

₿

# Blockstream Internship

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



Blockstream

### Summary

Bitcoin **Core** 

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

### 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.

#### Example transaction:

70736274ff0100fd0a0102000002ab0949a08c5af7c49b8212f417e2f15ab3f5c33dcf1 53821a8139f877a5b7be400000006a47304402204759661797c01b036b2592894868 6218347d89864b719e1f7fcf57d1e511658702205309eabf56aa4d8891ffd111fdf1336f3 a29da866d7f8486d75546ceedaf93190121035cdc61fc7ba971c0b501a646a2a83b102c b43881217ca682dc86e2d73fa88292feffffffab0949a08c5af7c49b8212f417e2f15ab3f5c 33dcf153821a8139f877a5b7be4010000000feffffff02603bea0b00000001976a91476 8a40bbd740cbe81d988e71de2a4d5c71396b1d88ac8e24000000000001976a9146f4 620b553fa095e721b9ee0efe9fa039cca459788ac000000015013545e6e33b832c470 50f24d3eeb93c9c03948bc716001485d13537f2e265405a34dbafa9e3dda01fb8230800 0001012000e1f505000000017a9143545e6e33b832c47050f24d3eeb93c9c03948bc7

### Tools and Methods

### •<u>GitHub</u> – Bitcoin Core's source code is hosted on Github which

is also used for issue handling and code change proposals. The repository for

bit	Ocin / bitcoin          Ø Unwatch → 3,190         ★ Unstar 30,216         ¥ Fork	18,
$\diamond$	Code ① Issues 533 17 Pull requests 259 III Projects 7 1 Insights	
Filt	ers - Q is:open is:pr author:achow101 Labels Milestones	requ
×c	lear current search query, filters, and sorts	
n	8 Open ✓ 50 Closed Author → Labels → Projects → Milestones → Reviews → Assignee →	Sor
n	[wallet] Upgrade path for non-HD wallets to HD RPC/REST/2M0 Wallet #12500 opened on Feb 27 by achow101	φ
n	[wallet] Reopen CDBEnv after encryption instead of shutting down ✓ Wallet #12493 opened on Feb 20 by achow101	$\square$
n	Implement BIP 174 Partially Signed Bitcoin Transactions ✓ Commensus #12136 opened on Jan 8 by achew101	Ģ
n	Remove most recent transaction timestamp stuff from nTimeSmart ✓ Water #12024 opened on Dec 25, 2017 by achow101	ç
n	Hide accounts system behind deprecation switch / RPCREST/ZMO Water #11497 opened on Oct 13, 2017 by achewrol 1 <sup>(**</sup> 0.17.0	ç
n	Allow for aborting rescans in the GUIX GUI FRC/REST/2000 #11200 opened on Aug 30, 2017 by achieve101 *** 0.17.0	$\square$

### Branch and Bound Coin Selection

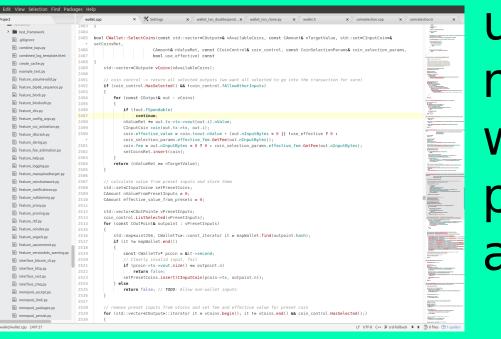
In order for Bitcoin Core's wallet to send Bitcoin, it must choose a set of coins to spend. The current algorithm used is somewhat inefficient and hard to understand. Thus I began working on a project to implement a new algorithm which we call Branch and Bound. This new algorithm is an exact matching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

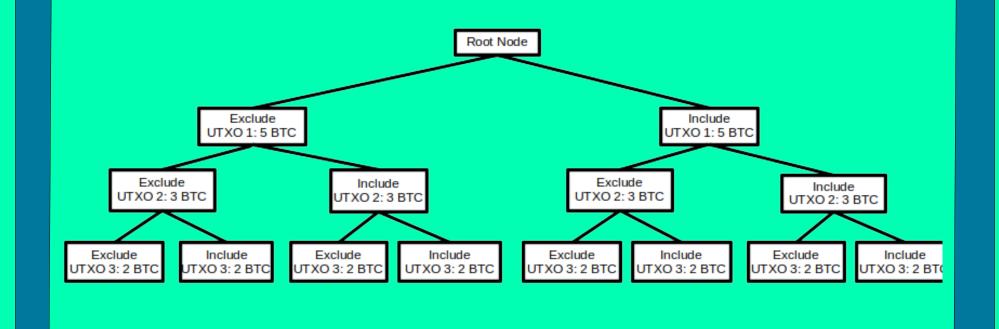
🛛 bitcoi	n / <b>bitcoin</b>			O Unwatch -	3,187	🖈 Unstar	30,188	Y Fork	18,092
<> Cod	e () Issues 534	n Pull requests 258	Projects 7	III Insights					
<b>Impl</b> #121		9 174 Partia	lly Signed	l Bitcoin Tr	ansad	ction	S		Edit
រ្ហា Open ជ្រា Conv	-		changed 10	Men	nber + (i)	¢	eviewers	+1,800	-3
	Achew101 commented on Jan 9 Member + (a) > BiP 174 specifies a binary transaction format which contains the information necessary for a signer to produce signatures for the transaction and holds the signatures for an input while the input does not have a complete set of signatures.					y	s jonassch		ç
						A	Assignees No one assigned Labels		
	BIP 174 is fully implemented in this pull request. It contains a struct for the a PSBT, serialization and deserialization functions, and a PSBT specific versions of producesignature (SignPartialTransaction).								

Bitcoin Improvement Proposals is also hosted on Github • <u>Atom</u> – The text editor which I



used to write
 my code
 which was
 primarily C++
 and Python

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



other changes to Bitcoin Core. Many of the

as well as make



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

<complex-block><complex-block>

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