



Webinar Mercatel - Market Pay

Cryptomonnaies : quelles perspectives ?



11 mai 2022

Rappel des bonnes pratiques pour la tenue des réunions à distance



Coupez votre micro (sur votre ordinateur et/ou téléphone) pour éviter les bruits parasites



Utilisez la fonction « Chat » pendant la session pour partager vos remarques et poser vos questions. Elles seront ensuite reprises par le modérateur et transmises aux intervenants



En fin de présentation, lorsque la session questions/réponses sera ouverte, vous pourrez rouvrir vos micros. Annoncez votre prénom et nom lorsque vous intervenez



Présentation des intervenants



Faustine FLEURET Présidente et CEO ADAN (Association pour le Développement des Actifs Numériques)



Hubert de VAUPLANNE Avocat Kramer Levin Naftalis & Frankel LLP



Aude VICAIRE Membre du Comité Exécutif Produits – Solutions – Marketing & Com Market Pay





Jean-Michel CHANAVAS Délégué Général Mercatel



Introduction

Eléments de marché sur les crypto-monnaies

- Valorisation de l'ensemble du marché: 1 500 milliards de dollars. 3 000 milliards de dollars en 2021
- Plus de 15 000 crypto-monnaies
- Plus de 1 000 blockchains différentes
- Le marché crypto est très corrélés à la situation économique et géopolitique globale. Quelques exemples impactants :
 - La guerre en Ukraine
 - L'interdiction du minage en Chine
 - L'évolution des taux directeurs au Etats Unis

Ancrage progressif dans la vie réelle

- Émergence de projets blockchain pour répondre aux cas d'usage des entreprise et des particuliers. Quelques exemples :
 - plateforme d'enchères d'énergie
 - gaming
 - assurance
 - paris en ligne
 - propriété intellectuelle
- Mais surtout : permettre aux possesseurs de crypto la possibilité de payer avec dans la vie réelle





Première partie

Origines et état actuel



Premier concept: la blockchain

Les technologies blockchains sont une famille de technologies de registres distribués (DLT).

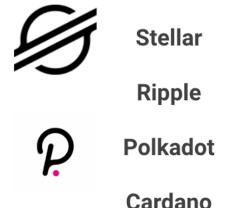
Par le biais du **consensus**, une **DLT** organise la synchronisation et la réplication d'un ensemble de données par des nœuds dans un réseau pair-à-pair, et dans le but de valider les transitions.

La genèse des blockchains avec consensus : Bitcoin

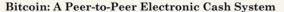
Bitcoin (et le bitcoin) a été créé par Satoshi Nakamoto, une personne ou un groupe de personnes anonymes, qui en a publié le *white paper* en octobre 2008. Objectif : concevoir un véhicule technique permettant de restaurer la vie privée et le libre échange (d'informations et de valeurs) sur la base des revendications originales des crypto-anarchistes.

Mais Bitcoin n'est qu'un réseau blockchain parmi d'autres!









Satoshi Nakamoto satoshin@gmx.com 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 proof-of-work chain as proof of what happened while they were gone.

Premier concept: la blockchain

Les principales caractéristiques d'une blockchain

- Un réseau pair à pair
- Un régime immuable et infalsifiable
- Un consensus décentralisé
- Des smart contracts (pas systématiquement)
- Des crypto-actifs (pas systématiquement)



Mrs A signs and sends "transaction 1" to the blockchain



"Transaction 1" is added to block X, along with other transactions, by one validator



Block X is broadcast to all participants in the blockchain



Participants validate block X





Mr B receives crypto from Mrs A

Block W transaction 1 transaction 2 transaction x

Block X is added to the blockchain

Block X transaction 1

transaction 2

transaction x



	BTC	$\frac{\mathbf{W}}{ETH}$	PoS	DPoS	PoET	PBFT et variantes
Matériel spécifique	ASIC	GPU	-	-	SGX	-
Type de		olique	Publique	Publique	Publique	Privée
blockchain	(permissionless)		et privée	(permissionless)	et privée	(permissioned)
Finalité de	Probabiliste		Probabiliste	Probabiliste	Probabiliste	Immédiate
transaction						
Débit de	Faible		Élevé	Élevé	Moven	Élevé
transaction			Die te	23.010	1.10,7011	210.0
Coin/Token	Oui		Oui	Oui	Non	Non
nécessaire?				oui	11011	1.01
Coût de	Oui		Oui	Oui	Non	Non
participation?			0 4.1		11011	11011
Consommation	Oui		Non	Non	Non	Non
énergétique?						
Scalabilité	Élevée		Élevée	Élevée	Élevée	Faible
du réseau						
Modèle de	Sans confiance		Sans confiance	Sans confiance	Sans confiance	Semi-confiance
confiance				Source Commence	Stills connuince	
Tolérance	<=25%		Dépend de	Dépend de	_	
aux fautes byzantines			l'algorithme	l'algorithme		<=33%
et à la compromission			spécifique utilisé	spécifique utilisé		
Niveau de	Très élevé		Faible	Élevé	Inconnu	Moyen
sécurité						
Niveau de	Moyen		Élevé	Très élevé	Moven	Faible
décentralisation			Lieve	1100 01010	oyen	Taioiq

Différents protocoles de consensus

Source: Medium

Signer une transaction « on-chain »





Second concept: les cryptomonnaies

Le point commun à tous **crypto-actifs** réside dans leur inscription sur un support **blockchain** permettant de garantir sous certains conditions :

- leur **permanence**;
- leur **unicité**, par la protection contre la duplication et la double dépense ;
- leur appréhension directe sans intermédiaire.

Cependant, les crypto-actifs sont une classe d'actifs très hétérogènes : leur design, leur utilité et leur finalité peuvent être très différentes.

L'émission et l'échange d'actifs sur les réseaux blockchains : quels **intérêts** ?

- Transparence
- Traçabilité / auditabilité
- Automatisation / Programmabilité (smart contract)
- Prévisibilité : se coordonner autour de règles sans besoin de confiance entre les participants
- Efficience (rapidité / économies)
- Innovation ouverte, stimulée
- Robustesse technologique



Second concept: les cryptomonnaies

Trois grandes familles de crypto actifs

Centralisation faible Les crypto monnaies originelles (Bitcoin etc.) Monnaies digitales décentralisées Valeur volatile, supports plutôt spéculatifs Plus des actifs que des instruments transactionnels pour payer

ethereum

bitcoin

Centralisation moyenne

Les Stablecoins

Monnaies digitales centralisées

Initiatives d'émetteurs privés

Valeur assise sur une contrepartie équivalente :

- Des devises (USD, EURO, YEN) (1)
- La valeur d'autres assets de référence (cours du blé, cours de l'or)

Des instruments à vocation transactionnelle → effectuer des règlements instantanément à travers le monde







USDCoin

Libra

Centralisation forte

Les MDBC (ou CBDC) (2)

Monnaies digitales de banques centrales

Monnaies émises centralement

Initiatives des banques centrales

Vocation transactionnelle

- Règlements « de masse » → vocation interbancaire d'abord
- Règlement de détail à terme → transactions courantes par la suite.

Contrer la menace des initiatives privées et maintenir la souveraineté monétaire des Etats





litecoin



Deuxième partie

Le paiement crypto : enjeux et opportunités pour les marchands



Ambitions du paiement crypto

- Simplifier la chaîne du paiement : moins d'acteurs → plus d'efficience et moins de coûts
- Permettre à l'utilisateur d'utiliser ses crypto-actifs dans l'économie réelle
- Profiter des caractéristiques uniques de la blockchain pour le paiement
 - Paiement instantané
 - Disponible 7/24
 - Incontestable et définitif
 - Flexible
 - Global
- Un développement en 2 étapes :
 - Dans un premier temps: acceptation des crypto par le marchand mais financement en FIAT
 - Dans un second temps: acceptation et financement du marchand en crypto



Opportunités pour le marchand

- Réduire les coûts du paiement
- Développer un nouveau canal de paiement :communication sur innovation produit
- Des plafonds de paiement plus élevés : augmentation de la dépense moyenne
- Des transactions incontestables : enregistrement dans la blockchain
- Une gestion plus souple de la trésorerie : fonds disponibles 24/7, transfert à faible coût et cross border immédiat, diminution des frais bancaires
- Placement de la trésorerie en crypto-actifs pour génération d'un revenu complémentaire



Troisième partie

Le paiement crypto, points d'attention et recommandations



Principaux points d'attention!

1. Un cadre législatif encore en construction

- Une réglementation propre à chaque pays
- Qui ne correspond plus à ces nouveaux actifs
- Le texte réglementaire européen MICA en discussion

2. Protéger le marchand des risques de fraudes / blanchiment

- Préjugés sur les crypto-monnaies
- Risques réel et obligations légales pour les marchands
- De nombreux outils à leur disposition pour limiter les risques

3. Comprendre la fiscalité associée à cette nouvelle monnaie

- Le fonctionnement de la taxation sur les plus-values
- Existence d'outils d'accompagnement
- Un non problème pour la phase 1 d'adoption du paiement crypto avec un financement en FIAT (€)



Choix du prestataire et solution idéale

4. Préférer des acteurs reconnus du paiement

- L'émergence de nouveaux acteurs de paiement
- Une adaptation nécessaire des marchands
- Préférer un acteur historique qui intègre la crypto dans sa solution omnicanale



Notre vision

Notre vision : un stablecoin / MDBC pour le paiement de demain

- Notre vision de la monnaie idéale est encore absente à ce jour
- Collatéralisée 1:1 en euro
- Encadrée et reconnue par les instances européennes
- Possédant un réseau d'acceptation global
- Émise par une structure fiable, identifiable et compétente

