



Blockchain

Hello!

Adrian Sauzade

Co-Fondateur de Czam

Fondateur de Wekeep

Antoine Ferron

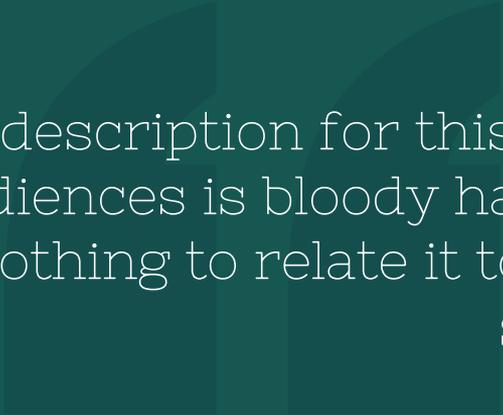
Goochain – Citadelle



1

De quoi parle-on ?

Pour une explication simple des
enjeux de la blockchain



Writing a description for this thing for
general audiences is bloody hard. There's
nothing to relate it to.

Satoshi, July 5, 2010



Internet permet de diffuser

Sur internet on duplique ce que l'on transmet



La Blockchain permet de donner

Sur la Blockchain ce que vous transmettez ne vous appartient plus



2000

Site
Internet

2010

Application
mobile

2020

Application
financière

Avant la Blockchain

Digicash (1990)

E-gold (1995)

Beenz (1998)

Liberty reserve (2002)

Linden Dollars (2003)

Problème de centralisation

digicash

e-gold



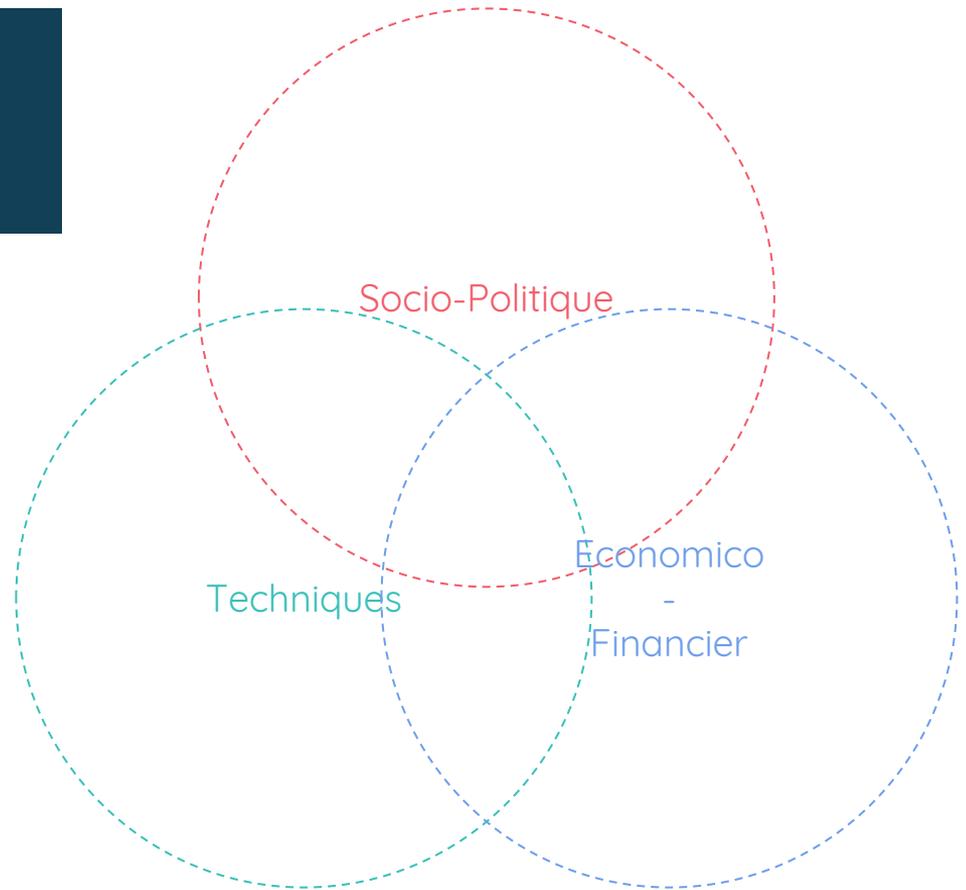
L\$

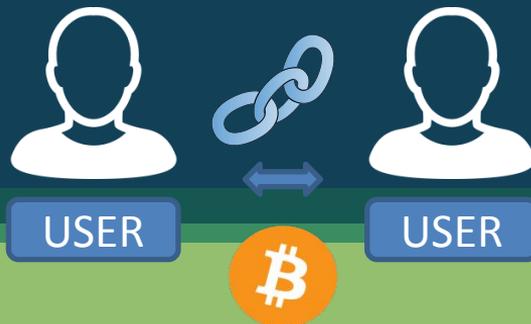
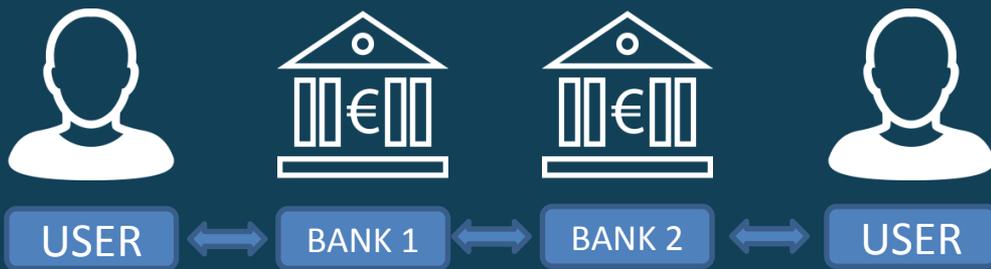
Les enjeux

Les implications de la Blockchain sont multiple :

- Les communautés au centre
- La création monétaire remise en cause ?
- Une perte de contrôle des banques et des gouvernements sur la finance
- Une nouvelle façon de gérer les données

Un prisme à plusieurs facettes qu'il est important d'explorer pour une compréhension globale du sujet





The promise of the blockchain

The trust machine

The technology behind bitcoin could transform how the economy works

Oct 31st 2015 | From the print edition



10K





Innovate

Record \$1 billion invested in Bitcoin firms so far

GRUPE

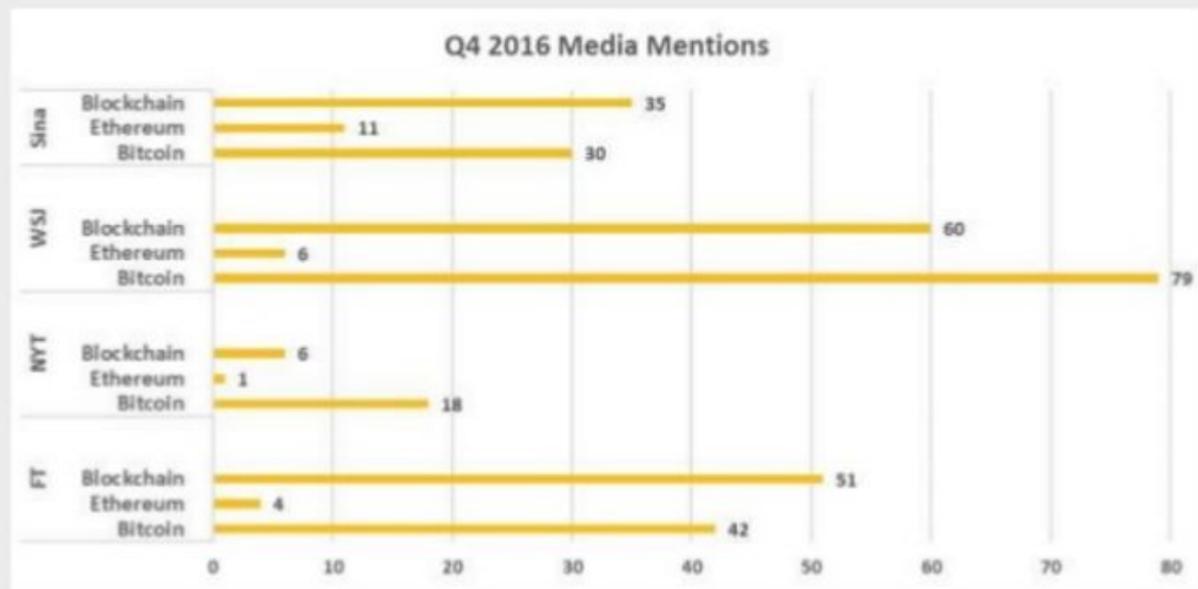


"Chain is thrilled to be working with Nasdaq on blockchain initiatives which will reduce the time, costs, and points of friction across the capital markets."



HYPERLEDGER PROJECT





**Blockchain media mentions pull ahead in UK and Asia,
bitcoin interest still strong in US**

Data Sources: [Sina](#), [WSJ](#), [NYT](#), [FT](#)

2

Les \neq blockchain

Histoire des blockchain



Publique - Privée - Hybride

Une Blockchain publique

Un protocole Internet qui gère la distribution de données prouvables uniques

Une Blockchain d'entreprise

Registre de consensus partagée par des intermédiaires de confiance

Une Blockchain Hybride

Registre de consensus sur lequel certains clients ont la possibilité de se connecter



Exemples

Blockchains publiques



Blockchain privées



HYPERLEDGER



Chain



Blockchain Project Funding Models

Entrepreneurs have begun considering blockchain token sales ('ICOs') as fundraising alternatives to traditional venture capital and angel investment

	ICO	HYBRID	VC
PROTOCOL			
COMPANY	 		  
APPLICATION	   		

ICOs rather than VC has driven the development of most public blockchain applications, as well as numerous protocols and companies, a line which is becoming increasingly blurred

Notes: Numerous protocols are also maintained by companies like the Zerocoin Electric Coin Company, open source communities, non-profits like the Ethereum Foundation, and consortiums like Hyperledger

DASH EXCHANGE

DASH/BTC

Last Price 0.07830670	24hr Change 28.16%	24hr High 0.08080000	24hr Low 0.06100000
24hr Volume: 34454.38905968 BTC / 474878.62762081 DASH			



https://poloniex.com

MARKETS

show ★ only

Filter (Ctrl+F)

	BTC	ETH	XMR	USDT	
★ Coin	Price	Volume	Change	Name	
★ DASH	0.07830670	34454.389	+28.16	Dash	
★ ETH	0.02476602	22211.324	+9.01	Ethereum	
★ XMR	0.01450000	4562.361	+4.88	Monero	
★ FCT	0.00310211	1269.893	+1.09	Factom	
★ ETC	0.00136287	1229.744	+2.85	Ethereum Classic	
★ ZEC	0.03613003	740.549	+3.82	Zcash	
★ DCR	0.00378000	596.620	-1.54	Decred	
★ GNT	0.00001939	509.954	-4.39	Golem	
★ LSK	0.00012116	505.675	+0.94	Lisk	
★ LBC	0.00002749	499.790	+7.97	LBRY Credits	
★ REP	0.00720001	484.676	+6.31	Augur	
★ SDC	0.00300674	444.247	-1.39	Shadow	
★ LTC	0.00340200	363.121	+1.53	Litecoin	
★ XRP	0.00000502	300.078	+0.40	Ripple	
★ STEEM	0.00006130	250.712	-13.73	STEEM	
★ XEM	0.00000899	241.327	-3.95	NEM	
★ MAID	0.00014104	213.504	+2.20	MaidSafeCoin	
★ NXT	0.00000883	199.942	+20.96	NXT	
★ BELA	0.00003749	156.185	-12.16	Belacoin	
★ BTS	0.00000349	151.837	+8.39	BitShares	

TROLLBOX ^

🔗 📄 ⚙️

uptown: lets git this monnaaaa i need to pay no insurance f the government f the system

Problématiques BTC / ETH



Débat sur la scalabilité

- Taille des Blocks
- Gouvernance



Débat sur la sécurité

- Preuves formelles
- Gouvernance

3



Bitcoin

Quelques éléments techniques

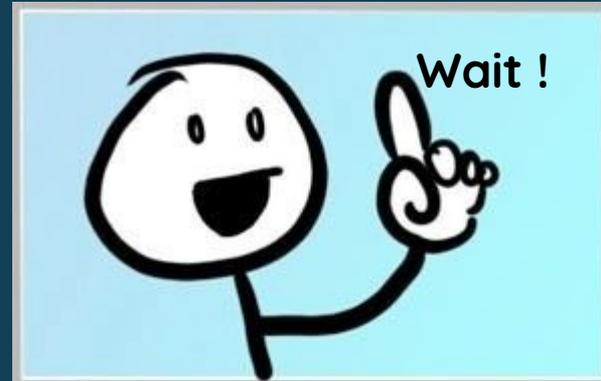


Bitcoin est une réalisation cryptologique remarquable. La possibilité de créer des choses non-duplicables dans le monde du numérique, cela a une énorme valeur.

Eric Schmidt

Trust no one !

La confiance dans l'économie
Bitcoin se résume en ces 3
mots !



Une clé ?

Bitcoin Address Private Key

 **6** **SHARE**  **=** **2+5-1** **SECRET** 

1QBYeTQKdQsqEtQxbf146NasWG3xPgtvUH KxR2VNDWwNZTk4PeRsr9CvZjdj2Q2wvynnLuiJLQY6dMb872Vd7X



Multisignature

Il est nativement possible de demander à plusieurs utilisateurs de valider une transaction.

Exemple d'applications

B2B

Séquestre tiers

Sécurisation des fonds

Vote pour transferts

Minimum share threshold needed to combine

Number of shares

Bitcoin Address: 13ZQRUgnxpb9xuMC5MoCfqhzfRNHWDE1mM



Share 1: 3XwNhQAvqUHHnBennLMfPV9J95z1jkNd42ehhKxGJgpu3FN

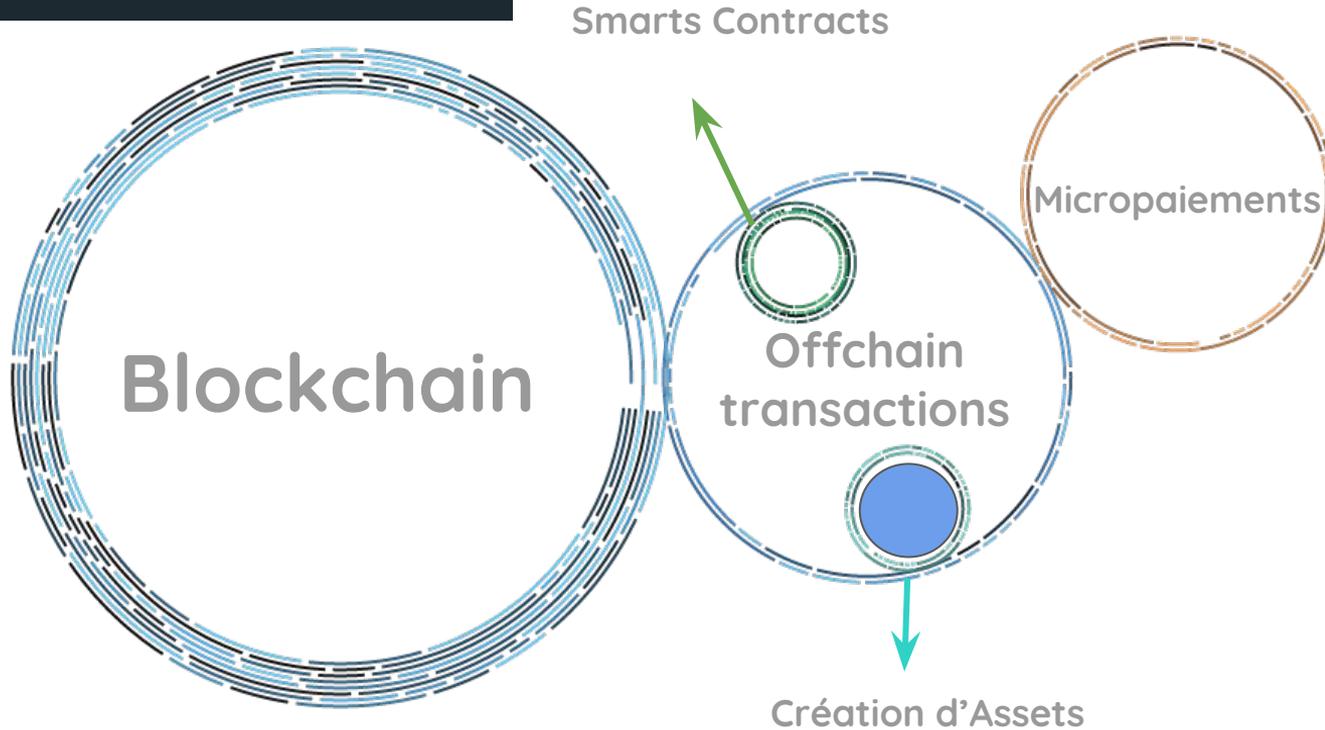


Share 2: 3Y2abzqHYizipmoBqS8DBTPx5cPhjnxno3P5hHKsTdyBWeb



Share 3: 3Y7orfdsop4FAw3KVTtF7BYNrnMkDa1Z2v45aYi4pFhqAJA

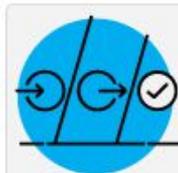




Blockstream vision



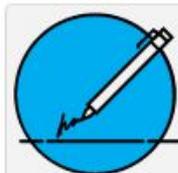
Ct
CONFIDENTIAL
TRANSACTIONS



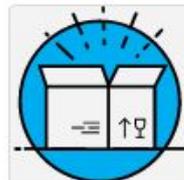
Sw
SEGREGATED
WITNESS



Rtl
RELATIVE TIME
LOCK



Ss
SCHNORR
SIGNATURES



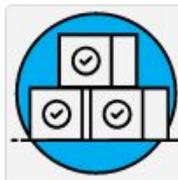
Op
NEW OPCODES



Scv
SIGNATURE
COVERS VALUE



Dp
DETERMINISTIC
PEGGS



Sb
SIGNED BLOCKS



4



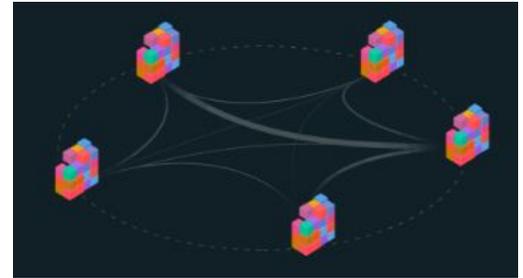
Ethereum



Pour créer :

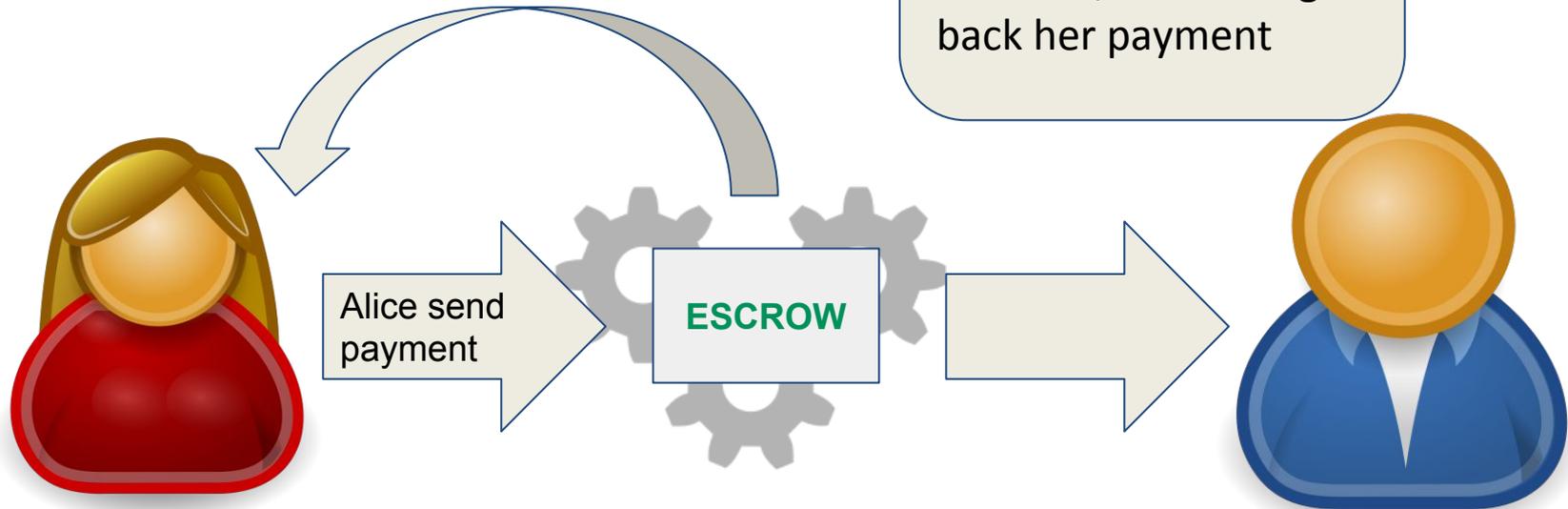
- Des applications
- Des monnaies
- Des smart contracts
- De nouvelles formes d'organisations

Un langage transactionnel complet

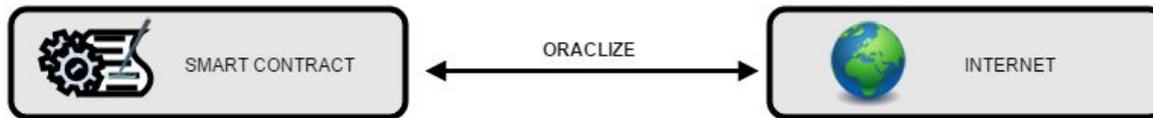


Smart contract simple

Bob receives payment only if some conditions are resolved, else Alice get back her payment



Les Oracles



Event	Multisig address	Transaction	Options	Review
1	2	3	4	5

Formula

WolframAlpha price of gasoline in Dallas * 1 litre $\lt;=gt;$ =

Check type

< 0.50

Date range

06/27/2016 11:07 AM - 06/28/2016 11:07 AM

Interval between checks

1m + 143.9 mB	10m + 14.4 mB	1h FREE
1d FREE		

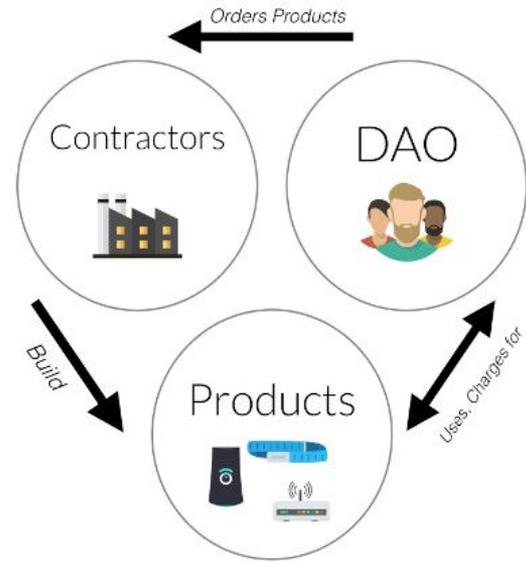
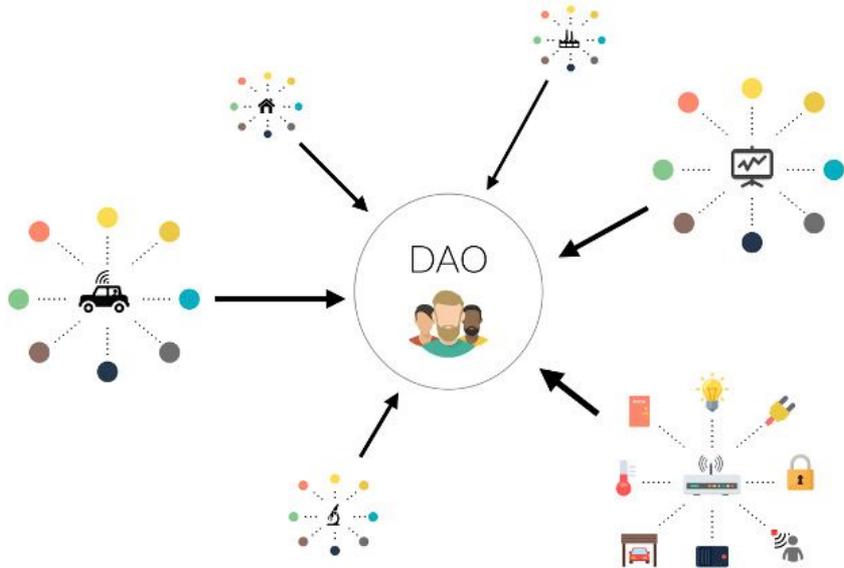


Vlad Zamfir @VladZamfir · 4 mars

Ethereum isn't safe or scalable. It is immature experimental tech. Don't rely on it for mission critical apps unless absolutely necessary!

« Ethereum n'est ni sûr ni "scalable". C'est une technologie expérimentale et immature. Ne vous y fiez pas pour des missions d'applications critiques à moins d'absolue nécessité ! ».





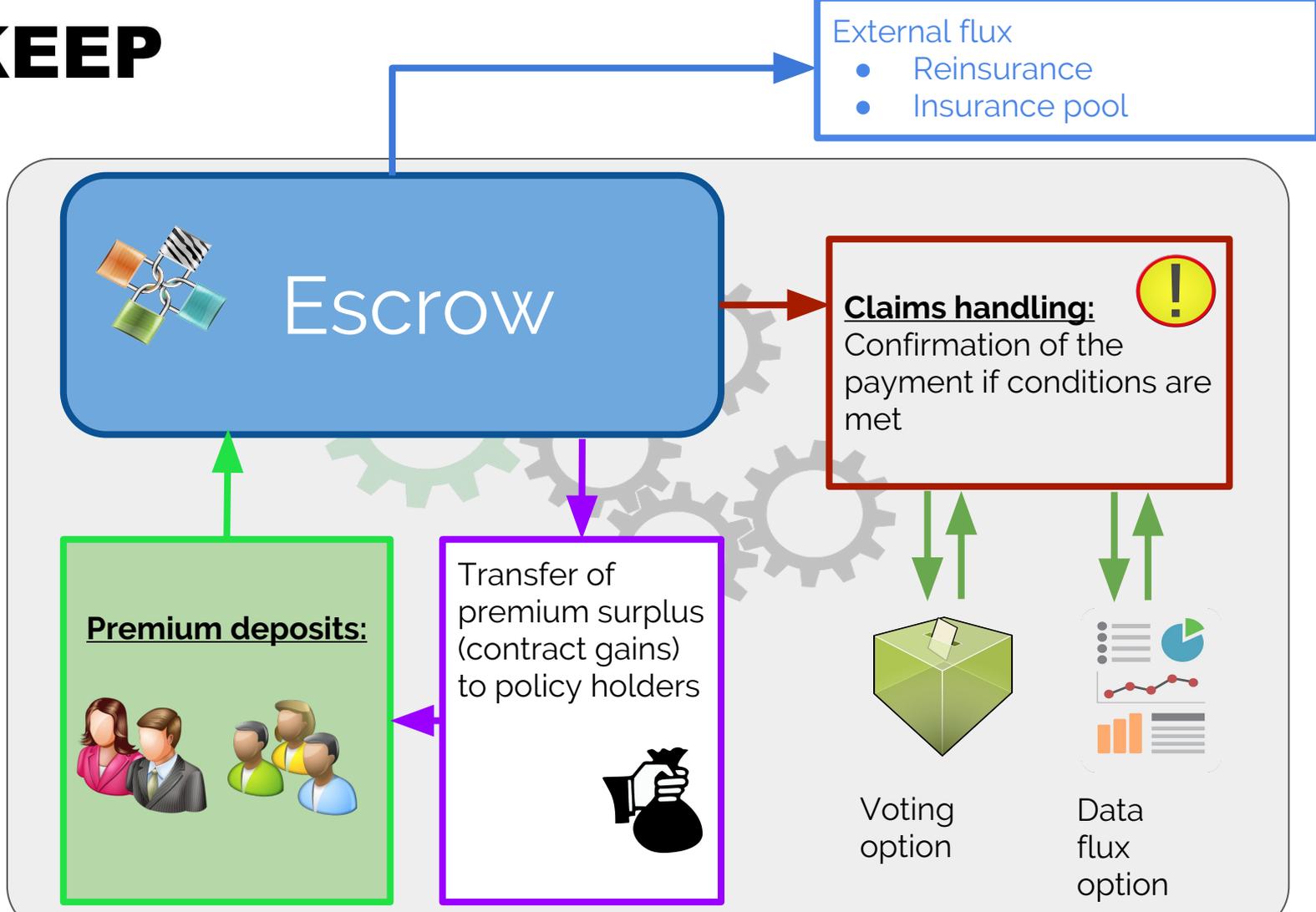
4

About Insurance

Les initiatives et freins



WE KEEP

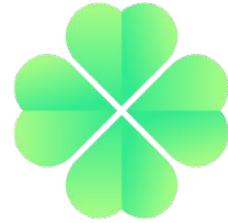


DYNAMIS

A PEER TO PEER INSURANCE COMPANY

Dynamis APP (dynamisapp.com) est un projet d'assurance chômage aux US qui utilise la blockchain pour la gestion des fonds et LinkedIn pour le suivi des membres.

5



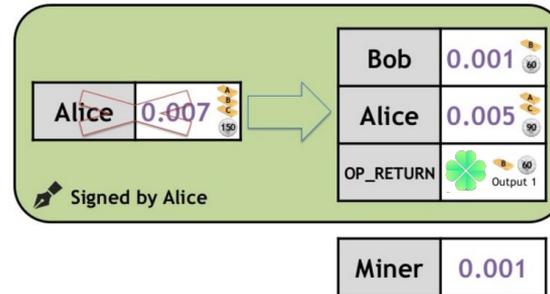
Czam

Coloredcoins & Czam

Quelques mots sur le protocole

ColoredCoins permet de :

- créer des actifs
- les transférer
- Les gérer



Que fait Czam ?

Copay

Transfert de valeurs

- Monnaies Locales
- Monnaie Internes
- Points de fidélité
- Titres financiers

Billeterie

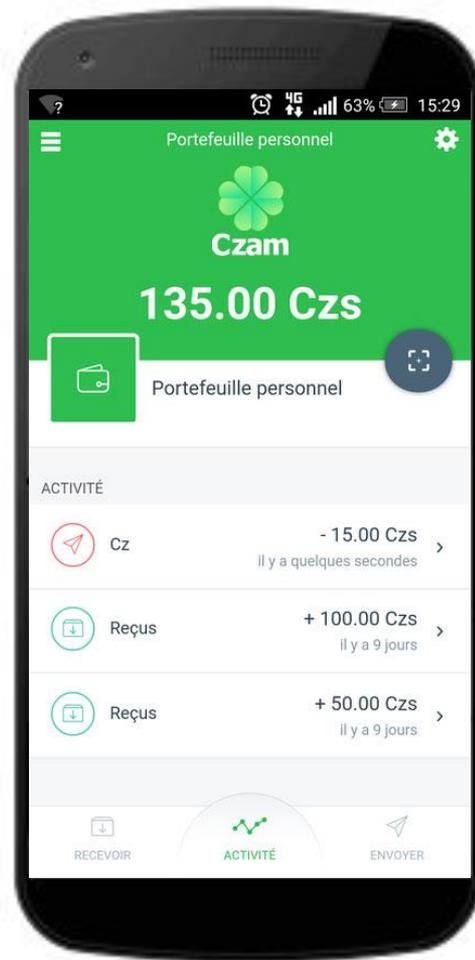
- Places spectacles
- Contrôle d'accès
- Billets de train
- Bons d'achat

Communauté

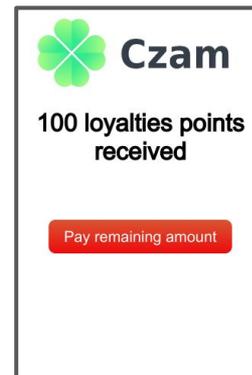
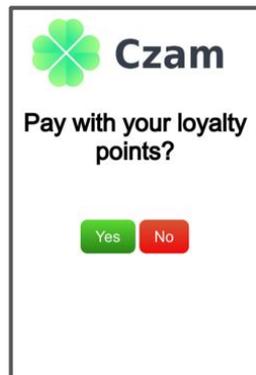
- Vote électronique
- Animation de réseaux-sociaux

Certification

- Certificats d'authenticité
- Systèmes anti-contrefaçon



Paiement in-store



Paiement Web

CHOISISSEZ VOTRE MÉTHODE DE PAIEMENT

Résumé Identifiez-vous Adresse Frais de port Paiement

MERCI DE CHOISIR VOTRE MOYEN DE PAIEMENT AFIN DE RÉGLER LA SOMME DE 21,75 € TTC

 Payer par chèque (le traitement de la commande sera plus long)

 Payer avec vos points Czam

Payer par carte bancaire
Vous utilisez le formulaire sécurisé standard SSL, choisissez une carte ci-dessous

« Précédent



Questions !

Adrian Sauzade

Co-Fondateur de Czam

Fondateur de Wekeep

adrian@czam.me

[adrian_sauzade](https://twitter.com/adrian_sauzade)

