Blockchain et Smart Contracts

Opportunités pour l'industrie de l'assurance

Jonathan Hamel, Fondateur

Académie Bitcoin

Vires In Numeris

UNIVERSITÉ LAVAL

Mars 2018

Académie Bitcoin

Vires In Numeris

Blockchain….. Mais encore?

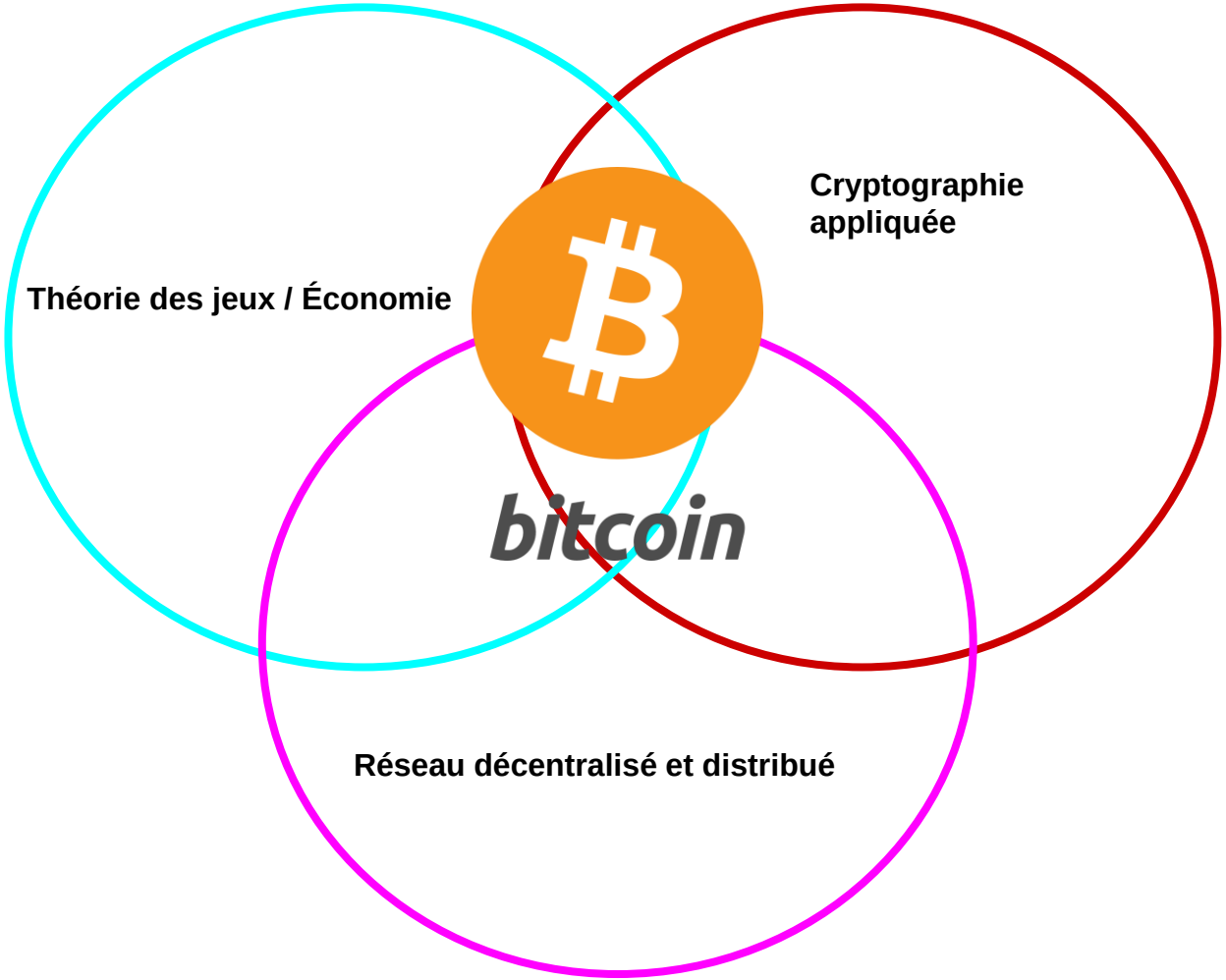
La Blockchain

- Est le produit (la conséquence) du consensus Bitcoin
- **N’est pas une technologie en soi**
- Nécessite plusieurs éléments clés pour fonctionner
  - Consensus (Décentralisation + incitatif)
- Distributed Ledger Technology : Pas un blockchain!

Académie Bitcoin

Vires In Numeris

Pourquoi ça fonctionne?


Théorie des jeux / Économie
Cryptographie appliquée
bitcoin
Réseau décentralisé et distribué

Académie Bitcoin

Vires In Numeris

Quelques exemples

Finance & Légal

Cas d’utilisation Blockchain

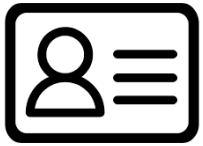
Présent → Futur

Cryptomonnaie

Compensation

Chaîne d’approvisionnement

Gouvernance / Vote

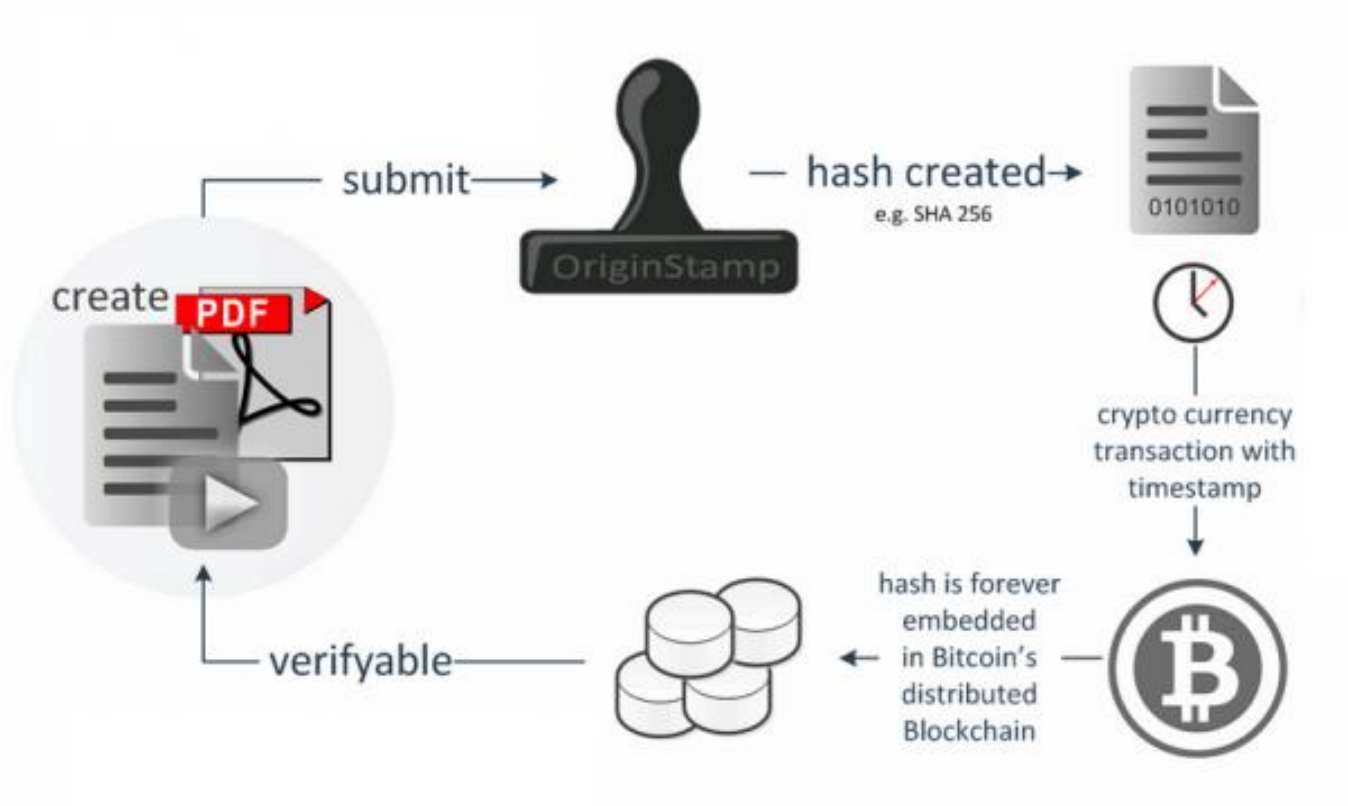


Identité

Académie Bitcoin

Vires In Numeris

Notarisation / Timestamping


submit
OriginStamp
hash created
e.g. SHA 256
0101010
create
PDF
crypto currency
transaction with
timestamp
hash is forever
embedded
in Bitcoin's
distributed
Blockchain
verifyable

A new security paradigm

Certify and authenticate any kind of data without relying on trusted third parties.

Proof of Ownership

Attribution and audit trails that can be independently verified

Proof of Existence

Certify that a file, dataset or communication existed at a certain point in time

Proof of Integrity

Monitor your data in real time to ensure it has not been tampered with

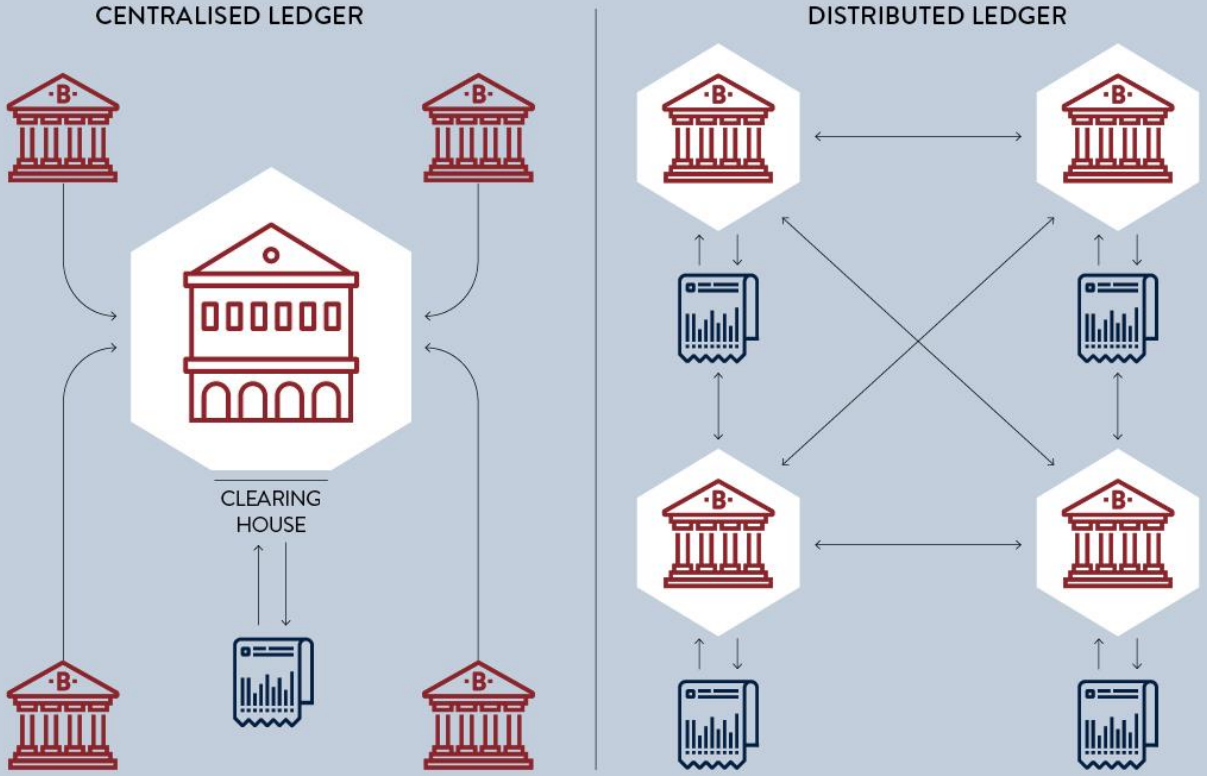
Proof of Receipt

Certify that a specific recipient read your email at a certain point in time

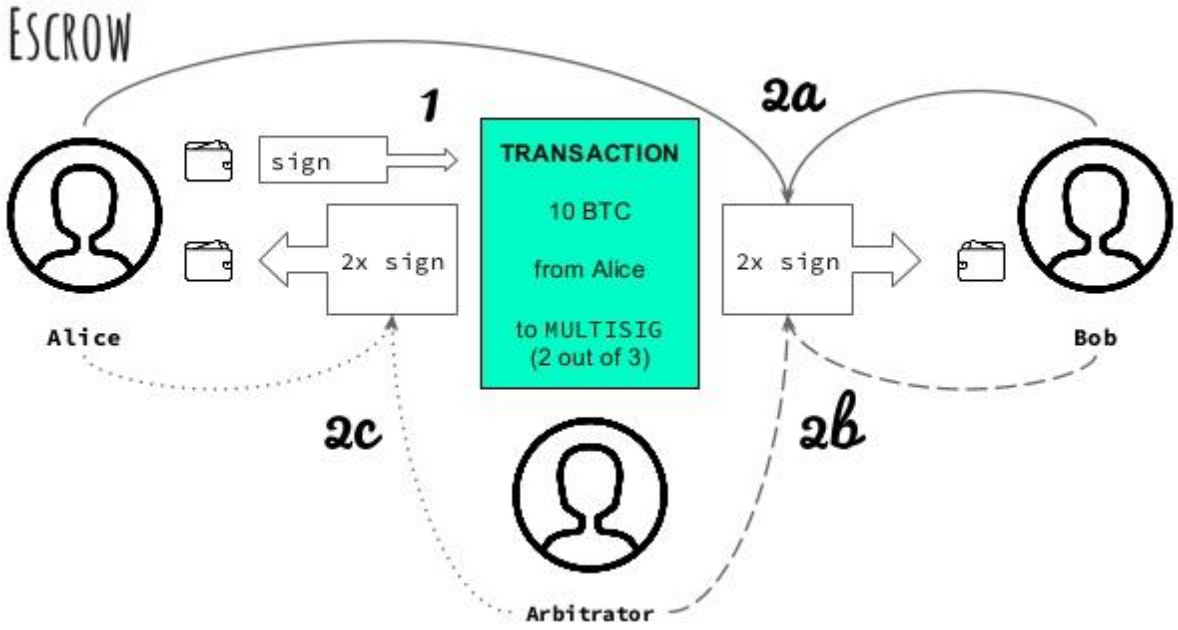
Compensation

CENTRALISED OR DISTRIBUTED LEDGER?

A DISTRIBUTED LEDGER IS A NETWORK THAT RECORDS OWNERSHIP THROUGH A SHARED REGISTRY



Multi Signature / Fiducie


ESCROW
1
2a
sign
TRANSACTION
10 BTC
from Alice
to MULTISIG
(2 out of 3)
2x sign
2x sign
Alice
Bob
2c
2b
Arbitrator

Académie Bitcoin

Vires In Numeris

Mouvement de valeur

Pour transférer 500,000,000$ CAD ...

- Frais de transaction?
- Délais de transaction?
- Sécurité de la transaction?

https://blockchain.info/tx/2248452e2122ff2d446565462cac276bbc8420c5874695a9b5c8e3bca8afa2b2

Transaction View information about a bitcoin transaction

2248452e2122ff2d446565462cac276bbc8420c5874695a9b5c8e3bca8afa2b2

19Mz2o9RDABT74SA9njZqMtJXKEzj2qUoH → 1PzGnXGvoGGtCcGpqzkJHebZVgM48VL2x4 $ 317,876,588.29

$ 317,876,588.29

Summary	
Size	1519 (bytes)
Weight	6076
Received Time	2017-08-04 21:20:46
Included In Blocks	479079 (2017-08-04 21:22:41 + 2 minutes)
Confirmations	36496 Confirmations
Visualize	View Tree Chart

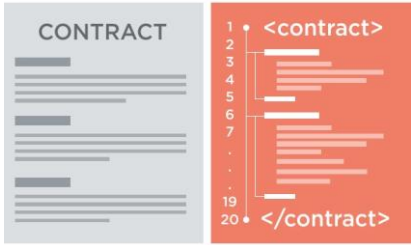
Inputs and Outputs	
Total Input	$ 317,876,589.58
Total Output	$ 317,876,588.29
Fees	$ 1.29
Fee per byte	10.666 sat/B
Fee per weight unit	2.666 sat/WU
Estimated BTC Transacted	$ 317,876,588.29
Scripts	Show scripts & coinbase

Académie Bitcoin

Vires In Numeris

Contrats Intelligents

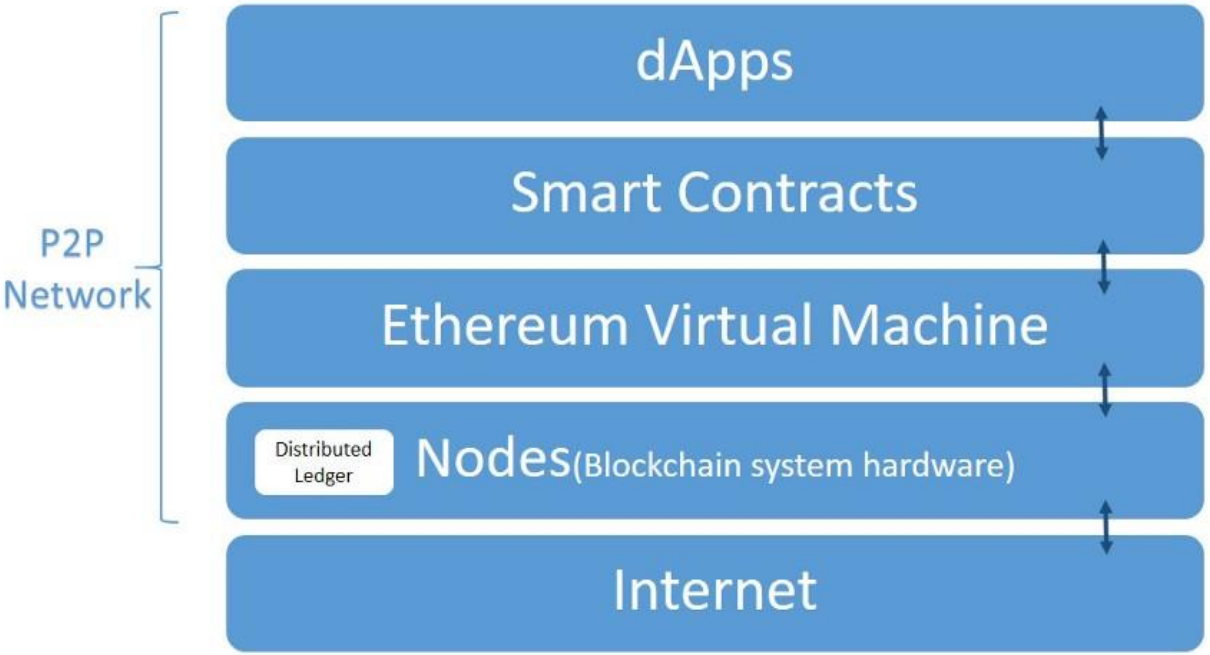
Contrats intelligents



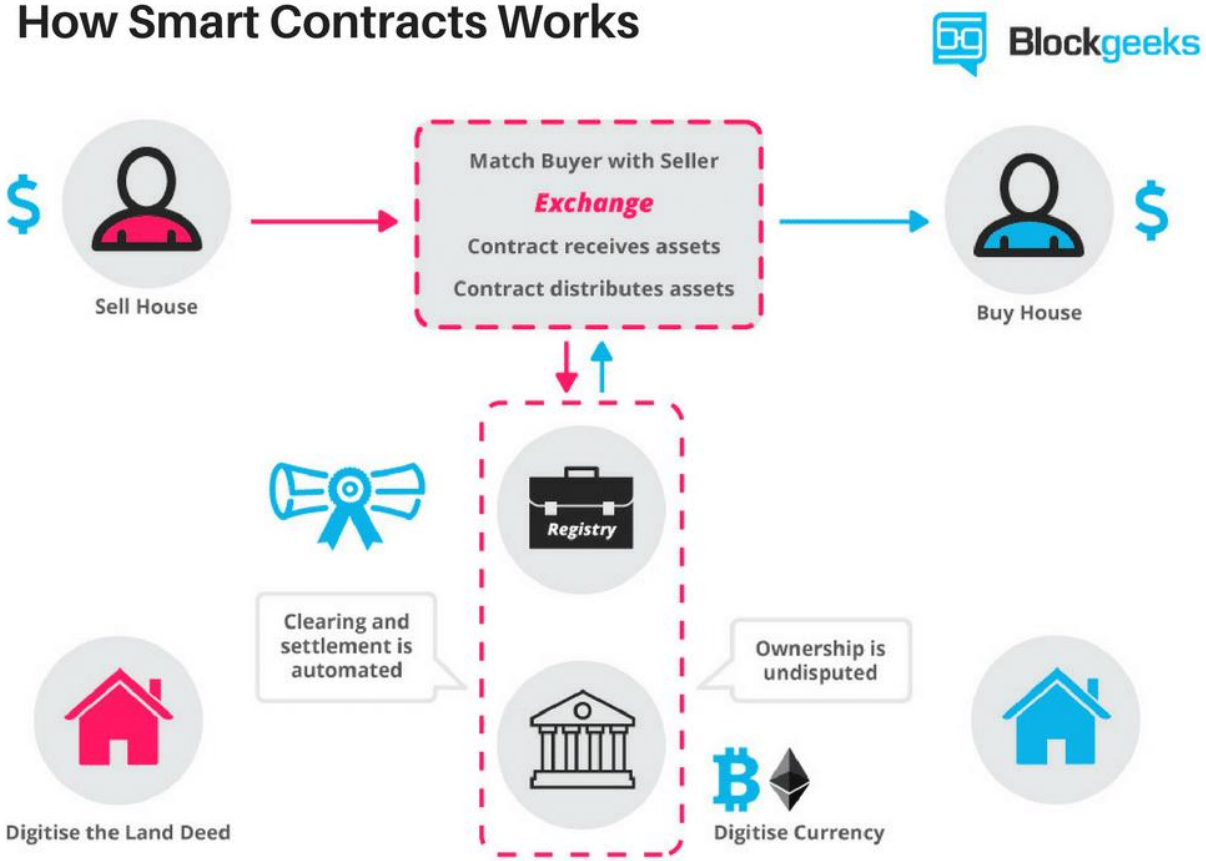
- Ethereum ou “sidechain” Bitcoin
- Ni un contrat
- Ni intelligent
- Transparent
- Prévisible
- Conditions préprogrammées
- Déclenché par un événement

Contrats intelligents

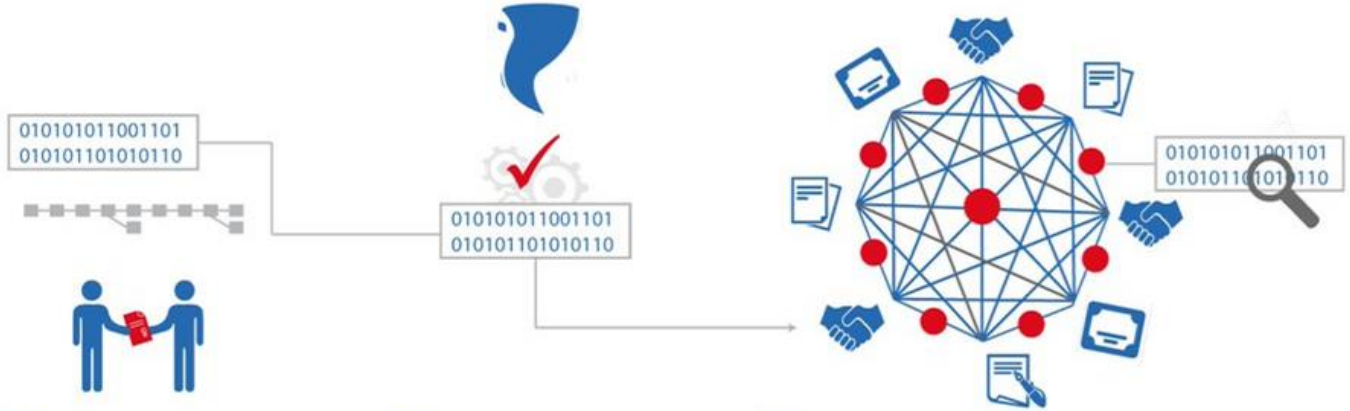
ethereum



How Smart Contracts Works

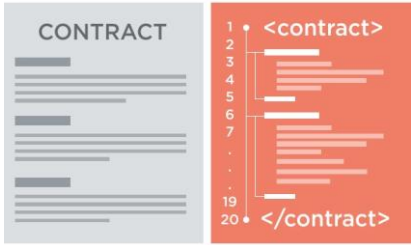


Contrats intelligents



1. A smart 'FbF' contract is written to the blockchain. The contract states that once a weather event occurs, a smart contract is executed.
2. An event like 'likelihood of monsoon occuring in Dhaka' triggers the execution of the smart contract. Digital assets are automatically distributed. to population group.
3. NGO has complete and permantent real-time records of all assets that have been distributed e.g. 100,000 water vouchers, and all transactions that have occurred e.g. 90000 water bottles purchased. This data can be used for analysis and future planning.

Contrats intelligents



- Micro-assurance
- Réassurance
- “Escrow”
- Distribution automatique de revenus
  - À certaines personnes
  - À un moment précis

Académie Bitcoin

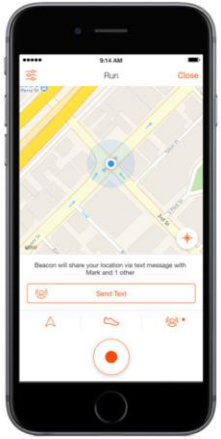
Vires In Numeris

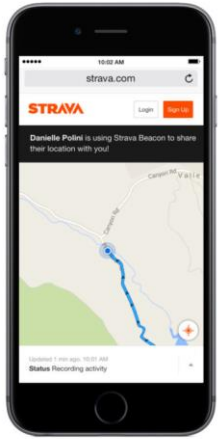
Identité

Indentité Blockchain

- Centralisation des données est un problème (ex: Equifax)
- Trop d’intermédiaires : délais, frais
- Duplication des données (ex: faire plusieurs tests sanguins)
- Un des cas les plus complexe à exécuter
  - Incertitude de plate-forme
  - À venir : “storage” décentralisées (ex: FileCoin, IPFS)
  - Barrière à l’entrée

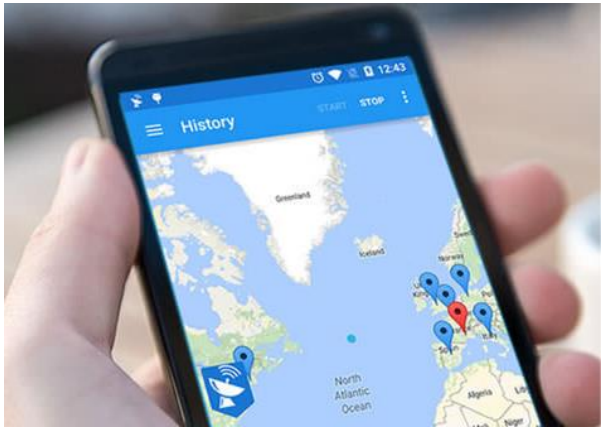
Preuve d’activité





- En partenariat avec une app comme Strava ou MapMyRide
- Captage des données biométriques
- Statistiques (fréquences des activités, données bio)
- Ajustement de la police en fonction du niveau de forme
  - Moins d’incertitude sur le niveau de risque
  - Incitatifs pour le client (récompenses? Ex: abonnements)

Preuve de localisation



- Voyage, déplacement d’affaire, mouvement d’objet de valeur
- Captage des données GPS
- Est-ce que X était à Y endroit à Z moment dans le temps?
- Ajustement de la police en fonction du risque :
  - République démocratique du Congo vs. Longueuil
  - Assurance spontanée (au besoin)

Menaces et limites

Menaces Non-techniques

- Législatif : reconnaissance légale des enregistrements Blockchain
- Validation et audit des smart contracts (fait par qui?)
- Complexité d'adaptation du cadre juridique

Menaces techniques

- Informatique Quantique (menace à la cryptographie SHA256)
- “Scaling” (performance vs. solidité)
- Failles et piratage d’acteurs (échanges, “Wallet”, etc.)
- Problème de l’oracle : source des données qui alimente les smart contracts
- Risque de plate-forme : encore très tôt pour déterminer un gagnant

Académie Bitcoin

Vires In Numeris

Conclusion

Académie Bitcoin

Vires In Numeris

Q&A

Académie Bitcoin

Nos services

- ➔ Consultation et formation Blockchain
- ➔ Recherche cryptoactifs
- ➔ Vérification diligente
- ➔ Accompagnement pour investissement Blockchain

LinkedIn : Jonathan Hamel
Email : jhamel@academiebitcoin.com