Blockstream Internship

Andrew Chow | achow101@umd.edu
Science, Discovery, and the Universe | Computer Science

Summary

Over the summer, I interned at Blockstream where I worked on four projects to improve Bitcoin Core – an open source software project which powers the Bitcoin network. These four projects were coverage testing, wallet and node separation, coin selection, and partially signed transactions. Coverage testing and wallet and node separation were smaller projects done in the beginning while we were still thinking of ideas for major projects. The majority of the internship focused on implementing Branch and Bound coin selection and writing the specification for Partially Signed Transactions.

Partially Signed Transactions

Bitcoin clients are frequently incompatible with each other. I created Partially Signed Bitcoin Transactions (PSBTs) to be a way to increase client interoperability by specifying a common transaction format that can be used for incomplete transactions. This format contains all of the information necessary for any offline device to sign and construct a final transaction. This format is specified in Bitcoin Improvement Proposal 174

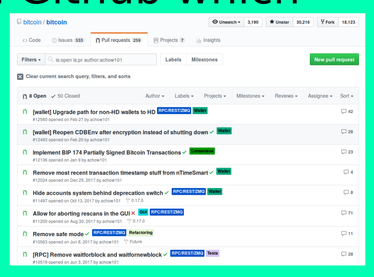
Example transaction:
70736274ff0100fd0a010200000002ab0949a08c5af7c49b8212f417e2f15ab3f5c33dcf153821a8139f877a5b7be4000000006a473044022047596617970 1b036b25928948686218347d89864b719e1f7fcf57d1e511658702205309eabf56aa4d8891ffd111fdf1336f3a29da866d7f8486d75546ceedaf93190121035cdc61fc7ba971c0b501a646a2a83b102cb43881217ca682dc86e2d73fa88292feffffffab0949a08c5af7c49b8212f417e2f15ab3f5c33dcf153821a8139f877a5b7be401000000000feffffff02603bea0b000000001976a914768a40bbd740cbe81d988e71de2a4d5c71396b1d88ac8e240000000000001976a9146f4620b553fa095e721b9ee0efe9fa039cca459788ac00000000150135 45e6e33b832c47050f24d3eeb93c9c03948bc716001485d13537f2e265405a34dbafa9e3dda01fb82308000001012000e1f50500000000017a9143545e6e33b832c47050f24d3eeb93c9c03948bc78700

Impact

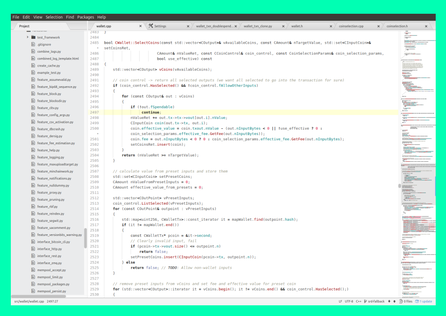
Interning at Blockstream has allowed me to have a bigger impact on Bitcoin. The changes to Bitcoin Core, especially Branch and Bound coin selection, allow Bitcoin Core to function better and makes progress towards some of Bitcoin Core's long term goals. PSBT will hopefully be adopted by more wallet software and it will allow more software to be compatible with each other. While these do not directly effect Blockstream, improving Bitcoin Core and Bitcoin in general allows Blockstream to continue working as their products rely on Bitcoin being functional.

Tools and Methods

- GitHub – Bitcoin Core's source code is hosted on Github which is also used for issue handling and code change proposals. The repository for Bitcoin Improvement Proposals is also hosted on Github



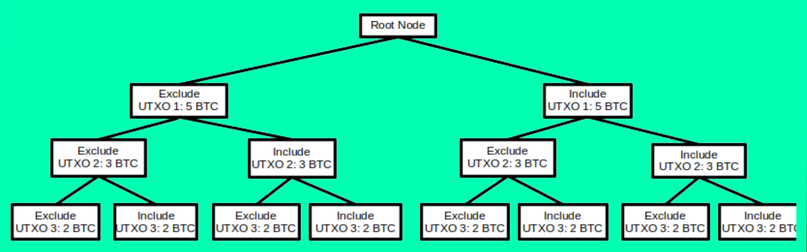
- Atom – The text editor which I used to write my code which was primarily C++ and Python



- Make/GCC/G++/Autotools – The compiler and build system that Bitcoin Core uses. These are command line tools that are run from the terminal.

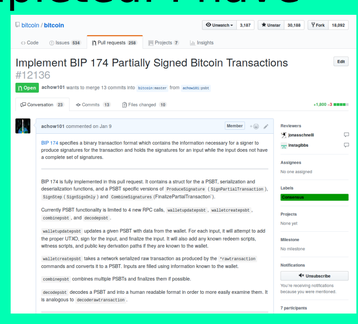
Branch and Bound Coin Selection

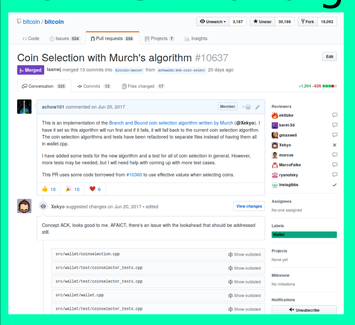
In order for Bitcoin Core's wallet to send Bitcoin, it must choose a set of coins to spend. The current algorithm used is somewhat inefficient and hard to understand. Thus I began working on a project to implement a new algorithm which we call Branch and Bound. This new algorithm is an exact matching algorithm. Currently, if it fails to find a match, Bitcoin Core will fall back to its current algorithm.



Future Work

While I began working on these projects at Blockstream, they were not fully completed. I have and will continue to work on them as well as make other changes to Bitcoin Core. Many of the changes I made have been submitted to be merged into Bitcoin Core but are currently unmerged. I will continue to work on PSBT and get it implemented into other Bitcoin wallet software. I Continue to work on coin selection and plan on also changing the fall back strategy.





Thanks to my mentors Pieter Wuille and Greg Maxwell as well as Dr. Alan Peel and the Scholars faculty