



crypto.com

On-Chain Market Sizing

Estimating Crypto Users with On-Chain Data

June 2020

Research and Insights

Data Report



Data Analyst
Kevin Wang

RESEARCH DISCLAIMER

This report alone must not be taken as the basis for an investment decision. The user assumes the entire risk of any use made of this information. The information is provided merely complementary and does not constitute an offer, solicitation for the purchase or sale of any financial instruments, inducement, promise, guarantee, warranty, or as an official confirmation of any transactions or contract of any kind. The views expressed therein are based solely on information available publicly/internal data/other reliable sources believed to be true. This report includes projections, forecasts and other predictive statements which represent [Crypto.com](https://crypto.com)'s assumptions and expectations in the light of currently available information. These projections and forecasts are based on industry trends, circumstances and factors which involve risks, variables and uncertainties. Opinions expressed therein are our current opinion as of the date appearing on the report only.

No representations or warranties have been made to the recipient as to the accuracy or completeness of the information, statements, opinions or matters (express or implied) arising out of, contained in or derived from this report or any omission from this document. All liability for any loss or damage of whatsoever kind (whether foreseeable or not) which may arise from any person acting on any information and opinions contained in this report or any information which is made available in connection with any further enquiries, notwithstanding any negligence, default or lack of care, is disclaimed.

The reports are not for public distribution. Reproduction or dissemination, directly or indirectly, of research data and reports of [Crypto.com](https://crypto.com) in any form is prohibited except with the written permission of [Crypto.com](https://crypto.com). Persons into whose possession the reports may come are required to observe these restrictions.

Contents

1.	Executive Summary	4
2.	Introduction	5
3.	Methodology	6
3.1	Overview	6
3.2	Exchange Users	7
3.3	Deposit Sweeping	10
3.4	Overlapping Users	13
3.5	ETH and Altcoins	18
3.6	Non-Exchange Users	18
4.	Results and Analysis	19
4.1	BTC Calculation Table	19
4.2	ETH Calculation Table	20
4.3	Aggregation	20
5.	Summary	21
5.1	Conclusion	21
5.2	Limitations and Caveats	22
6.	References	23

1. Executive Summary

Welcome to our Data Report for on-chain marketing sizing.

Key Takeaways:

- We introduced a new method to estimate the total number of crypto owners based on on-chain data (for Bitcoin and Ethereum):
 - The number of users in crypto exchanges can be used to approximate the overall number of users in crypto space;
 - Most exchanges use an architecture called “deposit sweeping” to handle crypto deposit inflows. We can estimate the number of users in an exchange by counting its on-chain deposit addresses;
 - By adding the number of users from some largest exchanges today (with adjustments) and dividing the overall market share of those exchanges, we can therefore reasonably estimate the overall number of bitcoin owners;
 - The exercise will be conducted for both bitcoin (BTC) and ether (ETH) to estimate BTC and ETH populations separately;
 - Lastly, we will scale up the number by considering non BTC / ETH owners as well as non-exchange users.
- The final estimate of the number of cryptocurrencies owners in the world is around **66 million**;
- The above number is a proxy only and subjected to various limitations and caveats.

2. Introduction

12 years have passed since the creation of bitcoin. How many people own cryptocurrencies today? This is an old, yet, crucial question to be answered. It is obvious that crypto will be here to stay in the coming decades, but the market size will determine whether it is something only for a niche group of people, or whether we are on the right track to reach crypto mass adoption.

One trivial way for conducting a market size estimation is through survey. For instances, [Kaspersky](#) and [Statista](#) conducted surveys in different regions. But such surveys are very costly or maybe even impossible.

Another way is to measure web-traffic of popular crypto websites as a proxy for the number of users. However, this method is highly inaccurate and susceptible to give false readings, since website visitors and crypto owners are distinct populations, albeit somewhat related.

One may also simply take the totality of user numbers claimed by crypto exchanges. However, different exchanges use different methodologies to count their user bases, and it is difficult to validate these numbers.

Lastly, since bitcoin (and many other cryptocurrencies) has publicly available data on its blockchain network, some have suggested to count the total addresses to estimate the number of owners. This methodology, however is limited as bitcoin's UTXO architecture means that one person can, and probably does, have multiple addresses. Besides, some addresses can be owned by entities (such as crypto exchanges, mining pools, other service providers) instead of the end user.

In light of the inadequacy of the aforementioned methods, we will use a modified and refined version of the last method (i.e. on-chain address counting) to arrive at a more accurate estimate of the crypto market's size.

3. Methodology

In this section, we will discuss our methodology in detail.

3.1 Overview

Here is the overall idea:

1. The number of users in crypto exchanges can be used to approximate the overall number of users in crypto space;
2. Most of exchanges use an architecture called “deposit sweeping” to handle crypto deposit inflows. We can estimate the number of users in an exchange by counting its on-chain deposit addresses;
3. By adding the number of users from some largest exchanges today (with adjustments) and dividing the overall market share of those exchanges, we can therefore reasonably estimate the overall number of bitcoin owners;
4. The exercise will be conducted for both bitcoin (BTC) and ether (ETH) to estimate BTC and ETH populations separately;
5. Lastly, we will scale up the number by considering non BTC / ETH owners as well as non-exchange users.

3.2 Exchange Users

Most people in the crypto space will use at least one crypto exchange. This is supported by the research from (Voskoboynikov, Obada-Obieh, Huang, & Beznosov) [here](#):

While all of the users interacted with an exchange, the nature of their interactions varied. PU1 only purchased Ethereum on Coinbase, just to transfer it over to his personal software wallet, whereas others kept most of their crypto-assets on exchanges...

Our [Crypto Adoption Survey](#) further strengthen this statement. Result indicated that 89% of our users have used crypto exchanges before.

Most exchanges use an architecture called “deposit sweeping” to handle crypto deposit inflows. By counting the deposit addresses via on-chain data, we can approximate the number of users for that exchange.

Exchange can own some operational addresses (e.g. cold wallets, or temporary fund transfer addresses). However, the number of deposit addresses should be far more than that of operational addresses. We can assume that exchanges’ number of operational addresses are negligible in comparison to that of deposit addresses.

By assuming that the number of users on an exchange approximately equals to the number of exchange addresses, we can state our first formula:

$$N_{total\ exchange\ users} = \sum N_{individual\ exchange\ addresses} \dots\dots\dots(1)$$

However, on-chain addresses will only appear once people have performed a deposit / withdrawal action, to account for the fact that some people have never deposited into / withdrawn from the exchange.

To estimate the true number of exchange users, we need to further scale up the number in formula (1): it should be divided by the ratio that people have deposited into an exchange.

$$r_{deposit} = \frac{\text{number of users who have deposited BTC in an exchange}}{\text{number of total BTC owner of the exchange}}$$

We calculated the deposit ratio by blended metrics from our internal data, [survey](#) data and industry benchmark.

Then, the true number of exchange users is:

$$N_{adjusted\ exchange\ users} = \frac{N_{total\ exchange\ users}}{r_{deposit}}$$

We have selected 21 exchanges to measure their user bases via their on-chain addresses. However, more exchanges and addresses exist, which is computationally difficult to accommodate. To solve this, we further scale up the number of users from these 21 exchanges by measuring their total market share ($r_{total\ market\ share}$), which can be obtained from our [survey](#):






















$$N_{total\ exchange\ users} = \frac{N_{selected\ exchanges\ users}}{r_{total\ market\ share}}$$

Integrate above with the $N_{adjusted\ exchange\ users}$ formula, the adjusted number of users for all exchanges is:

$$N_{adjusted\ exchange\ users} = \frac{N_{selected\ exchanges\ users}}{r_{total\ market\ share} \times r_{deposit}} \dots\dots\dots(2)$$

Currently, we only considered centralized exchanges since decentralized exchanges (DEX) are still insignificant in size. We may adjust our methodology in future studies when the decentralized market becomes more prominent.

Below is the list of exchanges that are included in this study:

Exchange Name	Logo
Crypto.com	 crypto.com
Binance	
Bitfinex	
Bittrex	
BitMax	
Bithumb	
Bitstamp	
Gemini	
Huobi	
Kraken	
KuCoin	
OKEx	
Liquid	
BitFlyer	
Gate.io	
Zaif	
Poloniex	
UPbit	
BitMEX	
Deribit	
FTX	

3.3 Deposit Sweeping

Centralized exchanges normally have following types of addresses:

- **Deposit Addresses:** Deposit addresses are on-chain addresses (often temporary) used to transfer funds into an exchange. The purpose of this address type is to facilitate exchange on recognizing and collecting deposits from its users. They are also called “sweeping addresses”;
- **Hot Wallet:** The purpose of a hot wallet is to make an asset available to transfer and is the main interaction point between external addresses and exchange, or vice versa. Typically, exchanges use withdrawal hot wallets to handle fund transfers out (More about [Hot Wallets](#));
- **Cold Wallet:** Exchanges use cold wallets as secured storage of crypto assets in which larger amounts of crypto are held (More about [Cold Wallets](#));
- **Withdrawal Addresses:** Withdrawal addresses are on-chain addresses (often temporary) that are used to transfer funds out of the main exchange wallet. Sometimes withdrawal addresses can play a dual role for consolidating deposit addresses.

When user prepares to deposit funds into an exchange, there will be an address shown in the exchange's interface. This address is the deposit address, which is a [public key](#) generated by the exchange based on a [private key](#) owned by the exchange on behalf of the user.


Below are screen caps of deposit addresses in Crypto.com Exchange and Crypto.com App:


Deposit BTC


BTC Address



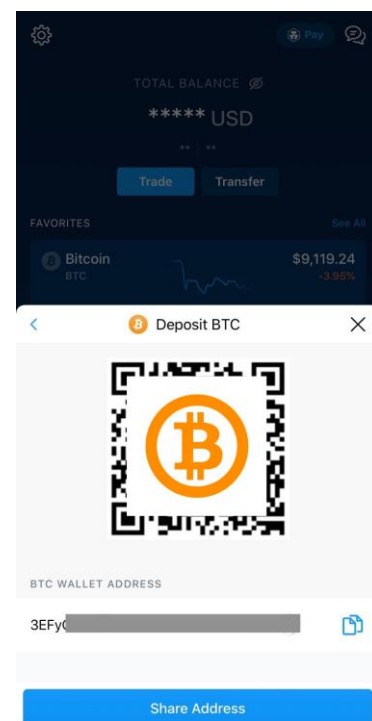
7vDKjX

 Copy Address Hide QR Code

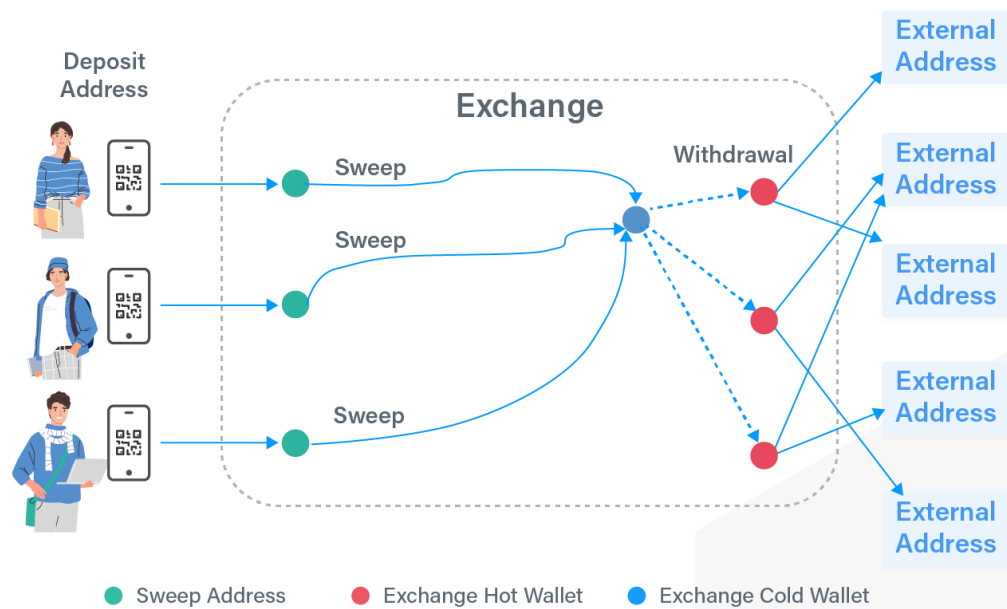
 Send only BTC to this deposit address.
Sending coin or token other than BTC to this address may result in the loss of your deposit.

 BTC confirmation required: 6

Source: Crypto.com Research



Users' private keys are held by exchanges, which then perform transactions on behalf of users. To protect users' assets, most exchanges will transfer the funds collected from deposit addresses (which are hot wallets with small balances held) into exchanges' cold wallets for consolidation and secure storage. The procedure is called "sweeping" and is illustrated below:



Source: [Crypto.com Research](#)

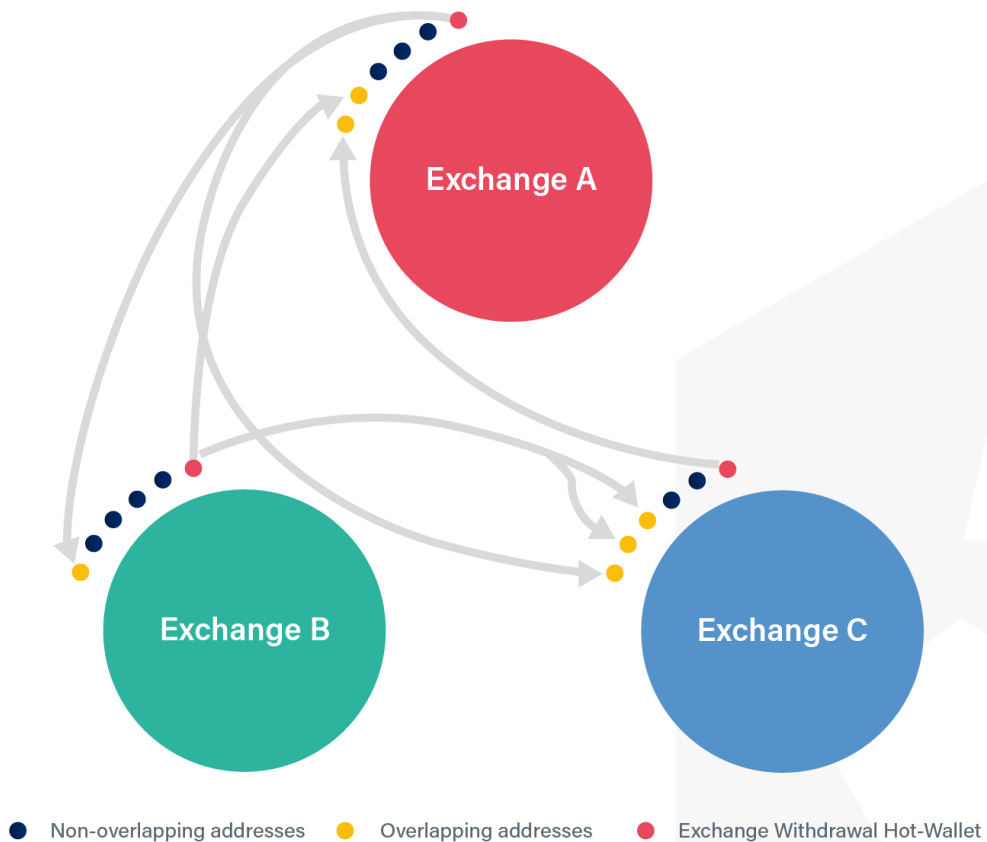
"Sweeping" usually occurs automatically and periodically. Our study assumed that most exchanges follow this similar procedure. Therefore, by counting all addresses of one exchange (which are made up predominantly of sweeping addresses), we can approximate the exchange's on-chain user base.

One challenge of using the above-mentioned method is that, on-chain addresses don't contain information about their owner's identity. For this report, we relied on the exchange addresses' tags provided by some third-party tools.

3.4 Overlapping Users

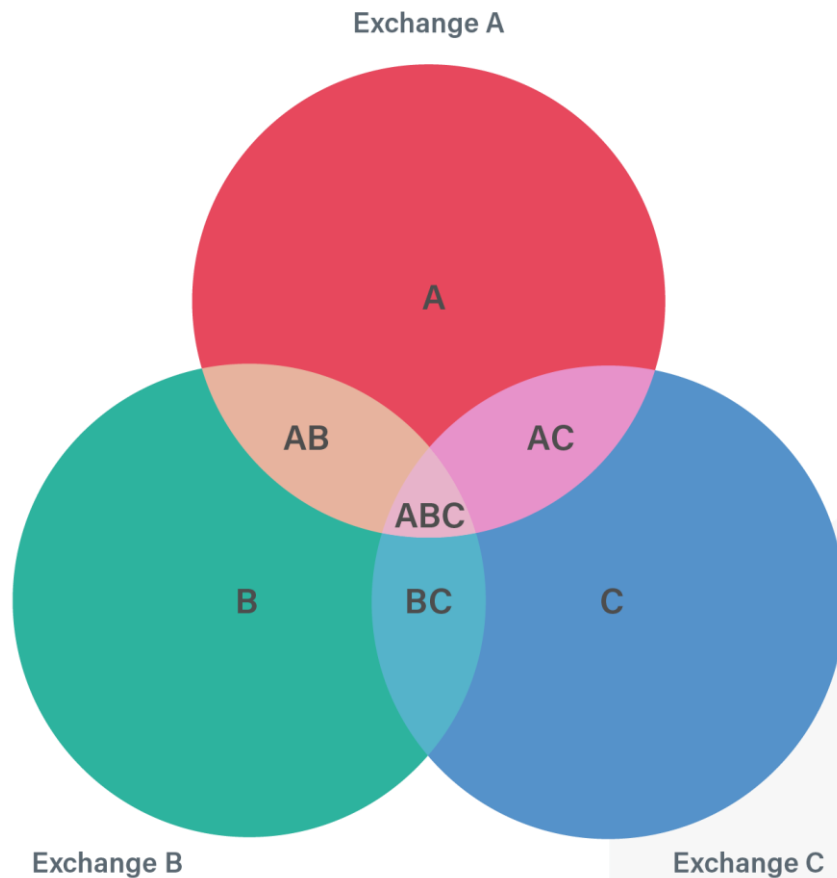
Summing up users from each individual exchange is easy, but many users have accounts in more than one exchange. It is crucial to find a way to prevent overcounting those users.

The idea: First we can find all addresses belonging to an exchange, then classify them into “overlapping addresses” and “non-overlapping addresses”. Finally, we can remove the duplicated addresses in the “overlapping addresses” to find the number of unique users.



Source: Crypto.com Research

Let's illustrate the problem in a Venn diagram below. Without loss of generality, assume that there are only three exchanges (A, B and C) and that their users are represented by the three circles below.



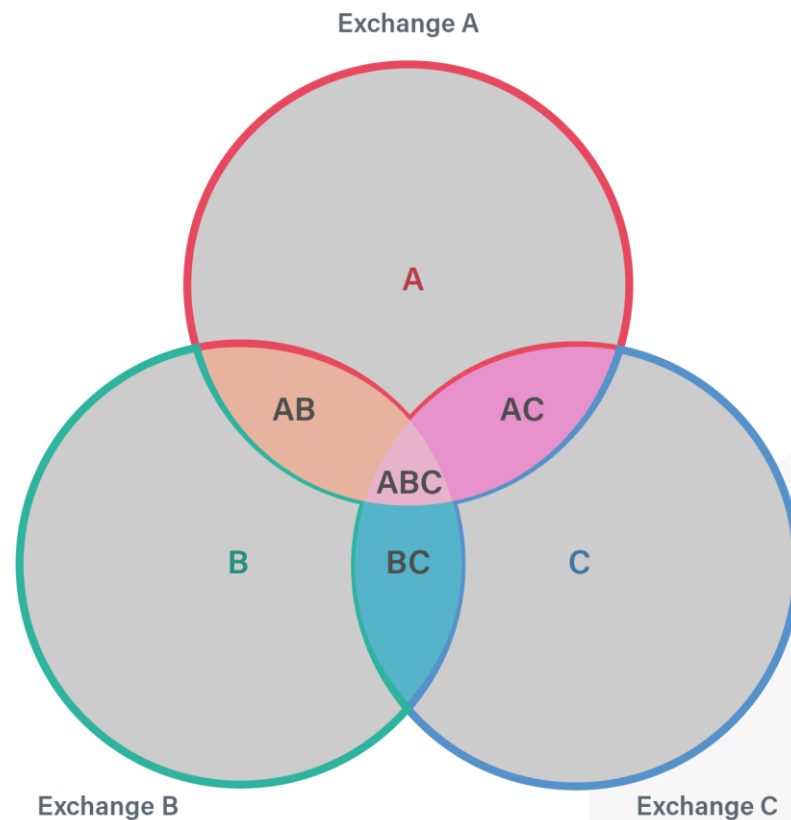
Source: Crypto.com Research

Let $\{A\}$, $\{B\}$ and $\{C\}$ denote the set of users who have used exchange A, B, C respectively.

The total number of unique users can therefore be denoted as:

$$N_{total\ exchange\ users} = \{A \cup B \cup C\}$$

We can find $\{A\}$, $\{B\}$ and $\{C\}$ by using the method introduced in section 3.2. However, we need to remove the overlapping users who own multiple exchange accounts. The overlapping users have performed *inter-exchange transactions*, i.e. 0.5 BTC was transferred from Exchange A to Exchange B on Alice.



Source: Crypto.com Research

The overlapping users are the highlighted parts in the graph above and can be denoted as:

$$N_{on-chain\ overlapping\ addresses} = \{A \cap B\} \cup \{B \cap C\} \cup \{C \cap A\}$$

To evaluate the number of overlapping users, we can first discover the on-chain overlapping addresses and then remove any duplicated addresses owned by the same user. The number of on-chain overlapping addresses can be extracted by querying the addresses that have performed inter-exchange transactions.

Assume the total number of on-chain addresses from the selected exchanges is $N_{\text{exchange total addresses}}$. Then the addresses belonging to non-overlapping users are:

$$\begin{aligned} & N_{\text{on-chain non-overlapping addresses}} \\ &= N_{\text{exchange total addresses}} - N_{\text{on-chain overlapping addresses}} \end{aligned}$$

These on-chain non-overlapping addresses are the reasonable representation of the on-chain non-overlapping users:

$$N_{\text{on-chain non-overlapping users}} \approx N_{\text{on-chain non-overlapping addresses}}$$

To remove the duplicated addresses owned by the same user, we rely on the overlapping ratios obtained from our [survey](#) and compute the weighted-average number of exchanges that each overlapping user own.

Among those who used 2+ exchanges, assume that there are $r_2\%$ of people who own 2 exchange accounts, and $r_3\%$ of people who own 3 exchange accounts. Therefore, the weighted-average number of addresses per user is:

$$k_{\text{addresses per user}} = 2 \times r_2\% + 3 \times r_3\%$$

Then we can recover the number of unique users who possess multiple exchange addresses by:

$$N_{\text{on-chain overlapping users}} = \frac{N_{\text{on-chain overlapping addresses}}}{k_{\text{addresses per user}}}$$

Therefore, we have the following equation:

$$\begin{aligned} N_{\text{total exchange users}} &= N_{\text{on-chain non-overlapping users}} + N_{\text{on-chain overlapping users}} \\ &= N_{\text{on-chain non-overlapping addresses}} \\ &\quad + \frac{N_{\text{on-chain overlapping addresses}}}{k_{\text{addresses per user}}} \\ &= N_{\text{on-chain non-overlapping addresses}} \\ &\quad + \frac{N_{\text{on-chain overlapping addresses}}}{2 \times r_2\% + 3 \times r_3\%} \end{aligned}$$

Generalize the above equation with M exchanges:

$$\begin{aligned}
 N_{total\ exchange\ users} &= N_{on-chain\ non-overlapping\ addresses} \\
 &+ \frac{N_{on-chain\ overlapping\ addresses}}{2 \times r_2\% + 3 \times r_3\% + \dots + M \times r_M\%} \\
 &= N_{on-chain\ non-overlapping\ addresses} + \frac{N_{on-chain\ overlapping\ addresses}}{k_{addresses\ per\ user}}
 \end{aligned}
 \tag{3}$$

Our [survey](#) indicated that less than 1% of our users own 10+ exchange accounts. Therefore, we set $M = 10$ and the r_{10+} will be consolidated into r_{10} for simplicity.

By combining equation (1), (2), (3), we can obtain our final formula for the approximation of BTC users:

$$\begin{aligned}
 N_{BTC\ owners} &= N_{adjusted\ exchange\ users} \\
 &= \frac{1}{r_{deposit} \times r_{total\ market\ share}} \times N_{selected\ exchange\ users} \\
 &= \frac{1}{r_{deposit} \times r_{total\ market\ share}} \times \\
 &\quad \left(N_{on-chain\ non-overlapping\ addresses} + \frac{N_{on-chain\ overlapping\ addresses}}{k_{addresses\ per\ user}} \right)
 \end{aligned}
 \tag{4}$$

3.5 ETH and Altcoins

We used the same approaches to approximate the number of ETH owners ($N_{ETH\ owners}$).

Next, the number of BTC owners and ETH owners are summed together while the number of overlapping users who hold both BTC and ETH is subtracted. Further, we scale up this calculation by considering the users who own neither BTC nor ETH.

To make our calculation clear, we denote the number of BTC owners as $N_{BTC\ owners}$, ETH owners as $N_{ETH\ owners}$, and $r_{BTC\&\ ETH}$ as the overlapping ratio (users who own both BTC and ETH) and $r_{\overline{BTC\&\ ETH}}$ as the ratio that users who own neither BTC nor ETH. Then, the total number of exchange crypto owners is given by:

$$N_{Exchange\ Total\ Crypto\ Owner} = N_{BTC\ owners} + N_{ETH\ owners} - (N_{Exchange\ Total\ Crypto\ Owner} \times r_{BTC\&\ ETH}) + (N_{Exchange\ Total\ Crypto\ Owner} \times r_{\overline{BTC\&\ ETH}})$$

Consequently,

$$N_{Exchange\ Total\ Crypto\ Owner} = \frac{(N_{BTC\ owners} + N_{ETH\ owners})}{1 + r_{BTC\&\ ETH} - r_{\overline{BTC\&\ ETH}}} \dots\dots\dots(5)$$

The $r_{BTC\&\ ETH}$ and $r_{\overline{BTC\&\ ETH}}$ parameters can be obtained by blended metrics from internal data, survey data and industry benchmark.

3.6 Non-Exchange Users

Considering the [survey](#) that there are still 11% of our users who haven't used crypto exchanges, the above result should be scaled up by being divided the crypto exchange adoption ratio ($r_{exchange}$). Based on formula (5), we get:

$$N_{Total\ Crypto\ Owner} = \frac{N_{Exchange\ Total\ Crypto\ Owner}}{r_{exchange}} = \frac{(N_{BTC\ owners} + N_{ETH\ owners})}{(1 + r_{BTC\&\ ETH} - r_{\overline{BTC\&\ ETH}}) \times r_{exchange}} \dots\dots\dots(6)$$

4. Results and Analysis

Following tables list the results of each step separate by BTC and ETH.

BTC Calculation Table

Step	Parameter (BTC)	Notation	Result
(1)	User deposit rate	$r_{deposit}$	38%
(2)	Total No. of on-chain overlapping addresses	$N_{on-chain \text{ overlapping addresses}}$	3,726,156
(3)	Total No. of on-chain addresses (selected exchanges)	$N_{exchange \text{ total addresses}}$	17,507,496
(4)	No. of on-chain non-overlapping addresses	$N_{on-chain \text{ non-overlapping addresses}} = (3) - (2)$	13,781,340
(5)	Weighted-Average No. of exchanges per user	$k_{addresses \text{ per user}}$	3.36
(6)	Selected exchanges' coverage ratio	$r_{total \text{ market share}}$	92%
(7)	Total No. of BTC owners	$\frac{[(2) \div (5) + (4)]}{(1) \times (6)}$	~ 43Mln

ETH Calculation Table

Step	Parameter (ETH)	Notation	Result
(1)	User deposit rate	$r_{deposit}$	38%
(2)	Total No. of on-chain overlapping addresses	$N_{on-chain \text{ overlapping addresses}}$	686,529
(3)	Total No. of on-chain addresses (selected exchanges)	$N_{exchange \text{ total addresses}}$	4,263,085
(4)	No. of on-chain non-overlapping addresses	$N_{on-chain \text{ non-overlapping addresses}} = (3) - (2)$	3,576,556
(5)	Weighted-Average No. of exchanges per user	$k_{addresses \text{ per user}}$	3.36
(6)	Selected exchanges' coverage ratio	$r_{total \text{ market share}}$	92%
(7)	Total No. of ETH owners	$\frac{[(2) \div (5) + (4)]}{(1) \times (6)}$	~ 11 Mln

Aggregation

Step	Estimates	Notation	Result
(1)	BTC Owners	$N_{BTC \text{ owners}}$	~ 43Mln
(2)	ETH Owners	$N_{ETH \text{ owners}}$	~ 11 Mln
(3)	BTC & ETH Overlapping Rate	$r_{BTC\Ð}$	24%
(4)	Rate of the users own neither BTC nor ETH	$r_{\overline{BTC\Ð}}$	32%
(5)	Exchange adoption rate	$r_{exchange}$	89%
(6)	Overall Crypto Population	$\frac{(1) + (2)}{[1 + (3) - (4)] \times (5)}$	~ 66 Mln

Therefore, the final estimate of the population of cryptocurrencies owners in the world is around **66 million**.

5. Summary

5.1 Conclusion

In conclusion, we have proposed a method to estimate the number of cryptocurrencies owners in the world.

Key Takeaways:

- We introduced a new method for using on-chain data (for Bitcoin and Ethereum) to estimate the total number of crypto owners:
 - The number of users in crypto exchanges can be used to approximate the overall number of users in crypto space;
 - Most exchanges use an architecture called “deposit sweeping” to handle crypto deposit inflows. We can estimate the number of users in an exchange by counting its on-chain deposit addresses;
 - By adding the number of users from some largest exchanges today (with adjustments) and dividing the overall market share of those exchanges, we can therefore reasonably estimate the overall number of bitcoin owners;
 - The exercise will be conducted for both bitcoin (BTC) and ether (ETH) to estimate BTC and ETH populations separately;
 - Lastly, we will scale up the number by considering non BTC / ETH owners as well as non-exchange users.
- The final estimate of the number of cryptocurrencies owners in the world is *around 66 million*;
- The above number is a proxy only and subjected to various limitations and caveats.

5.2 Limitations and Caveats

In this report, we proposed a method for the crypto market sizing problem. The method is built on Bitcoin and Ethereum's on-chain data, our survey analysis and internal data. While we believe that our proposed methodology presents a more accurate estimate than other methods in the market, it is still subject to the following limitations and caveats:

- Our method assumed that all on-chain users are still owning crypto today, while at least some may have already sold their holdings;
- We assumed that all the selected exchanges use the same deposit sweeping architecture;
- OTC trading may not be effectively captured;
- Sub-accounts in exchanges may not be effectively reflected;
- Parameters obtained by survey / internal data may change over time;
- Since all parameters are at least partially sourced from Crypto.com users (either by survey or internal data), sampling bias is inevitable;
- The result has dependency on the tools / data from the third-party that we have used.

6. References

Bucquet, P., Lermite, M., & Jo, A. (2019, June). *How many active crypto traders are there across the globe?* Retrieved from https://www.chappuishalder.com/wp-content/uploads/2019/06/Publication_Crypto-traders-06-2019.pdf

How Many Bitcoin Users Are There? (n.d.). Retrieved from <https://www.buybitcoinworldwide.com/how-many-bitcoin-users/#own>

Thomas, E. (2019, Nov). *Is Bitcoin Adoption Really on the Horizon?* Retrieved from <https://cryptobriefing.com/bitcoin-adoption-horizon/>

Rodriguez, J. (2019, Sep 18). *Understanding the Internals of Crypto-Exchanges Using Machine Learning and Data Visualizations: Binance and Poloniex Explained.* Retrieved from <https://medium.com/intotheblock/understanding-the-internals-of-crypto-exchanges-using-machine-learning-and-data-visualizations-1404d21dc9c6>

Voskobojnikov, A., Obada-Obieh, B., Huang, Y., & Beznosov, K. (n.d.). *Surviving the Cryptojungle: Perception and Management of Risk Among North American Cryptocurrency (Non)Users .*

PARTZ, H. (2019, Jun). *19% of World Population Bought Crypto Before 2019: Kaspersky Report.* Retrieved from <https://cointelegraph.com/news/19-of-world-population-bought-crypto-before-2019-kaspersky-report>

Best, R. d. (2018, Aug). *How Many Consumers Own Cryptocurrency? .* Retrieved from <https://www.statista.com/chart/15137/how-many-consumers-own-cryptocurrency/>

Cryptography and Cryptocurrencies. (n.d.). Retrieved from <https://crypto.com/en/university/article.html?category=privacyAndSafety&page=cryptography>



e. contact@crypto.com

© Copyright 2020. For information, please visit crypto.com