BurstChat: A Peer-to-Peer Decentralized Free Speech System

[20-feb-2020]

CurbShifter
HotWallet.Cash
curbshifter@pm.me

Abstract

Chat systems on the Internet have come to rely almost exclusively on trusted third parties running servers to connect peers. BurstChat [1] is a tool designed to enjoy free speech without fears of being silenced or (shadow) banned by such a central authority. It allows anyone to anonymously converse or spread information to anyone that can reach a Burst blockchain node.

BurstChat is designed to work without much instructions or prior knowledge. This document is meant to give an more detailed outline of the usage and functionality of this chat in HotWallet.Cash.

1. Introduction

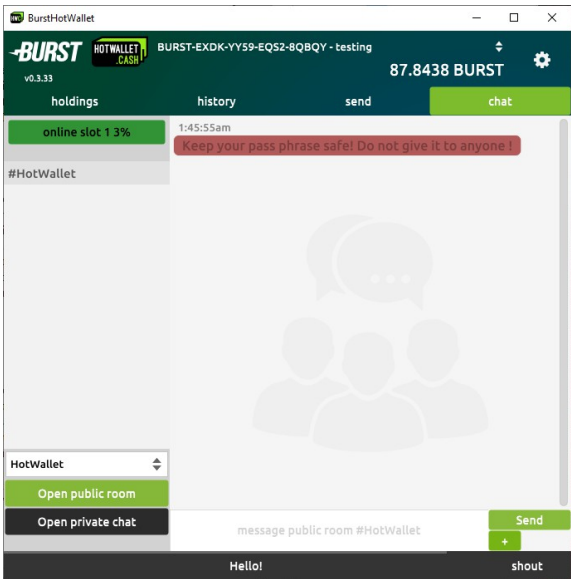
We live in a world where freedoms are continuously taken away by "trusted" third parties (ie. central authorities). Decentralized systems allow the development of tools that do not need or ask for permissions of third parties.

Where Bitcoin [2] has created unstoppable Peer-to-Peer cash. BurstChat leverages the Burst blockchain [3] to do this for freedom of speech. The Burst blockchain has the technology and unique properties needed for proper decentralization and to create a permission-less messaging system.

The first half of this document will explain the basic usage and functionality while the second part explains more technical details which will require some prior knowledge of the Burst blockchain mechanics.

2. Account creation

After installing and opening HotWallet.Cash for the first time, the user will be prompted to either create a new or import an existing wallet. This will be the account address from which others will recognize a user while chatting. Users should apply their own operational security (OPSEC) to keep their wallet address anonymous where needed. An account needs only a few Burst to function, at least 10 or more is recommend. Depending on many factors but this is an equivalent of many hours to days of use.



HotWallet.Cash - BurstChat interface

3. Public room

When opening the chat tab in HotWallet.Cash. The default public room that is listed is #HotWallet, users can use this as starting point to find other people.

The room name is an alias of an account [4]. Users can open the settings page to register their own unique alphanumeric aliases that will refer to their wallet address. Which can be used to direct people to your public rooms and private chats.

However an alias is not needed. The user can also enter any account address, either in the numerical or Reed Solomon (ie BURST-...) format. These rooms are free to enter and create.

A user can also enter any random number of a (non-)existing address and share that number to meet up with people.

Note that 'public' rooms means messages are not encrypted and thus publicly visible on all the nodes.

4. Private chat (AES-256 encrypted)

Peers can have a one-on-one private chat, by entering either the alias or address, just like the public chat. And click 'Open private chat'. Messages are then sent encrypted with the Advanced Encryption Standard at 256 bits. These messages are only readable by the recipient.

Note that both parties need to have made at least one transaction on the blockchain to have their public key recorded and available. This is needed to encrypt the sent messages. Otherwise messages will not arrive. To get a public key on the blockchain, the user makes any regular transaction from their wallet. For example, register an alias or send some Burstcoin.

5. Sending messages

Sent messages will show up in a gray font and will turn black once it is confirmed to be on the burst node. At this point the message will be propagated so it can be detected by recipients that are connected to other nodes. This process can take up to a few seconds. These messages will stay available on the network for up to 1 minute.

6. Logging

Currently a default build of BurstChat does not log any messages for operational security reasons (OPSEC). Which means that once the app is closed any messages will be lost without trace. Message logging can become available as optional feature for the user depending on demand.

Note however that users can double click a message in the chat to copy it to clipboard, which is useful for sharing text and hyperlinks.

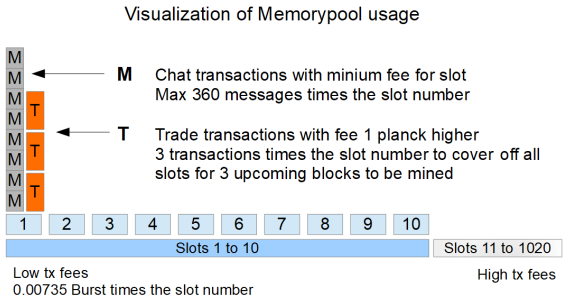
7. BurstSocket

The backbone of BurstChat is the BurstSocket system, which is part of BurstLib [5]. Which allows the near free transfer of data. The messages or data are temporarily stored in the memory pool of the nodes and are actively being prevented from being mined to stay off-chain.

While online, each user of the BurstSocket system is connected to an local or remote node. And keeps track of any existing transactions in the memory pool of that node. With this information it will predict the transactions that will be mined by looking at the transaction fees used. By comparing them to the node logic of selecting transactions when creating a block to mine. This logic is defined by the slot system [6].

With the mining prediction it will automatically create BurstSocket token trading transactions whenever needed. These transactions have a short deadline of +8 minutes and a fee higher of 1 planck. To prevent cheaper transactions such as the chat messages from being mined. Allowing the chat transactions to stay off chain. This keeps conversations ephemeral and prevents bloating the blockchain with data that does not need to be immutable.

This off-chain property improves privacy and stealth but also means any recipient needs to be online at the same time to receive the message. As the messages or data will only be available for 1 minute.



8. Token trading

The BurstSocket tokens that are auto traded while actively chatting (described in section 7) are bought for one Burstcoin at market price. Or depending on the user's holdings automatically sold for one Burstcoin above current market price. Through this mechanism fractions of BurstSocket tokens are being bought and sold at increasing prices. These fractions will become smaller over time. Which means the system will be up-trading while still keeping the price of each trade at one Burstcoin. (Excluding the transaction fee).

Users can still buy and sell the tokens at their own terms through the holdings tab of HotWallet.Cash just like any token on the Burstcoin blockchain. However this token system is designed as an utility to offset the fee costs of the trading transactions themselves. While creating an incentive to keep the BurstSocket channel open. The total amount of tokens is capped at 181800

(with 8 decimals), an initial sell wall is created by the author to support the described system.

9. File transfers

Besides messages small arbitrary file transfers are supported up to 64 kB through the + button, located right of the text message input box. Sending data over 1 kB in size will take multiple messages and more time to transfer. Recipients will get a message they can double click to save a copy of the file.

10. Always online

When users start chatting the 'Always online' option will be turned on automatically. However the user can still monitor the chat without sending any messages or data by opening the menu under the green button above the chat channel list. And select the option 'Always online'. This is useful when starting the application while not triggering token trading described in section 8. While still being able to see incoming messages. In other words a 'watch only' stealth mode.

11. Support mode

In contrast to the 'Always online' mode in section 10, the 'Support mode' allows a user to keep auto trading the tokens even when the user is not chatting. This keeps the socket channel open for other participants of the BurstSocket system.

This option is available under the green button menu, above the chat channel list. And is useful to support other users making their chat free and gaining a return on the trades over time while being away from keyboard.

12. Side-chain support

The asset trading system includes a basic side-chain, which can be further utilized and developed. As each bid order contains a block of raw data of max 1 kB. For each successful trade made (a bid and ask match) it is counted as a valid side-chain block.

Currently it only serves as a base for an oracle by saving the Burstcoin price in Bitcoin in the raw data. This is an experimental implementation that opens up possibilities for future applications to read the on-chain oracle data.

13. Limits

The maximum throughput of messages is currently 3600 transactions per minute. To not obstruct normal on-chain operations at max the lowest 10 slots [5] of 1020 slots are used of a node's memory pool.

The used slot and load is indicated above the chat rooms in the green menu button when online. It displays the current slot number followed by the load in percentage. Once the load reaches +50% of the slot space (360 tx per slot step) the used slot number will move up by one. And moves down when the load drops enough to fit the load in 1 slot lower. All this includes any normal on-chain transactions.

When moving up or down a slot, the fees for the trading BurstSocket tokens will increase or decrease by 0.00735 burst. Once the maximum throughput of the socket is reached, messages cannot be confirmed and will stay in the unconfirmed gray color.

13. Future

Considering the bandwidth limits of this system, it will lend itself best for disseminating information to groups. Rather than being a replacement of generic chat systems. Which is why a browser read only version of the chat is envisioned. From which users can connect to any Burst node to get distributed information. These rooms can then be moderated by anonymous posters that can widely share (encrypted) information.

14. References

[1] CurbShifter, BurstChat is part of hotwallet.cash. A Burstcoin desktop wallet.
< https://github.com/CurbShifter/BurstHotWallet >.

[2] Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System.
< https://bitcoin.org/bitcoin.pdf >.

[3] Burstcoin. The Pioneer of Proof of Capacity, an eco friendly blockchain.
< https://www.burst-coin.org >.

[4] BurstWiki, Burstcoin Alias System
< https://burstwiki.org/en/alias-system/ >.

[5] CurbShifter, BurstLib a standard C library to use the Burst node API
< https://github.com/CurbShifter/BurstLib >.

[6] BurstWiki, Slot based transaction fees
< https://burstwiki.org/en/slot-based-transaction-fees/ >.