

How a full SegWit and Batching Adoption Could Have Saved Users Nearly Half a Billion Dollars in Bitcoin Network Fees

Presented by Veriphi



Authors

Gustavo J. Flores Echaiz

Tristan Borges Solari

Maciej Cepnik

July 2020

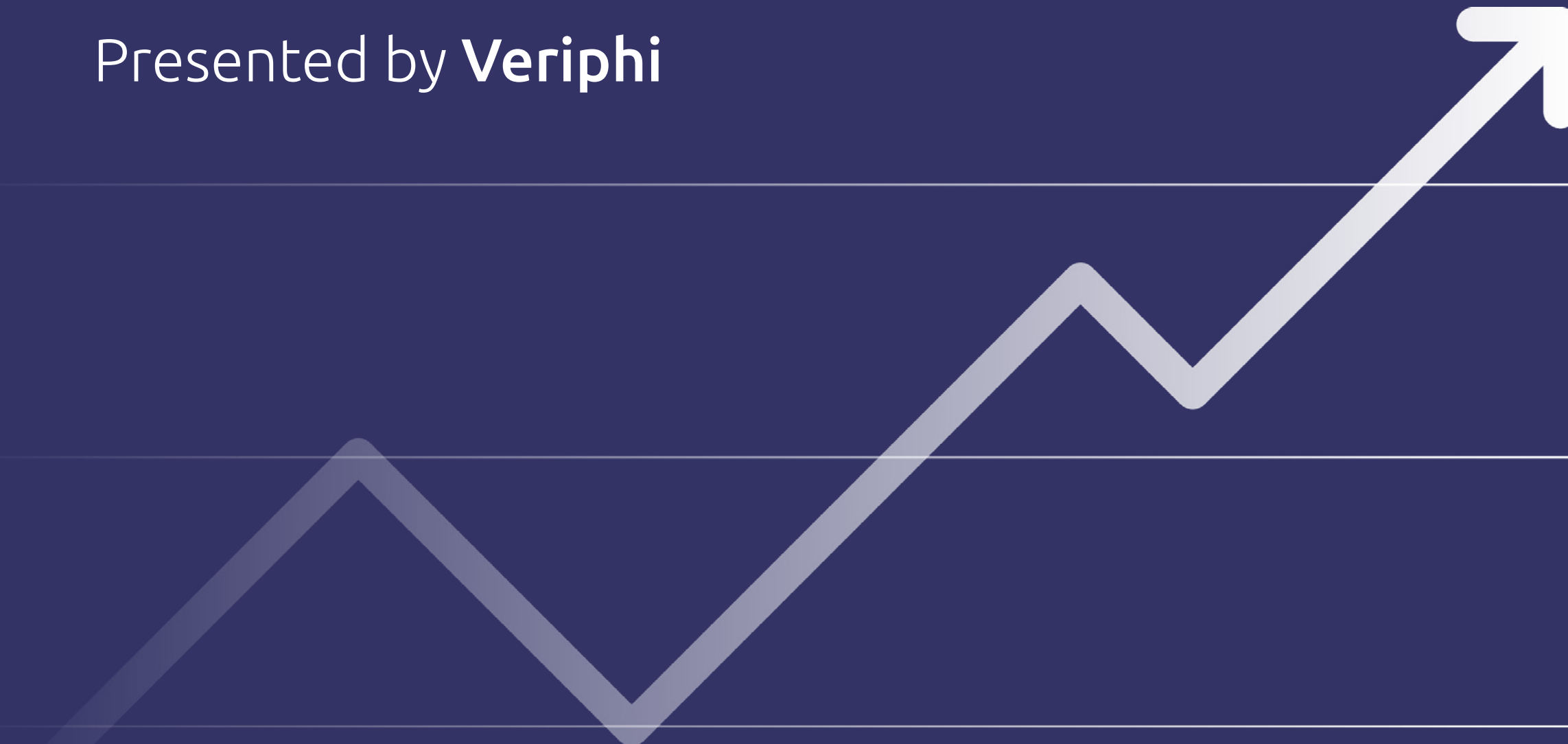


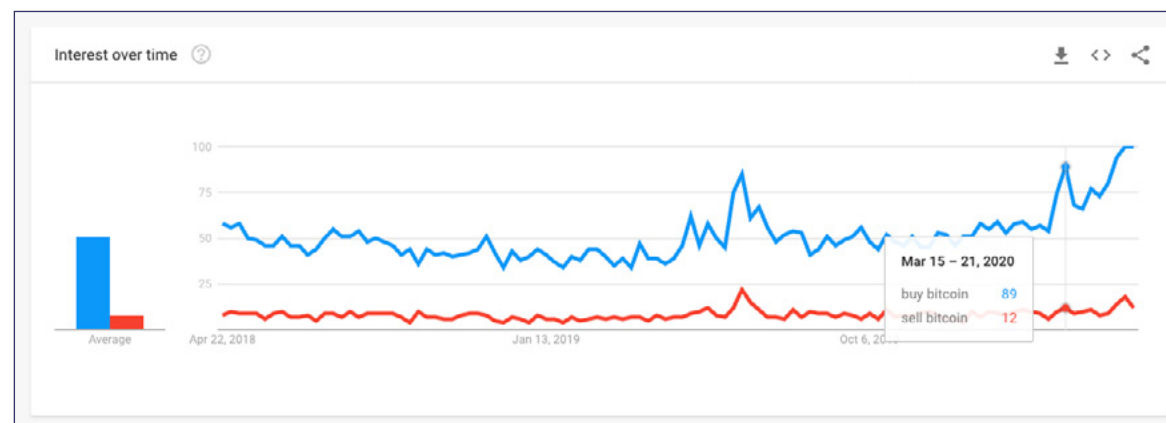
Table of Contents

Introduction	4
Transaction Batching	7
What is Batching?	7
Benefits of Batching	8
2020's picture of Batching adoption	10
Batching in our model of 100% adoption	14
SegWit	25
What is SegWit?	25
Witness Data	25
Block Weight	27
SegWit Scripts and Addresses Types	28
Benefits of Segregated Witness	30
SegWit Transactions Pay Less Fees	30
Block Size Increase	31
Transaction Malleability	31
Lightning Network	32
2020's Picture of SegWit's Adoption	32
Analyzing Segregated Witness Adoption Data	33
Segregated Witness Exchange Adoption	37
SegWit in our scenario	38
Conclusion	49
Appendix	52
References	62

Introduction

Bitcoin is the predominant cryptocurrency being exchanged worldwide. Exchange platforms and payment processors operating in the industry are incentivized to offer the best user experience in order to encourage repeat business and protect market share. In a time of political and economic uncertainty, demand and interest for Bitcoin has witnessed an important increase worldwide as seen on Google Trends (Figure 1).

Figure 1 : Google Trends on Bitcoin from April 2018 to April 2020



Bitcoin, being programmable by nature, offers its users multiple avenues in order to implement enhanced functionalities. Changing the Bitcoin source code is not often a viable solution for businesses since it requires research and development to be carried out over a long time period. Not only does these kinds of changes take time to pursue, they can only be implemented through soft forks, which in turn require consensus of the network. Often-times, the changes sought out are to make Bitcoin more efficient or increase

its uses. Businesses operating in the Bitcoin space, especially those that are transactional intermediaries, desire methods to make their operations more economical all the while maintaining a competitive edge.

The purpose of this case study is to determine the savings benefits that employing SegWit and Batching in Bitcoin transactions would have had, had there been a full adoption. Nearly half a million blocks of transactions have been scrutinized in order to calculate the amounts of bitcoins and mega-bytes saved thanks to these technologies. The savings potential presented is significant and those conducting large amounts of transactions should seriously consider employing these tools in order to remain competitive and save money.

Major takeaways:

- From January 2012 to June 2020 (until the 637,090th block) 211,266.95 bitcoins were paid in fees to miners. This amounts to a total of around \$1,954,219,287 USD with a Bitcoin price of \$9250.00 USD at the time of latest update in July 2020.
- Over 21,131.97 bitcoins could have been saved by Bitcoin users if they would have all been using Transaction Batching. 190,134.98 bitcoins could have been paid in fees instead of the 211,941.32 bitcoins, which represents savings of 9.97%. The 21,131.97 bitcoins saved represents a staggering amount of \$195,470,722 USD (with a Bitcoin price of \$9,250.00 USD).

- From August 24th 2017 to the 30th of June 2020, 36,685.72 bitcoins could have been saved by Bitcoin users if they would have all been using SegWit Native (Bech32). Fees would have amounted to 59,848.61 bitcoins, down from 96,534.33 bitcoins actually paid in fees, which is 38.00% in savings. The 36,685.72 bitcoins saved represent \$339,342,910 USD (with a Bitcoin price of \$9,250.00 USD).
- The advantages brought through optimized fee management techniques such as SegWit and Batching are mostly impressive and apparent during high transactional activity periods. A large percentage of the possible savings would have been achieved in only a few months over the span of 8 years and 6 months analysed.
- Bitcoin market actors, such as exchanges, should strongly consider implementing any optimized fee management techniques with clear financial advantages. In anticipation of future price appreciation and higher transactional activity, Bitcoin users have to acknowledge that bitcoin transaction fees will continue to rise and prepare consequently.

Transaction Batching

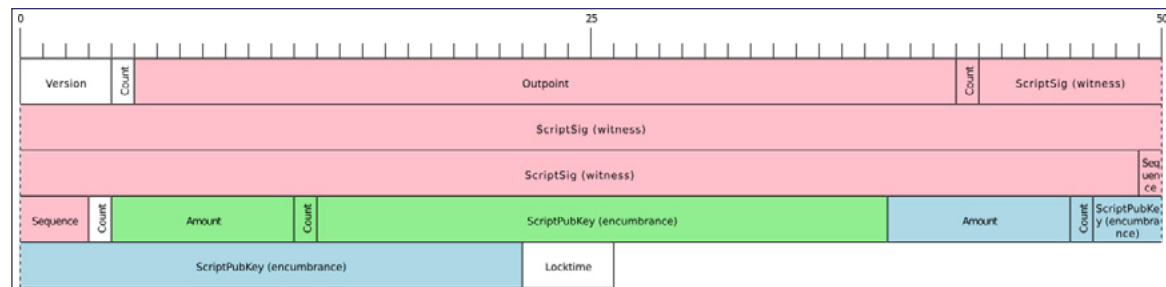
To better understand how our research has applied, it's important for everyone to understand the technologies studied. We will explore what transaction batching is, what are the benefits of its usage and how 2020's adoption looks like. We will finish this section by presenting our data analysis that compares bitcoin network fees and block size from January 2012 to March 2020 to an hypothetical scenario where transaction batching had an adoption of 100%, where applicable.

What is Batching?

Bitcoin transactions include inputs, the coins being spent, and outputs, where the coins get sent. In contemporary wallets and applications, Bitcoin transactions have at the very least 2 outputs for the most part, one where the money gets sent and another where you get your change back to another address you control. What if you want to send funds to multiple addresses? You could make two transactions with each two outputs including the change output, however doing so makes you pay fees for every separate transaction. You could instead use Transaction Batching. Briefly, this technique simply signifies having more than 3 outputs in a transaction, thus making a payment to two different parties at the same time.

A typical P2PKH (Pay to Public Key Hash) Bitcoin transaction (As seen in Figure 2) containing one input, an output and a change output would be 226 bytes in size. Knowing this, every additional independent transaction would then at least have another 226 bytes. For entities making multiple transactions, the fees paid can add up quickly. Imagine having the below image multiplied by every individual transaction you make.

Figure 2 : A P2PKH Bitcoin Transaction Decomposition



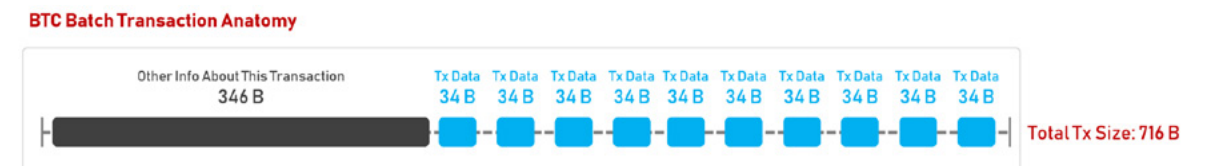
Bitcoin used to have a limit of 1MB for every block of transactions. Since this limit was replaced with a block weight limit that can reach 4MWU, we can calculate that if all the transactions in a block were using SegWit, the block size could reach 2.4 MB. Even though we can fit more transactions now, the case still is that we can only fit a certain amount of transactions in every block depending on their sizes. The larger transactions must then pay a greater amount in fees if they want to be included in a block, since space is limited. The impact of Transaction Batching becomes more apparent the more transactions we make.

Benefits of Batching

The input of the above transaction represents about 65% of the transactions (148 bytes) and the outputs around 30% if we assume it has a change output. In order to save on fees paid when making multiple transactions, you can either use as few inputs as possible by consolidating your UTXOs, or you can use Transaction Batching, where the output part scales linearly but the input part stays the same, no matter the amount of outputs.

By aggregating multiple outputs into a single transaction, you are effectively saving up on space required for your payments, thus reducing the amount of fees paid to miners. Instead of making a second separate payment of 226 bytes, effectively doubling your fees, you are instead paying 15% (34 bytes) more than the single transaction for each output (as seen in Figure 3).

Figure 3 : Bitcoin Batch Transaction Anatomy



The savings further increase the more outputs you add onto the transaction. A batched transaction that contains 10 outputs represents 25% of the total byte size of 10 individual payments, saving you up to 75% in fees paid.

Batching also has the benefit of minimizing your UTXO set since you'd only have one change address per batched transaction instead of one for each individual payment made. By reducing your number of change outputs you are further saving on fees spent since a change output typically takes up at least 69 vbytes when spent later on.

There are however potential privacy concerns when it comes to batching. A user can very easily see every other address that received a payment in the same transaction, or someone else analysing these transactions can identify →

users whose public address is known and tie them to an exchange with an amount. On the other hand, even if the transactions are done separately, those links can still be inferred by analyzing the change outputs.

Batching is a simple yet effective method to implement in order to save on fees paid by making your payments more efficient. Large scale organizations that have multiple transactions per day can greatly benefit from batching, especially during times when fees spike like in the December 2017 to January 2018 periods where fees rose significantly in USD terms. As your number of payments increases, there are potentially huge savings to be made which in turn can either increase your revenues or be passed along to your customers.

2020's picture of Batching adoption

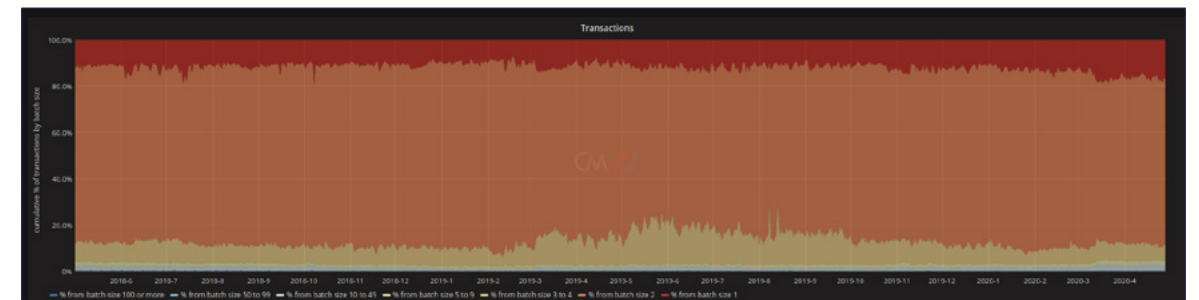
Before jumping into our analysis, we want to present 2020's picture of Transaction Batching adoption on the Bitcoin Network. We'll also take a look at a few exchange platforms that have implemented and use the technique in their production environments.

Nic Carter and Hasu wrote an [awesome piece in 2018](#) that analyzed the period from November 2017 to May 2018 and concluded that Transaction Batching accounted for around 12% of transactions, 40% of outputs and between 30 to 60% of volume transacted on the Network. We will look at how the situation has evolved by analyzing data and charts available on the P2SH.info site, a collaboration between BitMex Research and CoinMetrics.

Analyzing Transaction Batching Data (May 2018 to April 2020)

As seen on the chart below (Figure 4), the number of batched transactions are around the previously mentioned average of 12%. At the end of 2018, it went lower to test the 10% threshold. It stayed there until March 2019, when it went higher and stayed north of 17% for a few months, going as high as 30% in August 2019. Ever since October of that same year, it's been back to the initial 10-12% range.

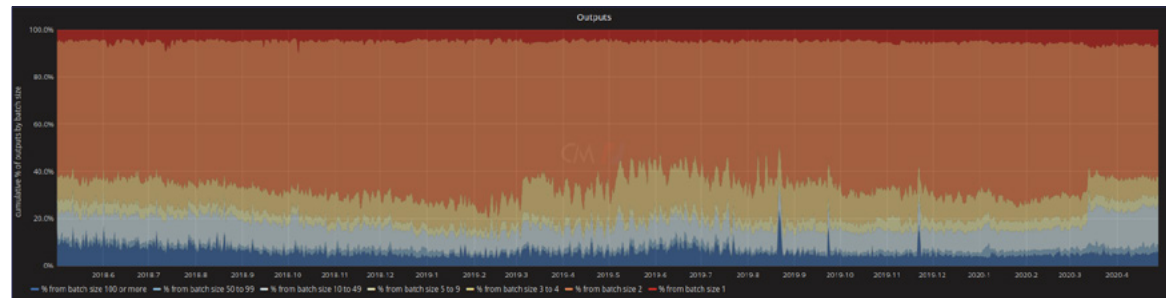
Figure 4 : Percentage of Batched Transactions Over Total (May 2018 to April 2020)



In terms of outputs, Transaction Batching began the period lower than the previously established average of 40% (as seen in Figure 5) and pushed consistently down until reaching 20% in February 2019. March also brought an increase for this metric and it took until May 2019 to see Transaction Batching percentage of the total outputs gravitating around 40% and reaching a high of 51% on the 21st of August 2019. From October 2019 until the →

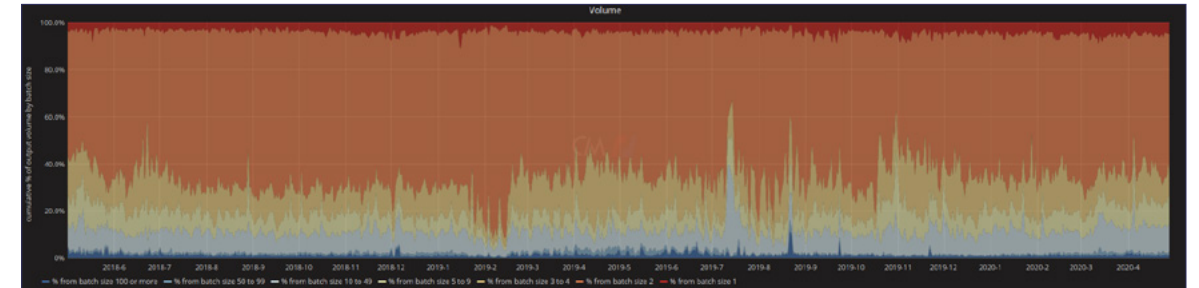
second week of March, it has averaged 30% with a recent pickup that has brought it to levels right under 40% and testing the average of the previous bull market period.

Figure 5 : Percentage of Batched Outputs Over Total (May 2018 to April 2020)



Being the most short term volatile metric out of the bunch, batched volume percentage (Figure 6) of total transacted volume has for the most part stayed in the previously established range of 30-60%. However, it's much closer to the bottom of 30%, rarely surpassing 40%. A brief period between mid January 2019 and February 2019 saw volume lower than 30%, reaching a low of 8% on the 6th of February 2019. Ever since, we've seen it come upwards from the floor of 30% with only a few exceptions in the month of August 2019, but has been consistently between 30-40% for the most part. There were brief moments in July and October 2019 where it went upwards of 60% but never broke the high of 70% established in the previous period.

Figure 6 : Percentage of Batched Volume Over Total (May 2018 to April 2020)



Transaction Batching Exchange Adoption

Also found on Carter's and Hasu's article on the CoinMetrics blog, back in May 2018 the following exchanges had already implemented the scaling technique.

- Binance
- Shapeshift
- Bitfinex
- Bitstamp
- Kraken
- Bittrex
- Poloniex
- HitBTC

Ever since, a few smaller exchanges have adopted Batching: Bull Bitcoin, BTSE and River Financial. However, in March 2020, the biggest news of Transaction Batching was Coinbase's adoption which will reduce their

Bitcoin transaction fees by around 50%, a savings they will pass to their customers for the most part.

Batching in our model of 100% adoption

Now that we have a clearer understanding of Batching, why it's advantageous to implement it and how the landscape looks like, let's take a look at our hypothetical scenario, a reality where there would've been Transaction Batching at full capacity from January 2012 until the 30th of June 2020.

The data collected and presented below is based on David A. Harding's [formula](#) for detecting whether there's multiple transactions with matching input prevout (transaction id of the previous output). If matching, those transactions are hypothetically batched and we combine the size of the hypothetical block and compare it to the real block size. From there, we can calculate the amount of bytes that were saved and the percentage this saving represents. Finally, if we take the size of each block and remove the size of the block header and the coinbase transaction (since it's data that has no fees), we can divide the saved size by this new amount. The percentage we get is an approximation of the fees that would be paid if full adoption would've happened. We tweaked David's code slightly in order to increase the number of variables we can analyse for this report. You can find our version [here](#).

Here are the main takeaways of the data collected about Batching from the 1st of January 2012 until the 30th of June 2020

The original time of publication of the case study was in April 2020 covering data and analysis from January 2012 until the 31st of March 2020. We have updated the data and case study to cover the time period from January 2012 until 30st of June 2020.

- There is the equivalent of 284.37 GB of data that were used by transactions.
- Over 211,266.95 bitcoins were paid in fees to miners. At the time of writing, in July 2020, this amounts to a total of around \$1,954,219,287 USD (when accounting with a Bitcoin price of \$9250.00 USD).
- During this same period, the total size could have been 251.15 GB. 32.91 GB could have been saved from the 284.37 GB of data actually used. This results in 11.57% savings, if full Batching adoption had taken place.
- Over 21,131.39 bitcoins could have been saved by Bitcoin users if they would have all been using Batching. Fees would have amounted to 19,0134.98 bitcoins, down from 211,266.95 bitcoins which is a 10.00% savings. Savings of 21,131.39 bitcoins would represent a staggering number of \$195,465,357.5 USD (with a Bitcoin price of \$9250.00 USD).

The following section will explore the modeling of fee and block space savings over time. We have made a section focusing on the months around the Bitcoin 3rd Halving Block, April to June 2020.

Data from January 2012 to March 2020 : Fees and Savings Exploration

In the first and second graphic we compared the transaction fees paid in Bitcoin month over month to the sum fees that would have been paid if Batching was fully supported by all the market participants of the Bitcoin Network since the 1st of January 2012. The blue bars represent the calculated monthly sums that were paid in reality to the miners and the orange bars represent the theoretical fees that would have been paid if Batching was fully supported. Since we collected the data over a long period of time we divided the graph in two parts to facilitate the reading and comparison with the SegWit timeframe. The first graph goes from January 2012 to March 2017 and the second one from March 2017 to June 2020.

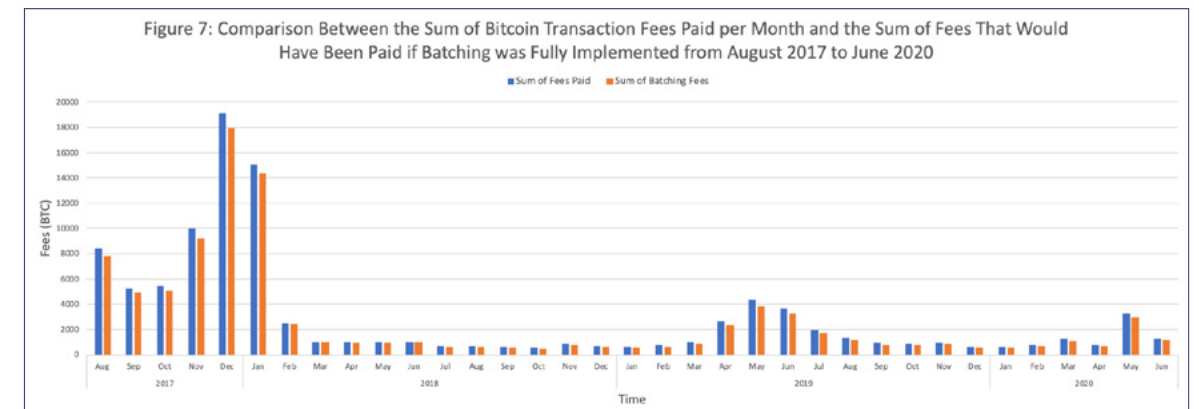
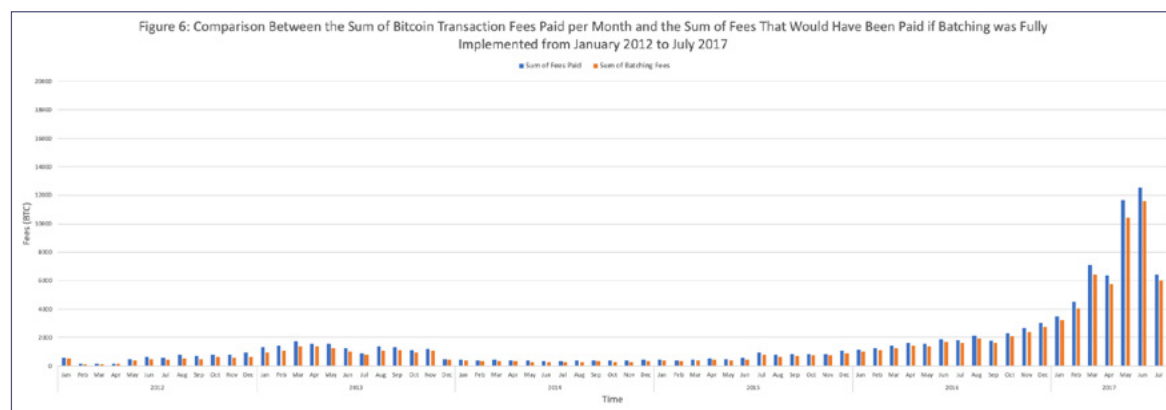
You can quickly notice that the theoretical sums are all lower than the actual fees paid in real life. This of course is self-evident as batching optimizes the block space by compacting multiple transactions into one, effectively reducing the amount of space they would have taken individually. Transaction fees are calculated according to how much block space your transactions take. Therefore the less space your transactions take, the less fees you will have to pay.

We can observe prominent increases in transaction fees paid in real life in three distinctive periods: in 2013, from mid 2017 until the beginning of 2018 and recently, during April, May and June 2019. All these periods coincide strongly with strong bullish Bitcoin price action.

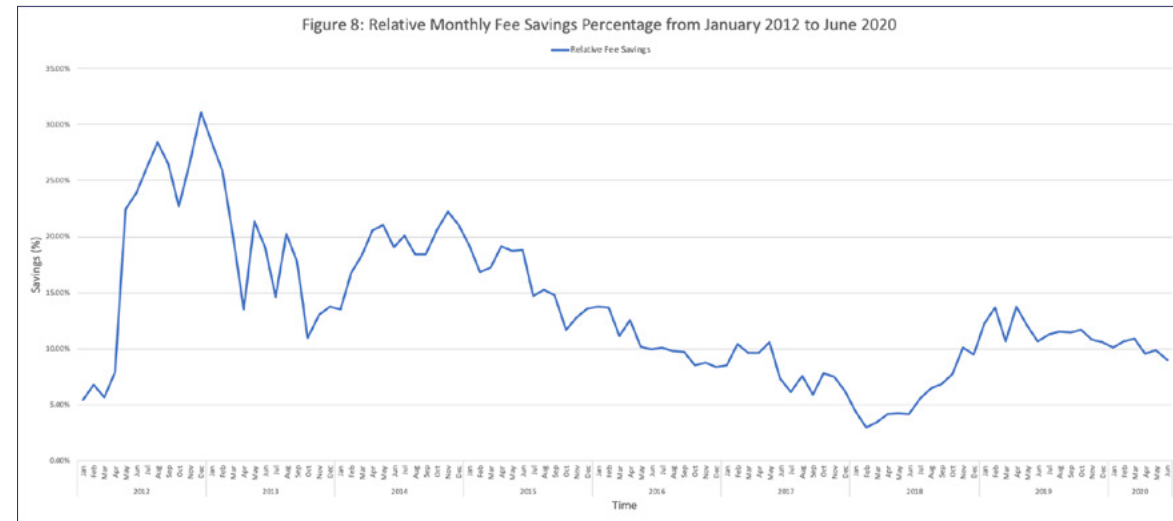
There are also three low fee periods, the first spawning from December 2013 to July 2015, the second from February 2018 to March 2019 and the third one from July 2019 up until April 2020. All these periods experienced bearish price action overall.

This leads us to believe that transaction fees rise considerably as the Bitcoin price rises and are considerably lower during downward price action. This can be explained by higher transaction activity and demand for Bitcoin during bull markets.

The three most expensive months in terms of transaction fees were December 2017 (19,126.07 bitcoins), January 2018 (15,043.70 bitcoins) and June 2017 (12,528.41 bitcoins). Although if we observe the highest three months in possible savings that could have been made if batching was adopted at a 100% rate we have the following months: May 2017 (1,236.34 bitcoins), December 2017 (1,185.20 bitcoins) and June 2017 (918.36 bitcoins). Totalling over 3,339.90 bitcoins in savings in just 3 months (\$29,892,105 USD at the time of writing with Bitcoin at \$8950 USD). When calculating the relative percentage of the total savings of these three months to the total of savings that could have been done during the whole analyzed period, they represent respectively 5.85%, 5.61% and 4.35%. The sum of savings adds up to 15.81%, even if those three months only represent 2.94% of the analyzed time period.



In Figure 8, we plotted the percentages of the theoretical monthly fee savings over the monthly fees paid in real life. The graphic starts with a staggering increase of the relative percentage of possible savings with a 100% Batching adoption, from just over 5.00% to over 30%. This can be explained by a quickly rising number of daily Bitcoin transactions and its considerable price appreciation. After that, we can observe a descending pattern on the graph showing that the relative percentage of monthly possible savings with a 100% batching adoption has been gradually going down since January 2012 until the end of 2017, from a high of over 35% in 2012 and just over 2% at the end of 2017. Since the technique could have been used since the inception of Bitcoin, we can assume it's been adopted gradually by exchanges, Bitcoin services providers and its users.



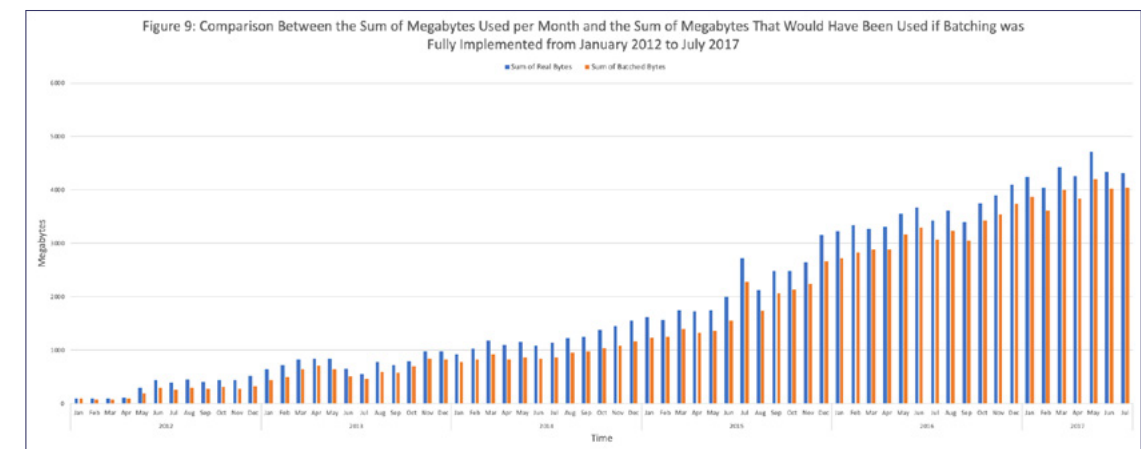
Although the relative percentage of savings has been going down for the past 5 years, it has been slightly increasing since February 2018 and it now hovers around 10%. Even though it could seem trivial for some, this is an interesting metric considering that over the analyzed period from January 2012 to June 2020, 211,266.95 bitcoins have been paid in fees to miners. Overall, 21,131.39 bitcoins (\$195,465,357.5 USD at the time of writing with Bitcoin at \$9250 USD) could have been saved if batching was adopted at a 100% rate.

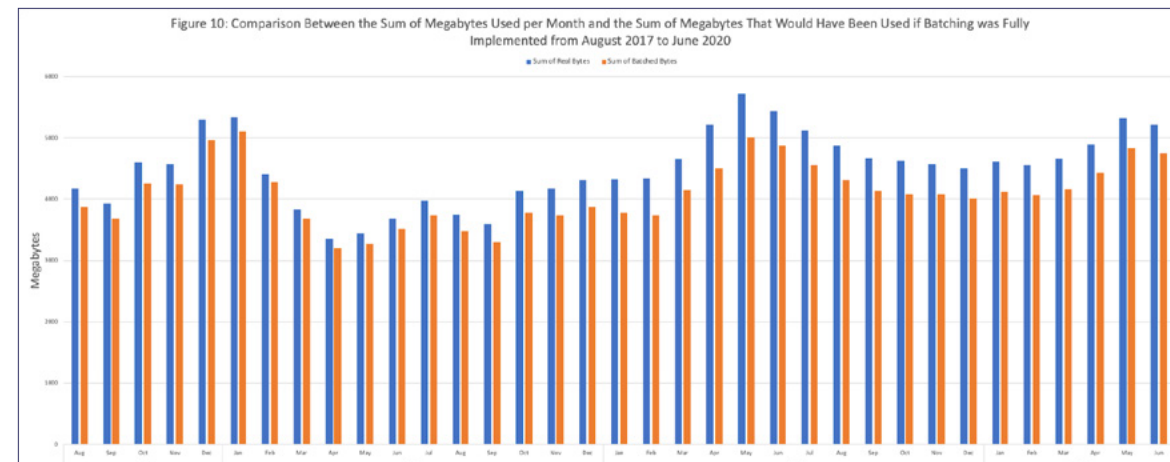
Batching transactions, in theory, can help save users making 10 payouts or more up to 75% in transaction fees. This savings potential is not necessarily reflected here since what is displayed is the additional savings possible with transactions that could have been batched during these periods. Savings of around 10% can still be substantial for users and organizations making several transactions over time.

Therefore the batching technique still has to be adopted quite substantially by some before no possible savings could be done with the method. Not only does it reduce transaction costs for those who adopt it, batching also has a great effect for the Bitcoin network, since batched transactions take up less space in a block, leading to a higher theoretical number of singular transactions that can be included in each block.

Block Space Exploration

In Figures 9 and 10, we compared the sum of megabytes used by Bitcoin transactions month over month to the sum of bytes that would have been used if Batching was fully supported by all the market participants of the Bitcoin Network since the 1st of January 2012. The blue bars represent the calculated monthly megabyte sums that were used in reality by transactions and the orange bars represent the theoretical sum of megabytes that would have been used if Batching was fully supported. Since we collected the data over a long period of time we divided the graph in two parts to facilitate the reading. The first graph goes from January 2012 to March 2017 and the second one from March 2017 to June 2020.





Naturally, as Bitcoin grew in popularity during these years, the number of daily Bitcoin transactions grew as well. This led to more bytes of data being used and Bitcoin blocks to be fuller. Our graphic indicates a steady and linear increase of total monthly megabytes used from January 2012 until reaching a maximum of 5,329.31 megabytes in January 2018. After that, we observe a decrease of transactional activity and therefore less megabytes being used in blocks. This coincides with the bear market spawning from the beginning of 2018 until March 2019. The previous record was broken in May 2019 with 5,709.45 megabytes of data used.

Overall, if Batching was adopted fully from January 2012 until March 2020, over 31,492.44 megabytes of data could have been saved of the 268,942.88 megabytes that were actually used, representing savings of 11.71%.

The Halving Three Month Period, April to June 2020

As we can see in Figure 7, the months following March have witnessed relatively higher fees paid to miners by Bitcoin users and relative possible savings that could have been made during the April to June period. This statement is especially true for the month of May with over 3,251.58 bitcoins paid in transactional fees, which is 258.91% higher than the second most expensive month of 2020, which is June with 1,255.89 bitcoins paid to miners. Overall in these three months (April, May and June 2020), 512.05 bitcoins could have been saved by Bitcoin users if Batching was to be adopted at a 100% rate when applicable. At the time of writing of this update with a price of \$9,250.00 US per Bitcoin, that would represent \$4,736,462.50 USD.

Halving Effect on Transaction Fees and Potential Savings

We can clearly see that the month of May distinguished itself from all the other months of 2020 with a significant increase of transactional fees paid during that month when compared to the rest of 2020. This increase coincides with the third Bitcoin halving that happened on the 11th of May 2020.

Bitcoin halving events are highly awaited by Bitcoin market participants and especially miners as their revenue simply gets cut in half from one moment to another. There is also a lot of hype and discussions regarding the price action and effect of the halvings on the Bitcoin price. Whenever its →

Transaction Batching

investors want to get in or out of Bitcoin depending on their personal view of the effect of the halving on Bitcoin's price, or miners moving coins around to adapt their strategy for the expected and awaited drop in revenue, the halving is probably the cause of higher transactional activity. This higher transactional activity led to a higher utilization of the Bitcoin blocks space, which brought in return higher fees explaining the increase in May. Other events could have influenced that increase as well.

Overall, before the third halving, miners were receiving 12.5 bitcoins per block every 10 minutes on average, which represents approximately 54,900 bitcoins every month given to miners through the block subsidy. After the halving, 27,450 less bitcoins per month on average are given out through the block subsidy to miners. Therefore, even if the month of May has been the highest during this year in terms of transactional fees paid by users, it only covers 11.84% of the loss of revenue in terms of bitcoin coming from the mining subsidy post halving.

Batching follow-up update from March 2020 to July 1st 2020 - Block Space

As we can see in Figure 10, there is an increase in the sum of megabytes used in the Bitcoin blockchain during the last three months analyzed. April, May and June have respectively used 4.89 GB, 5.32 GB and 5.22 GB, totaling 15.43 GB. With the usage of Batching at a 100% level when applicable, a total of 1.44 GB could have been spared in terms of Block space utilization

SegWit

In this section we will explain what SegWit is, what it allows for and the current status of the network adoption of SegWit. We will conclude on this technology with our scenario modeling.

What is SegWit?

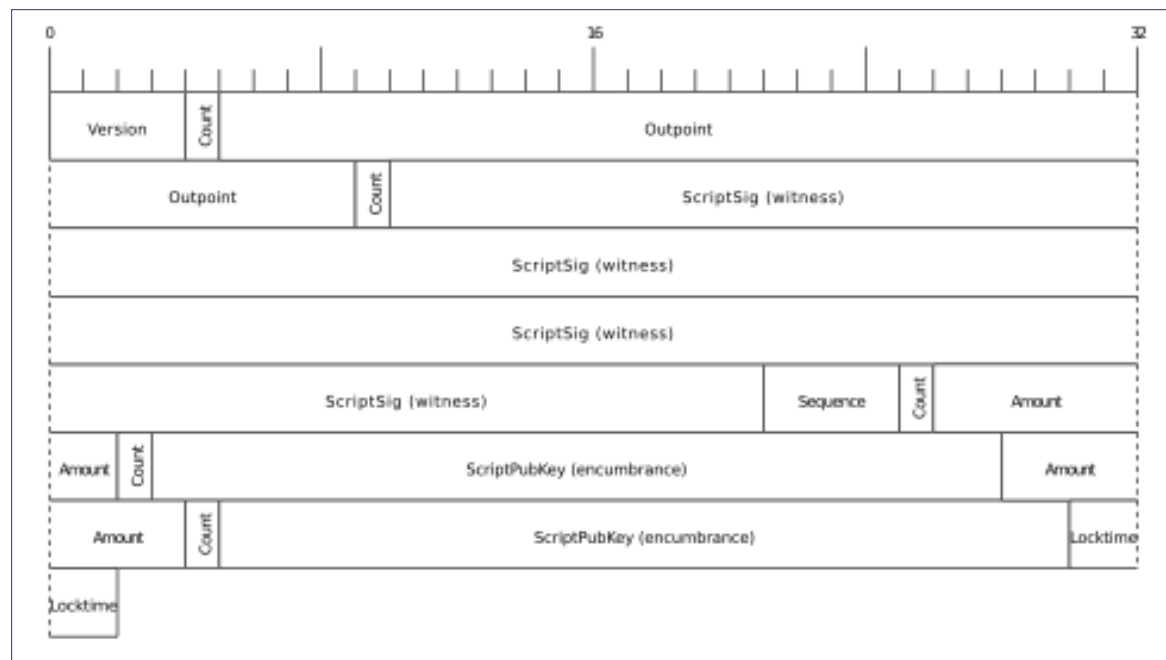
Segregated Witness (SegWit) is a protocol upgrade proposed on December 21st, 2015 and activated on August 24, 2017 through a soft-fork, an opt-in upgrade to the Bitcoin consensus rules and network protocol. Essentially, it is an architectural change to Bitcoin transactions that aims to move the witness data from the scriptSig field into a separate witness data structure that accompanies a transaction. By creating this new data field, a modification in a block's size is evaluated and was also introduced with a concept called Block Weight. There are many different scripts and address types for transactions that implement Segregated Witness.

Witness Data

Every Bitcoin transaction is composed of many inputs, which were previously UTXOs (Unspent Transaction Outputs). In simple terms, inputs are the coins you spend. A user has to prove to the whole network they're the owner of those inputs so they must provide a valid signature for each input which is called a ScriptSig or a Witness. To complete a transaction, one has to mark the outputs, or to which bitcoin addresses the coins will get sent, and in which proportion. The difference between the inputs and the outputs is the amount that will get paid to the block miner as a transaction fee. In the →

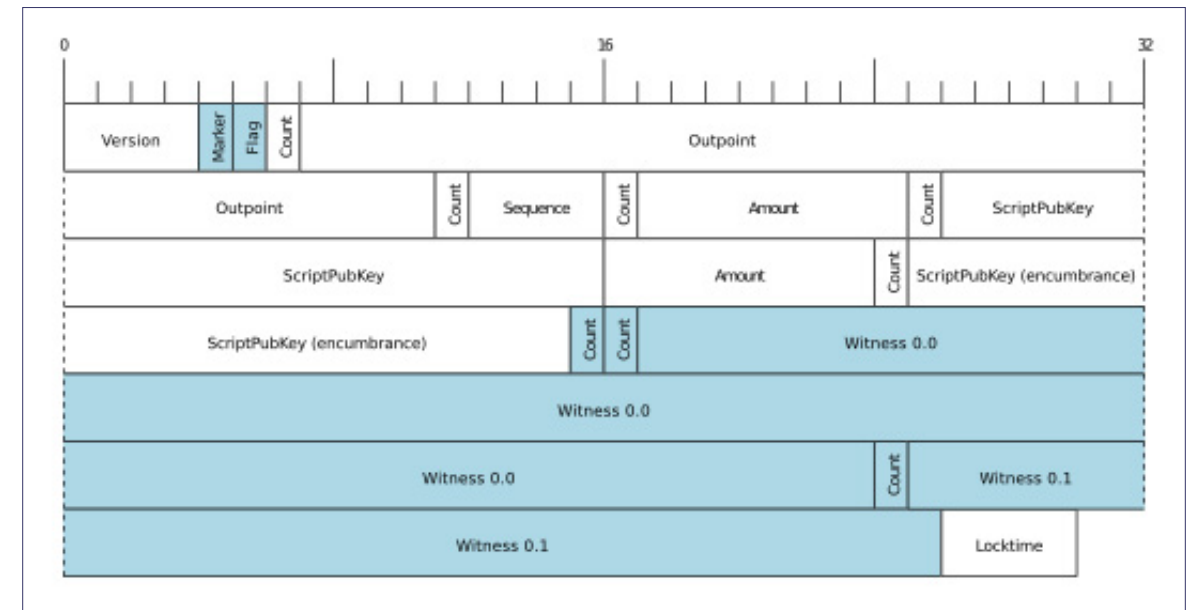
image (Figure 11) below, you can observe that the ScriptSig finds itself in the middle of a P2PKH (Pay to Public Key Hash) transaction.

Figure 11 : Decomposition of a P2PKH Transaction



On the other hand, a SegWit transaction looks differently (Figure 12), where the ScriptSig isn't anymore in the middle of the transaction but rather towards the end, it's segregated. That's all the difference there is between a legacy and a segwit transaction when it comes to their look. They are of the same size but there's simply a new data field for the SegWit transaction where the ScriptSig used to be.

Figure 12 : Decomposition of a SegWit Transaction



To legacy software, which doesn't include the SegWit upgrade, the Witness data field isn't viewable, only the transaction data without it, called Stripped data. This signifies that running legacy software isn't secure anymore because it can't verify the signature related to inputs of SegWit transactions. Also, legacy software enforces the block size limit of 1 MB, but if they can't view the Witness data of SegWit transactions, how can they count that data and make sure it doesn't surpass 1MB?

Block Weight

For the reason mentioned above, the block size limit is now irrelevant and the way blocks are limited is done through the introduction of a new con- →

cept: block weight. Since SegWit is a soft-fork, every protocol modification it brings has to match up with the requirements of legacy software so the block size couldn't be raised, it had to be bypassed.

Given that legacy software is still receiving all the Stripped data, the sum of all that received information still has to be under 1MB under the new rule. Block weight is measured in weight units and their limit is 4 million. Since there can only be a million of Stripped data bytes in a block, each Stripped data byte is equal to 4 weight units.

However, Witness data is calculated in a different way. Instead of being multiplied by 4, a witness data byte is simply equal to a weight unit which means that theoretically, if a block was composed of witness data bytes only, the new block size limit could go as high as 4 MB. In reality, a transaction always requires a minimum of Stripped data which makes the practical limit 2.4 MB if all transactions in a block are SegWit. This upgrade is remarkable by achieving a block size increase without making legacy software incompatible through a hard-fork.

Segwit Scripts and Addresses Types

In Bitcoin's early days, the concept of addresses didn't exist and folks would send coins to an I.P. address. Thankfully, P2PKH (Pay to Public Key Hash) was introduced which allowed transactions to be sent to bitcoin addresses. They're now called Legacy addresses and can be identified by the "1" found at their beginning.

Some time later, P2SH (Pay to Script Hash) transactions were added so that transactions could be programmable and functions such as multi-signature schemes or timelock were now easily possible. A user sending coins doesn't have to deal with the script, they just send it to an address that begins with "3" and the script is hidden in the address.

The SegWit Upgrade has introduced a new type of address that begins with a "bc1" and all transactions with that address are natively Segregated Witness. They're also commonly known as bech32 addresses and two types of scripts use that address format, P2WPKH (Pay to Witness Public Key Hash) and P2WSH (Pay to Witness Script Hash) which are very similar to their previous versions, but they are SegWit native.

Since bech32 is an address format not recognized by legacy software, SegWit transactions are also possible to do with P2SH transactions where the Segregated Witness conditions are included in the script. They're more commonly known as P2SH Wrapped and look no different from regular P2SH addresses. However, whenever they are spent and the script has to be revealed, the Stripped data is bigger than regular P2SH transactions, of 21 bytes when it's a P2SH-P2WPKH and 35 bytes when it's a P2SH-P2WSH.

Benefits of Segregated Witness

Now that we understand the technical improvement, let's quickly explore its benefits.

Segwit Transactions Pay Less Fees

You've always heard that SegWit transactions pay less in fees, but if they're of the same size, how is that possible? With the introduction of block weight, fee calculation has also changed. Instead of fees being calculated based on the bytes of a transaction, they're calculated on the virtual bytes notion, which is simply the block weight divided by four. For legacy transactions, bytes are equal to virtual bytes but for SegWit transactions, the Witness data pays four times less fees.

To determine how many fees could be saved by using bech32 instead of legacy or P2SH transactions, on each input, you have to multiply the ScriptSig by 3, then sum them and divide it by the total weight of the transaction. You will get the percentage of fees you could save. For SegWit Wrapped, you have to subtract either 21 bytes (for P2SH-P2WPKH) or 35 bytes (for P2SH-P2WSH) times four from the sum of all ScriptSig multiplied by three.

Bech32 transactions are preferable since they can substantainly make one save more fees than a SegWit Wrapped transaction. The transaction fee saved will mostly depend on the amount of inputs a transaction has and there's more potential for fee saving when it comes to multi-signature trans-

actions. Fee saving for single input transactions can go from as low as 26% for a single signature P2SH Wrapped towards 52% for a 2 of 3 multi-signature Native SegWit transaction. When it comes to multi input transactions, fee saving on the [biggest transaction ever](#) would be 58%.

Block Size Increase

As mentioned earlier, SegWit allows for a block size increase through the replacement of the previous limit with the introduced block weight concept. The limit depends on the adoption of SegWit since if all transactions are Legacy or P2SH ones, the block size limit of 1 MB is still on. As mentioned earlier, if there's a complete SegWit adoption, blocks could be as big as 2.4 MB.

Transaction Malleability

When you propagate a transaction, it makes its way through the peer-to-peer network and it waits in the mempool until it's included in a block. While it's unconfirmed, a part of the transaction can be modified by a node due to transaction malleability issues and the transaction would still be valid and the important part (where it's going) can't be changed. However, since an information was changed, the transaction id hash is now different from what you had when you propagated the transaction. SegWit transactions are not vulnerable to this.

Lightning Network

Finally, through the transaction malleability fix, SegWit makes the safe deployment of the Lightning Network a reality, which is a technology to scale Bitcoin off-chain.

2020's Picture of SegWit's Adoption

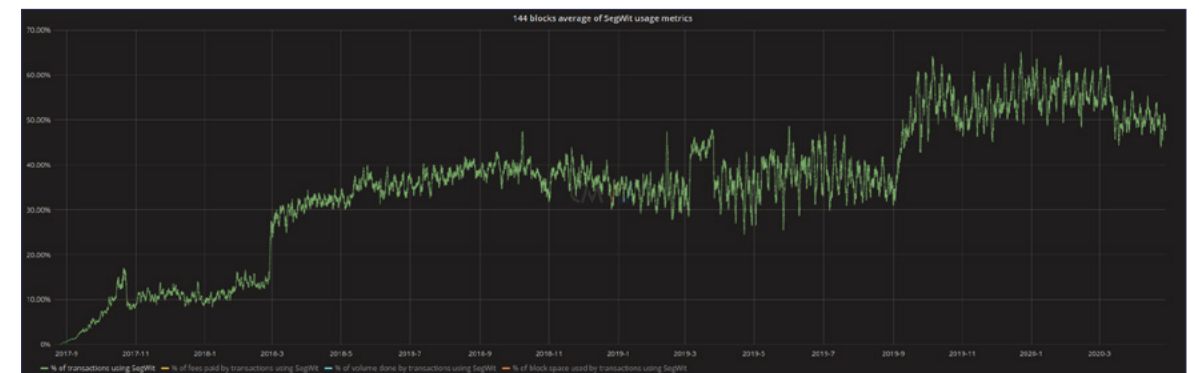
Since Segregated Witness has existed since the 25th of August 2017, there's much less data to analyse to determine usage compared to Transaction Batching. We've used the same data site, txstats.com, to get the data of SegWit Adoption that regroups four different metrics as seen on the charts below (Figures 13-16):

- Percentage of transactions using SegWit (Green)
- Percentage of fees paid using SegWit (Yellow)
- Percentage of transacted volume using SegWit (Blue)
- Percentage of block space used by SegWit transactions (Orange)

Analyzing Segregated Witness Adoption Data

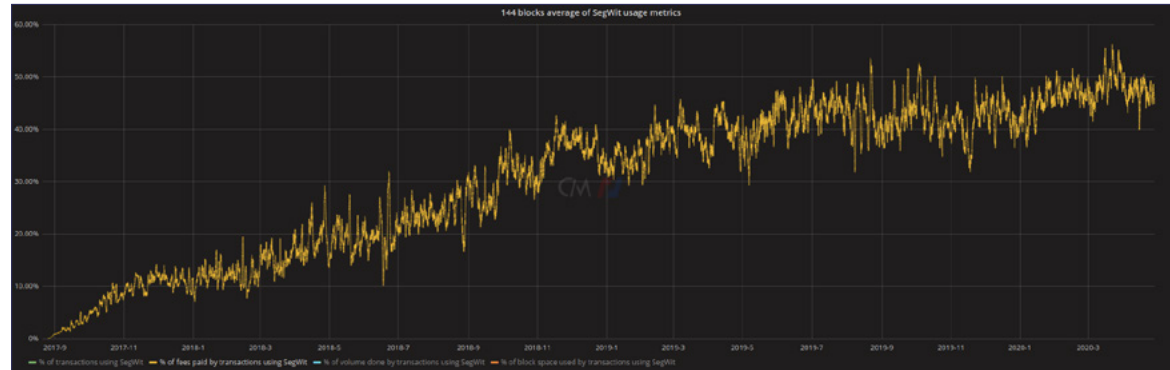
We can observe in the following chart, SegWit transactions adoption (Figure 13), that three distinct periods have taken place. The first began on SegWit's inception and near March 2018 where adoption never got higher than 20%. The second period began with a gradual jump from 16% to 30% and it never went back down again, it stayed in between 30-45% for more than a year. In September 2019, there was another great jump which took it to the range of 50-60% for many months, up until the second week of March 2020 where it regressed to 40-50%.

Figure 13 : Percentage of SegWit Transactions over Total (August 2017 to April 2020)



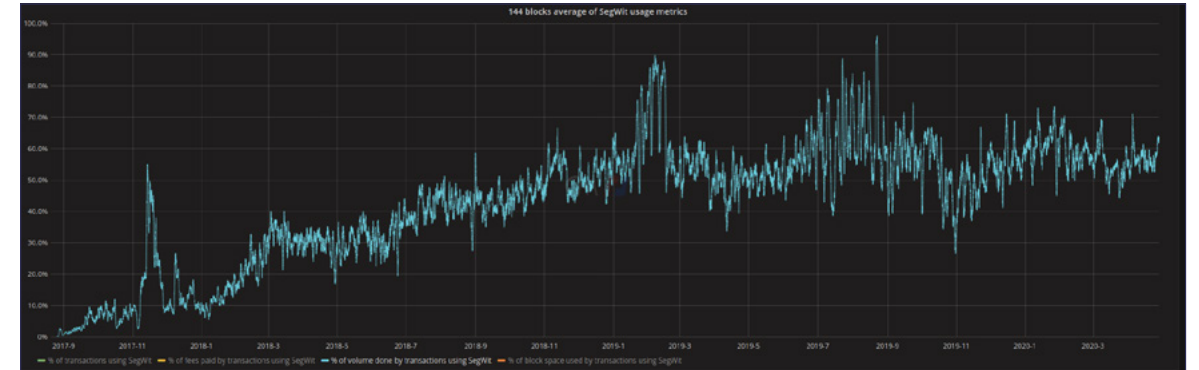
The next chart (Figure 14) shows fees paid from SegWit adoption rose from the beginning until November 2018 when it attained 35% and marked a new stability in between 30 to 50%, but always pushing slowly higher. Recently, since January 2020, it hasn't gone under 40% and has even burst upwards of 50% to reach 55% on March 23rd 2020.

Figure 14 : Percentage of Fees Paid by SegWit Transactions Over Total (August 2017 to April 2020)



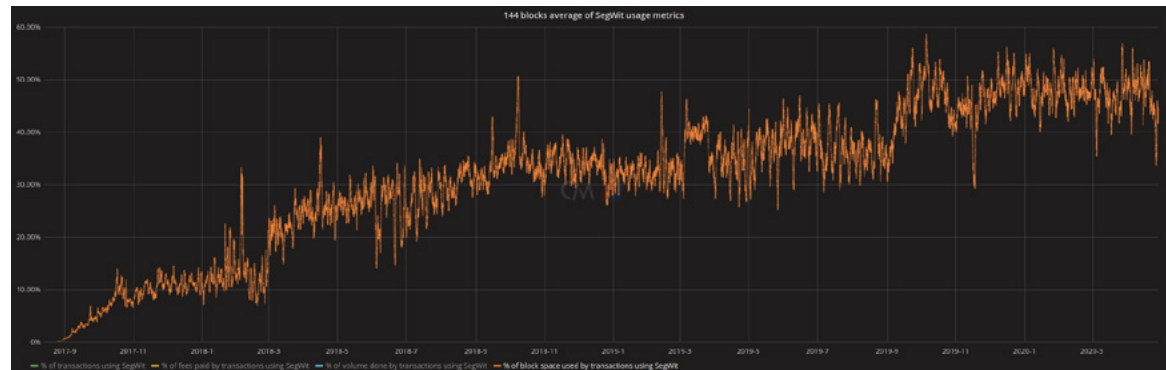
Volume by SegWit Transactions (Figure 15) is probably the most volatile chart of all and is also marked by having weekly long periods that come out of the lot. The first was in December 2017, when it surged to 50% for a few days but was consistently higher for weeks but dropped back to the tens. It rallied for a long year to regain the 50s and has since stayed in that range but with periods of higher highs such as in August 2019. It attained a high of 95% during that long volatile period but has since established in a range between 40 to 70%.

Figure 15 : Percentage of Volume by SegWit Transactions Over Total (August 2017 to April 2020)



The last metric of SegWit adoption, consumption of block space (Figure 16), has four periods but with less pronounciation than the first chart. It's also characterized by having pronounced but small moments that come out of the lot, which are probably only blocks or days long. First, it was quickly growing but remained under 20% until March 2018, where it entered the second period where adoption was more stable in the 20's but still flirting with the 30's. It succeeded by bursting through around September 2018 into the 30s where it stayed for a whole year until September 2019. Ever since, it's been playing between 40 and 55% but testing upwards a few times.

Figure 16 : Percentage of Block Space by SegWit Transactions Over Total (August 2017 to April 2020)



We can observe that SegWit adoption consistently goes up even if it has slowed down in the last year, unlike Batching which has been stuck in the same zone for a couple years now.

Segregated Witness Exchange Adoption

Many of the exchanges adopting Batching have also adopted SegWit such as

- BTSE
- Bull Bitcoin
- Gemini
- Hitbtc
- River Financial
- Bitfinex
- Bitstamp
- Coinbase
- Kraken
- Shapeshift

A few more can be added to the list, by announcements they have made :

- Bitwala
- Bitso
- Bitflyer
- Changelly
- Okex

In December 2019, a big news made surface, BitMex had joined many others by finally adopting Segregated Witness. [Else, it's been talked on Twitter that Binance will do it this year in exchange for Udi Wertheimer's endorsement.](#) [SegWit in our scenario](#)

SegWit in our Model

In the previous sections, we explained the theoretical virtues and benefits derived from SegWit. This improvement elegantly resolves issues with malleability, but in our case we're mostly interested in the possible advantages it could bring to the network and its actor in terms of scalability. As we will see with our data analysis below, Bitcoin users and especially Bitcoin services providers such, as exchanges, would have strongly benefited from SegWit if they would have implemented SegWit from the beginning.

The Bitcoin network would also have benefited from better press in regards of its transactional capacity and costs if SegWit would have been implemented on a wider scale. The bull run of 2017, and especially the last months of 2020, have spawned a wide range of critics in regards to the enormous fees that were paid to miners. According to bitinfocharts.com (Figure 17), during the peak of the bull run, the average transaction fee was around \$55USD. That amounted for close to 1,000 satoshi per byte at the time. On April 21st 2020, a regular bitcoin user can expect a transaction to pass within 6 blocks by paying less than 10 sats/vbyte. Therefore the cost to do a bitcoin transaction during late 2017 was over 100 times higher than it is close to today.

Figure 16 : Bitcoin Average Transaction Fee Historical Chart



We will discover the real-world implications of this improvement with the information we have collected and triaged below.

The analysis and graphics presented below are based on data collected from 143,199 blocks collected by using Blockstream's API. We analysed from block 481,825, which happened on the 24th of August 2017, until the 637,090th block on the 30th of June 2020. Our method goes through every input of every transaction and if the input isn't a SegWit Native one, it calculates the amount of block weight it could save, which can then indicate to us the amount of fees it could save. Finally, we collect the block weight and block fee of each block in reality and also collect the potential block weight and potential block fee of our model by summing up the results of each transaction. You can find the repository of our code used [here](#). The blocks weights and the fees paid to the miners over this period have been computed and compiled on a monthly basis. In order to demonstrate the savings in efficiency in terms of block weight and related costs savings, we juxtaposed this data with a theoretical scenario in which 100% of the transactions were using SegWit.

Here are the main takeaways of the data collected from the from the 24th of August 2017 until the 30th of June 2020:

- There is the equivalent of 516.71 GB of weight units that were used by transactions.
- Over 96534.33 bitcoins were paid in fees to miners. At the time of writing in April 2020, this amounts to a total of around \$892,942,552USD (with a Bitcoin price of \$9250.00USD).
- Transactional data could have been reduced to 327.59 GB weight units using SegWit, down 189.12GB from 516.71 GB actually used. This represents a drop of 36.60% in terms of space saved.
- Over 36,685.72 bitcoins could have been saved by Bitcoin users if they would have all been using SegWit. Fees would have amounted to 59,848.61 bitcoins, down from 96,534.33 bitcoins which represents savings of 38.00%. At the time of writing in July 2020, savings of 36,685.72 bitcoins would represent a staggering number of \$339,342,910 USD dollars (with a Bitcoin price of \$9250.00USD).

Data from January 2012 to March 2020 - Transaction Fees

In the first graphic (Figure 18), we compared the transaction fees paid in Bitcoin month over month to the sum of fees that would have been paid if SegWit was fully supported by all the market participants of the Bitcoin Network since the beginning of its implementation. The blue bars represent

the calculated monthly sums that were paid in reality to the miners and the orange bars represent the theoretical fees that would have been paid.

You can quickly notice that the theoretical sums are all lower than the actual fees paid. This of course is self-evident as the SegWit implementation redefined how data is calculated inside a transaction and a segwit transaction always takes up less blockweight than a regular non-segwit transaction. Transaction fees are calculated according to a ratio of satoshis to block weight units. Therefore the less weight units your transaction uses, the cheaper it will be compared to the same non-SegWit transaction, all other things remaining equal, such as the sats/vbyte ratio.

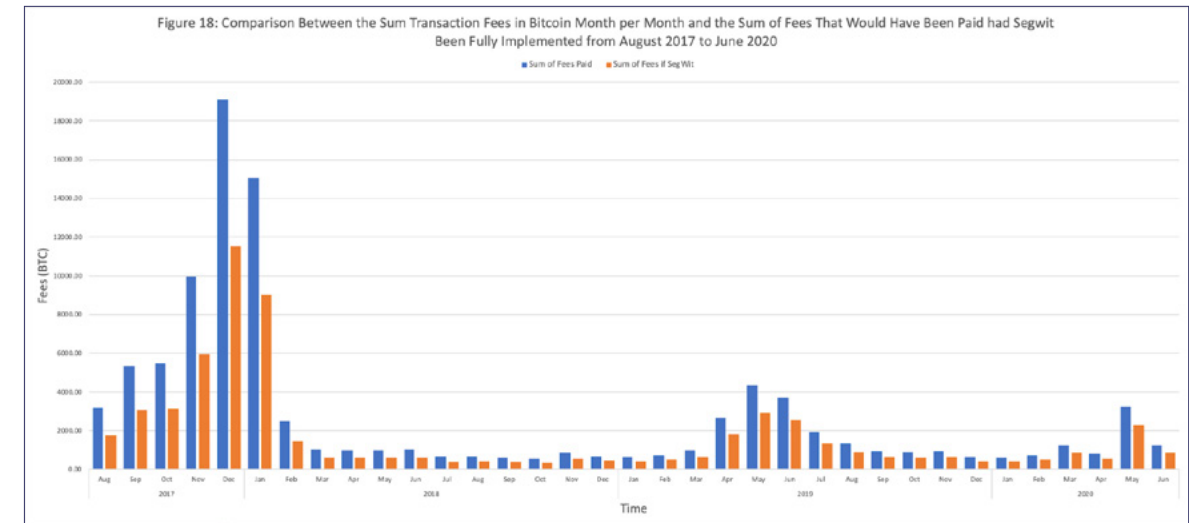
The graph gives us insightful information on the bitcoin fee market. We can see a prominent increase for the fees paid in real life in the last two months of 2017 and January 2018. We can also observe a significant increase in fees over the span of April, May and June 2019. The two increases in fees coincide with significant positive price action in the Bitcoin market. The price rose from \$7,060.00 USD to a maximum of \$19,665.39 USD and \$4,140 USD to a maximum of \$13,000 USD for the first and second periods respectively (according to coingecko). In both cases the price rose approximately 300%.

There are also two low fee periods, the first one spawning from February 2018 to March 2019 and the second one from July 2019 up until March 2020. Both periods experienced bearish price action overall. This leads us to →

believe that transaction fees rise considerably as Bitcoin price rises and are considerably lower during downward price action. This can be explained by higher transaction activity and demand for Bitcoin during bull markets.

The first three most expensive months in terms of transaction fees were December 2017 (19,119.57 bitcoins), January 2018 (15,049.27 bitcoins) and November 2017 (9,964.34 bitcoins). When calculating the relative percentage of the total fees of these three months to the total fees paid during the whole analyzed period, they represent 19.81%, 15.59%, 10.32% respectively, and sum up to a staggering 45.72%. The fees paid are therefore highly concentrated in a short span of time, 45.72% of the fees have been incurred in just 8.57% of the identified time period (3 months over 35 months). We arrive at a similar conclusion with the theoretical fees that would have been paid with the fully implemented SegWit scenario with fees totaling 20.70%, 16.45% and 10.97% and amounting to 48.12% for the three most expensive months. Not surprisingly, from the 35,067.61 bitcoins that would have been saved in fees with a complete SegWit implementation, 17,656.54 (50.35%) bitcoins would have been saved in these same three months, representing close to \$158,026,047 USD using Bitcoin price at the time of writing of \$8,950.00USD.

This makes us believe that SegWit benefits are mostly apparent when the rising price of Bitcoin triggers an increase in the total activity on the Bitcoin network, fomenting a relative scarcity for the block space and creating a bidding war of transaction fees from bitcoin users.



All in all, even if close to a half of the possible savings in our theoretical scenario would have been in just three months, the savings made over the remaining months are still significant.

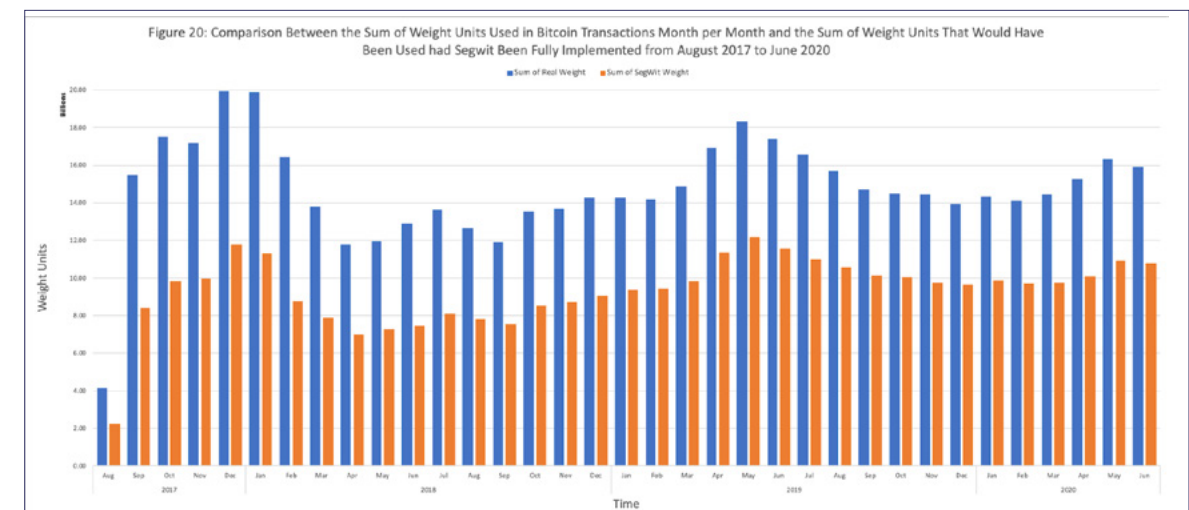
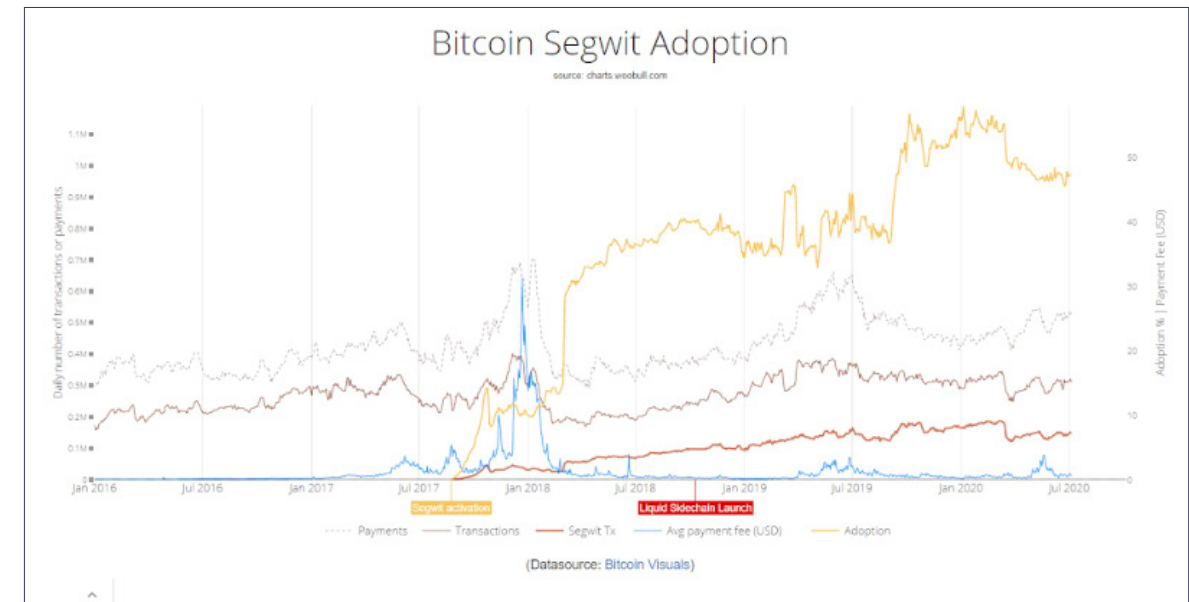
With the graphic displayed below we can see that the second busiest period in terms of on-chain activity during the analyzed time period is also coinciding with the previously identified periods. The months of April, May and June 2019 were when a lot of fees could have been saved. In fact around 3,411.89 bitcoins could have been spared in fees, totaling \$30,536.415 USD.

Curiously enough, the period from April to June 2019 almost reached the peak of daily number of transactions of the 2017 mania. It's record of 661,000 daily transactions is short of about 46,000 transactions of the 707,000 daily transactions record of 2017, only 6.51% lower. So why exactly do the total fees paid in real and possible savings are significantly lower in →

2019 than 2017? This is indeed highly linked to SegWit’s level of adoption by Bitcoin users and market participants. At the time of the bull market of 2017, SegWit just got introduced through a soft-fork and its benefits weren’t widely recognized yet and resulted in only a 10% adoption rate. Although, as more exchanges and market participants were benefiting from it, it had a larger impact in terms of the fees that had to be paid to miners when transaction activity surged again in April, May and June 2019. At the peak of daily transactions previously identified at 661,000, SegWit adoption was estimated to hover around 40%, a 30% increase from the previous high traffic period. We notice that awareness increases as its use case becomes more pertinent. The lag between the spike in SegWit usage and the dramatic fee increases at the end of 2017 and mid-2019 demonstrates the reduction of information asymmetry as users actively seek ways to operate with Bitcoin efficiently.

Also, if SegWit hadn’t reached that level of adoption at the time of April, May and June 2019, transaction fees would have been significantly higher than they were in reality, this means that our theoretical scenario would also have rendered greater possible savings over that period. Therefore, we can conclude that the total reduction of fees is significant when one chooses to adopt SegWit with total savings accounting to 36,685.72 bitcoins or over \$339,342,910 USD dollars (with a Bitcoin price of \$9250.00USD) at the time of writing.

Figure 19: Level of SegWit Adoption and Transactions Made and Bitcoin Payments, Transactions and Average Fees Paid from January 2016 to July 2020



Block Weight Analysis

In the graphic (Figure 20) we compared the block weight used by Bitcoin transactions month per month to the block weight that would have been used had SegWit been fully supported by all the market participants of the Bitcoin Network since the beginning of its implementation. The blue bars represent the calculated monthly sums of block weight that were used by transactions and the orange bars represent the theoretical block weight that would have been used with a full SegWit implementation.

As explained in the technical section, SegWit is a fairly straightforward equation that redefines how space is treated inside a block. This explains the relative steady proportion between the orange bars (theoretical weight) and the blue bars (weight used in reality) no matter how much block weight was used in a particular month. However, you can notice a slow but noticeable reduction of the difference between the two sets of data. This is due to the fact that the amount of non-SegWit data that could benefit from SegWit's implementation is constantly shrinking as SegWit adoption rises. This is somewhat more noticeable when looking at the Table 2 (see Appendix), you can see that possible savings in terms of block weight passed from an average of 43.14% in 2017, to 40.22% in 2018, to 32.82% in 2019 to 31.59% in 2020 (so far).

Halving Three Month Period - Transactional Fees

As we can see in Figure 18 and Table 1 in the Annex, the months following March have been quite interesting. They differentiate themselves from the previous months with relatively higher fees paid to miners by Bitcoin users and relative possible savings that could have been made during that period of three months (April, May and June).

This statement is especially true for the month of May, with over 3,252.40 bitcoins paid in transactional fees, which is 258.57% higher than the second most expensive month of 2020, which is June with 1,257.82 bitcoins paid to miners.

Overall in these three months (April, May and June 2020), 1,618.12 bitcoins could have been saved by Bitcoin users if Segwit was to be adopted at a 100% rate when applicable. At the time of writing this update in July 2020, with a price of \$9250.00US per Bitcoin, that would represent \$14,967,610 US.

Segwit follow-up update from March 2020 to July 1st 2020 - Block Weight

Since the original publication of the Case Study in April 2020, we have updated the data and charts from March 2020 to July 1st 2020. The following paragraph wasn't in the original publication.

SegWit

As we can see in Figure 20, there is an increase in the sum of gigabytes of weight units used in the Bitcoin blockchain during the last three months analyzed. April, May and June have had 15.26 GB, 16.30 GB and 15.93 GB respectively, totalling 47.49 GB of weight units in total. With the usage of Batching at a 100% level when applicable, a total of 15.68 GB of weight units could have been spared.

Conclusion

Bitcoin network fees are a crucial and inevitable expense that all Bitcoin users, particularly companies, have to deal with. Long-term successful enterprises will be those that manage this ever increasing cost through strategies such as leveraging SegWit, Payment Batching and much more.

In our analysis, full SegWit adoption would've allowed users to save up an additional 40% in transaction fees. Since August 2017, users could have saved up to 36,685.72 bitcoins according to the data collected in this report. We have identified and collected transactions that could have been batched since January 2012 in order to determine the practical savings that users would have obtained by employing this method. The data collected indicates that on average, those who have not utilized batching have overpaid 12% in fees. In other words, 21,131.39 bitcoins could have been saved using batching.

In total, users could've saved 57,817.11 BTC in fees since 2012. These fees were substantially higher during the 2017-2018 period. At \$9250 USD per Bitcoin (time of writing), this is equivalent to \$534,808,267.5 USD. By increasing available block size and later block weight through these techniques, less competition would've taken place and thus, fees would've probably never gotten so high during the Bitcoin all time high's of 2017. We can calculate many things but we can only imagine the complete repercussions these actions would've had, had they been extensively employed at the time.

Conclusion

Today, SegWit usage is around 50% and payment batching has been adopted by many exchanges. When the next bull market is around and fee competition becomes a daily reality again, we might not have similar consequences on the network. On the other hand, no one could've imagined the demand in 2017 and we probably can't imagine what the future users have to say. However, we can always compute and display what a 100% adoption scenario would look like and hopefully turn efficient block space use into tomorrow's reality.

Appendix

Table 1: Comparison of Transaction Fees Paid With and Without SegWit and Possible Savings from a Total SegWit Adoption from August 2017 until June 2020

Date	Sums of Fees Paid (In BTC)	Monthly paid fee over yearly paid fees (%)	Fees over total fees paid during the analyzed period. (%)	Theoretical sums of fees if Segwit was fully adopted. (In BTC)	Theoretical Sums of fees saved if Segwit was fully adopted (In BTC)	Theoretical saved fees over sums of fees paid (%)	Monthly theoretical saved fee over theoretical saved yearly sums of fees (%)	Theoretical fees saved over total theoretical fees saved during the analyzed period. (%)
2017	43105.14		44.65%	25438.77	17666.37	40.98%		48.16%
Aug	3198.98	7.42%	3.31%	1771.47	1427.51	44.62%	8.08	3.89%
Sep	5365.60	12.45%	5.56%	3052.11	2313.49	43.12%	13.10%	6.31%
Oct	5456.65	12.66%	5.65%	3151.34	2305.31	42.25%	13.05%	6.28%
Nov	9964.34	23.12%	10.32%	5939.96	4024.38	40.39%	22.78%	10.97%
Dec	19119.57	44.36%	19.81%	11523.89	7595.68	39.73%	43.00%	20.70%
2018	25704.82		26.63%	15469.42	10235.41	39.82%		27.90%
Jan	15049.27	58.55%	15.59%	9013.96	6035.32	40.10%	58.97%	16.45%
Feb	2494.12	9.70%	2.58%	1466.80	1027.32	41.19%	10.04%	2.80%
Mar	1017.59	3.96%	1.05%	599.10	418.50	41.13%	4.09%	1.14%
Apr	992.18	3.86%	1.03%	597.82	394.36	39.75%	3.85%	1.07%
May	1009.55	3.93%	1.05%	599.99	409.55	40.57%	4.00%	1.12%
Jun	1043.16	4.06%	1.08%	618.00	425.16	40.76%	4.15%	1.16%
Jul	669.31	2.60%	0.69%	403.96	265.35	39.65%	2.59%	0.72%
Aug	694.25	2.70%	0.72%	413.84	280.41	40.39%	2.74%	0.76%
Sep	618.86	2.41%	0.64%	383.27	235.59	38.07%	2.30%	0.64%
Oct	545.35	2.12%	0.56%	348.78	196.57	36.05%	1.92%	0.54%

Table 1: Comparison of Transaction Fees Paid With and Without SegWit and Possible Savings from a Total Segwit Adoption from August 2017 until June 2020 (Continued)

Nov	871.72	3.39%	0.90%	569.39	302.34	34.68%	2.95%	0.82%
Dec	699.46	2.72%	0.72%	454.52	244.94	35.02%	2.39%	0.67%
2019	19787.71		20.50%	13447.83	6339.88	32.04%		17.28%
Jan	634.63	3.21%	0.66%	409.36	225.26	35.50%	3.55%	0.61%
Feb	749.31	3.79%	0.78%	493.88	255.43	34.09%	4.03%	0.70%
Mar	988.05	4.99%	1.02%	657.53	330.52	33.45%	5.21%	0.90%
Apr	2684.63	13.57%	2.78%	1817.69	866.94	32.29%	13.67%	2.36%
May	4337.20	21.92%	4.49%	2949.44	1387.76	32.00%	21.89%	3.78%
Jun	3706.17	18.73%	3.84%	2548.97	1157.19	31.22%	18.25%	3.15%
Jul	1945.05	9.83%	2.01%	1337.86	607.20	31.22%	9.58%	1.66%
Aug	1338.48	6.76%	1.39%	920.28	418.20	31.24%	6.60%	1.14%
Sep	924.96	4.67%	0.96%	634.39	290.57	31.41%	4.58%	0.79%
Oct	894.47	4.52%	0.93%	609.22	285.25	31.89%	4.50%	0.78%
Nov	951.43	4.81%	0.99%	641.39	310.04	32.59%	4.89%	0.85%
Dec	633.33	3.20%	0.66%	427.82	205.51	32.45%	3.24%	0.56%
2020	7936.66		8.22%	5492.59	2444.07	30.79%		6.66%
Jan	618.55	7.79%	0.64%	417.20	201.35	32.55%	8.24%	0.55%
Feb	743.69	9.37%	0.77%	508.78	234.91	31.59%	9.61%	0.64%
Mar	1250.08	15.75%	1.29%	860.39	389.70	31.17%	15.94%	1.06%
Apr	814.11	10.26%	0.84%	555.14	258.97	31.81%	10.60%	0.71%
May	3252.40	40.98%	3.37%	2277.85	974.55	29.96%	39.87%	2.66%

Table 1: Comparison of Transaction Fees Paid With and Without SegWit and Possible Savings from a Total Segwit Adoption from August 2017 until June 2020 (Continued)

Jun	1257.82	15.85%	1.30%	873.23	384.60	30.58%	15.74%	1.05%
-----	---------	--------	-------	--------	--------	--------	--------	-------

Grand Total	96534.33		35.48	59848.61	36685.72	38.00%		
--------------------	-----------------	--	--------------	-----------------	-----------------	---------------	--	--

Table 2: Comparison of Weight Units With and Without SegWit and Possible Savings from a Total Segwit Adoption from August 2017 until June 2020

					Theoretical saved sums of weight units over yearly theoretical saved weight units (%)	
2017	74189644793	42185494260	32004150533	43.14%		16.92%
Aug	4140784183	2221327390	1919456793	46.35%	6.00%	1.01%
Sep	15489022172	8388977472	7100044700	45.84%	22.18%	3.75%
Oct	17492545015	9835378117	7657166898	43.77%	23.93%	4.05%
Nov	17153808738	9969706397	7184102341	41.88%	22.45%	3.80%
Dec	19913484685	11770104884	8143379801	40.89%	25.44%	4.31%
2018	166405461055	99483137847	66922323208	40.22%		35.39%
Jan	19887889587	11309860237	8578029350	43.13%	26.80%	4.54%
Feb	16421718306	8743637722	7678080584	46.76%	23.99%	4.06%
Mar	13799914242	7884311998	5915602244	42.87%	18.48%	3.13%
Apr	11752663318	6995784542	4756878776	40.47%	14.86%	2.52%
May	11953288799	7285232951	4668055848	39.05%	14.59%	2.47%
Jun	12892966350	7465096812	5427869538	42.10%	16.96%	2.87%
Jul	13634869158	8113453030	5521416128	40.49%	17.25%	2.92%
Aug	12644846870	7811249678	4833597192	38.23%	15.10%	2.56%
Sep	11919166120	7558147293	4361018827	36.59%	13.63%	2.31%
Oct	13543093156	8536931346	5006161810	36.96%	15.64%	2.65%

Table 2: Comparison of Weight Units With and Without SegWit and Possible Savings from a Total Segwit Adoption from August 2017 until June 2020 (Continued)

Nov	13688115938	8721391329	4966724609	36.28%	15.52%	2.63%
Dec	14266929211	9058040909	5208888302	36.51%	16.28%	2.75%
2019	185766321352	124790783951	60975537401	32.82%		32.24%
Jan	14262088440	9372514213	4889574227	34.28%	15.28%	2.59%
Feb	14181846224	9432802570	4749043654	33.49%	14.84%	2.51%
Mar	14858706915	9833728587	5024978328	33.82%	15.70%	2.66%
Apr	16921269022	11330951891	5590317131	33.04%	17.47%	2.96%
May	18346803433	12175296091	6171507342	33.64%	19.28%	3.26%
Jun	17384491299	11557614028	5826877271	33.52%	18.21%	3.08%
Jul	16543051494	10983817421	5559234073	33.60%	17.37%	2.94%
Aug	15713971320	10550063639	5163907681	32.86%	16.14%	2.73%
Sep	14715822301	10112588240	4603234061	31.28%	14.38%	2.43%
Oct	14479185064	10031825382	4447359682	30.72%	13.90%	2.35%
Nov	14444127351	9764043436	4680083915	32.40%	14.62%	2.47%
Dec	13914958489	9645538453	4269420036	30.68%	13.34%	2.26%
2020	90343545030	61127579278	29215965752	32.34%		15.45%
Jan	14323778519	9861760553	4462017966	31.15%	13.94%	2.36%
Feb	14085077505	9689203229	4395874276	31.21%	13.74%	2.32%
Mar	14447811643	9766882816	4680928827	32.40%	14.63%	2.48%
Apr	15261642530	10110790330	5150852200	33.75%	16.09%	2.72%
May	16297488764	10916302097	5381186667	33.02%	16.81%	2.85%

Table 2: Comparison of Weight Units With and Without SegWit and Possible Savings from a Total Segwit Adoption from August 2017 until June 2020 (Continued)

Jun	15927746069	10782640253	5145105816	32.30%	16.08%	2.72%
-----	-------------	-------------	------------	--------	--------	-------

Grand Total	516704972230	327586995336	189117976894	36.60%		
--------------------	---------------------	---------------------	---------------------	---------------	--	--

Table 3: Comparison of Transaction Fees Paid With and Without Batching and Possible Savings from a Total Batching Adoption from January 2012 until June 2020

Date	Sum of fees paid (In BTC)	Theoretical Sums of fees if Batching was fully adopted (In BTC)	Theoretical Sums of fees saved if Batching was fully adopted (In BTC)	Theoretical saved fees if Batching was fully adopted over sums of fees paid (%)	Monthly theoretical saved fees over sum of theoretical saved yearly fees if Batching was fully adopted (%)	Theoretical sums of fees saved over total theoretical fees saved during the analyzed period (%)
2012	6798.41	5225.29	1573.12	23.14%		7.44%
Jan	582.04	550.35	31.69	5.44%	2.01%	0.15%
Feb	157.12	146.52	10.59	6.74%	0.67%	0.05%
Mar	155.38	146.54	8.84	5.69%	0.56%	0.04%
Apr	164.91	151.92	12.99	7.88%	0.83%	0.06%
May	467.95	363.03	104.92	22.42%	6.67%	0.50%
Jun	646.24	492.00	154.23	23.87%	9.80%	0.73%
Jul	590.43	436.03	154.40	26.15%	9.82%	0.73%
Aug	777.52	556.64	220.88	28.41%	14.04%	1.05%
Sep	692.11	508.72	183.39	26.50%	11.66%	0.87%
Oct	811.29	627.39	183.89	22.67%	11.69%	0.87%
Nov	819.93	602.73	217.19	26.49%	13.81%	1.03%
Dec	933.50	643.41	290.09	31.08%	18.44%	1.37%
2013	15273.86	12405.78	2868.08	18.78%		13.57%
Jan	1319.17	944.35	374.82	28.41%	13.07%	1.77%
Feb	1416.34	1049.67	366.67	25.89%	12.78%	1.74%
Mar	1720.12	1375.47	344.65	20.04%	12.02%	1.63%

Table 3: Comparison of Transaction Fees Paid With and Without Batching and Possible Savings from a Total Batching Adoption from January 2012 until June 2020 (Continued)

Apr	1593.60	1378.64	214.96	13.49%	7.49%	1.02%
May	1589.17	1249.40	339.77	21.38%	11.85%	1.61%
Jun	1251.44	1012.75	238.68	19.07%	8.32%	1.13%
Jul	923.15	787.89	135.27	14.65%	4.72%	0.64%
Aug	1355.06	1081.29	273.77	20.20%	9.55%	1.30%
Sep	1337.16	1099.57	237.59	17.77%	8.28%	1.12%
Oct	1088.44	968.76	119.67	11.00%	4.17%	0.57%
Nov	1186.02	1031.59	154.43	13.02%	5.38%	0.73%
Dec	494.19	426.40	67.80	13.72%	2.36%	0.32%
2014	4636.34	3751.48	884.86	19.09%		4.19%
Jan	438.63	379.55	59.08	13.47%	6.68%	0.28%
Feb	396.66	330.36	66.30	16.71%	7.49%	0.31%
Mar	419.40	342.65	76.75	18.30%	8.67%	0.36%
Apr	398.02	316.09	81.93	20.58%	9.26%	0.39%
May	370.84	292.80	78.04	21.04%	8.82%	0.37%
Jun	329.09	266.32	62.76	19.07%	7.09%	0.30%
Jul	334.74	267.60	67.14	20.06%	7.59%	0.32%
Aug	371.91	303.55	68.36	18.38%	7.73%	0.32%
Sep	390.81	318.98	71.83	18.38%	8.12%	0.34%
Oct	385.20	305.75	79.44	20.62%	8.98%	0.38%
Nov	390.19	303.52	86.66	22.21%	9.79%	0.41%
Dec	410.85	324.30	86.54	21.06%	9.78%	0.41%

Table 3: Comparison of Transaction Fees Paid With and Without Batching and Possible Savings from a Total Batching Adoption from January 2012 until June 2020 (Continued)

2015	8200.63	6934.20	1266.43	15.44%		5.99%
Jan	450.14	363.56	86.57	19.23%	6.84%	0.41%
Feb	385.69	320.73	64.96	16.84%	5.13%	0.31%
Mar	451.80	373.97	77.83	17.23%	6.15%	0.37%
Apr	563.22	455.65	107.57	19.10%	8.49%	0.51%
May	495.12	402.41	92.70	18.72%	7.32%	0.44%
Jun	568.35	461.23	107.13	18.85%	8.46%	0.51%
Jul	954.15	814.08	140.07	14.68%	11.06%	0.66%
Aug	780.71	661.60	119.10	15.26%	9.40%	0.56%
Sep	827.27	705.24	122.03	14.75%	9.64%	0.58%
Oct	826.75	729.98	96.77	11.71%	7.64%	0.46%
Nov	836.84	729.63	107.21	12.81%	8.47%	0.51%
Dec	1060.60	916.12	144.48	13.62%	11.41%	0.68%
2016	22556.80	20276.68	2280.12	10.11%		10.79%
Jan	1150.70	992.84	157.86	13.72%	6.92%	0.75%
Feb	1267.60	1094.58	173.02	13.65%	7.59%	0.82%
Mar	1401.39	1244.94	156.45	11.16%	6.86%	0.74%
Apr	1613.32	1410.41	202.91	12.58%	8.90%	0.96%
May	1550.69	1392.45	158.25	10.21%	6.94%	0.75%
Jun	1871.38	1685.69	185.69	9.92%	8.14%	0.88%
Jul	1817.16	1633.06	184.10	10.13%	8.07%	0.87%

Table 3: Comparison of Transaction Fees Paid With and Without Batching and Possible Savings from a Total Batching Adoption from January 2012 until June 2020 (Continued)

Aug	2129.15	1920.29	208.86	9.81%	9.16%	0.99%
Sep	1803.90	1628.51	175.39	9.72%	7.69%	0.83%
Oct	2301.40	2105.90	195.51	8.50%	8.57%	0.93%
Nov	2644.26	2413.28	230.98	8.74%	10.13%	1.09%
Dec	3005.84	2754.74	251.10	8.35%	11.01%	1.19%
2017	100383.49	92466.63	7916.86	7.89%		37.46%
Jan	3504.90	3207.41	297.49	8.49%	3.76%	1.41%
Feb	4504.11	4033.32	470.79	10.45%	5.95%	2.23%
Mar	7096.51	6416.19	680.32	9.59%	8.59%	3.22%
Apr	6371.80	5760.91	610.89	9.59%	7.72%	2.89%
May	11678.16	10441.82	1236.34	10.59%	15.62%	5.85%
Jun	12528.41	11610.05	918.36	7.33%	11.60%	4.35%
Jul	6435.49	6042.16	393.32	6.11%	4.97%	1.86%
Aug	8463.27	7823.42	639.84	7.56%	8.08%	3.03%
Sep	5251.19	4940.34	310.85	5.92%	3.93%	1.47%
Oct	5464.06	5038.28	425.78	7.79%	5.38%	2.01%
Nov	9959.53	9211.86	747.67	7.51%	9.44%	3.54%
Dec	19126.07	17940.87	1185.20	6.20%	14.97%	5.61%
2018	25690.61	24466.04	1224.57	4.77%		5.79%
Jan	15043.70	14376.67	667.03	4.43%	54.47%	3.16%
Feb	2487.08	2413.12	73.96	2.97%	6.04%	0.35%

Table 3: Comparison of Transaction Fees Paid With and Without Batching and Possible Savings from a Total Batching Adoption from January 2012 until June 2020 (Continued)

Mar	1016.24	981.19	35.06	3.45%	2.86%	0.17%
Apr	992.81	951.25	41.56	4.19%	3.39%	0.20%
May	1009.05	966.53	42.52	4.21%	3.47%	0.20%
Jun	1042.80	999.37	43.43	4.17%	3.55%	0.21%
Jul	669.40	632.16	37.24	5.56%	3.04%	0.18%
Aug	694.45	649.72	44.74	6.44%	3.65%	0.21%
Sep	618.41	575.79	42.62	6.89%	3.48%	0.20%
Oct	545.30	503.14	42.16	7.73%	3.44%	0.20%
Nov	873.36	785.09	88.27	10.11%	7.21%	0.42%
Dec	698.01	632.03	65.98	9.45%	5.39%	0.31%
2019	19787.65	17459.94	2327.71	11.76%		11.02%
Jan	636.61	558.76	77.85	12.23%	3.34%	0.37%
Feb	747.75	645.75	102.00	13.64%	4.38%	0.48%
Mar	989.30	883.83	105.47	10.66%	4.53%	0.50%
Apr	2685.17	2316.17	368.99	13.74%	15.85%	1.75%
May	4342.98	3819.65	523.34	12.05%	22.48%	2.48%
Jun	3700.81	3305.17	395.64	10.69%	17.00%	1.87%
Jul	1943.90	1724.80	219.10	11.27%	9.41%	1.04%
Aug	1337.01	1182.53	154.48	11.55%	6.64%	0.73%
Sep	926.58	820.21	106.37	11.48%	4.57%	0.50%
Oct	894.19	789.41	104.78	11.72%	4.50%	0.50%
Nov	951.00	848.08	102.92	10.82%	4.42%	0.49%

Table 3: Comparison of Transaction Fees Paid With and Without Batching and Possible Savings from a Total Batching Adoption from January 2012 until June 2020 (Continued)

Dec	632.34	565.59	66.75	10.56%	2.87%	0.32%
2020	7939.15	7148.92	790.23	9.95%		3.74%
Jan	618.60	556.18	62.41	10.09%	7.90%	0.30%
Feb	744.09	664.92	79.17	10.64%	10.02%	0.37%
Mar	1250.83	1114.23	136.60	10.92%	17.29%	0.65%
Apr	818.16	739.81	78.35	9.58%	9.91%	0.37%
May	3251.58	2931.08	320.50	9.86%	40.56%	1.52%
Jun	1255.89	1142.69	113.20	9.01%	14.33%	0.54%

Grand Total	211266.95	190134.98	21131.97	10.00%		100.00%
--------------------	------------------	------------------	-----------------	---------------	--	----------------

Table 4: Comparison of Megabytes Used With and Without Batching and Possible Savings from a Total Batching Adoption from January 2012 until June 2020

Date	Sums of megabytes in reality. (in MB)	Theoretical sums of megabytes if batching was fully adopted. (in MB)	Theoretical saved sums of megabytes if batching was fully adopted. (in MB)	Theoretical saved sums of megabytes if batching was fully adopted over yearly theoretical saved megabytes. (%)	Theoretical saved sums of megabytes over theoretical saved megabytes of the whole analyzed period. (%)
2012	3775.71	2570.23	1205.48		3.66%
Jan	96.15	88.47	7.67	0.64%	0.02%
Feb	92.27	84.18	8.09	0.67%	0.02%
Mar	93.52	86.26	7.26	0.60%	0.02%
Apr	102.70	93.01	9.68	0.80%	0.03%
May	292.87	197.11	95.76	7.94%	0.29%
Jun	436.85	288.66	148.18	12.29%	0.45%
Jul	390.04	247.30	142.73	11.84%	0.43%
Aug	459.30	291.14	168.16	13.95%	0.51%
Sep	412.00	276.86	135.14	11.21%	0.41%
Oct	441.54	311.36	130.18	10.80%	0.40%
Nov	436.89	281.23	155.66	12.91%	0.47%
Dec	521.59	324.64	196.95	16.34%	0.60%
2013	9357.88	7439.78	1918.10		5.83%
Jan	644.41	432.36	212.05	11.06%	0.64%
Feb	726.71	502.40	224.32	11.69%	0.68%

Table 4: Comparison of Megabytes Used With and Without Batching and Possible Savings from a Total Batching Adoption from January 2012 until June 2020 (Continued)

Mar	824.48	634.43	190.05	9.91%	0.58%
Apr	843.29	714.92	128.37	6.69%	0.39%
May	841.69	643.68	198.01	10.32%	0.60%
Jun	655.88	510.62	145.25	7.57%	0.44%
Jul	558.97	460.62	98.35	5.13%	0.30%
Aug	781.24	600.58	180.66	9.42%	0.55%
Sep	718.40	577.00	141.39	7.37%	0.43%
Oct	796.82	695.89	100.93	5.26%	0.31%
Nov	979.24	838.71	140.53	7.33%	0.43%
Dec	986.74	828.56	158.18	8.25%	0.48%
2014	14486.80	11152.26	3334.53		10.13%
Jan	923.17	775.22	147.96	4.44%	0.45%
Feb	1027.73	817.95	209.78	6.29%	0.64%
Mar	1186.95	926.38	260.57	7.81%	0.79%
Apr	1097.33	828.91	268.42	8.05%	0.82%
May	1148.66	865.99	282.66	8.48%	0.86%
Jun	1083.42	843.02	240.40	7.21%	0.73%
Jul	1142.29	873.20	269.09	8.07%	0.82%
Aug	1226.55	959.15	267.40	8.02%	0.81%
Sep	1255.97	986.53	269.44	8.08%	0.82%
Oct	1377.84	1037.79	340.05	10.20%	1.03%
Nov	1456.67	1075.68	380.98	11.43%	1.16%

Table 4: Comparison of Megabytes Used With and Without Batching and Possible Savings from a Total Batching Adoption from January 2012 until June 2020 (Continued)

Dec	1560.22	1162.42	397.80	11.93%	1.21%
2015	26020.15	21285.13	4735.03		14.39%
Jan	1621.82	1245.23	376.60	7.95%	1.14%
Feb	1574.34	1254.86	319.48	6.75%	0.97%
Mar	1760.37	1395.39	364.98	7.71%	1.11%
Apr	1720.75	1328.64	392.10	8.28%	1.19%
May	1752.13	1362.53	389.60	8.23%	1.18%
Jun	1991.71	1554.24	437.47	9.24%	1.33%
Jul	2722.62	2282.99	439.62	9.28%	1.34%
Aug	2127.48	1736.29	391.19	8.26%	1.19%
Sep	2482.20	2073.94	408.26	8.62%	1.24%
Oct	2476.92	2143.36	333.57	7.04%	1.01%
Nov	2633.65	2241.53	392.11	8.28%	1.19%
Dec	3156.15	2666.12	490.03	10.35%	1.49%
2016	42565.81	37886.31	4679.50		14.22%
Jan	3221.77	2732.76	489.01	10.45%	1.49%
Feb	3334.09	2833.21	500.89	10.70%	1.52%
Mar	3273.85	2886.64	387.20	8.27%	1.18%
Apr	3315.82	2878.32	437.50	9.35%	1.33%
May	3554.35	3167.61	386.75	8.26%	1.18%
Jun	3663.96	3291.45	372.51	7.96%	1.13%

Table 4: Comparison of Megabytes Used With and Without Batching and Possible Savings from a Total Batching Adoption from January 2012 until June 2020 (Continued)

Jul	3428.04	3074.69	353.36	7.55%	1.07%
Aug	3615.04	3246.05	368.99	7.89%	1.12%
Sep	3405.11	3057.89	347.23	7.42%	1.06%
Oct	3757.06	3427.17	329.89	7.05%	1.00%
Nov	3897.38	3547.49	349.89	7.48%	1.06%
Dec	4099.34	3743.04	356.30	7.61%	1.08%
2017	52909.39	48621.79	4287.60		13.03%
Jan	4247.45	3873.67	373.78	8.72%	1.14%
Feb	4037.46	3615.73	421.73	9.84%	1.28%
Mar	4424.44	3997.05	427.39	9.97%	1.30%
Apr	4249.94	3842.71	407.23	9.50%	1.24%
May	4719.90	4205.72	514.18	11.99%	1.56%
Jun	4347.03	4030.34	316.70	7.39%	0.96%
Jul	4313.02	4048.51	264.51	6.17%	0.80%
Aug	4169.58	3874.83	294.74	6.87%	0.90%
Sep	3930.82	3683.02	247.80	5.78%	0.75%
Oct	4603.44	4253.25	350.19	8.17%	1.06%
Nov	4564.91	4236.65	328.26	7.66%	1.00%
Dec	5301.39	4960.31	341.08	7.96%	1.04%
2018	47971.96	44951.15	3020.81		9.18%
Jan	5329.31	5099.89	229.42	7.59%	0.70%

Table 4: Comparison of Megabytes Used With and Without Batching and Possible Savings from a Total Batching Adoption from January 2012 until June 2020 (Continued)

Feb	4406.28	4278.55	127.73	4.23%	0.39%
Mar	3831.38	3688.23	143.15	4.74%	0.44%
Apr	3353.72	3197.89	155.83	5.16%	0.47%
May	3443.44	3271.68	171.76	5.69%	0.52%
Jun	3682.87	3513.40	169.48	5.61%	0.52%
Jul	3970.43	3735.76	234.67	7.77%	0.71%
Aug	3747.16	3479.10	268.06	8.87%	0.81%
Sep	3593.96	3305.32	288.64	9.55%	0.88%
Oct	4135.08	3780.41	354.67	11.74%	1.08%
Nov	4167.01	3730.54	436.46	14.45%	1.33%
Dec	4311.33	3870.38	440.95	14.60%	1.34%
2019	58018.97	51192.41	6826.57		20.75%
Jan	4322.29	3776.71	545.58	7.99%	1.66%
Feb	4336.94	3734.05	602.89	8.83%	1.83%
Mar	4644.70	4150.02	494.67	7.25%	1.50%
Apr	5216.62	4493.28	723.34	10.60%	2.20%
May	5709.45	5007.25	702.20	10.29%	2.13%
Jun	5436.07	4869.13	566.94	8.30%	1.72%
Jul	5119.58	4550.83	568.75	8.33%	1.73%
Aug	4863.71	4305.17	558.54	8.18%	1.70%
Sep	4675.72	4136.50	539.23	7.90%	1.64%

Table 4: Comparison of Megabytes Used With and Without Batching and Possible Savings from a Total Batching Adoption from January 2012 until June 2020 (Continued)

Oct	4627.77	4080.73	547.04	8.01%	1.66%
Nov	4565.20	4074.68	490.51	7.19%	1.49%
Dec	4500.92	4014.04	486.88	7.13%	1.48%
2020	29266.09	26367.22	2898.87		8.81%
Jan	4612.22	4118.83	493.39	17.02%	1.50%
Feb	4560.18	4068.33	491.85	16.97%	1.49%
Mar	4663.81	4164.23	499.58	17.23%	1.52%
Apr	4885.94	4432.04	453.89	15.66%	1.38%
May	5322.83	4831.56	491.27	16.95%	1.49%
Jun	5221.12	4752.23	468.90	16.18%	1.42%

Grand Total	284372.77	251466.27	32906.49		
--------------------	------------------	------------------	-----------------	--	--

References

References

- Antonopoulos, A. (2017). Mastering Bitcoin. Sebastopol, CA: O'Reilly Media
- Billfodl. (n.d.) Bitcoin Transaction Fees. [Graphs displaying historic daily average Bitcoin transaction fees]. Retrieved from <https://billfodl.com/pages/bitcoinfees>
- BitInfoCharts. (n.d.) Bitcoin average transaction fee. [Graph displaying historical average Bitcoin transaction fees]. Retrieved from <https://bitinfocharts.com/comparison/bitcoin-transactionfees.html>
- Blockstream. (n.d.) Esplora (version 2.1). [Source code]. Retrieved from <https://github.com/Blockstream/esplora/blob/a2b8e10df01fbd7bc94949d27b31662f-f18a46dd/client/src/lib/fees.js>
- Flores Echaiz, G. (2020). Ref-payment-batching. [Source code]. Retrieved from <https://github.com/Gfloresechaiz/ref-payment-batching>
- Flores Echaiz, G. (2020). all_transactions_segwit. [Source code]. Retrieved from https://github.com/Gfloresechaiz/all_transactions_segwit
- Harding, D. (2017). Ref-payment-batching. [Source code]. Retrieved from <https://github.com/harding/ref-payment-batching>
- Harding, D. (2017). Saving up to 80% on Bitcoin transaction fees by batching payments. Retrieved from <https://bitcointechtalk.com/saving-up-to-80-on-bitcoin-transaction-fees-by-batching-payments-4147ab7009fb>
- Hasu. (2018). An analysis of batching in Bitcoin. Retrieved from <https://medium.com/@hasufly/an-analysis-of-batching-in-bitcoin-9bdf81a394e0>
- Mempool. (n.d.) Mempool by vbytes. [Graph displaying mempool by vbytes (satoshis/vbyte) and Transactions weight per second (vBytes/s)]. Retrieved from <https://mempool.space/graphs#6m>
- Segregated Witness Benefits. (2016). Retrieved from <https://bitcoincore.org/en/2016/01/26/segwit-benefits/>
- Segregated Witness Wallet Development Guide. (n.d.). Retrieved from https://bitcoincore.org/en/segwit_wallet_dev
- Stack Exchange. (2018). SegWit Transaction fee/byte. Retrieved from <https://bitcoin.stackexchange.com/questions/67680/segwit-transaction-fee-byte>
- Techniques to reduce transaction fees. (n.d.). Retrieved from https://en.bitcoin.it/wiki/Techniques_to_reduce_transaction_fees
- Walker, G. (2017). Transaction Weight. Retrieved from <https://learnmeabitcoin.com/guide/transaction-weight>
- Weight Units. (2018). Retrieved from https://en.bitcoin.it/wiki/Weight_units
- Wuille, P. (2014). BIP-0062: Dealing with malleability. Retrieved from <https://github.com/bitcoin/bips/blob/master/bip-0062.mediawiki>

If you have any questions about this case study or on how you can implement these savings technologies in your organization, feel free to reach out to us at contact@veriphi.io

At **Veriphi**, we are open to work with you on addressing any case study that is of particular interest to you.

If you liked this case study and would like to see more, consider supporting us by sharing this one, donations are also appreciated.



bc1qq26ywt28xqpk2s7r2ckya56qf98h4hnnfp9p2mcpqlwsp7cmr3lsspuxvy

We have free presentations of this topic that we share with the Bitcoin community! Follow Bitcoin Montreal to stay up to date with our events.

<https://www.meetup.com/Bitcoin-Montreal/>

We also have an upcoming seminar that focuses on the technical aspects of SegWit and Transaction Batching and how you can implement it in your organization. Sign up [here](#).

All of our free content is published on our Youtube page, you can visualize it [here](#).