# BITCOIN

## CLEF PRIVÉE ET CLEF DE VOUTE

PAR ADLI TAKKAL BATAILLE
ET JACQUES FAVIER

P2P FESTIVAL - PARIS
LE 8 JANVIER 2020

# CLEF DE VOUTE ?

## PLAN

I - Le Bitcoin en 10 minutes

II - Le Bitcoin comme cheval de Troie du pair à pair.

III - Débat

I

# LA RÉVOLUTION BITCOIN

## BITCOIN EST UN OBJET MULTIPLE

# HISTOIRE

## UNE LONGUE ROUTE

**1997**

HASHCASH PAR ADAM BACK
Hashcash et principe de preuve de travail (proof-of work)

**1998**

B-MONEY PAR WEI DAI
Utilisation du principe de hashcash et de l'horodatage.
Système P2P.

**2005**

BITGOLD DE SZABO
Principe similaire à B-Money. Les puzzles mathématiques sont toujours l'unité monétaire.

**2008**

BITCOIN PAR SATOSHI NAKAMOTO
La publication du papier fondateur de Bitcoin :
*Bitcoin, a peer-to-peer electronic cash system*
par Satoshi Nakamoto

# UN OBJET MULTIPLE

## PROTOCOLE ET JETON

**Bitcoin EST UN PROTOCOLE :**

- Comme HTTP
- Modèle de communication
- Implémentations libres (logiciels)
- Un réseau (une communauté et du matériel)

**bitcoin EST UNE UNITÉ :**

- Des jetons (bitcoins)
- Infalsifiables
- Transférables (la propriété)
- Conservables
- Limités (21 Millions)
- Avec une valeur
- Inscrits sur un livre de compte : la *blockchain*

# LE FONCTIONNEMENT

## COMMENT ÇA MARCHE ?

**UN SUBTILE ÉQUILIBRE DE PLUSIEURS TECHNOLOGIES:**

- La cryptographie asymétrique
- La fonction de hachage
- Le pair-a-pair

**CELA PERMET D'AVOIR UN RÉSEAU :**

- Sûr grâce aux clefs et signatures
- Résistant et incensurable car décentralisé et distribuée
- Autonome grâce au minage (proof-of-work)
- Fiable, transparent et immuable grâce à sa Blockchain

EX

# DERRIÈRE LE RÉSEAU

## DES HOMMES ET DES MACHINES

BITCOIN P2P FESTIVAL | 01/2020

# QUE FAIRE AVEC ?

## USAGES MONÉTAIRE ET EXTRA-MONÉTAIRES

**Ouvrir un compte avec seulement une connexion internet.**

**Envoyer de l’argent partout dans le monde instantanément.**

**Ouvrir des comptes communs très simplement.**

**Programmer la monnaie pour effectuer divers opérations. (smart contract / monnaie machine)**

**Effectuer des preuves d’existence.**

**Voter en ligne.**

**Micro-transactions et monnaie internet.**

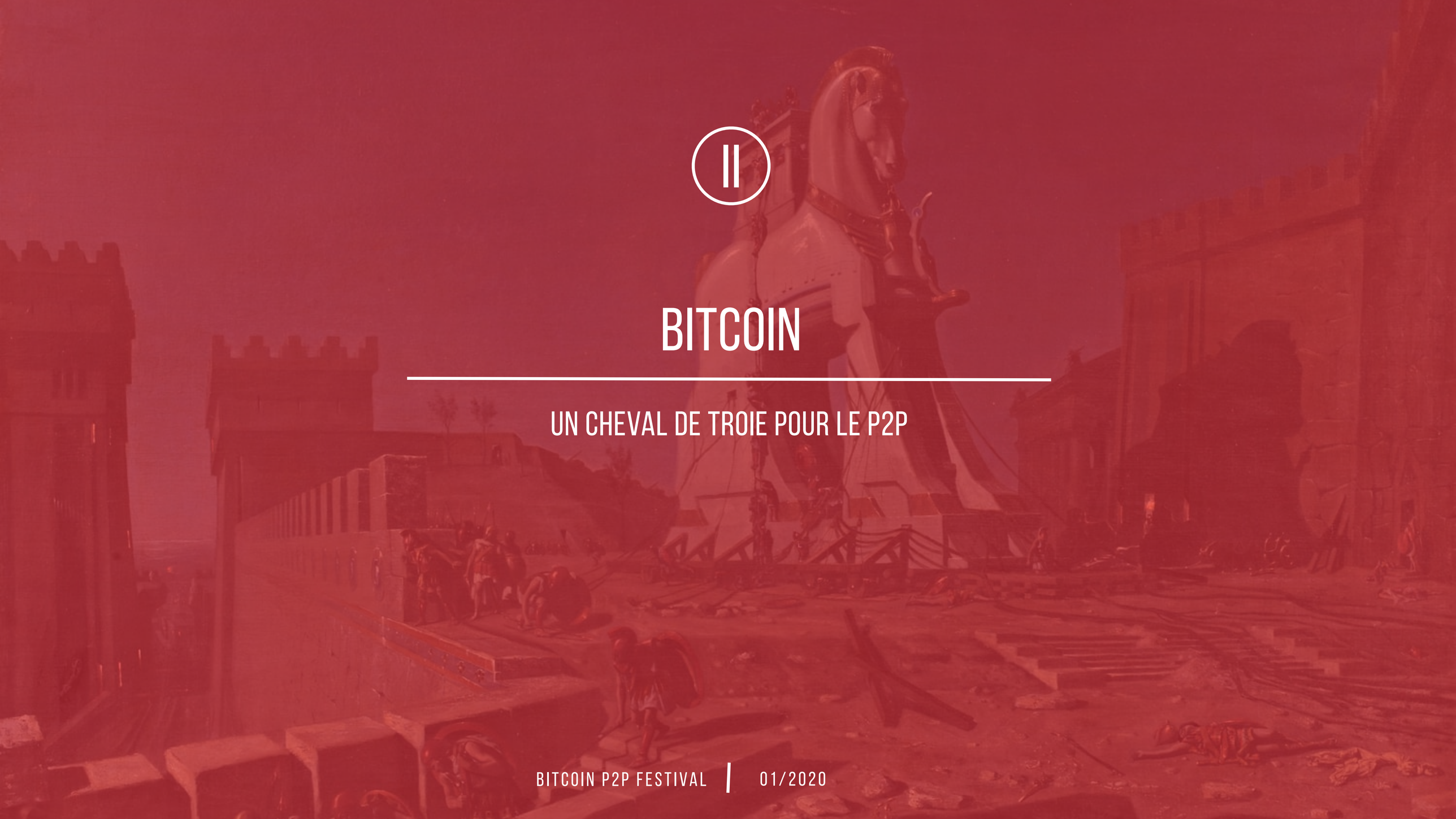
**Créer des assets (fonds/actifs) personnalisés.`**

**Authentifier des personnes.**

**Et bien d’autres à inventer ...**

# UNE NOUVELLE COSMOLOGIE

DES RÉSEAUX **HORIZONTAUX** ET **AUTONOMES**
AU **CONSENSUS DÉCENTRALISÉ**



II

# BITCOIN

## UN CHEVAL DE TROIE POUR LE P2P

# PROOF OF KEY

## PRISE DE CONSCIENCE

**LE BITCOIN INTRODUIT UNE LOGIQUE DE GESTION DES CLEFS LÀ OÙ CELA N'ÉTAIT PAS UNE NÉCESSITÉ :**

- La **prise de conscience** sur la notion d'intégrité et de propriété numérique. Le courrier semble avoir moins d'impact que l'épargne. (*not your keys, not you property*)

**Bitcoin en tant que propriété numérique permet d'attirer de nombreuses personnes en dehors des sentiers habituels du P2P. Ces personnes sont alors confrontés à des problèmes qui n'avaient pas d'importance pour eux ou qu'ils n'avaient pas identifié.**

# PROOF OF KEY

## PRISE DE CONSCIENCE

CELA PERMET UNE PRISE DE CONSCIENCE :

- **L’identité** peut être un bien que les personnes se réapproprient via la gestion d’un porte-clefs numérique. L’usage systématique de la cryptographie asymétrique dans les cryptomonnaies force l’utilisation de ces principes essentiels à un monde réellement P2P.
- **De nombreuses solutions** sont développés pour faciliter l’usage de la cryptographie asymétrique avec du hardware dédié (même si cela existait avec les YubiKey par exemple).
- Un énorme travail **d’éducation** est fait car le fait de ne pas posséder ses clefs et un véritable vecteur d’attaque.

**Bitcoin agit donc comme un révélateur sur la notion de clef privée. Permettant alors l’émergence d’une société qui a pour socle des identités numériques avec souveraineté.**

# MARGINALITÉ DORÉE

## RENDRE LA R&D LIBRE POSSIBLE

**LE SUCCÈS DU BITCOIN A RENDU SA COMMUNAUTÉ RICHE ET PEU AVERSE AU RISQUE :**

- Le développement du Bitcoin est **auto-financé** et c'est le cas pour de nombreux autres projets dont les capitaux sont immenses.

**Cela permet pour peut-être la première fois dans l'histoire de rendre viable de la recherche et développement au niveau protocolaire.**

# MARGINALITÉ DORÉE

## RENDRE LA R&D LIBRE POSSIBLE

**LE P2P A TOUJOURS SOUFFERT D'UNE CERTAINE DIFFICULTÉ À TROUVER DES MODÈLES ÉCONOMIQUES VIABLES ET PERMETTANT UN FORT EFFET DE RÉSEAU.**

- **Les dons** sont un système qui a montré parfois sa force comme avec Wikipedia mais dont on connait également les faiblesses sur le long terme face aux puissances économiques numériques
- Bitcoin permet **de financer massivement de la R&D** sans aucune limite. Cela a permis une véritable explosion cambrienne du développement de protocoles bas niveau.
- La recherche n'est plus cantonnée à du court terme.
- **L'alignement des intérêts** est au coeur de la majorité des projets et permet de ne plus concentrer la richesse sur une seul entité mais de la partager en réseau
- La **collectivisation des revenus** à grande échelle permet la baisse des prix de l'intermédiation, car le réseau devient en quelque sorte un intermédiaire en soi. Permettant un vrai P2P non prédateur.
- Les projets peuvent ne plus avoir de limite de par **l'incensurabilité** des protocoles et leur résilience.
- La nécessite d'une certaine **accessibilité**.

# GOUVERNANCE

## UNE QUESTION OBLIGATOIRE

**LA OÙ LE P2P SOUFFRAIT DE PROBLÈME DE GOUVERNANCE ET DE GESTION DES PROJETS, BITCOIN APPORTENT UNE POSSIBILITÉ DE GESTION DES BIENS COMMUNS.**

- Bitcoin de part son **essence décentralisée** mais aussi sa valorisation a permis de véritablement se poser la question de la **gouvernance** et des enjeux que cela suppose.

**C’est une véritable révolution dans le P2P où il a toujours régné une certaine difficulté à s’organiser a grande échelle sans en revenir à un système centralisé.**

# GOUVERNANCE

## UNE QUESTION OBLIGATOIRE

**BITCOIN ET LES CRYPTOMONNAIES SONT DES RÉSEAUX AVEC UNE GOUVERNANCE DÉCENTRALISÉE PLUS OU MOINS ORGANISÉE LÀ OÙ CELA ÉTAIT FORT COMPLEXE SANS CHAÎNE DES ÉVÈNEMENTS ET IDENTITÉS.**

- Bitcoin apporte la possibilité de s'organiser et à **motiver des mises à jour logiciel** de bas et de haut niveau.
- D'autres projets comme Tezos vont jusqu'à intégrer la **gouvernance dans le protocole même**. Les réseaux deviennent alors eux aussi souverains et autonomes, en plus des individus.
- **Le modèle est réplicable** à souhait et permet de penser son adaptation pour de nombreuses organisations dont la gouvernance est complexe de part leur nature décentralisée et P2P. L'âge des **DAO**.

**Bitcoin est donc un véritable labo de la gouvernance à grande et petite échelle, ce qui permet d'entrevoir un monde où le P2P est possible à la fois grâce à la souveraineté individuelle mais aussi à la souveraineté des réseaux P2P.**

# UNE CLEF DE VOUTE

## OU UN CHEVAL DE TROIE

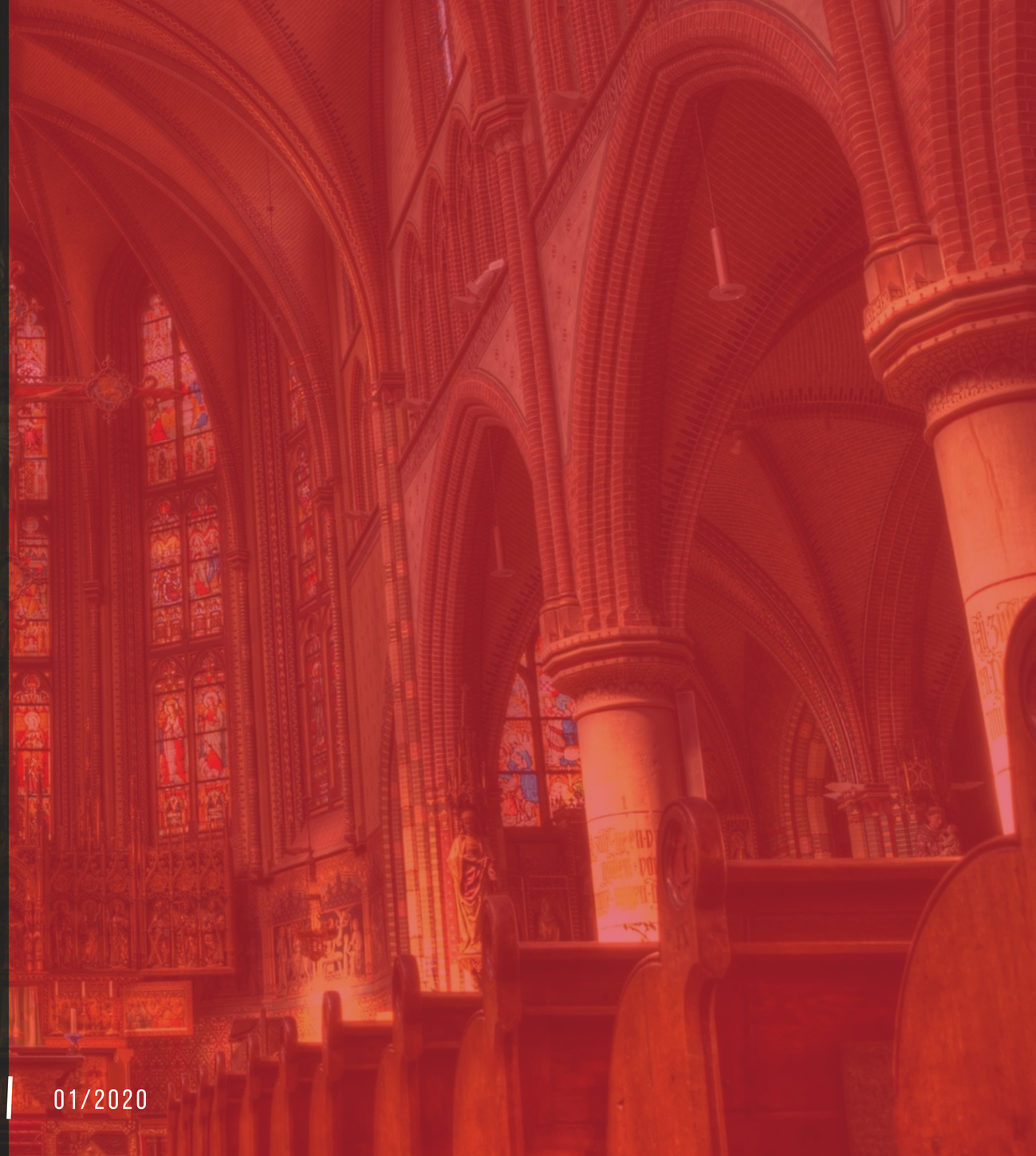
**BITCOIN EST BIEN SOUVENT DÉCRIÉ OU MIS AU BAN POUR SA RÉVOLUTION MONÉTAIRE. APPORTANT UNE VÉRITABLE ALTERNATIVE A LA MONNAIE FIAT ET PERMETTANT UNE SOUVERAINETÉ TOTALE SUR LA VALEUR.**

Mais lorsque le sage montre la lune, l'idiot regarde le doigt. En ce sens Bitcoin est **un cheval de troie**, car même si l'impact monétaire est fort conséquent, l'impact sur les **usages sociétaux** du numérique peut être encore plus fort.

Ainsi Bitcoin est **une clef de voute pour le P2P** et le cyberespace permettant enfin une émancipation des individus et surtout des groupes d'individus grâce à des **briques technologiques essentielles au P2P** qui n'avait, soit pas trouvées leur public, soit pas vue le jour, soit n'étaient pas assez accessibles.

**Bitcoin est la première pierre de l'édifice d'une future société P2P et décentralisée** et c'est comme ça que nous devons le considérer, même si c'est une aubaine qu'il soit juste aperçu comme une prédateur des monnaies.





# CONCLUSION | QUESTIONS ? DÉBAT

## MERCI DE VOTRE ATTENTION

## IMPLICATION

## LE CERCLE DU COIN

ESPACE FRANCOPHONE


BITCOIN, LA MONNAIE ACÉPHALE.
ÉDITIONS DU CNRS
HTTPS://BITCOINLAMONNAIEACEPHALE.FR


BITCOIN, MÉTAMORPHOSES.
ÉDITIONS DUNOD


BITCOIN & PROTOCOLES À BLOCKCHAIN
ÉDITIONS MARDAGA