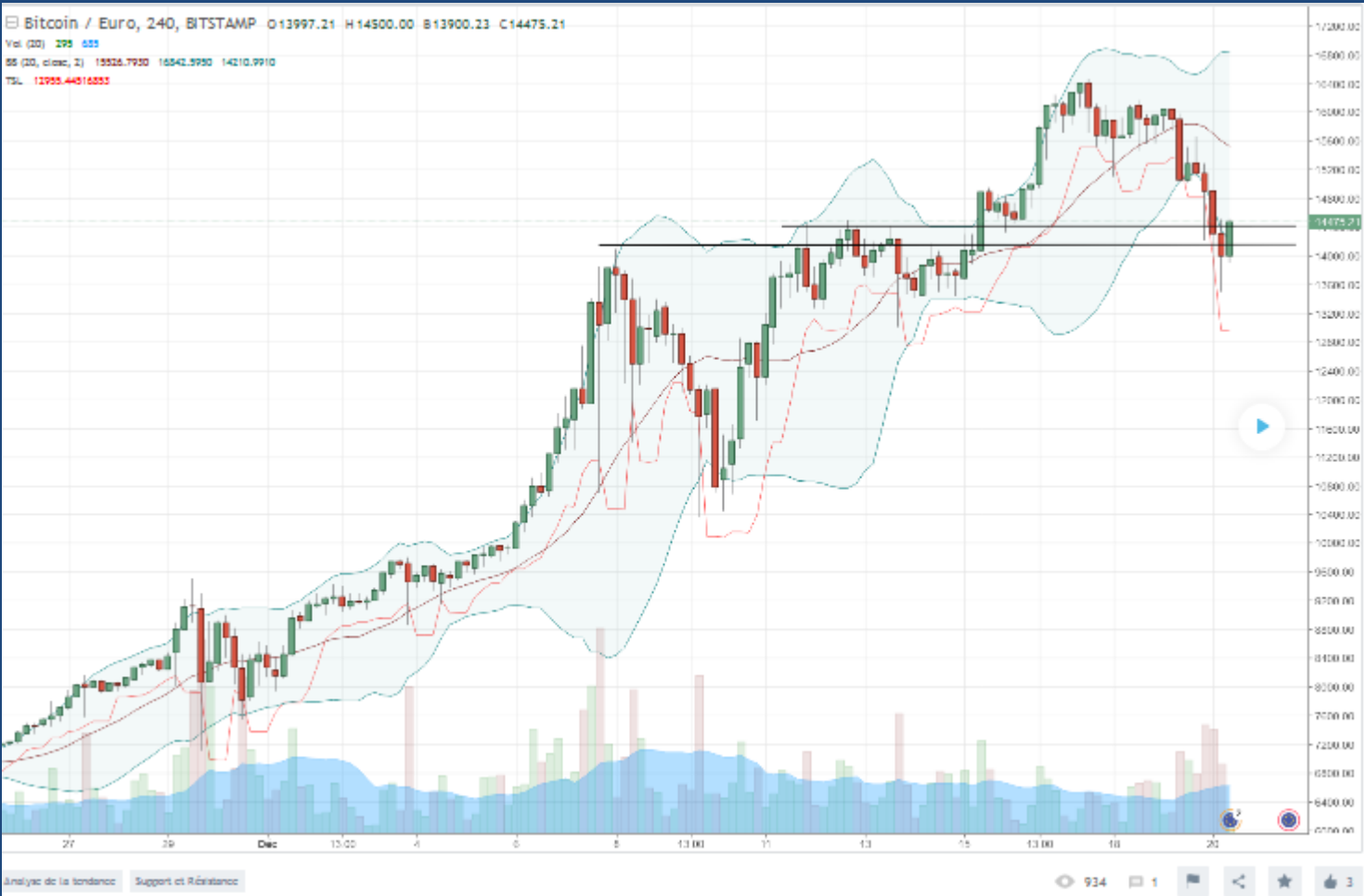
Satoshi Nakamoto  
satoshin@gmx.com  
[www.bitcoin.org](http://www.bitcoin.org)

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest



- 394.256 blocs
- Nombre de bitcoins en circulation : 15.106.400 BTC
- $(50 \times 210.000 + 25 \times (n - 210.000))$  – un block = 25 ou 50 BTC
- Capitalisation : 186 866 000 000 USD
- Taille du fichier blockchain du bitcoin : 100 Go
- 1 BTC = 1,275USD (6 mars 2017)
- 1 BTC = 9 996 EUR (18 janvier 2018)
- La taille de la blockchain est un problème à terme. A long terme les utilisateurs n'auront plus de client sauvegardant la blockchain. Les noeuds ayant une blockchain seront des super-noeuds gérés de manière décentralisés.

# BTC Graph



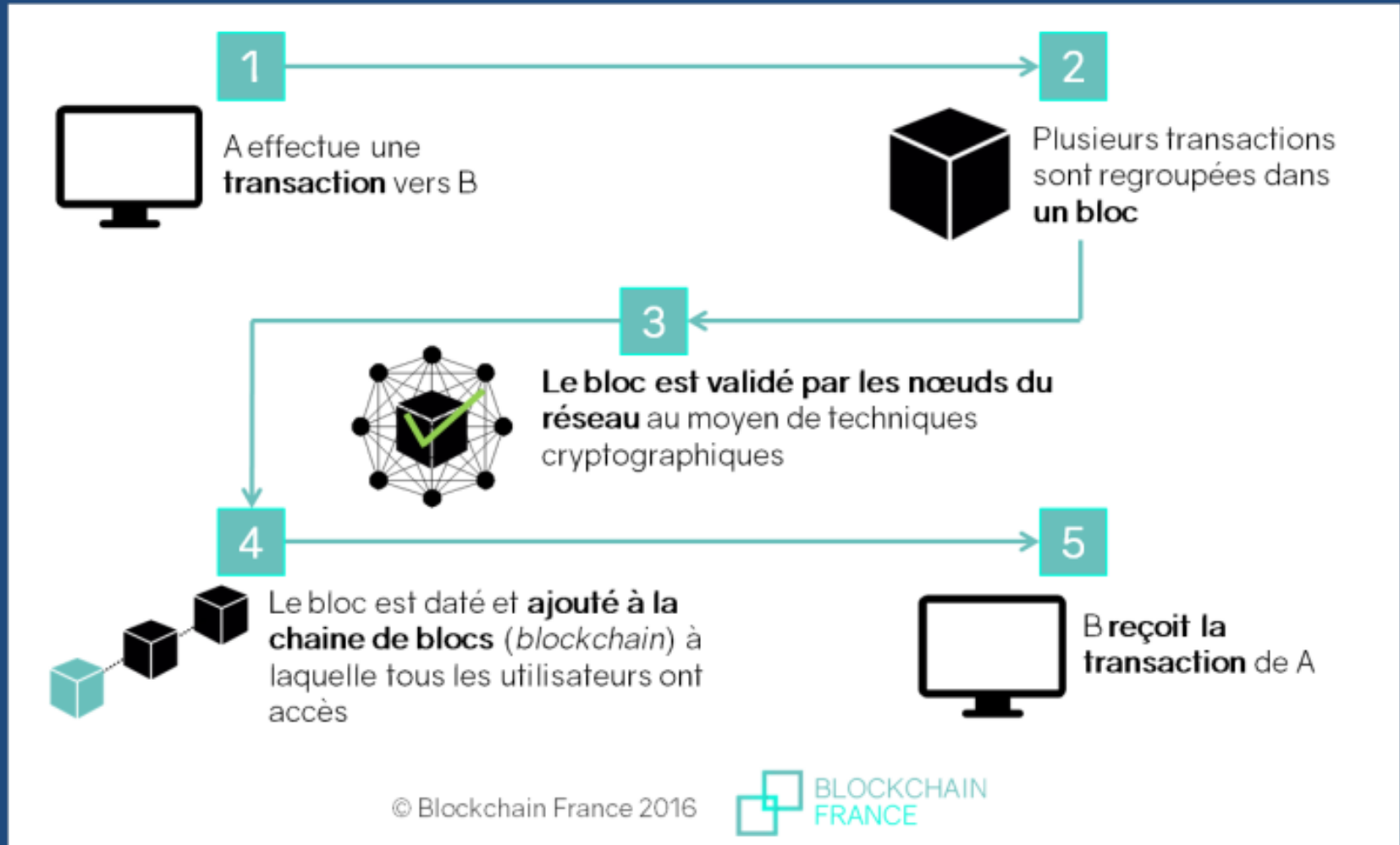


- N'importe qui peut se générer une adresse bitcoin et recevoir des bitcoins sur cette adresse.
- Sans procédure KYC particulière, le système est anonyme.
- Le fait de générer une adresse bitcoin par transaction permet de ne pas connaître le solde d'une personne en analysant la blockchain qui est publique.
- Il est possible d'analyser les transactions si l'on connaît les adresses bitcoins. Le fait que la blockchain soit publique conduit certains analystes à dire que bitcoin est un système qui permet de faire des contrôles très efficacement si le KYC est bien réalisé.

## Comment ça marche ?

- Les transactions effectuées entre les utilisateurs du réseau sont regroupées par blocs.
- Chaque bloc est validé par des acteurs appelés les “mineurs”.
- Dans la blockchain du bitcoin cette technique est appelée le “**Proof-of-Work**”, et consiste en la résolution de problèmes algorithmiques.
- Une fois le bloc validé, il est horodaté et ajouté à la chaîne de blocs. La transaction est alors visible pour le récepteur ainsi que l’ensemble du réseau.

# BLOCKCHAIN



Ce processus prend un certain temps selon la blockchain dont on parle (environ une dizaine de minutes pour bitcoin, 15 secondes pour Ethereum).

# LE MINAGE

- Le minage c'est le procédé par lequel les transactions Bitcoin sont sécurisées. A cette fin les mineurs effectuent avec leur matériel informatique des calculs mathématiques pour le réseau Bitcoin.
- Comme récompense pour leurs services, ils collectent les bitcoins nouvellement créés ainsi que les frais des transactions qu'ils confirment.
- Actuellement cette récompense est de **12,5 bitcoins par bloc**. Elle est divisée par deux tous les quatre ans environ.
- Les mineurs sont en concurrence et leurs revenus sont proportionnels à la puissance de calcul déployée.

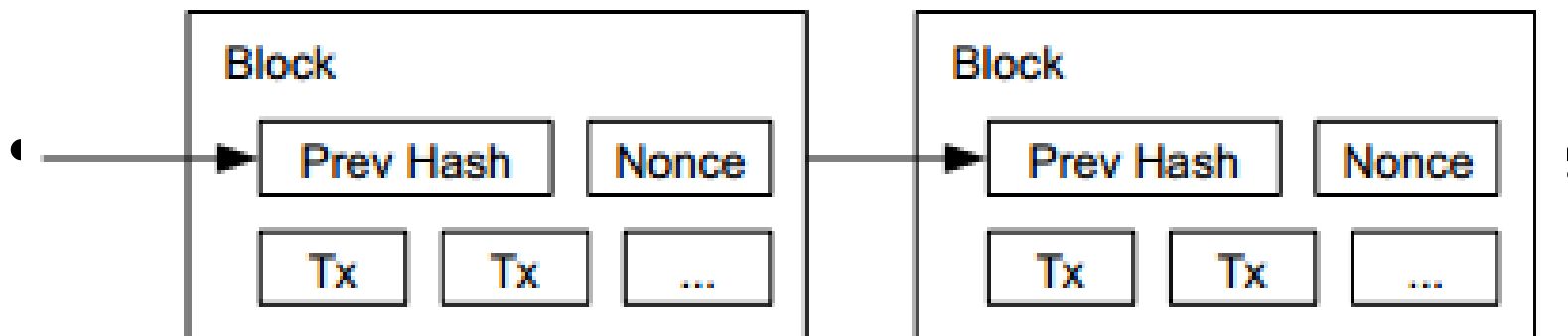
# LE MINAGE

- Le minage consiste à résoudre un problème mathématique aléatoire. Il faut trouver une valeur numérique: le NONCE, qui sera combiné aux transactions pour obtenir un résultat avec une fonction de Hash. Ce résultat devra satisfaire un niveau de difficulté: produire un maximum de zéro dans le résultat
- Bien entendu, la fonction de Hash étant irréversible, il n'est pas possible de trouver la solution en "inversant" / "résolvant" le problème.
- La difficulté du problème est ajustée régulièrement de façon à valider un block en 10 minutes.



# LE MINAGE

- Chaque transaction est enregistrée dans un bloc:
- Les blocs sont reliés par le Hash: SHA256
- L'ensemble est horodaté
- Les transactions sont SEQUENTIELLES
- Les mineurs sont tirés au hasard sur un pool



# HASHCASH

- Like many great ideas to become realized, it takes a confluence of other great ideas
- Based on the idea of HashCash, a Proof of Work concept invented by Adam Back in 1997 (<http://www.hashcash.org/papers/hashcash.pdf>)
- Originally proposed as an anti-spam throttling mechanism
- The core idea is that before accepting a transaction, the sender must first demonstrate a “cost” via a computationally “hard” problem that can simultaneously be easily verified.
- This generally referred to as a “**Proof of Work**”

# FONCTION HASH

Une **fonction de HASH** transforme une chaîne de caractère de longueur quelconque en une chaîne de longueur fixe.

- Une petite différence dans la chaîne génère de grandes différences dans le résultat
- Protocoles: MD5, SHA1, SHA256
- Ex: MD5 produit le résultat suivant sur les string 'abc' et 'abC'

abc

0bee89b07a248e27c83fc3d5951213c1

abC

2217c53a2f88ebadd9b3c1a79cde2638

“The Quick Brown Fox Jumped Over the Lazy Dog”

2dfd75162490ed3b4c893141f9ab37cf

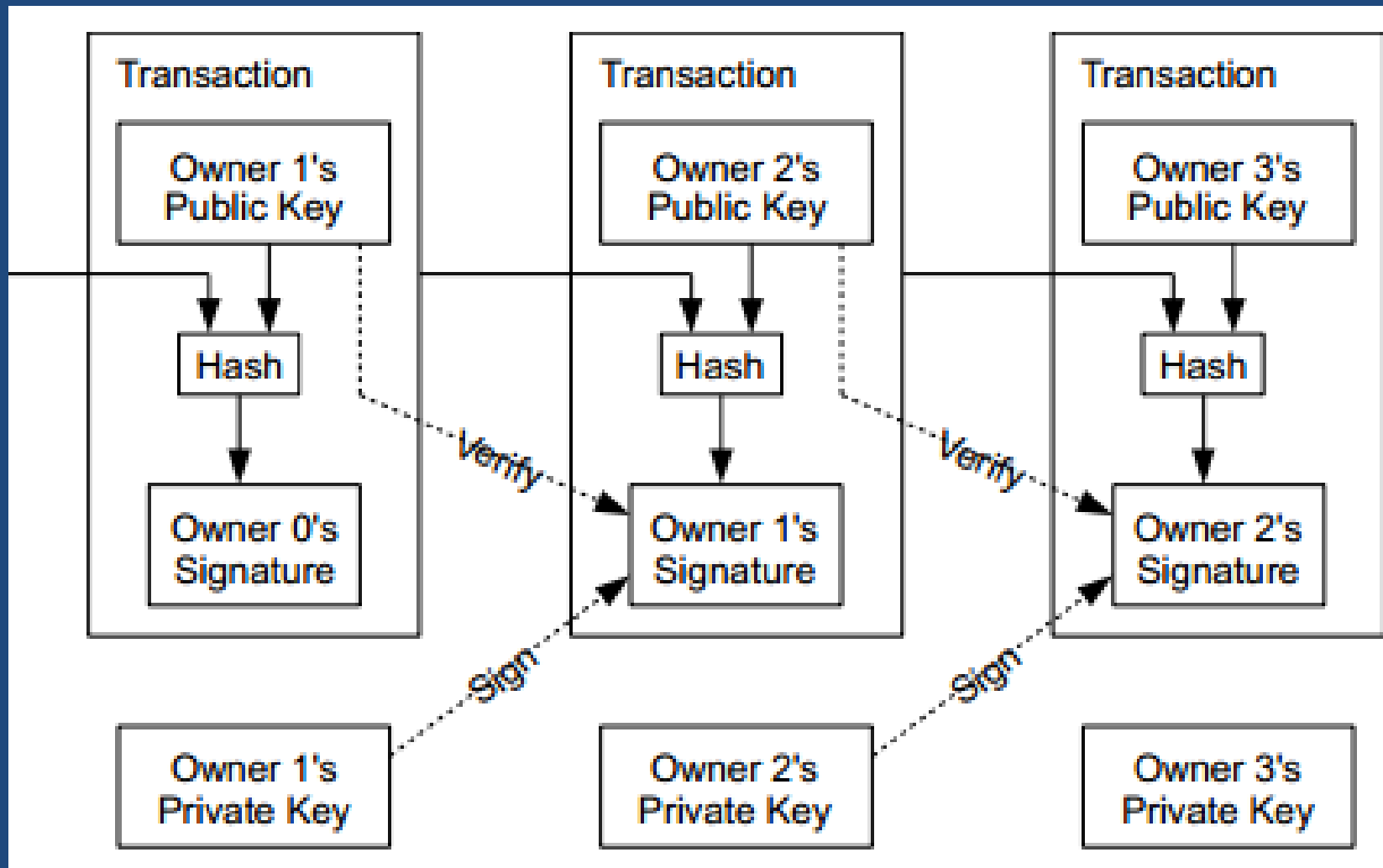
<https://blockchain.info/fr/blocks/1516292565121>

504847			00000000	
(Chaîne	2018-01-		00000000	
principale	18	SlushPool	004fb6d4	
)	15:35:39		098484d1	1,065.38
			2647cb45	
			91c0a166	
			26d6987c	
			8dcccccc5	

<https://blockchain.info/fr/blocks/1516292565121>

Date (timestamp)	2018-01-18 15:35:39
Date de réception	2018-01-18 15:35:39
Relayé par	SlushPool
Difficulté	2,227,847,638,503.63
Morceaux	394155916
Taille	1065.381 kB
Poids	3992.358 kWU
Version	0x20000000
nonce	660503917
Récompense du bloc	12.5 BTC

# FONCTION HASH



# LE MINAGE

- Une transaction acceptée provisoirement dans un bloc signale au réseau que la transaction est valide.
- Chaque nouveau bloc accepté dans la chaîne une fois la transaction validée est confirmé
- Il faut 6 confirmations pour valider définitivement un échange soit une heure si un bloc est validé toutes les 10 minutes
- On considère qu'il faut 120 confirmations pour une validation définitive.
- C'est pour assurer qu'un nœud avec 51% de la puissance de calcul ne puisse pas invalider une transaction

## Le potentiel de la blockchain

- Le caractère décentralisé de la blockchain, couplé avec sa sécurité et sa transparence, promet de nombreuses applications:
- 1-Les applications pour **le transfert d'actifs** : monnaie, titres, immobilier
- 2-Les applications de la blockchain en tant que **registre (ledger)** : elle assure ainsi une meilleure traçabilité: cadastre, ...
- 3-Les **smart contracts** et « **DAO** » **Distributed Autonomous Organization** : il s'agit de programmes autonomes qui exécutent automatiquement les conditions et termes d'un contrat, sans nécessiter d'intervention humaine une fois démarrés.



# SMART CONTRACT

- 1994 : Nick Szabo
- 2013 Vitalik Buterin

Entièrement informatisé et automatisé, il sera avant tout autonome et intelligent... et surtout, il pourrait modifier en profondeur la notion de confiance dans les relations commerciales.

# SMART CONTRACT

## Le potentiel des Smart Contracts

- Les smart contrats sont des programmes autonomes qui, une fois démarrés, exécutent automatiquement des conditions définies au préalable.
- Règles = Instruction conditionnelle de type « if – then »
- L'avantage de mettre en place des smart contracts dans une blockchain réside dans la garantie que les termes du contrat ne pourront pas être modifiés. Un smart contract qui ne serait pas dans la blockchain serait un programme dont les termes pourraient être changés en cours d'exécution.

SMART CONTRACT + OBJETS CONNECTES (IoT)  
(ORACLES = CAPTEURS)

# DAO : THE DIGITAL COMPANY

SLOCK.IT =BLOCKCHAIN +  
IoT (Internet Of Things)

IoT=smart device

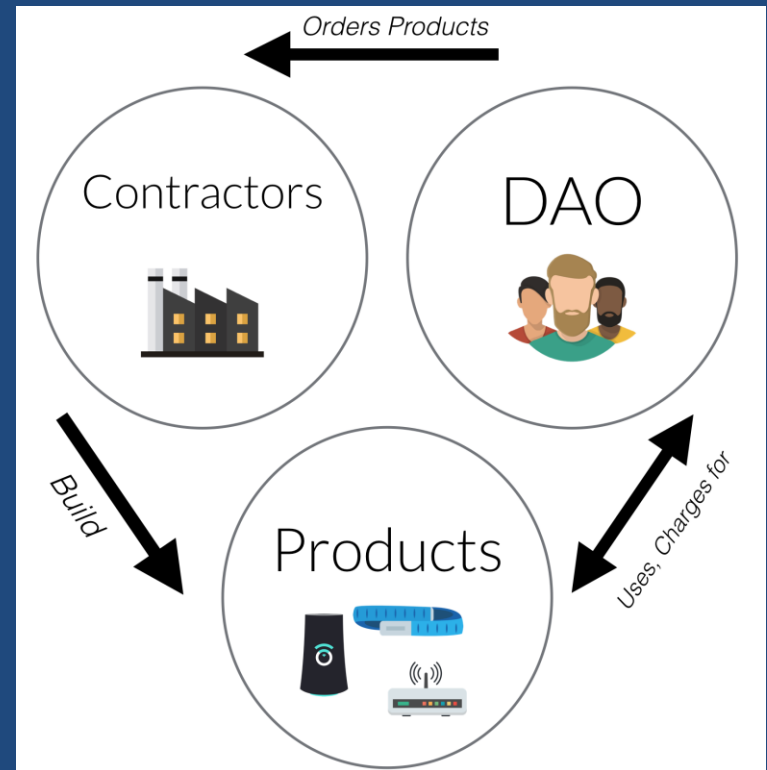
M2M:

RFID: radio frequency id

NFC:near field communication

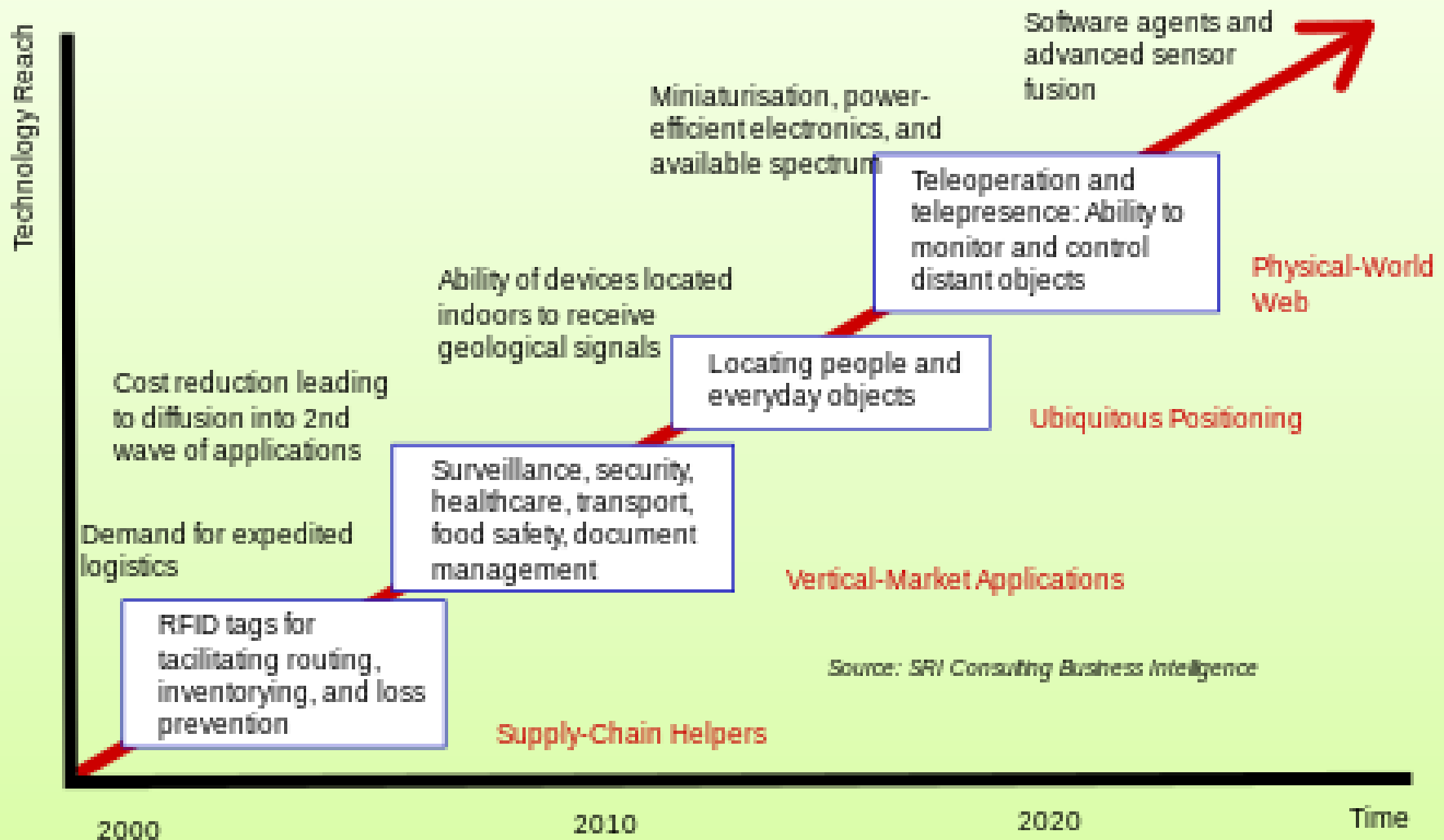
BLUETOOTH

Smart Grids, Smart Cities, Smart  
Homes, Smart Cars, Smart Humans



# INTERNET OF THINGS

## Technology roadmap: The Internet of Things



# EXTENSIONS

- Les champs d'exploitation sont nombreux : banques, assurance, immobilier, santé, énergie, transports, vote en ligne...
- De façon générale, des blockchains pourraient remplacer la plupart des « tiers de confiance » centralisés (métiers de banques, notaires, cadastre,...) par des systèmes informatiques distribués.
- Bien évidemment, ces promesses ne sont pas exemptes de défis et de limites, qu'elles soient économiques, juridiques, de gouvernance, ou encore écologiques.

# ETHEREUM

- Ethereum est une infrastructure logicielle de base pour le développement d'applications distribuées, décentralisées et utilisant les principes fondamentaux des cryptocurrencies, introduits par Bitcoin et repensés et améliorés par Ethereum.
- Ethereum peut être utilisé pour construire tout type d'applications.
- L'ETH est la monnaie créée par Ethereum pour récompenser les nœuds qui exécutent les scripts.
- En juillet 2014, Ethereum a levé l'équivalent de 18,4 millions de dollars en vendant sa propre monnaie, l'ETH contre des bitcoins.

# APPLICATIONS Ethereum

- Digital signatures that ensure authenticity and proof of existence of documents: the Luxembourg Stock Exchange has developed such a system
- Secure identity systems for the Internet: *uPort*
- Interactive grids for the Internet of Things (IoT), such as verification for physical assets utilizing Bluetooth low energy and near field communication chips. *Slock.It* is developing smart locks
- Digital tokens pegged to fiat currencies: *Decentralized Capital*. Spanish bank Santander is also involved in such a project

# APPLICATIONS Ethereum

- Digital tokens pegged to gold: *Digix*
- Improved digital rights management for music: Imogen Heap used the technology
- Platforms for prediction markets: *Augur (software), Gnosis*
- Social media platforms with economic incentives: *Backfeed, Akasha*
- Decentralized marketplaces for physical items, financial products or energy: *FreeMyVunk, Etheropt, TransActive Grid*
- Mobile payments services for foreign workers: *Everex*



## Platforms for crowdfunding



- Le concept de Smart Contracts passe au niveau d'une « entreprise » autonome.
- L'expérience d'Ethereum, appelée The DAO, s'est rapidement arrêtée après un bug, faisant perdre 50 millions de USD le 16 avril 2016! Mais ce n'est pas la fin....

# ETHEREUM *Turing complete contracts on a blockchain.*

- Contracts are the main building blocks of Ethereum.
- A contract is a computer program that lives inside the distributed Ethereum network and has its own ether balance, memory and code.
- Every time you send a transaction to a contract, it executes its code, which can store data, send transactions and interact with other contracts.
- Contracts are maintained by the network, without any central ownership or control.
- Contracts are written in languages instantly familiar to any programmer and powered by Ether, Ethereum's cryptofuel.

# Financial Industry Applications best suited for Blockchain

- Stack of Processes
  - Clearing Networks
  - International Transfers
  - Clearing and Settlement
  - auditing, reconciliation, reporting, settlement
  - Asset Ownership
- Financial Instruments
  - Payments – Cross Border, P2P, Corporate and Interbank
  - Private Equity
  - Bonds
  - Derivative commodities
  - Trading records
  - Spending records
  - Mortgage/Loan records
  - Microfinance
  - Servicing records

## CONTRAT DE DERIVE – FUTURE

- Contrat bilatéral entre un tiers et une chambre de compensation.
- Le contrat est soumis à de nombreuses contraintes:
- Appels de marge: 'initial margin' et 'maintenance margin'
- Appels de marge intra-day et arrêt du marché
- Valorisations et comptabilité: gestion de stock
- Livraison à terme: cash ou physical settlement
- Couverture et roll'over automatique
- Gestion des anomalies : le plus difficile – « auto repair »

DERIVES CLIMATIQUES : C°/F° capture, scandale EURIBOR

## EXTENSION 'BIOLOGIQUE'

- Définition d'un smartcontrat/smartlife
- Data model de structure: JSON (Java Script Object Notation)
- Règle de comportement: what if = ADN
- Collecteurs/capteurs d'informations = oracles
  
- Echanges temps réel d'information, actions et notifications.

# Projets et usages de la Blockchain

- ICO: Initial Coin Offering: token contre cryptomonnaies: Ledger 60 M
- Bitcoin cash: bifurcation (fork) le 1 aout 2017 faisant passer le block de 1 à 8 M
- Cadastre pays émergents
- Regroupements: hyperledger, R3, B3i, Enterprise Ethereum Alliance
- Bourses (contrats), banques, fonds
- Avancée législatives en 2016

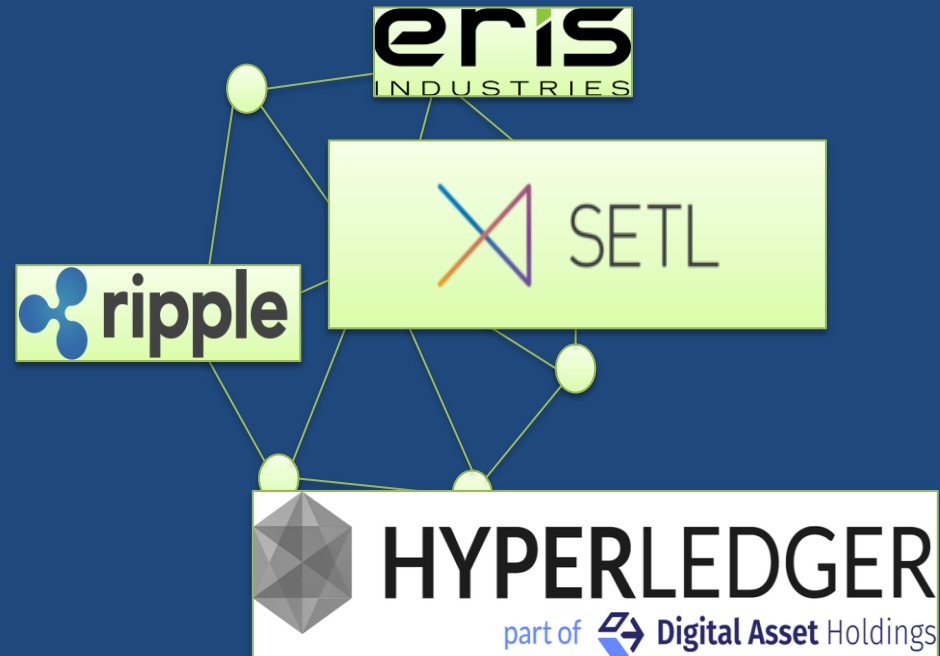
# INVESTMENTS in BLOCKCHAIN

- Blockchain has the potential to reduce infrastructure cost by up to \$20 billion a year.
- P2P money Transfer across international borders - segment worth \$500 B.
- Anderseen Horowitz ( VC firm) has invested over USD \$100 million into Blockchain technology
- All time Public/VC investment into Blockchain startups - \$894 million.
- Over 4000 active fintech startups in the NY arena and investment in the sector tripling last year to \$12 billion.

**Public Network Fabric**



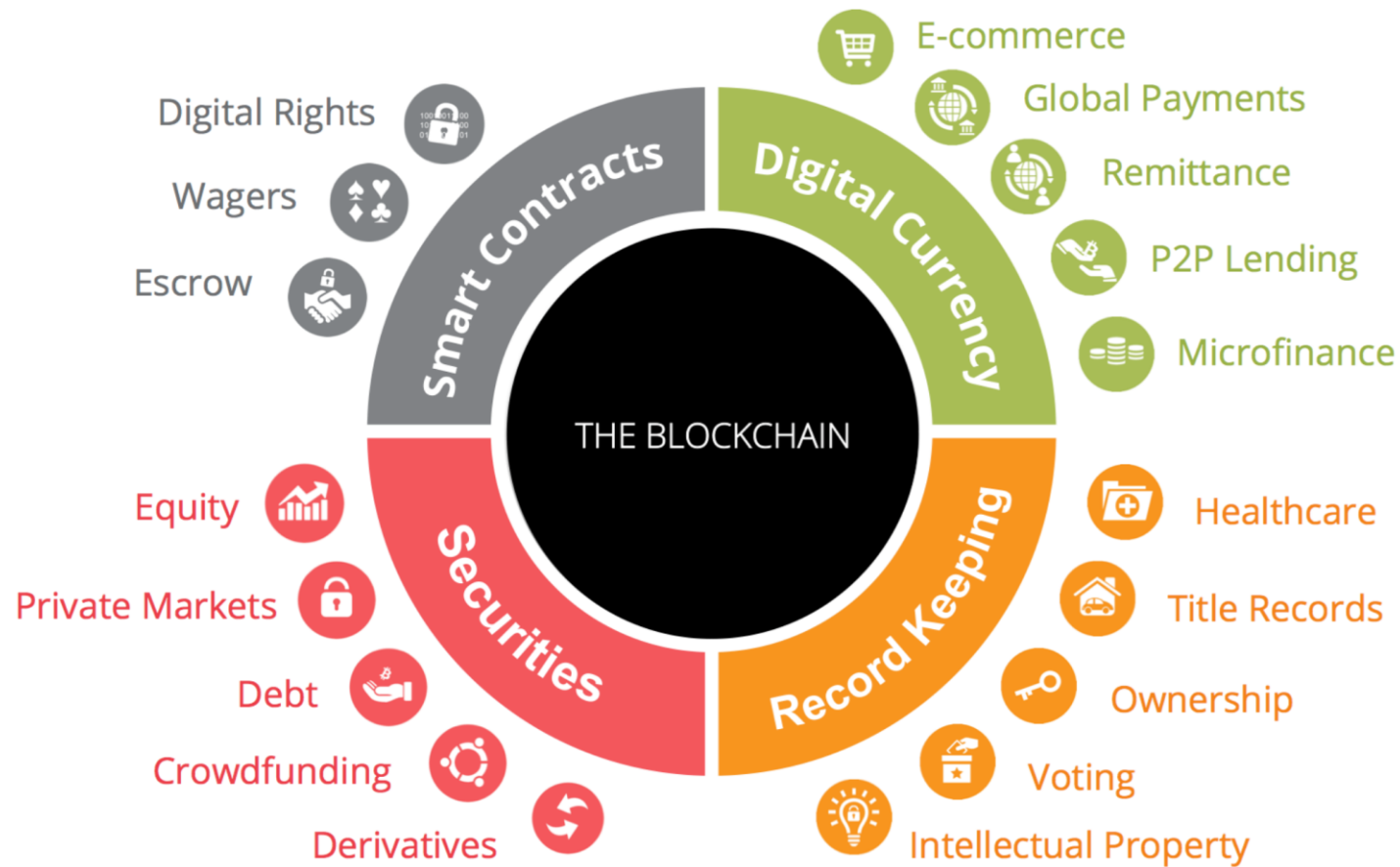
**Private Network Fabric**





# Blockchain Potential Applications & Disruption

The blockchain is radically changing the future of transaction based industries



MERCI DE VOTRE ATTENTION

QUESTIONS

PHILIPPE DUCHEMIN

phducheminfr@gmail.com