Blockchain

PRÉSENTATION

Institut des actuaires

pwc

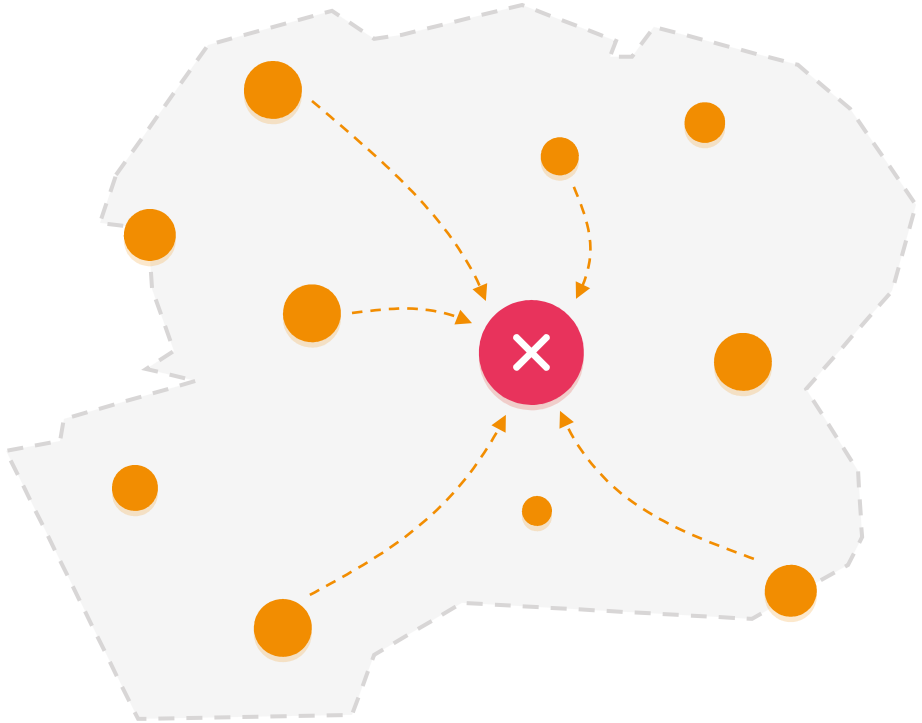
www.pwc.com

21 septembre 2016

*Le problème des **généraux byzantins***

Le problème des généraux byzantins consiste en 2 objectifs contradictoires. Vous jouez ici le rôle d'un dirigeant d'une cité Etat.

1

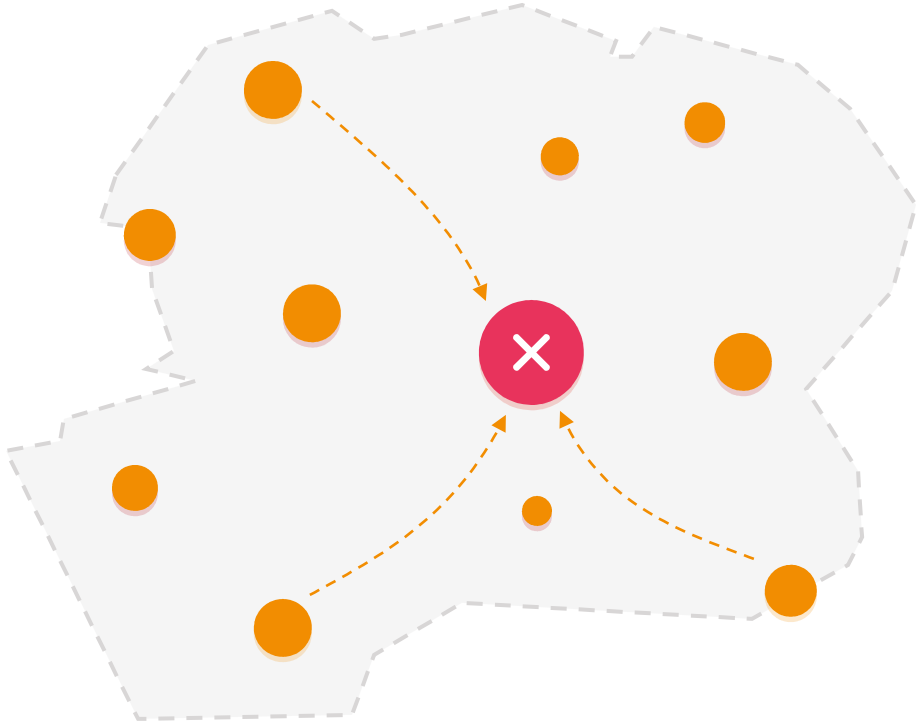


10 cités Etats pourraient empocher un immense butin en pillant une très grande ville, Byzance. Pour ce faire, elles doivent attaquer Byzance à **au moins 5**.

*Le problème des **généraux byzantins***

Le problème des généraux byzantins consiste en 2 objectifs contradictoires. Vous jouez ici le rôle d'un dirigeant d'une cité Etat.

2



Si elles attaquent à **moins de 5**, **elles sont vulnérables au pillage de leurs voisines**. Comment, avec éventuellement des traîtres parmi leurs émissaires, les dirigeants des cités peuvent-ils se coordonner efficacement?

*Le problème des **généraux byzantins***

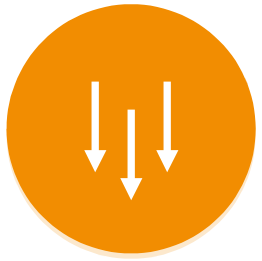
Le problème des généraux byzantins consiste en 2 objectifs contradictoires. Vous jouez ici le rôle d'un dirigeant d'une cité Etat.

On verra que ce **problème a de nombreuses applications**, notamment **l'exécution de contrat**.

*Le problème des **généraux byzantins***

Le problème des généraux byzantins consiste en 2 objectifs contradictoires. Vous jouez ici le rôle d'un dirigeant d'une cité Etat.

Nous verrons aussi que la solution est une blockchain publique telle que **Bitcoin** qui permet de :



Réduire le nombre d'intermédiaires, voire s'en abstenir

Pallier à l'asymétrie d'information

Principes d'une ***blockchain***

Une **blockchain** est **une chaîne de blocs**, outil de digitalisation d'informations élémentaires utiles aux échanges.

Principes d'une ***blockchain***

Il y en a aujourd'hui **plus de 600**.
Certaines sont publiques, d'autres non.

Principes d'une ***blockchain***

Ce qui les caractérise c'est :

qui peut et comment
ajouter un nouveau bloc

le contenu éventuel
de chaque bloc

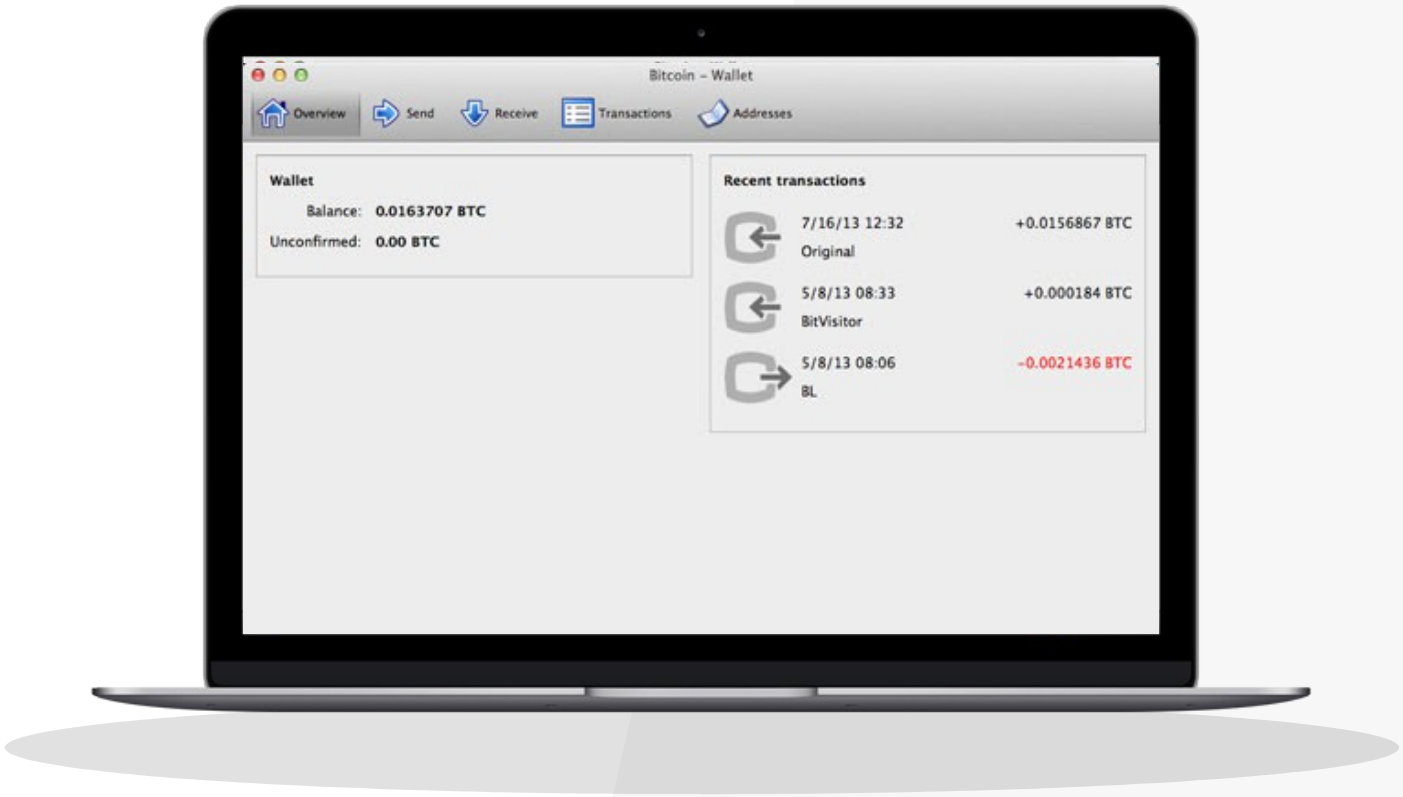
Principes d'une ***blockchain***

2 blockchains publiques seront présentées :
Bitcoin et **Nxt**. Nous parlerons aussi d'**Ethereum.**

1

TRUSTED **LEDGER**

*Ecosystème de la **blockchain Bitcoin***



Bitcoin en chiffres :

10 milliards de dollars de capitalisation

100 millions de dollars de volume quotidien

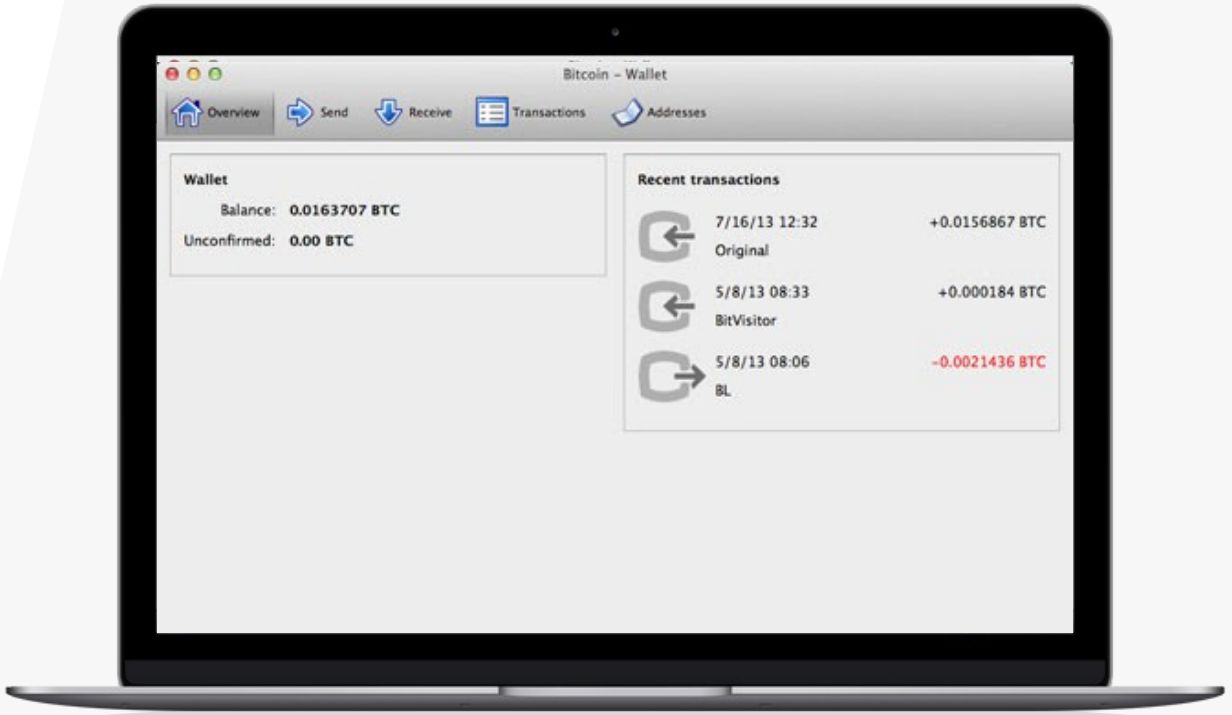
5 millions d'utilisateurs

3 transactions par seconde

*Ecosystème de la **blockchain bitcoin***

Plusieurs acteurs assurent la pérennité de son écosystème :

1. Les mineurs ajoutent les nouveaux blocs.
2. Les nœuds du réseau assurent l'intégrité de la blockchain.
3. Les développeurs proposent des mises à jour et de nouvelles fonctionnalités.
4. Les utilisateurs effectuent des transactions.



Bitcoin en chiffres :

10 milliards de dollars de capitalisation

100 millions de dollars de volume quotidien

5 millions d'utilisateurs

3 transactions par seconde

La première blockchain : ***Bitcoin (janvier 2009)***

La blockchain Bitcoin se perpétue par le minage.

La première blockchain : ***Bitcoin (janvier 2009)***

Chaque bloc créé initie un nouveau problème de calcul qui donne le droit au premier qui le résout :

d'ajouter un nouveau bloc
à la chaîne

de recevoir une récompense
de bitcoins (BTC)
nouvellement crées

La première blockchain : ***Bitcoin (janvier 2009)***

La difficulté du problème est réajustée de façon à ce qu'un bloc soit créé toutes les 10 minutes en moyenne.

Ces calculs sécurisent la blockchain.

La première blockchain : ***Bitcoin (janvier 2009)***

12,5 BTC

La récompense est divisée par 2 tous les 210 000 blocs (soit environ 4 ans) : au début 50 BTC, puis 25, désormais **12,5**.

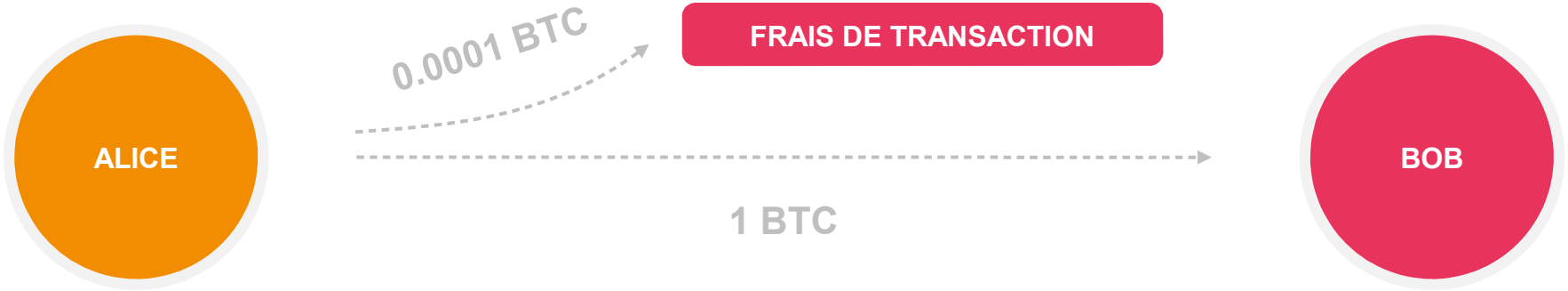
21 MILLIONS

La création de BTC est donc permanente mais un seuil ne sera jamais atteint : **21 millions** de BTC.

16 MILLIONS

Aujourd'hui, près de **16 millions** de BTC ont été émis.

*Une **transaction de BTC***



Chacun peut se créer une adresse Bitcoin avec clé privée/clé publique.
Cela correspond à un identifiant visible par tous et un mot de passe à protéger.

Une adresse créée permet de recevoir et d'envoyer des BTC.
Il n'y a pas de découvert : on ne peut envoyer plus de BTC qu'il n'y en a en stock à l'adresse utilisée.

Le Mempool

Une fois qu'Alice a tapé son mot de passe, l'adresse de Bob, le montant qu'elle veut envoyer à Bob et les frais de transactions qu'elle choisit de payer, la transaction est enregistrée dans le mempool.

C'est l'ensemble des transactions en attente de confirmations.

Les confirmations ***des transactions***

Chaque mineur qui parvient à ajouter un nouveau bloc à la blockchain choisit les transactions enregistrées dans le mempool pour les inclure dans son bloc.

Les confirmations ***des transactions***

Le mineur reçoit sur l'adresse Bitcoin de son choix :

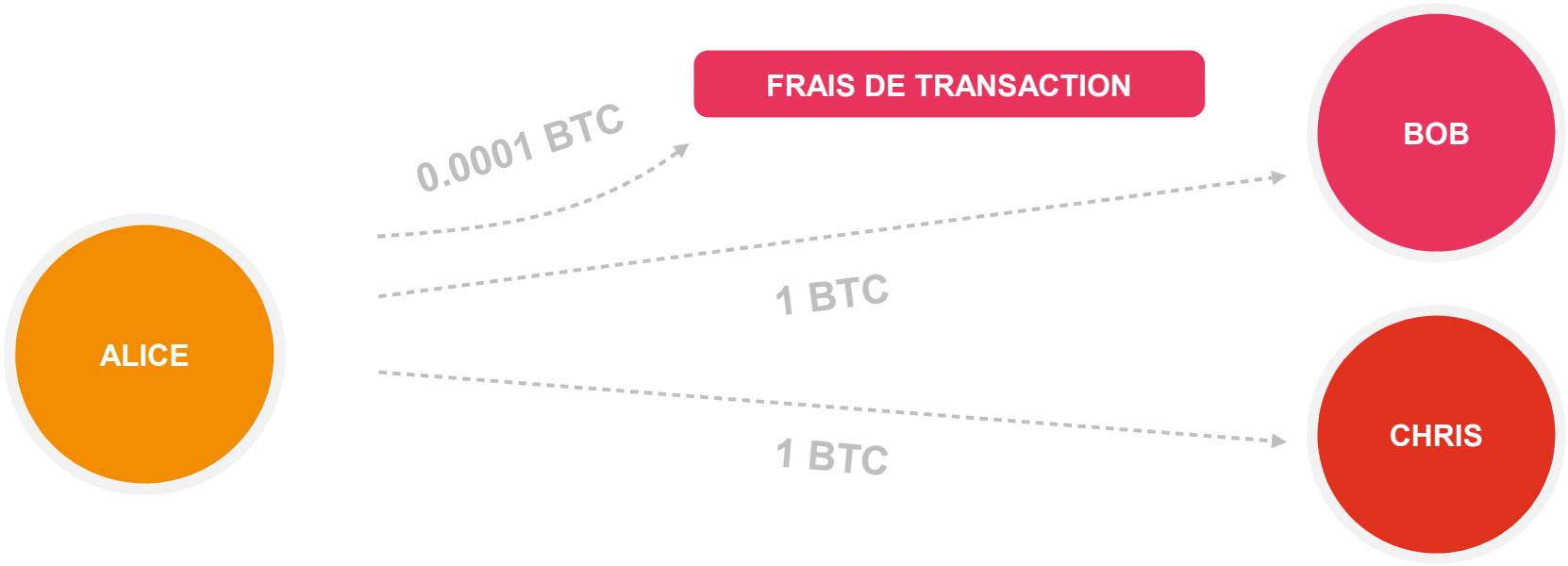
- ***La récompense** correspondante à son bloc*
- ***Les frais** des transactions du mempool qu'il ajoute dans son bloc*

Ces transactions choisies par le mineur ont alors 1 confirmation.

Les confirmations ***des transactions***

En pratique, choisir un frais de transaction élevé assure que la transaction sera ajoutée rapidement dans la blockchain.

*Les confirmations **des transactions***

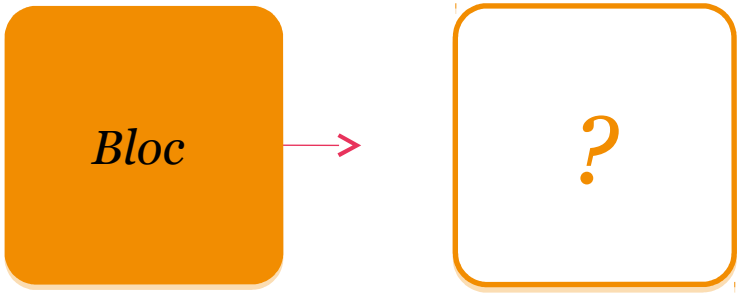


PAS DE DOUBLE SPEND:

Si Alice n'a que 1.0001 BTC sur son compte, elle peut faire 2 transactions non confirmées de 1 BTC avec 0.0001 BTC de frais, à Bob et à Chris. Mais au moins une des 2 transactions ne sera jamais confirmée.

Résolution des ***conflits***

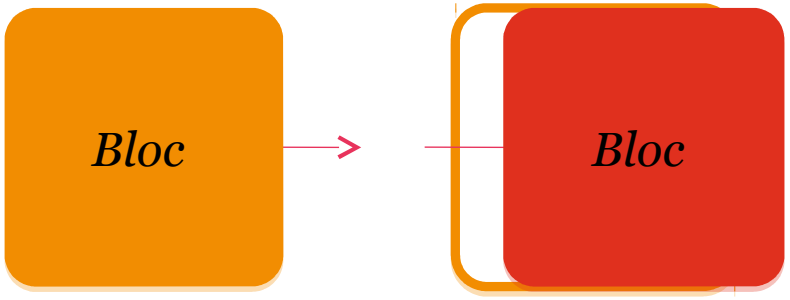
Les mineurs tendent à vouloir s'assurer la valeur de leur récompense



Ce qui le décidera, c'est si les autres mineurs vont chercher à **ajouter un bloc à « leur » nouveau bloc**… ***ou pas.***

Résolution des ***conflits***

Les mineurs tendent à vouloir s'assurer la valeur de leur récompense



Il est donc **très risqué** pour un mineur de proposer un bloc en conflit avec les règles admises par les autres mineurs.

*Résolutions des **conflits***

Les mineurs tendent à vouloir s'assurer la valeur de leur récompense

En pratique, **3 règles** (parmi beaucoup d'autres) sont respectées depuis 7 ans :

1. Pas de double spend
2. Pas de découvert
3. Les récompenses des mineurs sont bien celles convenues

*Trusted **ledger***

Chaque nouveau bloc ajoute une confirmation aux transactions inclues dans les blocs précédents.

Après 2 ou 3 confirmations, la probabilité que la transaction ne soit finalement pas inclue dans la blockchain Bitcoin est quasi nulle.

*Trusted **ledger***

C'est pourquoi on parle de livre de compte sécurisé (trusted ledger).

De plus, il n'est pas possible :

- *D'imposer une transaction sans le mot de passe correspondant*
- *De modifier les accomptes sans transaction explicite*

*Trusted **ledger***

On parle de réseau sans tiers, trustless, permissionless.

On parle également de livre de compte distribué (distributed ledger).

*Trusted **ledger***

APPLICATION : WIKILEAKS

Se finance par la blockchain Bitcoin depuis 5 ans.

*Une transaction **BTC en pratique***

ADRESSE D'ENVOI

12PLDZZ2dsDpsV22Qrak
NU97jwogMSeRjw

0.1 BTC, frais dynamiques

ADRESSE DE RECEPTION

1M9zRA3h6GXGFd3LiGw5DJ9D
LGenAs5MqX

UN AUDIT D'UN NOUVEAU GENRE : PROOF OF RESERVE

Effectuer une transaction BTC permet de certifier l'accès à la clé privée de l'adresse émettrice et donc l'accès aux BTC sur cette adresse.

*Une transaction **BTC en pratique***

ADRESSE D'ENVOI

12PLDZZ2dsDpsV22Qrak
NU97jwogMSeRjw

0.1 BTC, frais dynamiques

ADRESSE DE RECEPTION

1M9zRA3h6GXGFd3LiGw5DJ9D
LGenAs5MqX

PROOF OF RESERVE

Effectuer une transaction BTC permet de certifier l'accès à la clé privée de l'adresse émettrice et donc l'accès aux BTC sur cette adresse.

DE NOUVELLES POSSIBILITÉS :

Remarque : un compte peut consister en plusieurs adresses.

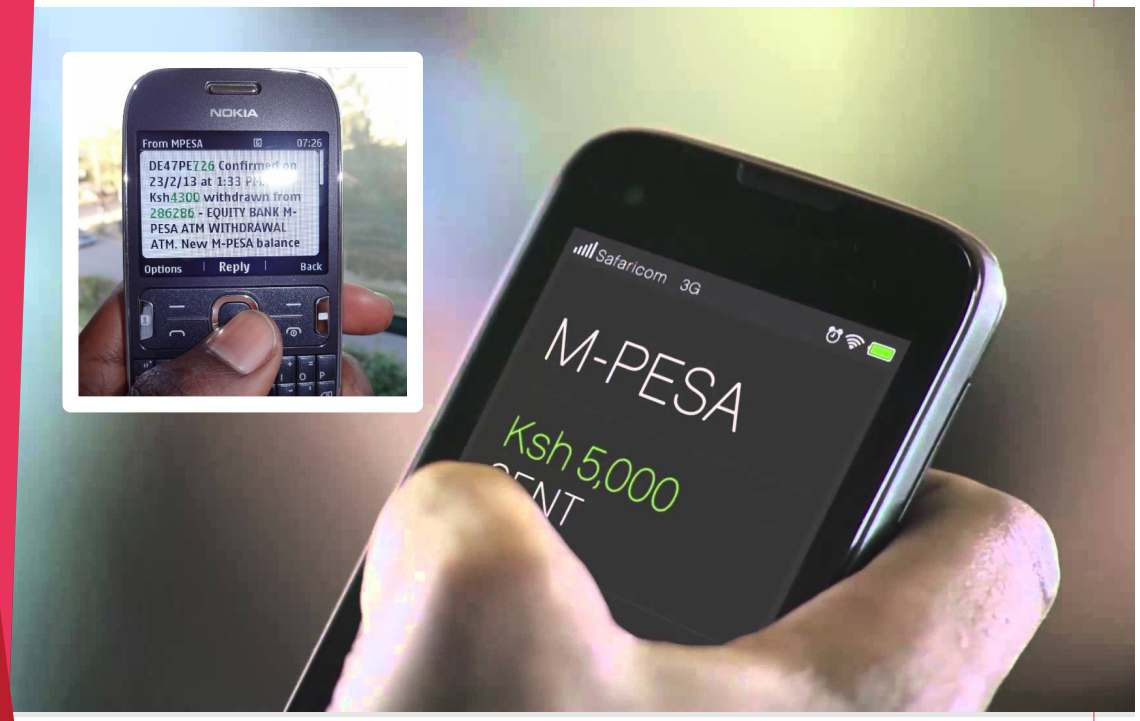
Une transaction de 25 millions de dollars a été effectuée un dimanche après-midi en quelques minutes pour quelques centimes de frais.

Possibilité de transmettre des BTC sans notaire.

Baisse des coûts du crowdfunding

Cependant, l'humain reste la clé pour la gestion de nouveaux risques qui émergent.

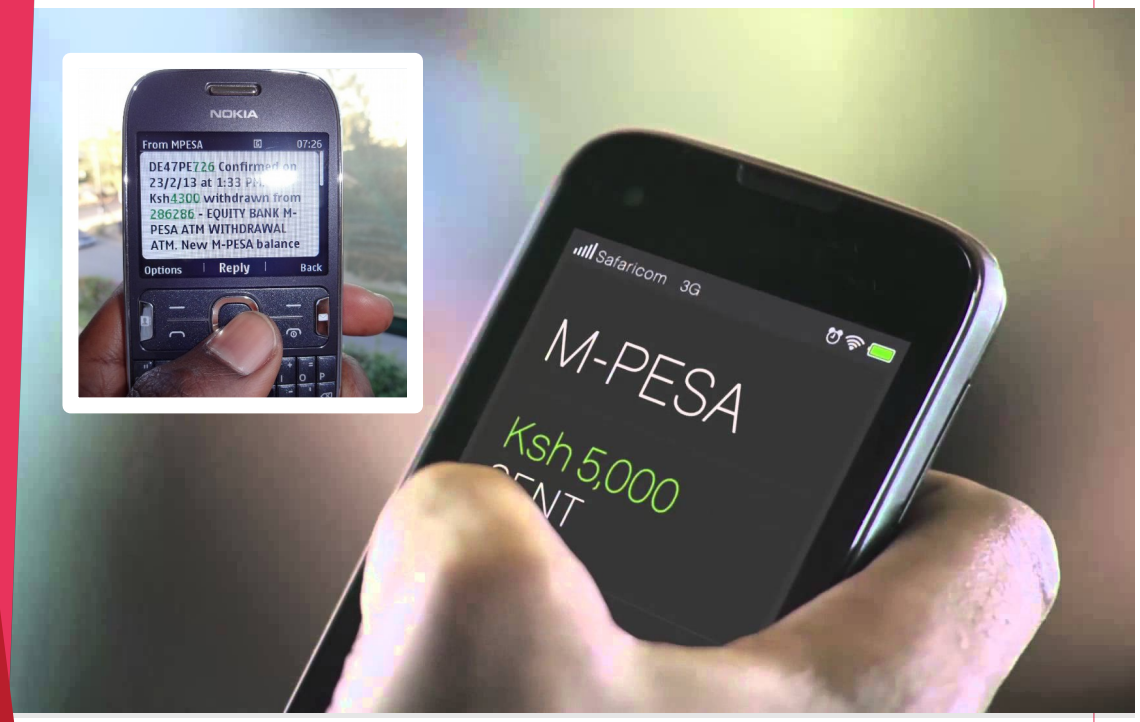
*Des virements **moins coûteux***



M-PESA

M-Pesa (M pour mobile et ***pesa***, argent en swahili) est un système de micro-financement et de transfert d'argent par téléphone mobile, lancé en 2007.

*Des virements **moins coûteux***

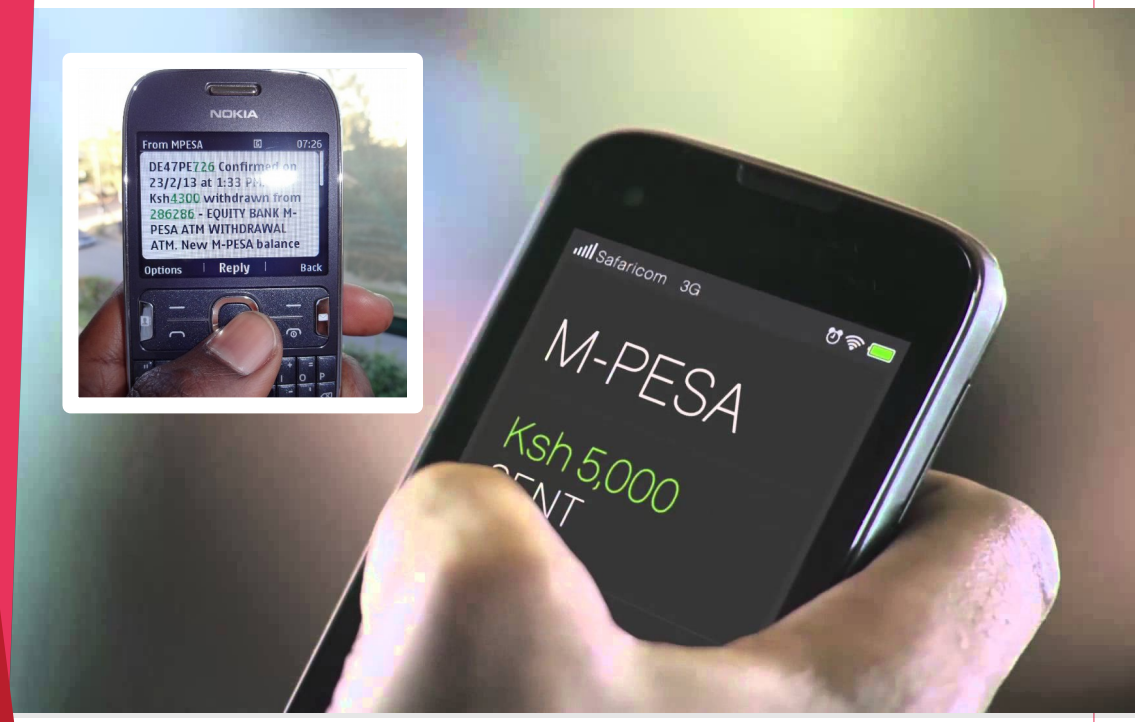


M-PESA

M-Pesa fut d'abord lancé par l'opérateur mobile kényan Safaricom en mars 2007. M-Pesa capta rapidement une part significative du marché des transferts d'argent et crût jusqu'à obtenir, en décembre 2011, ***17 millions de clients pour le seul Kenya***.

Wikipedia, M-pesa

*Des virements **moins coûteux***



M-Pesa par Bitcoin : Bitpesa

Les blockchains permettent l'accès

à des services bancaires et assurantiels

à des clients n'ayant pas aujourd'hui de compte en banque.

Un autre enjeu est **la baisse des coûts de compliance (KYC/AML)** par des blockchains.

Plusieurs concepts émergents découlant les uns des autres…

comme internet

INTERNET

Mail s

Premier mail
1971

Sites internet

Wold Wide Web
1993

Assurance en ligne

Année
2000

BLOCKCHAIN

Smart contracts

Ethereum
Juillet 2015

Tokenized assets

Nxt
Novembre 2013

Trusted ledger

Bitcoin
Janvier 2009

2

TOKENIZED **ASSETS**

*La première **Blockchain 2ème génération : NXT***

Nxt est la première cryptomonnaie dite **Proof of Stake** (PoS), par opposition aux cryptomonnaies basées sur le minage dites **Proof of Work** (PoW).

*La première **Blockchain 2ème génération : NXT***

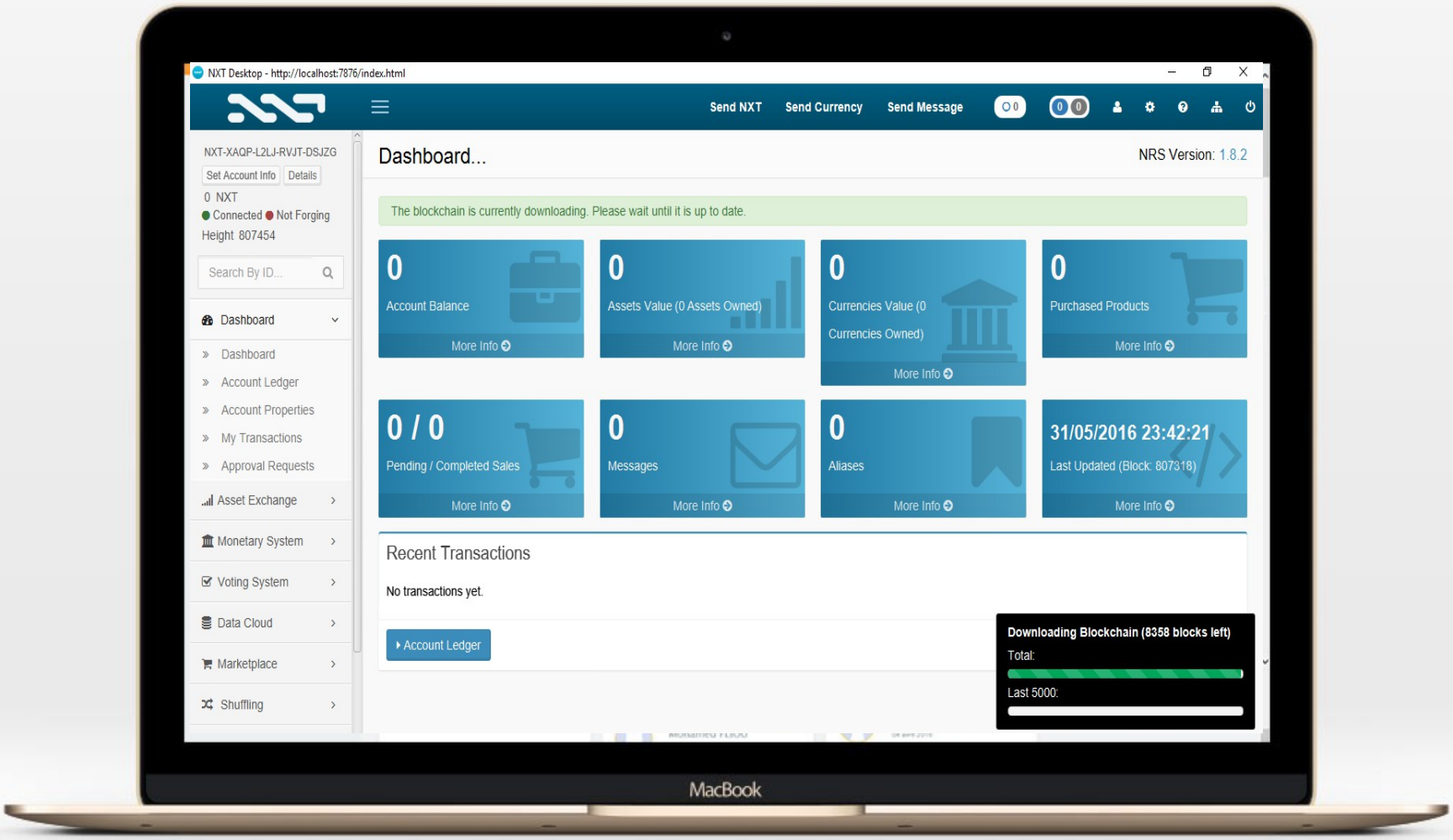
Ici le calcul nécessaire pour ajouter un nouveau bloc est **simple**.

Celui qui ajoute un nouveau bloc est **tiré au sort** au prorata du nombre de Nxt qu'il détient sur son compte et ne touche pas de récompense.

*La première **Blockchain 2ème génération : NXT***

On parle de **forgeage**,

par opposition au minage.


NXT Desktop - http://localhost:7876/index.html
Send NXT
Send Currency
Send Message
NXT-XAQP-L2LJ-RVJT-DSJZG
Set Account Info
Details
0 NXT
Connected
Not Forging
Height 807454
Search By ID...
Dashboard
Dashboard
Account Ledger
Account Properties
My Transactions
Approval Requests
Asset Exchange
Monetary System
Voting System
Data Cloud
Marketplace
Shuffling
Dashboard...
NRS Version: 1.8.2
The blockchain is currently downloading. Please wait until it is up to date.
0
Account Balance
More Info
0
Assets Value (0 Assets Owned)
More Info
0
Currencies Value (0
Currencies Owned)
More Info
0
Purchased Products
More Info
0 / 0
Pending / Completed Sales
More Info
0
Messages
More Info
0
Aliases
More Info
31/05/2016 23:42:21
Last Updated (Block: 807318)
More Info
Recent Transactions
No transactions yet.
Account Ledger
Downloading Blockchain (8358 blocks left)
Total:
Last 5000:
MacBook

*De nombreuses **innovations***

ASSET EXCHANGE

MONETARY SYSTEM

(interaction entre blockchains, surtout BTC/Nxt)

VOTING SYSTEM

DATA CLOUD

MESSAGES

SHUFFLING

(anonymisation)

*Asset **exchange***

L'asset exchange de Nxt, décentralisé, permet « d'insérer » un fichier à un échange de Nxt. Il permet donc l'échange de :

Musique, films, jeux vidéos, photos, e-books,…

Emission et échange d'actions

On parle de tokenized assets.

Voting ***system***

Par blockchains (déjà réalisé par Bitcoin et Nxt), il est possible de faire une élection où :

Le résultat est donné à une heure fixée.	Le vote se fait par téléphone, Internet...	Chacun peut s'assurer que son vote a correctement été pris en compte.	Eventuellement, chacun peut s'assurer de la liste des votants comptabilisés.

L'aspect trusted ledger et les possibilités de Proof of Reserve d'une blockchain permettent une élection facilement auditable pour des coûts faibles.

*Adresses **M of N***

Une adresse M of N est constituée de N clés, et l'accès des fonds correspondants est débloqué avec seulement M de ces N clés. Les adresse M of N commencent par 3 sur Bitcoin.

Pour qu'une transaction s'effectue il faut :

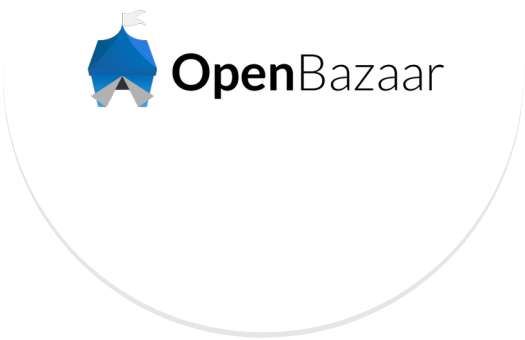
1. L'apparition dans la blockchain d'une transaction vers une autre adresse avec l'activation d'une clé

2. Que la même transaction apparaisse dans la blockchain avec l'activation d'au moins 2 autres clés

EXEMPLE : UNE ADRESSE 3 SUR 5

*Une adresse 5 of 10 est **la solution** du problème des généraux byzantins évoqué précédemment.*

OPENBAZAAR

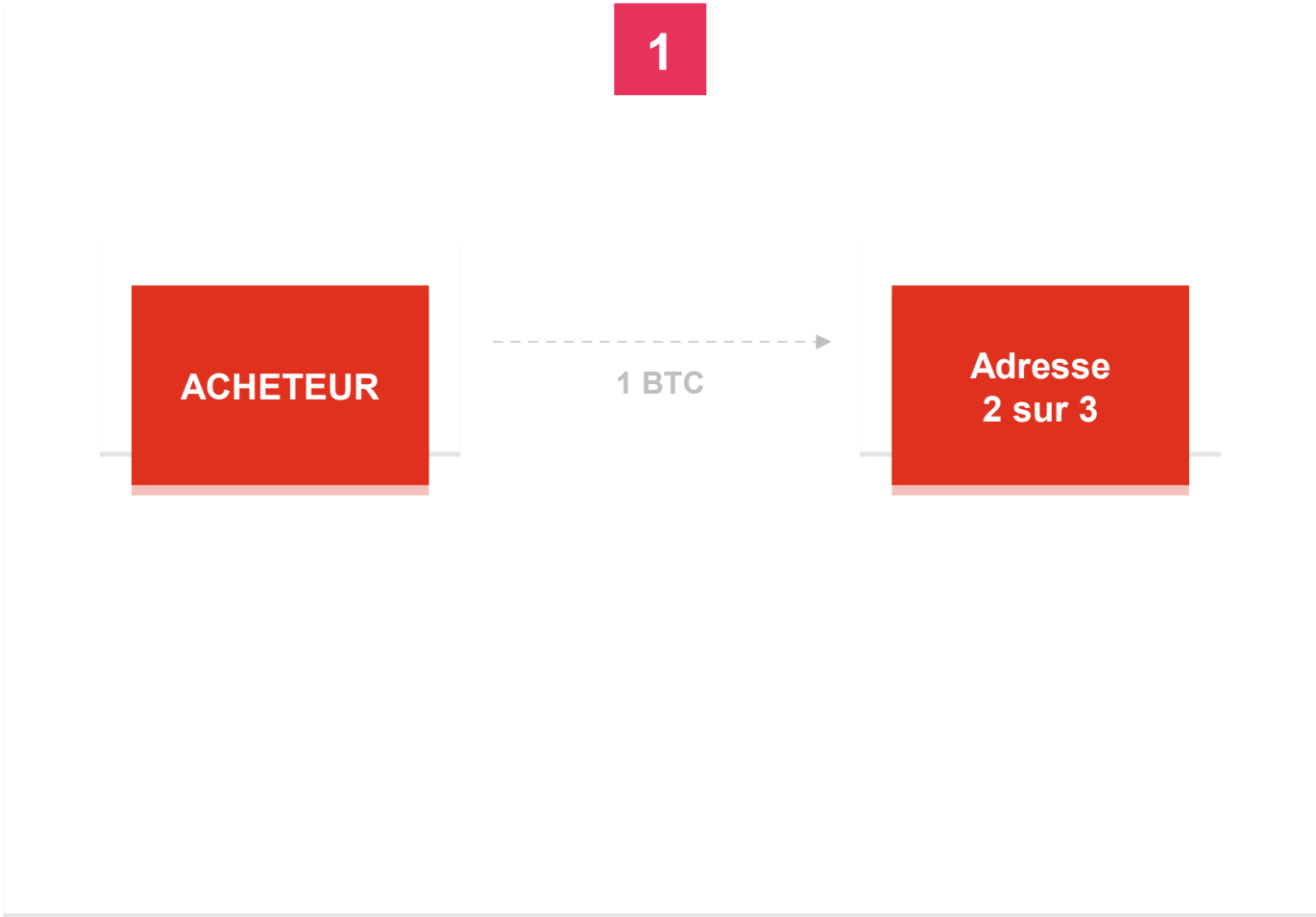


OpenBazaar est un site équivalent à eBay, mais sans intermédiaire. L'acheteur et le vendeur peuvent s'ils le souhaitent se mettre d'accord sur un tiers qui garantit la transaction en 2 of 3.

L'acheteur envoie l'argent demandé sur une adresse 2 of 3 dont **les 3 détenteurs d'une clé sont l'acheteur, le vendeur et le tiers choisi.**

OPENBAZAAR

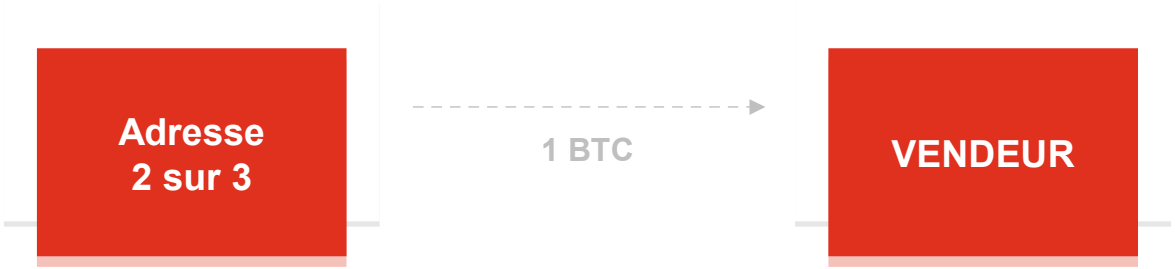
L'acheteur envoie l'argent demandé sur une adresse 2 of 3 dont les 3 détenteurs d'une clé sont l'acheteur, le vendeur et le tiers choisi.



OPENBAZAAR

L'acheteur envoie l'argent demandé sur une adresse 2 of 3 dont les 3 détenteurs d'une clé sont l'acheteur, le vendeur et le tiers choisi.

2

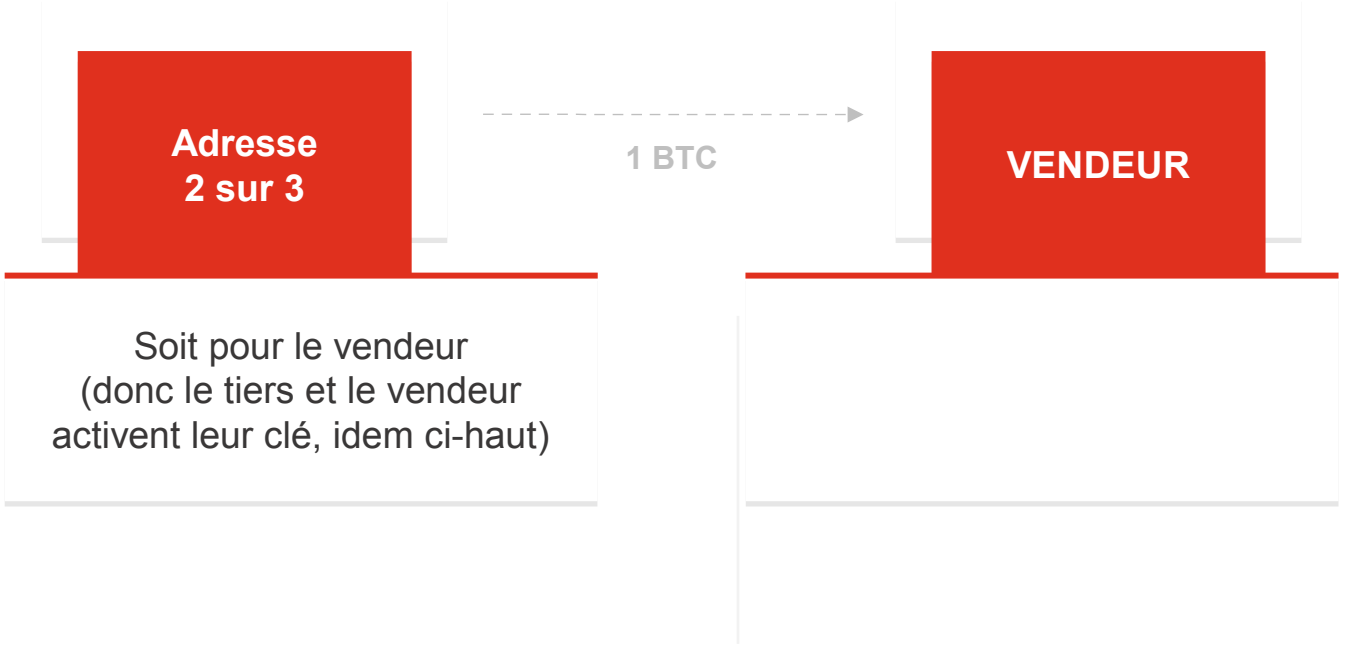


Si l'acheteur est satisfait, le vendeur et l'acheteur activent leur clé

OPENBAZAAR

L'acheteur envoie l'argent demandé sur une adresse 2 of 3 dont les 3 détenteurs d'une clé sont l'acheteur, le vendeur et le tiers choisi.

En cas de litige, le tiers tranche :



OPENBAZAAR

L'acheteur envoie l'argent demandé sur une adresse 2 of 3 dont les 3 détenteurs d'une clé sont l'acheteur, le vendeur et le tiers choisi.

Il y a un **rating** des tiers volontaires.

L'innovation est que le **tiers ne détient aucun fonds à aucun moment**.

*Possibilités de **tokenized assets***

Everledger travaille à la mise en place d'une blockchain pour l'enregistrement des échanges de diamants qui permettrait d'aider les diamantiers et leurs assureurs à réduire le vol et la fraude.

Nasdaq a mis en place une blockchain pour enregistrer ses transactions, et utilise partiellement la blockchain Bitcoin.

Une SCPI revient à une adresse M of N. La propriété immobilière pourrait donc s'échanger par blockchain (implémentation testée par la Suède le 10 juillet 2016).

Un « syndicated bank loan » peut permettre une mutualisation des contreparties.

3

SMART **CONTRACTS**

Description d'un ***smart contract***

> ***Les smart contracts*** *sont des protocoles informatiques qui facilitent, vérifient, ou appliquent la négociation ou l'exécution d'un contrat, ou rendent des clauses contractuelles non nécessaires.*
>
> *Wikipedia, Smart contracts.*

Description d'un ***smart contract***

Un smart contract est un contrat pour lequel tous les paiements et les clauses se déclenchent automatiquement. Les avantages d'un smart contract sont donc :

1

L'efficacité transactionnelle de générer automatiquement des contrats basés sur des schémas et des syntaxes convenues entre les parties

2

La capacité d'appliquer une logique de conformité

3

L'économie de temps et la réduction de coûts induites par l'automatisation de la fonction d'intermédiaire

Description d'un ***smart contract***

Pour la réalisation d'un smart contract, il faut :

1

Que **les paiements éventuels s'effectuent par une blockchain**

2

des règles claires stipulées au lancement du contrat et définies par protocole

Un contrat qui implique un paiement en euros ne peut être un smart contract.

*Fonctionnement d'un **smart contract** pour une assurance habitation*

Alice souscrit une assurance habitation auprès de l'assurance de Bob.

Le contrat d'assurance est déployé **sur une blockchain.**

1

Création et déploiement

Fixer
les paramètres du contrat

Déterminer
les conditions pour l'exécution

*Fonctionnement d'un **smart contract** pour une assurance habitation*

La maison d'Alice brûle et elle fait une déclaration de sinistres.

2

Evènements

Les évènements déclenchent l'execution du contrat

*Fonctionnement d'un **smart contract** pour une assurance habitation*

Une fois les conditions vérifiées par Bob, **un ordre de paiement est envoyé.**

3

Exécution et transfert de valeur

La valeur est transférée à partir d'un ensemble de règles prédéterminées

*Fonctionnement d'un **smart contract** pour une assurance habitation*

La réclamation est gérée de façon **transparente.**

4

Règlements

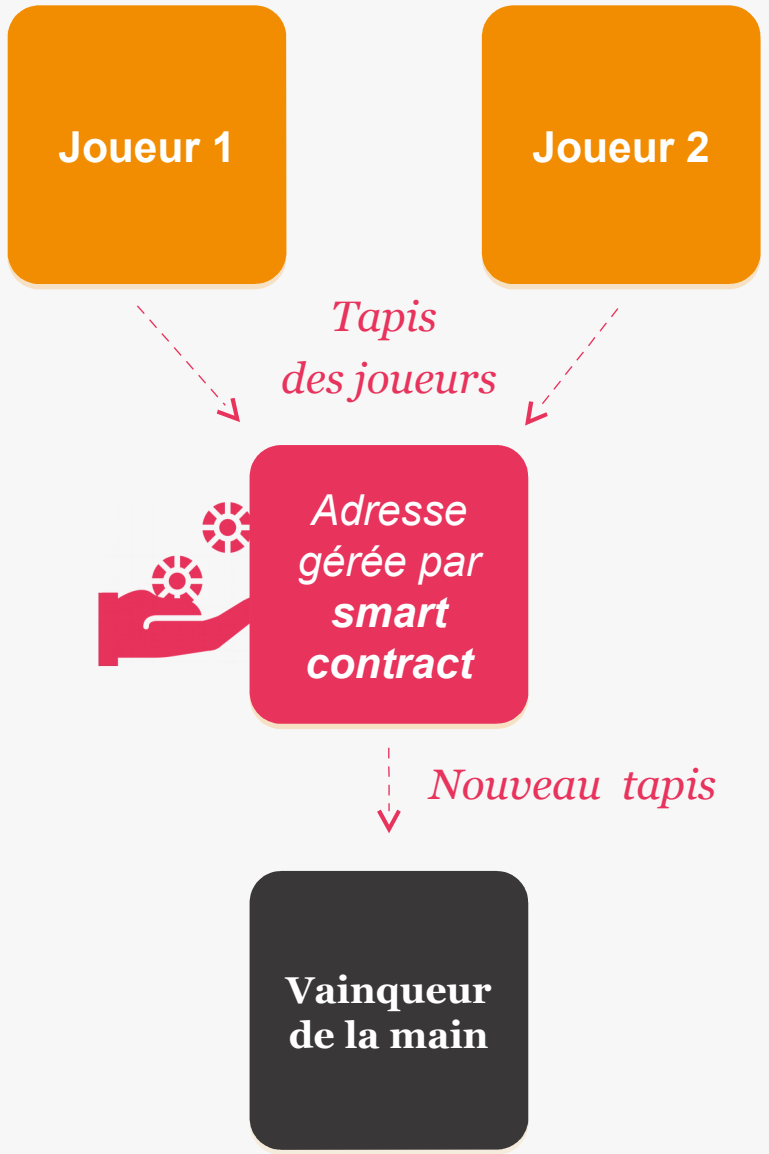
Règlement online/offline

*Autres exemples de **smart contracts***

> *Pokereum : jouer au poker par smart contract avec Ethereum.*

> *Ici, le joueur **ne porte plus le risque de ne pas être payé quand il gagne** et le rake peut se réduire aux fees des transactions.*

1. **Initialisation de la main**
2. **Déroulé de la main**
3. **Actualisation des tapis**



Autres exemples de ***smart contracts***

IMPOSSIBLE PAR SMART CONTRACT :

Parier sur le costume que portera Mr X à une réunion…

Autres exemples de ***smart contracts***

Un exemple en banque et en assurance :

UBS

Le smart bond d'UBS par Bitcoin (2015)

Les paiements de ce bond sont entièrement automatisés.

Allianz

Le natural catastrophe swap d'Allianz (juin 2016)

Il faut ici l'implémentation d'une interface enregistrant l'évènement déclencheur du paiement (dans ce cas le statut de catastrophe naturelle et la circonscription à la bonne zone géographique).

InsurETH lets you insure your flight directly with an ethereum smart contract
The contract is resolved automatically on the Ethereum blockchain
You can also apply to InsurETH as investor

Enter your flight number

ex: BA 2599

Insure for

£ 200
0.43 BTC
18.8 ETH

INSURE

*De nombreuses **startups***

Quelques projets :

La Maison du Bitcoin, lieu notamment d'achat de BTC en cash

Ledger, qui vend un moyen de sécuriser des BTCs

stratumn

Microassurance entre particulier par Stratumn

La'Zooz
Collaborative Transportation

Ubériser Uber et BlaBlaCar (La`Zooz)

*Un projet de smart contract public : **The DAO***

1 The DAO (Distributed autonomous organisation) est une forme de « venture capital en smart contract » public basé sur la blockchain Ethereum et versant des ETH (jetons d'Ethereum) lancé le 30 avril 2016.

2 Les développeurs ont pris un engagement juridique de ne jamais modifier le code du contrat.

3 Le 17 Juin 2016 le market cap de The DAO a atteint 160 millions $ avec plus de 10 000 investisseurs: plus important projet de smart contract à ce jour en capitalisation.

4 Un hacker trouve une faille dans le code et un moyen de « vider » progressivement la cagnotte sous-jacente de ce smart contract : chute de -50% du cours en 3h.

5 Les développeurs s'empressent de dire qu'ils vont modifier le code pour empêcher le hacker de percevoir ce qu'il a « vidé ».

6 Le hacker fait valoir ses droits juridiques : le code ne doit
pas être modifié.

7 Un autre hacker effectue le même « vidage » que le premier.

*Conséquence de the DAO : **le fork d'Ethereum***

8 Les développeurs d'Ethereum ont proposé une modification de la blockchain « contraire aux principes» : prendre tous les ETH récupérés par le hacker et les renvoyer à une adresse « convenable » du projet the DAO, malgré l'absence d'activation de clé privée.

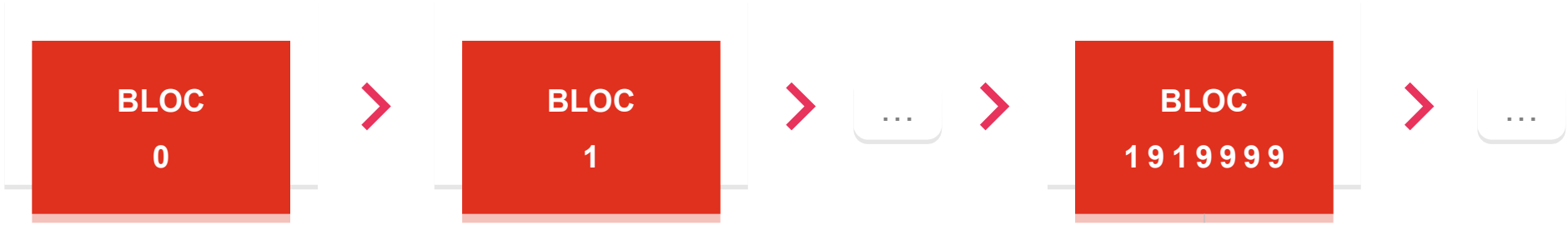
9 Certains ont refusé ce choix, et ont donc persisté à miner de nouveaux blocs sur les blocs « post-hack ».

10 Il y a donc eu fork : la blockchain Ethereum s'est séparée en deux, Ethereum (ETH) et Ethereum classic (ETC). Le hacker a bien des ETC, mais pas d'ETH.

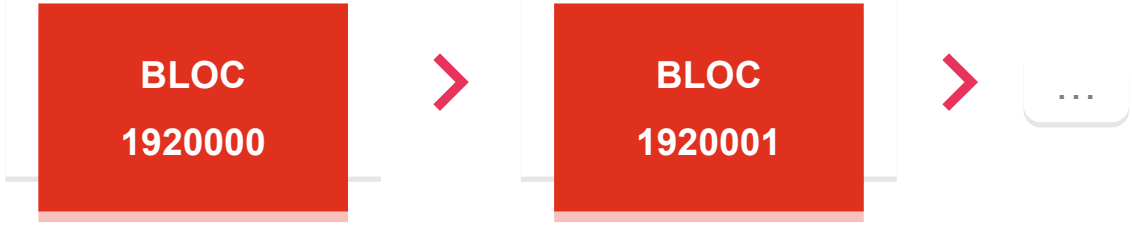
11 Les 2 blockchains semblent pérennes aujourd'hui.

Conséquence de the DAO : ***le fork d'Ethereum***

ETHEREUM CLASSIC



ETHEREUM - BLOC 1920000 MODIFIÉ



> *Conclusion : Un tiers tel qu'une banque ou une assurance peut être préférable pour un smart contract, surtout de longue durée.*

*Applications possibles des **blockchains***

1

Baisse des coûts de documentation des contrats

2

Amélioration du bookkeeping :
une blockchain pourrait notamment permettre une vérification des registres plus efficiente et un data mining plus fiable car sans outliers.

3

Une gestion des déclarations de sinistre plus efficiente

4

Une gestion des réserves plus flexibles :
Un marked to market instantané du portefeuille de l'assureur, mais aussi de celui de l'assuré, pourrait réduire les réserves de cash ou autres collatéraux nécessaires.

5

Une baisse des coûts de compliance

6

Design de nouveaux produits assurantiels adaptés aux économies émergentes


CREDENTIALS PwC

*Un blockchain lab de PwC avec **50 personnes***

Une connexion d'équipes

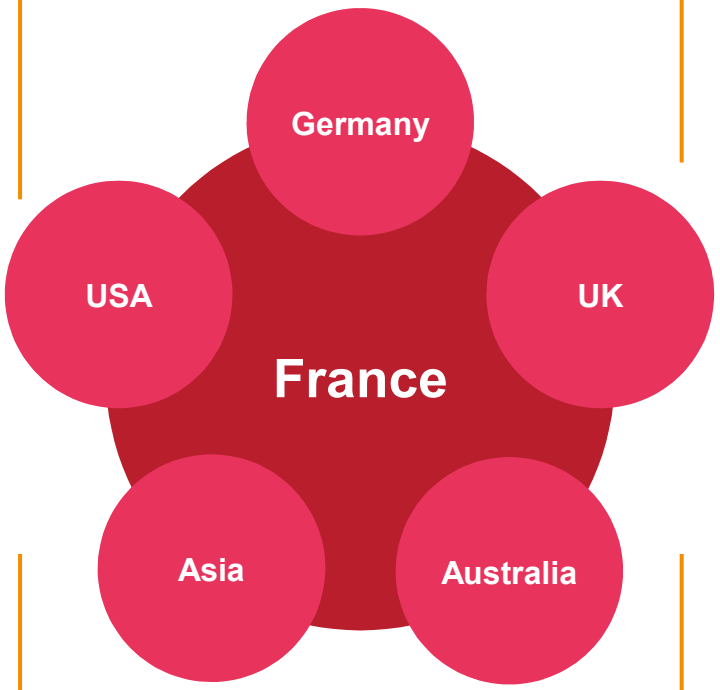
En combinant nos équipes d'experts en *cybersécurité, juridique, règlementaire, audit, Big Data, quants risque et actuaires*, nous pouvons aider à résoudre les problèmes qu'implique une intégration Blockchain.

Les accomplissements de PwC sur les blockchains incluent notamment :

Le design et le développement d'un prototype pour l'émission, l'échange, le règlement et l'administration de « syndicated bank loan » pour un grand groupe bancaire

Implémentation d'une solution de financement du commerce par smart contract pour une grande banque européenne

Le développement d'un prototype de blockchain pour le marché de la réassurance impliquant réassureurs, brokers et cédants.



Un Proof of Concept d'un système de règlement d'opérations sur titres pour la Bank of England

Aide d'une grande banque chinoise pour sa stratégie d'innovation concernant les blockchains

Implémentation d'une bourse par blockchain aux Emirats Arabes Unis

Blockstream, partenaire de PwC

Blockstream est une startup regroupant les core developers de Bitcoin. Elle est notamment spécialiste pour :

- L'anonymisation
- Les smart contracts
- Les sidechains

D'autres partenaires :

- Eris Industries, qui propose une plateforme pour les smart contracts
- Z/Yen, qui a conçu une solution par blockchain de gestion des recouvrements pour les contrats de réassurance XS

Blockstream

eris INDUSTRIES

Yen