# Blockchain & Monnaie numérique de banque centrale (MNBC)

# Implémentation sur le protocole Bitcoin[SV]

Une fondation pour le projet MNBC de la Banque du Canada

**Par** : Pascal Ngu Cho, BA-GIS/Consultant Blockchain Senior

23/10/2020

## A- Introduction

Les autorités financières mondiales comme la Banque mondiale, le FMI et les 20 plus grandes économies du monde travaillent à établir des normes et standards pour réglementer et émettre des monnaies numériques souveraines. Dans un rapport [1] publié le 13 octobre 2020, le G20 prévoit d'ici fin 2022 terminé le cadre réglementaire autour des monnaies stables [stablecoins], ainsi que la recherche, la conception et l'expérimentation des monnaies numériques de banque centrales (MNBC) ou encore CBDC.

En vue de moderniser les systèmes de paiements, la Banque du Canada, tout comme plusieurs autres banques centrales a annoncé effectué des travaux sur une éventuelle émission d'une monnaie numérique de banque centrale. En février 2020, elle publiait son plan de prévoyance[2] advenant le lancement d'une MNBC.

Compte tenu du fait que la monnaie est un bien publique et que la Banque du Canada aura besoin de l'approbation du gouvernement et de l'acception du public pour assurer son adoption, nous présentons dans ce papier notre contribution au projet, en **proposant un protocole, une infrastructure et un écosystème opérationnel** capable de répondre aux exigences techniques du plan de prévoyance de la Banque du Canada : **Le protocole Bitcoin[SV]**

"*Pour l'instant, la Banque n'envisage pas d'émettre de MNBC. Toutefois, elle se dotera des moyens nécessaires pour pouvoir émettre une MNBC à usage général, semblable à de l'argent comptant, si le besoin s'en faisait ressentir. Comme cela demandera plusieurs années, elle ne peut pas attendre que le besoin soit manifeste avant de commencer. Il est essentiel qu'elle commence à se préparer à une telle éventualité. En même temps, elle anticipe divers changements possibles dans les domaines de l'argent et des paiements au Canada, à mesure que l'innovation se poursuit*"

Plan de prévoyance concernant une monnaie numérique de banque centrale

[1] https://www.fsb.org/2020/10/regulation-supervision-and-oversight-of-global-stablecoin-arrangements
[2] https://www.banqueducanada.ca/2020/02/plans-prevoyance-concernant-monnaie-numerique-banque-centrale/?_ga=2.241875842.1413365133.1603210325-2022147350.1579613322

## B- Caractéristiques principales du protocole Bitcoin$^{sv}$

Le protocole Bitcoin$^{sv}$ ou BSV pour Bitcoin Satoshi Vision, repose sur 4 piliers pour créer un système électronique de paiement et de transfert de donnée: **la stabilité, l'évolutivité, la sécurité et les transactions instantanées**.

**1- La stabilité:** La vision de Bitcoin$^{sv}$ est de fournir une stabilité au protocole. Un nombre de changement à être apporté pour restaurer sa conception d'origine et permettre à l'innovation de se faire sur une base stable. Les entreprises ont besoin d'un système stable pour engager des investissements et des ressources. C'est ce que offre aujourd'hui Bitcoin$^{sv}$.

**2- L'évolutivité ou montée en échelle :** Pour assurer sa monté en échelle, comparativement aux autres protocoles de la Preuve de travail (PoW), Bitcoin$^{sv}$ a fait le pari des gros blocs. Ce choix lui permet de traiter des milliers de transactions à la seconde, voir des millions à l'avenir. Être capable de monter en échelle et offrir des transactions à haut débit est important pour convaincre les entreprises d'utiliser Bitcoin$^{sv}$ pour développer des applications blockchain.

En éliminant la limite sur la taille des blocs, Bitcoin$^{sv}$ maximise le volume des transactions et fait passer le modèle de revenus des mineurs de la récompense vers les frais de transactions. Une plus grande taille des blocs permet aussi de mettre toutes les transactions et toutes les données sur chaînes.

**3- Sécurité :** Bitcoin$^{sv}$ est conçu pour être une monnaie mondiale, un registre unique, une source de vérité unique. Il doit être prêts à garantir un niveau de sécurité à la hauteur d'un système monétaire mondial. Les mineurs (producteur et validateur de blocs) sont tenus à offrir des services fiable et disponible 24/7. Une monnaie numérique mondiale doit offrir la confiance. Il ne doit pas changer au gré des développeurs, ni au gré des politiques. Il doit répondre aux attentes d'un système capable de perdurer pendant plusieurs décennies. C'est ce que offre aujourd'hui Bitcoin$^{sv}$.

**4- Transactions instantanées :** Les transactions instantanées sont importantes pour les paiements électroniques dans les commerces. Aujourd'hui, Bitcoin$^{sv}$ traite des transactions de manière instantanée et sécuritaire grâce à l'implémentation du protocole SPV (Simple Payment Verification). La vérification de paiement simple ou SPV est une technique décrite dans le livre blanc de Satoshi Nakamoto qui permet à un client léger, sans télécharger le registre entier de vérifier qu'une transaction est incluse dans la chaîne de bloc. À l'avenir, Il est possible d'apporter des améliorations de sécurité pour mieux traiter des transactions instantanées.

# C- Comment le protocole Bitcoin$^{sv}$ répond aux exigences du plan de prévoyance pour une MNBC?

Dans son plan de prévoyance, la Banque du Canada a identifié des caractéristiques techniques que devrait intégrer une éventuelle MNBC. Nous présentons ici comment le protocole **Bitcoin$^{sv}$** répond à ces exigences techniques :

## 1- Monnaie comparable à l'argent comptant.

**Bitcoin$^{sv}$** (BSV) est un système électronique de paiement pair-à-pair qui fonctionne comme l'argent comptant. Cela est possible parce que tout le monde n'a pas besoin d'être un mineur, mais les individus peuvent effectuer des transactions entre eux directement et rapidement vérifier qu'un noeud a reçu la transaction. Sur le réseau BSV, les mineurs forme la couche de règlement. Les transactions pair-à-pair sont confidentielles mais pas anonyme. Le système est accessible à tous et offre un niveau de résilience qui a fait ses preuves depuis 10 ans. À une échelle mondiale, il devient résilient et fonctionne aussi bien que les systèmes de carte de crédit tout en offrant beaucoup plus : confidentialité, faible coût et capacité programmatique. Aujourd'hui et selon blocktivity[3], Bitcoin$^{sv}$ traite quotidiennement +2M de transactions/jour.

> "*Bitcoin is designed to be stable money and for that reason it is not designed to have new opcodes added outside the need for a new security based replacements or to be altered*"
>
> Craig Wright in 'The Art of Bitcoin'

## 2- Accessibilité universelle.

Bitcoin$^{sv}$ est conçu pour fonctionner en ligne et hors ligne. Comme monnaie numérique, il a l'avantage d'être accessible à tous parce qu'avec une simple application mobile comme *HandCash* ou *SimplyCash*, tout le monde peut y avoir accès. Dans un environnement où les services bancaires ne sont pas disponibles, le protocole Bitcoin$^{sv}$ peut servir de base pour le développement de services bancaires localisés. Permettant alors d'offrir à une population sous bancarisée ou non bancarisée des services électroniques de paiement sur un téléphone mobile. *HandCash* par exemple est pratiquement la seule application sur le marché capable de réussir à un "*test grand-mère*".

[3] https://blocktivity.info/

### 3- Stabilité

Bitcoin$^{SV}$ est un protocole stable. Il peut donc servir comme système de base pour le développement d'un système de paiement ou pour l'émission d'une Monnaie numérique de banque centrale (MNBC) adossé à une commodité. Cela accroîtrait la confiance des consommateurs tout en accélérant l'adoption. Bitcoin, tel que restauré dans le protocole Bitcoin$^{SV}$ en février 2020 peut remplacer tous les systèmes de paiement dans le monde par une meilleure expérience utilisateur, une meilleure sécurité et un coût moins cher pour les marchands. Les entreprises peuvent aussi faire confiance au protocole Bitcoin$^{SV}$ pour fournir un système stable à petite, moyenne et grande échelle. Elles peuvent donc engager des investissements et ressources pour développer des solutions d'affaires qui utilisent la blockchain Bitcoin$^{SV}$. Des entreprises canadiennes comme TAAL, ont fait ce choix pour offrir des services transactionnels de gros (wholesale) aux entreprises.

### 4- Résilience et sûreté des paiements.

Le protocole Bitcoin$^{SV}$ est un système fiable. En implémentant un système à 2 niveaux de validation (P2P), il permet d'assurer le fonctionnement des transactions dans une optique où une panne d'électricité ou de réseaux cellulaires surviendrait. D'autres moyens de transmissions seraient alors utilisés. Le déploiement d'une MNBC sur un réseau fiable, sécuritaire et conçu pour être un réseau de transfert de valeur et de données, lui permet de mettre en place des dispositifs nationaux d'opérabilités en cas de panne d'électricité ou de réseau internet.

"*I always saw how things would end up in data centers. It is part of the design. Bitcoin is about competitive corporations securing the network.*" Dr Craig Wright, nChain Chief Scientist

### 5- Confidentialité des paiements.

En utilisant un protocole stable, fiable, conçu pour monter en échelle et qui utilise la vérification simple des paiements (SPV) comme le Bitcoin$^{SV}$, il est possible de déployer une monnaie numérique de banque centrale (MNBC) qui offre la fonction de confidentialité des transactions. Cela peut se faire directement sur la couche de niveau 1 du protocole et prendre avantages des fonctionnalités de base déjà implémenter par *HandCash* ou *MoneyButton*. Bitcoin$^{SV}$ n'est pas un système anonyme. Il est conçu pour fonctionner en respect des lois et règlements.

*"Bitcoin… It is not decentralization for the sake of it, nor is it the creation of a system that removes all government and corporations."* Dr Craig Wright, nChain Chief Scientist

6- **Intégration aux systèmes de paiement existants**.

En utilisant le réseau Bitcoin$^{sv}$, une MNBC s'intégrerait aux systèmes existant compte tenu de son ouverture, de sa flexibilité programmatique et du développement de l'écosystème à l'échelle mondiale. Aujourd'hui, plus de 400 projets sont en cours de développement sur Bitcoin$^{sv}$ .

# D- Conclusion & proposition.

Bitcoin$^{sv}$ est un ordinateur mondial. Il peut exécuté n'importe quel calcul, n'importe quel contrat intelligent et accueillir des données sur chaîne. En adoptant un protocole ouvert, stable et universel pour l'émission de sa MNBC, la Banque du Canada se donne les moyens d'une une adoption sociale rapide contenu tenu de son avancée technique, de ses capacités programmatiques, de sa facilité d'utilisation, de sa réputation dans l'industrie des technologies blockchain et même de l'avantage à émettre une monnaie qui repose sur une commodité ayant toutes les caractéristique de l'argent : **Le BSV**.

Pour le développement et le déploiement d'une monnaie numérique de banque centrale réussit et compte tenu du fait qu'un système monétaire est un bien publique, qu'il forme la base des échanges, **nous proposons,** dans une éventuelle décision du gouvernement canadien d'autoriser l'émission une MNBC de :

1- Considérer les aspects qui font consensus dans l'industrie de la chaîne des blocs ou des registres distribués pour faciliter l'adoption et l'acceptation du public.

2- Soutenir la recherche et le développement des filières locales des technologique de la chaîne des blocs.

3- Favoriser des politiques qui permettent de développer des systèmes de paiements locaux du type "**Achat local, Paiement local**".

4- Favoriser le développement des monnaies numériques adossées au dollar canadien sur les principales chaînes de blocs publiques comme Bitcoin, Ethereum, EOS, Stellar, etc…

*"The existing Visa credit card network processes about 15 million Internet purchases per day worldwide. Bitcoin can already scale much larger than that with existing hardware for a fraction of the cost. It never really hits a scale ceiling."* ***Satoshi Nakamoto*** *(April 2009).*

# E- Références et ressources:

=======

- Plans de prévoyance concernant une monnaie numérique de banque centrale.

https://www.banqueducanada.ca/2020/02/plans-prevoyance-concernant-monnaie-numerique-banque-centrale/?_ga=2.241875842.1413365133.1603210325-2022147350.1579613322

- Rapport de recommandations de haut niveau du BSF (Bureau de Stabilité Financière) pour la réglementation, la supervision et la surveillance globale des monnaies numériques stables ou stablecoins.

https://www.fsb.org/2020/10/regulation-supervision-and-oversight-of-global-stablecoin-arrangements/

- Rapport de six (6) banques centrales définissant les principes fondamentaux et caractéristiques de base d'une monnaie numérique de banque centrale (MNBC).

https://www.bis.org/publ/othp33.htm

- La monnaie numérique canadienne en 5 étapes:

https://lactualite.com/techno/la-monnaie-numerique-canadienne-en-cinq-questions/

- Bitcoin$^{sv}$: https://bitcoinsv.io/

- Back2Satoshi: https://www.back2satoshi.com/

- Livre Blanc Bitcoin : https://bitcoin.org/files/bitcoin-paper/bitcoin_fr.pdf

- Livre : Satoshi's Vision, The Art of Bitcoin , Craig Wright.