Bitcoin Libre: Simple, Usable Bitcoin

www.libre.org

Abstract: Bitcoin has established itself as the dominant contender for “Digital Gold” but has had limited success so far as a peer-to-peer cash system. Pegged bitcoin provides a cost effective and fast solution for everyday use, and, when combined with Lightning on-and-off ramps, could transform Bitcoin into a mass market payment system. With smart contract support, this could also facilitate the use of Bitcoin in apps for ecommerce and other uses.

The Libre DAO is set up as a decentralized collective to explore the idea of merging pegged bitcoin and lightning technologies together in a single, compelling consumer platform. All voting will be done with a fair launched token, with no pre-mine, and no tokens reserved for any specific team. The DAO will determine which blockchain(s) to use, which version(s) of pegged bitcoin to use, what fees if any should be charged to the consumer and what future development will be done, and how it will be funded.

Libre’s mission is to develop scalable solutions for Bitcoin using pegged bitcoin and Lightning. A working product, exists on both iOS and Android, which allows fee-less transfers of bitcoin, and low-cost lightning on and off ramps. The target market for the Libre wallet is South America, and the first implementation is in both Spanish and English.

1 Introduction

As Elon Musk has noted, the ecological footprint of Bitcoin, combined with the long transaction times and high transaction fees make it a less than ideal candidate for a planetary crypto currency. On the other hand, the finite supply of bitcoin, and the fair-launch mechanism of its original deployment in 2009 make it the only real contender amongst tens of thousands of “altcoins.”

In order for Bitcoin to flourish, not only as a store of value for the rich, but also as a global cryptocurrency for the unbanked, two solutions exist. The first is the lightning network, invented in 2015, which is effectively a “Layer 2” solution built on top of Bitcoin. The

second is the concept of “pegged bitcoin” - where the bitcoin is represented transparently and efficiently as a token on a smart contract that can be audited by anyone.

Both approaches are valid, but the pegged bitcoin approach is by far the most popular, measured in dollar volume. Versions of pegged bitcoin exist now on every major chain, including Ethereum, Binance Smart Chain, Polygon, Solana, Liquid, and Proton. Sending these pegged coins is near instant, and at a very low transaction cost. Using Automated Market Makers (AMMs) these pegged coins can be easily converted to stablecoins such as USDC. In some implementation schemes, the pegged coins can easily be unpegged in a self service mode, by simply sending them to a smart contract together with a destination Bitcoin address.

The integration of this pegged bitcoin system with Lightning on and off ramps is compelling. Over 3 million users in El Salvador alone have downloaded the state-run Chivo wallet, which can pay Lightning invoices. Lightning has been integrated into Twitter as a tipping mechanism, and there are multiple pure Lightning wallets that allow easy off ramps from any platform that is Lightning compatible.

2 Genesis Wallet

Two blockchain companies and some independent developers have come together to create a new app that combines pegged bitcoin, human readable @names, and smart contract authentication with Lightning and Bitcoin compatibility.

The app is live in both the iOS and Android app stores. It was built on top of the Proton Blockchain, but this is entirely hidden from the user as the app does not require you to have any Proton tokens. The only token in the app is bitcoin.

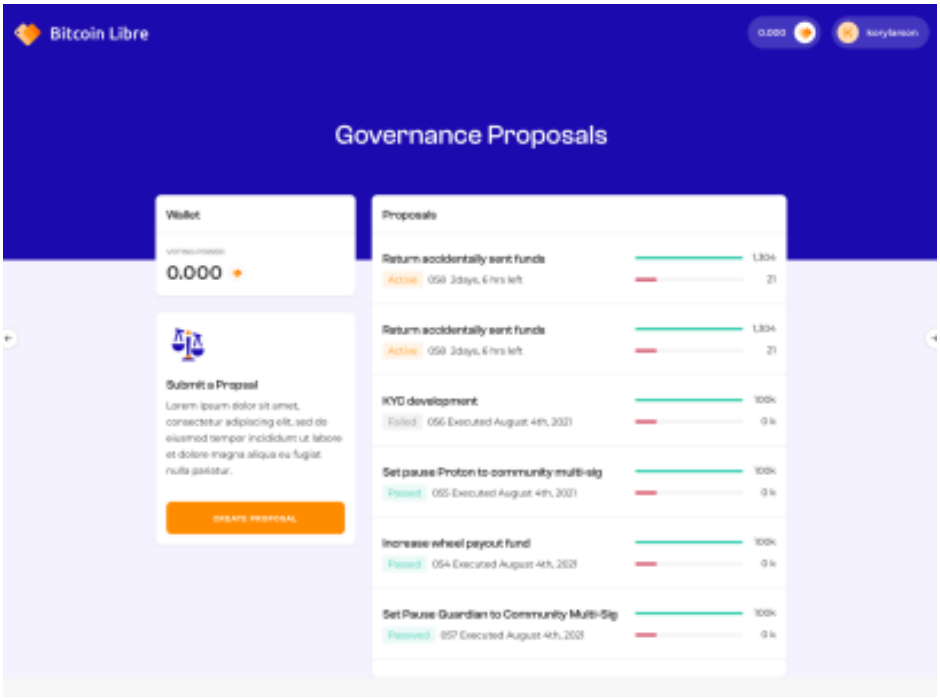
The goal of the initial product was to create a wallet that is completely lightning compatible, meaning that it can receive and pay lightning invoices, but also has the immutable @name addresses and reliability of pegged bitcoin. These @names are

critical, we believe, for mass user adoption. Like venmo in the United states, these simple human readable addresses can be easily communicated, and written on signs affixed to stores, non-profits, and marketplaces.

Because the names are allocated and saved on a blockchain, and not in a central database, there is no risk that they become hacked or corrupted. The entire underlying blockchain would need to suffer such an attack. And because Libre is a non-custodial solution, users are not at risk that the app locks them out and denies them access to their funds. In fact, all pegged coins can be accessed separately on multiple other wallets using the private key which only the user knows.

3 Libre DAO

Rather than launching and funding this company as a for-profit enterprise, the project is going to operate as a Decentralized Autonomous Organization (DAO) with a governance token that all interested parties can purchase at the exact same price in bitcoin. Once the token is initially distributed, all decisions will be determined by community voting, using a DAO voting model based on Compound.



Decentralized Governance using Libre DAO

The LIBRE token is not intended to be an appreciating store of value, or a means of

funding a centrally run project, but instead a way of decentralizing the product governance and providing all stakeholders in the Bitcoin and Lightning ecosystem a voice in where this project goes.

A decentralized governance protocol has been built that will use the LIBRE token. This model allows LIBRE token holders to make proposals, submit them for vote, and execute them to move treasury funds (bitcoin) to dev projects, or to inform the dev team of product direction. In the future, the entire codebase will come under direct control of the DAO.

4 Implementation on the Proton Blockchain

The initial version of the Libre ecosystem is built on a non-custodial mobile wallet that can send and receive bitcoin in both pegged and unpegged form. We have built this mobile wallet on the Proton Blockchain, a fast delegated proof of stake blockchain chain with free accounts, identity on chain, and optimized resources.

The core developer of Proton is MetalPay - they use Fireblocks for the bitcoin custody service. The Libre wallet makes calls to backend services on Proton to wrap and unwrap bitcoin.

The pegged bitcoin (XBTC) is completely transparent and fungible. XBTC can be swapped for Lightning BTC or on-chain XBTC by any user at any time. Anyone can also audit the amount of pegged bitcoin by looking at the address tables on the Proton block explorer and comparing it to the total of pegged XBTC.

Proton also has an identity layer with the ability to KYC users and store that status online. In the future, this may be integrated in Libre to unwrap the BTC coins. The sending and receiving of pegged bitcoin is completely non-custodial, in the exact same way that pegged bitcoin on ETH can be sent non-custodially via MetaMask.

It’s important to note that once the DAO governance takes over, the community will have full power to potentially move to a complete implementation of Libre on Lightning, move to a different blockchain, or investigate a cross-blockchain approach. In this sense there is no “roadmap” for the Libre project -- it will be determined by the community.

For the rest of this whitepaper, we will describe in more detail the features of the existing Libre wallet on iOS and Android. Note that these features can and will change subject to community vote.

5 Long term future with Lightning

Bitcoin Libre has developed its own submarine swap service to enable transactions on the Lightning Network. This service balances transactions between several Lightning nodes. We first attempted to build the app completely on Lightning, but were limited by technical, routing, and liquidity challenges that collectively created a “usability hole.”

Our hope would be for Libre’s functionality to eventually be integrated into the Lightning Network itself, making the pegged bitcoin approach obsolete. This might be possible with, for example, lnURL and lnAuth in the near future. However, this will be up to the DAO to determine.

If Bitcoin gains mass adoption with @names being the universal way to send SATS, we would consider this a success.

6 Initial Sign Up

The Initial sign up to the current version of Bitcoin Libre requires copying down a seed phrase and choosing a human readable username.

These short, human readable names are built into the Proton blockchain, and provide a significant advantage for day to day consumer transactions. This is true for peer to peer transactions between two individuals, as well as between an individual and a merchant.

7 Receiving bitcoin

Once the user has signed up, they have a simple on-chain @name address that can easily and cheaply receive bitcoin. Relatives, friends, or other personal contacts can send them pegged bitcoin in small amounts, at zero transaction costs. They can also receive bitcoin at a standard Bitcoin address, or via a Lightning Invoice. If they do that, the funds are automatically pegged and placed in the wallet.

8 Receiving bitcoin via bech32 address

Each user has a bech32 address (begins with “bc1”) that is compatible with any Segwit Bitcoin wallet or exchange. Once bitcoin is deposited here, it takes 6 confirmations on the Bitcoin network to be credited on their account where they will receive the same amount of pegged bitcoin.This is a good option to get bitcoin into the Libre ecosystem, but there are fees that can vary and even spike depending on the mempool of Bitcoin mainnet.

9 Sending bitcoin via bech32 address

Bech32 addresses are also supported for sending bitcoin. The minimum is currently 563 SATS, but that can change depending on the costs of sending a Bitcoin segwit transaction.

10 Receiving bitcoin on Lightning Network

Users can receive bitcoin via the Lightning Network by generating an invoice in bitcoin Libre. The Libre Lightning service will handle the receiving of a lightning payment to an invoice and credit pegged bitcoin to the user.

11 Sending bitcoin on Lightning Network

Any user can scan or paste a Lightning Network invoice into Bitcoin Libre. The user can send pegged bitcoin on-chain with a special memo and the Libre Lightning service will attempt to make a payment bitcoin via Lightning.

12 Receiving pegged bitcoin

The primary method of sending and receiving bitcoin is via @names on the Proton chain. The reason is that this will succeed 100% of the time for any amount that is sent - from 1 sat to 100,000,000,000 or more - this is not true for Lightning at this time and Bitcoin mainnet transaction fees are a major impediment to small transactions.

13 Sending Pegged bitcoin

Once the user has bitcoin, the main use of the Libre wallet will be sending pegged bitcoin to an @name.

14 Conclusion

Bitcoin Libre is a unique scaling system for Bitcoin with a goal of making Bitcoin very simple and easy to use for the entire world. Future direction of this scaling system will be determined by a fair-launched decentralized DAO.