Hello Aave community,

I humbly submit this proposal to add support for renBTC.

Ren Project Background

Ren Project developed and launched RenVM, a byzantine fault-tolerant protocol that provides ECDSA threshold key generation and signing via sMPC, which allows RenVM to securely manage (ECDSA) private keys of different assets like Bitcoin, and wrap these assets on smart-contract chains like Ethereum. Since launch, RenVM has processed $847m (77.8k BTC) in total volume of Bitcoin going to and from Ethereum (figures are at time of writing and are growing). renBTC comes in at 2nd place for BTC on Ethereum making up roughly 19% of the supply (22k BTC), with wBTC at 74% (89k BTC). In addition, there is over $200m (18,299 BTC) in liquidity locked in Curve pools between the Ren and sBTC pools.

renBTC is a tokenized representation of BTC on the Ethereum blockchain.

It is implemented as a standard ERC-20 contract, and backed 1:1 with real BTC locked in RenVM, a decentralized custodian. It is redeemable at any time for real BTC. Individuals can acquire renBTC by minting it with real BTC via the RenBridge.

In addition, Aave is one of the original members of the Ren Alliance and currently supports the Ren token itself

(https://medium.com/renproject/introducing-the-ren-alliance-fde594450113). Given 1) renBTC's price peg to BTC and 2) the ease at which users are able to swap between BTC, wBTC, and renBTC through the Renbridge, wbtc.cafe, and the Curve pools, the price of renBTC can quickly and easily be arbitraged to the price of BTC supporting a healthy lending and flash loan market.

RenBTC is currently supported by:

- Curve
- Yearn Vaults
- Uniswap + Mooniswap
- Uma Protocol
- Cream
- Huobi
- Pillar
- Loopring
- VirgoX

renBTC is in the process of integrating with:

- Akropolis Delphi
- Polkadot/Acala Network
- Cosmos/Terra
- Solana
- Binance Smart Chain
- Bancor
- And many more (See Ren Alliance and Ecosystem updates inRen's Medium)

About RenVM

RenVM is a byzantine fault-tolerant protocol that provides ECDSA threshold key generation and signing via sMPC. What makes RenVM unique is that it does all key management and rotation using its sMPC based protocol that the team has pioneered. The state, inputs, and outputs of all programs that RenVM runs (e.g. ECDSA private keys) are kept hidden from everyone, including the Darknodes that power it.

This allows RenVM to securely manage (ECDSA) private keys of different assets, making it possible to mint or burn

tokenized representations of these assets on external blockchains in a trustless, permissionless, and decentralized manner.

One of the core features of RenVM is bringing BTC to Ethereum (i.e renBTC). renBTC serving as collateral within the Aave ecosystem is the sole focus of this application, although RenVM also supports renBCH and renZEC.

(Citing the MakerDAO Improvement Proposal that passed

https://forum.makerdao.com/t/renbtc-mip6-collateral-application/2971)

I've pasted the TL;DR for RenVM from the Ren Wiki below:

RenVM is a decentralized crypto asset custodian that:

- enables universal interoperability between blockchains: anyone can use RenVM to send any asset to any application on any chain in any quantity.
- has robust security: large bonds, large shard sizes, and continuous shuffling make RenVM extremely difficult to attack, even for irrational adversaries. In the unlikely event of a successful attack, RenVM can restore lost funds.
- is scalable: as more assets are locked into the custody of RenVM, the algorithmic adjustment of fees allows RenVM to automatically scale its capacity to meet demand.
- provides an optimal user experience: users can interact with multiple assets, applications, and chains with only one transaction.

The benefits of onboarding renBTC for Aave include:

- Diversification of BTC assets as currently Aave only supports wBTC.
- Increased adoption of Aave usage by renBTC users.
- Increased Total Value Locked (Market Size on Aave's dashboard) with renBTC users depositing their assets as collateral.
- If renBTC is onboarded and subsequently, RenJS is integrated into Aave, Aave/renBTC users will have the abilities to directly 1) deposit/lend BTC into Aave in a single BTC transaction and 2) pay-off/withdraw real BTC in a single Ethereum transaction. An example of a RenJS integration is with Curve (https://www.curve.fi/ren/deposit)

Big thank you to @MaxRoszko for providing comments, edits, and additions during the drafting process of the proposal.

Relevant Ren Project documents below:

- Ren Project Wiki and Github
- RenVM Deep Dive with Coinmarketcap
- Official Ren Website
- Ren Twitter
- renBTC Token Contract
- Trail of Bits sMPC (Secure Multi Party Computation) audit
- MakerDAO polling proposal that passed