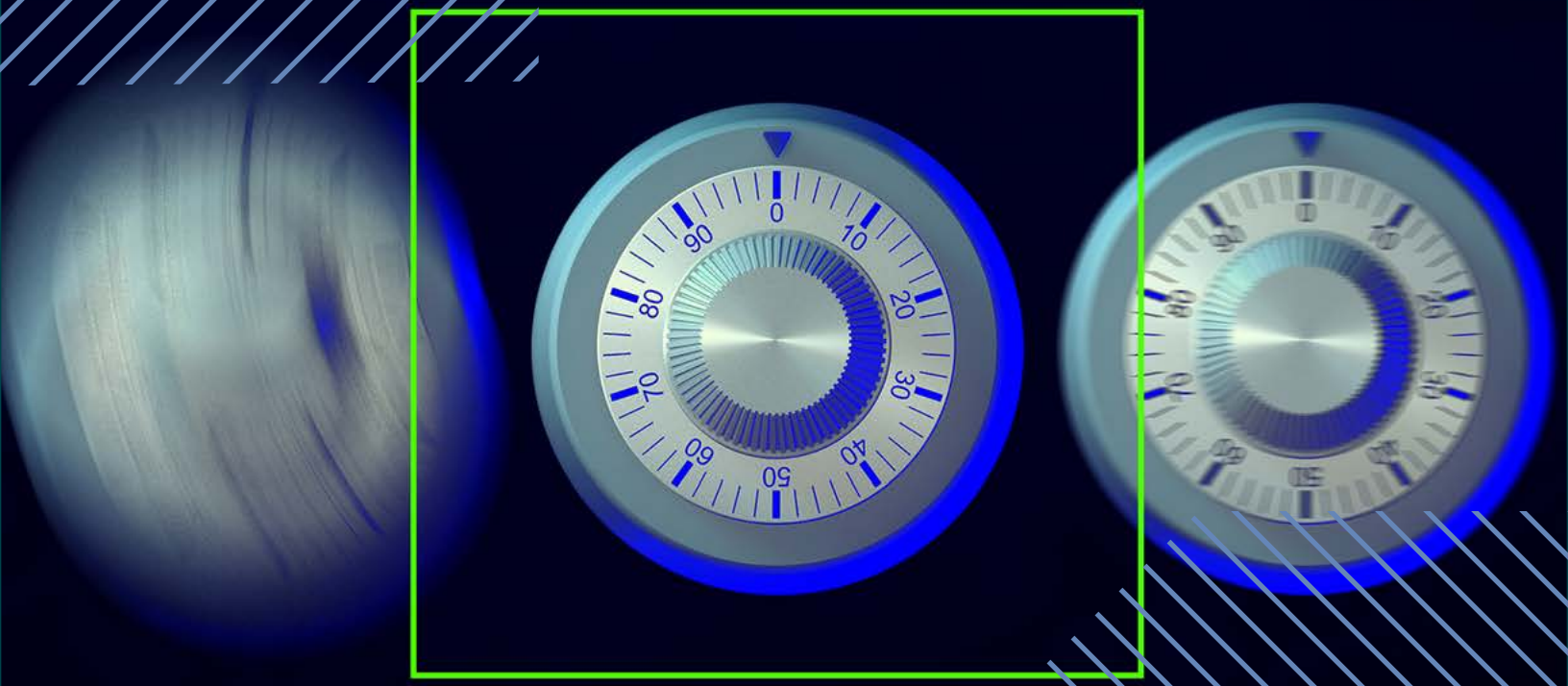
THE BLOCK | Research

Financial Privacy:

Exchanges & Regulation

DEVELOPED BY

Karim Helmy & Matthew Batsinelas



Financial Privacy: Exchanges & Regulation

Quick Take

- As crypto exchanges face increased pressure from regulators, the opportunities presented by regulatory arbitrage are diminishing.
- Across crypto trading platforms, users are increasingly required to disclose personal information to keep accounts open. The amount of sensitive information that users need to provide is also increasing.
- P2P exchanges, Bitcoin ATMs, and distributed exchanges provide alternatives to regulated exchanges for privacy-minded individuals.

Know Your Exchange
The second-hardest part of using Bitcoin privately is getting it. The hardest part is getting rid of it.

For privacy-focused users, trading on exchanges with few to no KYC (Know Your Customer), AML (Anti-Money Laundering), and CFT (Combating the Financing of Terrorism) policies has its appeal. Users can move funds in and out of these unregulated entities without exposing sensitive data. However, opportunities to trade on these platforms are drying up as regulators force the adoption of KYC and AML policies.

P2P exchanges, like Local Bitcoins and Paxful, have strengthened customer information policies over the years. Similarly, non-custodial coin swapping service Shapeshift has added personal information requirements for users.

There are ways for users to acquire Bitcoin privately, but they have drawbacks. Distributed services like Bisq lack liquidity. Bitcoin ATMs are convenient, but typically only accept cash.

It's important for users to understand the privacy implications of the different methods of trading Bitcoin. To do so, they need to know what kind of information exchanges collect, why they collect it, and what happens when things go wrong.

Exchanges and Regulation
Some exchanges abide by regulation more closely than others. Regulatorily-compliant exchanges typically have better access to

the banking system, enabling smoother on- and off-ramps between fiat and crypto.

This class of exchanges includes Bitstamp, Coinbase, Kraken, and Gemini. These companies tend to operate in highly regulated jurisdictions, where they need to abide by both local and national regulations. Coinbase recently launched Coinbase Analytics, a blockchain analytics tool targeted at governments. Kraken CEO Jesse Powell sees a conflict of interest in this new Coinbase product, as the exchange may profit from selling users' financial records.

In addition to implementing stringent KYC/AML policies, these businesses typically must obtain a money transmitter license. Some regulated exchanges run *dark pools*, which allow investors to facilitate block trades and not reveal their volumes.

Regulated exchanges require users to submit information to meet KYC/AML requirements, the processing of which is typically outsourced. In the case of KYC, some popular providers are Jumio, Onfido, JVerify, and Identity Mind. Providers of fiat AML compliance tooling include NICE Actimize, Refinitiv, LexisNexis, Beam Solutions, and ComplyAdvantage.

Privacy-focused users should understand how exchanges use their data. During the KYC process, some exchanges require as little as a name, address, and date of birth. However, most regulated exchanges also require more intrusive documents like selfies, passports, social security numbers, and utility bills. This sensitive information is used to verify users but compromises user privacy.

In June of 2019, the Financial Action Task Force (FATF), an intergovernmental organization aimed at fighting money laundering, introduced guidance for Virtual Asset Service Providers (VASPs) to strengthen AML and CFT requirements. According to FATF, countries will now be required to assess and mitigate their risks with VASPs.

VASPs will also be subject to relevant FATF measures that apply to financial institutions, such as the much-debated travel rule. This controversial rule requires exchanges to collect and transfer customer information during transactions. This information includes data on customers' names, account numbers, and locations.

The FATF guidance is non-binding. However, companies in countries that fail to implement it may find it difficult to do business with entities in jurisdictions where the guidance has been applied.

The governments of most large countries have expressed their intent to implement the guidance, and several jurisdictions have already begun to increase their AML requirements regarding crypto. In January, the EU implemented 5AMLD, which requires crypto-to-fiat firms and custodial wallets to implement baseline AML procedures. That same month, Singapore implemented the Payments Services Act, explicitly requiring VASPs to enforce AML and CFT policies.

Users can upload fake KYC documents or otherwise work around exchanges' AML and CFT policies. To combat this, exchanges use tools provided by blockchain analysis companies, allowing them to trace the flow of funds on-chain. The largest service providers in this space are Chainalysis, Elliptic, and Ciphertrace.

Exchanges use this data to make risk-based decisions about whether to allow users to make deposits and withdrawals. This data is also used to inform decisions related to freezing funds and onboarding users.

Regulatorily-compliant exchanges will likely block the transfer of money to an address flagged as belonging to a darknet market, but may allow users to move funds to a gambling site if gambling is legal in their jurisdiction. For these exchanges, funds that have gone through a mixer fall in a gray area.

Under the Bank Secrecy Act, VASPs operating in the United States must file a suspicious activity report (SAR) within 30 days of observing a high-risk incident. Some blockchain analytics providers have launched wallet screening tools to help companies prescreen wallets before high-risk incidents occur, limiting this overhead.

The sheer amount of data collected by these exchanges raises concerns of abuse. These fears are compounded when one considers that the data could be leaked through a hack or other compromising event. Recently, the lending and exchange platform, BlockFi, suffered a data breach on May 14th, 2020, which exposed retail client account activity, along with legal names, email addresses,

and postal addresses. Exchanges that are friendly to regulation are also likely to cooperate with subpoenas and surrender user data to law enforcement, driving privacy-conscious users to less-regulated exchanges.

Unregulated Centralized Exchanges

Among exchanges, there exists a spectrum of varying levels of regulation, and some exchanges have particularly relaxed attitudes toward compliance as a result of loose regulations in their jurisdictions.

Users looking to maintain user privacy have gravitated toward loosely-regulated exchanges. Lightly-regulated exchanges can effectively be used as mixers, obfuscating the source and destination of funds. This may cause blockchain analytics companies to flag transactions involving these exchanges as risky.

Since many of these exchanges require little information from users, observers may find it difficult to link funds withdrawn from a lightly-regulated exchange back to their original depositor. If an exchange handles fiat withdrawals or deposits, it can also be used as a discreet fiat on- or off-ramp.

YoBit, a Russian cryptocurrency exchange, has been used by extensively illicit actors in the past. In one example, Elliptic traced the proceeds from the Bithumb hack by the North Korean-affiliated Lazarus Group, now an OFAC sanctioned entity, to Yobit.

Some of these exchanges have unorthodox or unethical business practices. YoBit, for example, regularly facilitates pump-and-dump schemes for low-cap coins. A large number of exchanges fake trading volume.

Others, however, operate as relatively normal businesses that have struggled with regulatory requirements. These entities include large, global exchanges like Binance and Bitfinex, both of which have at least minimal KYC procedures in place. Notably, crypto derivatives exchange BitMEX has rolled out a new KYC program to its users, which comes after regulatory scrutiny.

In 2019, Chainalysis traced $2.8 billion in Bitcoin transactions that moved from criminal entities to exchanges, with over 50% going to

Binance and Huobi. Since this report, Huobi has launched an on-chain analytics tool for the monitoring of illicit cryptocurrency transactions.

As countries increase restrictions on crypto businesses, crypto exchanges that have less strict KYC/AML policies tend to move to jurisdictions with privacy-friendly regulations like the Seychelles and Malta. This strategy is colloquially known as *regulatory arbitrage*.

The days of regulatory arbitrage as a viable strategy may be drawing to a close. According to Liat Shetret, Senior Policy Advisor at Elliptic, "the FATF Presidency, starting with Marshall Billingslea from the US, has made it very clear that cryptoasset regulation expectations and FATF guidance is applicable to all jurisdictions. No jurisdiction can lurk in the shadows with a global framework and regime."

Unregulated centralized exchanges provide a way for users to remain relatively anonymous while trading and will likely continue to exist in some capacity. Many are sufficiently liquid and easily accessible to users in most countries. However, they're increasingly facing regulatory scrutiny, and have several drawbacks stemming from their custodial nature and vulnerability to a single point of failure.

Peer-to-Peer Exchanges

Peer-to-peer, or P2P, exchanges are defined by having at least one leg of a trade take place directly between counterparties, rather than both legs of the trade being routed through the exchange.

These exchanges connect bitcoin buyers with sellers and allow a variety of different payment options such as cash and bank transfers. Historically, P2P exchanges have had lax KYC/AML policies and have been considered inherently risky by blockchain analytics companies.

Using a P2P exchange can be inconvenient and slow. However, these platforms often have better privacy properties than centralized exchanges and can be more accessible, especially in countries with restrictive banking laws.

LocalBitcoins and Paxful are two particularly notable P2P exchanges.

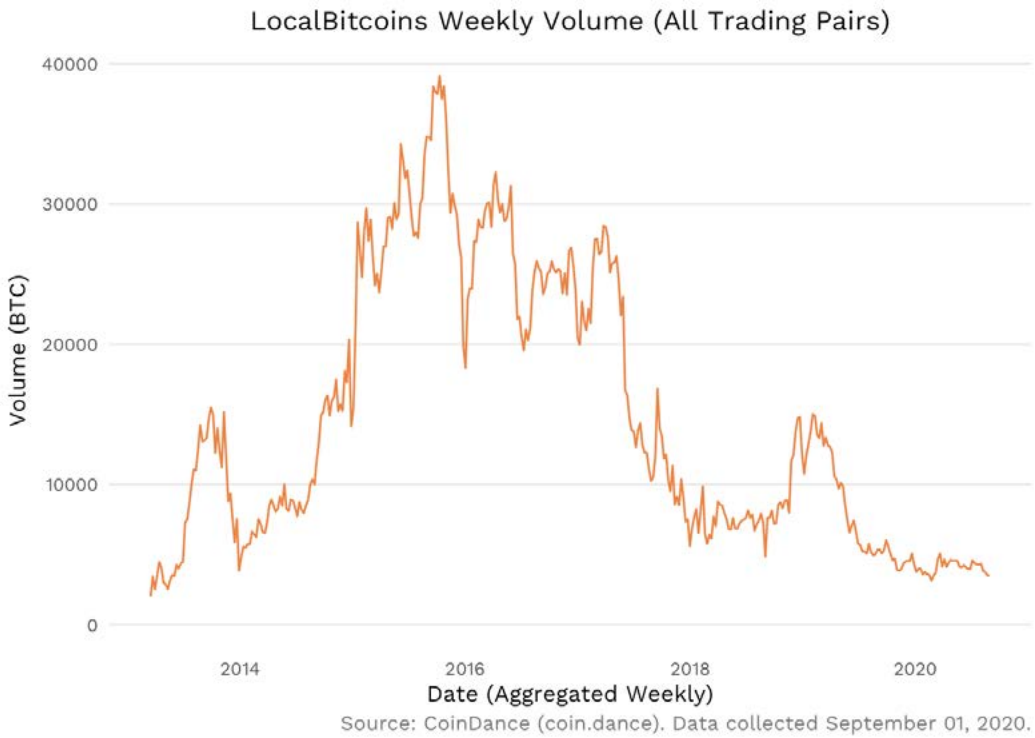
LocalBitcoins

LocalBitcoins, based in Helsinki, Finland, is the most well-known P2P Bitcoin exchange and has historically been the largest by trading volume. The platform services the purchase of bitcoin with bank transfers, credit card payments, digital currencies, and other methods.

LocalBitcoins requires users to store their bitcoin on the platform's custodial wallet, introducing the potential for loss or seizure of funds. However, LocalBitcoins does not require users to keep other assets on the platform.

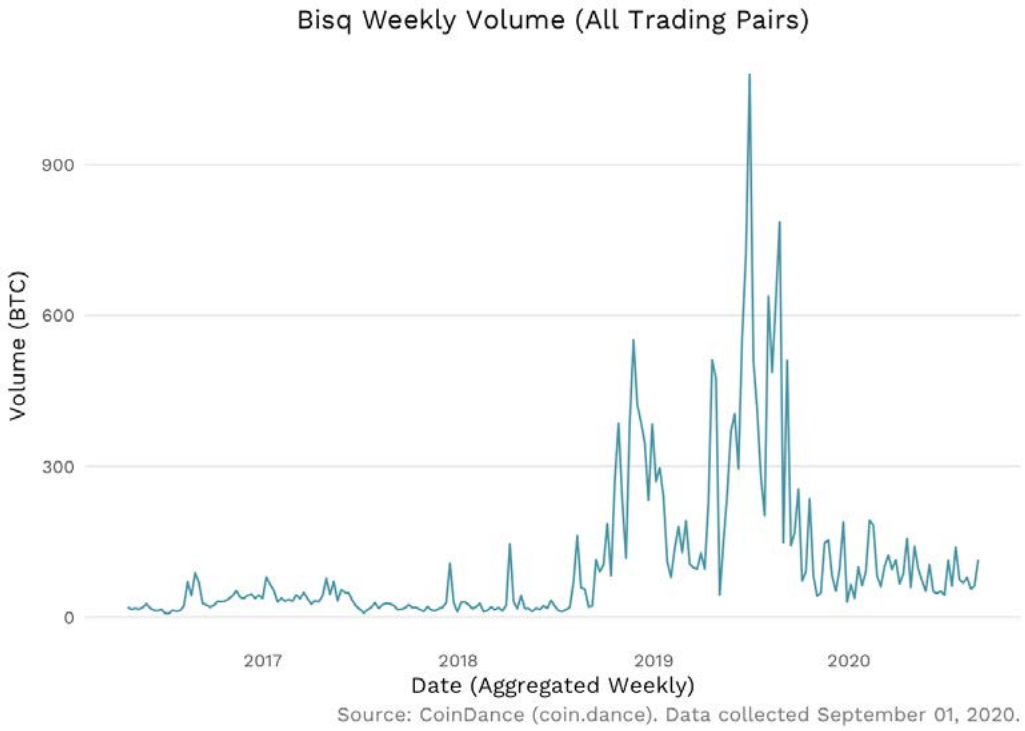
LocalBitcoins allows users to advertise their intent to purchase or sell bitcoin directly on the page. Once a buyer and seller have been matched, the seller moves their funds to an escrow controlled by the company. The buyer then pays the seller, and the seller releases the funds from escrow to the buyer. LocalBitcoins resolves any payment disputes that may arise.

While volumes have declined over the past few years, and even at their peak were low compared to those of custodial exchanges, LocalBitcoins has significant global usage.

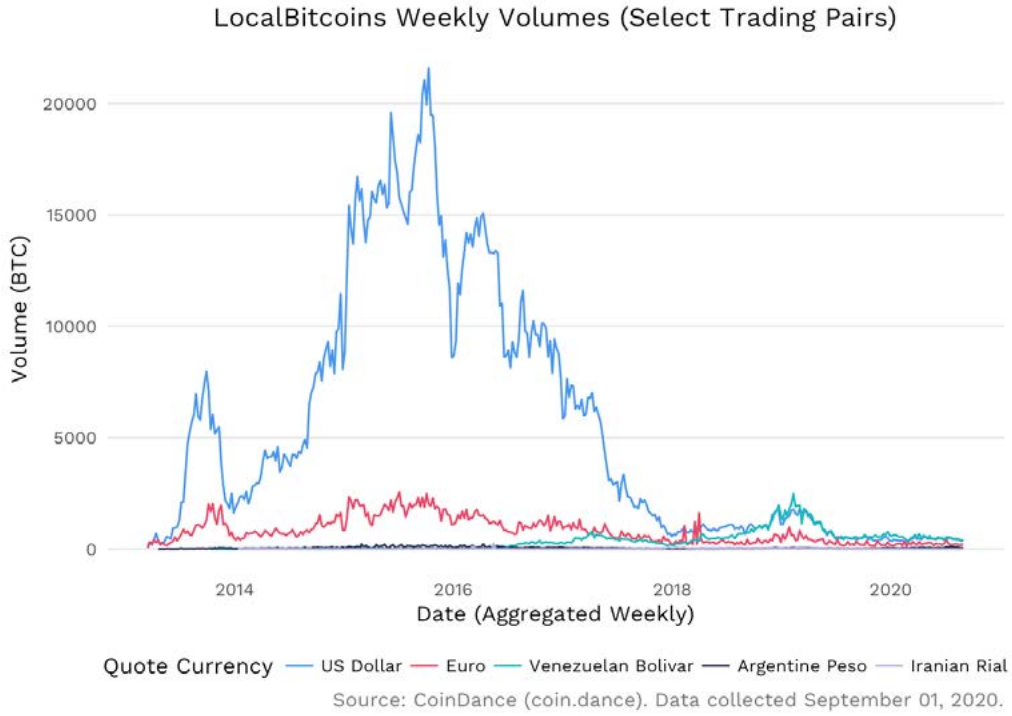


Financial Privacy: Exchanges & Regulation

The decline in LocalBitcoins volume appears to be attributable to a drop in dollar-denominated trades. Historically, dollar-denominated trading has accounted for the vast majority of volume on the platform. The volume of dollar trades has recently converged with the volumes of trades quoted in other currencies.



Source: CoinDance (coin.dance). Data collected September 01, 2020.



Source: CoinDance (coin.dance). Data collected September 01, 2020.

In June of 2019, LocalBitcoins removed cash advertisements due to regulatory restrictions. Later that month, LocalBitcoins added Onfido as a KYC provider to increase its KYC/AML requirements.

With this new provider came changes to the exchange's KYC policy. Today, the lowest KYC tier requires users who trade less than 1,000 euros per year to provide their full name, country of residence, email address, and phone number. Users who trade above this threshold must provide more details and identifying information.

In November of 2019, LocalBitcoins registered with the Finnish Financial Supervisory Authority as a Virtual Currency Provider. This registration was required by Finland's Act on Virtual Currency Service Providers as a condition of continued operation.

While LocalBitcoins has been a pioneer in financial privacy since launching in 2012, increased regulatory requirements have made it harder for its users to escape surveillance. This has negatively affected its customers living under authoritarian regimes who were using Bitcoin to escape dysfunctional financial systems, such as users in Venezuela.

On several occasions, users of LocalBitcoins have been charged with or accused of money laundering or operating an unlicensed money transmitting business. The defendant in one of these incidents was also accused of misusing another peer-to-peer exchange, Paxful.

Paxful

Paxful is a Delaware-incorporated and New York-based peer-to-peer exchange. The platform has begun to catch up with LocalBitcoins in usage with the latter's drop in volume. Users can pay for bitcoin with a variety of instruments, including gift cards, bank transfers, cash, online wallets, debit or credit cards, digital currencies, and physical goods.

Paxful is particularly well-known for allowing users to buy bitcoin with gift cards, enabling an additional layer of privacy. Bitcoin purchases made with gift cards account for the bulk of Paxful's USD-denominated trading volume.

Paxful functions similarly to LocalBitcoins. It requires each user to store their bitcoin in a custodial wallet and facilitates trades with its escrow service. Like LocalBitcoins, Paxful does not require users

to keep other assets on the platform.
To set up an account on Paxful, users need to verify their email and phone number. The company performs ID verification on all customers who hit $1,500 in trading volume or wallet activity in a day.

Paxful has recently tightened its KYC policies, requiring all US residents to verify their identity with Jumio. The exchange has also signed a contract with Chainalysis to implement the vendor's Know Your Transaction (KYT) and Reactor compliance tools to identify and investigate high-risk crypto transactions.

Paxful has historically been a compelling option for users looking to avoid surveillance. With the platform's continued increase in KYC/AML restrictions, privacy-conscious users may flock to other, less-surveilled venues.

Distributed Exchanges
Both Paxful and LocalBitcoins custody users' bitcoin, meaning that a hack or other compromising event on either platform could lead to loss of user funds. Distributed exchanges are a type of peer-to-peer exchange that can protect users from losing funds to an exchange hack, which has happened all too often.

Distributed exchanges are hosted by a diverse group of actors rather than a single organization, ensuring robustness against malicious operators and regulatory enforcement. Distributed exchanges are almost always non-custodial, meaning that users' funds would not be lost in the event of a hack.

Because distributed exchanges are robust to regulatory enforcement and may not need to perform KYC/AML, they also have privacy benefits. The most prominent distributed exchange for Bitcoin today is Bisq.

Bisq
Bisq is a distributed exchange that allows users to exchange bitcoin for fiat and other cryptocurrencies. The source code for Bisq is open-source, and each user of the exchange operates a node on the Bisq network that runs a Tor hidden service.

Bisq trades are conducted using a 2-of-2 multisig into which the bitcoin seller's funds are deposited, with each party controlling one key.

Before depositing funds into this contract, users also sign a backout transaction spending the contract's funds to a donation address controlled by the Bisq decentralized autonomous organization (DAO). The market maker in a trade may choose to require a security deposit, which is paid into the multisig by both users.

In the optimistic case, the buyer pays the seller, and the parties sign a transaction sending funds to the buyer and refunding both security deposits. Otherwise, the users enter mediation; if this is unsuccessful, the users can enter arbitration by sending the funds to the donation address. If a user is found to be acting maliciously, the arbitrator refunds the aggrieved party, and the malicious user's security deposit is kept by the donation address. The DAO then repays the arbitrator.

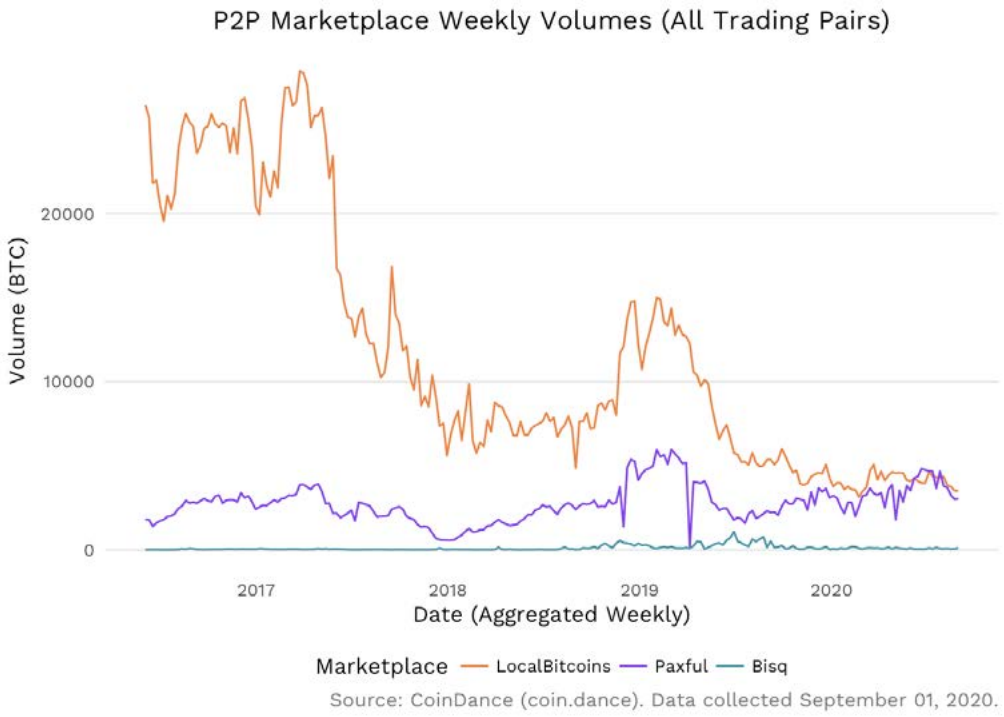
Bisq's trade settlement times and size limits are designed to protect users from loss of funds and vary by payment method according to chargeback risk, verifiability, and other relevant factors. With bank-based payment methods like SEPA and Zelle, users can exchange up to 0.25 BTC per transaction. For mobile payment services like AliPay, the maximum trade size is 1 BTC. Unlike traditional financial payments, payments made with digital currencies do not have chargeback risk and are easily verifiable. As a result, Bisq allows users to trade up to 2 BTC per transaction of this type.

Bisq does not require users to undergo KYC. This advantage, combined with the fact that each user runs a hidden service, allows users to transact in relative privacy. As with unregulated exchanges, this may cause compliance companies to interpret transactions involving the platform as risky.

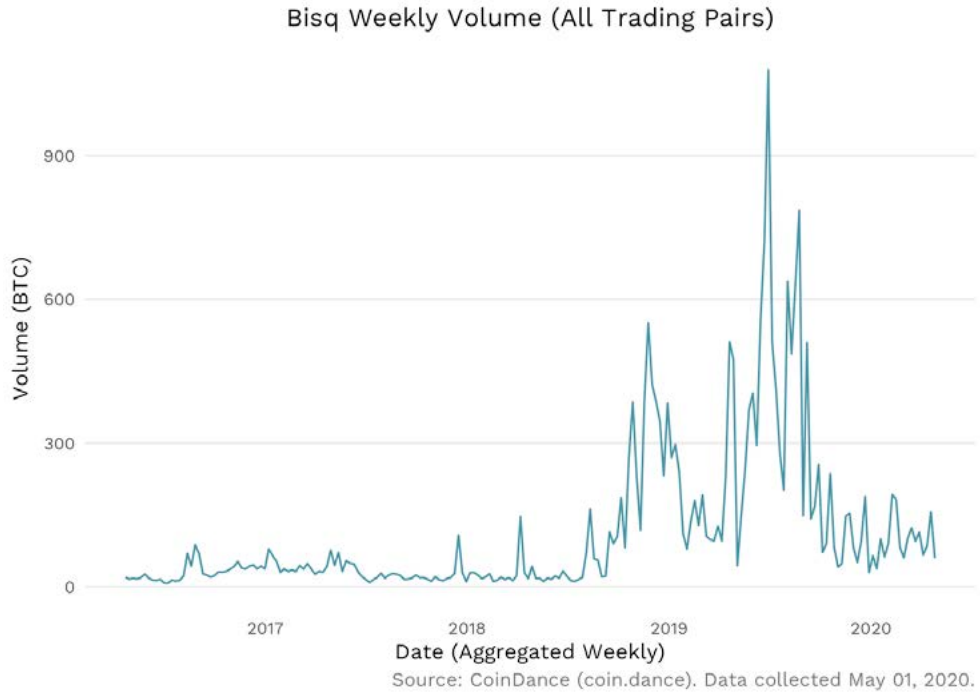
Bisq is governed by a DAO that leverages the BSQ token. This token is depicted on-chain as a colored coin, using satoshis that have been marked as representing units of BSQ. The Bisq DAO rewards mediators, arbitrators, and codebase contributors with BSQ tokens. BSQ-holders vote on the compensation received by these stakeholders. These stakeholders are potential points of centralization in the protocol, so are required to post fidelity bonds that can be seized by the DAO in the case of malicious behavior.

Traders can also use BSQ to pay the platform's fees, in the process burning the tokens. Using BSQ allows traders to save approximately 90% on fees compared to paying in BTC.

A major downside to using Bisq is the platform's lack of liquidity, even as compared to other P2P exchanges. This is aggravated by long settlement times on trades.



Due to the exchange's illiquidity and long settlement times, even some of the exchange's most liquid pairs regularly experience negative spreads. After a surge in usage in 2019, volume on the platform has subsided.



Despite this, Bisq is a promising privacy technology, and a recent report by Chainalysis cites it as a privacy tool that will continue to gain popularity.

Non-Custodial Swapping Services

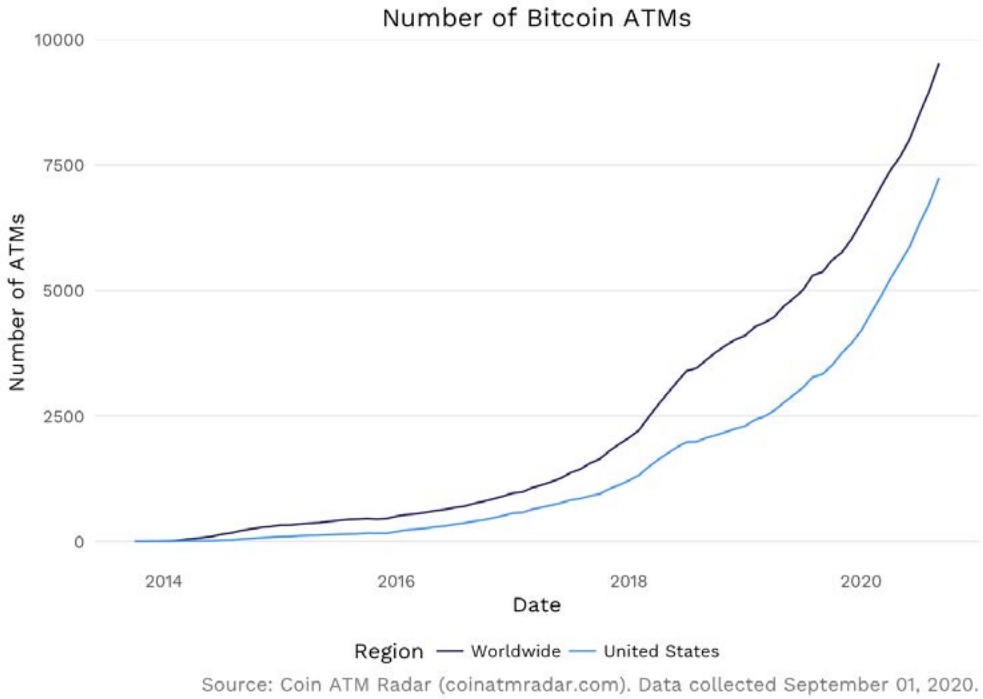
One of Bisq's key features is that it allows users to self-custody funds and retain control of their assets. Similarly, non-custodial swapping services enable users to trade without keeping money on the platform.

By reneging on their side of a trade, these services could steal the funds involved in a single transaction. Because users are storing their own funds, however, they put less money at risk of theft.

These services have significant benefits to customer security, and using them can be significantly more convenient than trading on a custodial exchange. That said, they tend to charge significantly more than their custodial counterparts.

These services have historically played a critical role in maintaining user privacy, but have also been criticized and pressured by regulators for facilitating money laundering.

Bitcoin ATMs



Source: Coin ATM Radar (coinatmradar.com). Data collected September 01, 2020.

Bitcoin ATMs are automated kiosks where retail users can buy bitcoin with cash. With some of these machines, users can also sell bitcoin and withdraw cash. Because these machines typically require very little identifying information and accept cash, they have strong privacy properties and are highly accessible.

Compared to exchanges, Bitcoin ATMs tend to have very high fees. Despite this, the number of available ATMs has increased dramatically over the past few years.

Due to their privacy benefits and relatively high low-KYC transaction limits, as well as the ease with which these limits can be skirted, Bitcoin ATMs have faced criticism over concerns related to money laundering. Regulatory compliance hurdles have also made it difficult for ATM operators to maintain banking relationships.

Nonetheless, some operators have maintained regulatory compliance. A few operators, including Coinsource, Cottonwood Vending, and LibertyX, have even attained the notoriously-strict BitLicense, allowing them to provide services in the state of New York.

ShapeShift

Founded in 2014 by Erik Voorhees, ShapeShift is a trading platform that provides non-custodial, crypto-to-crypto trading, allowing users to hold their own funds and private keys.

The advantages of ShapeShift's model came to light in 2016, when ShapeShift was repeatedly hacked due to the actions of a rogue employee who stole funds and sold sensitive information, yet no user funds were lost.

While legally based in Switzerland, the company is mainly run out of Denver, Colorado. The company was friendly to privacy-minded individuals for years, allowing them to trade anonymously on the platform.

As a result, ShapeShift has attracted negative attention for the money laundering activity that has occurred on the platform. Using data provided by Elliptic, the Wall Street Journal found millions of illicit dollars going through ShapeShift. The executors of Wannacry, a high-profile ransomware attack, notably used Shapeshift to swap bitcoin for monero.

ShapeShift has increasingly conceded to regulatory obstacles over the years. The company stopped serving users in New York and Washington in 2015 and 2017, respectively, over regulatory licensing restrictions. In late 2018, Shapeshift began to require personal identification information from customers.

Conclusion

While privately trading Bitcoin is challenging, options exist for improving financial privacy and hiding sensitive information. However, some of these vehicles, like P2P exchanges, have become more regulated over time.

Sufficiently-private distributed options like Bisq have emerged, but it's likely that regulated exchanges and blockchain analytics tools will try to flag funds coming from these types of exchanges as high risk. This will make those coins harder to move around, highlighting Bitcoin's fungibility problem.

Distributed exchanges also tend to lack the deep order books and minimal price slippage that centralized spot exchanges offer. This is a natural effect of the slower settlement times that such exchanges require. These vehicles may grow in popularity as centralized exchanges begin to work more closely with regulators, filling a necessary vacuum for privacy-minded individuals looking to avoid surveillance in the traditional financial system.

THE BLOCK | Research

THEBLOCKCRYPTO.COM