



Forensic Analysis & Deep Dive

Powered by



Contents

1. EXECUTIVE SUMMARY	4
1.1. Company Overview	4
1.2. Market Overview	5
1.3. Financial Highlights	6
2. ABOUT COINBASE	9
2.1. Introduction	9
2.2. Coinbase – Products & Services	10
2.3. How Coinbase Works	12
2.4. Coinbase Business Model	13
2.5. Coinbase Future: Strategies and Challenges	15
2.5.1. Strategic Expansion:	15
2.5.2. Coinbase Acquisitions:	16
2.5.3. Challenges and Risks	16
3. LITIGATION, LAWSUITS & LEGAL ISSUES	18
3.1 Adam Alfia filed a lawsuit against Coinbase for not safeguarding customer accounts	18
3.2 Scott + Scott Attorneys at Law LLP filed a securities Class Action lawsuit against Coinbase Global Inc.	19
3.3 Plaintiff filed a class-action lawsuit against Coinbase (Cryptsy Case)	20
3.4 Coinbase sued for misleading Sweepstakes Advertising (Suski v. Coinbase Global)	21
3.5 Jonathan Zubin filed a civil action lawsuit against Coinbase Global Inc.	21
3.6 Craig S Wright vs Coinbase	22
4. GLOBAL MARKET OVERVIEW	24
4.1. Global Cryptocurrency Exchanges	24
4.2. Centralized Vs. Decentralized Cryptocurrency Exchange	24
4.3. Global Crypto Exchange Market Segmentation	27
4.4. Global Crypto Exchange Market Size	27
4.5. Global Crypto Exchange Regulations	29
4.6. Global Crypto Exchange Market Growth	30



4.7. Crypto Exchange Key Players	31
5. US Crypto Exchange Market	34
5.1. Overview	34
5.2. U.S. Crypto Exchange Market Trend	34
5.3. U.S. Crypto Exchange Market Key Drivers	37
5.4. SWOT Analysis.....	39
5.5. U.S. Crypto Exchange Market Challenges	39
5.6. Outlook	47
Patents and Intellectual Property	49
The Popping of the Crypto IP Bubble is Nigh	49
Trademarks and Brands	50
Copyrights and Commercial vs Open-Source Licenses	51
Patents – The Big Kahuna	52
nChain Holdings	53
True Return Systems	55
Veritaseum and Patents US11196566 and JP6813477	91
Ethereum	95
Solana.....	96
Bitcoin	97
6. FINANCIALS – HISTORICALS.....	100
6.1. Components of Results of Operations	100
6.2. Total Revenue	103
6.3. Total Operating Expenses	104
6.4. Total Operating Income / (Loss).....	105
6.5. Net Profit & Net Profit Margin	106
7. FINANCIALS – FORECASTED	107
7.1. Revenue-Based Financials.....	107
7.2. Operating Expense Financials	109
7.3. Total Operating Income	111
7.4. DLT Patent Infringement Expense	113
7.5. Net Income / (Loss)	114
Disclaimer	115



1. EXECUTIVE SUMMARY

1.1. Company Overview

Coinbase Global, Inc. is a cryptocurrency trading platform operated by an American corporation. Coinbase is a dispersed corporation; all staff work remotely, and the company does not have a physical headquarters. Coinbase is an online marketplace for purchasing, trading, transferring, and storing digital assets. Its objective is to build a global, open financial system and to be the dominant global brand for converting digital currency into and out of fiat and sovereign currencies. It is a platform on which various apps are created that make use of their API. By trading volume, it is the largest cryptocurrency exchange in the United States.

Coinbase provides solutions for both retail and institutional investors, as well as other cryptocurrency-related services.

Name	Coinbase Global, Inc.
Founder	Brian Armstrong & Fred Ehrsam
Launch Date	June, 2012
Industry	Cryptocurrency
Headquarters	No Headquarters
Revenue (2021)	US\$7,839 million
Website	www.coinbase.com

Among the company's retail trade offerings are:

- Coinbase, a cryptocurrency exchange that allows you to purchase, store, and exchange various cryptocurrencies.
- Coinbase Pro, a specialized asset trading platform.
- Coinbase Wallet, an app that provides clients with access to decentralized cryptocurrency systems and platforms..

The Company's institutional trade offerings are:

- Coinbase Prime, a prime brokerage platform for institutional clients.
- Coinbase Custody provides expert-level services to organizations who store bitcoin and other cryptocurrencies with Coinbase.

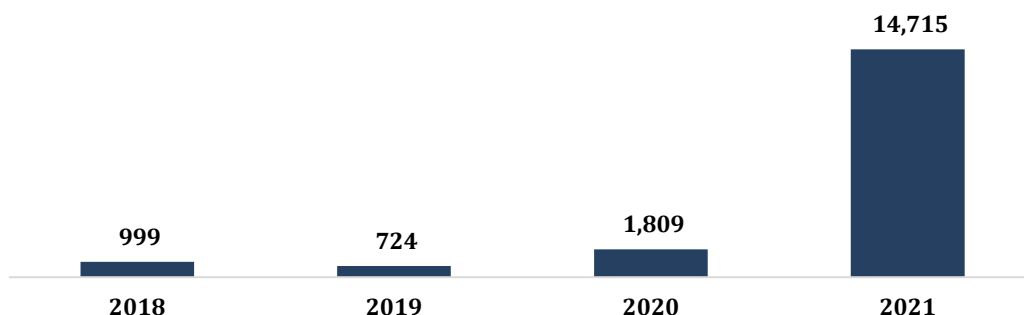


The firm creates an application programming interface (API) for developers and merchants to use in order to build applications and accept digital currency payments.

1.2. Market Overview

The Global exchange market witnessed positive trading volumes on both centralized and decentralized exchanges in 2021. We'd be remiss in not noting the market has significantly compressed during the 2nd quarter of 2022, thus this growth will not be replicated this fiscal year.

Figure 1: Cryptocurrency Exchange Volume (in US\$ billion)



Source: Cryptocompare, March 2022

Various financial institutions are cooperating with bitcoin companies to improve their services and client experience. Visa, for example, announced a relationship with 50 cryptocurrency firms, including Coinbase and FTX, in July 2021. Crypto exchanges are becoming increasingly popular in the financial business. Payments, smart contracts, and compliance management/KYC applications assist banks, investment banks, and insurance businesses in improving efficiency and lowering infrastructure costs. Due to the rising relevance of crypto exchange platforms, blockchain applications, and non-bank financial services are likely to dominate the market throughout the upcoming period. While the aggressive trading market route may lead some to doubt this, most of the value in crypto currently lies in the infrastructure, with future value to be born from the advanced applications springing from a more completely developed and advanced infrastructure. This is like how the Internet and World Wide Web developed rudimentary apps, a boom, then bust, then a considerably more advanced app and business model development came in the form of Google, Facebook, Amazon, etc.

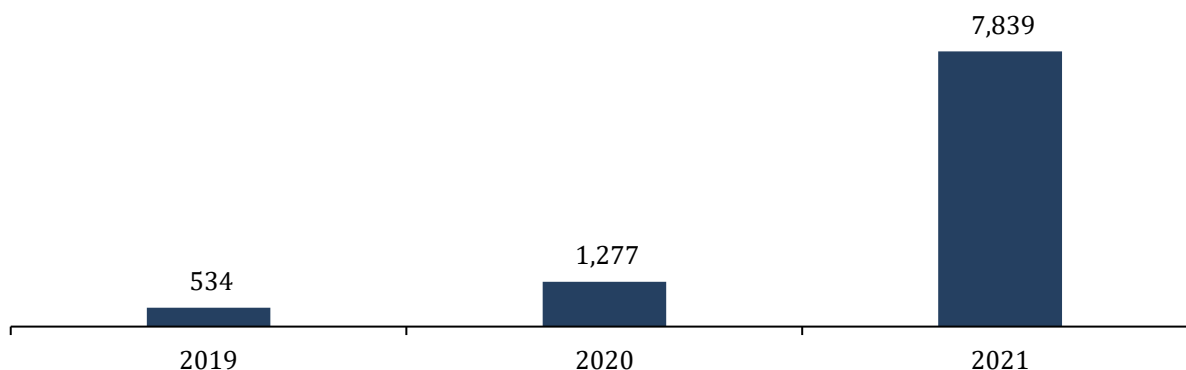
Furthermore, the increasing global penetration of smartphones is one of the major factors creating opportunities for market growth. Smartphones enable Web3 attributes and capabilities – allowing customers to take fuller advantage of the capabilities of cryptocurrency platforms. Many platform providers are focusing on providing their services via mobile phones in order to better satisfy the demands of their clients.

1.3. Financial Highlights

Coinbase generates its revenue from different segments that are transaction based, Subscription & service based, and other sources. Coinbase's principal source of revenue is transaction revenue, which is obtained directly from trading volume. As a result, transaction income is linked to the price of Bitcoin and the volatility of Crypto Assets.

Coinbase has generated total net revenue of ~US\$1,277 million during the year 2020, which is a 513% increase compared to the previous year. For the year 2021, it stood at US\$7,839 million+. The surge is mostly attributable to an increase in trading volume with the increase in MTUs (Monthly Transacting Users) and in the bitcoin average price. Whereas the total operating expense during 2020, was US\$868 million, and in 2021, it stood at US\$4,762 million.

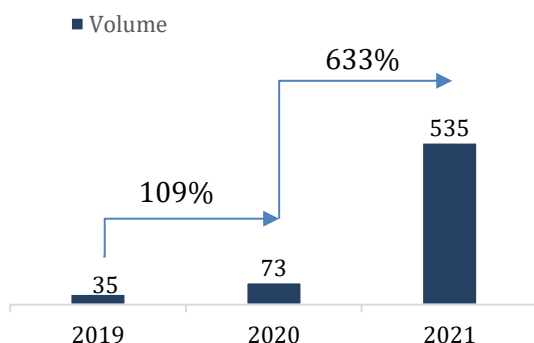
Figure 2: Historical Revenue Growth (US\$ million): 2019-2021



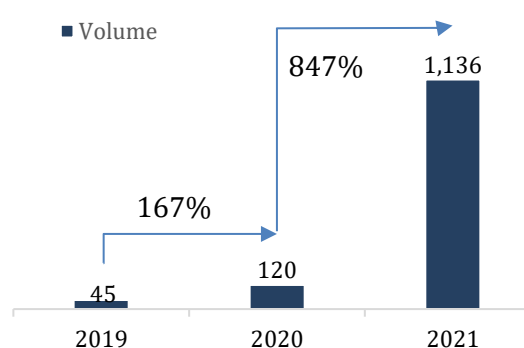
Source: Coinbase Annual Reports

Trading Volume: Retail and Institutional trading volume increased gradually from 2019 to 2020 along with retail users (MTUs). In 2021, the trading volume showed a sudden rise of volume in both segments.

Retail Trading Volume (in US\$ bn)

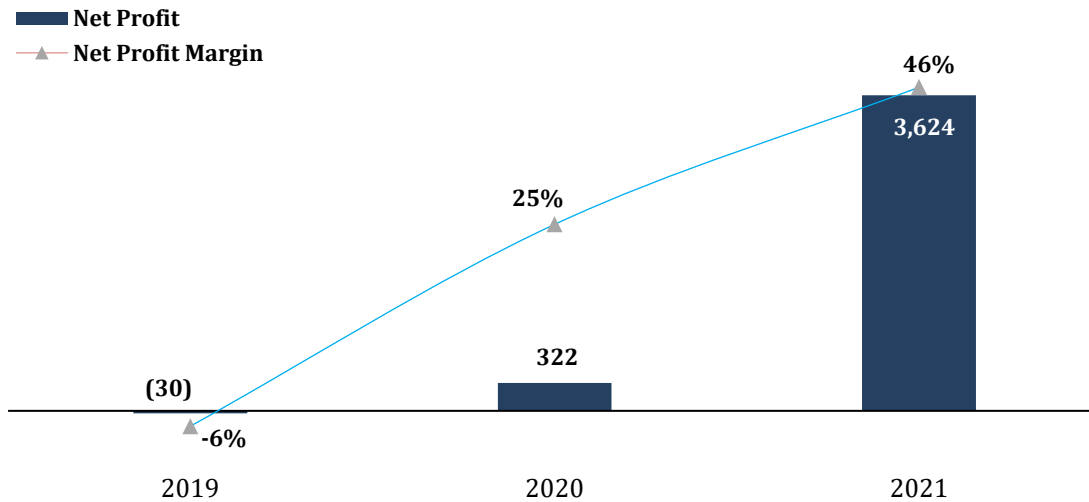


Institutional Trading Volume (in US\$ bn)



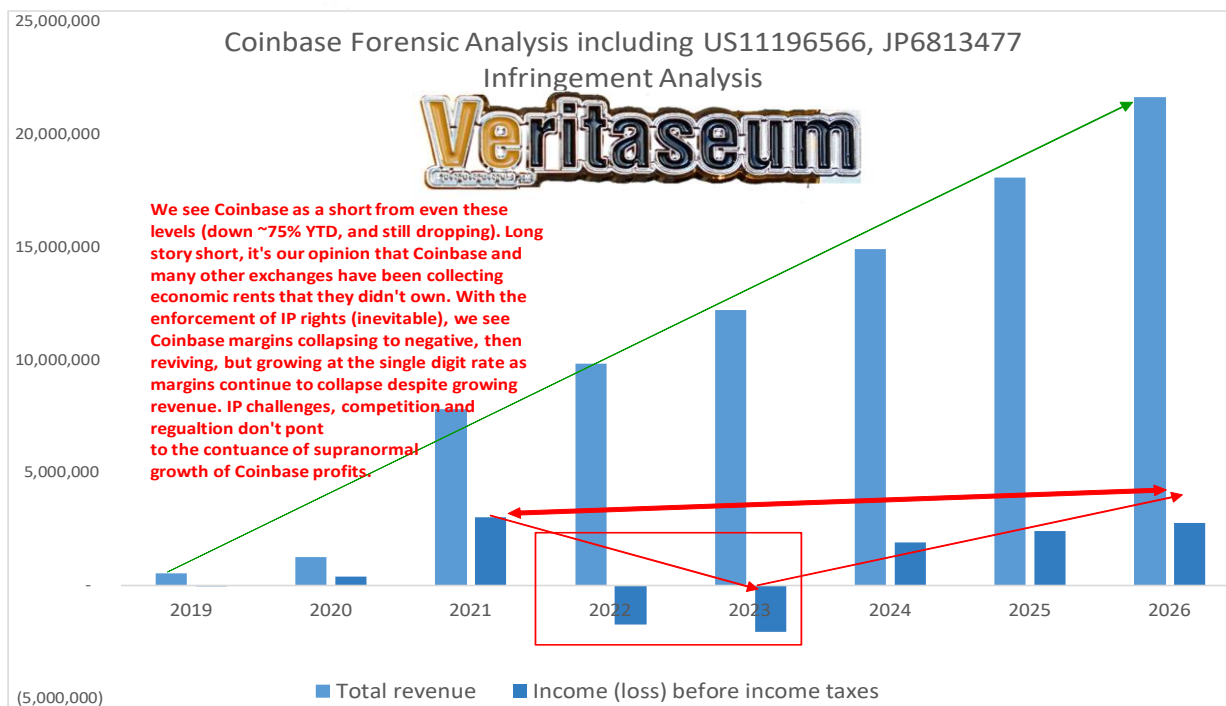
In retail trading, volume and fees per transaction showed a direct relationship. Volume increased as the fees increased gradually throughout 2019-2021. Whereas the institutional trading volume and its fees per transaction showed an inverse relationship as the volume increased drastically but the fees gradually decreased from 2019-2021. Coinbase generated a net income (Loss) of ~US\$30 million during 2019 but earned income in 2020 and reached US\$3,624 million in 2021.

Figure 3: Net Profit and Net Profit Margin



Source: Coinbase Annual Reports

The company earned profit due to a drastic rise in transactional revenue. During 2019-2021, the net profit margin increased as the Company witnessed outstanding growth in the overall revenue. We expect supranormal profitability to end 2nd quarter 2022, with deteriorating metrics until 2023-24.





2. ABOUT COINBASE

2.1. Introduction

Launched in 2012, three years after the launch of bitcoin by Brian Armstrong and Fred Ehrsam, Coinbase Global Inc. (the 'Company' or 'Coinbase') operates as a cryptocurrency exchange (although, technically, it is more akin to a broker/dealer) platform that allows users to buy, sell, or hold more than 100 virtual assets. The Company paved its way to new heights, and in 2022, it ranked 6th among the largest cryptocurrency exchanges in the world (Statista, 2022).

In 2014, the Company focused on escalating its operation with the acquisition of Blockr (a blockchain explorer service) and a web bookmarking company Kippt Inc. and partnered with Overstock, Dell, Expedia, Dish Network, and Time Inc. to enable bitcoin payments. In 2015, the Company launched a bitcoin exchange (Coinbase Exchange) in the U.S. for professional traders.

In Apr 2021, the parent Company – Coinbase Global Inc, became public with the direct listing on the Nasdaq Stock Exchange. Coinbase hit lofty heights in revenue of US\$7.3 billion in 2021 from US\$1.1billion in 2020 with a Y-o-Y growth of 544.5%. This growth was attributable to the increase in demand for bitcoin, fueled by thousands of stimulus dollars and long hours at home quarantine. Bitcoin, the most famous digital currency, was valued at less than US\$5,000 in 2019 when Covid-19 arrived in America causing an economic slump that was addressed with historically unprecedented money printing and both fiscal and monetary policy stimulation measures, resulting in a price pop to more than US\$50,000 in 2021. This aided the Company in getting more people to purchase BTC.

Coinbase serves around 89 million verified users, 11,000 institutions, and 185,000 ecosystem partners across the world. With more than 3,700 employees around the world, Coinbase also has US\$278 billion of assets on the platform. The trading platform of Coinbase is beginner-friendly and simple to use for anybody with basic computer abilities. Coinbase is accessible via the web as well as mobile devices running Android and iOS.

Coinbase also offers a variety of investment possibilities for corporations and organizations, such as cryptocurrency storage and commerce services.

Coinbase, like other payment providers such as Stripe or PayPal, has created plugins for any major eCommerce platform, such as Shopify or Magento. A user only has to install the plugin to get started immediately.

Some of the big cryptocurrencies/coins traded on the Coinbase platform are depicted below:



Cardano



Enjin



Bitcoin



MANA



Vechain



Polygon



Avalanche



Chainlink



Tether



Litecoin



DAI



Solana



Ethereum



Dogecoin



Ripple



Stellar



NEO



Shiba Inu



Polkadot



Cosmos

2.2. Coinbase – Products & Services

Today, Coinbase runs in more than 100 countries. It's 26 products can be divided into three primary lines of business.

Coinbase provides many additional services to its clients - individuals, businesses, and developers.

The following are advantages that help Coinbase to compete in the market:

- **Wide Selection** – Over 150 cryptocurrencies are supported with Coinbase for trading.
- **Mobile App** – A user-friendly application for all users available on both Android and iOS.
- **Advanced Trading Platform** – Two separate trading platforms that offer real-time order books with lower trading fees.

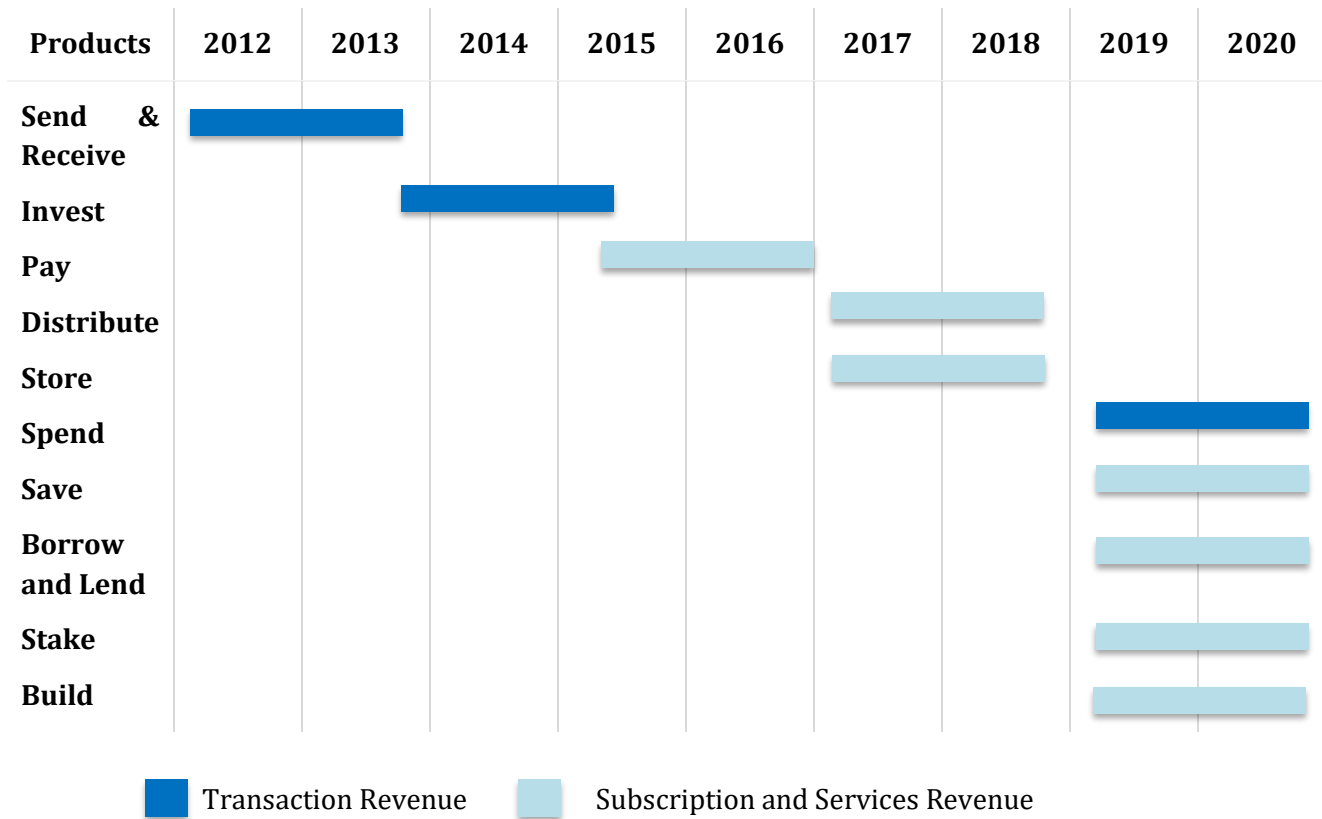


- **Debit Card Access** – Provides a Coinbase card (visa debit card) to its users that is acceptable to Visa worldwide.

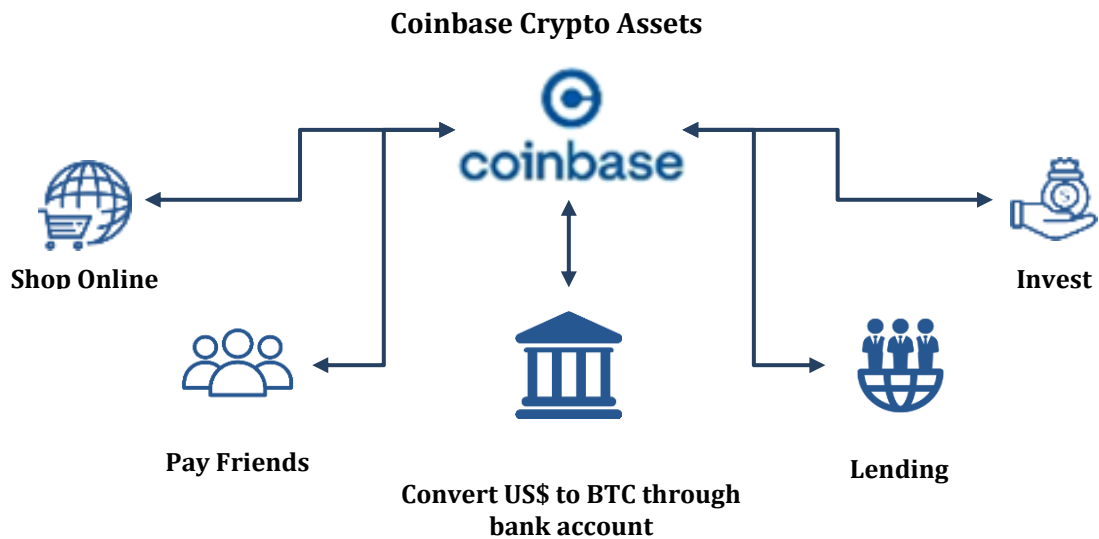
	Retail Users	Institutions	Ecosystem Partners
Transaction Revenues			
Invest	✓	✓	
Spend	✓		
Send & receive	✓	✓	✓
Subscription & Services			
Store		✓	✓
Save	✓		
Stake	✓	✓	
Borrow & lend	✓	✓	
Distribute			✓
Build			✓
Pay			✓



Progress of product development



Coinbase resembles a regular financial



2.3. How Coinbase Works

services provider by collecting transaction fees for its exchange. Like the NYSE or



NASDAQ, the Company holds user money. It offers a range of Crypto assets (such as

Bitcoin, Ethereum, Bitcoin Cash, Litecoin, and many more) for purchase and sale using fiat currencies in over 32 countries.

A trading platform and an intermediary are required to interface with the blockchain network and trade digital currency (that is, to do so on a centralized basis). GDAX (Global Digital Asset Exchange), an individual professional trading platform, developed into Coinbase Pro in 2018. GDAX

Figure 4: Transaction Fees

Total Transaction Value	Fess Cost
≤ US\$10	US\$0.99
US\$10 – US\$25	US\$1.49
US\$25 – US\$50	US\$1.99
US\$50 – US\$200	US\$2.99

offers an internal platform for transactions and sends transaction information to the blockchain network for verification. Anyone who already had a GDAX individual account was immediately upgraded to Coinbase Pro. The corporation has serviced over 10 million consumers and traded over US\$50 billion in digital money.

2.4. Coinbase Business Model

Coinbase's business strategy has evolved significantly since its inception. Initially, the firm solely earned through trading fees, but it has now expanded to include a range of items that it monetizes.

Today, Coinbase generates revenue through trading fees, maker and taker fees, interchange fees, interest on cash, sales of software tools, interest on personal loans,

and other means. Following are the key sources of revenue:

a. Fees on Trades

A large share of the Company's revenue is still generated by its fees for purchasing and selling cryptocurrency. Coinbase has a tiered commission structure reflecting the varied fees charged depending on the transaction volume. The break-up of transaction fees is discussed below:

When a user desires to exchange currencies (for example, US\$100 worth of Bitcoin into Litecoin), a spread margin is imposed. The spread margin is ~2%, although it is subject to market changes in the cryptocurrency price.

Also, depending on region and payment type, consumers will be charged a payment processing fee. For Example, A credit card transaction made by a cardholder from the United States adds another 3.99 % charge to the transaction volume. Fees account for the bulk of the firm's profits.

b. Coinbase Pro & Prime Trading Platform

Coinbase Pro and Prime are designed primarily for professional traders who work with cryptocurrency daily. Thus, the products include a variety of additional features, such as:

- Advanced filters and detailed history of trades
- To access real-time market data and create trade algorithms, the Company provides API
- A dedicated team of professionals to assist the prime members
- Offering insurance to cover digital assets protection (Up to US\$250,000) in case of a hacking attack

While the tools are free, clients must pay a fee when purchasing and selling currencies. Coinbase calculates its trading fees using a technique known as the maker-taker fee model. The following table shows the maker and taker fees for Coinbase Pro:

Figure 5: Coinbase Trading Fees

Pricing Tier	Taker Fee	Maker Fee
<\$10k	0.60%	0.40%
\$10k - 50k	0.40%	0.25%
\$50k - 100k	0.25%	0.15%
\$100k - 1M	0.20%	0.10%
\$1M - 20M	0.18%	0.08%
\$20M - 100M	0.15%	0.05%
\$100M - 300M	0.10%	0.02%
\$300M - 500M	0.08%	0.00%
\$500M+	0.05%	0.00%

Coinbase Prime has lower charges because its customers are

institutions that transfer millions of dollars each day.

c. Interchange Fees

Customers can get credit cards for free. Coinbase earns money every time a consumer uses the Card, mainly via the payment fee charged.

The fee is charged when the credit card is used to make a payment, like other credit cards a person owns (so-called interchange fees). The retailer deducts the money from the total transaction volume and pays it.

Besides interchange fees, Coinbase charges ATM fees (when withdrawing cash) as well as a 2.49% crypto liquidation fee (for users who do not utilize USDC).

d. Cashback

Coinbase launched its Visa debit card in October 2020. Previously, the Card was exclusively accessible to users in the United Kingdom and Europe. Now it can be used worldwide, where VISA is accepted.

Debit card customers in the United States can enjoy cashback benefits up to 4% in Stellar Lumens or 1% back in Bitcoin.

e. Interest Margin

Coinbase, like a bank, utilizes the funds in its user accounts to lend to other institutions, such as banks. The interest is then charged from these institutions (also called Net Interest Margin). As per the Statista report, the net interest margin for all U.S. banks in 2019 was 3.35%.

f. Coinbase Earn

Coinbase lets users explore new cryptocurrencies by attending the company's classes via Coinbase Earn. Post completion of a course, the users can earn pay-outs in the currency covered in the course. Users must view many videos and complete a quiz to finish the course.

In 2018, Coinbase acquired Earn.com in a US\$120 million transaction. Earn.com allows users to contact busy individuals for services in exchange for fees. These individuals are compensated in cryptocurrency for accepting those requests.

g. Analytics

The Analytics software gathers data from the public domain (rather than Coinbase user data) and enables users to analyze macro and micro levels of cryptocurrencies. Currently, the program is sold on a contract basis. For instance, The Secret Service secured a US\$183,750 contract that will expire in May 2024.

h. Personal Loans

Coinbase launched a lending product in August 2020, allowing customers to apply for personal loans using their crypto holdings as collateral.

The service is currently available for users in a few selected states in the United States. Users can borrow up to 30% of their Bitcoin amount and up to US\$100,000 (with a US\$2,000 minimum volume). Coinbase earns money by charging interest on these loans. The Company charges an APR

of 8% on its loans. Users have up to a year to pay it back.

i. Coinbase Ventures

Coinbase Ventures, a specialized investment team, that was established in 2018. Its goal is to fund promising early stage blockchain and cryptocurrency firms.

2.5. Coinbase Future: Strategies and Challenges

2.5.1. Strategic Expansion:

Coinbase CEO Brian Armstrong has sketched forth a roadmap for the Company's next 5+ years. The expansion plan is built on three pillars:

▪ Investments In Cryptocurrencies

Coinbase's primary business is cryptocurrency investing. The business intends to continue introducing additional cryptocurrencies to its platform at a higher rate than before. Coinbase also plans to offer advanced trading tools comparable to those seen in traditional markets to experienced traders.

▪ Accessing Financial System with Cryptocurrencies

Coinbase intends to create new solutions to assist cryptocurrency owners in accessing decentralized finance technologies. The Company also plans to develop technologies to allow businesses to accept

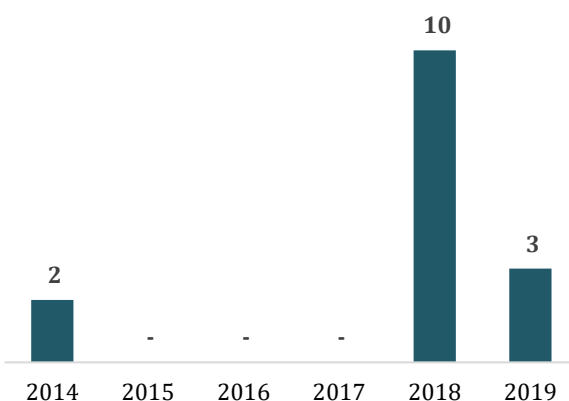
cryptocurrency, and users may make money by staking.

- **Crypto as a platform for app development**

Cryptocurrency innovations are believed to go beyond financial applications. Through Coinbase Ventures, the Company will assist its consumers in discovering new crypto applications and will fund such initiatives. In addition, non-crypto entities will be able to use the Coinbase crypto infrastructure to get access to the crypto economy.

2.5.2. Coinbase Acquisitions:

Figure 6: Number of Acquisitions



Source: C.B. Insights, 2021

- Since the beginning of 2018, Coinbase has purchased 19 businesses, with 21 purchased in total
- These purchases assist the corporation in carrying out its expansion plan and positioning cryptocurrency as an

investment tool, financial system, and app platform.

- Coinbase acquired Zabo (a tool to link crypto accounts) in August 2021, Tagomi (a cryptocurrency brokerage platform) in 2020, and Neutrino (a blockchain analytics Company) in 2019.

2.5.3. Challenges and Risks

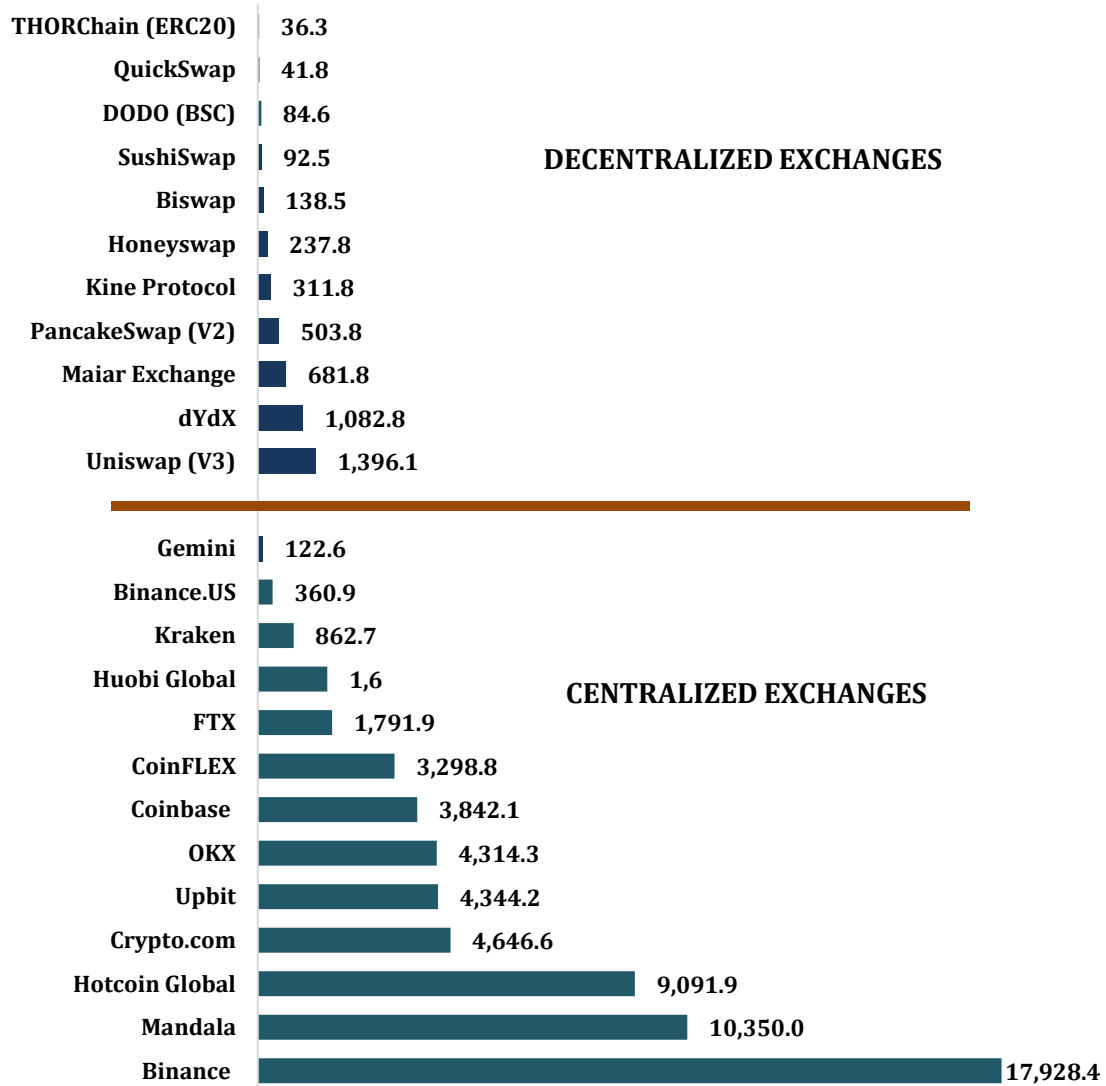
Coinbase is facing stiff competition from both established competitors and new decentralized exchanges. Coinbase is directly exposed to crypto asset values and must exercise caution during persistent market declines and excessive asset price volatility.

Coinbase also has competitors in the digital asset custody market. For retail and institutional consumers, the firm competes with Gemini and Blockchain.com. BitGo, PAXOS, and NYDIG are custodial rivals who mostly serve institutions.

Coinbase also has competitors in the digital assets derivatives market. Coinbase has acquired FairX, a derivatives exchange authorized by the CFTC, as it strives to catch up to competing exchanges in the massive and profitable sector. Competitors such as Binance, FTX, and OKEx have benefited from their early forays into providing futures trading. They are headquartered outside the United States, where laws are frequently less severe, and taxes are cheaper. As per Alex Tapscott, managing director at Canada's Ninepoint Partners, Coinbase has been largely overlooked, partly because it is located in the United States. All of these other exchanges have gained enormous financial benefits from derivative-related products

Coinbase Global Forensic and Fundamental Analysis

Figure 7: Centralized Vs. Decentralized 24h Trading Volume (in US\$ Million), March 2022



3. LITIGATION, LAWSUITS & LEGAL ISSUES

3.1 Adam Alfia filed a lawsuit against Coinbase for not safeguarding customer accounts

Source: <https://coingeek.com/coinbase-class-action-lawsuit-company-accused-of-not-safeguarding-customer-accounts/>

Published on: Nov 08, 2021

Published on: U.S. District Courts

Adam Alfia filed the case against Coinbase Global Inc regarding Coinbase's handling of customer balances. The case was brought by McCathern LLP (case number 3:21-cv-08689).

The arguments that Adam Alfia points out against Coinbase Global Inc. –

- Alfia proclaims Coinbase took unreasonable measures such as freezing accounts when dealing with breaches.
- The complaints of breach of contract, negligence, fraud, and negligent representation were put forward.
- Alfia claimed an unauthorized purchase of Ethereum worth US\$50,000 was made by his Coinbase account irrespective of his permission or consent to anyone.
- Alfia further claimed Coinbase locked his account for two months after complaining and made it impossible to reverse the US\$50,000 transaction taken from the Bank of America Account.
- The suit was filed on behalf of Alfia and all other similarly situated persons.
- Plaintiff claimed Coinbase failed to properly secure their private information and cryptocurrency from unauthorized transactions and dissemination, thus causing Plaintiff significant damage, worry, and stress.
- Thus, Alfia requested the Court to act against Coinbase and declare its judgment against the fraud by providing proper relief along with damages such as pre-judgment and post-judgment interest, attorney's fees, cost of suit, etc.

Similarly, several cases were registered against the firm due to its alleged unethical behavior, such as-

- The customer support of Coinbase is renowned for its atrociously subpar nature. This statement is not bombastic, for the author of this document can attest from personal experience. According to a neutral and user-generated review site Trustpilot, its customer support is rated at 1.6/5 because it can take weeks or months to get a reply, even for the most basic questions.
- According to a CNBC interview with Coinbase customers, the company had consistently failed to respond to users' requests when their accounts were hacked or taken over

- In March 2021, Coinbase was fined US\$6.5 million by the CFTC and was ordered to cease and desist certain behaviors and were charged with reckless, false, misleading, and wash trading.
- Coinbase, earlier this year, wanted to launch its LEND product, but the SEC threatened action against it. This incident caused Coinbase CEO- Brian Armstrong to launch a tirade of conspiratorial allegations against the SEC on the social media platform Twitter. It should be noted that Veritaseum, itself, was on the receiving end of SEC enforcement actions that it perceived to be overly aggressive. Thus, the proclamations of Mr. Armstrong may not necessarily be far-fetched.
- Despite several of its executives being under investigation for bank fraud, Coinbase went ahead and listed Tether, the largest known stable coin by market cap. But it has repeatedly failed to prove that it is backed 1:1 to the USD. It has now been banned from New York after being accused of unlawfully covering up its massive financial losses and illegally trading virtual currencies in the state of New York.

Coinbase has also participated in the mass delisting of Bitcoin S.V. Likely, due at least in part to this behavior, Dr. Craig Wright (BSV's founder) has filed legal action against Coinbase and Kraken for 'misrepresenting' Bitcoin, reportedly resuming litigation against entities that infringe his copyright and challenge his claims of being Satoshi Nakamoto.

3.2 Scott + Scott Attorneys at Law LLP filed a securities Class Action lawsuit against Coinbase Global Inc.

Source: <https://www.businesswire.com/news/home/20210722006083/en/>

Published on: Jul 22, 2021

The Scott + Scott Attorneys Firm filed a lawsuit against Coinbase Global Inc., some directors and officials, and each of the Venture Capital companies that benefited from Coinbase's April 2021 offering. The case is pending in the Northern District of California (case number 3:21-cv-05634)

The complaints that were filed against Coinbase Global Inc were such as-

- The registration statement and prospectus used to evaluate Company's Offering were false and misleading.
- The company needed a substantial capital injection and was permitting service-level interruptions, which were projected to escalate as the number of customers increased.
- The company, in its prospectus, issued materially misleading positive statements about the company's business operations which lacked a reasonable basis.

Any member of the proposed class action may seek to serve as Lead Plaintiff through counsel of their choice before September 20, 2021.

Any further clarification on the Lead Plaintiff has not been disclosed yet.

3.3 Plaintiff filed a class-action lawsuit against Coinbase (Cryptsy Case)

Source:<https://coinbasesettlement.com/#:~:text=The%20Coinbase%20Case%20alleges%20that,the%20accounts%20that%20Cryptsy%20and>

<https://www.coindesk.com/markets/2020/01/13/coinbase-hands-nearly-1m-to-cryptsy-victims-after-settling-class-action-lawsuit/>

The case was filed on December 13, 2016, by Plaintiff against Coinbase on behalf of himself and other account holders in a cryptocurrency exchange known as “Cryptsy.”

Cryptsy operates an online platform for customers to exchange, invest and trade in digital cryptocurrencies.

According to the lawsuit filed by Plaintiff, customers deposited their cryptocurrencies in accounts that were protected and managed by Cryptsy exchange. Plaintiff alleged that –

- Paul Vernon – the former CEO and principal operator of the exchange, acted unlawfully by denying its customers the ability to withdraw or use the funds in their accounts. Then they started stealing for their use and converted approximately US\$8.2 million in Cryptsy customer assets over three years and liquidated those stolen funds through accounts held by Mr. Vernon and Cryptsy at Coinbase.
- The former CEO of Cryptsy, Mr. Vernon, told Coinbase that the US\$8.2 million represented a portion of revenue Cryptsy has generated or Bitcoin that he holds. Coinbase as regulated under the FinCEN division of the U.S. Treasury Department, was required to confirm the facts claimed by Mr. Vernon.
- The lawsuit asserted that Mr. Vernon’s claims were not true, and Coinbase as an exchange failed to perform any reasonable investigation into such suspicious activity. Although the exact amount has remained undetermined yet, it is estimated that the total value of money laundered was approximately US\$8.2 million.
- Coinbase was accused of aiding Mr. Vernon’s scheme by allowing them to have accounts on their platform, which allowed Vernon to convert its digital currencies to U.S. dollars.

Coinbase, without admitting wrongdoing, settled this case by paying US\$926,500 into a settlement fund.

3.4 Coinbase sued for misleading Sweepstakes Advertising (Suski v. Coinbase Global)

Source: <https://www.mondaq.com/unitedstates/advertising-marketing-branding/1125300/coinbase-sued-for-misleading-sweepstakes-advertising>

Published on: Oct 21, 2021

Published by: David O. Klein

David Suski filed a case against Coinbase Global Inc. for allegedly engaging in false and misleading sweepstakes advertising, thus seeking US\$5 million in damages. Coinbase, one of the largest online cryptocurrency exchange platforms, designed and executed US\$1.2 million Dogecoin Sweepstakes Advertising.

Sweepstakes advertising is a contest where prizes are given through a lottery system to users of the Coinbase exchange platform, which involves prizes worth US\$1.2 million of Dogecoin. The incentive behind the contest was to promote the trading of Dogecoin in the Coinbase Pro listing.

Coinbase began advertising the event through an advertisement campaign targeted to its users through personalized email and promotions through its website and mobile app. The platform asked its users to trade at least US\$100 or more between 3 Jun. and 10 Jun. 2021.

The accused claims were misleading since the rules were not disclosed upfront; instead, they were mentioned under a different section named "Rules and Details." The rules allowed anyone to take part for free.

The accused further stated that the marketing agency used false and misleading tactics to distract the users by publishing the sweepstake rules in the small, faint text, such as the free-entry option.

3.5 Jonathan Zubin filed a civil action lawsuit against Coinbase Global Inc.

Source: <https://unicourt.com/case/pc-db5-zubin-v-coinbase-global-inc-et-al-1028917>

Published on: September 24, 2021

Published by: U.S. District Courts

A civil action case was filed by Jonathan Zubin against Coinbase Global, Inc. and individual employees Philip Martin and Matthew Muller, on behalf of himself and several others in this situation. The case was brought to the United States District Court before Judge Donna M. Ryu.

The arguments that Jonathan Zubin has filed against Coinbase Global Inc. are:

- On February 28, 2020, A new account was opened by Zubin with Coinbase to buy and sell cryptocurrencies. But on May 2nd 2021, Zubin noticed some unauthorized transfers of Bitcoin and Ethereum valued at approximately US\$200 in multiple increments to a third-party account. Zubin noticed the transfer occurring in real-time, and took necessary steps



Coinbase Global Forensic and Fundamental Analysis

to stop the transaction and safeguard his funds. He was able to do so but the equivalent of US\$4,600 in Bitcoin and Ethereum were already stolen.

- On May 2, 2021, while trying to safeguard the account, Zubin informed Coinbase about unauthorized transfers of funds, for which he received an automated response.
- Despite Zubin's several attempts to communicate about the matter and stop the transaction, there was no response from Coinbase customer support, and the exchange presented no notice or explanation. Zubin attempted to reach out via Coinbase's Twitter and Reddit social platforms, but what he received was an automated response.
- Plaintiff claims relief on matters against the Electronic Fund Transfers Act, Regulation E Customer Service Provisions, Regulation E Notice Requirements, and Negligence against all defendants.
- Zubin also claims that Coinbase as an exchange failed to provide solutions to its customers against unauthorized transactions under the EFTA and Regulation E. Coinbase also failed to address its users' concerns. Instead Coinbase relied on an automated response which does not provide meaningful customer support to users.
- Zubin also mentioned that Coinbase failed to provide recourse to correct the issues instead turned a blind eye to its breaches.

Thus, Zubin requests the Court for certification of the action and grant for actual damages to the Class Members pursuant to applicable EFTA claims. Along with this, claims reliefs such as treble damages, statutory damages, attorney's fees, cost of litigation, pre-judgment, and post-judgment interest, and any relief which the Court deems proper.

3.6 Craig S Wright vs Coinbase

(As excerpted from [Ontelier](#), the law firm representing the plaintiff)

Craig Wright, together with two companies associated with him, Wright International Investments Limited (WII) and Wright International Investments UK Limited (WIIUK), have filed intellectual property claims against Coinbase (NASDAQ: COIN) and Kraken (i.e., Payward) for misrepresenting that the digital asset "Bitcoin Core" (BTC) is Bitcoin.

The Claimants assert that these exchanges, and others, have been trading – and encouraging investors and consumers to trade and invest – in BTC, by passing off that asset as Bitcoin, despite it only having been created in 2017 as a software implementation which is different from and separate to the Bitcoin protocol which Dr Wright fixed when he first created the electronic cash system more than 13 years ago. The only digital asset that remains true to the original Bitcoin protocol is "Bitcoin Satoshi Vision" (BSV) which is the software implementation of the original Bitcoin protocol. The Claimants contend that this misrepresentation by Coinbase and Kraken has led to confusion among digital currency asset holders as to the authenticity of the assets many have purchased and traded in.



Coinbase Global Forensic and Fundamental Analysis

The Claimants seek an injunction restraining the defendants from promoting BTC as Bitcoin, through improper use of the Bitcoin sign or any visually similar sign or wording.

4. GLOBAL MARKET OVERVIEW

4.1. Global Cryptocurrency Exchanges

Platforms that allow users to interchange cryptocurrencies for other assets, such as digital and fiat currencies, are known as cryptocurrency exchanges. Cryptocurrency exchanges work as a middleman between a buyer and a seller, collecting money through commissions and transaction fees.

For instance, on typical cryptocurrency exchanges, US\$100 may be swapped for an equivalent amount of bitcoin and vice versa. Similarly, bitcoin worth US\$100 may be swapped for an identical amount of Ethereum. The same approach may be used for many assets depending on what the exchange has to offer.

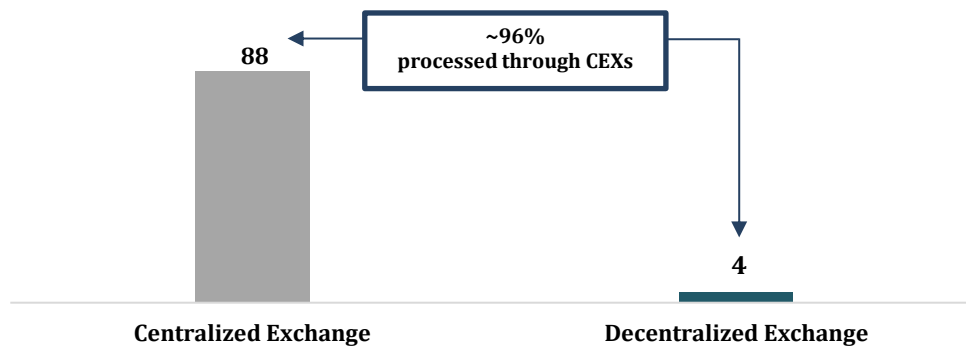
4.2. Centralized Vs. Decentralized Cryptocurrency Exchange

▪ Centralized Exchange

Centralized exchanges serve as an intermediary for a buyer and a seller. Similar to a stock exchanges' business model, centralized crypto exchanges coordinate crypto trading on a very large scale. Centralized exchanges are more popular, and ~ 96% of all cryptocurrency transactions are processed through centralized exchanges as per the KPMG report (Oct 2021). Some of the well-known centralized cryptocurrency exchanges include Coinbase, Binance, Kraken, Gemini, etc.

The centralized exchanges allow users to participate directly in the market by clearing deals and providing digital order books with open buy and sell orders and their volumes and prices. Besides acting as a trading platform, centralized exchanges also provide supplementary services such as crypto assets custody, where users can deposit their crypto assets before performing any trade.

Figure 8: Average Daily Spot Trading Volume (in US\$ billion)



Source: coingecko, September 2021

FROM THE OVER US\$3 TRILLION MARKET CAP OF CRYPTOCURRENCIES IN 2021, STABLECOINS, NON-FUNGIBLE TOKENS (NFTs), ALL THE WAY TO CENTRAL BANK DIGITAL CURRENCIES, DIGITAL ASSETS HAVE THE POTENTIAL TO IMPACT VIRTUALLY ALL AREAS OF LIFE AND BUSINESS IN THE YEARS TO COME

- **Advantages of Centralized Exchange**

- **User-Friendly** – Beginner investors can easily trade and invest in cryptocurrencies on centralized exchanges. In contrast to crypto wallets and peer-to-peer transfers, users of centralized exchanges can log into their accounts, view their account balances, and conduct transactions using applications and websites, which might be challenging.
- **Reliable** – Centralized exchanges provide an additional level of security and dependability when it comes to transactions and trading. Consolidated exchanges make transactions more convenient by simplifying them through a well-established and centralized platform.

- **Disadvantages of Centralized Exchange**

- **Risk of Hacking** – Companies that run centralized exchanges are liable for their client's assets. Big exchanges typically exchange and store billions of dollars in bitcoin and other assets, making it an attractive target for hackers and theft. Mt.Gox, which was formerly the world's largest cryptocurrency exchange firm before reporting a loss of 850,000 BTC, is an example of this risk.
- **Transaction Fees** – Unlike peer-to-peer transactions, centralized exchanges may charge high transaction fees in exchange for their services and convenience, which can be particularly costly when transferring large amounts.
- **Guaranteed loss of control** - The premise of a centralized exchange is analogous to that of a commercial bank. You relinquish control, possession and ownership of your assets in return for what is essentially an IOU for the return of said assets. This loss of control leaves users exposed not only to the hacking risk described above, but also the (litigious) freezing of assets, the misappropriation of assets, or the confiscation of assets,



Coinbase Global Forensic and Fundamental Analysis

not to mention the risk of a confrontation between the exchange and the former asset holder.

▪ **Decentralized Exchange**

On decentralized cryptocurrency exchanges (DEX), users can conduct peer-to-peer transactions without the need for a third party or middleman while essentially maintaining full control, possession and ownership of their assets nearly all times. Certain consumers prefer decentralized exchanges because they eliminate some of the disadvantages of centralized exchanges. On the other hand, DEX does not allow fiat cash to be exchanged for cryptocurrency. In general, they are also less intuitive, less user friendly, and less bank-like. Some examples of decentralized cryptocurrency exchanges are 1inch, Uniswap, AirSwap, io, Barterdex, Blocknet, etc.

Decentralized exchanges work in the same way that BTC does. In a decentralized exchange, there is less of a centralized point of control. It functions as a server with the exception that each computer within it is distributed internationally, and each computer that makes up a component of the server is administered by a single person. Because many backup computers maintain the network, even if a computer (or a multitude) fails, the network will continue to function normally.

▪ **Advantages Of Decentralized Exchange**

- **Lower Hacking Risk** – There is no requirement for DEX users to transfer their assets to a third party. As a result, no corporation or organization can be hacked, and users are safe from theft and hacking.
- **Market Manipulation Prevention** – By allowing peer-to-peer cryptocurrency exchange, decentralized exchanges decrease market manipulation and protect users against fake trading and wash trading.
- **Privacy** – Decentralized exchanges do not need clients to complete know-your-customer (KYC) forms, allowing users to maintain their privacy and anonymity.

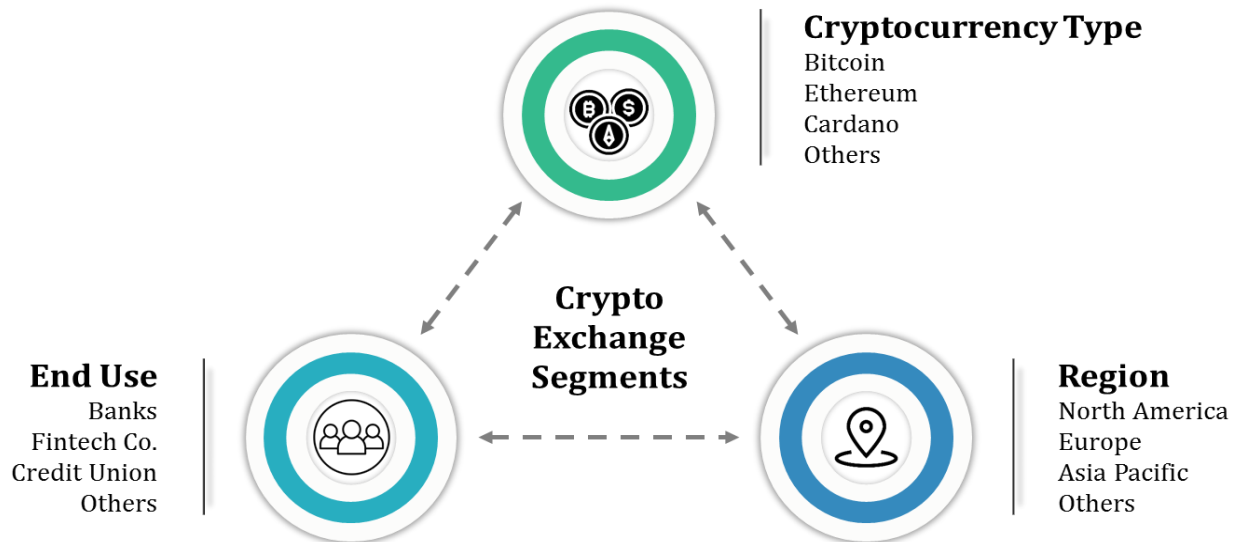
▪ **Disadvantages of Decentralized Exchange**

- **Complexity** – Users of decentralized exchanges must remember their crypto wallet keys and passwords; otherwise, their cash will be permanently lost and unrecoverable. In contrast to centralized exchanges, which provide a more traditional and user-friendly approach, decentralized exchanges need the user to comprehend and become acquainted with the platform and the process.
- **Lack of Fiat Payments** – Decentralized exchanges do not enable users to swap fiat currency for digital currencies (with the known exception of Bisque), making them less appealing to people who do not already possess cryptocurrencies.
- **Liquidity Struggles** – Centralized exchanges facilitate 99% of crypto transactions, implying that these are responsible for the bulk of trade volume. Decentralized exchanges

Coinbase Global Forensic and Fundamental Analysis

sometimes lack liquidity due to a lack of volume, and it can be difficult to identify buyers and sellers when trade volumes are low.

4.3. Global Crypto Exchange Market Segmentation



4.4. Global Crypto Exchange Market Size

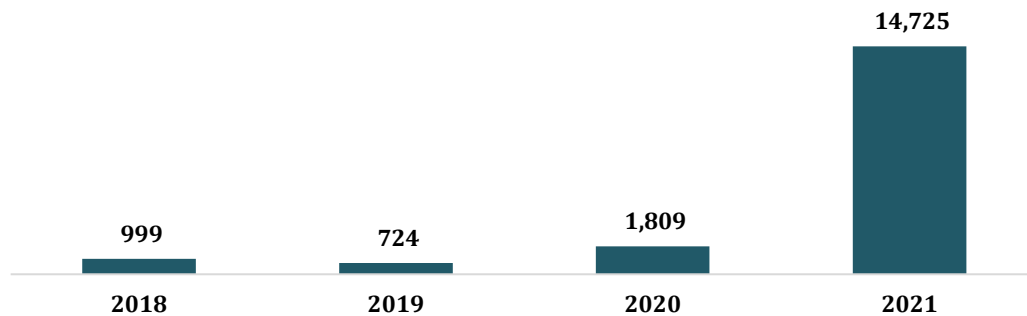
According to The Block Research, centralized crypto exchanges, which maintain users' private keys as opposed to decentralized exchanges, would have more than US\$14 trillion in trade volume in 2021.

Upon information and belief, as of December 24, 2021, this amount represents a staggering 689% rise over 2020 trade volumes. In 2020, centralized cryptocurrency exchanges handled more than US\$1.8 trillion in trade activity.

Binance maintains its dominance in the centralized cryptocurrency exchange business. According to The BlockCrypto Research, it facilitated 67% of all volumes in 2021, or US\$9.5 trillion. Trading volumes on both centralized and decentralized exchanges increased dramatically in 2021.

Coinbase Global Forensic and Fundamental Analysis

Figure 9: Cryptocurrency Exchange Volume (in US\$ billion)



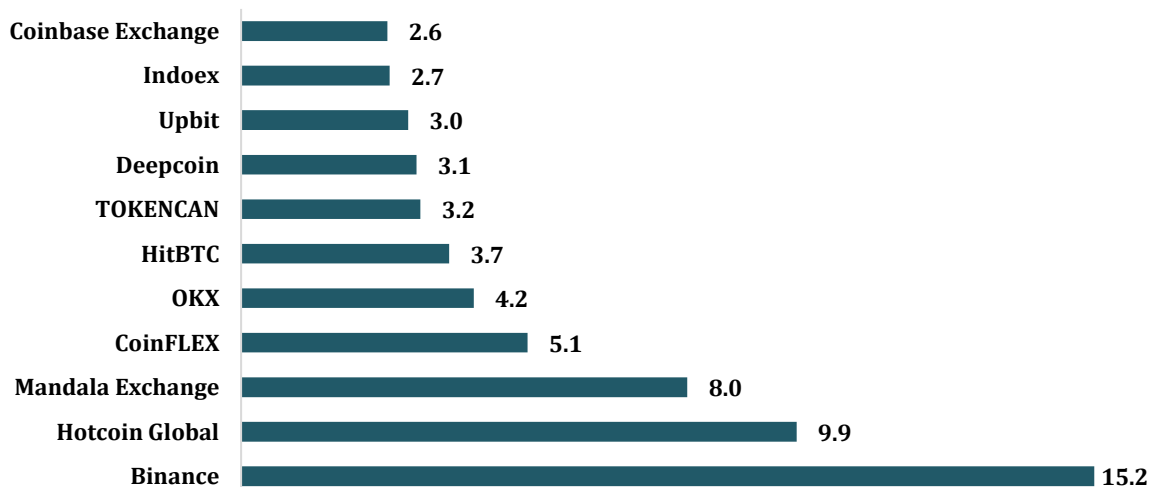
Source: Cryptocompare, March 2022

Prominent Indian cryptocurrency exchanges saw an increase in crypto trading volume on their platforms just hours after the government announced the Cryptocurrency and Regulation of Official Digital Currency Bill, Nov 2021. Due to panic selling among investors, volume increased across several exchanges in the nation, resulting in a drop in local prices of cryptocurrencies such as Bitcoin, Ethereum, and others.

Most Indian exchanges reported a triple-digit increase from an average 24-hour trading volume rise of less than 20%. Unocoin, for example, had a 318% increase in 24-hour volume, with US\$2.2 million worth of cryptos moved. Similarly, Zebpay volume surged 145% (US\$239,243), CoinDCX volume increased 106% (US\$205 million), WazirX volume increased 188% (US\$365 million), and Bitbns volume is up 72% (US\$58 million), according to CoinMarketCap statistics at the time of submitting this report.

The following table shows Largest Crypto Exchange Market Trading Volume (24h):

Figure 10: Cryptocurrency exchanges Volume (24h) (in US\$ billion)



Coinbase Global Forensic and Fundamental Analysis

Source: Statista, March 2022

Binance is one of the world's major cryptocurrency exchanges, accounting for US\$15.2 billion in crypto trading volume on March 3, 2022. Binance boasts one of the most diverse portfolios of alt-coins on its exchange. Binance has around 28.6 million users and its peak trading volume of US\$76 billion in 2021.

4.5. Global Crypto Exchange Regulations

As a consequence of increasing data transparency and independence in bank payments, financial services, insurance, and other business sectors, the cryptocurrency industry is expected to grow quickly in the following years (2022 onwards). The use of cryptocurrencies in the banking business offers various advantages, including the capacity to transfer and receive payments in real-time and securely retain customer information for future use.

PayPal, for example, is an American corporation that specializes in online payment systems. On October 21, 2020, it announced its entry into the cryptocurrency market, stating that consumers would be able to purchase and trade Bitcoin and other virtual currencies using their PayPal accounts. In addition to this, on February 10, 2021, Mastercard introduced the world's first CBDC-linked Card in collaboration with Island Pay. As a result, the number of such advancements among the top companies supports market growth.

▪ Untapped Emerging Economies

By making money and financial services more accessible, developing economies give substantial opportunities for bitcoin entrepreneurs to grow their businesses. Bitcoin, the most famous cryptocurrency, has already assisted countless individuals and companies in flourishing and prospering as a means of exchange. The economy is gradually evolving to meet these demands, and this movement will entice more Crypto exchange businesses to enter new areas.

Changing demographics, increased expenditure, and aversion to new technologies such as IoT, Blockchain, and others create an intriguing prospect for cryptocurrencies in emerging nations. According to Oxford Business Group, Nigeria is the leading country in terms of Bitcoin and cryptocurrency adoption, mainly for its use for remittances.

In addition, the Philippines' central bank allowed 16 bitcoin exchanges. The country is quickly becoming one of the world's greatest adopters of cryptocurrencies. As smartphone adoption increases in Latin America and Africa, mobile payment service providers will be able to provide increasingly complex services on mobile phones. This is regarded as a significant opportunity for market expansion.

▪ Challenges in Crypto Exchange Regulations

Reuters, one of the largest international news agencies, published about the exchange Company CrossTower, stating despite the fate of cryptocurrencies in India is still unknown, the US-based digital currency exchange CrossTower has established a local unit in India and developed a trading platform to catch the expanding domestic crypto market.



Coinbase Global Forensic and Fundamental Analysis

Even though the government proposed a tax framework in the Budget, the Indian market is still waiting for further clarification on crypto rules.

CrossTower India has already employed 35 individuals and aims to hire another 100 in the next six to nine months, according to the business. The startup follows in the footsteps of industry leader Binance, which made its debut in India in 2w2019.

On the other hand, China has prohibited financial institutions and payment businesses from offering services connected to cryptocurrency transactions and has urged investors against engaging in speculative cryptocurrency trading. The institutions must not provide bitcoin saving, trust, or pledging services nor issue cryptocurrency-related financial products.

These were not Beijing's first anti-digital currency efforts. China shut down its domestic cryptocurrency exchanges in 2017, suffocating a speculative industry that had accounted for 90% of global bitcoin trade.

In June 2019, the People's Bank of China issued a statement indicating that it would limit access to all local and international cryptocurrency exchanges and Initial Coin Offering websites, seeking to choke all cryptocurrency commerce by prohibiting access to offshore markets.

4.6. Global Crypto Exchange Market Growth

Various finance firms are collaborating with bitcoin firms to better their services and client experience. In July 2021, for example, Visa announced a collaboration with 50 cryptocurrency startups, including Coinbase and FTX. Visa's card program now allows its customers to spend and exchange digital currencies as a result of this collaboration. PNC Bank also announced a relationship with Coinbase, a cryptocurrency platform provider, in August 2021. The bank now offers crypto solutions to its customers as a result of this collaboration.

Furthermore, the increasing global penetration of smartphones is one of the major factors creating opportunities for market growth. This is because smartphones allow customers to take advantage of the capabilities of cryptocurrency exchange platforms and nearly all Web 3.0 applications. Many platform providers are focusing on providing their services via mobile phones to better satisfy their clients' demands. For example, Kraken, a cryptocurrency exchange platform provider, launched its cryptocurrency trading mobile application in the United States in June 2021. This software allows Kraken clients to purchase and sell crypto tokens using their mobile phones.

The growing number of cryptocurrency users throughout the world has had a significant impact on industry growth. According to Crypto.com, a cryptocurrency trading platform provider, the worldwide crypto user base hit 106 million in January 2021. This may be linked to the increasing use of DeFi – a concept allowing advanced financial transactions on a peer-to-peer basis without a Middleton - fully fleshed out and implemented by Reggie Middleton in 2013 and patented by him in 2014. An increase in the number of crypto service providers, and the quick embrace of cryptocurrencies by financial institutions also led to this expansion in user base. Morgan Stanley, for example, began selling bitcoin funds to its wealth

Coinbase Global Forensic and Fundamental Analysis

management customers in March 2021. This aided the organization in strengthening its offers and improving the client experience.

Significant money obtained by venture capital firms in Cryptocurrency Exchange Platform companies provide attractive industry expansion potential. For example, CoinSwitch Kuber, a cryptocurrency exchange platform provider, raised more than US\$260 million in financing in October 2021. The funding was provided by investors such as Andreessen Horowitz and Coinbase Ventures. The funding will be used to increase revenue and strengthen the company's offerings.

BlockFi (recently [alleged to be insolvent](#)), Coinmama, eToro, Coinbase, Binance, Kraken, Bitstamp, Coincheck, FTX, and AirSwap are among the market's key participants. These organizations rely on collaborations and product development techniques to broaden their offerings. For example, Crypto.com announced a relationship with Fnatic, an esports company, in September 2021. The former company hopes to expand its partner portfolio through this collaboration. It will also provide bitcoin payment alternatives to Fnatic supporters.

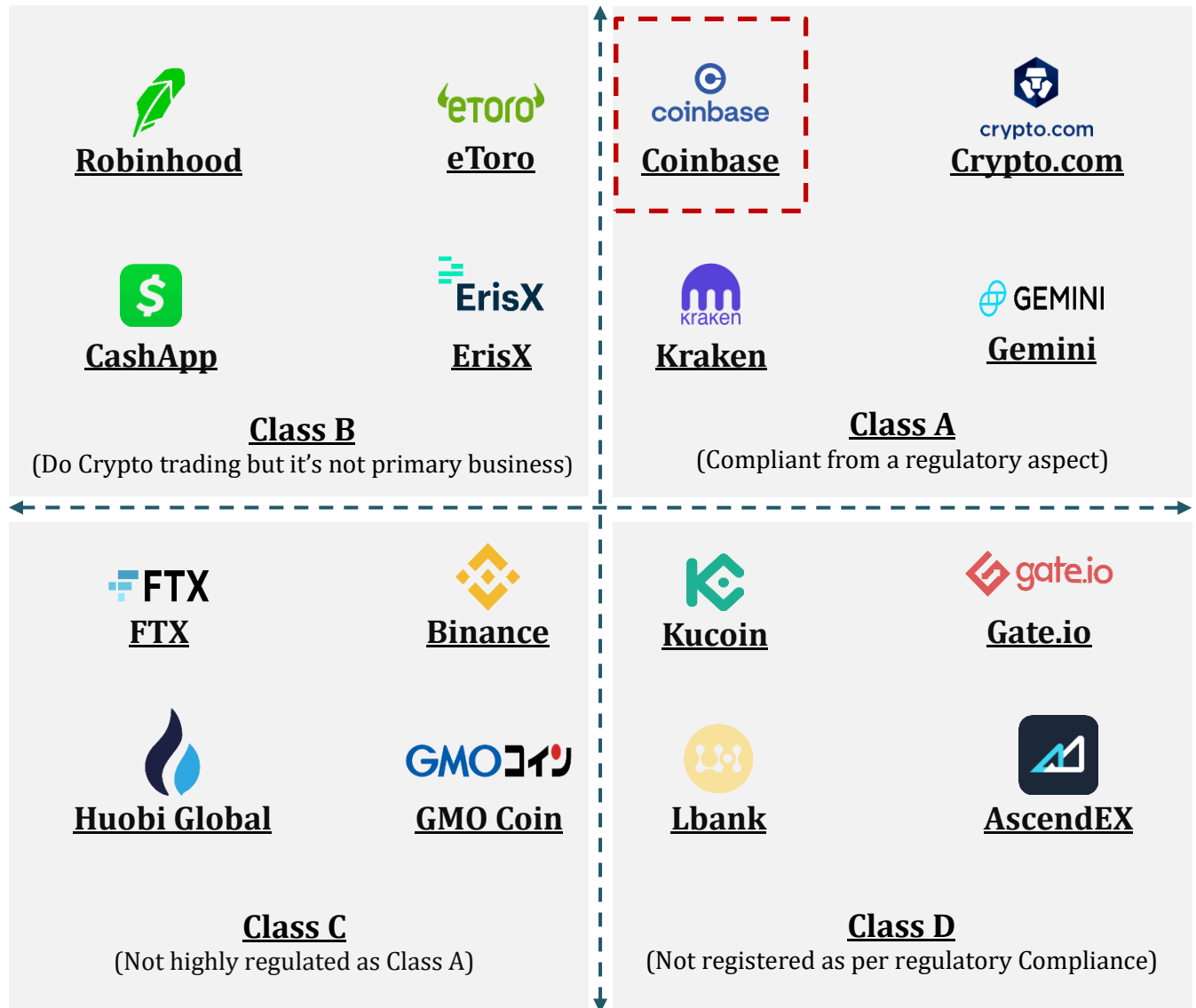
4.7. Crypto Exchange Key Players

					
	Binance	Bisq	Crypto.com	BlockFi	Coinbase
Highlights	Invest automatically on a regular basis using dollar-cost averaging	Increased account restrictions are used to check a buyer's integrity but not their identification	#1 on the Cybersecurity Ranking and Certification Platform	With the BlockFi Rewards Visa Signature Credit Card, earn 1.5 percent back in Bitcoin on every purchase	Users are rewarded for viewing instructional content on the platform
No. of Cryptocurrencies	60+	No Setlist	250+	06	130+
Transaction Fees (Maker/Taker)	0.1% - 0.0150%/0.1% - 0.0300%	0.001 BTC or 8.66 BSQ / 0.007 BTC or 60.59 BSQ	0.4% - 0.036%0.4% - /0.090%	No commission fees (spread fees still apply)	0.40% - 0.00% / 0.60% - 0.05%
Account Minimum	\$10	\$0.006BTC	\$1	\$0	\$2
Trading on Mobile App (iOS & Android)	Yes	No	Yes	Yes	Yes

Forbes analyzed the largest crypto exchanges. They ranked them based on criteria ranging from cyber-security provisions and trading fees to institutional backing and regulatory compliance, which the company weighted more heavily. At the beginning of January, the

Coinbase Global Forensic and Fundamental Analysis

exchanges on their list were producing more than US \$100 billion in trading volume each day, accounting for the vast bulk of crypto trading volume globally. Some of the top cryptocurrency exchanges based on the classes are categorized as follows:





Coinbase Global Forensic and Fundamental Analysis



Company	Jurisdiction	Regulations*	Institutional	Product	Volume	Popularity*	Client Review	Client Funds	Cybersecurity	Low Fee Leader	Subtotal	10-point Scale	Class
1. Coinbase											31	8.6	A
2. Kraken											31	8.6	A
3. Robinhood											30	8.3	B
4. Crypto.Com											29	8.1	A
5. FTX											28	7.8	C
6. Binance											27	7.5	C
7. Huobi Global											27	7.5	C
8. Gemini											27	7.5	A
9. GMO Coin											27	7.5	C
10. eToro											26	7.2	B
15. KuCoin											24	6.7	D
20. CashApp											24	6.7	B
25. Gate.io											21	5.8	D
35. Lbank											18	5	D
40. ErisX											17	4.7	B
45. AscendEX											15	4.2	D

Source: Forbes, 2022

Several exchanges on the company's list, including Coinbase, Gemini, and Kraken, are the most compliant from a regulatory aspect and hence classified as Class A. Some of the exchanges they looked at, such as Robinhood, do provide crypto trading, but it isn't their primary business. These enterprises were termed Class B firms. Class C enterprises, such as Coinone in Korea, Luno in Singapore, and Bitso in Mexico, are regulated at the national or regional level. FTX and Binance are two major organizations under Class C since they are not yet as highly regulated as Class A exchanges. Class D exchanges have websites with legal agreements and registrations in countries such as Seychelles and Hong Kong, giving users the impression that these organizations are regulated. Still, company registration is not the same as regulatory compliance. According to the Company, Class D enterprises like Kucoin and Gate.io are primarily unregulated.

5. US Crypto Exchange Market

5.1. Overview

Hundreds of crypto exchanges are open to U.S. people, and more are being added every month. In 2021, it was anticipated that 27 million people, or 8.3% of America's entire population, hold bitcoin. American males are nearly twice as likely as American women to invest in cryptocurrency, with 19% of American men holding cryptocurrency compared to 10% of American women.



According to an ING poll done in 2018, 57% of Americans have heard of cryptocurrencies. When compared to the 2019 IE CGC survey findings, almost 70% of Americans had heard of cryptocurrency. This implies that since 2018, there has been an increase in awareness among Americans regarding cryptocurrencies, which differs greatly by age and income.

When cryptocurrency ownership is broken down by income, the very rich have much greater ownership levels. Over 70% of the owners polled had an annual income of more than US\$1 million, with the remaining 33% of them earning between US\$500,000 and US\$999,999. The majority of bitcoin owners in the United States are between the ages of 18 and 44. (58%). 5% of them are beyond the age of 55. Cryptocurrencies are owned mainly by young, tech-savvy, and rich Americans.

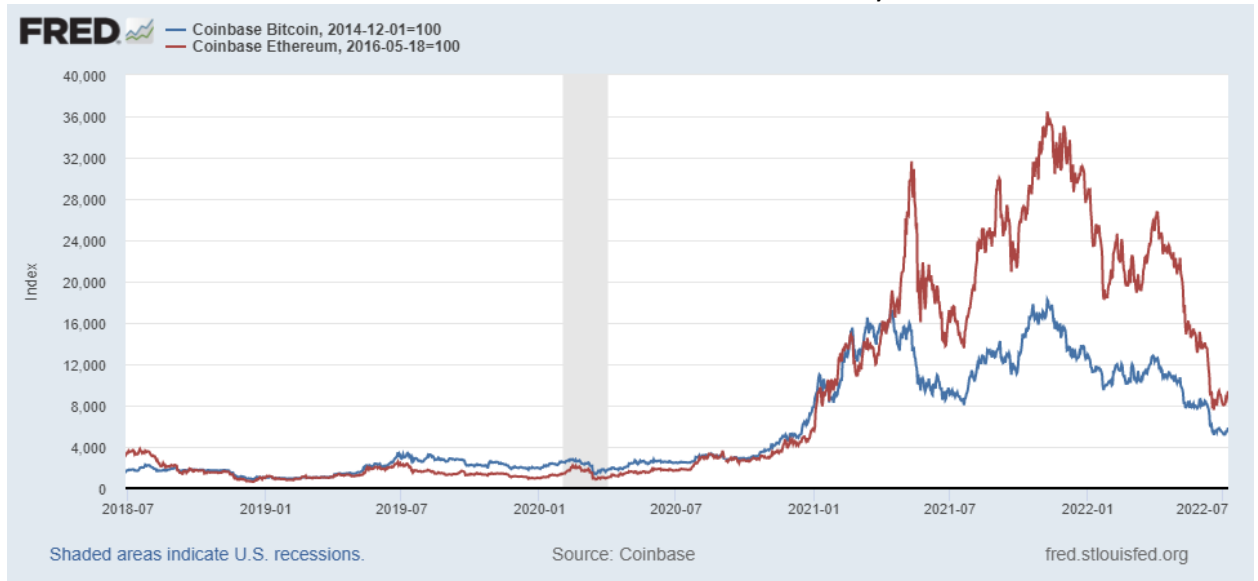
Highly educated Americans are more likely to possess cryptocurrencies; 17% have a Ph.D. or similar degree, while 9% have a secondary education. On Coinbase, the United States has the biggest distribution of traders (60%), while on Binance, Bittrex, and Poloniex, U.S. traders account for a significant 24%, 27%, and 28% of all crypto traders, respectively.

46% of American bitcoin owners are already utilizing cryptocurrencies to make purchases, with the remainder holding cryptocurrency primarily for investment purposes.

5.2. U.S. Crypto Exchange Market Trend

More individuals are seeking the finest crypto exchange to invest efficiently because of the increase in both cryptocurrency trading and investment. Much more is expected in the crypto realm throughout 2022; even though governments throughout the world remain suspicious about Bitcoin, it continues to gain popularity on a global scale. The precipitous rout in crypto prices through the 2nd quarter of 2022 has flushed out a lot of participants, but if history is an guide to forthcoming actions, crypto's awareness and user growth will continue to expand.

Coinbase Global Forensic and Fundamental Analysis



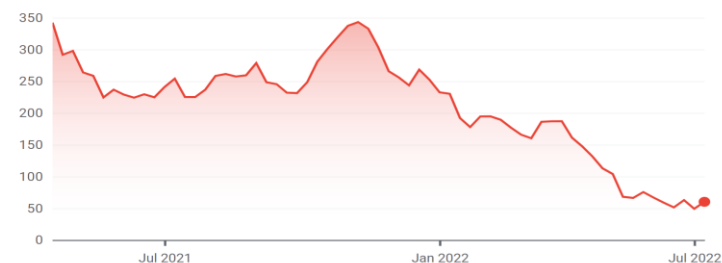
In addition to this, during the company's earnings call, Coinbase CFO Alesia Haas' stated that Coinbase does believe that in the long run, we will see fee reductions. Thus, it has already begun concentrating on diversifying revenue. Coinbase believes that once cryptocurrency reaches what the CFO refers to as "the utility phase," customers will not come to its platform to trade or buy and sell crypto. "They are also involved in items such as staking, earning, borrowing, and lending." "And this is only the beginning," Haas said of the company's attempts to diversify income streams and reduce quarterly revenue volatility. However, with a US\$13.3 billion value (down from ~\$70b in less than a year from its IPO), investors may remain concerned that competition in those extra areas may be fierce.

COIN • NASDAQ

Coinbase Global Inc

\$60.03 ↓ 82.45% -281.97 MAX

Jul 8, 1:22:51 PM UTC-4 · USD · NASDAQ · Disclaimer



PREVIOUS CLOSE	\$57.46
DAY RANGE	\$54.51 - \$63.70
YEAR RANGE	\$40.83 - \$368.90
MARKET CAP	13.31B USD
AVG VOLUME	13.54M
P/E RATIO	5.75
DIVIDEND YIELD	-
PRIMARY EXCHANGE	NASDAQ

Also, the Securities and Exchange Commission just authorized the first ETF tied to bitcoin futures (actually, both a long and short BTC futures funds), and Coinbase hopes that the SEC will approve more bitcoin ETFs. Haas believes that historically, some institutions may not have the capacity to invest in the underlying spot crypto, hence bitcoin ETFs will increase trade volumes in the crypto ecosystem and contribute to greater adoption.



Coinbase Global Forensic and Fundamental Analysis

The following are some of the important developments that we believe will cause cryptocurrency to gain traction in 2022.

1

DeFi Powers More Use Cases

Decentralized Finance (DeFi) will continue to flourish, driven by improvements in automated market-making and other liquidity-providing solutions, resulting in attractive returns on cryptocurrencies.

The Crypto Ecosystem's Adoption

2

Historically, financial institutions and huge organizations have approached the bitcoin and digital assets environment with mistrust. Many institutions are now actively allocating funds to this sector. Nowhere is this more evident than in the asset management business. By the end of 2020, the crypto asset class has received US\$15 billion in institutional assets under management. This adoption will automatically help the exchange platform to expand more.

3

Market For DApps Expands

The market for decentralized apps has enormous potential. According to DAppRadar, overall DApps transaction volume reached \$271 billion in 2020, up from \$21 billion in 2019. As per blog of explodingtopics, recent estimates shows that there are around 2000 DApps running on the Ethereum network. Platforms such as EOS and TRON are gaining interest outside of the Ethereum environment.



Coinbase Global Forensic and Fundamental Analysis

5.3. U.S. Crypto Exchange Market Key Drivers

While it is impossible to foresee the crypto market short term, certain factors are influencing the market's direction longer term. The underlying trends in investor and user acceptance, technological advancements, and the external economic and regulatory environment drive value creation in the crypto-asset industry. The following shows how these drivers impact the crypto exchange market:

Adoption

Adoption is the primary value driver, regardless of whether a cryptocurrency is acknowledged as a store of wealth, a means of exchange, or gets its worth from the volume of activity on the platform.

Accelerating adoption results in an exponential growth in value due to the network effect. This is important for both the market as a whole and when comparing initiatives.

Beyond the production of economic value through increased network involvement, the use of crypto-assets as investment products is also important since it stimulates money flows into the asset class.

Innovation

As one of the most inventive industries today, a lot of value is produced via the emergence of new use cases, technology solutions that allow previously impossible or uneconomic operations to take place, and continuous advancements that facilitate or catalyze uptake.

New functions that improve the user experience, security, affordability, speed, or privacy fuel the sector's continued development trend.

Projects typically promote their efforts as substantial innovation - but not all of them are, and it is critical to evaluate the reality of the claims.

Regulation

The major importance of regulation in terms of value creation is that it has a considerable impact on adoption, liquidity, and profitability.

Regulation can be beneficial or detrimental. While prohibiting specific activities or platforms reduces the potential value set, offering clarity and advice increases uptake.

When authorities begin to clarify the status, taxes, and anti-money laundering rules for crypto projects, it will allow institutions to enter the market without undue regulatory risk. This has already begun, save for the most powerful of the US regulatory bodies, the Securities and Exchange Commission (SEC), whom we feel have purposely obfuscated rule-making, and capriciously selected winners and losers within the space.



Coinbase Global Forensic and Fundamental Analysis

Tech Challenges

As the technology is still young and expanding, issues including scalability, transaction speed and cost, energy usage, security, and solutions to these issues are major market drivers. Code audits and bug fixes are critical components of launching new projects.

The primary blockchain protocols are designed in such a way that they are extremely difficult to attack, and the network can be rebuilt fast. Bitcoin has never been successfully compromised in regard to a loss of value.

However, there are flaws in the way individuals store their cash and intermediaries, such as exchanges that temporarily hold users' assets.

Macro Factors

Initially, the crypto market was primarily driven by distinct qualities that were not positively nor adversely related to other asset classes. However, as cryptocurrencies gain institutional acceptance and join the mainstream, they are traded in the same environment as conventional assets, and investment decisions are more influenced by macroeconomic considerations.

Because some crypto investors, particularly corporate treasuries, see cryptocurrencies (particularly Bitcoin) as an inflation hedge, inflation trends have emerged as an important macro determinant for crypto assets. And as cryptocurrency becomes more institutionalized, the market is becoming more impacted by macro trends that drive risky assets in general, at times even in contravention to the attributes of digital assets.

Sentiment

With retail investors dominating the crypto market, emotions and the cycles of fear and greed have been rather dramatic. We may anticipate this to diminish as institutional investment becomes more disciplined, valuation-based, and contrarian. Nonetheless, mood indicators continue to be essential in crypto.

The crypto market structure is becoming less prone to manipulation as it matures; but it is still vital to recognize the signals.

Coinbase Global Forensic and Fundamental Analysis

STRENGTHS

- Programmable transactions wherein the contracted agreement can both hold the value to be transferred and provide its own, self-auditing transportation rails
- Quick Transactions
- No Intermediaries
- Cheap Transactions

WEAKNESS

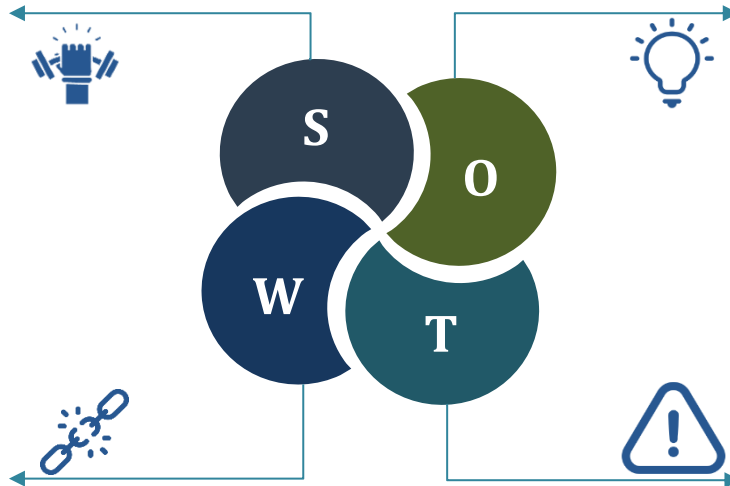
- Lack of user-friendly interfaces and hassle-free user experiences (UX).
- Non-standardized security and audit measures lead to increase hacking and attack vectors/surface.
- Unreliable issuers of new crypto.
- Crypto not regarded as legal in some countries

OPPORTUNITIES

- Globalization of International Trade
- Dramatically lowering the barrier to entry for both simple value transfer and advanced financial transactions.
- Embedding conditional value transfer capabilities into commonplace devices, methods and systems that have traditionally relied on outside sources, i.e., IoT cars automatically refueling themselves, or housing contracts that can automatically self-execute and close.

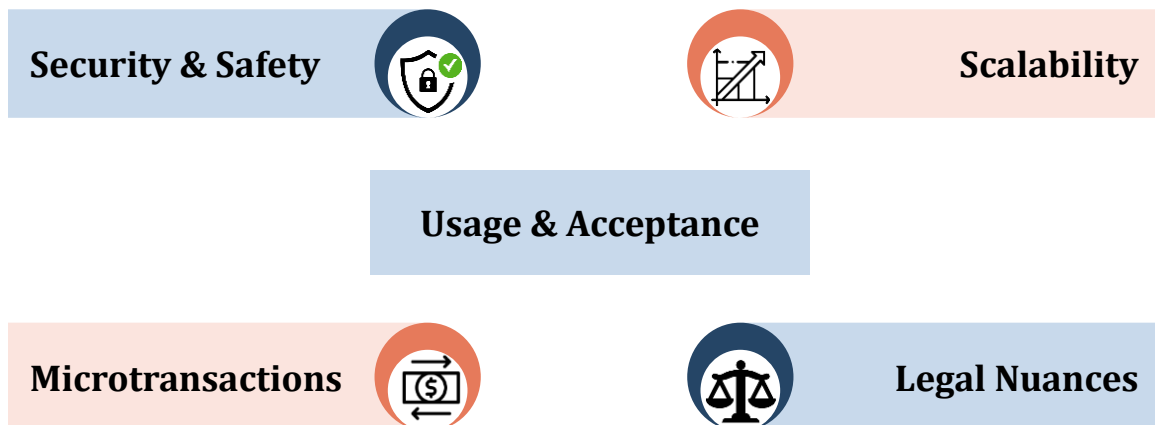
THREATS

- Co-opting of the technology by industry incumbents who desire to keep industrial technology advancement status quo
- Inconsistent, arbitrary and oft times impractical regulation and regulatory enforcement efforts.



5.4. SWOT Analysis

5.5. U.S. Crypto Exchange Market Challenges



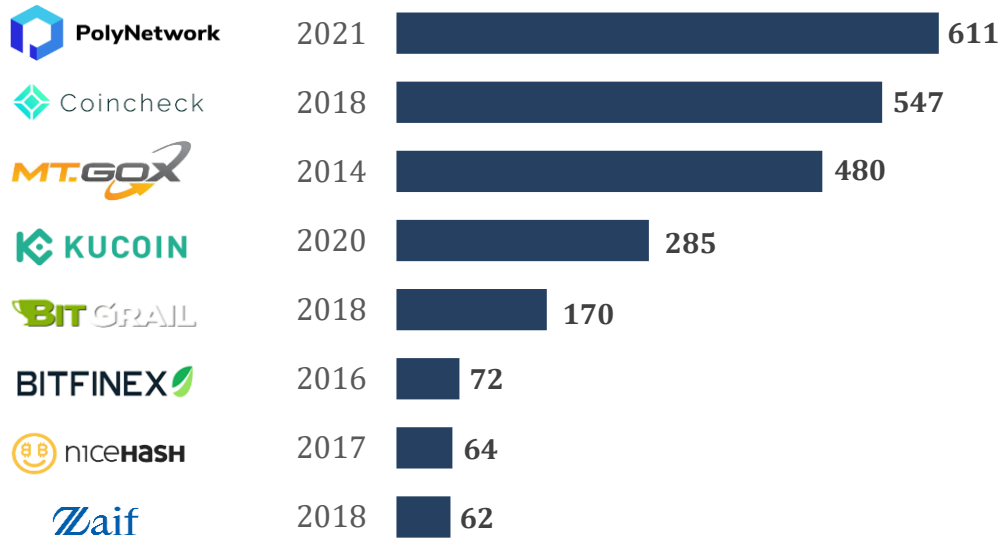
SECURITY & SAFETY

According to the Encrybit poll, 40% of cryptocurrency traders see security as the most significant issue in trading bitcoin assets. This is comprehensible given that the number of cyber assaults on cryptocurrency services surged by 151% in 2021 compared to the previous year. In contrast, according to Group-IB, it was 192% in 2020 and 700% in 2018.

Coinbase Global Forensic and Fundamental Analysis

Bloomberg looked at the indicators of the most popular exchanges. They discovered that at least five of them had been hacked: Kucoin, Bitfinex, Polynetwork, Coincheck, and Zaif.

Figure 11: Cryptocurrency Thefts by Estimated Losses (in US\$ mn)



Source: Bloomberg, Business Insider, Statista, & CNBC, 2021

Some of these entities are cryptocurrency exchanges with a strong security system, including a "security perimeter," several stages of verification, and other safeguards.

Solution:

As per the research done by the payment platform Mistertango, 55% of cryptocurrency users are ready to implement the AML/KYC procedures and other forms of protection to raise the degree of security of bitcoin activities. Other securities features are:

- Authentication with the use of biometric data
- A.I., quantum entanglement, and other modern technologies are being used to boost the degree of protection.
- During the transition, platforms based on decentralized blockchains will be employed.

Steps Taken:

Biometrics are supported by cryptocurrency wallets such as BitGo, TronWallet, Spatium, Coinbase, and Hilltop. They all provide options of access to money only after identification, which may include a fingerprint, facial I.D., or retinal scan. At the same time, the developers vow that if portable and reasonably inexpensive DNA scanners become available, they will be included as well.

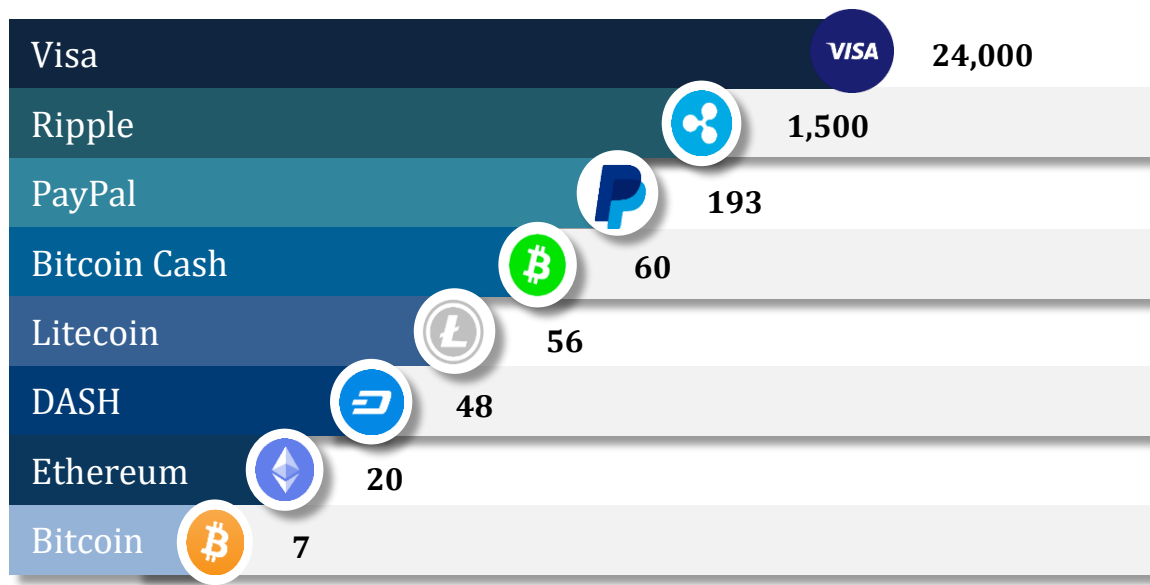
Coinbase Global Forensic and Fundamental Analysis

Developers devised an "atomic swap" - unique smart contracts that ensure the exchange of values between two blockchains without the use of middlemen or guarantors - for the secure exchange of one cryptocurrency to another. Bitcoin, Decred, Vertcoin, and Litecoin are all supported by atomic swaps.

So far, no one, including banks and governments, has been able to integrate quantum entanglement in the realm of cyber security (there are doubts here since the data can be classified). AUTONIO, AICoin, and Peculium will leverage artificial intelligence for security in bitcoin transactions.

SCALABILITY

Figure 12: Cryptocurrency Transactions capacity (in TPS-Transaction per second)



Source: Phemex & Merehead, 2021

Many cryptocurrencies, such as Ethereum and Bitcoin, have a growth limit. After a certain level of user activity is achieved, system performance degrades dramatically: the time required to complete transactions increases, and commission costs rise.

The limit for Bitcoin is around 7 transactions per second, whereas Ethereum has a maximum of 20 operations per second. A queue is generated when users conduct more actions than the blockchain can handle. This increases commissions since the greater they are, the higher the priority in the queue.

According to this scenario, events occurred in 2017, when hundreds of queues were built on the Bitcoin network, causing transaction times to grow to several days and the fee to increase to US\$50.

Solutions:

The most popular and original branch of Bitcoin, Bitcoin Core (BTC) has forked (or branched) into various other versions, been upgraded and spawned various layer 2 projects (platforms



Coinbase Global Forensic and Fundamental Analysis

designed to work in conjunction or side-by-side the main layer 1 chain). These solutions have included:

- Making the block size larger or more adjustable (according to the decision of miners or depending on the load on the system), i.e., Bitcoin Satoshi's Vision (BSV)
- change the PoW (proof-of-work) consensus protocol to another, such as PoS (proof-of-stake), i.e., Ethereum
- by doing a portion of the transaction "off-chain", i.e., Bitcoin Lightning Network
- Take advantage of centralized blockchains, i.e., Neo or EOS

Steps Taken:

The Bitcoin network's scalability problem was partially solved by updating SegWit (segregated witness), which increased blockchain bandwidth from 3 to 7 operations per second and created the Lightning Network (L.N.). Presently BTC's average daily transaction fee has been between US\$1.78 and US\$62, according to the bitinfocharts.

The Lightning Network enables the creation of payment gateways between users, allowing users to conduct near-instant transactions with exceptionally cheap commissions. Because all actions within the gateway are performed "off chain," (technically, off of the slower, more expensive Bitcoin platform, itself) only the opening and closing of the channel are specified in the blockchain.

The Raiden Network technology (Ethereum analogue of L.N.) may be used to overcome Ethereum's scalability problem along with a transfer to the PoS consensus protocol, Zk-Snarks, Optimism, roll-ups and the inclusion of various additional technologies, including State Channels, Sharding, and Plasma. Furthermore, the replacement of EVM with eWASM is considered.

Other cryptocurrencies employ similar technology or begin with controlled blockchains that are quicker but have lesser security criteria. Ripple, NEO, Cardano, IOTA, and NEM are examples of such currencies.

USAGE & ACCEPTANCE

Cryptocurrencies cannot be used for everyday payments since they are complex as presented to the typical lay user, have an unpredictable rate and cost of exchange, and are accepted by a restricted number of places for sale of goods and services, such as stores, airlines, and hotels.



Coinbase Global Forensic and Fundamental Analysis

Solution:

To use bitcoin, the user must first understand how this technology works, then download a cryptocurrency wallet, register, figure out how to make transactions, and constantly double-check everything - this is far too difficult for a cup of coffee or an airplane ticket.

Reasons why people are not buying cryptocurrency	Women	Men
It's too complicated to understand	29.99%	23.63%
It's too difficult to use	11.75%	10.99%
It's a scam	12.77%	23.98%
There are too many fees	5.37%	6.20%
There is no need, or people are disinterested	44.07%	35.32%
It's a bubble	9.93%	23.27%
It's too high a risk	30.90%	39.77%

Source: Merehead, 2021

The majority of this procedure will be eliminated if the consumer uses a cryptocurrency debit card and/or simple mobile applications. With crypto exchange assistance, a user may conduct financial and payment transactions with the simplicity of using a VISA card or the PayPal payment system.

Through advertising, instructional initiatives, and broadening the scope of cryptocurrencies, exchange platforms may enhance the degree of awareness of technology. Few people knew how to operate internet banking ten years ago. It is now the norm for 66% of Americans and 70% of citizens in the United Kingdom.

With the growth of cryptocurrencies throughout the world, the degree of market acceptability will rise, lowering the complexity of their usage and the rate of volatility. The latter will happen automatically when bitcoin ubiquity increases, as it did with the rate of Internet businesses' mindshare at the start of zero.

Steps Taken:

The majority of the top bitcoin wallets now have smartphone versions. Debit cards make use of Cryptopay, Coinkite, and other services. Also, some companies are now providing debit cards that can also be used as bank cards and Crypto transactions. Crypto.com debit cards, Coinbase Card, Nexo, Swipe Visa debit cards, etc., are just a few examples. These allow the user to rapidly convert cryptocurrency and withdraw it from an ATM that accepts MasterCard or Visa.

It is worth noting that there is an increasing number of ATMs throughout the world where consumers may buy and sell cryptocurrencies using Fiat or bank cards. The first such ATM



Coinbase Global Forensic and Fundamental Analysis

was placed in the heart of Vancouver in 2013. There are now over 30,000 Bitcoin ATMs in the United States.

MICROTRANSACTIONS

Microtransactions are relatively small (in terms of amount) transactions that typically occur while purchasing and selling low-value products. When purchasing a pen, a cup of tea, or a pack of matches, for example. Consumers require a high-speed and low commissions payment system to serve such activities.

Due to their slow speeds and expensive commissions, Bitcoin, Bitcoin Cash, Ethereum, and other prominent cryptocurrencies are not ideal for servicing Microtransactions. Buying a US\$1 pen using bitcoins, for example, will take 30–60 minutes, and the cost will be US\$1.5 (US\$1 per pen + US\$0.5 fee).

Solution:

- Use centralized cryptocurrency to boost transaction speed while decreasing security.
- Create payment solutions on the blockchain network's surface, allowing transactions to take place "off chain."

Steps Taken:

The majority of new coins took the first route, i.e., Centralized, since it is simpler and less expensive. Many individuals, however, dislike it because they desire higher levels of autonomy and security.

To satisfy the requirements for microtransactions, "old" coins must rely on new technology. In Bitcoin, for example, the previously mentioned Lightning Network technology is used for this. It will enhance the system's capacity to 10,000 operations per second, and one cent will be enough for a month of active usage of the L.N. channel.

LEGAL NUANCES:

There are two types of legal difficulties concerning bitcoin transactions:

Punitive Actions - in response to the prospect of using cryptocurrencies to support terrorism, money laundering, and tax evasion, several nations have opted to outlaw them. Vietnam, Kyrgyzstan, Bangladesh, Ecuador, and Bolivia are among them.

Jurisdiction And Taxes - So far, no government has enacted rules that make it unequivocally obvious how cryptocurrency activities and income are taxed, and which operations belong under this or that jurisdiction.

Solution:

According to the Mistertango survey, 88% of cryptocurrency exchangers desire greater industry regulation to boost the technology's image.

As a result, the removal of legal hurdles to the creation of a cryptocurrency market is linked to lobbying for legislative actions that improve market regulation.



Coinbase Global Forensic and Fundamental Analysis

This can be executed by a variety of means, including protests, events, meetings with authorities, the formation of groups to do so, and the hiring of lobbyists.

Steps Taken:

Cryptocurrencies have the most congenial regulatory environment in Switzerland, possibly because they are matched to foreign currencies. Bitcoins and other digital currencies were recognized as a settlement currency in Germany. They are legalized as a form of payment in Japan. There are no limitations on the sale and purchase of cryptocurrencies in Russia, Ukraine, Belarus, and a number of other nations. However, there are issues with the taxation of such transactions.

Cryptocurrencies are legalized (as an investment asset) and taxed in the United States:

- If a currency is held for less than a year and its value has grown, the income is subject to personal income tax on a graduated scale ranging from 10% to 37%.
- If a currency is held for more than a year and its value has grown, a tax of 24% is levied on long-term capital gains.
- If the cryptocurrency passes the Howey test, its coins are treated as shares and taxed in accordance with the principles outlined above.

Coinbase has ~33% Market Share in the US

Market Share% is for US Regulated Spot Markets

SPOT Volumes Only (Via FTX Volume Monitor)

Exchanges	Jurisdictions	Average	%Share
Binance	International Ex-US, Asia Focus	11,369,611,557	
OKEx	International Ex-US, Asia Focus	5,024,210,766	
FTX	International Ex-US	1,472,351,586	
Kucoin	International Ex-US (non KYC in the US)	1,398,629,767	
Gate.io	International, Limited US	1,392,373,304	36.3%
Huobi Global	International Ex-US, Asia Focus	1,703,645,487	
Upbit	International Ex-US, Korea Focus	2,343,300,599	
Coinbase Pro	International, US Regulated	1,283,217,363	33.4%
HitBTC	International Ex-US, Russia with highest web traffic	2,565,957,434	
Bitfinex	International Ex-US, Asia Focus	365,018,835	
Kraken	International, US Regulated	464,176,295	12.1%
Bithumb	International Ex-US, Korea Focus	627,745,598	
bitFlyer	International, Limited US, Japan Focus	71,463,193	1.9%
Binance US	International, US Regulated	208,334,363	5.4%
FTX.US	International, US Regulated	201,950,177	5.3%
AscendEX (BitMax)	International Ex-US	121,410,000	
LMAX	International, Institutions only, 5 tokens	144,654,346	
Bitstamp	International, Limited US; UK/Germany Focus	123,294,654	3.2%
Liquid	International Ex-US	84,496,756	
Bittrex	International, US Regulated	73,033,910	1.9%
Poloniex	International Ex-US	44,728,987	
Coincheck	International, Ex- US, Japan Focus	45,740,259	
Bitbank	International, Ex- US, Japan Focus	44,309,174	
Serum	Decentralized Exchange	40,415,709	
OKCoin	International, Limited US	20,761,549	0.5%
Bybit	Derivatives Only	-	
BitMEX	Derivatives Only	-	
CME	Derivatives Only	-	
Deribit	Derivatives Only	-	
Total (US Only)		3,838,604,808	100.0%

5.6. Outlook

CEXs (Centralized Exchange) typically provide additional services such as crypto asset custody. Before trading can take place, they frequently need consumers to deposit their crypto assets at the exchange.

According to 2021 research by KPMG, one of the big 4 accounting firms, exchanges are the most valuable firms in the cryptocurrency market.

CEXs are still considerably more widespread than decentralized exchanges (DEXs) in February 2022. KPMG discovered that CEXs accounted for around 95% of exchange crypto transactions. Binance is the world's largest crypto exchange, and it is centralized, despite the fact that it has built its DEX. The centralized Binance exchange conducts more than US\$20 billion in daily transactions, while the biggest DEX Uniswap processes less than US\$2 billion.

Decentralized exchanges are unquestionably an interesting development in the crypto world. DEXs allow users to trade cryptocurrencies directly amongst themselves, eliminating the need for a trusted middleman. As a result, users may retain custody of their funds.

However, while DEXs have their advantages, they still fall short in terms of regulations and scalability, which are critical issues that might decide the crypto industry's future trajectory. Centralized exchanges will play an essential role in this ecosystem, providing the liquidity depth required to expand the larger crypto community.

Centralized exchanges have shown to be scalable, high-performance infrastructures with connectivity that enables a wide range of techniques including high-frequency trading. This allows centralized exchanges to attract professional traders and institutional capital, which the cryptocurrency sector requires to expand and eventually gain mainstream acceptance.

In reality, centralized exchanges have been following in the footsteps of DEXs by introducing features such as non-custodial solutions. These hybrid systems enable centralized exchanges to deliver a high-performance experience as well as the benefits of self-custody while being regulatory compliant.

As DEXs gain traction, it is evident that centralized exchanges will continue to evolve and play an important role in driving the crypto industry and community in the years ahead.

Over the projected period 2021-2028, the worldwide cryptocurrency exchange platform market is predicted to increase significantly. The market's expansion can be due to the significant demand for a platform that allows cryptocurrencies to be traded for fiat money. Cryptocurrency exchange platforms serve as middlemen between buyers and sellers, earning money through transaction fees and commissions. According to CoinMarketCap, a publishing business, there were 419 cryptocurrency exchanges worldwide in October 2021 (507 as of the penning of this missive), with a total 24-hour trading volume of US\$ 112 billion. The growing number of cryptocurrency users throughout the world has had a significant impact on industry growth. According to Crypto.com, a cryptocurrency trading platform provider, the worldwide crypto user base hit 106 million in January 2021. This may be linked to the



Coinbase Global Forensic and Fundamental Analysis

increasing use of DeFi, an increase in the number of crypto service providers, and the quick embrace of cryptocurrencies by financial institutions.



Coinbase Global Forensic and Fundamental Analysis

Patents and Intellectual Property

Introduction to distributed ledger intellectual property and the dearth of due diligence that has accompanied it.

The Popping of the Crypto IP Bubble is Nigh

Intellectual property, or more aptly put, intellectual property protections have been eschewed by the earliest adopters of Bitcoin, blockchain technologies and cryptocurrencies. This is mostly likely because the earlier adopters were generally not businessmen, lawyers or hardcore financial types who recognized the value of IP ownership over mere IP use. They were also primarily open-source software developers and engineers, and in combination with their lack of business and financial training, failed to recognize the need for ownership and control over IP – even if your intention is to consequently give said IP away for free. The eschewing went so far as considering IP protections to be anathema, tantamount to the antithesis of the ethos of blockchain technology and cryptocurrency technology.

Of course, this belief is nonsensical to those skilled in the art. For instance, if you are a staunch believer in the open source software ethos, then you (nearly by definition) are also a staunch believer in IP ownership (via copyright and commercial license over software code). One cannot “enforce” the terms and conditions necessary to keep code free and continuously available in an upgraded fashion without exercising your rights and ownership over said property (your intellectual property).^{1 2} Thus, chances are, regardless of your individual stance on IP and IP protections, if you are in the business of making money from IP (including software development and sales), you are in the business of protected IP – even if you are giving it away, you need to control its use to prevent abuse. Reference how this revelation is just now coming to light in the DeFi industry.

- [Uniswap V3 Introduces New License to Spoil Future SUSHIs](#)
- [Aave Latest DeFi Protocol to Delay Open Source and Lock Down V3 ...](#)
- [Open source does not mean what you think it means – CoinGeek](#)
- [Why We're Relicensing CockroachDB](#)
- [Curve DAO Contemplates Its Intellectual Property - CoinDesk](#)

This misunderstanding of the importance of IP and the protections available to IP has caused a horrendous bubble to form in this space. Tens of thousands of commercial entities (literally, 20,179 cryptos and 501 exchanges, as well as hundreds if not thousands of other operating [i.e., banks,

¹ Can open source software be copyrighted?

The three exclusive rights that pertain to copyright ownership of software under the Copyright Act are the rights to reproduce, prepare derivative works based upon, and distribute copies of the copyrighted work. 45 In general, **all open source licenses grant users these rights**. https://www.dwt.com/files/uploads/documents/Presentations/11-11_Montague_OSSpaper.pdf

² Is open-source software intellectual property?

Open source software by its nature includes protectable intellectual property rights, most notably copyright.

Therefore, if a person wishes to use any open source software, that person will be obliged to comply with the associated license terms .May 6, 2020 <https://www.iptechblog.com/2020/05/is-the-use-of-open-source-software-putting-your-business-at-risk/>

Coinbase Global Forensic and Fundamental Analysis

securities exchanges, investment entities], supporting, advisory and consulting entities) have adopted, rely, and base their businesses upon sell and resell. They use this technology as if it is free of consequences and wholly open source. This is not the case. Multiple entities who did not share the apathy for IP protection early on in this crypto space have staked out fertile territory upon which they have secured valuable IP rights, complete with the power of enforcement. Thus, those companies such as crypto exchanges have been operating and even going public under the ruse that rents they've been collecting over the past decade solely belong to them when in reality they have been collecting the rents of the actual IP holders. The validity of the IP claims is often subject to court adjudication, but in the case of clear cut infringement and/or a court win, the margins and profitability of these previously rent collecting entities will be severely compressed, if not totally eliminated. Hence, the popping of the IP bubble! The balance of this section will walk the reader through a summary cross section of a sampling of these entities as well as a summary analysis.

Trademarks and Brands

What a trademark means?

A trademark can be **any word, phrase, symbol, design, or a combination of these things that identifies your goods or services**. It's how customers recognize you in the marketplace and distinguish you from your competitors. The word "trademark" can refer to both trademarks and service marks. Mar 31, 2021

<https://www.uspto.gov/trademarks/basics/what-trade...>

[What is a trademark? - USPTO](#)

The popularity of NFTs (non-fungible tokens) have brought many lesser-known entities into the crypto space, marketing visible wares in the fashion, apparel, branding and

brand awareness sectors. These sectors have large and powerful industry stalwarts, whose brands command both significant followings and significant prices. The offering of these brands, trademarks, and services without the express permission of intellectual property holder has caused a new form of litigation in the crypto space.

Nike vs StockX

Enforcement from larger companies like Nike are being seen against smaller entities such as StockX NFT for offering digital products on the blockchain bearing Nike's trademarked logo without permission.



StockX's Nike NFTs.



Coinbase Global Forensic and Fundamental Analysis

This was Nike's [first trademark infringement litigation](#) in the NFT space.³

[Hermès International vs. Mason Rothschild](#)

Hermès sued Mason Rothschild in January of 2022, alleging infringement of the Birkin brand of luxury handbag trademarks through the creation of "MetaBirkins." "MetaBirkins" is the name given to the NFTs minted by Rothschild as the online version of the exclusive high-end Birken bag. Reference the initial filing here [Hermès International vs. Mason Rothschild](#).

Note that Coinbase has just opened a dedicated NFT trading platform -

Copyrights and Commercial vs Open-Source Licenses

DeFi, or decentralized finance, a segment of digital finance [pioneered by Reggie Middleton](#), sports a development community that is heavily ensconced in the open source software arena. As explained earlier in this missive, this community often failed to address IP ownership and enforcement issues. This has led to an entire subindustry that was perceived as devoid of patents, trademarks and commercial licenses. At least, that was the perception. The reality is a bit more nuanced.

1. In April of 2014, Middleton et. al. filed the first patent application for distributed finance. None of this work was open source.
2. Roughly 3 years later, an Israeli entity called Bancor released an opensource liquidity pricing algorithm after its ICO. The net effect of this launch was a product that was/is covered by the patent.
3. Bancor's product, which was based on already patented property, was subsequently copied by a young man who consequently launched the modified fork as Uniswap. Uniswap went on to be the most successful DeFi application to date – materially outstripping the success of Bancor's product, with Bancor's own idea, which was originally in Middleton's patent application.
4. Uniswap's very successful product was then copied by a group of developers and modified to create a sweeter payout incentive to liquidity providers and renamed Sushiswap. Sushiswap drained ~55% of the liquidity off of Uniswap's platform.
5. Not to be outdone, a group of developers forked (copied) Sushiswap's code, brought it over to BinanceSmartChain and created PancakeSwap, which is the largest DEX in the Binnace ecosystem.

Yes, an original, patented idea was copied and distributed more than 5 times without any requisite due diligence in regards to the IP being copied. Searching "swap" and "DEX" in CMC will yield hundreds of additional copies – literally - as seen below in the content copied from CoinMarketCap.com's search function. These results likely contain the original patented IP copied from the original filing.

³ Trademark Infringement in the Metaverse: Nike Sues Online Resale Platform Alleging Infringing Use of Logo in StockX NFT - Kattison Avenue | Issue 8 - Spring 2022 <https://www.jdsupra.com/legalnews/trademark-infringement-in-the-metaverse-2139118/>

Coinbase Global Forensic and Fundamental Analysis

swap Cryptoassets  TrustSwap SWAP  Swap XWP #2211	 SatoshiSwap SWAP #3796  safeswap.online SWAP See all results (100) Categories	Trustswap Launchpad Exchanges  AirSwap  Uniswap (V1) #335  CtcSwap See all results (100)
--	---	---

As a result of this copying of expensive to produce IP (which was ironically copied by Uniswap's founder), Uniswap decided to [exercise its copyrights and created](#) a new business license to [spoil SushiSwap-like attempts](#). Many other DeFi platforms have either considered or actually done the same thing – Be it [55% of Aave's Community Voting for the Change](#) to a 'Business License' to Curve Finance also [wrangling with enforcing its IP rights](#).

Despite the attempts to limit and/or prevent the pilfering for profit of valuable and expensive business IP, the original, patented Middleton IP has already permeated the industry due to rampant copying and forking.

Patents – The Big Kahuna

A U.S. patent is a grant of property rights for an invention that is given by the U.S. Patent and Trademark Office (USPTO). Anyone receiving a patent can **prohibit anyone else from making, using, or selling the patented invention in the U.S., nationwide.**

U.S. patent law allows only the patent holder to retain these exclusive rights. The only path for other parties to legally obtain said rights is the authorization of the patent holder, an authorization that is generally given through a patent license agreement.



Coinbase Global Forensic and Fundamental Analysis

Since patents are national and nation-specific, in terms of jurisdiction, rights granted under US patent law give the US patent holder the exclusive rights to make, use, or sell the invention both from within the US towards the US. Any party that is not the patent holder or is not explicitly licensed by the patent holder doing the aforementioned during the valid term of the patent is subject to infringement. **If a patent is infringed upon, a patent holder may sue.** Remedies can include an injunction to prevent further continued infringement, compensatory damages to make the patent holder whole from past infringement, as well as an award for punitive damages in the case of willful or purposeful infringement.

A determination of infringement by the court stems from analyzing the language of the original patent claim(s) and comparing them to the invention which the defendant(S) have made use of. A court may come to the determination that material differences between the language of the patent claims and the invention utilized by the defendant do not result in infringement.

Note, that the following is not the result of an exhaustive analysis of the patents in question. Warranty of accuracy or fitness is neither implied nor offered and the following is presented for informational purposes only and should be considered our unqualified opinion.

nChain Holdings

According to nChain Holding's unofficial PR and media arm, more recently granted patents cover the *entire* Bitcoin ecosystem. We are skeptical as to the breadth of that claim but do concede that it's very possible that roughly 3 of the 53 some odd DLT-related patents issued do cover fairly wide swaths of the Bitcoin ecosystem, and quite possibly chains and players outside of that particular ecosystem as well. While we haven't thoroughly reviewed these patents for reach and effect, we are presenting the representations of nChain's unofficial media (CoinGeek) for informational purposes only, along with our comments,

1. **NFTs** → [EP3420669B1: Cryptographic method and system for secure extraction of data from a blockchain](#) - disclosure relates generally to cryptographic techniques for secure processing, transmission and exchange of data. It also relates to peer-to-peer distributed ledgers such as (but not limited to) the Bitcoin blockchain and associated technologies. In particular, it relates to control solutions for identifying, protecting, extracting, transmitting and updating data in a cryptographically controlled and secure manner. It also relates to system inter-operability and the ability to communicate data between different and distinct computing systems.

This patent family is only active through the EPO thus far, meaning that only Europe/UK are valid enforcement jurisdictions.

Tokens [0105] Tokens may represent an asset, or a contract conferring specified rights upon the holder to be redeemed for fiat currency (virtual banknotes), to denote ownership of property (e.g., title deeds), or grant access to an event (tickets), to name a few of many examples. Goods and services may include new or second hand products, labour (e.g., charged by the hour), complete jobs (e.g., mowing the lawn), to name a few of many examples. [0106] A token is an exchangeable entity represented by/representative of a contract. The contract may take one of

Coinbase Global Forensic and Fundamental Analysis

several forms. For example, the contract may confer a right upon the holder or denote ownership of property. The value of the token may be contractually specified and is linked to the underlying BTC amount via a 'pegging rate'. The token is exchangeable via novel type of transaction using a cryptocurrency protocol such as the bitcoin protocol. The bitcoin value on the transaction acts as a token representing a rights contract in digital form. The contract itself may be stored on the transaction or may be kept in a publicly accessible location, or may be held privately by the parties to the contract depending on the particular embodiment. Where the contract is not stored on the transaction, the transaction may store a unique pointer to the contract. [0107] Tokens may be divisible. A divisible token is one in which the value on the transaction output can be subdivided into smaller amounts which can be allocated across multiple new tokens. Examples of divisible tokens include tokens for fiat currency or for shares in a race horse. Divisible contracts may be defined as those that specify a non-zero pegging rate. In other words, the token value is tied to the underlying bitcoin value. Alternatively, tokens may be non-divisible. A non-divisible token is a contract that specifies the holder's rights in terms of a fixed value, e.g. a contract to redeem a house or AU\$1000. Non-divisible tokens are therefore not linked to the value of the underlying bitcoin. [0108] Tokens must be digitally signed by a token issuer to be valid. The issuer may, for example be an authority such as a Registrar of Title deeds. The issuer may issue a token to a user in return for payment. That token may then give the user the right to exercise the contract linked to the token, whether the contract represents the right to redeem fiat currency or for a service to be performed. [0109] Examples of tokens in accordance with the above, include the following: • A fiat currency token that is pegged to the BTC value of the transaction output by the issuer of the contract. For example "the spender of this token (bitcoin transaction) is entitled to redeem any fraction of this token for Canadian dollars (CAD) at a rate of 1 share (10cents) for every 1000 satoshis". • A race horse owned by several members of a syndicate • Any item where the ownership is by a title deed, e.g., a house or other property could be treated in this way. • An electronic contract representing a concert ticket. This is inherently non-divisible. • A bearer bond (non-divisible) • A unique identifier attached to a Goods/service (such as a bar code or RFID). If used, this identifier is still preferably validated by a signature of an authorised entity; without a signature it will fall into the less secure 'goods/service' category (described below). • A contract for the right to a service to be performed. It is noted that this is not the same as the actual service itself, but only the right to have the service performed for them. This right can be traded. For example, a voucher from Michael's Mowing for up to 3 hours lawn mowing within the Sydney metropolitan area. The holder of this voucher (contract) can redeem it for the actual service. [0110] Tokens must specify the value of a share, e.g., 1 share = 10 cents CAD, 1 share = 1 rupiah, or 1 share = 1% ownership of an item or property (race horse, house, etc.).

2. **"DeFi" exchanges** → [1182782: Tokenisation method and system for implementing exchanges on a blockchain](#) - In accordance with the invention there may be provided a method and corresponding system for controlling the performance of a process conducted via a blockchain. The blockchain may or may not be the Bitcoin blockchain. The process may be a lending process.



Coinbase Global Forensic and Fundamental Analysis

Advantageously, the invention provides a mechanism which enables the ultimate owner of a property or other asset to borrow funds against that asset, and sets out how this can be achieved in a manner which does not require the return to the investor(s) to be determined through the payment of interest. This makes it compliant with non-interest forms of lending. The invention provides a blockchain-implemented method (and corresponding system) of embedding data in a blockchain transaction (Tx). The method comprises the steps of deriving a public-key-private key cryptographic pair for the data; deriving a signature for the data using the public key-private key cryptographic pair; codifying the data to generate codified metadata for the data. The codified metadata is transmitted to the blockchain in a transaction. A signature is received and a script from at least one user to enable access to the embedded data. The script comprises a public key of a signatory. The metadata comprises a hash of the data and a pointer to the data so that it can be located. The hash is used as a primary key in a lookup table where the data is stored.

This is a US patent with material reach, if upheld.

3. **Ethereum's ERC721** → [GB2561465B: A method and system for securing computer software using a distributed hash table and a blockchain](#) – this is a UK only patent

True Return Systems

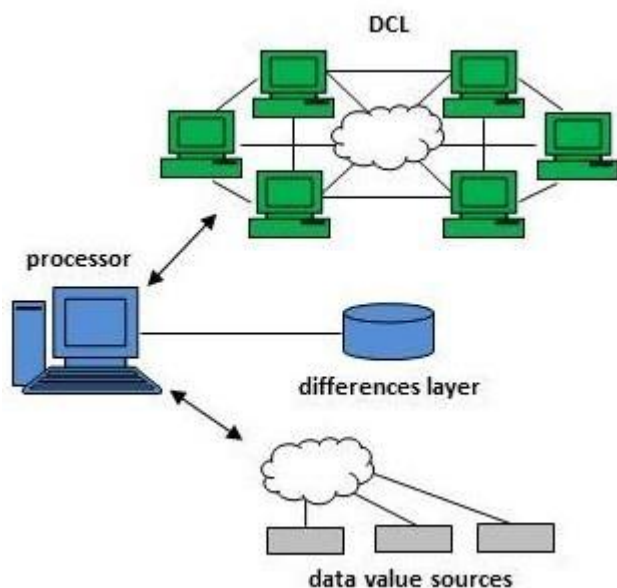
(as excerpted from <https://www.truereturnsystems.com/>)

U.S. Patent No.: 10,025,797 Method and System for Separating Storage and Process of a Computerized Ledger for Improved Function | Inventor: Jack Fonss, February 23, 2018 priority (provisional application), Issued: July 17, 2018; first-office-action allowance

TECHNOLOGY OVERVIEW

'797 teaches technology for extending the capabilities of traditional distributed computerized ledgers ("DCLs") such as blockchains. The invention addresses a number of failings of traditional DCLs, such as transaction processing speed, data storage limitations, and security issues raised through methods incorporated into DCLs (e.g., conventional smart contracts). By addressing the failings of the prior art, the invention extends DCLs, making them suitable for industries and applications for which they were previously unsuitable or cumbersome.

Coinbase Global Forensic and Fundamental Analysis



Mr. Fonss recognized that transactions within a DCL can be independent and separately processed from the data items required to specify a value, disposition, distribution, or resolution of a unit of the DCL. By separating the transaction processing methods and data from the DCL itself, the invention reduces the data requirements for the DCL, and thereby decreases the DCL consensus processing requirements.

This separation may be accomplished using electronically published data that is exogenous to the DCL but related to the DCL record (e.g., package tracking information, commodity price information, relevant news). This data feed is connected to a processor that processes the

time-sequenced data to determine differences over time and links the processed data to the appropriate DCL records. The linked data and associated processes may be stored in a data layer separate from the DCL (which may be centralized or decentralized, and secured separate from the DCL). Only those items required for transaction record keeping are maintained in the DCL. This reduces the data burden on the DCL—and thereby the consensus-processing burden. This also reduces the security and privacy concerns posed by exposing processing code and sensitive transaction details in the DCL. Thus, the invention enables faster processing of transactions (enabling a far higher transaction rate than what is currently supported by traditional DCLs). And the invention extends DCL functionality without exposing the DCL to security threats that are inherent to exposing methods on the DCL.

Veritaseum's View

A patent on off chain data sources teaches what we feel is at the heart of many layer 2 implementations, plus a dollop of the tokenization, and on/offchain lending and AMM protocols. This likely includes the Compound Finances, MakerDAOs, Uniswaps and even the Chainlinks of the crypto world. The tokens of these projects, and many more like them, are traded for revenue through the Coinbase Global platform.

Below are the notice letters, legal complaints and supplementary addendums as published by True Return Systems itself and was available from [their website](#) at the time of publication of this analysis.



Coinbase Global Forensic and Fundamental Analysis



David A. Boag

BOAG | LAW, PLLC
447 Broadway, Ste. 2-270
New York, NY 10013
212.203.6651
dab@boagip.com

March 10, 2022

Compound Finance
(d/b/a Compound Protocol, Compound Finance, compound.finance)
COMP Owners and Compound Finance Governance

via forum post to www.comp.xyz
via Twitter to twitter.com/compoundfinance

RE: Compound Finance's Use of U.S. Patent No. 10,025,797: Method and System
for Separating Storage and Process of a Computerized Ledger for Improved
Function

Dear COMP Owners and Compound Finance Governance:

Our firm represents True Return Systems, LLC ("TRS"). This letter summarizes TRS's position concerning the use of its patented technology without a license.

U.S. Patent No. 10,025,797 is generally directed to systems and methods that improve distributed ledger technology by addressing computational, time, storage, and security constraints inherent to distributed ledgers such as blockchains. The general approach of the '797 Patent is to separate certain processing and storage functions from a base distributed computerized ledger while linking the separated processing and storage to a base distributed computerized ledger. The technology described in the '797 Patent was developed exclusively by TRS.

TRS and its predecessor organizations are inventor-led and have been inventing solutions relating to ledger systems, integrated data sourcing, and linked storage arrangements for more than a decade. We are confident in the novelty and enforceability of the '797 Patent, which was duly issued by the USPTO and thus entitled to a statutory presumption of validity under 35 U.S.C. § 282. The '797 Patent was granted under the USPTO's Track One or "prioritized examination" which exists so that patents covering cutting-edge, economically significant subject matter can take priority.

www.boagip.com



Coinbase Global Forensic and Fundamental Analysis

Based on publicly-available information, we believe that Compound Finance is using the technology claimed in at least Claims 1 and 7 of the '797 Patent. The '797 Patent and claims charts showing the correspondence between the Compound Finance system and Claims 1 and 7 of the '797 Patent are attached as a link under "preliminary exhibits" and are accessible at www.truereturnsystems.com/c-docs.

In earlier communications, counsel representing Compound Labs, Inc. denied that Compound Labs, Inc. (itself) is infringing the '797 Patent, but they declined to make similar representations for the Compound Finance protocol or the owners of the COMP token.¹

DAOs and Membership Liability

To the best of our knowledge, Compound is not legally organized to operate in any state, but rather represents that it is operated by the owners of the COMP token through decentralized governance. The COMP token serves essentially the same purpose as tradable partnership interests or voting tradable shares in an unincorporated entity. According to Compound Finance documentation and press releases from Compound Labs, Inc., COMP owners operate the governance functions, treasury functions, and control the rights over distributions and distribution entitlements for the Compound Finance DAO's business operations.

Counsel for Compound Labs Inc recently authored an article directed at the partnership liability for a DAO, titled entitled "Opinion – How to Do Business as a DAO." In the article counsel argues:

There is a risk the DAO could be considered a general partnership or unincorporated association. This might expose its members to personal liability for any of the DAO's actions and obligations, and discourage businesses, institutional investors, or other vulnerable or regulated entities from participating in DAOs.²

Crypto counsel for Andresseen Horowitz's a16 co-authored a whitepaper in which he similarly noted risks to DAOs include:

Significant legal precedent exists for U.S. courts utilizing a functional approach to determining whether a partnership was formed irrespective of disclaimers and specific intent to not form a partnership.

In a practical sense, the operational structure of a DAO provides certain advantages against liability as the smart contracts prevent much of the legal risk of a typical

¹ For the avoidance of doubt, TRS believes that Compound Lab Inc's counsel distinctions between Compound Finance and Compound Labs Inc will have no bearing on TRS's claims or the anticipated outcomes.

² See "Opinion – How to Do Business as a DAO", Oct. 20, 2021, www.coindesk.com/policy/2021/10/20/how-to-do-business-as-a-dao/.



Coinbase Global Forensic and Fundamental Analysis

organization by providing an unambiguous and efficient method for transactions to be processed...However, if a judgement were to be entered, accessing DAO resources would require a vote of the widely dispersed and pseudonymous members, who could be unwilling to utilize treasury assets to satisfy any judgement, increasing the risk that such liability falls on individual DAO members.

³

To paraphrase, if it looks like a general partnership and acts as a general partnership, courts are likely to treat it as a general partnership.

The author of a 2018 law review article was even more forthright, predicting that courts will ultimately put form over substance and recognize DAOs as general partnerships:

Because decentralized organizations do not have a recognized legal status, the limited liability protection afforded to many other organizations is not available—leaving individuals subject to personal liability because of their investments.⁴

While the writings of private practice attorneys and internet commentators do not make law, it appears that the majority of papers and articles are similarly aligned on matters of potential DAO liability.⁵ General partnerships have no corporate form and do not provide partners with the liability limitations contained in other common entity structures.

The Compound Finance DAO, COMP owners, and Compound Labs, Inc.

We expect the owners and operators of the Compound Finance protocol may rely on entanglement of names to misdirect the identity of the DAO's owners and operators where the mix of names may include Compound, Compound Finance, the Compound Protocol, the Compound Finance Protocol, Compound Labs, Inc., and the website compound.finance. We do not expect a

³ See D. Kerr et al., A Legal Framework for Decentralized Autonomous Organizations, pp. 12-13, a16z.com/wp-content/uploads/2021/10/DAO-LegalFramework-Jennings-Kerr10.19.21-Final.pdf, last accessed Dec. 6, 2021.

⁴ See L. Metjahic, Deconstructing the DAO: The Need For Legal Recognition and the Application of Securities Laws to Decentralized Organizations, *Cardozo Law Review*, v. 39, pp. 1547-48 available at cardozolawreview.com/wp-content/uploads/2018/07/METJAHIC.39.4.pdf, last accessed Dec. 6, 2021.

⁵ See Skadden, Arps, Slate, Meagher & Flom LLP, "The Distributed Ledger: Blockchain, Digital Assets and Smart Contracts", August 2021 (In the absence of legal entity status and direction from courts or legislators, concern has surfaced among users that DAOs are general partnerships, and therefore each of a DAO's members would be personally liable for the actions (including fraud or material misrepresentations) of the partnership and of the other general partners."); Orrick Herrington & Sutcliffe LLP, "Get to Know This Acronym for a Crypto Regulatory Alternative: DAOs", Sept. 24, 2021 (describing a Wyoming bill as "designed with several benefits in mind, including protecting DAO participants from theories of liability based on general partnerships and giving a corporate form for recently passed legislation that allows DAOs to register as LLCs; Gibson Dunn & Crutcher LLP, *Financier Worldwide*, "Legal implications of expanded use of blockchain technology", Judith Alison Lee, Jeff Steiner and Dustin McKenzie, November 2016 ("Decentralised organisations raise liability issues as ultimate responsibility may be difficult to define. Because the organisation's 'management' is conducted automatically, legal systems would have to decide who is responsible if laws are broken. Similarly, the legal status of such organisations will be in question.")).



Coinbase Global Forensic and Fundamental Analysis

strategy of name misdirection or the use of pseudo-anonymous handles to materially impact any legal proceedings or outcomes.

We have taken the precaution of attaching an unfiled complaint for the purpose of identifying the parties to this correspondence. Possibly unintended confusion may arise because of the overlap of names among founding entities, governance foundations, software providers, website address locations, trademark filers, and the DAO itself. The use of anonymous and pseudo-anonymous identities by the DAO and entities related to the DAO may also lead to possibly unintentional confusion.

TRS remains open to an amicable resolution of this matter. Parties interested in acquiring a license to TRS's technology should contact us immediately while preferred terms remain available for early adopters. Should TRS need to formally enforce its rights, the terms will change to reflect the additional expense.

Very truly yours,

David A. Boag



Coinbase Global Forensic and Fundamental Analysis
TRS vs Compound Labs Complaint

IN THE UNITED STATES DISTRICT COURT
FOR THE [...]

TRUE RETURN SYSTEMS LLC

Plaintiff,

v.

COMPOUND PROTOCOL

Defendant.

§
§
§
§
§
§
§
§
§

Case No. X:xxx-cv-xxxxx-ABC

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff True Return Systems LLC (“True Return”), by and through its undersigned counsel, brings this Complaint for patent infringement against Defendant Compound Protocol (“Compound”), and in support thereof alleges as follows, upon personal knowledge as to itself and upon information and belief as to all others:

NATURE OF ACTION

1. This action seeks legal and equitable relief against Compound’s unlawful infringement of True Returns’ United States Patent No. 10,025,797, generally relating to technology for improving computerized ledgers, including distributed computerized ledgers such as blockchains.

PARTIES

2. True Return is limited liability company organized and existing under the laws of the state of Connecticut with its principal place of business located at 253 Turtle Back Road, New Canaan, CT 06840.



Coinbase Global Forensic and Fundamental Analysis

3. Upon information and belief, Compound is a decentralized autonomous organization controlled and operating at the Ethereum blockchain contract address 0xc00e94cb662c3520282e6f5717214004a7f26888 and operating from the website <https://compound.finance/>.

4. On information and belief, in January 2018, Robert Leshner introduced the Protocol and the name "Compound" in an online blog post on Medium, and informed readers that Compound was in the process of developing the Protocol.

5. On information and belief, in September 2018, Compound [Labs] deployed the Protocol to the Ethereum mainnet.

6. Compound was launched for the principal purposes of creating a cryptocurrency lending business and marketplace governed by the owners of the COMP token and Compound Labs Inc. (as Compound's initial administrator and software provider). The ownership and governance rights of Compound are based on COMP tokens created and distributed by Compound; Compound Labs, Inc. and Robert Leshner are holders of COMP tokens. Compound Labs, Inc. is located at 3001 19th Street Suite 200, San Francisco, CA 94110 but on information and belief, Compound (the Protocol) operates, by design, without a U.S. address or location.

7. Investment tokens in Compound are freely tradable in the U.S. on the largest cryptocurrency exchanges including Coinbase, Gemini, and Kraken. Similarly, access to Compound's borrowing and lending technology services are available throughout the U.S.



Coinbase Global Forensic and Fundamental Analysis

8. On information and belief, Compound is not formally organized as a corporation, LLC, partnership, or other recognized organization type which would serve to limit the liability of its COMP token owners.

JURISDICTION AND VENUE

9. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1 et seq.

10. This Court has exclusive subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a). This Court has personal jurisdiction over Defendant because it has engaged in systematic and continuous business activities in this District. As described below, Defendant has committed acts of patent infringement giving rise to this action within this District.

11. Venue is proper in this District under 28 U.S.C. § 1400(b), because Defendant has committed acts of patent infringement in this District. In addition, Plaintiff has suffered harm in this District.

TRUE RETURN AND THE '797 PATENT

12. True Return was founded by Jack Fonss.

13. Mr. Fonss is a technology consultant focusing on financial technology (FinTech) platforms and offerings. After college, Mr. Fonss was a computer programmer and systems analyst at both McKinsey & Company and Morgan Stanley & Co on a range of platforms, operating systems, and computer languages. He has consulted for numerous asset managers and technology companies on a wide variety of FinTech issues related to funds, trading systems, and digital currencies.



Coinbase Global Forensic and Fundamental Analysis

14. Mr. Fonss founded and managed AccuShares Investment Management, LLC (“AccuShares”), a FinTech startup offering innovative technological solutions to problems limiting exchange traded funds. While running AccuShares, Mr. Fonss was the principal inventor of a range of systems and software technologies which have been adopted by many crypto-currency, digital money, and exchange middleware environments.

15. By 2015, Mr. Fonss recognized that distributed computerized ledger technology (including blockchain technology) provided the potential to improve computer system environments and their interaction with real-world assets and electronically published data sources. In particular, Mr. Fonss’ work included the design and integration of separate linked ledgers and architectures for computer system efficiency, security and persistent auditability.

16. Mr. Fonss worked through the issues and invented distributed computerized ledger technologies that could, among other applications, efficiently integrate on-chain and off-chain data and processes for improved computer system efficiency and security. He filed a provisional patent application for his invention with the U.S. Patent and Trademark Office on February 23, 2018 and a non-provisional patent application on March 16, 2018.

17. On July 17, 2018 the U.S. Patent and Trademark Office duly and legally issued U.S. Patent No. 10,025,797 (the “’797 Patent”), naming Jack Fonss as the inventor. The ’797 Patent is entitled “Method and System for Separating Storage



Coinbase Global Forensic and Fundamental Analysis

and Process of a Computerized Ledger For Improved Function.” A true and correct copy of the ’797 Patent is attached hereto as **Exhibit A**.

18. The ’797 Patent is generally directed to systems and methods that improve distributed-ledger technology by addressing computational, time, storage, and security constraints inherent to distributed ledgers (such as blockchains). The general approach of the ’797 Patent is to separate certain processing and storage functions from a base distributed computerized ledger (such as a blockchain) but link such separated processing and storage to the base distributed computerized ledger.

19. The systems and methods of the ’797 Patent can be generally understood with reference to the exemplary embodiment depicted in Figure 18 of the ’797 Patent, which is reproduced in annotated form below.

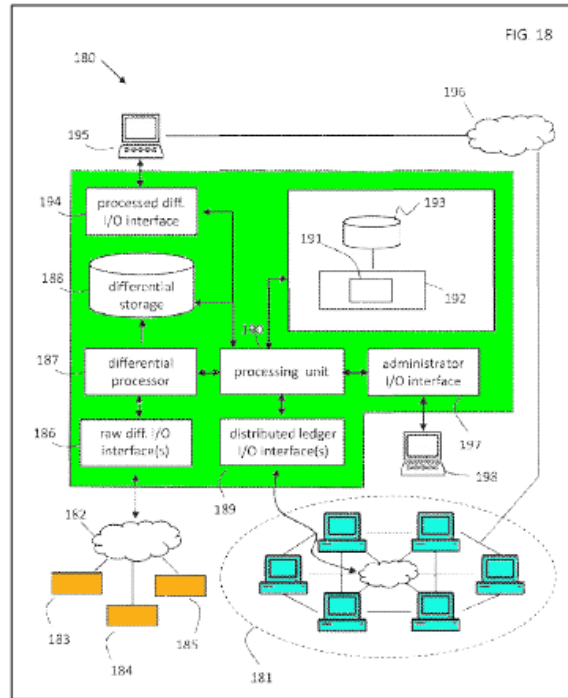
20. An exemplary differentials processing/storage system (in green) includes a differentials computer node (item 191) and a differential storage unit (item 188) linked to one or more electronically published time-sequenced data streams or descriptive differentials (items 183, 184, 185, in orange). The system processes (187)

data from the data stream / descriptive differentials (183, 184, 185) and stores the processed data on the differential storage unit (188). For example, the system may process logistical data provided by a shipping network, financial data and market prices provided by an exchange, or information provided by a news outlet.

21. The differentials processing/storage system (in green) is also linked to a base distributed computer ledger

("DCL," 181, in cyan) that includes one or more transaction records. The system processes (187, 190, 191) differential data (188) to link the differential data (188) to the DCL, which can then, e.g., update a transaction record of the DCL (181) according to the differential data (188).

22. This system improves over the prior-art distributed computerized ledgers in a number of ways including moving certain functionality and storage off the DCL while simultaneously allowing the DCL to utilize exogenous data to update transaction records on the DCL. This is possible because the differentials





Coinbase Global Forensic and Fundamental Analysis

processing/storage system links the DCL to the exogenous data while keeping and implementing certain computing-intense processes and storage-intense data so that the DCL is not burdened with such. This provides several technological advantages. For instance, processing and storage constraints inherent to a DCL are overcome by shifting certain processing and storage to a differentials processing/storage system. Similarly, security issues related to exposing DCL processes to the public are ameliorated by shifting processes to the differentials processing/storage node. Through a layered or parallel architecture, system access, processing, and storage can be performed more efficiently, and distributed ledgers such as blockchains can realize increase functionality.

COMPOUND

23. Compound provides methods and systems that use a processing/storage system to link published data to a distributed computerized ledger, specifically a blockchain.

24. Compound establishes the Compound blockchain data environment which includes the Compound Protocol and related system components; on belief and information, the system components and integrations of Compound were provided by and performed by Compound Labs Inc. The Compound blockchain data environment creates and manages the cTokens (an Ethereum compliant representation of balances supplied to Compound) and COMP (ownership and governance) interests.

25. Compound is a self-described “algorithmic, autonomous interest rate protocol” which operates as a decentralized autonomous organization for the benefit



Coinbase Global Forensic and Fundamental Analysis

COMP token owners. Compound operates autonomously, carrying out the business of creating and maintaining its cToken balances, and running its decentralized cryptocurrency borrowing and lending ecosystem for the benefit and profit of the COMP token owners. Compound has been periodically controlled by an administrator account which was originally operated by Compound Labs Inc. The administrator's centralized control is subject to a timelock delay to promote Compound's autonomous character.

26. The COMP token is the currency for the ownership, operation, and governance of the Compound blockchain integrated system. Compound ownership and governance, through the COMP token, is based on collective management and decision making by the business owners, where owners collectively submit proposals, and owners vote on proposals in proportion to their proportional investment in COMP ownership tokens.

27. As of February 3, 2022, Compound maintains approximately 10,000,000 COMP tokens for the purposes of owning, funding, governing, and promoting Compound's cryptocurrency banking. The current market value of COMP ownership tokens is approximately \$1.2 billion as of February 3, 2022.

28. Compound and Compound Labs Inc. develop and promote the Compound blockchain environment to individuals and institutions in the U.S. in large part to expand the use and adoption of the COMP token and thereby increase the value of the COMP token. COMP is widely regarded as a cryptocurrency investment asset, and a number of pooled investment funds have registered funds with the U.S.



Coinbase Global Forensic and Fundamental Analysis

Securities and Exchange Commission for investors to gain access to COMP and its expected returns from price appreciation.

29. Compound's mainnet launch was in September 2018, and Compound was upgraded to a version 2 in May 2019. Prior to May 2020, Compound's protocol balances remained below \$500 million. Since June 2020, Compound's balances have generally exceeded \$500 million. As of February 3, 2022, Compound balances exceed \$10.5 billion.

COMPOUND SYSTEM

30. Compound authored and published a whitepaper titled "Compound: The Money Market Protocol" ("Compound Whitepaper"). A true and correct copy of this publication is attached hereto as Exhibit B.

31. In the Compound Whitepaper, Compound states: "Governance: Compound will begin with centralized control of the protocol (such as choosing the interest rate)".

32. In the Compound Whitepaper, Compound states: "The [interest rate] demand curve is codified through governance ...governance will begin with centralized control"

33. In the Compound Whitepaper, Compound states: "the history of each interest rate, for each money market, is captured by an Interest Rate Index, which is calculated each time an interest rate changes...."

34. In the Compound Whitepaper, Compound states: "assets supplied to a market are represented by an ERC-20 token balance ("cToken") which entitles the owner to an increasing quantity of the underlying asset"



Coinbase Global Forensic and Fundamental Analysis

35. In the Compound Whitepaper, Compound states: "Each money market is unique to an Ethereum asset (such as Ether, an ERC-20 stablecoin) and contains a transparent and publically-inspectable ledger with a record of all transactions ..."

36. In the Compound Whitepaper, Compound states: "A Price Oracle maintains the current exchange rate of each supported asset...pools prices from the top 10 exchanges...used to determine a borrowing capacity and collateral requirements..."

37. In the Compound Whitepaper, Compound states: "Compound money markets are defined by an interest rate, applied to all borrowers uniformly which adjust over time..."

38. In the Compound Whitepaper, Compound states: "...as the market earns interest, its cToken becomes convertible into an increasing quantity of the underlying asset"

39. Compound authored and published an article titled "The Open Oracle System". A true and correct copy of this publication is attached hereto as Exhibit C.

40. In the Open Oracle System, Compound states: "The Compound protocol currently relies on a price feed, maintained by our team, to determine each user's borrowing capacity and to measure liquidation thresholds."

41. Compound authored and published an article titled "Compound API Introduction". A true and correct copy of this publication is attached hereto as Exhibit D.

42. In the Compound API Introduction, Compound states: "The market history service retrieves historical information about a market. You can use this API to find



Coinbase Global Forensic and Fundamental Analysis

out the values of interest rates at a certain point in time. Its especially useful for making charts and graphs of the time-series values.”

43. In the Compound API Introduction, Compound states: “Returns 10 buckets of market data” and “[fetch\(https://api.compound.finance/api/v2/market_history...](https://api.compound.finance/api/v2/market_history...)”.

44. In the Compound API Introduction, Compound states: “The market history graph API returns information about a market between two timestamps.”

45. In the Compound API Introduction, Compound states: “The market history graph API response contains the rates for both suppliers and borrowers, as well as the sequence of total supply and borrows for the given market.”

46. Compound authored and published an article titled “Open Price Feed”. A true and correct copy of this publication is attached hereto as Exhibit E.

47. In the Open Price Feed, Compound states: “If valid, the `UniswapAnchoredView` is updated with the asset's price. If invalid, the price data is not stored.”

48. In the Open Price Feed, Compound states: “`UniswapAnchoredView` only stores prices that are within an acceptable bound of the Uniswap time-weighted average price and are signed by a reporter. Also contains logic that upscales the posted prices into the format that Compound's Comptroller expects.”

49. In the Open Price Feed, Compound states: “The Open Price Feed accounts price data for the Compound protocol. The protocol's Comptroller contract uses it as a source of truth for prices.”



Coinbase Global Forensic and Fundamental Analysis

50. In the Open Price Feed, Compound states: "The Compound Protocol uses a View contract ("Price Feed") which verifies that reported prices fall within an acceptable bound of the time-weighted average price of the token/ETH pair on Uniswap v2, a sanity check referred to as the Anchor price."

51. In the Open Price Feed, Compound states: "Anchor Period - Get the anchor period, the minimum amount of time in seconds over which to take the time-weighted average price from Uniswap."

52. In the Open Price Feed, Compound states: "Anchor Bounds: Get the highest and lowest ratio of the reported price to the anchor price that will still trigger the price to be updated. Given in 18 decimals of precision."

53. Compound authored and published FAQ (frequently asked questions) on its website titled "Compound FAQ". A true and correct copy of this publication is attached hereto as Exhibit F.

54. In the Compound FAQ, Compound states: "When you supply assets to the Compound protocol, your balance is represented as a cToken, which can be transferred, traded, or programmed by developers to create new experiences. Think a cToken like a receipt [sic] — it's used to show who owns a balance inside Compound."

55. In the Compound FAQ, Compound states: "In each market, interest rates are determined algorithmically (based on supply and demand), and interest accrues every Ethereum block."



Coinbase Global Forensic and Fundamental Analysis

56. In the Compound FAQ, Compound states: "Compound is managed by a decentralized community of COMP token-holders and their delegates, who propose and vote on upgrades to the protocol."

57. Compound authored and published a codebase post titled "compound-finance/open-oracle". A true and correct copy of this publication is attached hereto as Exhibit G.

58. In the codebase post open-oracle, Compound states: "The Open Price Feed accounts price data for the Compound protocol. The protocol's Comptroller contract uses it as a source of truth for prices. Prices are updated by Chainlink Price Feeds. The codebase is hosted on GitHub, and maintained by the community."

59. In the codebase post open-oracle, Compound states: "The Open Oracle is a standard and SDK allowing reporters to sign key-value pairs (e.g. a price feed) that interested users can post to the blockchain. The system has a built-in view system that allows clients to easily share data and build aggregates (e.g. the median price from several sources)."

60. Compound authored and published a documentation titled "cTokens Introduction". A true and correct copy of this publication is attached hereto as Exhibit H.

61. In cTokens Introduction, Compound states: "Each asset supported by the Compound Protocol is integrated through a cToken contract, which is an EIP-20 compliant representation of balances supplied to the protocol. By minting cTokens, users (1) earn interest through the cToken's exchange rate, which increases in value



Coinbase Global Forensic and Fundamental Analysis

relative to the underlying asset, and (2) gain the ability to use cTokens as collateral.”

62. In cTokens Introduction, Compound states: “cTokens are the primary means of interacting with the Compound Protocol; when a user mints, redeems, borrows, repays a borrow, liquidates a borrow, or transfers cTokens, she will do so using the cToken contract. There are currently two types of cTokens: CErc20 and CEther. Though both types expose the EIP-20 interface, CErc20 wraps an underlying ERC-20 asset, while CEther simply wraps Ether itself.”

63. Compound authored and published a documentation titled “Comptroller Introduction”. A true and correct copy of this publication is attached hereto as Exhibit I.

64. In Comptroller Introduction, Compound states: “The Comptroller is the risk management layer of the Compound protocol; it determines how much collateral a user is required to maintain, and whether (and by how much) a user can be liquidated. Each time a user interacts with a cToken, the Comptroller is asked to approve or deny the transaction.”

65. In Comptroller Introduction, Compound states: “The Comptroller maps user balances to prices (via the Price Oracle) to risk weights (called Collateral Factors) to make its determinations. Users explicitly list which assets they would like included in their risk scoring”



Coinbase Global Forensic and Fundamental Analysis

66. Compound authored and published an article titled "Supplying Assets to the Compound Protocol". A true and correct copy of this publication is attached hereto as Exhibit J.

67. In Supplying Assets to the Compound Protocol, Compound states: "When users and applications supply an asset to the Compound Protocol, they begin earning a variable interest rate instantly. Interest accrues every Ethereum block (currently ~13 seconds), and users can withdraw their principal plus interest anytime."

68. In Supplying Assets to the Compound Protocol, Compound states: "Supplying Ether (ETH) to the Compound Protocol is as easy as calling the "mint" function in the Compound cEther smart contract. The "mint" function transfers ETH to the Compound contract address, and mints cETH tokens. The cETH tokens are transferred to the wallet of the supplier."

69. In Supplying Assets to the Compound Protocol, Compound states: "Remember that the amount of ETH that can be exchanged for cETH increases every Ethereum block, which is about every 13 seconds. There is no minimum or maximum amount of time that suppliers need to keep their asset in the protocol. See the varying exchange rate for each cToken by clicking on one at <https://compound.finance/markets>."

70. In Supplying Assets to the Compound Protocol, Compound states: "The Comptroller contract provides an easy to use function that calculates your account's liquidity, which is a USD-denominated value of the maximum allowed borrow



Coinbase Global Forensic and Fundamental Analysis

amount. You should never borrow this much at once because your account would instantly be liquidated as soon as the protocol's "accrue interest" operation is executed."

71. In Supplying Assets to the Compound Protocol, Compound states: "Before we borrow ETH, we need to determine the maximum amount of ETH we can borrow. This is important because if we try to borrow more than we are allowed to, the operation will fail. Also, if we borrow too close to the limit, our account will be liquidated. This is done by calling the `getAccountLiquidity` function on the protocol's comptroller contract."

FIRST CLAIM FOR RELIEF **(Infringement of U.S. Patent No. 10,025,797)**

72. True Return incorporates by reference its allegations in the preceding paragraphs of this Complaint.

73. The '797 Patent is valid and enforceable.

74. The '797 Patent is directed to patentable subject matter.

75. True Return owns all rights, title, and interest in the '797 Patent, and holds all substantial rights pertinent to this suit, including the right to sue and recover for all past, current, and future infringement.

76. Compound has and continues to directly infringe and/or indirectly infringe by inducement and/or contributory infringement, literally and/or under the doctrine of equivalents, the '797 Patent under 35 U.S.C. § 271.

77. Compound directly infringes the '797 Patent because it has made, used, and offered the Compound protocol, its related components and system services,



Coinbase Global Forensic and Fundamental Analysis

cTokens, and COMP ownership interests in the United States. Compound represents to the public and its owners that it performs all the operations and services relating to its cTokens cryptocurrency banking products and COMP ownership interests. Compound describes itself as a decentralized autonomous protocol.

78. The Compound algorithmic, autonomous interest rate protocol satisfies all the limitations of one or more claims of the '797 Patent, including Claim 1 and Claim 7.

79. Claim 1 of the '797 Patent recites:

1. A computer based method comprising:

creating at least one electronic parallel storage of a differences layer linked to a distributed computer ledger (DCL); the DCL contains an electronic transaction record by a time-sequenced value or a time-sequenced string;

accessing and storing a value through the at least one electronic parallel storage of the differences layer, the value from a group comprising of at least one time-sequenced electronically published data stream and at least one descriptive differential, wherein at least one differences processing engine running on a specialized computer system creates and stores parameters from a group comprised of a measurement differences and a descriptive differences;

storing the DCL containing an electronic transactions record on at least one of a distributed network of connected independent computers or a decentralized network of computers wherein the electronic transaction record is time sequenced, and a writing or an appending of the electronic transaction records is performed on the distributed network of connected independent computers or the decentralized network of computers;

storing the at least one electronic parallel storage of the differences layer on at least one of a centralized storage device controlled by the specialized computer system or a



Coinbase Global Forensic and Fundamental Analysis

decentralized storage device controlled by the specialized computer system for increasing functionality and utility of the DCL, reducing data storage requirements, eliminating transmission of redundant data, and improving data security;

linking the electronic transaction record in the DCL to records of the at least one electronic parallel storage of the differences layer utilizing at least one time sequenced value, string, code, or key; and

imputing at least one measured differential with a descriptive identifier or at least one descriptive identifier to the electronic transaction record of the DCL through data storage and processing on the at least one electronic parallel storage of the differences layer.

80. Operation of the Compound implements a computer based method.

81. For instance, Compound is a self-proclaimed algorithmic, autonomous interest rate protocol built for developers, and the Compound protocol cTokens and COMP tokens are managed and controlled by Compound's computer based method.

82. Operation of Compound meets the limitation of "creating at least one electronic parallel storage of a differences layer linked to a distributed computer ledger (DCL); the DCL contains an electronic transaction record by a time-sequenced value or a time-sequenced string."

83. For instance, Compound accesses and stores price feed data such as published market prices to determine each user's borrowing capacity and liquidation thresholds; price feed data is stored within a service run by a Compound API (application programming interface), and these stored data feeds are linked to Compound tokens on the Ethereum blockchain through Compound's family of tokens such as cTokens. cTokens are compliant with



Coinbase Global Forensic and Fundamental Analysis

Ethereum blockchain protocols and Ethereum uses incrementing time sequenced blocks including identifying keys or strings, such as a nonce, to arrange transactions records.

84. Operation of Compound meets the limitation of “accessing and storing a value through the at least one electronic parallel storage of the differences layer, the value from a group comprising of at least one time-sequenced electronically published data stream and at least one descriptive differential, wherein at least one differences processing engine running on a specialized computer system creates and stores parameters from a group comprised of a measurement differences and a descriptive differences.”

85. For instance, Compound’s UniswapAnchorView stores prices within acceptable bounds of a time-weighted average price which are also signed by a reporter. Compound stored values possess descriptive differences such as coded tickers (e.g. “ETH”, “UNI”, “WBTC”), and values possess time-in-seconds anchor periods and [time-based] anchor value-bounds to trigger updating. Compound’s Anchor Bounds functions are based on differentials of values and descriptors, getting the highest and lowest ratio of the reported price to the anchor price that will still trigger the price to be updated (based on 18 decimals of precision).

86. Operation of Compound meets the limitation of “storing the DCL containing an electronic transactions record on at least one of a distributed network of connected independent computers or a decentralized network of computers wherein the electronic transaction record is time sequenced, and a



Coinbase Global Forensic and Fundamental Analysis

writing or an appending of the electronic transaction records is performed on the distributed network of connected independent computers or the decentralized network of computers.”

87. For instance, Compound operates with two types of cTokens: CErc20 and CEther. Though both types expose the EIP-20 interface, CErc20 wraps an underlying ERC-20 asset, while CEther simply wraps Ether itself. The EIP-20 interface is an Ethereum blockchain token standard for transaction records on a distributed network of connected independent computers operating a blockchain.

88. Operation of Compound meets the limitation of “storing the at least one electronic parallel storage of the differences layer on at least one of a centralized storage device controlled by the specialized computer system or a decentralized storage device controlled by the specialized computer system for increasing functionality and utility of the DCL, reducing data storage requirements, eliminating transmission of redundant data, and improving data security.”

89. For instance, Compound’s UniSwapAnchoredView is updated with an asset’s price, but where price data is determined invalid, price data is not stored. Further UniSwapAnchoredView only stores prices that are within an acceptable bound of the Uniswap time-weighted average price and are signed by a reporter. Also, Compound contains logic that upscales the posted prices into the format that Compound’s Comptroller expects. Compound’s Open Price Feed price data is described as the system’s “source of truth for prices”; Compound’s price storage protocol limits and protects Compound’s storage of data based on a variety of factors



Coinbase Global Forensic and Fundamental Analysis

including rates of change for the purpose of reducing redundant or invalid values storage.

90. Operation of Compound meets the limitation of “linking the electronic transaction record in the DCL to records of the at least one electronic parallel storage of the differences layer utilizing at least one time sequenced value, string, code, or key.”

91. For instance, Compound’s cTokens operate through an EIP-20 interface, and cTokens are transactions recorded on the Ethereum blockchain, and Compound’s Comptroller operates as a risk management layer for the Compound protocol applying system time sequences and string coded descriptors such as “ETH” or “WBTC”. Each time a user interacts with a cToken (a transaction record on the distributed Ethereum blockchain), the Comptroller is asked to approve or deny the transaction. The Comptroller maps user balances to prices (via the Price Oracle) to risk weights (called Collateral Factors) to make its determinations. Compound’s Open Price Feed price data is described as the system’s “source of truth for prices”; Compound’s price storage protocol limits and protects Compound’s storage of data based on a variety of factors including rates of change and validity.

92. Operation of Compound meets the limitation of “imputing at least one measured differential with a descriptive identifier or at least one descriptive identifier to the electronic transaction record of the DCL through data storage and processing on the at least one electronic parallel storage of the differences layer.”



Coinbase Global Forensic and Fundamental Analysis

93. For instance, Compound publishes and stores interest rates for its Ethereum-based cTokens. Compound's market history service retrieves values through an API where the system has stored market differentiated interest rates (differentiated by collateral type including "ETH" or "WBTC") applicable to certain points in time. The interest rates, specific to time-sequencing and the descriptive identifiers of type (e.g. "ETH", "WBTC"). When users and applications supply an asset to Compound, they begin earning a variable interest rate instantly, and interest accrues time-sequenced by every Ethereum block (currently ~13 seconds). Compound accruals are effected through cToken transactions written and recorded on the Ethereum blockchain.

94. Also for instance, Compound uses a price feed contract that determines if pricing falls within an acceptable bounds of the time-weighted average price; price values are stored along with collateral factors map to descriptive differentials, and collateral factors are subject to change and are stored based on time-sequence. An asset's collateral factor (based on descriptive differentials such as "ETH", "USDC" or "WBTC") can be obtained using the Comptroller contract. Collateral factors are subject to change by Compound Governance with a minimum transition period of five days. An example of a collateral factor is as follows, a user supplies 100 USDC as collateral and the posted collateral factor for USDC is 50%. The user can borrow at most 50 USDC worth of another asset at any given time resulting in an Ethereum recording. Before a borrowing, Compound determines the maximum amount available for borrow based on stored prices and stored collateral factors. If



Coinbase Global Forensic and Fundamental Analysis

borrowed amounts are too close to the limits (based on prices and collateral values), an account will be liquidated through Compound's `getAccountLiquidity` function on the protocol's comptroller contract, resulting in a transaction recording on the Ethereum blockchain.

95. Claim 7 of the '797 Patent recites:

7. A system comprising:

a system having a memory device, the memory device further including a Random Access Memory (RAM);

a processor connected to the memory device, the processor is configured to:

create at least one electronic parallel storage of a differences layer linked to a distributed computer ledger (DCL), both the electronic parallel storage of the differences layer and the DCL containing a respective electronic transaction record, a time-sequenced value, or a time-sequenced string;

access a value from a group comprising of at least one time-sequenced electronically published data stream and at least one descriptive differential;

store the values from a group comprising of at least one time-sequenced electronically published data stream and at least one descriptive differential on the at least one electronic parallel storage of the differences layer;

align and link a stored value record of the at least one electronic parallel storage of the differences layer to the electronic transaction record of the DCL utilizing at least one time sequenced value, string, code, or key; and

impute at least one measured differential with a descriptive identifier or at least one descriptive identifier to the electronic transaction record of the DCL.

96. Compound is a system which operates as an algorithmic, autonomous interest rate protocol.



Coinbase Global Forensic and Fundamental Analysis

97. Compound meets the limitation of “a system having a memory device, the memory device further including a Random Access Memory (RAM)”

98. For instance, Compound is an autonomous protocol operating on the Ethereum blockchain. Compound's UniswapAnchoredView is updated with an asset's price (e.g. “ETH”, “WBTC”), and only valid prices are stored. Relating to Compound's interest rate values, the history of each interest rate, for each money market, is captured by an Interest Rate Index, which is calculated each time an interest rate changes; Compound's market history service retrieves historical information about a market. You can use Compound's market history API to find out the values of interest rates at a certain point in time.

99. Compound meets the limitation of “a processor connected to the memory device.”

100. For instance, Compound's UniswapAnchoredView only stores prices that are within an acceptable bound of the Uniswap time-weighted average price and are signed by a reporter and Compound also contains logic that upscales the posted prices into the format that Compound's Comptroller expects.

101. Compound meets the limitation of “the processor is configured to: create at least one electronic parallel storage of a differences layer linked to a distributed computer ledger (DCL), both the electronic parallel storage of the differences layer and the DCL containing a respective electronic transaction record, a time-sequenced value, or a time-sequenced string.”



Coinbase Global Forensic and Fundamental Analysis

102. For instance, Compound's price oracle maintains the current exchange rate of each supported asset, pooling prices from the top 10 exchanges, where pooled prices are time sequenced and stored on Compound's protocol and used to determine a borrowing capacity and collateral requirements for Compound's cTokens which are written as time-sequenced transaction records to the distributed Ethereum blockchain. Compound stored values possess descriptive differences such as coded tickers (e.g. "ETH", "UNI", "WBTC"), and values possess time-in-seconds anchor periods and time-based anchor (value) bounds to trigger updating. Compound's Anchor Bounds functions are based on differentials, getting the highest and lowest ratio of the reported price to the anchor price that will still trigger the price to be updated (based on 18 decimals of precision).

103. Compound meets the limitation of "the processor is configured to: ... access a value from a group comprising of at least one time-sequenced electronically published data stream and at least one descriptive differential."

104. For instance, related to price values, Compound protocol relies on a price feed, maintained by our team, to determine each user's borrowing capacity and to measure liquidation thresholds. A Price Oracle maintains the current exchange rate of each supported asset (each with a differentiating descriptor such as "ETH" or "WBTC") pools prices from the top 10 exchanges; Compound's UniswapAnchoredView only stores prices that are within an acceptable bound of the Uniswap time-weighted average price and are signed by a reporter. Relating to published rates, the market history service retrieves historical information about a



Coinbase Global Forensic and Fundamental Analysis

market. You can use this API to find out the values of interest rates at a certain point in time, and it's especially useful for making charts and graphs of the time-series values.

105. Compound meets the limitation of "the processor is configured to: ... store the values from a group comprising of at least one time-sequenced electronically published data stream and at least one descriptive differential on the at least one electronic parallel storage of the differences layer."

106. For instance, Compound's UniswapAnchorView stores prices within acceptable bounds of a time-weighted average price which are also signed by a reporter. Compound stored values possess descriptive differences such as coded tickers (e.g. "ETH", "UNI", "WBTC"), and values possess time-in-seconds anchor periods and time-based anchor (value) bounds to trigger updating. Compound's Anchor Bounds functions are based on differentials, getting the highest and lowest ratio of the reported price to the anchor price that will still trigger the price to be updated (based on 18 decimals of precision).

107. Compound meets the limitation of "the processor is configured to: ... align and link a stored value record of the at least one electronic parallel storage of the differences layer to the electronic transaction record of the DCL utilizing at least one time sequenced value, string, code, or key."

108. For instance, Compound cTokens operate through an EIP-20 interface, and cTokens are transactions recorded on the Ethereum blockchain, and Compound's Comptroller operates as a risk management layer for the Compound protocol



Coinbase Global Forensic and Fundamental Analysis

applying system time sequences and coded descriptors such as “ETH” or “WBTC”. Each time a user interacts with a cToken (a transaction record on the distributed Ethereum blockchain), the Comptroller is asked to approve or deny the transaction. The Comptroller maps user balances to prices (via the Price Oracle) to risk weights (called Collateral Factors) to make its determinations. Compound’s Open Price Feed price data is described as the system’s “source of truth for prices”; Compound’s price storage protocol limits and protects Compound’s storage of data based on a variety of factors including rates of change and validity

109. Compound meets the limitation of “the processor is configured to: ... impute at least one measured differential with a descriptive identifier or at least one descriptive identifier to the electronic transaction record of the DCL.”

110. For instance, Compound cTokens operate through an EIP-20 interface, and cTokens are transactions recorded on the Ethereum blockchain, and Compound’s Comptroller operates as a risk management layer for the Compound protocol applying system time sequences and coded descriptors such as “ETH” or “WBTC”. Each time a user interacts with a cToken (a transaction record on the distributed Ethereum blockchain), the Comptroller is asked to approve or deny the transaction. The Comptroller maps user balances to prices (via the Price Oracle) to risk weights (called Collateral Factors) to make its determinations. Compound’s Open Price Feed price data is described as the system’s “source of truth for prices”; Compound’s price storage protocol limits and protects Compound’s storage of data based on a variety of factors including rates of change and validity. Relating to interest rates,



Coinbase Global Forensic and Fundamental Analysis

Compound publishes and stores interest rates for its Ethereum-based cTokens. Compound's market history service retrieves values through an API where the system has stored market differentiated interest rates (differentiated by collateral type including "ETH" or "WBTC") applicable to certain points in time. The interest rates are specific to time-sequencing and the descriptive identifiers of type (e.g. "ETH", "WBTC"). When users and applications supply an asset to Compound, they begin earning a variable interest rate instantly, and interest accrues time-sequenced by every Ethereum block (currently ~13 seconds). Compound accruals are affected through cToken transaction records recorded and written on the Ethereum blockchain. Relating to linked and imputed liquidation, Compound uses a price feed contract that determines if pricing falls within an acceptable bounds of the time-weighted average price; price values are stored along with collateral factors, where collateral factors are subject to change, stored based on time-sequence and an asset's collateral factor (e.g. based on descriptive differentials "ETH", "USDC" or "WBTC") can be obtained using the Comptroller contract. Collateral factors are subject to change by Compound Governance with a minimum transition period of five days. An example of a collateral factor is as follows, a user supplies 100 USDC as collateral and the posted collateral factor for USDC is 50%. The user can borrow at most 50 USDC worth of another asset at any given time resulting in an Ethereum recording. Related, before a borrowing, Compound determines the maximum amount available for borrow based on stored prices and stored collateral factors. If borrowed amounts are too close to the limits (based on



Coinbase Global Forensic and Fundamental Analysis

prices and collateral values), an account will be liquidated through Compound's getAccountLiquidity function on the protocol's comptroller contract, resulting in a transaction recording on the Ethereum blockchain.

PRAYER FOR RELIEF

WHEREFORE, True Return respectfully requests the following relief:

- (a) judgment in favor of True Return that Compound has infringed, literally or under the doctrine of equivalents, U.S. Patent No. 10,025,797;
- (b) a judgment and order finding that Compound's infringement has been willful;
- (c) a judgment and order requiring Compound to pay True Return its damages, costs, expenses, prejudgment interest, post-judgment interest, and enhanced damages for Compound's infringement, and to provide an accounting of ongoing post-judgment infringement;
- (d) a judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding True Return its reasonable attorneys' fees against Compound;
- (e) an order preliminarily enjoining Compound from making, using, selling, or offering for sale the claimed subject matter of U.S. Patent No. 10,025,797;
- (f) an order permanently enjoining Compound from making, using, selling, or offering for sale the claimed subject matter of U.S. Patent No. 10,025,797, or such other equitable relief the Court deems warranted; and
- (g) any and all other relief any and all other relief as the Court may deem appropriate and just under the circumstances.



Coinbase Global Forensic and Fundamental Analysis

DEMAND FOR JURY TRIAL

True Return requests a trial by jury on all issues so triable.



Coinbase Global Forensic and Fundamental Analysis

Veritaseum and Patents US11196566 and JP6813477

Veritaseum, an inventor-led consortium of companies, is working with Mr. Middleton to administer the '566 and '477 patents worldwide. The patents cover the traditional transfer of value through distributed ledger technologies. As excerpted from the PCT application:

Abstract

Devices, systems, and methods enabling parties with little trust or no trust in each other to enter into and enforce value transfer agreements conditioned on input from or participation of a third party, over arbitrary distances, without special technical knowledge of the underlying transfer mechanism(s), optionally affording participation of third-party mediators, substitution of transferors and transferees, term substitution, revision, or reformation, etc. Such value transfers can occur reliably without involving costly third-party intermediaries who traditionally may otherwise be required, and without traditional exposure to counterparty risk.

Veritaseum believes several centralized and decentralized digital asset exchanges employ devices, methods and systems which may use unlicensed patented IP. Coinbase Global, et. al., is one of those exchanges. At least one patent holder has proffered notice to Coinbase (reference below), and they have acknowledged said notice.



Coinbase Global Forensic and Fundamental Analysis

BRUNDIDGE & STANGER, P.C.

ATTORNEYS AT LAW

1925 BALLENGER AVENUE, SUITE 560

ALEXANDRIA, VIRGINIA 22314

(703) 684-1470

July 3, 2022

CARL I. BRUNDIDGE
THEODORE C. SHIH*
DAVID E. MOORE*

MISUNG LEE
LEENA MAUSKAR*
KUMIKO KITAKA
YVONNE HE

OF COUNSEL
THOMAS L. PETERSON*
ISAAC A. ANGRES, Ph.D.**

* Bar Membership Other Than
Virginia or New York
** Registered Patent Agent

NEW YORK OFFICE:
1180 AVENUE OF THE AMERICAS
8TH FLOOR
NEW YORK NY 10036
(212) 382-4635

LOS ANGELES OFFICE:
826 WILSHIRE BLVD
LOS ANGELES CA 90017
(213) 816-2010

FACSIMILE: (703) 684-1460
EMAIL:
C.BRUNDIDGE@BRUNDIDGE-
STANGER.COM

VIA Courier (FedEx)

Mr. Brian Armstrong
Chief Executive Officer
Coinbase Global, Inc.
c/o The Corporation Trust Company
1209 Orange Street
Wilmington, Delaware 19801

Re: U.S. and Japan Patents, Veritaseum Capital LLC

Dear Mr. Armstrong,

Brundidge & Stanger, P.C. ("Brundidge & Stanger") represents Veritaseum Capital LLC ("Veritaseum") in connection with its intellectual property rights. We have recently become aware that Coinbase Global, Inc. ("Coinbase") is providing through its Coinbase App and platform, offerings and services that appear to use the patented devices, systems and methods as claimed in Veritaseum's patented IP. We note that the Coinbase App and platform and your products and offerings implement functions covered by Veritaseum's patents.

Please be advised that Veritaseum's Patents are directed to Low Trust and Zero Trust Value Transfer technology as set forth in the claims of U.S. Patent No. 11,196,566 and Japan Patent No. 6813477. Also, there are several pending U.S. and Japanese Patent applications directed to this technology.

- Regarding your Bitcoin, Bitcoin Cash and Litecoin products, we direct your attention to Claims █, █ and █ of U.S. Patent No. 11,196,566, as well as Claims █, █, █, █ and █ of Japan Patent No. 6813477.
- Regarding your use of Ethereum, and its related products and assets, via the Ethereum platform, we direct your attention to Claims █ and █ of U.S. Patent No. 11,196,566, as well as Claims █ and █ of Japan Patent No. 6813477.



Coinbase Global Forensic and Fundamental Analysis

Mr. B. Armstrong
July 3, 2022
Page 2 of 3

- Regarding your use of Solana, and its related products, via the Solana platform, we direct your attention to Claims [REDACTED] and [REDACTED] of U.S. Patent No. 11,196,566, as well as Claims [REDACTED] and [REDACTED] of Japan Patent No. 6813477.
- Regarding use of NFTs in your products and services, we direct your attention to Claims [REDACTED] and [REDACTED] of U.S. Patent No. 11,196,566, as well as Claims [REDACTED] and [REDACTED] of Japan Patent No. 6813477.

Regarding your use of the Bitcoin, Bitcoin Cash, Litecoin, Ethereum, Solana platforms as well as NFTs for your products and offerings that run on top of and facilitate said platforms, we direct your attention to one or more of Claims [REDACTED] and [REDACTED] of U.S. Patent No. 11,196,566, as well as Claims [REDACTED] and [REDACTED] of Japan Patent No. 6813477. Your products and offerings that are covered by U.S. Patent No. 11,196,566 and Japan Patent No. 6813477 include, but are not necessarily limited to:

- Coinbase Exchange and Coinbase Pro Exchange
- Wallet
- NFT
- Earn
- Card
- Borrow
- Payroll
- Private Client
- USD Coin
- Prime
- Commerce
- Asset Hub
- Ventures
- Commerce
- Rosetta
- Participate
- Prime API

We are agreeable to providing Coinbase with a reasonable amount of time to respond. However, we believe the situation is clear and look to receive your response within 14 days of the date of this letter.

We welcome a request for a meeting if it helps to resolve this matter. We are quite open to discussions that may involve licensing one of more of the above noted patents. In any event we would request that you give this matter your immediate attention.



Coinbase Global Forensic and Fundamental Analysis

Mr. B. Armstrong
July 3, 2022
Page 3 of 3

We await your response.

Very truly yours,

BRUNDIDGE & STANGER, P.C.

Carl I. Brundidge

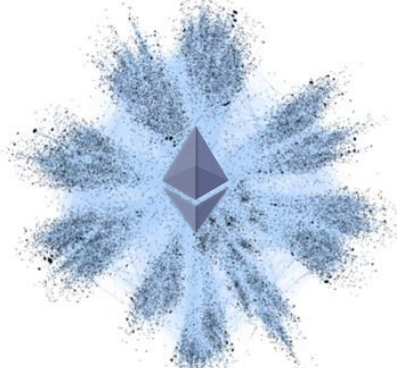
CIB/cb

Enclosures:
U.S. Patent No. 11,196,566
Japan Patent No. 6813477

Coinbase Global Forensic and Fundamental Analysis

Ethereum

Ethereum as a World Computer
Value Transfer through Smart Contracts
 Interaction with the Ethereum EVM to transfer value via Smart Contracts.



POS Transaction Fee
 Payment of a transaction fee from the user to the block producer (and attesting validator nodes) for using the Ethereum Network

POW Transaction Fee
 Payment of a transaction fee from the user to the block producer for using the Ethereum Network.



What Do the Foundational TechDeFi Patents US11196566 & JP6813477 Mean for Users of Ethereum? Twitter Discussion:
 @reggiemiddleton @veritaseuminc



The effective application of smart contracts and compensation payments to validators in the Ethereum ecosystem are covered by the aforementioned patented technology, which includes the projects and service providers that run on top of, alongside, or use Ethereum.



Ethereum IP Assessment:
 Analyzing and Assessing Middleton Patents
 JP6813477B2 and US11196566B2

4th January 2022

Contents	
1. Introduction	3
2. Patent Claim Assessment 1	4
2.1 Incentive Payment to Miner as part of a Transaction Call	4
2.1.1 Overview	4
2.1.2 Background	6
2.1.3 Claim (US Patent – Device Claim)	11
2.1.5 Claim (JP Patent – System Claim)	27
2.1.6 Claim (JP Patent – System Claim)	31
2.2 General Notes	44
3. Patent Claim Assessment 2	46
3.1 Paying Block Rewards to Validators under Proof of Stake	46
3.1.1 Overview	46
3.1.2 Background	49
Ethereum 2.0 - The current progress of PoS Implementation	49
Ethereum 2.0 - Proof-of-Stake	50
Ethereum 2.0 - Beacon Chain State and State Transition	51
Ethereum 2.0 - Deposit to Become a Validator	54
Submit deposit	54
Process deposit	54
Validator index	55
Ethereum 2.0 - Validator Keys	55
3.1.3 Claim (US Patent – Device Claim)	57
Attesting	63
Construct aggregate	63
3.1.4 Claim (US Patent – Device Claim)	64
3.1.5 Claim (US Patent – Device Claim)	66
3.1.5 Claim (US Patent – Device Claim)	68
3.1.6 Claim (JP Patent – System Claim)	70
3.1.7 Claim (JP Patent – System Claim)	71
3.1.4 Claim (JP Patent – System Claim)	80
3.2 General Notes	82

Figures

No table of figures entries found.



Coinbase Global Forensic and Fundamental Analysis

Solana

The effective application of smart contracts and compensation payments to validators in the Solana ecosystem are covered by the aforementioned patented technology, which includes the projects and service providers that run on top of, alongside or use Solana.

Veritaseum

Solana - IP Assessment



Solana IP Assessment:
Assessing Infringement of Middleton Patents
JP6813477B2 and US11196566B2

4th January 2022

Page 1 of 79

Veritaseum

Solana - IP Assessment

Contents

1. Introduction	3
2. Solana Overview	4
3. Patent Claim Assessment 1	7
3.1 Payment to Lead Validator as part of a Transaction	7
3.1.1 Application State Transaction	7
3.1.2 Voting Transaction	7
3.1.3 Claim Overview	7
3.1.4 Claim (US Patent – Device Claim)	10
3.1.5 Claim (US Patent – Device Claim)	25
3.1.6 Claim (US Patent – System Claim)	27
3.1.7 Claim (JP Patent – Device Claim)	41
3.1.8 Claim (JP Patent – Device Claim)	56
3.1.8 Claim (JP Patent – System Claim)	58
3.1.9 Claim (JP Patent – System Claim)	72
4. Patent Claim Assessment 2	76
4.1 Paying Rent from Accounts to Validators	76
4.1.1 Overview	76
4.1.2 Claim Assessment	77
5. Patent Claim Assessment 3	78
5.1 Paying Rewards to Validators under Proof of Stake	78
5.1.1 Overview	78
5.1.2 Claim Assessment	79
5.1.3 Claim (US Patent – Device Claim)	79

Figures

No table of figures entries found.

Page 2 of 79

Coinbase Global Forensic and Fundamental Analysis

Bitcoin

Although Bitcoin predates the aforementioned patents, and it's original code and its whitepaper may be considered prior art, the significant and material improvements incorporated into the Bitcoin code and platform infringe on multiple claims of both patents. As a result, many of the various products, platforms and services built on top and alongside Bitcoin also infringe on said claims.

How



Devices, systems, and methods for facilitating low trust and zero trust value transfers

Abstract

Devices, systems, and methods enabling parties with little trust or no trust in each other to enter into and enforce value transfer agreements conditioned on input from or participation of a third party, over arbitrary distances, without special technical knowledge of the underlying transfer mechanism(s), optionally affording participation of third-party mediators, substitution of transferors and transferees, term substitution, revision, or reformation, etc. Such value transfers can occur reliably without involving costly third-party intermediaries who traditionally may otherwise be required, and without traditional exposure to counterparty risk.

US11196566B2

United States



Download PDF



Find Prior Art



Similar

Inventor: Reginald Middleton, Matthew Bogosian

Powered by 

Veritaseum

Does Bitcoin Infringe on the Patent for conditional transfer of value?

Bitcoin's scripting system has been upgraded to allow a transaction output to be made unspendable until some point in the future.

Key Points

- This feature allows the enforcement of a complete locking capability (until the expiration time – such as Escrow) as described by the Patents JP6813477B2 & US11196566. This brings the Bitcoin Network under the scope of the Patents and it's claims primary building blocks– Principle, Datasource and Expiration Timestamp
- Claim language describes this functionality explicitly: **"the first computer processor is further configured to obtain the output data on or after the expiration timestamp"**

Bitcoin Core has been updated to introduce a Partially Signed Bitcoin Transaction (PSBT) as a Bitcoin standard that facilitates portability of unsigned transactions, which allows multiple parties to easily sign the same transaction.

Key Points

- Before the introduction of PSBT, the ability to achieve the same outcome was implementation specific. The PSBT became a Bitcoin Network standard and thus brings Bitcoin, as a platform and network, under the scope of the JP6813477B2 & US11196566 Patents.
- Claim language describes this functionality explicitly: **"The first client signs (i.e., computes a cryptographic signature and associates it with) a first principal input of an inchoate commit transaction record for creating a complete commit transaction record, the inchoate commit transaction record comprising:**



Coinbase Global Forensic and Fundamental Analysis

Veritaseum Significant Parts of Bitcoin's Zero Trust/DeFi Components Have Been Patented by Reggie Middleton

DeFi Patents US11196566, JP6813477

...Party A wishes to purchase goods from Party B. The parties do not know each other well. Party B wants assurances of availability of funds from Party A, but Party A does not want to release those funds to Party B (or an assignee) until Party B has demonstrated proof of shipment (or some other condition)...

... a first device called a "client" and a second client participate in a series of transactions where assets (e.g., unspent transaction outputs) from a first party and assets from a second party are committed until a combination of two of the first party, the second party, and an intermediary release them in accordance with a calculation by the intermediary based on observation of external state, such as the relative value of certain financial instruments at a specific time.

The assets may be refunded if no such observation can be made by an expiration timestamp

...In a typical embodiment, a refund transaction record is not created until well after the commit transaction or it is created such that it is only valid after a certain time in the future and only if the commit output has not yet been spent

Present Day Bitcoin (BTC/BCH/BCG)

Trustless Payments for Publishing Data

The PayPub protocol makes it possible to pay for information in a trustless way by first proving that an encrypted file contains the desired data and secondly crafting scriptPubKeys used for payment such that spending them reveals the encryption keys to the data. However the existing implementation has a significant flaw: the publisher can delay the release of the keys indefinitely.

This problem can be solved interactively with the refund transaction technique with

CHECKLOCKTIMEVERIFY the problem can be non-interactively solved using scriptPubKeys of the following form:

The buyer of the data is now making a secure offer with an expiry time. If the publisher fails to accept the offer before the expiry time is reached the buyer can cancel the offer by spending the output.



Bitcoin Network Partially Signed Bitcoin Transaction (PSBT)

A Partially Signed Bitcoin Transaction (PSBT) is a Bitcoin standard that facilitates portability of unsigned transactions, which allows multiple parties to easily sign the same transaction.

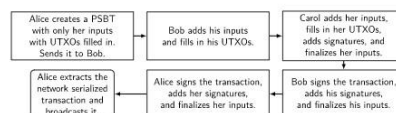
Motivation

Creating unsigned or partially signed transactions to be passed around to multiple signers was implementation dependent, making it hard for people who use different wallet software from being able to easily do so. The goal of the PSBT incorporation was to create a standard and extensible format that can be used between clients to allow people to pass around the same transaction to sign and combine their signatures. The format is also designed to be easily extended for future use which is harder to do with what was the extant transaction formats.

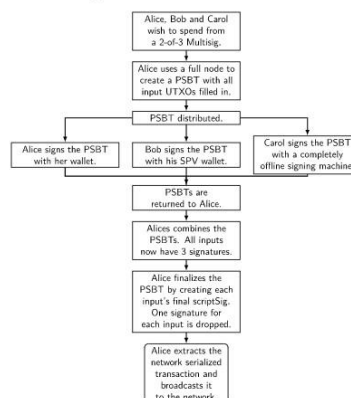
Signing transactions also requires users to have access to the UTXOs being spent. This transaction format allows offline signers such as app wallets and hardware wallets to be able to sign transactions without needing direct access to the UTXO set and without risk of being defrauded.

```
BIP: 174
Layer: Applications
Title: Partially Signed Bitcoin Transaction Format
Author: Andrew Chow <achow101@gmail.com>
Comments-Summary: No comments yet.
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BIP-0174
Status: Final
Type: Standards Track
Created: 2017-07-12
License: BSD-2-Clause
```

Manual CoinJoin Workflow



2-of-3 Multisig Workflow





Coinbase Global Forensic and Fundamental Analysis

Veritaseum Bitcoin Network – Partially Signed Bitcoin Transaction (PSBT) Roles & Patent Assessment

Role	Bitcoin Core	JP6813477B2, US11196566Patent Assessment
Creator Updater	The Creator creates a new PSBT. It must create an unsigned transaction and place it in the PSBT. The Creator must create empty input and output fields. The Updater must only accept a PSBT. The Updater adds information to the PSBT that it has access to. If it has the UTXO for an input, it should add it to the PSBT. The Updater should also add <code>redeemScripts</code>, <code>witnessScripts</code>, and BIP 32 derivation paths to the input and output data if it knows them. A single entity is likely to be both a Creator and Updater.	Client 1 - Inchoate Transaction: The Inchoate Transaction is created by the Client performing the 'Creator' role.
Input Finalizer Transaction Extractor	The Input Finalizer must only accept a PSBT. For each input, the Input Finalizer determines if the input has enough data to pass validation. If it does, it must construct the <code>0x07 Finalized scriptSig</code> and <code>0x08 Finalized scriptWitness</code> and place them into the input key-value map. If <code>scriptSig</code> is empty for an input, <code>0x07</code> should remain unset rather than assigned an empty array. Likewise, if no <code>scriptWitness</code> exists for an input, <code>0x08</code> should remain unset rather than assigned an empty array. All other data except the UTXO and unknown fields in the input key-value map should be cleared from the PSBT. The UTXO should be kept to allow Transaction Extractors to verify the final network serialized transaction. The Transaction Extractor must only accept a PSBT. It checks whether all inputs have complete <code>scriptSigs</code> and <code>scriptWitnesses</code> by checking for the presence of <code>0x07 Finalized scriptSig</code> and <code>0x08 Finalized scriptWitness</code> typed records. If they do, the Transaction Extractor should construct complete <code>scriptSigs</code> and <code>scriptWitnesses</code> and encode them into network serialized transactions. Otherwise the Extractor must not modify the PSBT. The Extractor should produce a fully valid, network serialized transaction if all inputs are complete. https://github.com/bitcoin/bips/blob/master/bip-0174.mediawiki#roles	Complete Transaction: The Complete Transaction is created by the Client performing the 'Input Finalizer' and 'Transaction Extractor' roles. Note that all signatories will have signed the inputs which will be in the 'finalized <code>sigScript</code>' field. <i>Note:</i> The Transaction Extractor does not need to know how to interpret scripts in order to extract the network serialized transaction. However it may be able to in order to validate the network serialized transaction at the same time. A single entity is likely to be both a Transaction Extractor and an Input Finalizer
Signer	The Signer must only accept a PSBT. The Signer must only use the UTXOs provided in the PSBT to produce signatures for inputs. Before signing a non-witness input, the Signer must verify that the TXID of the non-witness UTXO matches the TXID specified in the unsigned transaction. Before signing a witness input, the Signer must verify that the <code>witnessScript</code> (if provided) matches the hash specified in the UTXO or the <code>redeemScript</code>, and the <code>redeemScript</code> (if provided) matches the hash in the UTXO. The Signer may choose to fail to sign a <code>segwit</code> input if a non-witness UTXO is not provided. [7] The Signer should not need any additional data sources, as all necessary information is provided in the PSBT format. The Signer must only add data to a PSBT. Any signatures created by the Signer must be added as a "Partial Signature" key-value pair for the respective input it relates to. If a Signer cannot sign a transaction, it must not add a Partial Signature. The Signer can additionally compute the addresses and values being sent, and the transaction fee, optionally showing this data to the user as a confirmation of intent and the consequences of signing the PSBT.	Device/Facilitator: The Bitcoin Network (i.e., Bitcoin Blockchain as a state machine) that facilitates the sharing and manipulation of the PSBT for ultimate serialisation and submission to the blockchain. As per the patent definitions: "facilitator" (100)—A device for facilitating a value transfer between a first party utilizing a first client (120, 160) and a second party utilizing a second client (120, 170) via a transfer mechanism (110) according to the invention, the device comprising a computer processor (160), a memory (170) comprising a transaction record sector and a key pair sector (200) for storing an asymmetric key pair, and a network interface (190).
Combiner	The Combiner can accept 1 or many PSBTs. The Combiner must merge them into one PSBT (if possible), or fail. The resulting PSBT must contain all of the key-value pairs from each of the PSBTs. The Combiner must remove any duplicate key-value pairs, in accordance with the specification. It can pick arbitrarily when conflicts occur. A Combiner must not combine two different PSBTs. PSBTs can be uniquely identified by <code>0x00</code> global transaction typed key-value pair. For every type that a Combiner understands, it may refuse to combine PSBTs if it detects that there will be inconsistencies or conflicts for that type in the combined PSBT.	Transfer Mechanism: The Bitcoin Network includes miners and nodes for receiving complete transactions for inclusion in the mined block.

6. FINANCIALS – HISTORICALS

6.1. Components of Results of Operations

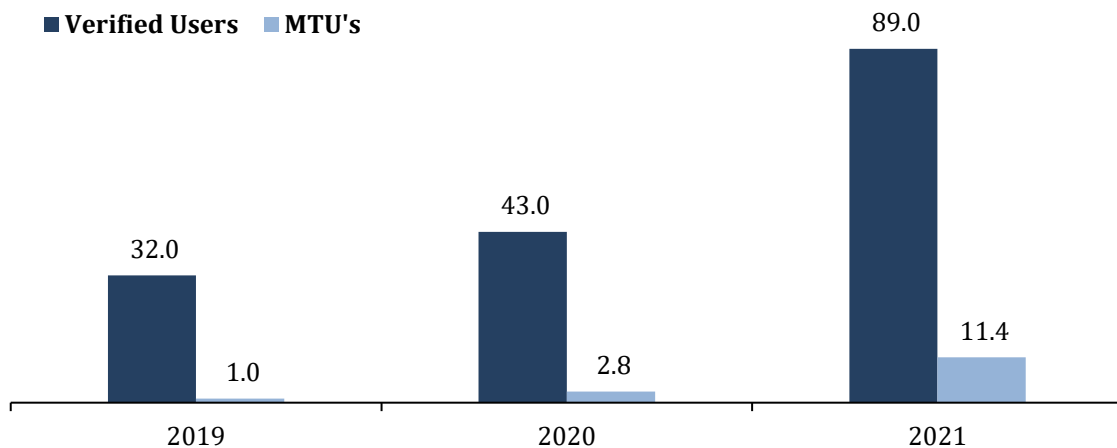
Net Revenue

Transaction-Based Revenue

Coinbase generates the majority of its net income from transaction fees from trades that take place on its platform. The transaction fee is calculated depending on the price and quantity of the crypto asset purchased, sold, or withdrawn. Transaction revenue is recorded at the moment of transaction processing and is directly proportional to trading volume on its platform.

Other key business factors that are affecting Company's revenue are:

Figure 13: Verified and Monthly Transacting Users (in millions) 2019-2021



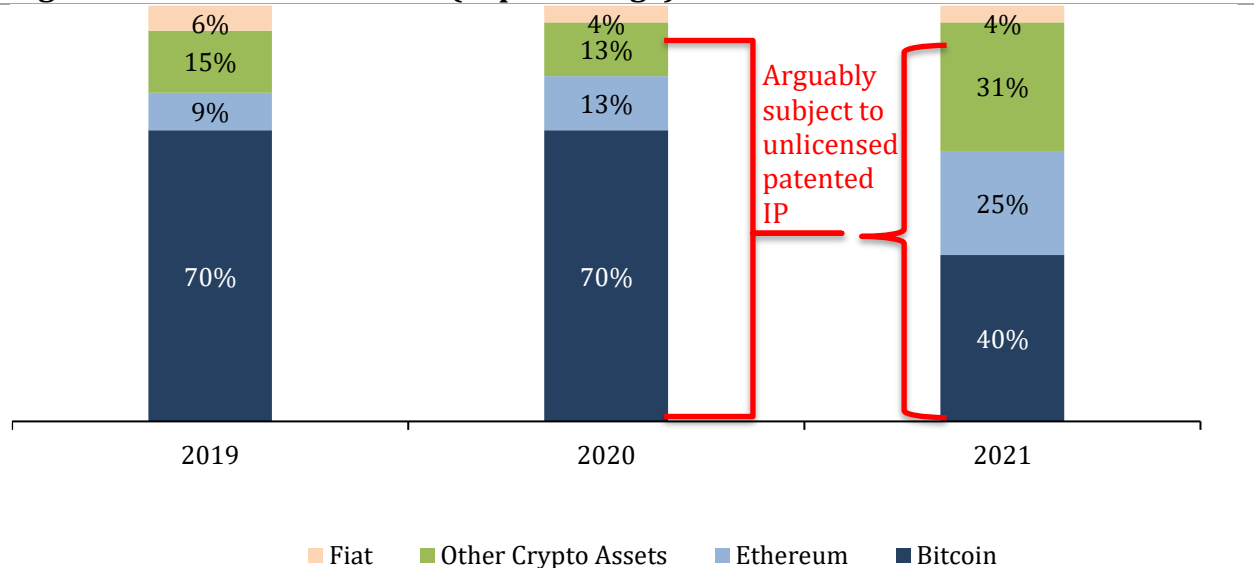
Source: Coinbase Annual Reports

- **Verified Users:** "Verified Consumers" are defined by Coinbase as all retail users, institutions, and ecosystem partners who have made an account on the platform and validated either their email address or phone number. Verified Users offer a possible income opportunity and a sign of the Company's scale. The top level of the customer acquisition funnel is verified users.
- **Monthly Transacting Users:** A retail user who actively or passively transacts one or more goods on the platform at least once during the rolling 28-day period ending on the date of measurement is defined as an MTU by the Company. MTUs provided at the end of a year indicate MTUs for the previous quarter. MTUs conduct transactions that produce transaction, subscription, and service income. Active transactions such as purchasing or selling crypto assets, as well as passive activities such as collecting a staking incentive, are examples of revenue-generating transactions. MTUs also participate in non-revenue producing transactions such as transmit and receive.
- **Assets on the platform:** "Assets on Platform" are defined by Coinbase as the entire US dollar equivalent value of both fiat money and crypto assets owned or managed in digital wallets on the platform, including custody services. The volume of balances held throughout the firm's portfolio of goods and services, the trust consumers have in the

Coinbase Global Forensic and Fundamental Analysis

Company to safely hold their assets, and the underlying expansion of the crypto economy are all demonstrated by Assets on Platform. Assets on the Platform offer monetization potential for subscription products and services, such as Custody, Stake, Borrow and Lend. When clients interact with platform assets, fees are generated that are reported as subscription and service revenue.

Figure 14: Assets on Platform (in percentage) 2019-2021



Source: Coinbase Annual Reports

- **Trading Volume:** "Trading Volume" is defined by Coinbase as the total US dollar equivalent value of matched transactions conducted between a buyer and seller via the platform during the measurement period. Trading volume is the product of the amount of asset transacted and the trading price at the moment the transaction was completed.

Subscription and Service-Based Revenue

The majority of subscription and service revenue is made up of:

- **Blockchain Rewards:** Controlling the staking validator address in numerous blockchain protocols provides the Company with blockchain benefits. Users are rewarded for participating in various blockchain activities such as the proof-of-stake consensus mechanism by blockchain protocols or protocol network participants. Coinbase is compensated with Blockchain incentives in the form of cryptocurrencies.
- **Custodial fee revenue:** Custodial fee revenue is calculated as a percentage of the daily value of clients' crypto assets maintained in a specialized cold storage service. The amount, price, and kind of crypto asset held in custody are governed by the same rules that influence the value of assets on the platform.
- **Earn campaign revenue:** The Company provides a platform for asset issuers to educate consumers via videos and tasks, with users earning crypto assets for completing the activities. The Company is paid a commission based on the total amount of crypto assets provided to consumers.



Coinbase Global Forensic and Fundamental Analysis

- **Interest Income:** The Company makes interest income in fiat currency under a revenue-sharing agreement with the customer and by taking custody of the client's fiat cash at third-party banks. The income is determined using the interest technique based on the balance of such fiat funds and current interest rates. Interest earned on loans to retail and institutional users is also included in interest income.
- **Other:** Additional subscriptions and services Revenue is mainly comprised of Coinbase Cloud fees, which consists of staking application, delegation, and infrastructure services, as well as subscription licensing revenue.

Other Revenue

Other sources of revenue include the selling of cryptocurrency assets, where Coinbase plays the primary role in the transaction. As a courtesy to consumers, the Company may, from time to time, perform customer transactions using its own crypto assets. It fulfills client accommodation transactions with its assets for orders that do not reach the minimum trade size for execution on its platform or to preserve customers' trade execution and processing times during unplanned system outages. Coinbase has custody and control of these crypto assets before sale to the consumer, and income is recorded when the transaction is performed. As a result, the whole transaction amount is recorded as revenue, and the cost of the crypto asset is recorded as other operating expenditure.

Operating Expenses

Transaction, technology and development, sales and marketing, general and administrative, restructuring, and other operational expenditures are all part of the operating expenses.

- **Transaction Expense:** Transaction charges cover the price of running the Platform, processing crypto-asset trades, and providing wallet services. Account verification fees, miner fees for processing transactions on blockchain networks, fees paid to payment processors and other financial institutions for user transaction activity, and crypto-asset losses due to transaction reversals are all part of these expenses. Transaction costs also include incentives given to users for blockchain activity carried out by the Company, such as staking. Fixed-fee expenses are expensed over the contract's life, whereas transaction-level costs are expensed as they are incurred.
- **Technology and Development:** Technology and development expenses include personnel costs associated with managing, maintaining, and improving platforms. Website hosting, infrastructure fees, development expenditures for new goods and services, and amortization of purchased generated technology are all also included in these costs.
- **Sales and Marketing:** Customer acquisition costs, advertising and marketing programs, and personnel-related expenses are all major components of sales and marketing expenses.
- **General and administrative:** personnel-related costs incurred to support company activities, such as legal, finance, compliance, human resources, customer service, executive, and other support tasks, are included in general and administrative expenses.

Coinbase Global Forensic and Fundamental Analysis

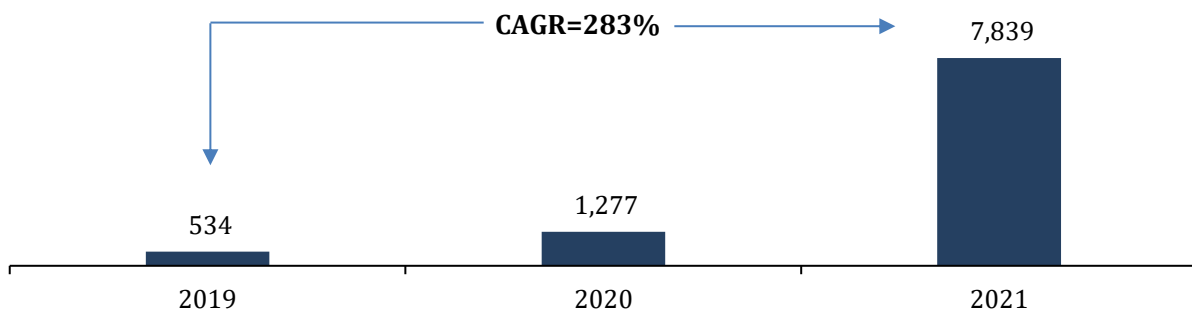
These expenditures include software subscriptions for support services, facility and equipment expenses, depreciation, amortization, gains and losses on fixed asset sales, etc.

- **Other operating expenses, Net:** Other operational expenses net include the cost of cryptocurrency assets required to complete client accommodation transactions. As a courtesy to consumers, it may, from time to time, complete customer transactions using its own crypto assets. Prior to the sale to the consumer, Coinbase has custody and control of the crypto assets. As a result, the whole amount of the transaction is recorded as other revenue, while the cost of the crypto asset is recorded as another operating expenditure. Other operating expenditure, net comprises impairment and realized profits on the sale of crypto assets, realized gains and losses on derivative instrument settlement, and fair value gains and losses on derivatives and derivatives recognized in qualifying fair value hedging accounting relationships.
- **Other Expense (Income), Net:** Other income (expenses) net comprises the following items:
 - Net profits and losses on investments, which generally consist of realized and unrealized gains and losses from fair value adjustments on assets.
 - Realized foreign exchange impacts from the settlement of foreign currency assets and liabilities, as well as unrealized foreign exchange impacts from the remeasurement of transactions and monetary assets and liabilities denominated in non-functional currencies.
 - Interest in Convertible Notes and Senior Notes.

6.2. Total Revenue

In 2021, the Company registered revenue of US\$7,839 million, exhibiting an impressive growth at a CAGR of 283% during 2019-2021. The significant increase in revenues was primarily driven by the rise in trading volume with the increase in MTUs, and the average price of Bitcoin, Ethereum, and other crypto assets. The Company also witnessed a surge in the number of crypto assets supported on its platform.

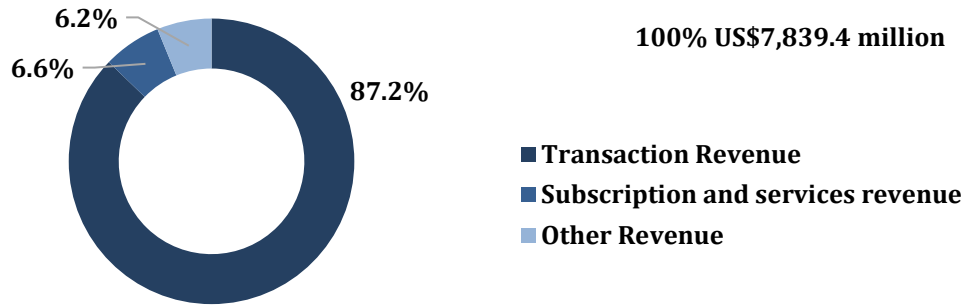
Figure 15: Historical Revenue Growth (US\$ million): 2019-2021



Source: Coinbase Annual Reports

Coinbase Global Forensic and Fundamental Analysis

Figure 16: Revenue by Segment, 2021



Source: Coinbase Annual Reports

On a segmental basis, transaction revenue grew at a CAGR of ~284% during 2019-2021, attributable to the following factors:

- A 633% rise in Retail Trading Volume in 2021, as a result of a growth in both MTUs (monthly transacting users) and the average price of Bitcoin, Ethereum, and other crypto assets.
- A rise in the number of crypto assets supported by the platform, which was 30+ in 2019 and 45 in 2020, further rose to 139 in 2021. The capacity of Coinbase to support more crypto assets prompted huge trading volume.

Subscription and services revenue grew at a CAGR of ~409% during 2019-2021, attributable to the following factors:

- A 4,429% increase in custodial fee revenue from 2019-2021 resulted from an increase in the number of customers and crypto assets held under custody.
- An increase in blockchain rewards & earn campaign revenue as a result of increased user participation & MTUs.

Other revenue during 2019-2021 grew by US\$433.9 million, resulting from a rise in crypto-asset sales revenue over the same period. Coinbase made revenue from crypto-asset sales in which transactions were completed with Company's crypto assets to accommodate consumers.

6.3. Total Operating Expenses

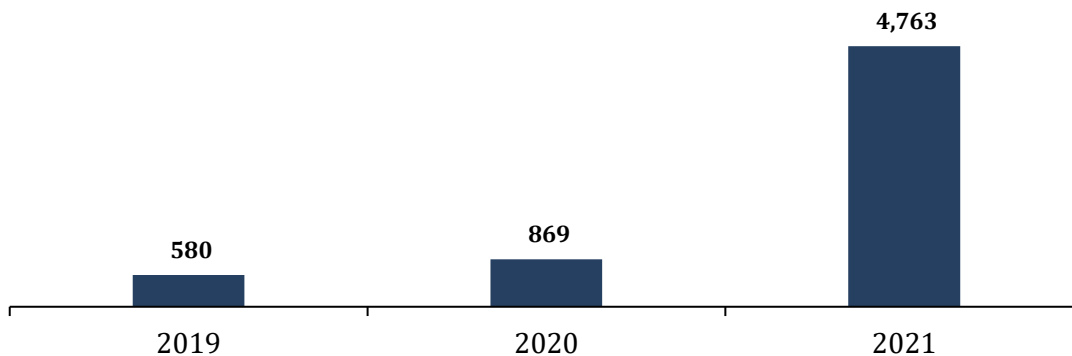
The total operating expenses during 2019-2021 rose by ~US\$4,183 million. The following expenses segment showed an increase in the figures resulting in an increase in the overall operating expense:

Transaction expenses grew by ~US\$1,186 million from 2019-2021.

Technology & development expense and Sales & Marketing expenses grew by ~US\$1,106 million and US\$639.5 million during 2019-2021.

In addition to the expenses above, general & administrative and other operating expenses also increased by US\$677.5 million and US\$584.1 million.

Figure 17: Overall Operating Expense (US\$ million): 2019-2021



Source: Coinbase Annual Reports

6.4. Total Operating Income / (Loss)

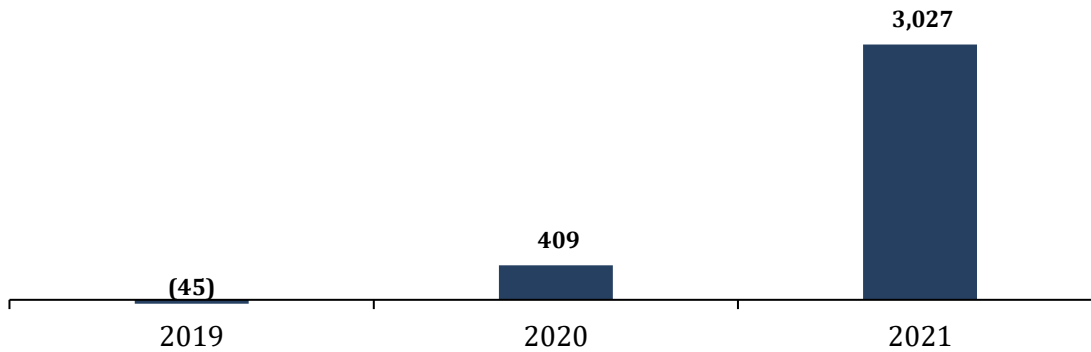
Even with the increase in overall expenses, the Company's EBITDA improved in 2021 compared to 2020 and 2019.

In 2021 the Company witnessed an increase in overall expenses, which stood at US\$4,762.9 million; this increase was due to the following factors:

- A major increase in transaction expenses, including miner fees, transaction reversal losses, rewards paid & payment processing fees.
- An increase in technology and development expenses was owing to the rise in the cost of software and services.
- An increase in sales and marketing expenses also contributed to the rise in the overall expense. These expenses include digital advertising, customer referral, and promotion fees.
- An increase in general & administrative expenses due to customer support service and corporate business taxes.

Despite an increase in such expenses, the Company's EBITDA rose by US\$3,072.3 million during 2019-2021, primarily due to a steep rise in revenues resulting from the addition of crypto assets on the platform and a surge in trading volume & users.

Figure 18: Operating Income/ (Loss) (US\$ million): 2019-2021



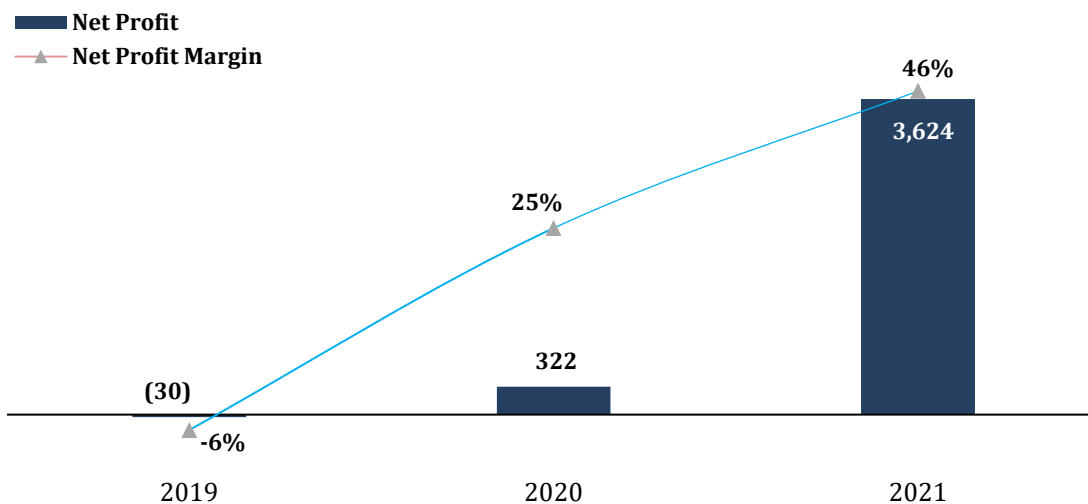
Source: Coinbase Annual Reports

6.5. Net Profit & Net Profit Margin

The Company incurred net losses in 2019; however, it improved in 2020 and reached US\$322.3 million. In the year 2021, net income surges to US\$3,624.1 million, mainly due to a gain in transactional revenue.

During 2019-2021, the net profit margin increased as the Company witnessed outstanding growth in the overall revenue.

Figure 19: Net Profit and Net Profit Margin



Source: Coinbase Annual Reports

7. FINANCIALS – FORECASTED

7.1. Revenue-Based Financials

As shown in the earlier section of this report, the Company's revenue is driven by three key segments - Transaction, Subscription, and Other Revenue.

For detailed insights into projected numbers, revenue is further bifurcated into sub-segments. For instance, Transaction-based Revenue is further sub-divided into two sub-segments; subscription-based revenue has five sub-segments, whereas other revenue has two sub-segments.

The historical data depicts that Coinbase's trading volume is increasing in both segments, i.e., retail and institutional. Furthermore, the company is working to attract new customers to its platform to boost its revenue. It is expected that transaction-based, subscription-based, and other revenue would increase in volume throughout the predicted period, i.e., 2022-2026. Following are some Coinbase growth strategies designed to increase revenue volume:

- **Attract more customers:** Through education, marketing, involvement at developer conferences, crypto community interaction, and the expansion of institutional sales and support teams, the company hopes to improve product acceptance and engagement. In addition, they are broadening access to products and services by introducing new payment options and expanding into new markets. All these factors will help the company to increase its customers.
- **Increasing the depth and breadth of the Company's assets:** The Company intends to continue expanding asset access, support native blockchain protocol capabilities such as staking and governance and increase access to the sorts of crypto assets it offers to users, such as NFTs.
- **Launching creative products:** To give clients with more options to connect with crypto assets, the company wants to offer both first-party products and access to third-party products via the platform. It will also continue to develop APIs and products that will enable other firms to harness its technology and incorporate crypto goods and solutions into their operations. In addition to this, the company is also planning to actively pursue acquisitions of technologies, companies, and products that will help them expand their business and increase their customers. E.g., Bison Trails and FairXchange, Inc.

We have considered the three cases – Base, Best, and Worst cases - to get a clearer and more appropriate picture for future financials. The Best case depicts future growth in the company's business due to changes in the technology and updates of the features in the Company. On the other hand, the Worst case depicts declining growth as technology and the environment evolve quickly in addition to improvements in payment methods and payment processing, resulting in market rivalry at an all-time high.

The graphs depicted below are based on the base case Scenario.

Coinbase Global Forensic and Fundamental Analysis

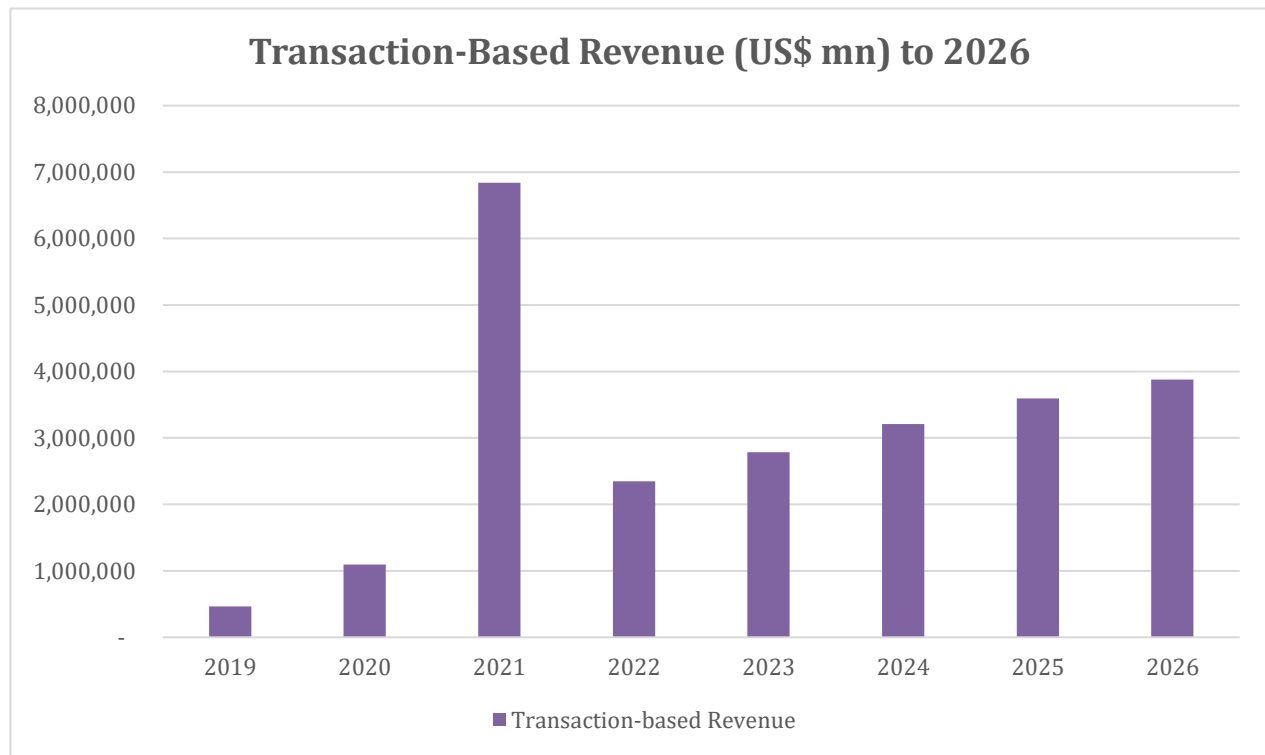
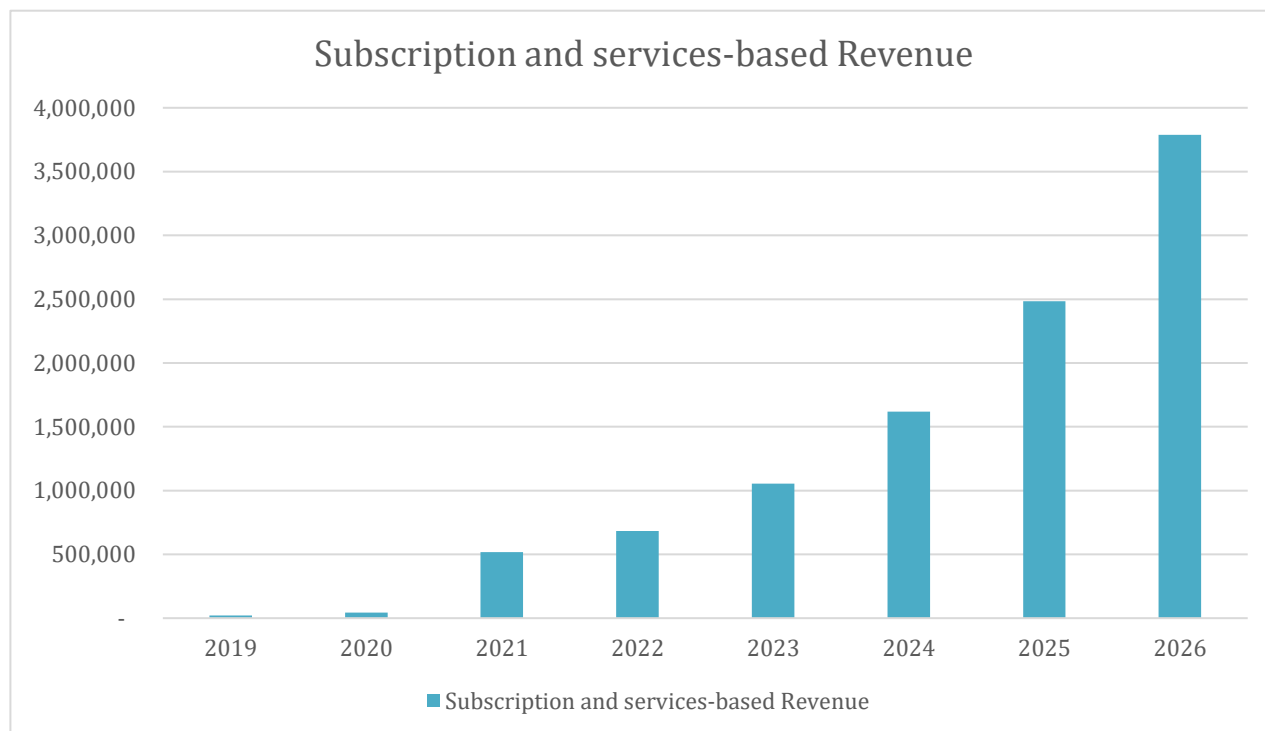
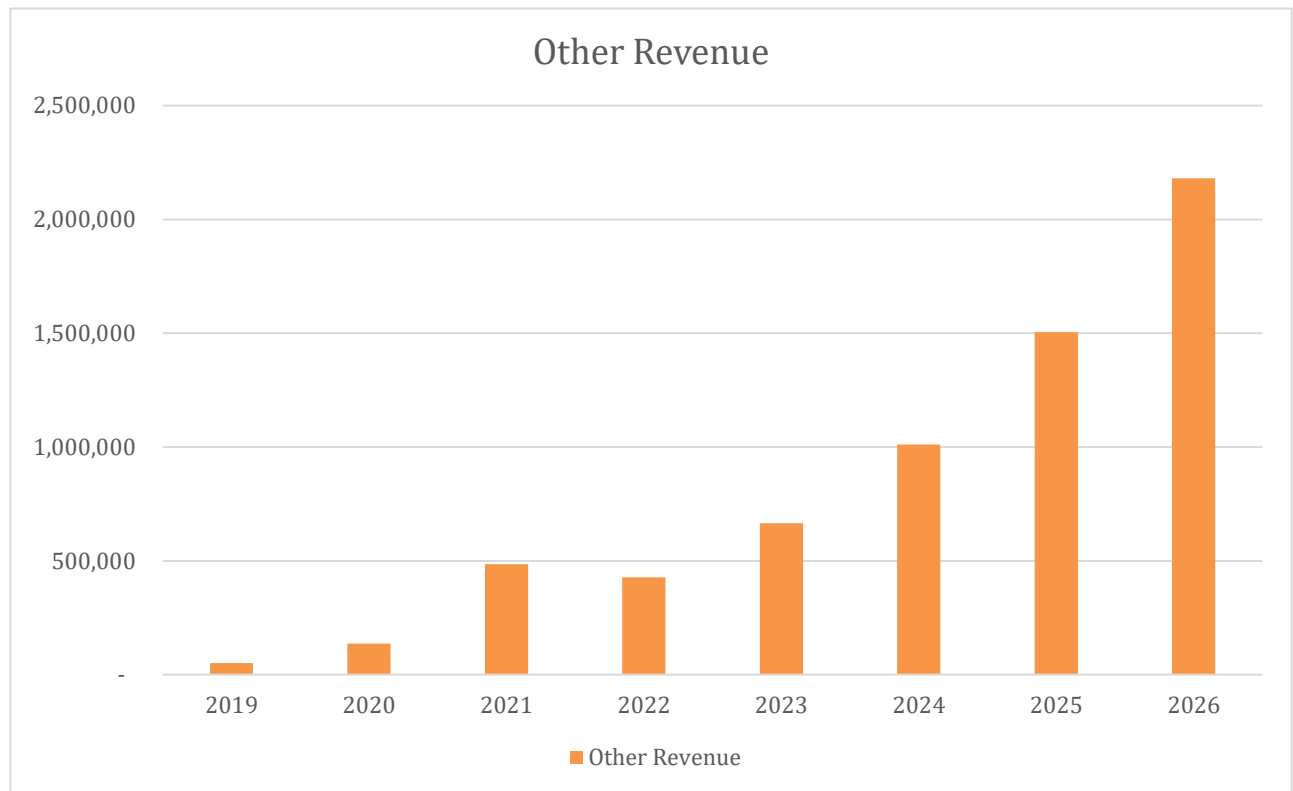


Figure 20: Subscription & Service-Based Revenue (US\$ mn): 2022-2026



Coinbase Global Forensic and Fundamental Analysis



7.2. Operating Expense Financials

The operating expense projections are linked to the expansion of the Company. Operating expenses include transaction expenses, sales and marketing, general and administrative expenses, technology & development, and other operating expenses. It is assumed that all these costs are correlated to the expansion of business. As a result, these costs will rise in line with the expansion.

Figure 21: Transaction-Based Expenses (US\$ mn): 2022-2026

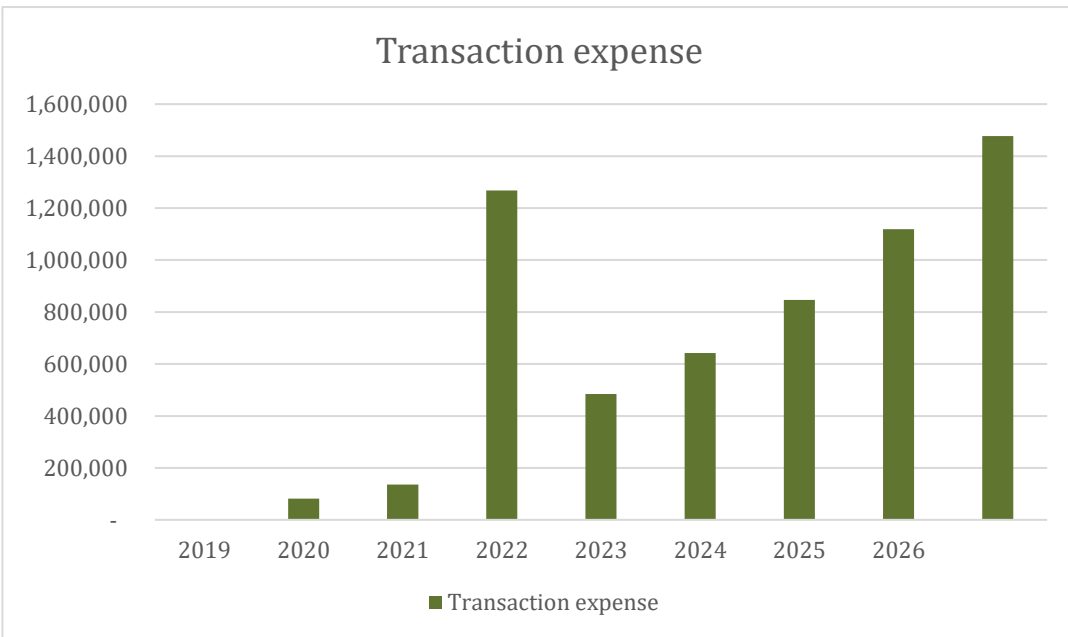
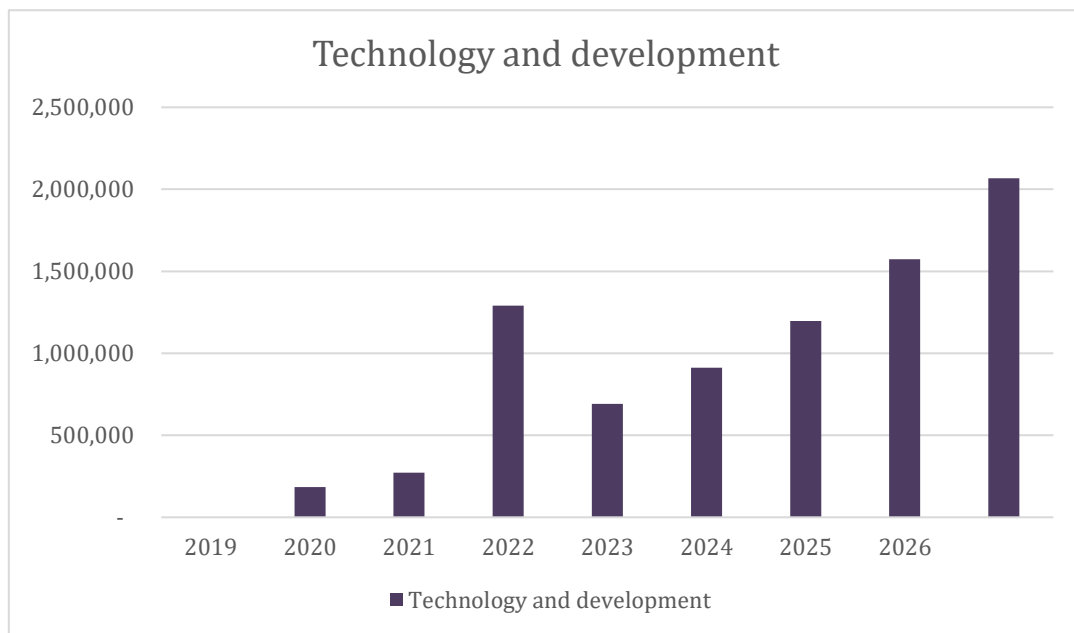


Figure 22: Technology and Development Based Expenses (US\$ mn): 2022-2026



Coinbase Global Forensic and Fundamental Analysis

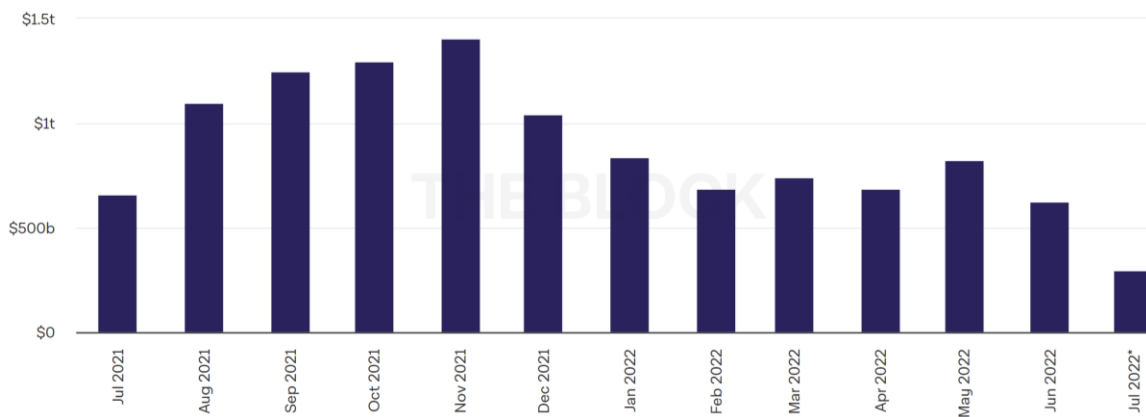
7.3. Total Operating Income

The Company is projected to record an operating profit for the current fiscal year despite transaction volume and crypto asset prices plunging.

This projection is tempered, in large part, by the significant Q2 2022 market correction and resultant shakeout of the industry wherein the more profligate, higher risk and less solvent market participants collapsed, spreading contagion. Of note is the lending and investment provided by CoinbasePro and Coinbase Ventures, both of which are anticipated to suffer heavy losses.



Cryptocurrency Exchange Volume (The Block Legitimate Index)



Summary

Base Case

(All figures are in US\$ thousands, except otherwise specified)

(All figures are in US\$ thousands, except otherwise specified)		Actual	Actual	Actual	Forecasted	Forecasted	Forecasted	Forecasted	Forecasted
Items	Units	2019	2020	2021	2022	2023	2024	2025	2026
Summary Income Statement									
Revenue									
Transaction-based Revenue		463,005	1,096,174	6,837,266	2,346,550	2,783,595	3,207,703	3,592,738	3,877,751
Subscription and services-based Revenue		19,944	44,993	517,487	683,676	1,053,946	1,619,760	2,484,253	3,788,429
Other Revenue		50,786	136,314	484,691	427,320	665,683	1,010,705	1,504,624	2,180,193
Operating Profit		(45,783)	408,951	3,076,570	1,078,754	1,429,773	1,885,728	2,486,769	3,180,378
Total Revenue		533,735	1,277,481	7,839,444	3,457,546	4,503,223	5,838,168	7,581,614	9,846,372
Net Profit		(30,387)	322,317	3,624,120	(634,813)	(2,050,971)	680,206	933,690	1,179,739
Summary Balance Sheet									
Cash and cash equivalents		548,945	1,061,850	7,123,478	5,418,842	8,364,044	11,324,994	15,026,611	19,450,127
Current asset		1,986,946	5,133,948	18,373,863	13,239,745	19,793,024	25,523,031	32,348,262	40,102,678
Non Current asset		404,823	721,466	2,900,562	1,650,704	1,827,513	2,060,562	2,373,980	2,818,208
Total assets		2,391,769	5,855,414	21,274,425	14,890,449	23,227,828	29,463,198	36,875,671	45,358,169
Current liabilities		1,223,444	4,246,855	11,419,035	5,677,294	7,379,733	9,551,611	12,387,026	16,087,066
Non-Current Liabilities		106,542	82,508	3,473,701	3,466,279	3,468,441	3,471,178	3,474,735	3,479,626
Total liabilities		1,329,986	4,329,363	14,892,736	9,143,573	10,848,174	13,022,789	15,861,760	19,566,691
Shareholders' Equity		1,061,783	1,526,051	6,381,689	5,746,876	(230,499)	1,583,795	3,876,608	6,526,918
Share capital		93,820	231,024	2,034,658	2,034,658	2,034,658	2,034,658	2,034,658	2,034,658
Summary Cash Flow Statement									
Cash from Operating Activities		(80,594)	3,004,070	10,730,031	(5,498,401)	1,474,556	2,680,198	3,534,715	4,551,552
Cash from Investing Activities		(105,353)	50,822	(1,124,740)	631,374	(104,199)	(131,848)	(171,361)	(235,672)
Cash from Financing Activities		(16,605)	18,801	3,284,225	-	-	-	-	-
Key Ratios									
Revenue Growth		0.0%	139.3%	513.7%	-55.9%	30.2%	29.6%	29.9%	29.9%
EBITDA Margin		-8.6%	34.4%	40.0%	32.2%	32.5%	32.9%	33.3%	32.7%
Operating Profit Margin		-8.6%	32.0%	39.2%	31.2%	31.8%	32.3%	32.8%	32.3%
Net Profit Margin		-5.7%	25.2%	46.2%	-18.4%	-16.8%	11.7%	12.3%	12.0%
Current Ratio		1.6	1.2	1.6	2.3	1.0	1.0	1.1	1.1
Return-on-Assets (ROA)		-1.3%	7.8%	26.7%	-3.5%	-9.2%	6.9%	6.9%	6.4%
Return-on-Equity (ROE)		-2.9%	24.9%	91.7%	-10.5%	-258.0%	268.1%	84.0%	51.0%



Coinbase Global Forensic and Fundamental Analysis

7.4. DLT Patent Infringement Expense

We have assumed patent charges (infringement cost) equivalent to 0.0%, 48.1%, and 50% of the revenues in Best, Base, and Worst cases, respectively for the first year, which include punitive damages. The infringement cost will rise in tandem with the company's revenue and is levied as a percentage of revenue but derived from historical profit growth., but the punitive damages are modelled for one year only. Punitive damages won't come into play if the company does not litigate, litigates and wins or negotiate a pre-trial settlement. As sales rise, so will the cost of infringement/patent charges.

The levied Infringement/patent charges that were modelled are not resulting in operating losses, but will register net income losses for two years if the company unsuccessfully challenges the patent(s) in court (resulting in punitive damages), and considerably steeper losses still if all three of the patent families from the three entities mentioned above have to be dealt with through litigation. The most favorable risk/reward scenario modelled is settlement.

Other Expense / (Income)

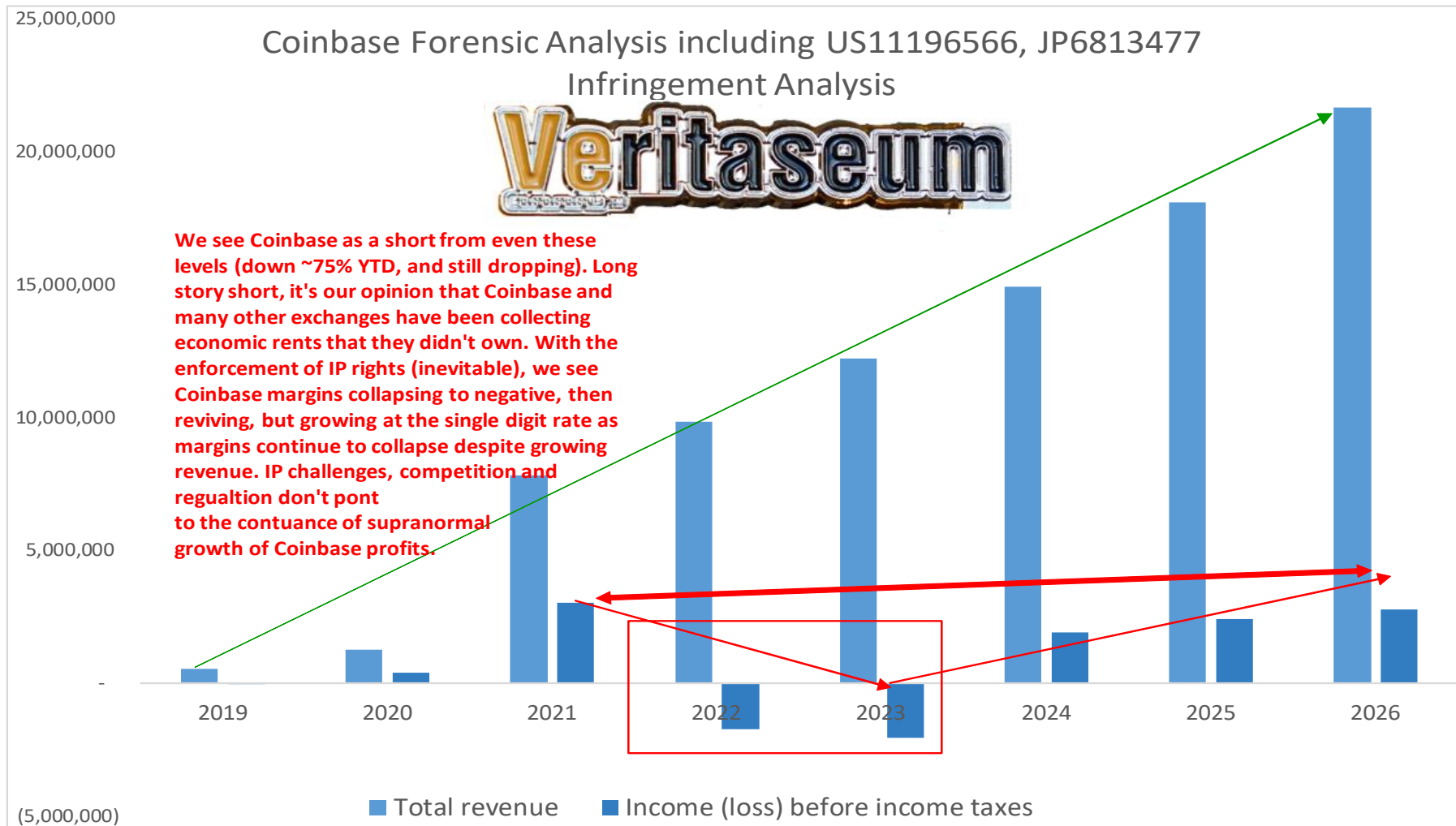
(All figures are in US\$ thousands, except otherwise specified)

		Base Case			Veritaseum				
Items	Units	Actual	Actual	Actual	Forecasted	Forecasted	Forecasted	Forecasted	Forecasted
		2019	2020	2021	2022	2023	2024	2025	2026
Revenue		533,735	1,277,481	7,839,444	3,457,546	4,503,223	5,838,168	7,581,614	9,846,372
Transaction Revenue		463,005	1,096,174	6,837,266	8,300,248	9,846,169	11,346,241	12,707,992	13,715,753
Other Expenses / (Income)									
Other expense (income), net		(367)	(248)	49,623	49,623	49,623	49,623	49,623	49,623
Total subscription and services revenue		(367)	(248)	49,623	49,623	49,623	49,623	49,623	49,623
Infringement Cost									
US11196566, JP6813477 Licensing Cost					1,663,944	2,352,729	1,123,847	1,459,461	1,895,427
As a % of Revenue		0.0%	0.0%	0.0%	48.1%	19.3%	19.3%	19.3%	19.3%
Fiat (excluded from infringement calc.)	4%								
Other crypto Assets	31%								
Bitcoin	25%								
Ethereum	21%								
Total Revenue Contribution to Infringement Calculation	77%				2,662,310.49	3,467,481.81	4,495,389.15	5,837,842.89	7,581,706.61
US11196566, JP6813477 Licensing Fee Contribution to Total	25%				665,577.62	866,870.45	1,123,847.29	1,459,460.72	1,895,426.65
US11196566, JP6813477 Punitive Damages	150%				998,366.43	3,529,094.18			
Total Likely Payments to US11196566, JP6813477 Infringement					1,663,944.06	4,740,621.58	1,123,847.29	1,459,460.72	1,895,426.65
As a % of Total Revenue					48.1%	48.1%	19.3%	19.3%	19.3%



Coinbase Global Forensic and Fundamental Analysis

7.5. Net Income / (Loss)



The Company is expected to register Net Losses between 2022 and 2023, then nominal profit growth until 2026 under the base case.



Coinbase Global Forensic and Fundamental Analysis

Disclaimer

Veritaseum LLC and Boom Bust Blog analysis and conclusions in this presentation are based on publicly available information. Veritaseum LLC recognizes that there may be confidential information in the possession of the Companies discussed in the presentation that could lead these Companies to disagree with Veritaseum LLC's conclusions. The analyses provided may include certain statements, estimates and projections prepared with respect to, among other things, the historical and anticipated operating performance of the Companies. Such statements, estimates, and projections reflect various assumptions by Veritaseum LLC concerning anticipated results that are inherently subject to significant economic, competitive, and other uncertainties and contingencies and have been included solely for illustrative purposes. No representations express or implied, are made as to the accuracy or completeness of such statements, estimates or projections or with respect to any other materials herein. Actual results may vary materially from the estimates and projected results contained herein. Veritaseum LLC and its affiliates may own investments that are bullish or bearish on the subject entity in this material. These investments may include credit-default swaps, equity put or call options, warrants and short sales of common stock. Veritaseum LLC is in the business of creating and trading –bringing into existence, buying, licensing and selling -public and private assets and properties, including intellectual properties. It is possible that there will be developments in the future that cause Veritaseum LLC to change its position regarding the Companies and possibly increase, reduce, dispose of, or change the form of its investment or positions in (or relative to) the Companies.

Nothing in this communication shall bear any warranty of fitness, whether express or implied.

This is not financial, investment or legal advice and should not be considered as such. It is only the opinion of the author(s),

This information and work is copyrighted.