

Blockchain et sécurité : applications à la banque et l'assurance

GS Days – 28 mars 2017

RENAUD LIFCHITZ
renaud.lifchitz@digitalsecurity.fr

digital security | econocom

INTERVENANT

Renaud Lifchitz, IoT security expert, DIGITAL SECURITY

renaud.lifchitz@digitalsecurity.fr



Quelques activités de Digital Security

CONSEIL

Définition

En amont des projets :

- Stratégie, schéma directeur
- Cartographie des risques et plan de traitement
- Etudes prospectives et de cadrage
- Recherche d'opportunités

Construction & mise en œuvre

Ingénierie sécurité :

- Politique & système de management (processus sécurité)
- Conduite du changement (formation, communication, sensibilisation)
- Intégration de la sécurité dans les projets
- Tests et recette des solutions

AUDIT

Evaluation

Au cœur des vérifications

- Tests d'intrusion
- Audits d'architecture
- Audits de conformité
- Audits de maturité
- Audit de code
- Audit de configuration
- Exercices en mode red team
- Préparation aux certifications
- Laboratoire de test et d'essai IoT

CERT

Maintien en condition de sécurité

Accompagnement opérationnel

- Réponse à incidents / Aide à la réaction (traitement des alertes, analyse forensic & post-incident)
- Contrôle continu
- Aide à la détection (veille, surveillance)

ISO 27001 Lead Auditor, ISO 27005 Risk Manager,
ISO 22301 Lead Implementor, ITIL, CMMI



Qualifié PASSI



TF-CSIRT
Trusted Introducer

Introduction

Blockchain

- Registre global distribué
(aucun point unique de défaillance)
- Transmission d'informations authentifiée, fiable et sûre
- Multiples usages
- Multiples intérêts
- Entièrement personnalisable selon le contexte métier



Blockchain

Intérêts



- Scalabilité : facilité pour déployer des nœuds
- Résilience : résistance aux attaques de tout type (réseau, applicatives, dénis de service, ...)
- Intégrité et authenticité des données : données authentifiées et immuables
- Décentralisation : pas de point de défaillance unique, plus besoin de tiers de confiance
- Rapidité des transactions par rapport aux réseaux interbancaires (ex.: SWIFT)

Réseau de confiance

Smarts contracts

- Exécution automatisée, décentralisée, conditionnelle et sûre d'engagements (contrats) programmés à l'avance
- Contrats non modifiables une fois déployés sur la blockchain
- Exécution infalsifiable
- Grande variété de contrats modélisables
- Une partie, deux parties, ou contrats multipartites
- dApp : application web décentralisée se connectant à un ou des contrats sur une blockchain



Smarts contracts

STATE OF THE DAPPS

Search i

328 dapps listed Sort: Updated

FirstBlood.io Joe & Zack A decentralized eSports reward platform. Work In Progress 2017-01-21	Flight Delay Insurance Christoph Mussenbrock Get indemnification if your plane is late Working Prototype 2017-01-21	GroupGnosis ConsenSys / Martin Köppelmann & Stefan George Prediction market Live 2017-01-21	Etherplay wighawag Skill Games : Play games on Ethereum Live 2017-01-03
EtherGit Miles Albert Incentivized open source software development Work In Progress 2016-12-01	Verity Matt Goldenberg Credible, Decentralized Reputation and Governance Work In Progress 2016-11-26	SmartToken Nikita Dubrovin NFC smart-token with SMS Secure Work In Progress 2016-11-24	Chainy.Link Everex Create Irreplaceable short URLs, Messages, Links to File Live 2016-11-24
PixelMap Ken Erwin The Million Dollar Homepage, on the Blockchain!	Dragoo Gabriele Rigo decentralized hedge fund and social trading	Time Clock Daniel Moscufo Service Delivery / Labor hire contract	AuctionHouse Doug Petkanics, Eric Tang Auction platform for non-fungible on-chain assets.

« State of the dApps », un annuaire public de dApps Ethereum :

<http://dapps.ethercasts.com/>

Oracles

- Programmes jouant le rôle de passerelles entre une blockchain et le monde physique ou plus généralement le web
- Les conditions d'exécution d'un contrat dépendent très souvent d'indicateurs externes : météo, cours de bourse, actualités, résultat d'un match de sport, solde sur un compte...
- Un oracle se présente le plus souvent sous forme d'une fonction callable depuis un smart contract



Une blockchain prometteuse : Ethereum



- Première version : 30 juillet 2015
- 15 secondes par bloc
- Des smart contracts très puissants (« Turing-complets »), contrairement à Bitcoin
- Un système d'oracle mûre et bien intégré : <http://www.oracize.it/> , apportant une preuve d'honnêteté (« TLSNotary »)
- Un bon support de la communauté et de quelques professionnels
- Une documentation riche
- Une majorité d'exemples et de démonstrations seront réalisés avec Ethereum lors de cette présentation
- Langage de développement des smart contracts : Solidity (variante typée de Javascript)

Cas d'usages

Pourquoi une blockchain ?

Ou pourquoi ne pas en abuser...

- De nombreux cas d'usage ne justifient pas l'usage d'une blockchain :
 - Transactions très limitées en taille et en nombre (Bitcoin est limité à 3-7 transactions par seconde, Ethereum à 7-15)
 - Système coûteux énergétiquement parlant (par rapport à une redondance informatique classique)
- Plusieurs facteurs favorisent et légitiment par contre l'adoption d'une blockchain :
 - Absence de confiance à priori entre participants
 - Ecriture par des acteurs indépendants
 - Bénéfices pour les participants
 - Désintermédiation



Cas d'usages généraux

- Banque
- Assurance
- Notariat
- Vote électronique
- Conservation de la preuve
- Collecte/Levée de fonds
- Exécution conditionnelle de transactions (contrats électroniques)

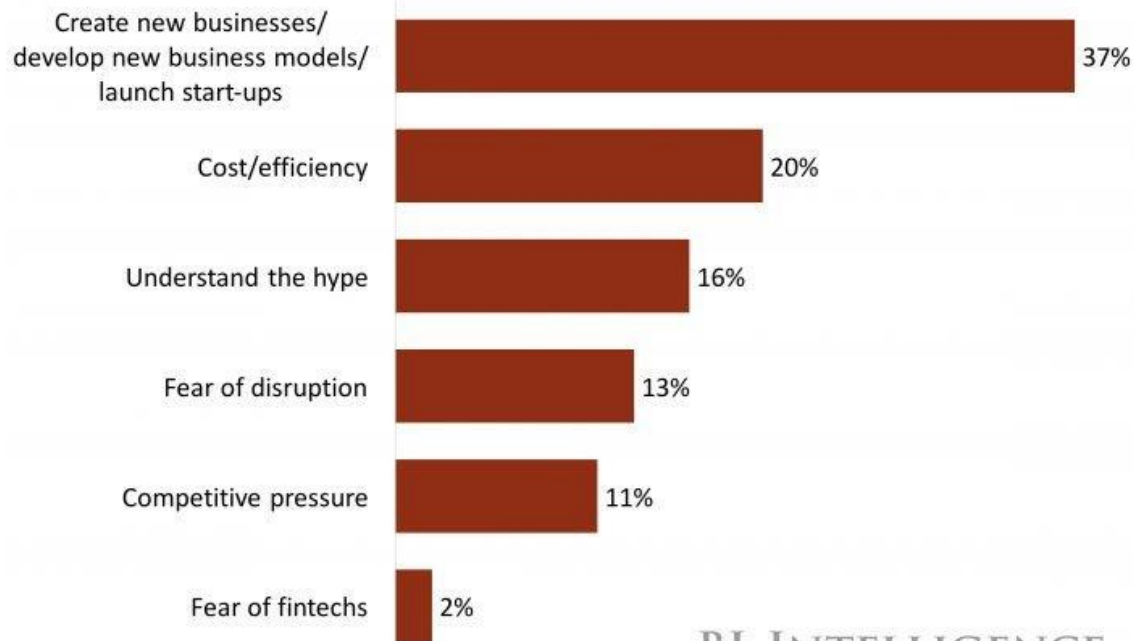


Cas d'usages généraux

Intérêts des services financiers EMEA dans la blockchain

Why Financial Services Firms In EMEA Are Exploring Blockchain

2016



Source: EFMA and Deloitte

BI INTELLIGENCE

Cas d'usages généraux

Démonstration



Notariat / Ancrage de données / Preuve d'antériorité sur la blockchain Bitcoin :

<https://woleet.io/>

Banques

Cas d'usages

Top Bank Initial Use Cases For Blockchain
2015



Source: EFMA and Deloitte, n=3,000

BI INTELLIGENCE

Banques

Elles ont franchi le pas blockchain...



BNP PARIBAS



Banques

Cas d'usages & exemples



6 McKinsey has identified 7 genuine use cases and associated pain points; all of those sized could generate ~\$80B to 110B in impact

	Value generated by blockchain (\$B)	Blockchain benefits	Examples of impacted players	Drivers of cost today	Application by type of bank		Impact levers			
					CIB	Retail	Cost	Revenues	Capital	
<p>64 Identified >60 viable use cases from a database of >200 fintech startups, press clippings, and research</p> <p>24 Focused on 24 financial services applications</p> <p>7 Selected 7 use cases for analysis, based on initial hypothesis of potential for disruption and size of impact</p>	A Trade finance	14 - 17	<ul style="list-style-type: none"> Lower cost and operational risk, faster turn-around, increase in revenues 		<ul style="list-style-type: none"> Paper-based and labor heavy structure Error-prone processes Capital that is locked up in the TF processes 	✓	✓	✓	✓	✓
	B Cross-border B2B payments	50 - 60	<ul style="list-style-type: none"> Lower cost and fees Increased security and speed 		<ul style="list-style-type: none"> High fees and slow processing due to intermediaries High operational costs 	✓	✓	✓	✓	✗
	C Cross-border P2P payments	3 - 5	<ul style="list-style-type: none"> Lower cost and fees from competition, increased security and transparency 		<ul style="list-style-type: none"> Paper-based High fees due to lack of intermediary competition Capturing incorrect receiver information 	✗	✓	✓	✓	✗
	D Repurchase agreement transactions (repos)	2 - 5	<ul style="list-style-type: none"> More effective netting Lower systematic risk Reduced operational costs 		<ul style="list-style-type: none"> Inability to net the obligations Counter-party risk Credit sensitive repo buyers 	✓	✗	✓	✗	✓
	E OTC Derivatives	4 - 7	<ul style="list-style-type: none"> Reduced operational costs and capital due to streamlined processing and settling 		<ul style="list-style-type: none"> Manual and duplicative data entry and verification processes High capital requirements 	✓	✗	✓	✗	✓
	F KYC / AML management	4 - 8	<ul style="list-style-type: none"> Reduced duplicative efforts in on-boarding customers Improved transaction monitoring 		<ul style="list-style-type: none"> Manual and duplicative data entry and verification processes Low visibility into transactions 	✓	✓	✓	✗	✗
	G Identity fraud	7 - 9	<ul style="list-style-type: none"> Secure storage of ID credentials More secure account opening, transaction authentication 		<ul style="list-style-type: none"> Direct losses due to fraudulent activity (90-95%) Fraud prevention infrastructure and processes (5-10%) 	✓	✓	✓	✗	✗

SOURCE: McKinsey analysis

McKinsey & Company | 9

Banques

Un standard pour l'émission de jetons sur la blockchain ?

- Jeton : unité de valeur dont on souhaite contrôler l'émission, l'utilisation et/ou les contreparties
- Standard ERP20 sur Ethereum (<https://github.com/ethereum/EIPs/issues/20>)
- Utilisation :
 - Monnaie électronique
 - Points de fidélité (enseignes commerciales)
 - Bons d'achat / bons de réduction
 - Preuves



Assurances

Cas d'usage



- Automatisation du paiement des primes à échéance
- Assurances indicielles ou paramétriques : estimations actualisées des risques par oracle
- Garantie d'unicité de déclaration de sinistre
- Acquiescement de sinistre par oracle
- Rationalisation du paiement des indemnités

Assurances

Cas d'usage

7 In Insurance, blockchains have potential for impact across the entire value chain

NOT EXHAUSTIVE

	Product development and distribution	Pricing/underwriting	Payment & collections	Claims	Policy/administration and back offices	Risk capital & investment management
Potential						
Potential use cases		<ul style="list-style-type: none"> Use blockchain as a reliable registry for on-demand / usage-based insurance or micro-insurances 	<ul style="list-style-type: none"> Using blockchain as payment infrastructure (especially across multiple countries) 	<ul style="list-style-type: none"> Leverage blockchain for information about insured goods and events in order to fight fraud 	<ul style="list-style-type: none"> Use blockchain for onboarding of new customers or verification of policy-holder identity 	<ul style="list-style-type: none"> Make data available for re-insurers or other parties in a controlled way
Potential use cases with smart contracts	<ul style="list-style-type: none"> Offer P2P insurance via blockchain for customer to customer promotion and sales, and automated ops with smart contracts 	<ul style="list-style-type: none"> Use blockchain for P2P insurance underwriting, include external data, smart contracts and peers (humans) to determine tariff 	<ul style="list-style-type: none"> Automate payments through smart contracts evaluating conditions for paying out claims 	<ul style="list-style-type: none"> Automate claims triggering and handling with smart contracts, and e.g., with sensors (IOT) 		<ul style="list-style-type: none"> Use smart contracts to automatically determine payouts – e.g. triggering process of catastrophe swaps and bonds
Key benefits	<ul style="list-style-type: none"> Reduce cost related to commission and sales and operations Increase trust of customers due to open, distributed system 	<ul style="list-style-type: none"> Reduce cost of operations Reuse platform for other types of insurances Include external data for (semi-) automatic pricing 	<ul style="list-style-type: none"> Reduce cost and increase speed for payments 	<ul style="list-style-type: none"> Reduce average claims cost related to <ul style="list-style-type: none"> Claims administration Damage from fraud and fraud detection Improve identification of claim events 	<ul style="list-style-type: none"> Reduced admin cost and speed-up process for onboarding 	<ul style="list-style-type: none"> Reduce admin costs Automate and increase reliability, auditability and speed for financial instruments transactions based on defined events
Examples ¹	 	 	 	 	 	

1 Not all insurance-specific

Assurances

Exemples

- Assurance couvrant les retards d'avion :
« Flight Delays Suck! » : <https://fdd.etherisc.com/>
- Assurance couvrant les cultures contre les risques de sécheresse ou d'inondation :
« Jamii Crop Insurance » : <https://crop.etherisc.com/>
- Sécurité sociale décentralisée (en test) :
« Etherisc Social Insurance » <https://govhack.etherisc.com/>
- Mise en oeuvre de swaps de risque de catastrophe naturelle, négociation facilitée des obligations catastrophe (Allianz Risk Transfer AG & Nephila Capital Limited)
- Développement de sidechains pour l'interopérabilité entre blockchains et le traitement de transactions massives (Axa Strategic Ventures & Blockstream)



Assurances

Démonstration



etherisc.com
how it works
apply for policy
watch your policy
meet the team
contact

Ropsten Testnet
Block: 389848
Contract:
0x0963b...
Account: 0x53f2f...
104.48€

© 2016 Christoph Musenbrock
image credits

Flight Delays Suck!

You'll love to be late! Get your instant payout in case your flight is late.

[find out more](#)

Assurance couvrant les retards d'avion :
« Flight Delays Suck! » : <https://fdd.etherisc.com/>

Sécurité

L'affaire « The DAO » (1/2)

- The DAO est un smart contract de levée de fonds (Organisation Décentralisée Autonome) développé par Slock.it (serrure connectée à la blockchain)
- Equivalent de plus de 150 millions d'euros collectés pour un projet initial qui ne nécessitait que quelques centaines de milliers d'euros (15% de la masse monétaire émise)



L'affaire « The DAO » (2/2)

- 17 juin 2016 : détournement du tiers par exploitation d'une vulnérabilité d'implémentation (appels récursifs) dans le contrat
- « Hard Fork » pour liquider le contrat et récupérer les fonds, puis naissance d'ETC : quid de la gouvernance ?
- Analyse juridique de la contractualisation avec un smart contract via la société suisse DAO.LINK : <https://www.ethereum-france.com/dao-link-permet-a-des-entreprises-de-contracter-avec-des-dao/>



Impacts du choix de la technologie

La blockchain

- Critères importants :
 - Maturité
 - Sécurité
 - Possibilité d'interopérabilité (oracles et sidechains)
 - Support
 - Puissance des smart contracts
 - Montée en charge (taille des transactions et délai entre les blocs)

- Quelques blockchains :
Bitcoin, Ethereum, Zcash, Ripple,
Lisk, Tezos, Iota, (Byteball) ...

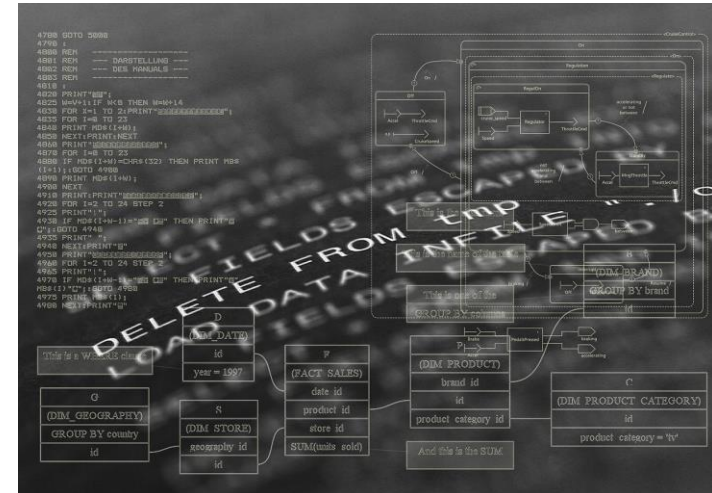


Impacts du choix de la technologie

Le langage de développement des smart contracts

- Langages impératifs :
 - Courants en développement
 - Plus simples à écrire
 - Plus complexes à vérifier par preuve formelle (effets de bord)

- Langages fonctionnels :
 - Peu communs
 - Complexes à écrire
 - Plus faciles à vérifier (pas d'effets de bord)



Bonnes pratiques de sécurité

Bonnes pratiques fonctionnelles

- Simplicité, modularité et réutilisabilité du code
- Ecriture de tests unitaires et de tests d'intégration
- Incitations économiques diverses :
 - Limites de montants traités
 - Bug bounties
(ex. : <https://bountyfactory.io>)
 - Marchés de prédiction (ex. : <https://gnosis.pm/> , <https://augur.net/>)
- Séparation des conditions et des actions dans le code (« Condition-Oriented programming »)



Bonnes pratiques de sécurité

Bonnes pratiques techniques

- Implémentation d'un « killswitch » dans les contrats
- Pré et post-conditions sur les fonctions
- Preuves formelles : plus faciles avec les langages fonctionnels (mais incitations économiques non prises en compte)
- Utilisation de « mocks » pour les tests
- Utilisation d'environnements de test (frameworks, testnets...)



Nos prestations de service blockchain orientées sécurité

Nos savoir-faire blockchain / sécurité

- Accompagnement à la conception et mise en œuvre de solutions blockchain
- Evaluation des risques techniques et juridiques
- Formation aux technologies blockchain
- Développement de preuves de concept
- Audit de primitives cryptographiques
- Développement de smart contracts
- Maîtrise des technologies Bitcoin, Ripple et Ethereum



Digital Security participe à la rédaction d'une étude sur la blockchain pour un ministère

Questions ? / Contact



Renaud LIFCHITZ
Consultant Sécurité Senior
renaud.lifchitz@digitalsecurity.fr

info@digitalsecurity.fr