crypto research
.report

June 2020

Edition X.

Modeling Bitcoin's Price with Irving Fisher's Equation of Exchange

An Absolute Valuation of Bitcoin & Co.

Is Tether a Black Swan for Bitcoin?

Coin Corner: Privacy Coins and MimbleWimbleCoin

We would like to express our profound gratitude to our premium partners for supporting the Crypto Research Report:

Contents

Disclaimer:

This publication is for information purposes only and represents neither investment advice, nor an investment analysis or an invitation to buy or sell financial instruments. Specifically, the document does not serve as a substitute for individual investment or other advice. The statements contained in this publication are based on the knowledge as of the time of preparation and are subject to change at any time without further notice. The authors have exercised the greatest possible care in the selection of the information sources employed, however, they do not accept any responsibility (and neither does Crypto Research Report) for the correctness, completeness, or timeliness of the information, respectively the information sources made available, as well as any liabilities or damages, irrespective of their nature, that may result there from (including consequential or indirect damages, loss of prospective profits or the accuracy of prepared forecasts).

Editorial

Dear Reader,

For the first time in Bitcoin's young life, the global economy plunged into recession. In the wake of Covid-19, 40 million Americans were left unemployed (15 %). In Austria, there are 571,477 unemployed (12 %). In Germany, 2.639 million (5.8 %). Despite having an entire quarter's GDP erased from 2020, hedge fund managers are all singing the slogan, **"*All Time High by the Fourth of July*."** What this slogan means is that the S&P 500 is expected to hit a new all-time high by July. Although, this sounds unbelievable, central banks around the world have the power to make this happen; and so far, they seem to be doing everything they can do to weaken their currencies and artificially prop up asset prices.

If we take America for example, the S&P 500 and Dow Jones dropped double-digit percentages during March. In response, the Federal Reserve created $3 trillion out of thin air, and financial markets bounced back. The stimulus that the Federal Reserve took two months to inject is larger than the entire stimulus that they injected in response to the 2008 "Great Recession." The Federal Reserve acted so quickly and so swiftly, because they know how fragile the financial system is, and how dependent markets are on cheap money. Six months ago, hard money advocates laughed at US Representative Alexandria Ocasio-Cortez for championing Modern Monetary Theory (MMT), and now, the Fed has promised to do unlimited quantitative easing until "we recover." To be clear, **there is really no difference between MMT and quantitative easing.** The only difference is that with the former we drop the pretenses and stop pretending that we will pay back the debt one day.

Despite unprecedented quantitative easing, trillions of short-term credits to the repurchase agreement market, and lowering interest rates to zero, **the US dollar index (DXY) barely moved.** This means that the dollar can take a lot more abuse from the printing machines before it starts to devalue against other fiat currencies. Also, the 5-year forward inflation expectation for the US dollar is sitting at a low 1.43 %. This means that despite massive debasement of the US dollar, markets expect inflation to be below the Federal Reserve's target 2 %. Traditional markets are no longer reflecting the state of the economy. Instead, they are reflecting the central bank's effort to keep the pension system alive and to get Trump reelected. **Unfortunately, there is no turning back now.** Every hiccup in the economy needs to be met with even greater inflation, leading to an even wider gap between reality and finance.

Let's not forget that every time the central bank creates new unbacked units of currency, this comes at the expense of everyone that currently holds the currency. Unfortunately, this expense isn't evenly distributed. Single handedly, the largest cause of wealth inequality in the West is inflation. Google Cantillon Effect.

And where was Bitcoin during all of this? From $3,600 in March to $10,000 in May and then back down again to $9,000, the ride on the Bitcoin rollercoaster has made some nauseous and some rich. Many cryptocurrency companies are in dire shape due to the shut-down and lack of customers, but Bitcoin hodlers just keep holding on in hopes of a posthalving bull market. So far, the halving has been a non-event. Bitcoiners around the world joined in on Zoom webinars to celebrate Bitcoin's special day, but the Bitcoin price hardly budged. The uncertainty surrounding the economy has definitely put a damper on the crypto market. However, there is still hope yet. As governments around the world wage currency wars to protect their export markets and inflate away their burdensome debt, some households may turn to Plan B.

We hope that you enjoy this special edition of the Crypto Research Report, marking its 10th publication! In the last edition, we covered Plan B's stock-to-flow model. In this edition, we present another popular model that is used to forecast Bitcoin's future price called the Equation of Exchange model. We discuss how Ethereum's Vitalik Buterin and Multicoin Capital's Kyle Samani approached this model, and we discuss a devastating critique of it by Basic Attention Token's Scott Locklin. In this special edition, we also feature a guest article by Schlossberg&Co's Pascal Hügli on the topic of Tether. Hügli investigates whether Tether is really being used to manipulate the price of Bitcoin or not. Since the beginning of this year, $5 billion worth of Tether USDT have been issued. If the new Tether isn't fully backed, and if Tether eventually collapses, this will most likely bring down at least one exchange and wreak havoc on the price of Bitcoin. Finally, this edition of the CRR features an exclusive interview with the development team of MimbleWimbleCoin, which is a new privacy-based coin that was airdropped to Bitcoin holders for free in December. Since December, the price has soared 6000 %, and the authors argue that their token economics are superior to the privacy coin Grin, that they are more scalable than Monero, and that they can prove their total supply unlike Zcash.

Also, we are happy to announce that the *Crypto Research Report* has struck a strategic partnership with CoinTelegraph, the largest crypto news company in the world. The September edition of the Crypto Research Report will be distributed by CoinTelegraph on their website, which gets 10 million views a month. The goal of the joint effort is to publish the results of a landmark study on institutional demand for crypto assets in the German-speaking countries. This study is being conducted by Professor Dr. Philipp Sandner from the Frankfurt School of Finance and Management, Professor Dr. Alfred Taudes from the Vienna University of Economics and Business (WU), and the editor of the *Crypto Research Report*, Demelza Hays. To make sure you are the first to receive this free quarterly report, subscribe on our website.

Last but not least, we especially want to thank our Premium Partners of the *Crypto Research Report*. Coinfinity in Graz is a broker in Austria that is famous for creating an easy-to-use Bitcoin cold wallet called The Card Wallet. Coinfinity also enabled Bitcoin purchases at 4,000 retail outlets across Austria via the Bitcoinbon program. In addition to Coinfinity, we are exuberant that Bitpanda has joined as a Premium Partner of the *Crypto Research Report*! Bitpanda is a fully licensed exchange based in Austria. They have recently added Bitpanda Pro, which offers more liquidity and lower fees. We are personally excited about Bitpanda Metals, which allows investors to diversify their portfolio with physically backed and 100% insured precious metals. In addition to Coinfinity and Bitpanda, we have a new sponsor, MimbleWimbleCoin. They are a new privacy-based coin that has been on the market for six months.

Demelza Kelso Hays and the CRR Team

An Absolute Valuation Approach to Crypto Assets

"It has happened globally with such speed that even a market veteran like myself was left speechless. We are witnessing the Great Monetary Inflation -- an unprecedented expansion of every form of money unlike anything the developed world has ever seen."

Paul Tudor Jones, CEO Tudor Investment Corp.

Key Takeaways

- **On-chain velocity for most coins is decreasing, while off-chain velocity is increasing. This provides evidence that growth in speculative transactions on exchanges is faster than the growth in using cryptocurrencies to buy goods and services.**

- **Approximately 40+ million cryptocurrency-users exist globally according to our research. Surprisingly, the number of cryptocurrency users in a country is positively correlated with that country's GDP per capita. High GDP means more cryptocurrency adoption.**

- **The target addressable market for crypto assets is approximately $212 trillion. The largest use cases include medium of exchange including all global fiat currencies worth $126 trillion and consumer loans with a global value of $42 trillion. If Bitcoin penetrated 10 % of this market over the next ten years, each Bitcoin would be worth $397,000 in 2030.**

Bitcoin's off-chain velocity is at an all-time high. Fiat currency with high velocity is normally a bad sign, but does that rule apply to crypto?

One of the most common ways to estimate the price of a cryptocurrency is with the "equation of exchange". This model comes from the 20th century economist Irving Fisher. One of the main insights of this model **is that the more often a currency changes hands, the less value the currency has.** Money changes hands more frequently when people believe the money will lose value. For example, if there is high inflation, people will hold on to the money for the shortest amount of time possible before tossing the hot potato to someone else.

For the past few years, Bitcoin's off-chain velocity has been increasing. But what does this mean? Vitalik Buterin famously applied this model to crypto assets in 2017 in order to argue that coins need velocity sinks that encourage hoarding. Partner of Multicoin Capital, Kyle Samani, wrote an article in agreement with Vitalk's understanding of velocity. He wrote,

> *"As I noted in Understanding Token Velocity, the V in the equation of exchange is a huge problem for basically all proprietary payment currencies. Proprietary payment currencies are, generally speaking, susceptible to the velocity problem, which will exert perpetual downwards price pressure. Due to this effect, I expect to see utility tokens that are just proprietary payment currencies exceed a velocity of 100. Velocities of 1,000 are even possible."*

However, Scott Locklin, an engineer for Brave Attention Token explains in a recent papr that both Buterin and Samani are wrong. This article models Bitcoin's price with the equation of exchange model and discusses why the relationship may not be as straight-forward as Buterin and Samani surmised.

"Gold is up 12 % year-to-date and Bitcoin is up 25 % in the same time period.

"I won't hold my breath for the media to write articles stating, "Bitcoin proving to be the best safe haven asset in the economic crisis.

"But even their silence can't change the truth."

Anthony Pompliano
Morgan Creek Digital
May 2020

Introduction to the Equation of Model

Each distributed ledger network offers a specific range of abilities to their cryptocurrency users. **The fundamental value of a coin can be defined as the aggregate summation of each individual user's valuation of the network.** The short-term prices of cryptocurrencies are determined by supply and demand and may not reflect their fundamental values. However, price can be a noisy signal of a cryptocurrency's fundamental value over the long-term. Long-term refers to multiple periods of macroeconomic cycles including expansions and recessions, which the cryptocurrency market has still not completed.

Several papers have used the equation of exchange model to estimate Bitcoin's price in 5 years, 10 years, and even on longer time horizons. For example, Kraken and the Economist estimate Bitcoin's price to be $1.91 million by 2022[1], Satis estimate $96,000 by 2023[2], and Vision & $65,000 by 2028.[3] The main reason each report has different prices is that estimating future demand for Bitcoin and other coins is based on assumptions. The equation of exchange model is an absolute approach to valuing crypto assets. This means that the model gives a target price that crypto assets should be priced at based on assumptions regarding changes in supply and demand.

The equation of exchange model relies on the theory that the value of each cryptocurrency should be directly correlated with the dollar volume of the economy it supports. A cryptoasset economy that has $1,000 in trading volume each year and has 10 coins in circulation will have a fair coin value of $100 if each coin is traded once during that year. The value of each cryptoasset is inversely related to its supply, i. e. the number of coins that are in circulation and its velocity, i. e. the number of times each coin is traded per year. The growth in GDP of each coin or the cryptoasset economy will be determined by product-market fit. **The likelihood of future market adoption is what drives speculative today.**

The absolute valuation approach is inspired by Mill's equation of exchange later formulated by Irving Fisher.[4] In this model, the percentage of the total addressable market (TAM) can be used to estimate a cryptoasset's implied future price. The traditional equation, MV = PQ, was first applied to Bitcoin by Chris Burniske in his original 2016 report for Coinbase.[5] The equation of exchange, MV = PQ describes the balance between money in the economy and demand for that money for purchases of goods and services. To estimate the size of the economy supported by cryptoassets, the following steps are taken:

Interactive Excel Spreadsheets
This chapter is accompanied by Excel sheets that readers can use to estimate the price of crypto assets based on their research and assumptions.

- The economic size of all relevant use cases for a crypto asset are summed. This is referred to as the target addressable market (TAM). **This involves three assumptions:**
    - Which use cases are applicable for cryptocurrencies?
    - What is the total market capitalization in US dollars of each use case? **(PQ)**
    - What is the growth in the total market capitalization in US dollars of each use case over the next decade?
- An estimate of the percentage of each target addressable market that is penetrated by cryptoassets over a ten-year horizon is calculated. **This involves two assumptions:**

—

[1] Rodrigo Cherniauskas, Beatrice Gorski and David Murchland, *Kraken Investment Proposal*, The Economist, October 2016. Retrieved from https://www.economist.com/sites/default/files/fia__the_navigators__kraken_investment_case_analysis__full_submission.pdf

[2] Sherwin Dowlat, "Cryptoasset Market Coverage Initiation: Valuation August 30, 2018," *Satis Group*, 2018. Retrieved from https://research.bloomberg.com/pub/res/d37g1Q1hEhBkiRCu_ruMdMsbc0A

[3] Dr. Lidia Bolla and Christian Schüpbach, *The Blockchain Story. What's it all worth?* Vision&, May 2018. Retrieved from https://www.visionand.ch/wp-content/uploads/2018/06/vision_Valuation.pdf

[4] John Stuart Mill, *Principles of Political Economy*, London, John W. Parker, 1848.

[5] Chris Burniske and Adam White, "Bitcoin: Ringing The Bell For A New Asset Class" [White Paper], *Ark Invest,* January, 2017. Retrieved from https://research.ark-invest.com/hubfs/1_Download_Files_ARK-Invest/White_Papers/Bitcoin-Ringing-The-Bell-For-A-New-Asset-Class.pdf

“What is the one investment all of these investors have in common?

Paul Tudor Jones

Marc Lasry

Bill Miller

Mike Novogratz

Raoul Pal

Chamath Palihapitiya

Peter Thiel”

Barry Silbert
CEO Digital Currency Group
May 2020

    - How much of each use case will be penetrated by cryptocurrencies?
    - What is the growth rate of penetration for cryptocurrencies over the next decade? **This involves an assumption**:
        - To estimate the growth rate of penetration for cryptocurrencies over the next decade, an assumed adoption rate of cryptocurrencies can follow an S-curve, a linear curve, an exponential curve, a mean-reversion curve, a log curve. **This paper assumes an S-curve for all cryptocurrencies.**

- Each annual addressable market is divided by each coin’s velocity to determine the coin’s market capitalization. **This involves three assumptions:**
    - What is the supply **(M)** of each cryptocurrency over the next decade?
        - Some cryptocurrencies follow supply schedules, such as Bitcoin that follows a Poisson distribution.
        - Other coins have supplies that depend on a voting mechanism, such as EOS.
        - Therefore, the former will have a lower forecast error than the latter. In this analysis, the supply of each cryptocurrency is assumed to be the average size of the crypto asset base through the year, which is necessary due to the inflationary nature of most cryptoasset protocols, including Bitcoin.
    - What is the velocity **(V)** for each cryptocurrency?
    - What is the growth in velocity for each cryptocurrency over time?

- To determine the price per coin, the total addressable market multiplied by the penetration rate is divided by its circulating supply.

- Once the price per coin is forecasted for each year over the next decade, the discount rate must be applied in order to calculate the net present value of the price of each coin for each year. **This involves the following assumption:**
    - The discount rate should reflect each coin’s risk and the nominal inflation rate. **This report assumes a standard discount rate of 30 % for each coin.**

Assumptions in Depth

Monetary Supply

The (M) in MV = PQ is measured by the supply in circulation of a crypto asset. **(M) is the monetary base necessary to support an economy.** The supply of some cryptocurrencies is easy to estimate if their supply follows predetermined processes (Bitcoin and Poisson, etc.). Supply is coming from two main areas: new coins released into circulation either through mining, staking, or reserve sales and coins being sold on the market from wallets. The goal of "M" is to estimate the amount of coins that are in each year's circulation and will be available on the market. Often referred to as the float. The float is comprised of two parts: flow and stock. The flow is the amount of the cryptoasset that will be issued each year, and the stock is how much has already been issued.

This report assumes a stable supply of each cryptoasset for each year and forecasts the supply over the decade based on each cryptoasset's programmed supply schedule in its protocol. However, a more in-depth analysis would try to forecast future circulating supply by calculating the float or circulating supply of each cryptocurrency. To calculate the float, "hodled" assets or assets that are hoarded must be subtracted. For example, if 100 million coins are issued and 60 % are hoarded in wallets that never move, M is equal to 40 million coins. This applied to Coinbase users who purchased Bitcoin in 2016. 57 % of Coinbase users held their bitcoin in 2016 as a store of value and speculative asset instead of using it as a medium of exchange.[6]

Velocity

(V) is the velocity of each unit of money in the monetary base. If Alice passes a bitcoin to Bob once a year, that's an annual velocity of 1. If Bob passes on that same bitcoin to Eve, that's an annual velocity of 2. The value of a coin is inversely proportional to the total discounted supply and inversely proportional to velocity. Thus, a currency which increases its velocity will lose value with respect to any other currency whose velocity doesn't increase that much.

Velocity Example

If the total amount of economic transactions paid for with bitcoin in one year is $100 billion, and each bitcoin changes hands 10 times on average over the course of the year, then the collective value of the coins is $10 billion; and if there are 18 million bitcoin in circulation, then this would mean the utility price of each bitcoin is roughly $555. If they circulate 100 times, then the collective coins are worth $1 billion, which makes $55 per bitcoin.

Velocity is a key variable where many reports diverge. Vision &'s estimate of velocity was 10. To put this into perspective, the US M1 money supply has a velocity of approximately 5. What pulls down velocity is friction. Since cryptoassets are natively digital, their friction will be lower than physical cash, which will place an upward pressure on velocity compared to physical currencies. On the other hand, physical fiat currencies have high inflation rates, which promote high velocity. Cryptocurrencies with low inflation rates and purchasing power appreciation will have a downward pressure on velocity.

This report assumes a stable velocity of each coin over the next decade. The velocity figure is calculated based on the 2019 on-chain velocity of each coin. Velocity is calculated by dividing the annual trading volume in dollars by the network's on chain transaction volume and then taking an annual average for 2019. A more in-depth analysis would try to forecast the average amount of hoarded assets each coin will have each year. Hoarded cryptoassets pull down each coin's average yearly velocity because they have a velocity of zero. As previously mentioned, the 57 % of Coinbase users who held their Bitcoin in 2016 had a velocity of zero. Coins that incorporate staking such as Dash also need to have their velocity adjusted because staked coins have a velocity of zero.

—

[6] Ibid.

Target Addressable Market

- **(P)** is the average price of goods in the economy. With regards to currency, utility, and stable coins, the price is the cost of the good or service being provisioned.
- **(Q)** is the quantity of goods in the economy.

> *"In 2012, I paid 5 BTC for 1lbs of coffee beans. The coffee wasn't good. Everyone in bitcoin has had a "pizza day" spending moment. Some of you just haven't realized it yet."*
>
> Andreas Antonopoulos
> May 2020

The total global demand for cryptoassets, **(PQ),** is calculated by determining the size of each target addressable market (TAM) for each coin for each year and what percentage of the TAM will be penetrated by the coin each year.

However, not all use cases can be served by all coins. So, first we have to distinguish between four types of coins:

- A store of value coin is defined as a distributed ledger technology that can be used to securely store value over time. Currency coins often **don't have Turing-complete protocols** that enable sophisticated smart contracts on the first layer of their distributed network. This include first generation cryptocurrencies, such as Bitcoin, Litecoin, and Bitcoin Cash.
- Utility coins and tokens that enable smart contracts are considered second generation cryptocurrencies. Smart contracts are automated contractual agreements that are stored by a group of different computers controlled by often conflicting parties and strangers. This group includes coins such as Ethereum, EOS, and Stellar.
- The third generation of cryptocurrencies are stablecoins. Stablecoins are normally ERC-20 tokens built on top of Ethereum's blockchain that maintain relatively stable purchasing power over time in terms of real goods and services in the economy. Stablecoins include Tether, USDC, and also stablecoins issued on public and permissionless distributed network like MakerDao Sai.
- Privacy coins are an offshoot of the first-generation cryptocurrencies. They are often volatile in price and have additional features that obfuscate information about each transaction including the wallet addresses of the sender and receiver and the transaction amount. This includes coins such as Dash, Monero, Zcash, Beam, Grin, and MimbleWimbleCoin.

Table 1: Coin Categories

Store of Value	**Bitcoin, Litecoin, Bitcoin Cash**
Utility	**Ethereum, EOS, Stellar**
Stable	**MakerDao Dai, Tether**
Privacy	**Monero, Dash, Zcash, MimbleWimbleCoin**

Once we know which coins are demanded for which use cases, we need to calculate the demand for each use case. The values for each target market can be additive or cannibalistic; meaning there can be either dual demands on a single supply or the

"Technology evolves in a 14-year cycle around advances in computing power

'54 - Mainframe

'68 - Microchip

'82 - PC

'96 - Internet

'10 - Mobilenet

'24 - Trustnet

Imagine investing in $IBM in '50, Fairchild in '64, $MSFT in '78, $CSCO in '92, $AAPL in '06

That's #Bitcoin today…."

Mark Yusko
Morgan Creek Capital Management
April 2020

demands are mutually exclusive and should not be added. Table 2 presents the assumed TAMs for cryptocurrencies including remittance, tax evasion, offshore accounts, store of value, online transactions, micropayments, STO and ICO funding, crypto trading, gaming, online gambling, unbanked, consumer loans, unit of account and medium of exchange, and reserve currency.

To project the TAM of future years, a reasonable assumption about the growth of this market going forward is required. **This paper assumes a compound annual growth rate for each TAM.** Some of the categories listed above lack reliable CAGR data. For those, **we have assumed an estimate based on the CAGR of the S&P 500 index over the period from 2000 to 2018** because a reasonable assumption of the growth rate could be the long-term growth of the world economy. Furthermore, we believe that some of the CAGR values for the other categories might be inflated due to the long bull run over the last 10 years. A well overdue market correction is likely to drive them down at least by 20–30 %. **The Corona virus' V-shaped recovery is obviously sustained by devaluing fiat currencies, which itself isn't sustainable.** Therefore, the market capitalization for each TAM is most likely an upper bound.

(PQ) is normally measured as gross domestic product (GDP) in traditional economic models. However, speculation on financial assets is normally left out of GDP metrics. Foreign exchange volume isn't included in GDP for example. Estimates that approximately 30 % of a cryptoasset's on-chain transaction volume comes from investor speculation as they transfer cryptocurrencies between exchanges. Therefore, calculating PxQ by on-chain transaction volume is a noisy signal. Also, forecasting PxQ in the future by transaction volume today has a large estimation error. Instead, focusing on the target addressable markets and the growth in those markets is a better estimate.

Table 2: Target Addressable Markets for Cryptoassets in Billions of USD

Target Addressable Market	Current Capitalization	Implied 2020 End of the Year Capitalization	Implied 2029 End of the Year Capitalization	CAGR data	Applicable Coins
Unit of Account and Medium of Exchange[7]	126,800	136,094	187,101	3.60 %	Stable, Store of Value
Consumer loans[8]	42,263	46,489	71,381	4.9 %	Stable

—

[7] Jeff Desjardins, "All of the World's Money and Markets in One Visualization," *Visual Capitalist*, October 26, 2017. Retrieved from http://money.visualcapitalist.com/worlds-money-markets-one-visualization-2017/

[8] "Global consumer lending: size, segmentation and forecast for the worldwide market," *The Free Library*, May 4, 2016. Retrieved from https://www.thefreelibrary.com/Global+consumer+lending%3A+size%2C+segmentation+and+forecast+for+the...-a0451297122

Offshore Accounts[9,10]	19,000	19,684	27,061	3.6 %	Store of Value, Stable, Privacy
Reserve currency[11,12,13]	11,737	13,290	23,247	6.4 %	Store of Value
Store of Value[14]	7,070	7,112	7,307	0.30 %	Store of Value
Online Transactions[15,16]	3,403	3,869	13,971	13.7 %	All
Remittance[17,18,19]	706	755	1,389	7.0 %	Stable, Store of Value
Micropayments[20]	617	934	6,020	23.0 %	All
Tax Evasion[21,22,23,24]	600	769	1,346	6.4 %	Store of Value, Stable, Privacy
Unbanked[25]	380	388	429	1.1 %	Store of value, Stable
Gaming[26,27]	149	181	397	10.3%	Utility
Online Gambling[2829]	59	70	149	8.8%	Utility, Privacy

[9] Kenneth Rapoza, "Tax Haven Cash Rising, Now Equal To At Least 10% Or World GDP," *Forbes*, September 15, 2017. Retrieved from https://www.forbes.com/sites/kenrapoza/2017/09/15/tax-haven-cash-rising-now-equal-to-at-least-10-of-world-gdp/#2678190870d6; "Global GDP (gross domestic product) at current prices from 2010 to 2022 (in billion U.S. dollars)," Statista, 2019. Retrieved from https://www.statista.com/statistics/268750/global-gross-domestic-product-gdp/

[10] Jannick Damgaard, Thomas Elkjaer, and Niels Johannesen, "Piercing the Veil", *IMF,* June 2018. Retrieved from https://www.imf.org/external/pubs/ft/fandd/2018/06/inside-the-world-of-global-tax-havens-and-offshore-banking/damgaard.htm

[11] Richard Leong, "U.S. dollar share of global currency reserves fall further – IMF," *Reuters*, July 1, 2018. Retrieved from https://www.reuters.com/article/uk-forex-reserves/u-s-dollar-share-of-global-currency-reserves-fall-further-imf-idUSKBN1JR21G

[12] Used S&P CAGR, due to lack of data

[13] IMF, Currency composition of official foreign exchange reserves. Retrieved from http://data.imf.org/?sk=E6A5F467-C14B-4AA8-9F6D-5A09EC4E62A4

[14] Sean Williams, "How Does Bitcoin's Market Cap Stack Up Next to Gold, the S&P 500, and the U.S. Dollar?," *The Motley Fool*, August 17, 2017. Retrieved from https://www.fool.com/investing/2017/08/17/how-does-bitcoins-market-cap-stack-up-next-to-gold.aspx; Martin Fridson, "Time To Go For Gold?," *Forbes*, August 12, 2016. Retrieved from https://www.forbes.com/sites/investor/2016/08/12/time-to-go-for-gold/#74f2f6622969

[15] "Digital Payments," *Statista*, 2019. Retrieved from https://www.statista.com/outlook/296/100/digital-payments/worldwide

[16] Digital Payments Market – Growth, Trends and Forecasts (2020–2025). Retrieved from https://www.mordorintelligence.com/industry-reports/digital-payments-market

[17] Toby Shapshak, "Global Remittances Reach $613 Billion Says World Bank," *Forbes*, May 21, 2018. Retrieved from https://www.forbes.com/sites/tobyshapshak/2018/05/21/global-remittances-reach-613bn-says-world-bank/#6d1d2d625ddc

[18] 2019 World Bank data. Retrieved from https://www.worldbank.org/en/topic/migrationremittancesdiasporaissues/brief/migration-remittances-data

[19] World Bank Group, "Migration and Remittances," April 2019. Retrieved from https://www.knomad.org/sites/default/files/2019-04/Migrationanddevelopmentbrief31.pdf

[20] Medici Team, "Payment Entrepreneurs go after MicroPayments segment; $13 B+ Opportunity globally," *Medici*, February 1, 2014. Retrieved from https://gomedici.com/payment-entrepreneurs-go-micropayments-segment-13-b-opportunity-globally/

[21] Niall McCarthy, "The Global Cost of Tax Avoidance," *Statista*, March 24, 2017. Retrieved from https://www.statista.com/chart/8668/the-global-cost-of-tax-avoidance/

[22] Used S&P CAGR, due to lack of data

[23] Nicholas Shaxson, "Tackling Tax Havens", *IMF*, September 2019. Retrieved from https://www.imf.org/external/pubs/ft/fandd/2019/09/tackling-global-tax-havens-shaxon.htm

[24] Petr Janský, "Hearing on Evaluation of Tax Gap," Charles University, Prague, Czechia, 23 January 2019. Retrieved from http://www.europarl.europa.eu/cmsdata/161049/2019%2001%2024%20-%20Petr%20Jansky%20written%20questions%20-%20Ev_TAX%20GAP.pdf

[25] Jeff Desjardins, "Banking the Unbanked is a $380B Opportunity," *Visual Capitalist*, July 20, 2017. Retrieved from https://www.visualcapitalist.com/banking-unbanked-emerging-markets/

[26] Tom Wijman, "Mobile Revenues Account for More Than 50% of the Global Games Market as It Reaches $137.9 Billion in 2018," *Newzoo*, April 30, 2018. Retrieved from https://newzoo.com/insights/articles/global-games-market-reaches-137-9-billion-in-2018-mobile-games-take-half/

[27] Teodora Dobrilova, "How Much Is the Gaming Industry Worth?," April 4, 2019. Retrieved from https://techjury.net/stats-about/gaming-industry-worth/#gref

[28] "Global Gambling Industry: State of Play in 2018," *Casino.org*, 2018. Retrieved from https://www.casino.org/gambling-statistics/

[29] Online Gambling Market – Growth, Trends and Forecasts (2019–2024). Retrieved from https://www.mordorintelligence.com/industry-reports/online-gambling-market

Crypto Trading[30,31]	18.25	20,665	36,147	6.4%	All
ICO Funding[32,3334]	7.3	7.8	14.6	6.4%	Utility
STO Funding[3536]	0.57	0.61	1.1	6.4%	All

Target Addressable Markets of Crypto Assets

This section describes the main use cases of cryptocurrencies: store of value, remittance, tax evasion, offshore deposits, gaming, online gambling, providing financial services to the world's unbanked, lending, online transactions, medium of exchange and unit of account, reserve assets, micropayments, crypto trading, and ICO and STO investing.

Medium of Exchange and Unit of Account

A medium of exchange is an intermediary instrument or system used to facilitate the sale, purchase, or trade of goods between parties. For a system to function as a medium of exchange, it must represent a standard of value. Using a medium of exchange allows for greater efficiency in an economy and stimulates an increase in overall trading activity. In a traditional barter system, trade between two parties can only happen if one party has a commodity that another party desires, and vice versa. The chance of this happening simultaneously as a cross occurrence–where each party desires something that the other party has–is improbable. Thankfully, with a medium of exchange, such as gold, if one party had a cow and happened to be in the market for a lawnmower, the cow owner could sell his animal for gold coins, which he may, in turn, use to purchase the lawnmower.

> *"MALL of AMERICA in Minnesota announced it will miss 2nd payment on its $1.4 billion mortgage. An intelligent question is "Who is not getting paid?" Dominos starting to fall. IMF says debt will rise from $6 trillion to $66 trillion by end of 2020. Buy Gold Silver & Bitcoin."*
>
> Robert Kiyosaki
> May 2020

The unit of account and medium of exchange markets are currently estimated to be around $126.8 trillion USD.[37] We could argue that all crypto is technically a medium of exchange; however, none more so than Bitcoin being the primer cryptocurrency. If we consider all of BTC currently being used for this purpose, this gives us a current market penetration of 0.13 %.

—

[30] "Global Charts," *CoinMarketCap*, 2019. Retrieved from https://coinmarketcap.com/charts/

[31] Used S&P CAGR, due to lack of data

[32] "Cryptocurrency ICO Stats 2018," *CoinSchedule*, January 27, 2019. Retrieved from https://www.coinschedule.com/stats.html?year=2018

[33] Used S&P CAGR, due to lack of data

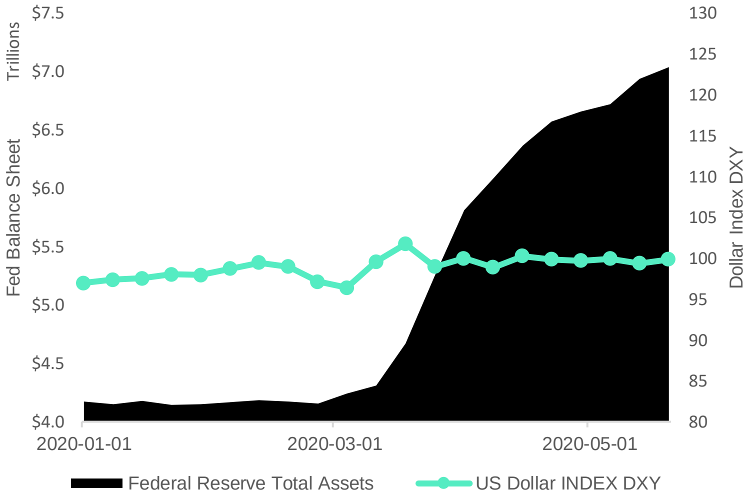
[34] *5th ICO / STO Report*, PWC, Summer 2019. Retrieved from https://www.pwc.ch/en/publications/2019/Strategy&_ICO_STO_Study_Summer_2019.pdf

[35] Ibid.

[36] Token sale statistics. Retrieved from https://www.coinschedule.com/stats/

[37] Jeff Desjardins, "All of the World's Money and Markets in One Visualization," *Visual Capitalist*, October 26, 2017. Retrieved from http://money.visualcapitalist.com/worlds-money-markets-one-visualization-2017/

Figure 1: Federal Reserve Assets Almost Double and Dollar Index Stays Flat



Source: St. Louis Federal Reserve Fred, Yahoo Finance, and CryptoResearch.Report

Despite unprecedented quantitative easing, trillions of short-term credits to the repurchase agreement market, and lowering interest rates to zero, **the US dollar index (DXY) barely moved.** This means that the dollar can take a lot more abuse from the printing machines, before it starts to devalue against other fiat currencies. Also, the 5-year forward inflation expectation for the US dollar is sitting at a low 1.43 %. This means that despite massive debasement of the US dollar, markets expect inflation to be below the Federal Reserve's target 2 %. Fed Chairman Powell understands that he can print more, and most likely he will.

"Gentlemen, you can calm down. The printing presses run day and night again in three shifts."

Rudolf Havenstein
German President of the
Reichsbank During the Weimar
Republic Hyperinflation
1921–1923

Fortunately, the blockchain technology has reduced the cost of switching between currencies. Phone applications, such as Crypto.com, already allow people to earn interest on several different types of cryptocurrencies and stablecoins that represent different fiat currencies. In the future, people will be able to hold portfolios of tokenized currencies in their bank account and on their phone, and they will easily be able to exchange currencies by pressing a few buttons. When the Turkish lira is losing value, they will be able to switch into a safe haven stablecoin like a tokenized Swiss franc. When Turkish banks offer high interest rates to attract capital, people will be able to easily switch back to the Turkish lira in order to earn higher interest rates on their deposits. This is already possible due to the dollarization of public blockchains discussed later in this report in *Tether or Not to Tether* by Pascal Hügli.

Offshore Accounts

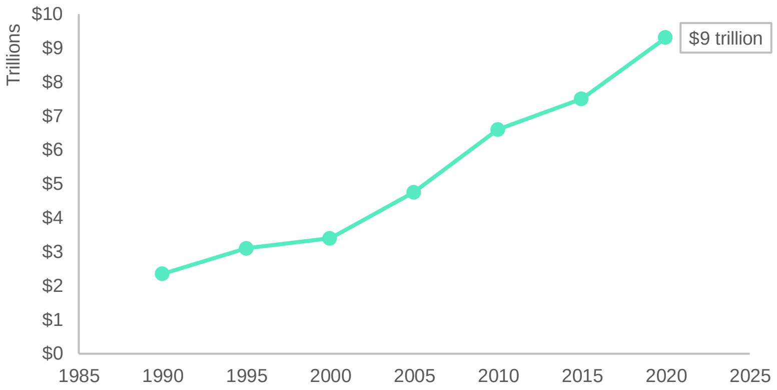
The Tax Justice Network estimates that governments lose $189 billion a year from $21–32 trillion in offshore accounts of private wealth.[38] The International Monetary Fund estimates tax evasion to be approximately $12 trillion a year

—

[38] "Estimates of tax avoidance and evasion," tax justice network, 2020. Retrieved from https://www.taxjustice.net/topics/more/estimates-of-tax-avoidance-and-evasion/

globally.[39] The Satis report analyzed the target addressable markets for the entire cryptoasset market and found that the total implied market cap to be $3.6 trillion by 2028 using the a similar equation of exchange model to the one developed in this research report. According to the Satis report, the major application of cryptocurrencies is offshore deposits. **They estimate cryptocurrencies will penetrate approximately 91 % of the offshore deposits market during the next decade.**[40] They also estimate the offshore deposit market to grow because of capital controls, national debt, unpopular fiscal policy, and debasement of national fiat currencies.

Figure 2: Cryptocurrencies Will Absorb Part of Global Offshore Wealth Market



Source: Forbes, IMF, CryptoResearch.Report

“According to Chainalysis, cryptocurrency e-commerce transactions account for $6 million daily.”

Although the Satis report uses “offshore accounts” and “tax evasion” synonymously, offshore accounts can also be used for non-illicit purposes such as opening up a business abroad and earning income. Also, many multinational companies have reserves abroad in case of a banking crisis in their domestic currency. In a bid to protect their assets from financial calamity, institutional investors are embracing the use of offshore crypto deposit accounts. According to several estimates, offshore tax havens account for 10 % of global GDP.[41] Ten percent of global GDP provides the offshore account estimates in the Excel spreadsheet. A 3.6 compound annual growth rate is assumed in order to forecast the future GDP and growth in demand for offshore deposits.

Reserve Currency

Reserve currencies are foreign currencies held by central banks. When a country acquires reserves, it doesn't place the currency in general circulation. Instead, it

—

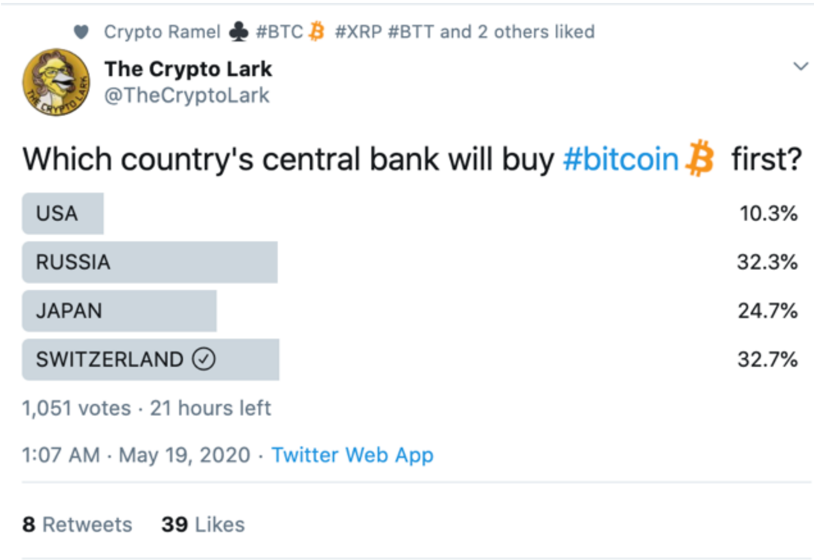
[39] Jannick Damgaard, Thomas Elkjaer, and Niels Johannesen, “Piercing the Veil,” *Finance and Development,* June 2018. Retrieved from https://www.imf.org/external/pubs/ft/fandd/2018/06/inside-the-world-of-global-tax-havens-and-offshore-banking/damgaard.htm

[40] Sherwin Dowlat, “Cryptoasset Market Coverage Initiation: Valuation August 30, 2018,” *Satis Group*, 2018. Retrieved from https://research.bloomberg.com/pub/res/d37g1Q1hEhBkiRCu_ruMdMsbc0A

[41] Kenneth Rapoza, “Tax Haven Cash Rising, Now Equal To At Least 10% Or World GDP,” *Forbes*, September 15, 2017. Retrieved from https://www.forbes.com/sites/kenrapoza/2017/09/15/tax-haven-cash-rising-now-equal-to-at-least-10-of-world-gdp/#2678190870d6/

parks the reserves in the central bank. The reserves are acquired through trade, with the acquiring country selling goods in exchange for currency.

Reserve currencies thus grease the wheels of international commerce by helping countries and businesses conduct transactions using the same currency, a much simpler task than settling transactions involving different currencies. Their popularity is easy to see: Between 1995 and 2011, the amount of currency held in reserve increased by over 730 %, from around $1.4 trillion to $10.2 trillion.



Crypto Ramel ♣ #BTC ₿ #XRP #BTT and 2 others liked

The Crypto Lark
@TheCryptoLark

Which country's central bank will buy #bitcoin ₿ first?

USA	10.3%
RUSSIA	32.3%
JAPAN	24.7%
SWITZERLAND ✓	32.7%

1,051 votes · 21 hours left

1:07 AM · May 19, 2020 · Twitter Web App

8 Retweets 39 Likes

Many central banks are rumored to have already bought cryptocurrencies. The rumors say they just aren't admitting this to the public. Source: Twitter

Reserve currencies are typically issued by developed, stable countries. The currency most commonly held as a foreign exchange reserve is the US dollar, which, according to the International Monetary Fund (IMF), comprised nearly 62 % of allocated reserves as of late 2012. Other currencies held in reserve include the euro, Japanese yen, Swiss franc and pound sterling. The dollar, while still the most widely held reserve currency, has seen increased competition from the euro. The euro has grown from slightly less than an 18 % share of allocated reserves when it was introduced into the financial markets in 1999 to 24 % at the end of 2011.

The IMF reports both allocated reserves, meaning that a country has identified the currencies held in reserve, and total foreign exchange holdings. The overall percentage of total holdings that are allocated reserves has fallen steadily over the years, from 74 % in 1995 to 55 % in 2011. Much of this shift can be explained by changing foreign exchange holdings in emerging and developing countries. In 1995, advanced economies held around 67 % of total foreign exchange reserves, with 82 % of these being allocated reserves. By 2011, the picture had been flipped on its head: Emerging and developing countries held 67 % of total reserves, with less than 39 % allocated. Emerging countries now hold roughly $6.8 trillion in reserve currency[42].

Currently, reserve currencies sit at around 11.7 trillion[43] and no central bank has officially admitted to holding any cryptocurrency in its reserves.

—

[42] Brent Radcliffe, "A Primer on Reserve Currencies," *Investopedia,* March 19, 2020. Retrieved from https://www.investopedia.com/articles/economics/13/reserve-currencies.asp

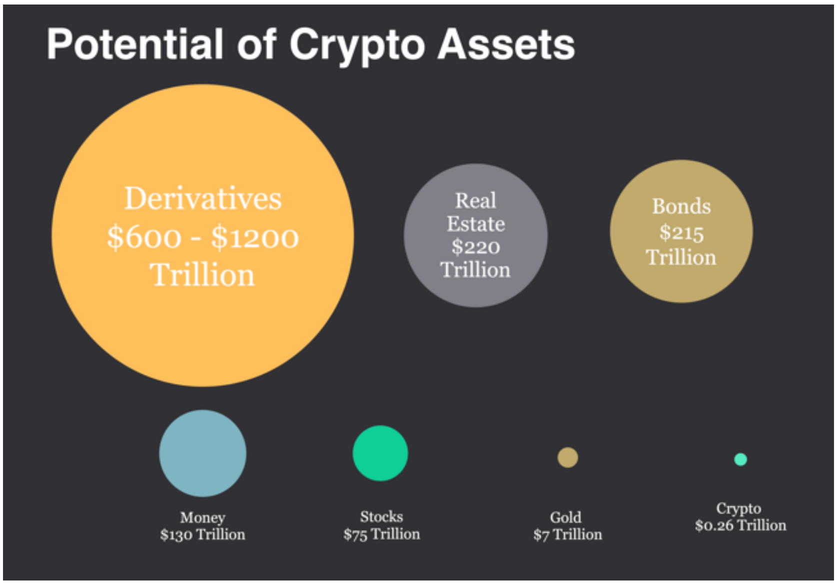
[43] "Currency composition of official foreign exchange reserves, " *IMF*, March 31, 2020. Retrieved from http://data.imf.org/?sk=E6A5F467-C14B-4AA8-9F6D-5A09EC4E62A4

Store of Value

“The majority of Bitcoins have been held for more than 6 months. This provides evidence that the main use case for Bitcoin is not speculation and day trading.”

As shown in **Table 2**, the target addressable market for stores of value is over $7 trillion.[44] This figure mostly comes from the global market capitalization of gold. However, people also store value in fiat currency. The US dollar alone has a market capitalization of $3.8 trillion, which is 20 times larger than Bitcoin’s market capitalization. People also store their wealth in stocks and bonds and real estate, so $7.07 trillion is a lower-bound on the largest target addressable market for cryptocurrencies. When it comes to store of value, the go-to cryptocurrency seems to be Bitcoin. If we consider that store-of-value seekers don’t move their bitcoin often, we can see that around 11 million BTC have not moved in nearly a year.[45] It is worth nothing that this amount inevitably includes some lost keys. As of the time of writing this report, this accounts to around $98.6 billion or a 1.4 % penetration.

Figure 3: Bitcoin’s Target Addressable Market is Worth $1247 Trillion



Source: CryptoResearch.Report

Some critics of cryptocurrencies argue that cryptocurrencies aren’t used as a store of value. They argue that cryptocurrencies are only used for day trading and speculation. A good measure of whether coins are used as a store of value or for short term speculation is the “age” of each coin. The average age of 20 % of all of the bitcoin in existence have been held for over 5 years.[46] We assume that these coins are being used as a store of value. The majority of bitcoins have been held for more than 6 months, which **provides evidence that bitcoin holders aren’t using bitcoin for day trading but are rather holding for long-term appreciation.** Factors promoting crypto use and adoption as a store of value

—

[44] Sean Williams, “How Does Bitcoin’s Market Cap Stack Up Next to Gold, the S&P 500, and U.S. Dollar?,” *The Motley Fool*, August 17, 2017. Retrieved from https://www.fool.com/investing/2017/08/17/how-does-bitcoins-market-cap-stack-up-next-to-gold.aspx

[45] Jamie Redman, “Close to 11 Million BTC Haven’t Moved in Over a Year,” *Bitcoin.com*, January 13, 2020. Retrieved from https://news.bitcoin.com/close-to-11-million-btc-havent-moved-in-over-a-year/

[46] “Bitcoin UTXO Age Distribution,” *Hodlwave*, 2020. Retrieved from https://hodlwave.com/

include scarcity, transparency, global availability, pseudonymity, and immutability.

One of the factors contributing to a rise in popularity is the fact that most digital currencies have a finite supply, resulting in scarcity. Currencies controlled by central authorities are often subject to arbitrary inflation, especially in emerging economies (Folkinshteyn & Lennon 2016). Paul Tudor Jones, who runs the Tudor BVI fund, holds a low single-digit percentage of its assets in Bitcoin futures, because of the massive fiscal spending and bond-buying by central banks to combat the coronavirus pandemic. **By his calculation, $3.9 trillion of money, the equivalent of 6.6 % of global economic output, have been printed since February 2020.**

Online Transactions

"The best profit-maximizing strategy is to own the fastest horse. If I am forced to forecast, my bet is it will be Bitcoin."

Paul Tudor Jones
CEO, Tudor Investment Corp.
May 2020

According to a report on the digital payment market by Mordor Intelligence and data from Statista, online transactions account for between $4.4 trillion and $3.4 trillion per year.[47] The research firm Chainalysis estimates that **cryptocurrency commerce transactions account for $6 million daily.**[48] This means that cryptocurrency payments have not even penetrated 1 % of online transactions. However, according to the same report by Chainalysis, the amount of digital money sent to 16 merchant service providers, such as BitPay, rose 65 % between January and July of 2019. This is because cryptocurrency transactions are comparatively faster, taking a few seconds optimally or about an hour when networks are congested. There are also no chargebacks with cryptocurrencies, which stops a lot of online fraud.

Transaction platforms like BitPay recorded consistent annual growth in transaction rates (DeVries, 2016). According to a BitPay annual report in 2017, the platform recorded a payments dollar volume increment of 328 % year-on-year from 2016. During that period, merchants using the platform were getting more than $1 million every month in bitcoin payments. Overall, the service provider was on track to process **over $1 billion annually** through bitcoin payment acceptance and payouts during 2017 and 2018.[49] BitPay's B2B business grew 255 % between 2017 and 2018 because law firms, data center providers, and IT vendors signed up to accept Bitcoin. BitPay also hired Rolf Haag, Former Western Union and PayPal executive as Head of Industry Solutions responsible for the B2B business.

The Copay wallet, BitPay wallet, and other wallets using BitPay's Bitcore Wallet Service (BWS) **have over 1.5 million unique wallets.** In the past year, the

—

[47] "Digital Payments Market – Growth, Trends and Forecasts (2020–2025)," *Mordor Intelligence*, 2020. Retrieved from https://www.mordorintelligence.com/industry-reports/digital-payments-market

[48] Olga Kharif, "From Online Gambling to Pot, Crypto Commerce Takes Off This Year," *Bloomberg*, November 6, 2019. Retrieved from https://www.bloomberg.com/news/articles/2019-11-06/crypto-commerce-jumps-65-as-tether-s-use-takes-off-this-year

[49] Jan Jahosky, "BitPay Sees Record Year for Revenue in 2018, with $1 Billion in Transactions," *BusinessWire*, January 16, 2019. Retrieved from https://www.businesswire.com/news/home/20190116005701/en/BitPay-Sees-Record-Year-Revenue-2018-1

BitPay wallet added integrations with major gift card brands, enabling users to buy gift cards in-app for travel, food, and shopping with Bitcoin and Bitcoin Cash.

Famous merchants such as Microsoft, CheapAir (Flights), Travala (hotel bookings)[50], and the Dallas Mavericks basketball team accept cryptocurrency payments in order to reach out to niche markets of cryptocurrency holders. Local governments are also accepting cryptocurrency payments, such as Ticino and Zug in Switzerland and Seminole County, Florida in the US to name a few.

Brick and mortar commerce, online e-commerce, casinos, and tax collectors all need a payment processor to handle the currency risk of accepting cryptocurrencies. For this reason, software and hardware point-of-sale (PoS) systems are an interesting business model that has increasing demand. The Crypto Research Report recently covered how Worldline and Ingenico are both rolling out PoS systems in Europe during the summer of 2020. Additional payment processors companies that settle cryptocurrency payments include Salamantex, AnyPay, CryptoBuyer, GoCoin, Coinpayments, Coingate. These companies offer hardware and software solutions for merchants. For example, Salamantex has a hardware that merchants can add to their existing hardware point of sale system. Gocoin, Coinpayments, and Coingate all offer plugins for e-commerce websites like Woocommerce, Shopify, and Wordpress.

“Still hilarious that oil went to $0 and Bitcoin didn’t.”

Anthony Pompliano
Morgan Creek Digital
May 2020

The largest start-up in this space is Spedn, which is owned by Flexa which the Winklevoss Twins invested in. They will enable all Starbucks coffee shops in the USA to accept cryptocurrency payments beginning in 2020. Coinbase also offers the service of payment processing. One of the most recent newcomers to this space is Crypto.com, but they are expected to make a big splash.

Although cryptocurrencies were originally designed to be digital cash, online transactions with cryptocurrencies have not really picked up traction. In a recent peer-reviewed journal paper, Nicole Jonker found that crypto acceptance from online retailers is a modest 2 % of all online stores.[51] This is mostly because most cryptocurrencies are deflationary, and investors don’t want to spend them. Most merchants convert crypto payments to fiat to avoid volatility issues. However, online transactions may gain adoption with stablecoins since they aren’t deflationary. For example, BitPay added settlement support for US dollar stablecoins from Circle, Gemini, and Paxos in 2018.

In addition to be used in brick and mortar stores and for online shopping, cryptocurrencies are also spent online on illegal goods and services. According to

—

[50] “Travala.com Monthly Report: October 2019,” *Travala.com*, November 1, 2019. Retrieved from https://blog.travala.com/travala-com-monthly-report-october-2019/

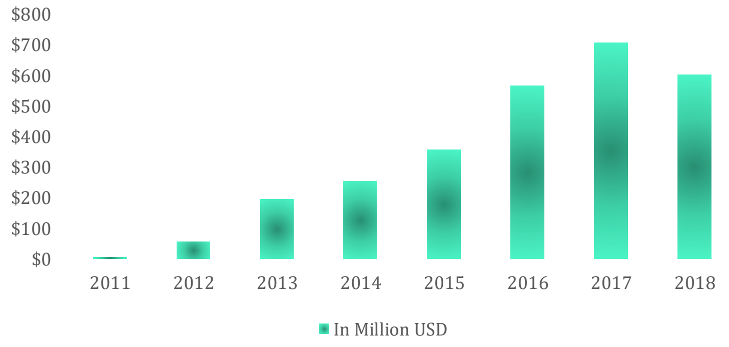
[51] Nicole Jonker, “What drives the adoption of crypto-payments by online retailers?,” *Electronic Commerce, Research and Applications*, 35, May-June 2019. Retrieved from https://www.sciencedirect.com/science/article/pii/S1567422319300250

Chainalysis, **darknet trading volume was estimated to be as high as $700 million in 2017 and $600 million in 2018.**[52,53]

"A firefighter has never been criticized for using too much water."

Stephen Poloz
Governor, Bank of Canada

Figure 4: $600 Million in Darknet Volume Annually

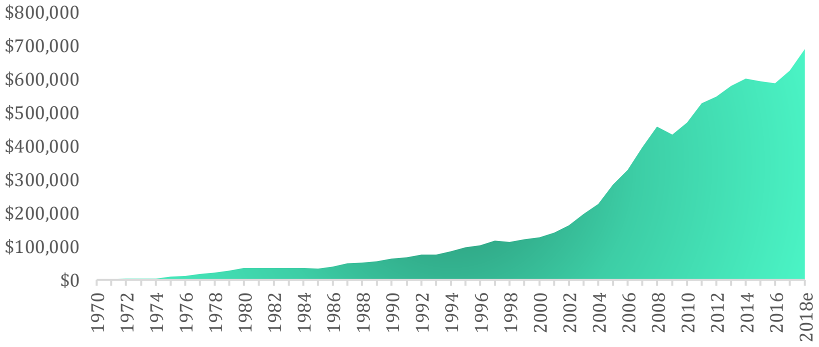


Source: Chainanalysis, CryptoResearch.Report

Remittance

In 2018, migrants in various parts of the globe sent upwards of $613 billion to their home countries. However, the use of traditional banking services means high transaction fees and slow processing. The Philippines, which is one of the world's top remittance markets, already has solutions like Coins.ph that use crypto and blockchain technology that allow individuals to send money home with lower fees.

Figure 5: Remittance Market is Annually Increasing



Source: World Bank, CryptoResearch.Report

Many remittances are being conducted via Bitcoin ATMs that have remittance features enabled. This feature allows an individual to put British pounds into an ATM in London and to receive a code. They can send that code to a relative or friend in New York. Their friend can go to a Bitcoin ATM in New York and put the

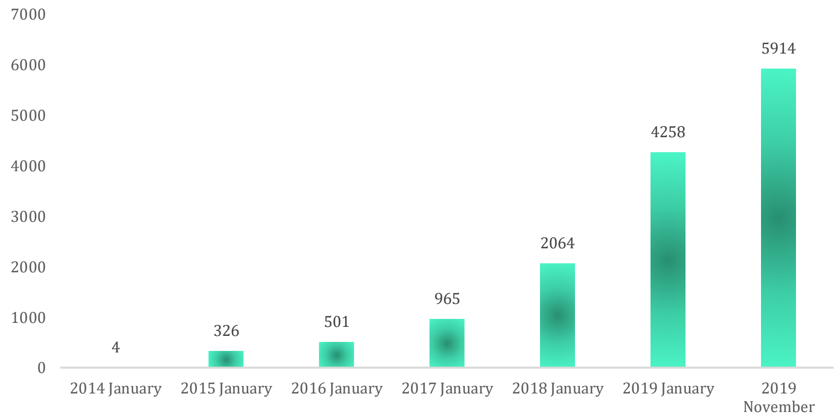
—

[52] Aaron van Wirdum, "Following the Waves Of Shutdowns, Remaining Darknet Markets Fill The Void (Again)," *Bitcoin Magazine*, June 17, 2019. Retrieved from https://bitcoinmagazine.com/articles/following-wave-of-shutdowns-remaining-darknet-markets-fill-the-void-again

[53] Chainalysis Team, "Crypto Crime Series: Decoding Darknet Markets," *Insights*, January 18, 2019. Retrieved from https://blog.chainalysis.com/reports/decoding-darknet-markets

code in and then receive US dollars. This feature is currently working for over 100 countries and 35 different currencies.

Figure 6: The Number of Bitcoin ATMs Installed Across the Globe

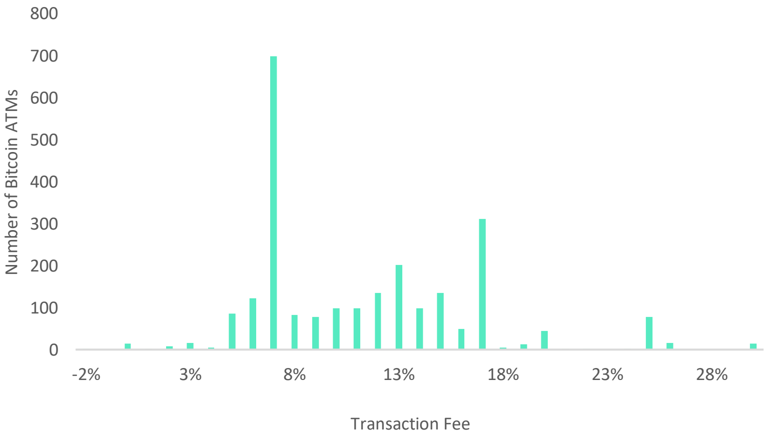


Source: Coinatmradar.com, CryptoResearch.Report

Statistical data on the number of Bitcoin ATMs globally reveals a consistent rise over the years. In January 2016, Coinatmradar shows that there were only 501 of them worldwide but by January 2017, the number had grown to 965. In January 2018, they had more than doubled to 2,073, almost doubling again by January 2019 to 4,112. However, the average Bitcoin ATM fee is 10 %. There are 84 Bitcoin ATMs in Switzerland, 296 in DACH, not including SBB and kiosk ATMs.

> *"Swiss banks have been extremely reticent with regard to blockchain-based business models. As a result, it was almost impossible for entrepreneurs from the Zug Crypto Valley to open a company account for payment transactions (salaries, rent, accounts payable) We view ourselves as being significantly ahead of our competitors. We have now welcomed about 300 of these blockchain-friendly firms as clients here at Bank Frick."*
>
> Bank Frick

Figure 7: Average Fee on Bitcoin ATMs is 10%.



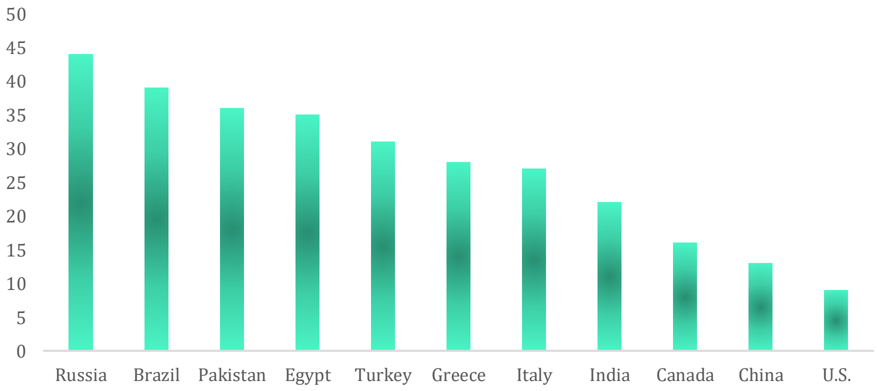
Source: Coinatmradar.com, CryptoResearch.Report

Tax Evasion

The original ethos of crypto was libertarian, and that attitude still prevails in the industry. It's no surprise that some cryptocurrency users aren't fully reporting their gains, and that some tax evaders adopt cryptocurrencies for this purpose. Each country has a unique level of tax evasion, and that level is dynamic over time and depending on variables such as tax rates, public debt amount, history of nationalization of industries, culture, etc. Cryptocurrencies offer tax evaders a new way to hide assets, and they will be used in this way. **Even if KYC/ AML is implemented on every exchange via the Travel Rule, money can still be laundered and hidden with cryptocurrencies by mining newly minted coins.** One way to ensure access to untracked or "dirty" Bitcoin and other cryptocurrencies is to become a cryptocurrency miner. Cryptocurrency miners can simply buy graphics cards and electricity and turn this into untracked assets. There is evidence that miners in Asia are entering the mining industry in order to get capital out of China and India without tax authorities knowing. Another way is to buy coins with cash; however, the war on cash (demonetization of large denominations) and inflation has reduced the ability to transact with large quantities of cash. Therefore, a large portion of tax evasion and money laundering in this space will focus on mining. This is a form of tax evasion for high net worth individuals (HNWI) and corporations.

> *"Even if KYC/ AML is implemented on every exchange via the Travel Rule, money can still be laundered and hidden with cryptocurrencies by mining newly minted coins."*

Figure 8: Size of the Untaxed "Shadow" Economy in Selected Countries 2010, as a Share of GDP



Source: Tax Justice Network, Bloomberg Businessweek, CryptoResearch.Report

Due to the difficulty of estimating the amount of tax evasion globally, and the difficulty in forecasting this variable into the future, this paper uses the S&P 500 growth rate and assumes the percentage of tax evasion in the economy is constant over time. **This paper estimates the tax evasion market to be $600 billion based on estimates provided by the United Nations University.**[54] Tax evasion by institutions and HNWIs will be more likely to target privacy coins and low-volatility coins such as stablecoins and Bitcoin rather than physical fiat cash because of the sums involved. However, this is also a large portion of tax evasion through "black economies" where lower and middle classes don't report earnings.

—

[54] Niall McCarthy, "The Global Cost of Tax Avoidance," *Statista*, March 24, 2017. Retrieved from https://www.statista.com/chart/8668/the-global-cost-of-tax-avoidance/

Physical fiat cash may be better for black market tax evasion by middle class and lower-class workers because there is no record and there is limited volatility. However, black markets in countries where this is heavy inflation in the domestic currency are more likely to switch to cryptoassets.

In this regard, the closest proxy which we can come for this in the crypto world are privacy coins. It stands to reason that anyone using crypto for tax evasion would focus primarily on fully untraceable coins. Looking at the two biggest ones, Monero and Dash have a combined market cap of $1.8 billion. Even if all of them are used solely for this purpose, this still gives us a penetration of less than 0.3 %.

> *"We do not interpret bitcoin's popularity as having a relationship with the public view of the Federal Reserve's conduct of monetary policy."*
>
> Janet Yellen
> Former Chairwoman
> Federal Reserve

Smaller Target Markets and Use Cases

Micropayments and Unbanked

Cryptocurrencies that are stable and have low transaction fees are well-suited for micropayments because they eliminate the inconvenience and security risk of submitting credit card data for every minor transaction (Spilka, 2018). In certain cases, merchants have been put off by the high fees associated with low-cost transactions on traditional systems. With lower fees, higher security and fast transaction processing, more businesses could adopt micro-transactions using crypto (Spilka, 2018). This could enable new business models such as a browser that pays online news websites to block advertisements. According to Business Insider, micropayments help solve a problem for online content providers, such as digital music and app purchases.[55]

Close to 2 billion people remain unbanked globally, a third of whom live in Sub-Saharan Africa (Bank4YOU, 2018). In some of the countries within this region, smartphone proliferation is quite high ("Banking is Only the Beginning," 2018). With an internet connection, they can access crypto services and get funding and remittance services among other opportunities with ease.

ICO and STO Funding and Crypto Trading

Ethereum has led to the rise of an alternative fund-raising model. Though these are often associated with fraud and poor investor protection, they have created new capital flow pathways with broader investor access. Creating digital representations of assets can reduce the costs and level of friction associated with management, transfer and issuance of traditional assets. They have therefore helped to enhance liquidity and transparency in the life cycle of such assets (Nagaraj, Hunter & Captain, 2018). These practical applications of the technology are highly likely to remain relevant and foster adoption.

—

[55] Jaime Toplin, "The Micropayments Report: Problems and solutions for low-value payments". *Business Insider*, January 12, 2017. Retrieved from https://www.businessinsider.com/micropayments-report-2017

"Grayscale's Bitcoin Trust is on a whole new level in 2020.

Average weekly investment (Q1 2019): $3.2 million

Average weekly investment (Q1 2020): $29.9 million

Institutional money has arrived."

Kevin Rooke
May 2020

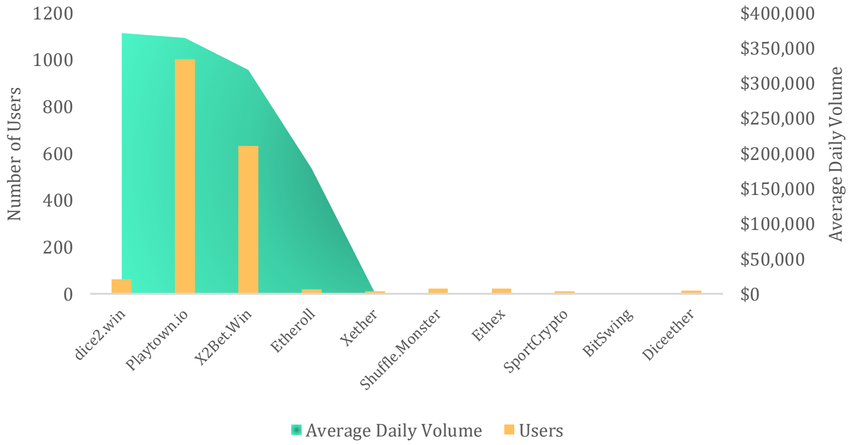
ICO funding has also fostered the adoption of crypto in spite of the bad press that has resulted from scams in the sector. By lowering the entry barrier to obtain funding for and making investments in start-ups, start-ups are now able to bypass early seed investment or use crowdfunding in addition to early seed investment (Davis, 2018). Interestingly, ICOs have not eliminated traditional venture capital but has made them adapt and evolve (Town, 2018). Start-ups raised $ 5.5 billion worldwide in 2017 by issuing tokens in the framework of ICOs – and this year the total amount has already swelled to $ 14.3 billion.[56]

It goes without saying that crypto has already a full penetration of this market, as token sales which accept only fiat currencies are practically non-existent.

Gambling and Gaming

In addition to online e-commerce, online gambling is also an important market for cryptocurrencies. In a few short years, Ethereum has become home to over 400 decentralized gambling applications, with gameplay ranging from traditional casino slots to gamified options trading and prediction markets. There are several online casinos, which offer payment in cryptocurrencies.[57] Casinoanbieter.com states that their clients' demand for crypto gambling is increasing.

Figure 9: Top 10 Decentralized Gambling Applications Have Over $1 Million in Total Daily Volume



Source: DappRadar, CryptoResearch.Report

Though the online gambling industry has been on an uptrend ("Banking is only the beginning," 2018), its core issues related to transparency have yet to find solutions. The use of crypto has however made it possible to reestablish trust, transparency and fairness. It curbs the vice of record manipulation, ruling out the "house always wins" mantra.

—

[56] Figures according to Coindesk ICO Tracker, accessed September 19, 2018.

[57] Frank Sellingen, "Beste Online Bitcoin Casinos im Überblick," *Casinoanbieter.com*, 2020. Retrieved from https://casinoanbieter.com/einzahlen-auszahlen/bitcoin/

"I've been wrong in thinking you could really have the developments you've had without inflation taking hold."

Warren Buffet
May 2020

The global gaming industry which is expected to grow to $143 billion by 2020 (Wolfson, 2018) is yet another ripe market for virtual currency adoption. Virtual money is in fact not new to the sector since digital gold has for over a decade been used for in-game purchases. With the advent of crypto, however, players can now trade virtual gaming items more easily with each other (Wolfson, 2018). It has also solved the problem of in-game asset ownership through tokenization. Under this model, gamers will retain ownership of their acquired assets within a digital wallet till they decide to trade or sell them.

According to the following report[58], the crypto-specific gambling scene sees volumes close to $2.5 billion annually on its top gambling apps. Compared to an estimated $59 billion for the industry as a whole[59], this makes it one of the most penetrated markets by crypto at 4.2 %.

Adoption Rate

Once the M, V, P, and Q are estimated, the penetration rate of each TAM by each cryptocurrency is calculated. This is called the adoption rate, and this is based on an assumption regarding future use of the currency for each use case. To estimate adoption, there are two mains methods: first, estimating the growth in the number of people owning crypto per year and, second, fitting a curve to the historical growth in active wallet addresses.

Forecasting Adoption with Historical Data on the Growth in the Number of People Using Crypto Worldwide

Approximately 40+ million cryptocurrency users exist globally according to our research. The number of registered accounts on the biggest crypto exchanges serve as a usable proxy. Coinbase for example has more than 30 million users (CoinTelegraph).[60] Binance founder Changpeng Zhao (CZ) recently said in an interview that they have about 12 to 15 million registered users and about 0.5 to 2 million daily active users. There are several other similarly big exchanges, like Kraken, Bitstamp, Bitfinex, Bittrex, Huobi, and OKEx. Assuming that Coinbase has the most users, there must be at least 30 million cryptocurrency users. **Binance and Coinbase together have about 45 million users.** This averages to 22.5 million users per exchange. For the eight biggest exchanges, a number of 180 million (22.5 x 8) users would come up. Adding the assumption that most users are registered on several exchanges, this number seems to be too big. **The correct answer probably lies between 35 to 70 million users.**

—

[58] *The Crypto Betting Industry* [Research Report], The Crypto Community. Retrieved from https://thecrypto.community/wp-content/uploads/2019/10/The-Crypto-Betting-Industry-TheCrypto.Community-3.pdf

[59] "Global Gambling Industry: State of Play in 2018," *Casino.org*, 2018. Retrieved from https://www.casino.org/gambling-statistics/

[60] Helen Partz, "Coinbase Added 8 Million New Users in the Past Year," *Cointelegraph*, July 23, 2019. Retrieved from https://cointelegraph.com/news/coinbase-added-8-million-new-users-in-the-past-year

"'Good and bad coin cannot circulate together."

Sir Thomas Gresham
Letter to Queen Elizabeth
1558

Having a look at different surveys, about 5–8% of US-American adults own cryptocurrencies (Statista Global Consumer Survey, Finder.com). There are countries like Turkey which have more users and countries like Japan that have fewer. Also, according to the survey, Spain has a higher level of cryptocurrency users when compared to other western European countries. In Spain, 10 % of adults own cryptocurrencies.[61]

A final estimate of the total number of users could be done with the following experiment. There are about 4.3 billion people with access to internet, therefore being possible crypto owners. Let's subtract 1.5 billion because of legislative restriction (i. e. China, Pakistan, and others). The following table shows the number of potential cryptocurrency users depending on the world's population.

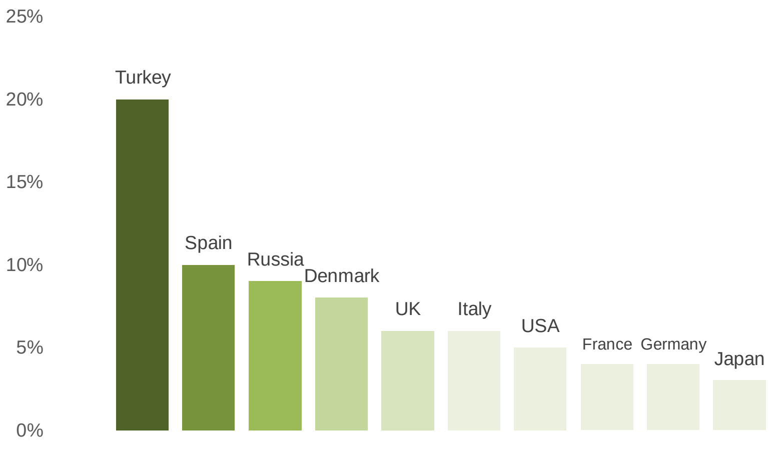
Table 3: Estimating the World's Population of Crypto Users

Percentage	World's Population
1 %	28,000,000
2 %	56,000,000
3 %	84,000,000

Source: CryptoResearch.Report

According to the CEO of Binance, SZ, the number of accounts from a country on Binance correlates positively with the GDP per capita (high GDP – more accounts).

Figure 10: Percentage of Cryptocurrency Users per Country



Source: Statista.com[62], CryptoResearch.Report

—

[61] Mathias Brandt, "So verbreitet sind Kryptowährungen," *Statista*, May 25, 2019. Retrieved from https://de.statista.com/infografik/18102/nutzung-von-kryptowaehrungen/

[62] Ibid.

Forecasting Adoption with Historical Data on the Growth in the Active Addresses

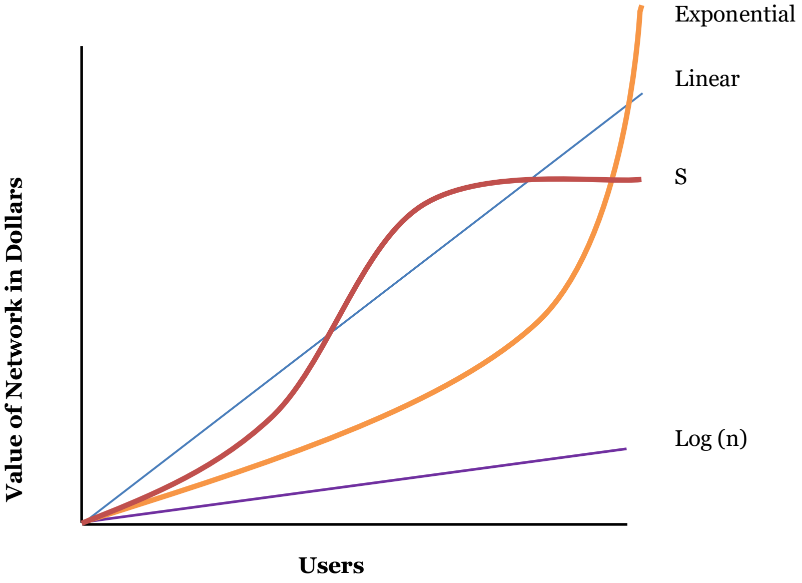
“You can print more money, but you can’t print more hard work. That takes time, effort and energy.”

The Bitcoin Rabbi

Another approach is to count the number of wallets. According to BitInfoCharts, there are currently more than 43 million Bitcoin addresses. If we use this as a proxy and take Bitcoin dominance into consideration, which is currently at 67 % (CoinMarketCap), we can assume that there must be about 64 million addresses 43 / 0.67) for Bitcoin and all Altcoins. Some users may have both, bitcoins and altcoins; therefore, there may be roughly about 37 to 52 million cryptocurrency users.

Most studies adopt an S-curve beginning on when the network is launched. There are several different possible curves for cryptocurrency adoption, such as S-curve and linear. Other curve options include exponential and log. All of the following curve assumptions can be seen on the following graph.

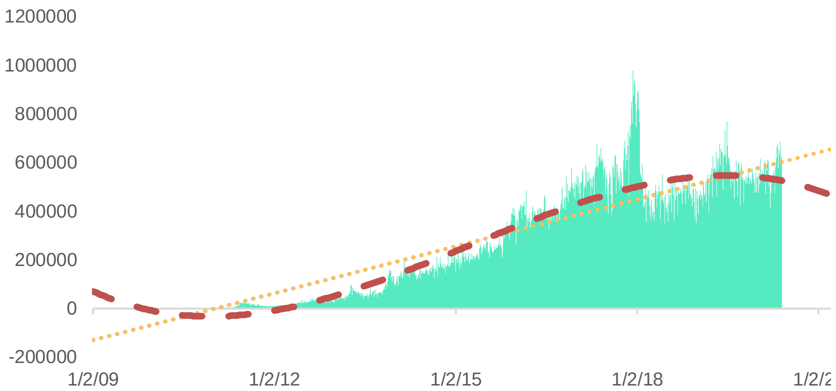
Figure 11: Adoption Curves for Network Use



Source: CryptoResearch.Report

After fitting the daily data of wallet use with a non-zero balance, **use of Bitcoin as a medium of exchange appears to be following a linear curve or an S-curve and currently has approximately 600,000 active users per day.**

Figure 12: Bitcoin’s Adoption Curve is Assumed to be an S-Curve



Source: Blockchain.info, CryptoResearch.Report

From behavioral economics, many variables impact adoption, such as path dependency, network effects, superior technology, market salience, and ambiguity aversion held by investors and users. Adoption is difficult to measure because once a metric becomes standardized, cryptocurrency developers and investors try to game that metric or trick that metric in order to manipulate the market.

Scenarios

To improve the robustness of the adoption rate analysis, several scenarios can be calculated for the adoption rate of each cryptocurrency for their respective TAMs. **This report assumes three different scenarios:**

- Bearish
  a. Cryptocurrency will only takeover 1 % of the entire target addressable market.
  b. The cryptocurrency will take two years to achieve 10 % of the 1 % adoption.
  c. The number of years that the cryptocurrency will take to achieve 90 % of the 1 % adoption will be seven.
- Modest
  a. Cryptocurrency will only takeover 10 % of the entire target addressable market.
  b. The cryptocurrency will take two years to achieve 10 % of the 1 % adoption.
  c. The number of years that the cryptocurrency will take to achieve 90 % of the 1 % adoption will be five.
- Bullish
  a. Cryptocurrency will only takeover 20 % of the entire target addressable market.
  b. The cryptocurrency will take two years to achieve 20 % of the 1 % adoption.
  c. The number of years that the cryptocurrency will take to achieve 90 % of the 1 % adoption will be five.

> *"The best way to think about Bitcoin is as a non-correlated asset most similar to gold, except that it's much more easily transportable than gold."*
>
> Bill Miller
> Founder and Chairman
> Miller Value Partners
> 2018

Discount Rate

A dollar today is worth more than a dollar a year from now. Stock valuation models, such as the discounted cash flow model, can use discounts rates of 10–50 % per year based on the risk of the industry and the company. Take the future current value and discount it back to the present. Taking the value of $7.45 and discounting it back 10 years at a rate of 40 % yields a rational market value of $0.26. The calculation is $7.45 / (1.40^{10}). An alternative approach is to discount each period utility value and use the weighted average by applying larger weights to periods that are closer. The Satis Report argues that discounting isn't required for the TAM analysis[63]; however, most reports incorporate a discount rate. Chris Burniske uses rates between 30 % and 40 %.[64] The 2015 Wedbush Securities report uses a discount rate of 40 %.[65] In this report, we apply 30 %; however, additional research on the property discount rate of each coin to reflect distinct risk profiles is needed.

Winner Take All

Since this analysis is investigating five coins instead of just one, an **additional assumption is required.**

Many of the coins in the top five are competing with each other to become global ledgers for storing and trading digital assets. Therefore, one assumption to make is whether or not there will be a **winner take all** or **an oligopoly of cryptoassets for each main use case**. Several studies assume each protocol is an isolated economy to simplify calculations. However, the cryptocurrency market is one of the most competitive markets in the world. The cryptocurrency market has less regulatory barriers to entry and switching costs between cryptocurrencies are low. This assumption is relevant for adoption rate, scenario probability, and discount rate.

"It's the single best hedge against traditional financial infrastructure. Whether you support the fiscal and monetary policy or not, it doesn't matter. This is the schmuck insurance you have under your mattress."

Chamath Palihapitiya
Founder and CEO
Social Capital
2019

One could argue that the winning protocols of these digital resources will become global standards, and global standards are typically "winner takes most" scenarios. **Therefore, this report makes the following assumptions:**

- Bitcoin will beat Ethereum, Bitcoin Cash, and Litecoin in the currency coin group.
    - This is reflected in the "discount rate". Bitcoin is **assumed** to have a discount rate of 30 %, while Bitcoin Cash and Litecoin are **assumed** to have a discount rate of 50 %.
- Ethereum will beat Stellar in the utility coin group.

—

[63] Sherwin Dowlat and Michael Hodapp, "Cryptoasset Market Coverage Initiation: Valuation August 30, 2018," *SatisGroup*, 2018. Retrieved from https://research.bloomberg.com/pub/res/d37g1Q1hEhBkiRCu_ruMdMsbc0A

[64] Burniske and White, 2017.

[65] Gil Luria and Aaron Turner, *Bitcoin Investment Trust (GBTC)*, Wedbush Securities, July 9, 2015. Retrieved from https://www.scribd.com/doc/271095696/GBTC-Initiation-2015-07-09?campaign=SkimbitLtd&ad_group=100652X1574425Xb33e774d2adb3cb7ff048b89c1f5ae1e&keyword=660149026&source=hp_affiliate&medium=affiliate

- This is reflected in the “discount rate.” Ethereum is **assumed** to have a discount rate of 30 %. Stellar is **assumed** to have a discount rate of 50 %.

These assumptions are based on current technology and regulatory strengths that Bitcoin and Ethereum have. The hash rate dedicated to Bitcoin is magnitudes larger than any other cryptocurrency. Finally, Bitcoin’s decentralized nature has prompted SEC officials to unofficially consider Bitcoin to not be a security. This provides some regulatory protection for Bitcoin that may hinder new blockchain start-ups. However, Bitcoin Cash and Litecoin also have advantages. Both coins offer faster confirmation times and lower transaction fees compared to Bitcoin, and they are sufficiently decentralized with large networks of investors and Bitcoin Cash has many developers working on protocol upgrades. Instead of a winner-takes-all during the next ten years, an oligopoly of payment coins is likely to remain in place. Plus, several investors use naïve 1/n strategies to invest in cryptocurrencies and, therefore, invest equally in the top currency coins in order to reduce risk and capture the market.

Valuation Results

Looking into all the variables and addressable markets, we have come up with a utility price estimate for each of the examined cryptocurrencies. It is worth nothing that each of those estimates is done on a non-discounted basis and with either bearish or moderate market penetration assumptions.

Table 4: Equation of Exchange Forecast of Crypto Asset Prices

Non discounted utility price predictions					
	Current	2020	2025	2030	2033
Bitcoin	$9,263	$19,044	$341,000	$397,727	$395,270
Ethereum	$208	$331	$3,549	$3,644	$3,441
Litecoin	$44	$83	$1,216	$2,252	$2,299
Bitcoin Cash	$235	$414	$6,690	$13,016	$12,941
Stellar	$0.07	$0.09	$2.40	$7.81	$8.26

Source: CryptoResearch.Report

It is worth noting that, as of the time of writing this report, the total crypto market cap (all currencies, not just the 5 listed above) sits at $256 billion. In the meantime, the TAM of all the potential markets as discussed above, is in excess of $188 trillion, which makes the current crypto penetration across those markets 0.136 %.

As seen by the charts above, we believe that Bitcoin is still at the very start of its adoption curve. The price of $7,200 at the end of 2019 suggests that Bitcoin has penetrated less than 0.44 % of its total addressable markets. If this penetration manages to reach 10 %, its non-discounted utility price should reach nearly $400,000.

“We should be happier to have a job than to have our savings protected.”

Christine Lagarde
President of the European
Central Bank and former Head
of the IMF
2019

Critique of the Equation of Exchange Model

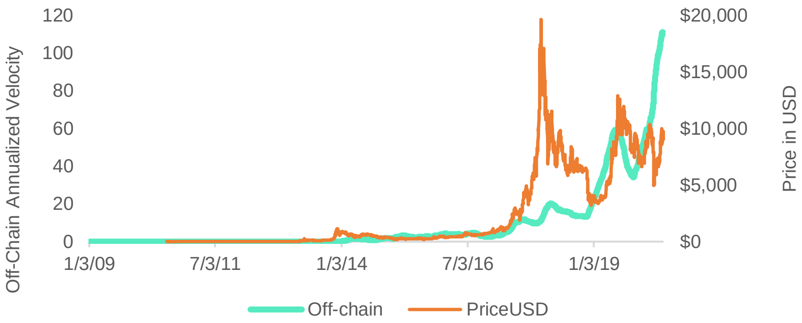
The theory of velocity presented in the equation of exchange model that is commonly applied to crypto assets **would question the business model of utility coins and payment coins that have no incentives to hoard via staking and are expected to have a high velocity as people spend the coins frequently.** In support of this theory and Buterin and Samani's analysis, Coin Metrics' State of the Network #37 showed how Bitcoin's on-chain velocity has been steadily decreasing and the price has been going up.

"The dollars that you work hard for are always buying less and less, yet the government tells you there's 'not enough inflation'. The Fed is a government-created monopoly that counterfeits dollars by the trillions, and you're supposed to believe that this is capitalism."

Ron Paul
Former US congressman and
Presidential candidate

However, we also calculated Bitcoin's off-chain transaction velocity and found the opposite pattern. We found that Bitcoin's price and Bitcoin's exchange activity both went up at the same time over the past few years. On-chain velocity is the velocity generated solely by transactions on the blockchain, whereas off-chain velocity is the velocity generated by trading activities on cryptocurrency exchanges.

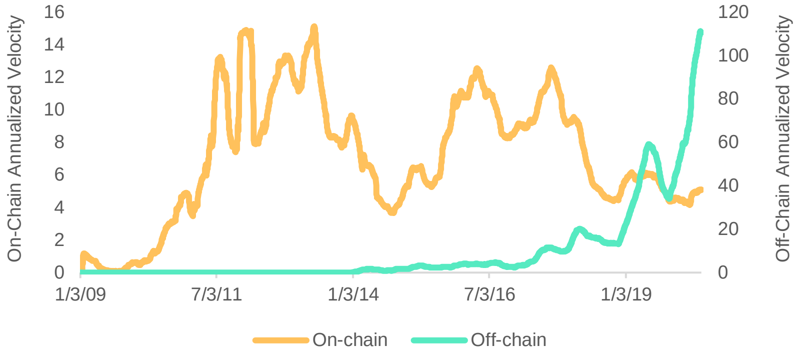
Figure 13: Bitcoin's Off-Chain Velocity is Positively Correlated with Bitcoin Price



Source: Coinmetrics.io, CryptoResearch.Report

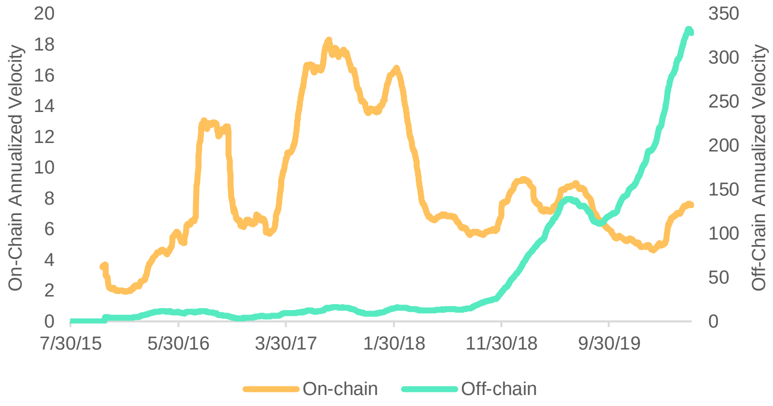
We wanted to check these results with other coins, so we calculated on-chain and off-chain velocity for Ethereum, Bitcoin Cash, Litecoin, and Stellar in order to see if coins were trading hands more frequently on-chain (inter-exchange and off-exchange) or off-chain (intra-exchange). We found that for almost all coins, on-chain velocity is decreasing, while off-chain velocity is increasing. We interpret this to mean that growth in the number of speculative transactions on exchanges is faster than growth of utility transactions to buy goods and services.

Figure 14: 90-Day Moving Average Bitcoin On-Chain and Off-Chain Velocity



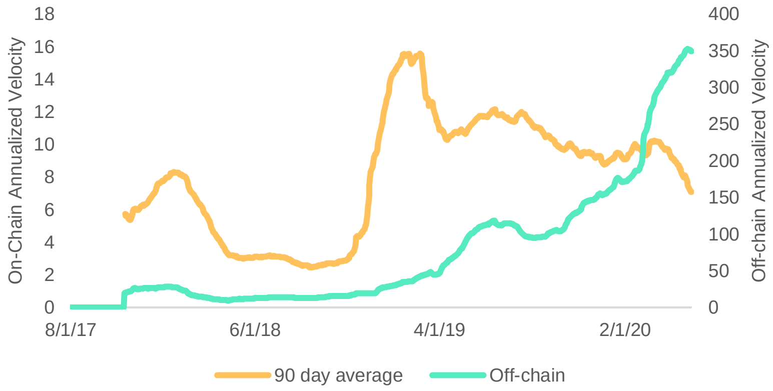
Source: Coinmetrics.io, CryptoResearch.Report

Figure 15: 90-Day Moving Average Ethereum On-Chain and Off-Chain Velocity



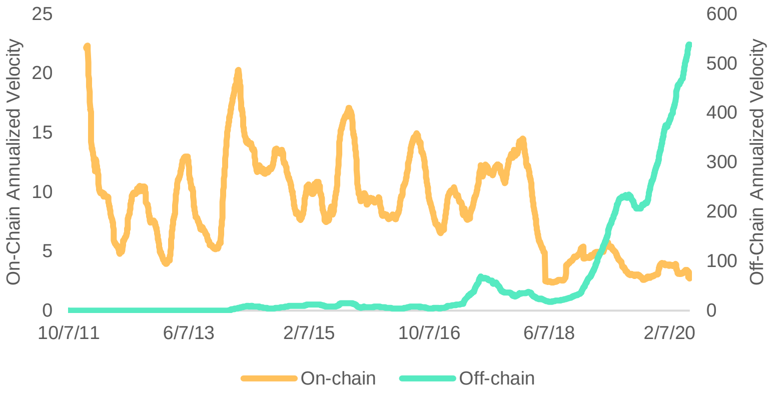
Source: Coinmetrics.io, CryptoResearch.Report

Figure 16: 90-Day Moving Average Bitcoin Cash On-Chain and Off-Chain Velocity



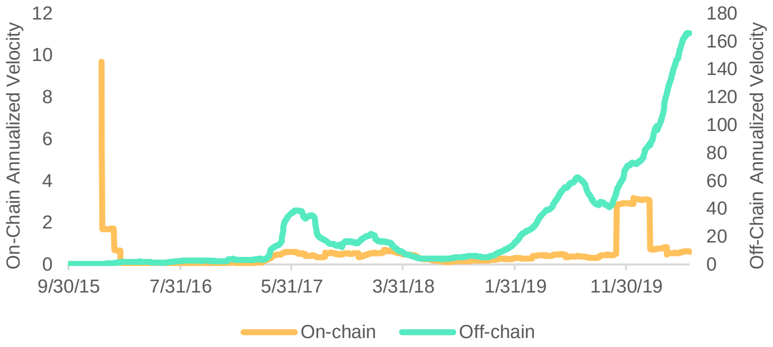
Source: Coinmetrics.io, CryptoResearch.Report

Figure 17: 90-Day Moving Average Litecoin On-Chain and Off-Chain Velocity



Source: Coinmetrics.io, CryptoResearch.Report

Figure 18: 90-Day Moving Average Stellar On-Chain and Off-Chain Velocity



Source: Coinmetrics.io, CryptoResearch.Report

"The key value proposition of blockchain is minimizing the cost of trust down to almost zero. The cost of trust is roughly 35 % of global GDP or $28 trillion dollars. Therefore, the target addressable market for blockchain is $28 trillion dollars."

Lasse Clausen
Founder 1kx
May 2020

It is interesting to observe similar trends in velocity among almost all of the cryptocurrencies. Higher velocities before the cryptocurrency matures and more stable and lower velocities later on. Stellar seems to be an exception to this rule (mainly looking at the huge jump in velocity late 2019), but as we know, Stellar's Coinbase is heavily centralized and it is likely that this is a foundation transaction distorting the numbers.

It is also worth noting the huge jump in off-chain velocities among all cryptocurrencies in 2019-2020 coinciding with the drop in on-chain velocity. This suggests that traders who operate exclusively on exchanges and trade with high volumes are becoming the dominant force in the crypto asset market instead of long-term holders.

The results that we found do contradict Buterin and Samani's theory because we found that velocity is increasing and the price is going up, even though their model says the price should be going down. Scott Locklin's critic of their work may hold the answer. As Locklin points out, applying Fisher's MV = PT equation of exchange directly to crypto assets doesn't work because of two main reasons:

> *"The inverse of (average) token velocity is not average holding time. For example, let us postulate a money supply of 10 tokens in an economy with a velocity of 10 times per day. If 9 of the tokens are traded once every 1000 days, and one of the tokens 99.991 times a day, this gives mean token velocity 10 times per day. However, the average holding time for a coin in this ecosystem is 900.001 days, not 1/10 day per transaction."*

> *"Similarly, while Fisher's equation of exchange is an equilibrium model (which I suppose could be called "steady state"), it does not depend on the number of users."*

Locklin does a few transformations to the equation and argues that user adoption really does matter for the price of a coin. As more people come to the network and demand the coin, the price goes up. Locklin's critique is straight forward. If more people demand Bitcoin and Ethereum for buying coffees or for speculating, the result is similar. Either way, people are trading economic resources for cryptocurrencies and bidding up their prices. In defense of Buterin and Samani, speculation on financial assets is normally left out of GDP metrics. Foreign exchange volume isn't included in GDP, for example, and therefore, analyzing the velocity of crypto asset speculation may not be appropriate.

Final Word. Vitalik's token economic concepts of velocity and velocity sinks that encourage hoarding are important; however, the analysis is static and doesn't consider new user adoption and growing demand. If cryptocurrencies gain adoption for long-term hoarding purposes or for short-term spending on speculation or coffees, the price of crypto assets will go up. **High velocity on-chain and low velocity off-chain suggests that crypto assets are becoming increasingly used for speculation and not for store of value.**

Storing Bitcoin
the safe and easy way
coinfinity CARD WALLET
Your Address 1AHx7RRjeMWFUZukB hypbebe7ppAQAhxSy
www.chainlock.com
1000019547236804S826
OESTERREICHISCHE STAATSDRUCKEREI
OSD
With the Card Wallet by Coinfinity and
the Austrian State Printing House
www.cardwallet.com

Image: Renaissance cassette, courtesy of Schell Collection

Tether or Not to Tether

"In April 2019, Bitfinex's general counsel Stuart Hoegner admitted in court documents that Tether was only 74% backed by "cash and cash equivalents," lending credence to the theory that Tethers are increasingly being minted out of thin air. Bitfinex is being investigated by the office of the New York Attorney General. He made that claim when there was only $2.8 billion worth of Tether in circulation. Now, there are three times that amount."

Amy Castor

Key Takeaways

- **Originally, the USD-pegged Tether stablecoin was thought to be an on-ramp into Bitcoin. However, today that is only a small use case. Instead, Tether is used as a settlement vehicle for trading strategies, arbitraging between cryptocurrency exchanges, and for circumventing capital controls. This trend can be referred to as the dollarization of public blockchains.**

- **The trend of "hyper-crypto dollarization" is expected to increase the demand for Tether and other fiat-pegged stablecoins. Since January, $4.7 billion USD worth of Tethers have been created. Now, there are nearly $9 billion USD worth of Tethers in circulation.**

- **Tether isn't fully backed, and there is evidence that unbacked Tethers support artificial price movements in Bitcoin. Bitfinex loans to miners may also be artificially supporting the price of Bitcoin.**

Pascal Hügli

Pascal Hügli is the Chief Research Officer at Schlossberg&Co, a Swiss Asset Manager focused on protecting its clients' wealth from unprecedented and increasing monetary socialism around the globe. Schlossberg&Co has integrated Bitcoin in its portfolio allocation since 2013. They have been a close observer of the Bitcoin market for years.

In September 2018, US Tether (USDT) reached a temporary high in market capitalization of just over $ 2.8 billion. By mid-November, market capitalization then dropped to below $2 billion. This correction was followed by a fall in the price of Bitcoin to almost $ 3,000 per Bitcoin shortly before the end of the year.

"New York does not like $USDT as it competes with their upcoming $22 trillion IEO to pay off US debt."

Simon Dixon

Today, the price of Bitcoin is once again higher, and the market capitalization of Tether has also risen continuously since then to over $8 billion. Not only has the outstanding amount of Tether hardly ever fallen, not even temporarily, but the issuance rate of new Tether has also shown sudden, erratic increases since the beginning of this year; a total of three in number, each greater than the previous one.

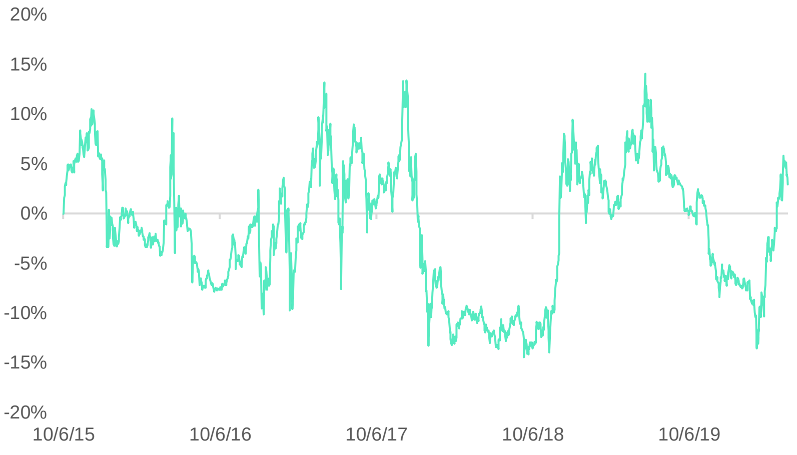
As one of the big black boxes of the crypto world, many secrets and speculations surround Tether, further fueled by these abrupt growth spurts in market capitalization. Aside from the rumors and speculation, USDT is still regarded as a so-called on-ramp for investors to easily and quickly invest in Bitcoin.

"Tether has a real-world use case: Chinese importers of cheap goods in Russia use it to send millions home daily."

Anna Baydakova

It's a fact that Tether has been used as a gateway into the Bitcoin world. However, if Tether was an on- and off-ramp, then the market capitalization of Tether would in theory have to fall every now and then, because USDT would have to be burnt at intervals by the Tether Treasury when holders cash back out into fiat or go into Bitcoin. Since, the market capitalization of Tether has risen steadily over the past 18 months without significantly falling even once, this suggests that Tether is essentially not acting as both on-and off-ramps.

Figure 19: Negative Correlation Between Change in Tether Supply and Bitcoin Price



Source: Coinmetrics.io, CryptoResearch.Report

The argument against this is that the demand for Bitcoin is very volatile. During the last two years, there have been repeated periods when Bitcoin's price fell, while Tether's market cap remained the same or even went up. If USDT were used primarily as an on- and off-ramp, its positive correlation with Bitcoin would have to be much stronger. This isn't the case, especially since there are even indications that the correlation is negative. This leads to the conclusion that something else more serious is afoot.

Alternative Explanation Sought

For example, some market observers suspect that USDT is being created without collateralization. So, Tether would be created specifically by Tether Limited and its parent company BitFinex and held in fractional reserves in order to drive up the Bitcoin price, so the argument goes.

> *"The coming crash of Tether/USDT will cause the crash of Bitcoin as the former was used to manipulate the latter."*
>
> Nouriel Roubini

This way the critics argue that BitFinex is trying to generate excitement among retail investors, which would then turn into a hysteria of FOMO leading up to a new Bitcoin bull run. This is how some analysts explain the fact that on May 14, a few days after the Bitcoin-halving, the Tether market capitalization suddenly rose from just over $6 billion to almost $9 billion.

What sounds like a conspiracy theory to some, others consider to be a fact: After all, the two companies BitFinex and Tether Limited would have strong incentives to run such games. As the New York Secretary of Justice pointed out, only about 70 % of outstanding Tether is secured by cash and cash equivalents.[66] This hole when it comes to collateralization, according to the skeptics of Tether, could of course be filled up step by step if Bitcoin stabilizes at a higher level supported by private investors. The collateralization that BitFinex partly holds in Bitcoin as well would then have more value that could be sold for dollars and improve the reserve ratio.

Tether as a Savior

Another hypothesis to explain the abrupt rise in Tether market capitalization on May 14 is that BitFinex is going out of their way to secure the survival of certain miners with USDT loans. Bitcoin miners today operate highly specialized ASIC processors, of which two different ones are currently in use: the Antminer S9 and the Antminer S17.

The major difference between these two mining hardware devices is mainly their different efficiency. Although the S17 has about 50 % higher power consumption than the S9, a miner using the former achieves a 300 % higher hash rate. As a result of this higher efficiency, Antminer S17 accounts for a much higher share of Bitcoin mining, at just over 61 %. The use of the S9 type is just over 38 %.

And it is precisely these miners, so the argument goes, that are dependent on support, as they have become unprofitable after the halving. However, in order to not have to empty out their Bitcoin treasuries and generate downward pressure on

—

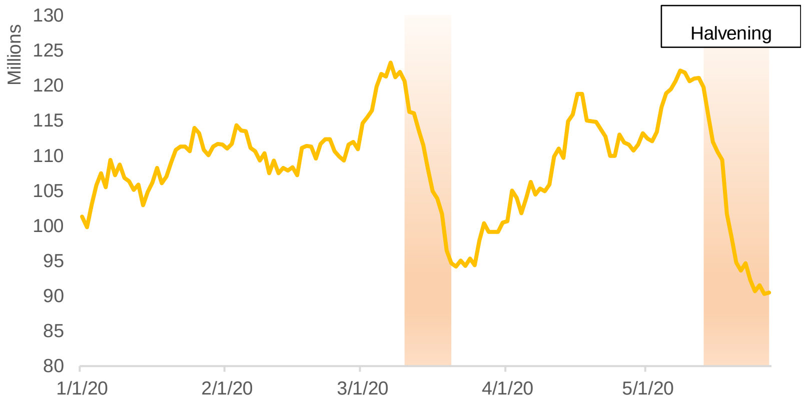
[66] William Suberg, "Fractional Reserve Stablecoin Tether Only 74% Backed by Fiat Currency, Say Lawyers," *Cointelegraph*, April 30, 2019. Retrieved from https://cointelegraph.com/news/fractional-reserve-stablecoin-tether-only-74-backed-by-fiat-currency-say-lawyers

the Bitcoin price, these miners could be buying time with USDT loans – time to renew their hardware equipment that had become unprofitable.

Speculations and theories of this kind always sound tempting. It is also difficult to refute them completely. But it is just as difficult to provide definitive evidence. In the end, it is argument against argument.

What stands against the BitFinex miner thesis is the fact that miners today are farsighted, long-term invested players. As rational players in a very competitive, highly innovative and little-regulated field, it can be assumed that precisely those miners with older Antminer S9 have taken precautions. They could have moved to a location with much lower electricity costs so that their Antminer S9s are still profitable even after the block reward was halved.

Figure 20: Miner Hash Rate Has Dropped



Source: Blockchain.com, CryptoResearch.Report

Again, there is friction and uncertainty in the real world. Not knowing the unpredictable could have caused miners to miscalculate long-term contracts with electricity providers, which is why they cannot easily relocate mining farms overnight. It is and remains a fact: We can only speculate about what is really the case.

Demand for Tether, not Bitcoin

However, the continuous rise in Tether's market capitalization doesn't necessarily have to be the result of increased USDT demand as a Bitcoin on-ramp. As is becoming increasingly apparent: It seems more likely that Tether in and of itself is seeing increasing demand. As a kind of settlement vehicle for arbitrageurs between crypto trading exchanges, stablecoins are being used extensively.

“Allow me to present the only piece of news in crypto that's worth your while. It's about what's really backing Tether's stablecoin. It's not dollars. It's not Bitcoin either – not entirely, at least. It's loans to miners, backed by Bitcoin.”

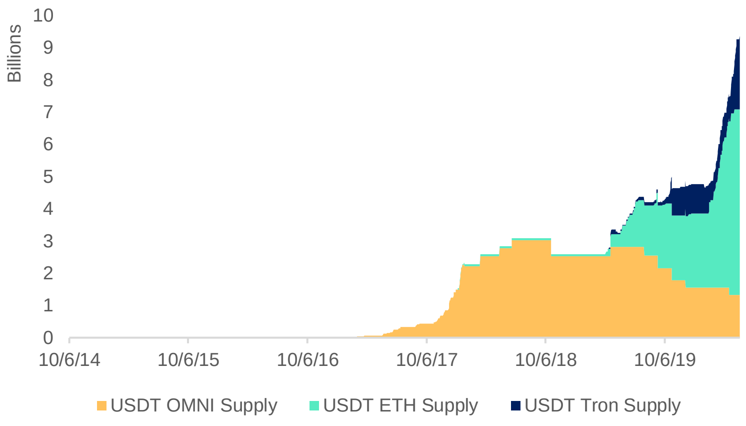
Trolly McTrollface

Over the past few years, the trading exchanges for cryptoassets have become more professional, which has also made the arbitrage business more professional. Arbitrage is being conducted with ever-larger sums of money – a stable settlement currency such as the USDT seems predestined for this. Tether is also used for arbitrage purposes by individual traders. If the Bitcoin price falls, these players switch their funds into the stablecoin in order to minimize losses and buy back in at a lower price.

Having a stable currency that is denominated in dollars lets you handle your books with more ease. So, as a matter of fact, there has been a tetherification of the crypto exchange industry. With exchanges, Bitcoin has been supplanted by Tether as the base currency. Several exchanges like Binance, OKEx, or Huobi have even launched Tether-denominated futures products.

Over the last couple of months, Tether supply on exchanges has been growing significantly. It’s not only exchanges that make use of Tether’s stable characteristics, USDT is also used for arbitrage purposes by individual traders. If the Bitcoin price falls, these players switch their funds into the stablecoin in order to minimize losses and buy back in at a lower price.

Figure 21: During the Last Two Years, Tether Supply on Exchanges has Grown from the Millions into the Billions.



Source: Coinmetrics.io, CryptoResearch.Report

But not only arbitrage trading between crypto exchanges but also the moving of funds between individual countries is facilitated by a stablecoin like Tether. It is well known that one of the first major uses for Bitcoin was to circumvent capital controls. The first major price increase at the end of 2013 is said to be mainly due to Chinese people moving their savings out of the country.

However, the volatility of Bitcoin has always been a thorn in the side of capital refugees. And indeed, little seems to be gained by taking your capital out of the country only to see it be eaten away by Bitcoin’s volatility during the trade. With the launch of Tether, new opportunities for capital flight have suddenly opened up. It is therefore understandable that USDT has been discovered as a killer application. Tether is used as a cross-border crypto dollar, especially by Chinese traders and business people exporting to Russia.

Everyone Wants US Dollars

There is a reason why Chinese businessmen hold a dollar-denominated stablecoin. The US dollar is currently the global reserve, reserve and trading currency. All major commodities are settled in US dollar, which is why it now accounts for 4.7 times global imports and 3.1 times global exports. For non-US companies it therefore often makes more sense to invoice in US dollars.

But it's not only invoices that are issued and settled in US dollars. Companies around the world have nearly 60 trillion US dollar-denominated debts. This creates an ongoing demand for US dollars to service the debts of emerging and developing countries, which will not leave their currencies unaffected. The latter currencies are likely to depreciate against the dollar, which is bound to result in increased capital controls.

The most recent example is Lebanon. Local banks there are currently in the middle of a fight against capital flight, which is why restrictions on foreign currency withdrawals, especially for US dollars, have been tightened. Tighter controls on capital movements are likely to increase not only in underdeveloped countries, but the eurozone could also become more restrictive in this regard in the foreseeable future.

"Crypto is an insanely powerful tailwind for the US Dollar, many people haven't understood this yet. Far from being crushed by bitcoin or cryptocurrency, the dollar will be its primary beneficiary (assuming the MMTers don't obliterate it first)."

Nic Carter

In contrast to the Japanese yen and the Swiss franc, which as currencies still enjoy the character of a safe haven, demand for the euro correlates mainly with the demand for exports from the eurozone. The sooner the euro liquidity created by the European Central Bank's ultra-expensive monetary policy exceeds international demand for the euro relative to the dollar, the faster the former will lose value. Tighter capital controls to support the euro would primarily affect European banks. They still carry large US dollar positions on their balance sheets. Without having sufficient US dollar deposits, they need to have open channels to access US dollars at all times. Tighter capital movement controls would certainly be an obstacle in that regard.

The use of crypto dollars, especially Tether, might serve as a helping and welcoming solution. Not only can potential capital controls be more easily be circumvented, but transactions using crypto dollars are generally easier to initiate and process than those using the traditional financial infrastructure.

The demand for Tether should, therefore, already satisfy several real needs today. Apart from the use cases described above, particularly the increasing demand for dollars in a world of increasing capital controls will accelerate a sort of "hyper crypto dollarization." Ironically, what we have been witnessing is the dollarization of public blockchains, which is bound to grow in next couple of years.

bitpanda pro
Market
BTCEUR
LIMIT ORDER
Market
Limit
Stop
BUY
SELL
Available
Locked
0.00 EUR
0.00 EUR
Limit Price
0.00
EUR
Amount
0.00000000
BTC
Fee (0.1%)
Total to receive
BUY BTC
DEPOSIT
WITHDRAW
ORDER BOOK
Total
Amount
Price
Book
History
LAST MATCHED PRICE
CURRENT SPREAD
COMPILE
7809.43
1.00
None
MY ORDERS
BTCEUR CHART
15M
Volume
LOG IN
SIGN UP
Open
Filled

Exclusive Interview with the MWC Team

Key Takeaways

- MimbleWimbleCoin (MWC) is a new privacy coin. Other privacy coins include Dash, Monero, Zcash, Zcoin, Beam, and Grin. MimbleWimbleCoin is more scalable than Monero but less private.

- MimbleWimbleCoin forked from Grin in November 2019 and hit a low of $0.25 per coin with less than a $2 million market cap in early December. However, since December, the market cap of MWC has grown 6,100 %. The MWC market cap is currently around $125 million, making it the 13th largest proof-of-work coin behind Bitcoin Gold and Decred.

- Unlike Grin, MWC has a hard cap on total supply of 20 million. When looking at the number of coins created per day, MWC, Monero, Bitcoin, and Bitcoin Cash are the lowest. In terms of the US dollar value of the number of coins created per day, MWC is still the lowest, followed by Monero and Dash. Finally, the US dollar value of new coins created per year in relation to their US dollar market capitalization is also the lowest for MWC with 1.2 % followed by Bitcoin with 1.7 %, Monero with 2.8 %, Litecoin with 6.1 %, Dash with 8.4 %, and Zcash with an astonishing 35.1 %(!).

MimbleWimbleCoin Team

We want to sincerely thank the MWC Team for this interview. The founders wish to remain anonymous; however, they agreed to do an exclusive interview with the *Crypto Research Report* on the topic of online privacy in the digital age. For more information about MWC, please visit mwc.mw.

One of the main reasons for Bitcoin's success and popularity, is its **trustless design.** Instead of trusting humans with clearance and settlement of financial transactions, Bitcoiners opt to trust software protocols. What was particularly revolutionary about Bitcoin was how the network used proof-of-work to stop double-spending attacks and how anyone around the world could validate new transactions and store a copy of the database's history. Imagine if Credit Suisse or Bank of America not only allowed anyone to see their entire database of transactions, but also allowed anyone to vote on the validity of new transactions.

However, over time becoming a validating node on the Bitcoin network became increasingly expensive and exclusive because of the size of the Bitcoin blockchain. Without heavy investments in computing power, relaying new transactions and storing a copy of the database is impossible. A newcomer to the Bitcoin blockchain needs to spend approximately one week downloading the 277-gigabyte database of existing transactions in order to participate in the validation of new transactions. However, the "blockchain" associated with Bitcoin is only one type of distributed ledger database architecture. There are also other kinds of distributed ledger databases, such as IOTA's directed acyclic graphs that we explored in the June 2018 edition of the *Crypto Research Report*. This article discusses a different type of distributed ledger architecture called MimbleWimble that has specific advantages and disadvantages compared to Bitcoin's blockchain.

"In economics, fungibility is the property of a good or a commodity whose individual units are essentially interchangeable, and each of its parts is indistinguishable from another part."

MimbleWimbleCoin

What Are Privacy Coins?

In a recent report by the European Union Blockchain Observatory and Forum called, *Legal and Regulatory Framework of Blockchains and Smart Contracts*, the authors explicitly state that regulators should use blockchain explorers to track transactions and to find out personal information about the senders and receivers of Bitcoin transactions.[67]

> *"While not always identifiable at the moment of the transaction, given enough time and effort, many parties to a transaction can be unmasked. Therefore, at this point there is no question of total impunity for blockchain actors.*
>
> *"Thirdly, however, it cannot be denied that some privacy-focused blockchains, for example Monero or ZCash, can provide bad actors with effective tools for true anonymity. It is important to note that in practice anonymous transactions are currently not widely used: Bitcoin and Ethereum, the most popular platforms, do not support anonymity.*
>
> *"Governments also try to discourage the use of anonymization techniques in blockchain networks by, for example, imposing AML rules, thereby policing the gateway between the worlds of cryptocurrencies and fiat money (see also next section). That said, while anonymisation does not*

—

[67] *Legal and Regulatory Framework of Blockchains and Smart Contracts* [Thematic Report], The European Union Blockchain Observatory and Forum, September 27, 2019. Retrieved from https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf

pose a significant enforcement risk on public permissionless blockchains at the moment, should the use of anonymous blockchains spread significantly, it could become a problem.

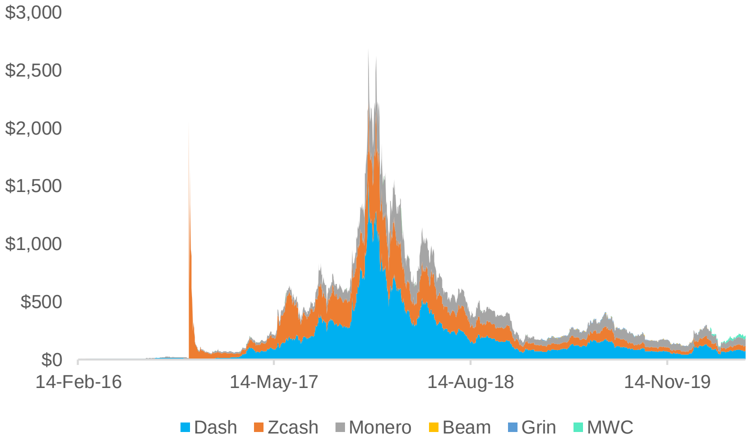
“It seems that providing states with identification tools (potentially under the control of courts or through the private sector on a payment basis) should be a minimum condition necessary for a state’s ability to enforce the responsibility and thus to ensure the impact of the law on human behaviour in the blockchain space.”

“A civilized society involves total transparency for institutions and full privacy for individuals.”

Marco Ricca

Many market participants consider fungibility a characteristic of good money. Bitcoin lacks fungibility, which means bitcoins can be traced to their initial transaction when they were mined. Privacy coins are coins that attempt to improve upon Bitcoin’s privacy by hiding the amounts that are traded and the wallet addresses involved in the transaction. Privacy coins use technologies such as coin mixing and confidential transactions. The largest privacy coins include Dash, Monero, Zcash, Grin, Beam, and MimbleWimbleCoin. In 2014, Dash was launched, and it was the first privacy coin on the market. Dash gives each user the option to make each transaction private or not. Dash’s technology uses coin mixing to obscure information about the sending and receiving addresses, and only 2 % of Dash transactions use Dash’s privacy option. The rest of Dash’s transactions are just as traceable as Bitcoin transactions. A few months after Dash came out, a new privacy coin called Monero was released to the market. Unlike Dash, every Monero transaction is private. Blockchain explorers don’t see the amounts being sent in Monero transactions. Monero introduced ring confidential signatures, which provide very strong privacy for Monero users. A few years later, Zcash came out in 2016, and then more recently, in 2018, the MimbleWimble base layer coins Beam and then Grin came out.

Figure 22: Performance of Privacy Coins, 2016–2020



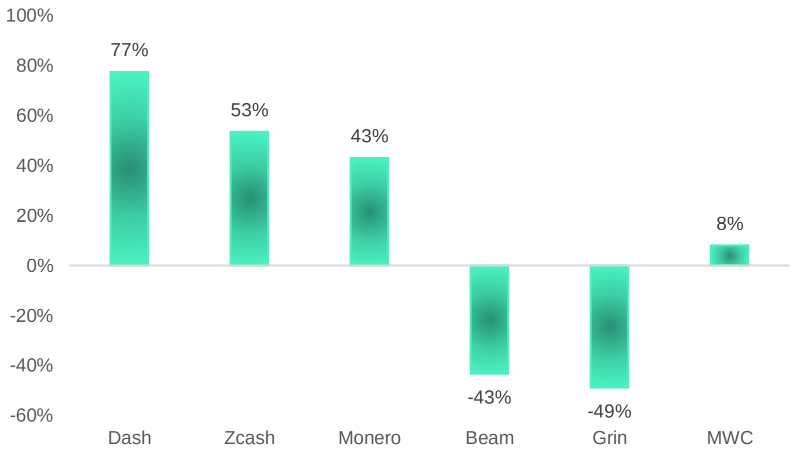
Source: Coinmarketcap.com, CryptoResearch.Report

"In October, eight months after discovery, the bug was surreptitiously patched during a planned network upgrade. Although Zcash have stated that they do not believe the bug was exploited, they cannot be certain."

The Bitcoinist

However, the developers of privacy coins face design choices that each have unique tradeoffs. For example, Monero is more private than Dash because the transaction amount is hidden, but Monero is less scalable because it takes more resources to run a full node, which makes it less censorship-resistant. Another tradeoff is between being able to prove a coin is scarce and having privacy features. Blockchains that obscure the amounts being transacted have difficulty determining the total amount of coins in circulation. In a recent interview on the Academic Blockchain Podcast with the Chief Technology Officer of Ledger, Demelza Hays discussed Zcash's "inflation bug." Zcash's inflation bug makes it impossible for anyone to actually calculate the total amount of coins in existence. This means that there could be an infinite amount of coins in existence, which goes against one of the pillars of a good money in the digital age, namely, scarcity. However, the MimbleWimble protocol uses mathematical proofs involving excess values of intermediate transactions to prove that all debits and credits in the ledger sum to zero.

Figure 23: Year-to-Date Return of Privacy Coins



Source: Coinmarketcap.com, CryptoResearch.Report

But what is MimbleWimble? In 2016, an anonymous person released the MimbleWimble protocol to increase Bitcoin's **scalability and privacy**. MimbleWimble is a way to sign and validate transactions without needing to validate each historical transaction and to include the inputs of a transaction into a new transaction's hash. This drastically reduces the size of the blockchain. Proponents originally proposed MimbleWimble as a sidechain or soft fork to Bitcoin; however, the current implementations of the MimbleWimble protocol are by new cryptocurrencies that created new blockchains including Grin, Beam, and MWC, that elegantly apply MimbleWimble in the base layer.

During 2019 and into 2020, much of the MimbleWimble hype had died down along with the market caps of Grin, currently about $19 million, and Beam,

Confidential Transactions in a Nutshell

In Bitcoin, when Person A sends a transaction to Person B, an unspent transaction output is created. When Person B wants to send a transaction to Person C, then person B uses that unspent transaction output as the input into the transaction.

A → B → C

In MimbleWimbleCoin, the blockchain summarizes these two transactions into one transaction by skipping the intermediary transaction from A to B and from B to C.

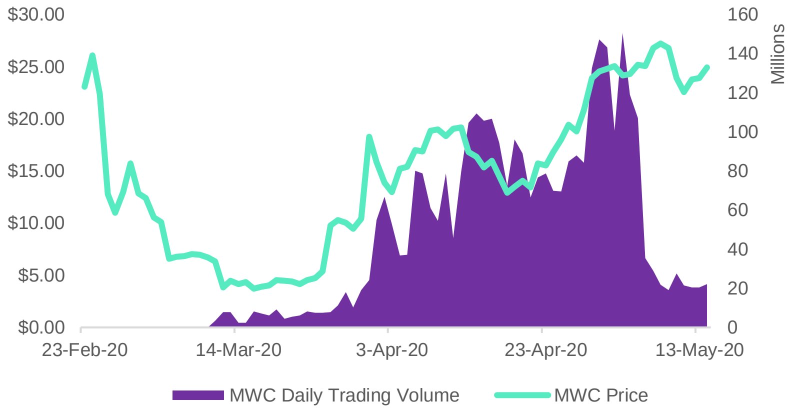
A → C

Although the entire transaction isn't stored, there is a small artifact of transaction B that is stored on the MimbleWimbleCoin blockchain. This is referred to as the "Excess." By removing B, you improve scalability and privacy at the same time.

currently about $16 million. MimbleWimbleCoin (MWC) forked from Grin in November 2019 and hit a low of $0.25 per coin with less than a $2 million market cap in early December. **However, since December, the market cap of MWC has grown 6,100 %.** The MWC market cap is currently around $125 million and has been consolidating over $100 million for most of the past two months. By market cap, MWC is currently the 3rd largest privacy coin behind Monero and Zcash and the 13th largest proof-of-work coin behind Bitcoin Gold and Decred. MWC is currently traded on Hotbit, Bitforex, Whitebit, Trade Ogre, and Toktok.

The two ideas that form the basis for MimbleWimble stem from the Blockstream co-founder Gregory Maxwell's work on "Confidential Transactions" and "CoinJoin." Confidential transactions use encryption so the public blockchain doesn't show the amount of coins being sent or received in a transaction. For example, in Bitcoin, anyone can see the amount of Bitcoin that is sent in each transaction. However, in MWC, the public cannot see how much is being sent even though verification can be done of adherence of the transaction to the consensus rules to, for example, prevent double-spending and enforcing the total number of coins. The second innovation that the MimbleWimble protocol uses is CoinJoin. This means that multiple transactions in the network are merged into one transaction so that blockchain forensics cannot discern the real sender and real receiver of a specific transaction.

Figure 24: The Newest Privacy Coin on the Market: MimbleWimbleCoin



Source: Coinmarketcap.com, CryptoResearch.Report

However, there are disadvantages of the MimbleWimble protocol as well. For example, the MimbleWimble protocol doesn't allow extensive scripting. Fortunately, there has been significant research done since then, and with MimbleWimble these types of scripts and applications are possible: Multi-signature transactions, time locks, atomic swaps, and hashed time-locked contracts which are the building block of payment channels and Lightning Network. Another large disadvantage of coins that use the MimbleWimble protocol including Grin, Beam, and MWC is that currently these blockchains aren't widely used. Until more people use these coins and more people send transactions, the benefit of privacy from their use may be limited.

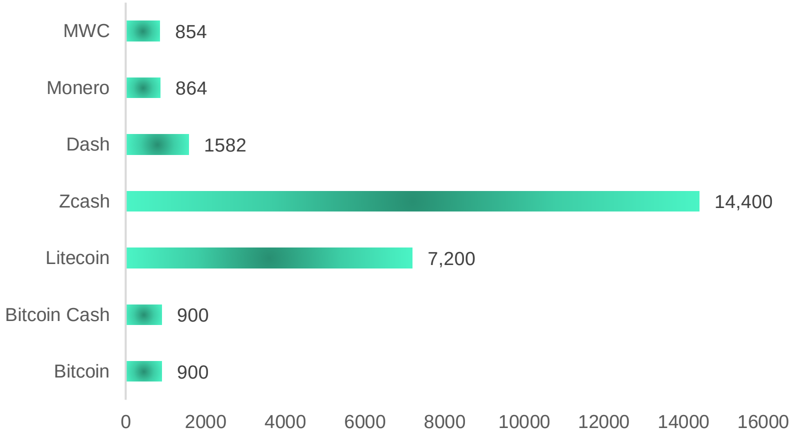
Where to Learn More on MimbleWimble

A good explanation for how MimbleWimble works can be found on the Smith & Crown website. Additionally, the original talk by Andrew Poelstra discussing how MimbleWimble validation occurs is on YouTube.

What Makes Good Money in the Digital Age

A good money in the digital age must be: (1) **recognizable**, (2) **scarce**, (3) **censorship resistant**, (4) **durable & indestructible**, (5) **extensible**, (6) **salable**, (7) **portable**, (8) **fungible**, (9) **private,** and (10) **divisible**.[68] However, most cryptocurrencies don't meet these criteria. In 2019, one of the most talked about coins was "Grin." However, investors quickly realized that Grin's high inflation rate and lack of a hard cap on supply was worse than the inflation in the US dollar. This made people wonder why they should buy Grin with US dollars if Grin is a worse store of value. The Grin emission rate is 1 Grin per second indefinitely. There will be 31,536,000 Grin created per year. Currently, there are approximately 43 million Grin. This results in a very low stock-to-flow ratio in the early years. During 2020, the stock-to-flow ratio of Grin is approximately 1.19x or approximately 43,000,000 Grin divided by the new production of 31,536,000. This acts as a transfer of wealth from holders to miners.

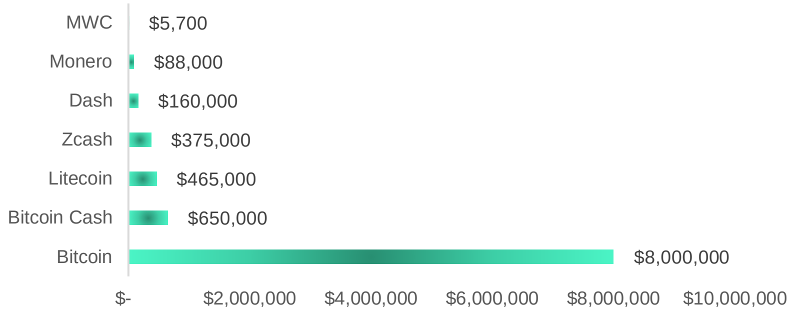
Figure 25: The Number of New Coins Created Per Day



Source: Coinmarketcap.com, various white papers, CryptoResearch.Report

[68] "What Makes Good Money in the Information Age?," *MWC*, 2020. Retrieved from https://www.mwc.mw/good-money

Figure 26: US Dollar Value of New Coins Created Per Day



Source: Coinmarketcap.com, various white papers, CryptoResearch.Report

As Saifedean Ammous explains, a low stock-to-flow ratio results in a transfer of value from holders of the asset to producers, while a high stock-to-flow ratio results in lower costs, measured in the asset itself, for holders. Before Grin launched, a MWC developer suggested there be an supply cap and emission rate change but was swiftly rejected by the Grin community which acted as a green light and was part of the inspiration for forking from Grin. After all, financial innovation is about trying many different approaches when bringing monetary products to market for consumers to enjoy. Every four years is a Bitcoin halving, and after the May 2020 halving the Bitcoin stock-to-flow ratio will be approximately 55. This will make it comparable to gold. MWC addressed the hard cap problem and low stock-to-flow ratio problem by placing a hard cap of 20,000,000 on the coin and then having a much slower emission rate Like Bitcoin, MWC uses a pure proof-of-work algorithm and has the highest stock-to-flow ratio of any base-layer MimbleWimble coin. By October 2020, MWC will have a stock-to-flow ratio almost equal to Bitcoin's. And by February 2021, it will have a significantly higher stock-to-flow ratio.

"Despite some common misconception, Bitcoin offers a very weak level of privacy."

Georg Fuchsbauer,
Michele Orrù, and Yannick Seurin

When looking at the number of coins created per day, MWC, Monero, Bitcoin, and Bitcoin Cash are the lowest. In terms of the US dollar value of the number of coins created per day, MWC is still the lowest, followed by Monero and Dash. Finally, the US dollar value of new coins created per year in relation to their US dollar market capitalization is also the lowest for MWC with 1.2 % followed by Bitcoin with 1.7 %, Monero with 2.8 %, Litecoin with 6.1 %, Dash with 8.4 %, and Zcash with an astonishing 35.1 %(!).

However, MWC has received some pushback from the cryptocurrency community because of how the initial stock was created. According to the whitepaper and protocol, half of the total supply of MWC were to be mined with proof of work mining, and the other half were created in the genesis block. From this initial stock of 10,000,000 MWC that was worthless when created, 2,000,000 MWC were immediately distributed to the developer team, 2,000,000 MWC were allocated to the HODL Program, and 6,000,000 MWC were airdropped to any Bitcoin holders who successfully registered over a three month period and claimed their MWC allocation during December 2019. Over 5.4 million MWC were successfully airdropped for free to Bitcoin holders and at the time had a total value less than $2 million. MWC primarily uses the C31 proof-of-work algorithm and MWC's new monthly emission from a pure proof of work algorithm is about $500k.

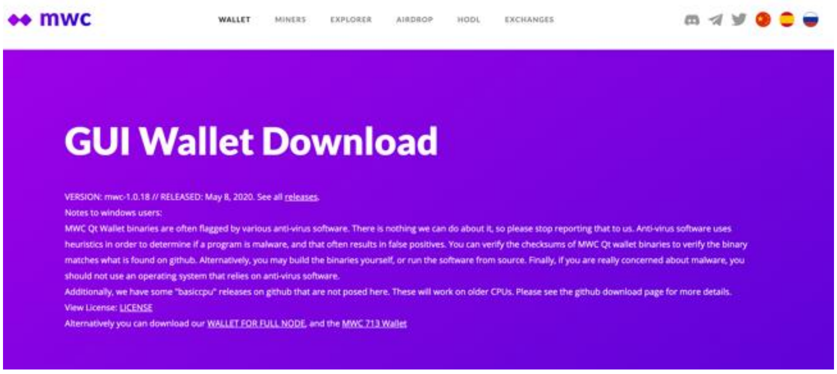
How To Do A MWC Transaction

"The most important thing Bitcoin is missing right now is privacy."

Edward Snowden

MWC was created to meet the demand for transferring money online with full privacy because Bitcoin transactions aren't that private or fungible.[69] MWC payments are slightly different to Bitcoin transactions, **the least of which being that there are only outputs and no addresses.** After all, everything is CoinJoined with Confidential Transactions and then the signatures are aggregated in the blocks.

To get started, you have to download a MimbleWimbleCoin wallet. To provide some context, the other privacy coin, Grin, relies mainly on command line interface tools, but they can be difficult for non-technical people to use. This is why MWC has created a very easy-to-use wallet that can be downloaded here: https://www.mwc.mw/downloads



GUI Wallet Download

VERSION: mwc-1.0.18 // RELEASED: May 8, 2020. See all releases.
Notes to windows users:
MWC Qt Wallet binaries are often flagged by various anti-virus software. There is nothing we can do about it, so please stop reporting that to us. Anti-virus software uses heuristics in order to determine if a program is malware, and that often results in false positives. You can verify the checksums of MWC Qt wallet binaries to verify the binary matches what is found on github. Alternatively, you may build the binaries yourself, or run the software from source. Finally, if you are really concerned about malware, you should not use an operating system that relies on anti-virus software.
Additionally, we have some "basiccpu" releases on github that are not posed here. These will work on older CPUs. Please see the github download page for more details.
View License: LICENSE
Alternatively you can download our WALLET FOR FULL NODE, and the MWC 713 Wallet

After you have successfully setup your wallet, there are two main ways to send and receive transactions called the MWCMQS method and the File method. In general, this involves six steps:

- The sender creates the transaction using output(s)
- The receiver signs the transaction
- The receiver returns the transaction to the sender
- The sender signs the transaction
- The sender broadcasts the transaction to the network
- The miners confirm the transaction in a block and add it to the blockchain

—

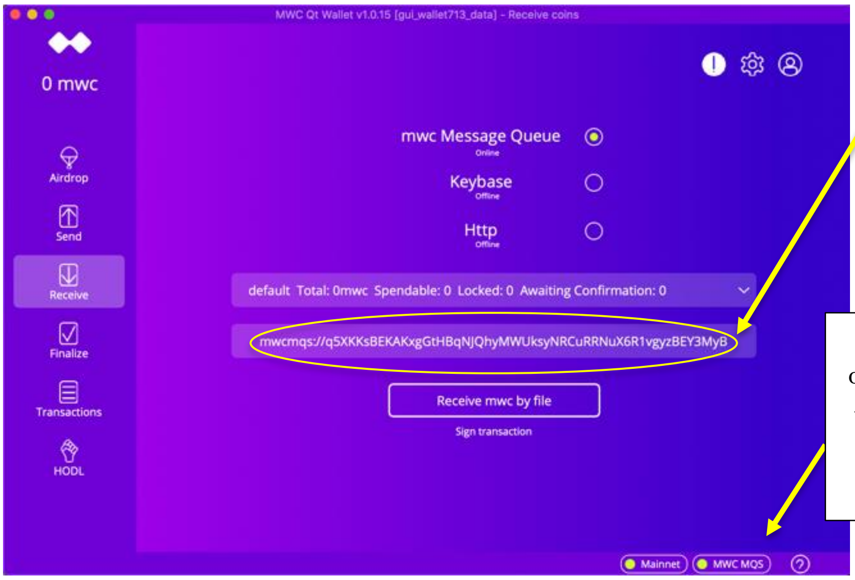
[69] Georg Fuchsbauer, Michele Orrú, and Yannick Seurin, "Aggregate Cash Systems: A Cryptographic Investigation of Mimblewimble," *The International Association for Cryptologic Research*, 2018. Retrieved from https://eprint.iacr.org/2018/1039.pdf

The MWCMQS Method

> *“While privacy coins offer bad actors a level of anonymity, the liquidity issues and barriers to entry for buying and selling privacy coins make them impractical for most dark market purchases.”*
>
> John Jefferies
> CipherTrace

Sending and receiving via the MWCMQS method will be most similar to a Bitcoin transaction. However, both the sender and receiver must be able to interact. **This means the receiver must be online and listening with the address the sender is attempting to send to.** This means you cannot just provide an address and turn off your laptop and go to bed like you can with BTC, LTC, etc.

To get started, open up the wallet and click “Receive” in the left-hand menu. Copy the mwcmqs:// address and send it to your partner. Sending via email or a messaging application is fine. In order for your partner to send you a transaction, **your wallet will need to be online** and listening (in the lower right the MWCMQS will need to be green) for that specific address.



MWC Qt Wallet v1.0.15 [gui_wallet713_data] - Receive coins

0 mwc

mwc Message Queue ● Online
Keybase ○ Offline
Http ○ Offline

default Total: 0mwc Spendable: 0 Locked: 0 Awaiting Confirmation: 0

mwcmqs://q5XKKsBEKAKxgGtHBqNJQhyMWUksyNRCuRRNuX6R1vgyzBEY3MyB

Copy this address and paste in an email to your partner.

You must be online to receive a transaction. This light should be green.

Once your sender copies in the address that you send them, they can paste in the address on the wallet by clicking on the “Send” option in the left-hand menu. They can also send a message along with the transaction.

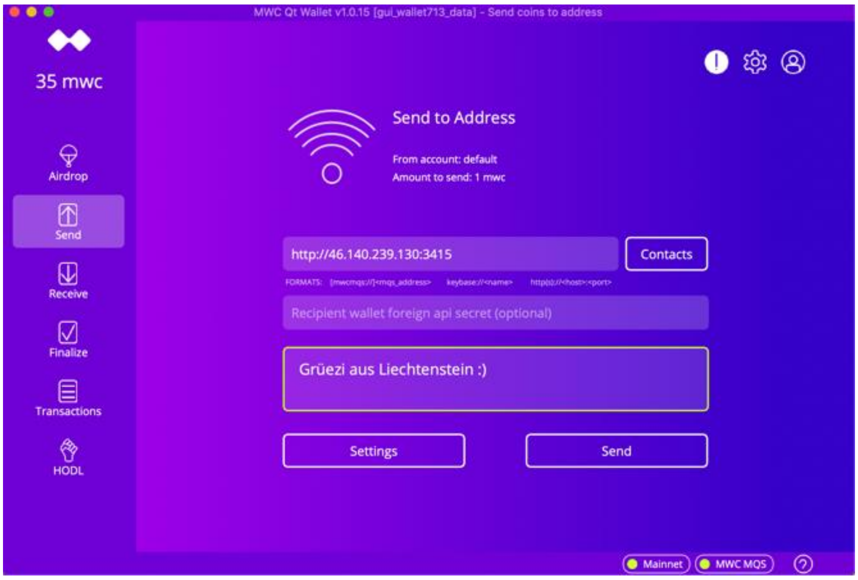
The File Method

Although the MWCMQS method is the easiest method for people that used to send Bitcoin transactions, the most private way to send MWC transactions is with the File method.

Sending and receiving by File requires five steps.

- The sender creates the transaction and generates a .tx file
- The sender provides the .tx file to the receiver
- The receiver signs the transaction and generates a .tx.response file
- The receiver provides the .tx.response file to the sender

- The sender signs the transaction and broadcasts it to the network by finalizing the transaction



MWC Qt Wallet v1.0.15 [gui_wallet713_data] - Send coins to address

35 mwc

Send to Address

From account: default
Amount to send: 1 mwc

http://46.140.239.130:3415

FORMATS: [mwcmqs://]<mqs_address> keybase://<name> http(s)://<host>:<port>

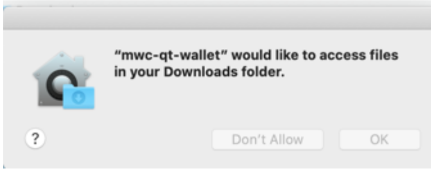
Recipient wallet foreign api secret (optional)

Grüezi aus Liechtenstein :)

“In cashless societies like Sweden, 95 % of all transactions are done using a plastic card. Every single one of those transactions is under full surveillance, not just by one intelligence agency, but you can assume by all simultaneously and surreptitiously. We already have a digital money future, which is a totalitarian surveillance nightmare.”

Andreas Antonopoulos

To get started, a sender will attach the mwc-payment.tx file to an email and then email this file to the receiver. This covers the first two steps. The receiver must then download the file from the email and then go into their MWC wallet and insert the file. Depending on your operating system, a little box may pop up when you click “Receive mwc by file.” This box will ask you for permission to access files in your Downloads folder. Once you click “OK” you will need to find the specific .tx file that the sender sent you.



“mwc-qt-wallet” would like to access files in your Downloads folder.

Then the receiver needs to email back a new mwc-payment.tx.response file, which will constitute the next two steps. Then, the final step will be finalizing the transaction on the sender’s side. The sender and receiver can check the transaction on the block explorer: https://explorer.mwc.mw/. By clicking in the upper right corner on the Gear, MWC users can see their transactions on the blockchain by double-clicking on the output. What is cool is that only you and the person you transacted know how many MWCs are associated with that particular output.

Fireside with the MWC Team

- Are you inspired by Austrian economics? If so, please who is your favorite Austrian economist? What is your favorite book on Austrian economics? And, last but not least, what is your favorite quote?

"Individual privacy online has decreased for the last nine consecutive years in a row."

Freedom on the Net Report 2019

- *Yes, we like the Austrian school of economics because of its objectivity. It is about understanding how things are in contrast to how we many want them to be. Mises, Rothbard, Gordon, Block and others have produced some excellent work. Human Action is a foundational text in the area. We are monetary sovereignty maximalists and are big fans of any means that help accomplish that purpose or aim whether that comes in the form of gold, silver, Bitcoin, Dogecoin, MWC or whatever. As Mises explained,* ***"It is impossible to grasp the meaning of the idea of sound money if one does not realize that it was devised as an instrument for the protection of civil liberties against despotic inroads on the part of governments. Ideologically it belongs in the same class with political constitutions and bills of rights. The demand for constitutional guarantees and for bills of rights was a reaction against arbitrary rule and the nonobservance of old customs by kings.*** *The postulate of sound money was first brought up as a response to the princely practice of debasing the coinage. It was later carefully elaborated and perfected in the age which—through the experience of the American continental currency, the paper money of the French Revolution and the British restriction period—had learned what a government can do to a nation's currency system... Thus, the sound-money principle has two aspects. It is affirmative in approving the market's choice of a commonly used medium of exchange. It is negative in obstructing the government's propensity to meddle with the currency system."*

- You mention that the MWC team are invested in Bitcoin. Are you invested in any other privacy-related coins?

- *We do not know. The MWC Team is composed of a significant number of people who are united by the purpose or aim of monetary sovereignty. And part of that means that what each of us does with our own money is our own business and not the business of others.*

- What do you say to the argument, "Only criminals use privacy coins?"

- *Without the ability to keep secrets, individuals lose the capacity to distinguish themselves from others, to maintain independent lives, to be complete and autonomous persons. This does not mean that a person actually has to keep secrets to be autonomous, just that she must possess the ability to do so. The ability to keep secrets implies the ability to disclose secrets selectively, and so the capacity for selective disclosure at one's own discretion is important to individual autonomy as well.*

  Secrecy is a form of power. The ability to protect a secret, to preserve one's privacy, is a form of power. The ability to penetrate secrets, to learn them, to use them, is also a form of power. Secrecy empowers, secrecy protects, secrecy hurts. The ability to learn a person's secrets *without his or her knowledge — to pierce a person's privacy in secret — is a greater power still.*

We want to help humanity exercise their unalienable right to secrecy, or in other words, to have you and your property left alone. This is even more important now that we have tools like Bitcoin and MWC which are based on public-private key encryption.

> *"While privacy coins may intuitively appear likely to be preferred by malicious actors due to their purported anonymity-preserving features, there is little evidence to substantiate this claim."*
>
> Rand Corporation

- ▶ Who is the target demographic for privacy coins? What do you think is the average demographic of a privacy coin user? I mean, do you think that privacy coins are primarily used in developed countries or in developing countries? Do you think they are used by relatively rich people or relatively poor people?

- ▶ *We are not really sure since we have not done much market analysis besides personal introspection. For the most part, we have been significant Bitcoin holders for many years but are cognizant of its characteristics and how it does not necessarily perform very well all of the jobs we may want it to. We saw the opportunity to build a product we wanted to use ourselves, extremely scarce ghost money, and the other monetary entrepreneurs in the marketplace were currently neglecting that market demand or choosing design characteristics we did not find compelling in a product. So we built the type of monetary product we wanted to use ourselves.*

- ▶ What are the main points on the roadmap for MWC during the next 12 months?

- ▶ *Fully distributing the initial stock via the unclaimed airdrop fund and HODL program, additional exchange integrations, greater market liquidity, additional Grin rebases, release a mobile wallet, atomic swaps, a decentralized exchange, multisig, Lightning Network and other features.*

Conclusion

The MWC network was launched in November 2019 and has functioned flawlessly with 100 % uptime. The MWC team considers the protocol ossified and currently sees no need for a future hard or soft fork unless a defensive action were required to protect the network. We feel the MimbleWimble sector may be neglected, to contain significant disruptive technological innovation potential, and there may be significant information asymmetry in the market. This type of technology is especially important in the age of surveillance.

Disclaimer: The author of this article owns MWC.

Introducing...

Crypto Research Newsletter

Tuesday, January 7, 2020
10 am cet

Crypto Research Newsletter

Professional Financial Analysis of Cryptocurrencies

crypto research .report

The Gist of the Week's Top Cryptocurrency Headlines

- XRP raises $200 million despite losing 95% of its market price during the last two years. Read more.
- Internal Revenue Service in the US published 43 frequently asked crypto tax questions. For example, if a hard fork is followed by an airdrop and you receive new cryptocurrency, you will have taxable income in the taxable year you receive that cryptocurrency. Read more.
- The highest return for the top ten cryptocurrencies in 2019 was Bitcoin with a 96% return. Read more.

Special Announcement

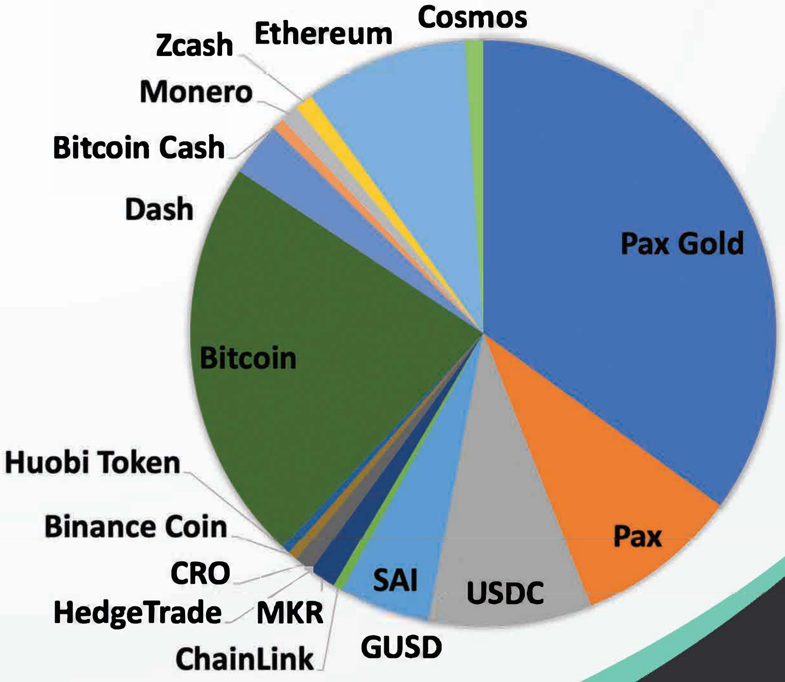
Meet the CRR Crew this week at Davos at the CV VC Summit.

Professional Financial Analysis of Cryptocurrencies

See what our portfolio holds and follow our weekly trades for the price of a coffee!

Sign up for our newsletter!

CRR Portfolio Jan 31st 2020



crypto research .report

Crypto Research Report Recommended Books

In the book, *The Liechtenstein Tax Law*, Matthias Langer hits the nail on the head in respect to taxation of blockchain and FinTech companies in Liechtenstein. Published in 2019, the book opens up with the history of the Principality of Liechtenstein before moving on to the main topics of company, foundation, and trust law. The existing legal forms are presented concisely, followed by an overview of the type and scope of Liechtenstein's audit, review and disclosure requirements, as well as the existing accounting regulations.

Matthias Langer has worked as a tax consultant in Liechtenstein for eleven years and now has his own law firm in Triesen. In the book, he delves into topics such as property and acquisition tax, gifts and inheritances, and income tax. The taxation of investment funds and foundations, as well as international tax law pertaining to offsetting and relocation find their way into the reading. Since Liechtenstein is also one of the pioneers in the blockchain and fintech, their handling of taxation is of great international interest. After a brief explanation of the basic terms and the balance sheet approach to cryptocurrencies, the peculiarities of the acquisition, income and value-added tax are discussed. In addition to differentiating different types of coins, the reader learns the tax significance of the transfer, trading, and storage of coins and tokens.

In summary, the book deals with all essential aspects of tax law in Liechtenstein. The treatment of tax law specifics of blockchain and fintech companies deserves special mention. The reader leaves the book with a deeper level of understanding of how crypto funds work and the taxation of cryptocurrencies. However, the book is easy to read due to the structure and short and accurate explanations that are illustrated with examples. In addition, the book enables quick reference and comprehension without the reader having to have in-depth tax knowledge. Although the book is primarily aimed at prospective entrepreneurs in Liechtenstein, it also contains information that is interesting for those who want to learn more about life in Liechtenstein and the country itself. The book is only available in German at this time and can be bought on the publisher website, Springer Verlag.

Dipl.-Kfm. Matthias Langer, LL.M.

Advisors

In order to provide accurate information on the most important and recent updates in the crypto space, a diverse team of thought-leaders, academics, and finance experts form our board of advisors. The mission of our board is to stimulate discussion on the most pressing risks and opportunities in the cryptocurrency market. Our advisors come from different countries, different education paths, and different careers. However, they all have one trait in common: their avid interest in the blockchain technology and cryptocurrencies. To stay up-to-date, the advisory board meets on a regular basis to discuss current affairs and the next quarter's outlook. All meeting minutes are posted as a transcript and released for free on our website at www.CryptoResearch.Report. Our board members include:

Max Tertinegg

Max Tertinegg is the CEO and co-founder of Coinfinity in Graz. Since 2014, Mr. Tertinegg has worked with merchants, investors, and regulators in Austria to build a cryptocurrency community. Currently, he is working on cryptocurrency storage solutions that are affordable and easy to use. In cooperation with the State Printing House of Austria, Coinfinity has designed a "Card Wallet" that is a bearer paper wallet for Bitcoin.

Oliver Völkel

Based in Vienna, Oliver Völkel is a partner at Stadler Völkel Attorneys at Law. He assists corporations and banks in all stages of capital market issuings and private placements (national and international). His focus is on new means of financing vehicles (initial coin offerings, initial token offerings) and drafting and negotiation of cross-border facility agreements and security-documentation, also in connection with cryptocurrencies and tokens. Mr. Völkel also advises on other cryptocurrency related banking matters, regulatory matters, capital markets regulation, general corporate, and corporate criminal matters.

In case you have missed our last Crypto Research Report and you would like to have a pleasant reading, please follow the links below.

crypto research .report

December 2017 Edition I.

Demelza Kelso Hays
Ronald-Peter Stoeferle
Mark J. Valek

incrementum

Crypto Research Report – December 2017 Edition

- Introduction to the Blockchain Technology and Cryptocurrencies
- U.S. Regulated Bitcoin Derivatives: Blessing or Curse?
- Constructing a Cryptocurrency Index
- Taxation of Cryptocurrencies in Europe
- Farewell 2017: Year of ICOs, Hard Forks, and Upward Trends

crypto research .report

March 2018 Edition II.

Demelza Kelso Hays
Mark J. Valek

incrementum

Crypto Research Report - March 2018 Edition

- In Case You Were Sleeping: Ikarus Edition
- Bubble or Hyperdeflation?
- Coin Corner: War Within Bitcoin
- Technical Analysis: Is a Crypto Winter About to Start?
- Crypto Concept: Fork
- 10 Facts About Max Tertinegg, the CEO of Coinfinity
- Incrementum Insights: How Will Cryptocurrencies Change Finance

crypto research .report

June 2018 Edition III.

Demelza Kelso Hays
Mark J. Valek

incrementum

Crypto Research Report - June 2018 Edition

- In Case You Were Sleeping: Wall Street Is Getting Ready
- Crypto Concept: Consensus Mechanisms
- Competing Currencies and Digital Money: How Hayekian are Cryptocurrencies?
- Coin Corner – Blockchain 3.0 The Future of DLT?

crypto research .report

October 2018 Edition IV.

Smart Contracts
Liechtenstein's Blockchain Strategy
The "Network Effect" as Valuation Methodology

Demelza Kelso Hays
Mark J. Valek

incrementum

Crypto Research Report - October 2018 Edition

- In Case You Were Sleeping: Cell Phone Theft Edition
- Crypto Concept: Smart Contracts
- Liechtenstein's Blockchain Strategy
- Coin Corner: ETH, NEO, ADA, & EOS
- The Network Effect as a Valuation Methodology

crypto research .report

January 2019
Edition V.

"Crypto Winter Edition"

Custody Solutions for Cryptocurrencies
Securitization or Tokenization?
Could a Bitcoin Standard work?

Demelza Kelso Hays
Mark J. Valek

Crypto Research Report - January 2019 Edition

- In Case You Were Sleeping: Crypto Winter Edition
- Crypto Concepts: Custody Solutions for Crypto Currencies
- A Bitcoin Standard? Saifedean Ammous Musing with the Crypto Research Report
- Institutional Requirements for an Investible Crypto Index
- Equity Tokens
- Legal Challenges for Blockchain-Based Capital Markets

crypto research .report

April 2019
Edition VI.

"Wenn die Ebbe kommt…"

Anlagestrategie: Gold und Bitcoin im Duett
Technische Analyse: Frühlingserwachen?
Mining - Theorie und Praxis

Demelza Kelso Hays
Mark J. Valek

Crypto Research Report - April 2019 Edition

- In Case You Were Sleeping: When the Tide Goes Out…
- Gold & Bitcoin: A Crypto Strategy, also for Institutional Investors
- Technical Analysis: Spring Awakening?
- Crypto Concepts: Cryptocurrency Mining in Theory and Practice
- John Tromp: Making Computer Science Great Again

crypto research .report

July 2019
Edition VII.

The Libra Edition

Libra: The End of the State Money Monopoly?
Coin Corner: Ripple Labs Inc. and XRP
Fieeside Chat with Nick Szabo on Scaling Bitcoin

Demelza Kelso Hays
Mark.J.Valek

Crypto Research Report - July 2019 Edition

- In Case You Were Sleeping: Facebook Edition
- Libra: The End of the State Money Monopoly
- Coin Corner:XRP and Ripple
- Gold Stablecoins
- Partner Insights: Lucas Ereth on Transforming Finance
- Fireside with Nick Szabo on Scaling Bitcoin

crypto research .report

October 2019
Edition VIII.

Crypto Liquidity Edition

How Crypto Brokers and Funds Source Liquidity
Security Token Regulation in Switzerland
Frankly Speaking About the Crypto Swiss Franc

Demelza Kelso Hays
Mark J. Valek

Crypto Research Report – October 2019 Edition

- In Case You Were Sleeping: Banking on the Blockchain
- How Crypto Brokers and Funds Source Liquidity
- A Primer on Regulation and Trading in Switzerland
- Tokenizing the Swiss Franc with Armin Schmid of Swiss Crypto Tokens
- Incrementum Recommended Books
- Upcoming Conferences

crypto research .report
February 2020
Edition XIV.
"Plan B Edition"
Is Bitcoin Evolving to Digital Gold?
The "Plan B" Model – Holy Grail of Bitcoin Valuation?
Crypto Custody: What's new in Germany?
Demelza Hays
Mark J. Valek

Crypto Research Report – February 2020 Edition

- In Case You Were Sleeping: Iran, Gold, and a Small Bitcoin Boom
- The “Plan B” - Model: The Holy Grail of Bitcoin Valuation?
- The Stock to Flow Model: Exclusive Interview with “Plan B”
- Crypto Custody: What’s new in Germany
- Bitcoin vs. Gold – a Fictitious Debate
- Incrementum Recommended Books

We sincerely want to thank the following friends for their outstanding support:
Our knowledgeable advisors including Max Tertinegg and Oliver Völkel and the authors who contributed to this report including Pascal Hügli. We are also grateful to our wonderful websmaster, Mark Mason, and our terrific editor Bianca Sayers.

Contact:

Crypto Research Report
9492 – Eschen/Liechtenstein
http://www.cryptoresearch.report
Email: info@cryptoresearch.report

Disclaimer:
This publication is for information purposes only, and represents neither investment advice, nor an investment analysis or an invitation to buy or sell financial instruments. Specifically, the document does not serve as a substitute for individual investment or other advice. The statements contained in this publication are based on the knowledge as of the time of preparation and are subject to change at any time without further notice. The authors have exercised the greatest possible care in the selection of the information sources employed, however, they do not accept any responsibility (and neither does Crypto Research Report) for the correctness, completeness or timeliness of the information, respectively the information sources, made available, as well as any liabilities or damages, irrespective of their nature, that may result there from (including consequential or indirect damages, loss of prospective profits or the accuracy of prepared forecasts.