

DECRYPTING CRYPTO: DIGITAL ASSET EXCHANGES

Edited by Yaya J. Fanusie, Visiting Fellow

Written by David Lee, Research Assistant

KEY INSIGHT

Digital asset exchanges are central to the acquiring and trading of crypto assets. Anti-money laundering regulations in the U.S. are clear for most exchanges, but some regulatory uncertainty around some issues persists.

SUMMARY

Digital Asset Exchanges are platforms that allow users to buy, sell, or swap **blockchain**-backed assets by keeping a record of ownership and facilitating the change of custody of digital assets. There are two types of Digital Asset Exchanges: **Centralized Exchanges (CEXes)**, which handle user funds and facilitate trade, and **Decentralized Exchanges (DEXes)**, which facilitate trades via contracts stored on a blockchain that is automatically executed when predetermined conditions are met. DEXes do not take custody of users' funds when facilitating trades.

KEY FACTS

Centralized Exchanges (CEXes) are intermediaries that act similarly to stock exchanges and hold **private keys** and funds on behalf of digital asset traders. Popular CEXes provide higher liquidity and are typically more user-friendly than Decentralized Exchanges. However, like the early bitcoin exchanges, CEXes are the target of hackers and users risk losing their investments.

Notable CEXes are Binance, Bybit, and Coinbase.

Decentralized Exchanges (DEXes) are automated platforms that facilitate digital asset trade through **smart contracts** on blockchain networks. DEXes' users retain control of their digital assets providing a higher level of security and privacy. However, DEXes have lower liquidity and are still susceptible to vulnerabilities in smart contracts that could be exploited by hackers. Notable DEXes are Uniswap, SushiSwap, and THORChain.

KEY INSTITUTIONS

Financial Crimes Enforcement Network (FinCEN) supervises digital asset exchanges that are money transmitters and subject to the Bank Secrecy Act (BSA). The BSA requires such exchanges to register with FinCEN as money service businesses and implement Anti-Money Laundering (AML) and Know Your Customer (KYC) procedures. In addition, both the Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) claim jurisdiction over regulating digital asset exchanges.

BACKGROUND

When Bitcoin first launched in January 2009, there were only two ways to obtain it: by using computer power to verify blockchain transactions and earn bitcoins in a process

called mining or arranging a peer-to-peer (P2P) trade with someone who owned bitcoins. P2P requires a high level of trust between parties to ensure that each party would fulfill the transaction. As interest in Bitcoin grew, the demand for a simpler way to obtain it grew. In March 2010, BitcoinMarket.com launched as the first Bitcoin exchange website. The centralized exchange introduced a floating exchange rate, which provided real-time price conversion between Bitcoin and U.S. Dollars (USD) determined by supply and demand. However, due to recurring problems with fraud, PayPal blacklisted the exchange in October 2010, leading to its collapse. Fraud and other illicit activities continued to haunt subsequent centralized exchanges, which stored the private keys for users' digital wallets on their company servers. One exchange, Mt. Gox, which once accounted for between 70% to 80% of Bitcoin trades, filed for bankruptcy in February 2014 after hackers stole 850,000 Bitcoin. Following the Mt. Gox hack, several major exchanges including Poloniex, Bitfinex, Bitstamp, Binance, Bithumb, and ShapeShift also had significant crypto funds stolen off of their centralized servers, giving popularity to the mantra, "not your keys, not your crypto." In July 2015, the Ethereum blockchain was launched, introducing smart contracts, and decentralized applications (dApps). Smart contract programmability made it possible for Ethereum developers to create decentralized exchanges where users would control their private keys so that their funds would not be vulnerable to hacks on CEXes. Smart contracts also made it easier for people to create new cryptocurrency tokens, laying the groundwork for the Initial Coin Offering (ICO) boom. Between 2017 and 2018, more than 2,000 unique tokens were created, raising more than \$10 billion.

However, scams and fraud proliferated around these ICOs, attracting scrutiny from U.S. financial regulators and law enforcement. The U.S. has had a robust anti-money laundering (AML) regulatory framework for centralized exchanges since 2013. However, rules relating to cryptocurrency investment markets are less clear. In November 2022, FTX, the third-largest exchange at the time, collapsed after questionable management practices and insufficient reserves for withdrawals instigated a liquidity crisis. FTX's collapse caused shockwaves throughout the industry, inviting regulatory scrutiny and calls to create a clearer regulatory framework for cryptocurrency markets.

POLICY AND REGULATION ISSUES

Digital Asset Exchanges face numerous policy and regulatory challenges. Key issues include:

- **Money Transmitter Definition:** Some legal disputes exist over whether DEXes can be considered money transmitters and how they may or may not fit under the BSA. Classifying a truly decentralized exchange platform as a money transmitter would bring regulatory challenges since it operates without an intermediary entity that can fulfill BSA obligations.
- **Regulatory Classification of Digital Assets:** As aforementioned, both the SEC and CFTC claim jurisdiction over digital assets as the SEC classifies digital assets as securities, while the CFTC classifies digital assets as commodities. This leads to overlapping and unclear responsibilities.

GLOSSARY

Blockchain: A shared and immutable record of transactions that are maintained in a decentralized, digital format.

Centralized Exchanges (CEXes):

Intermediary platforms that hold private keys and funds on behalf of digital asset traders.

Decentralized Exchanges (DEXes): Software platforms that facilitate digital asset trade through smart contracts on blockchain networks.

Mining: The use of computer processing power to solve cryptographic puzzles required to maintain and secure blockchain networks. This process is also called “proof of work” and results in the addition of a new block of records to the blockchain and rewards the miner with cryptocurrency.

Private Keys: An alphanumeric code used to authorize transactions and prove ownership of a blockchain asset.

Smart Contracts: Digital contracts programmed on a blockchain that are automatically executed when predetermined terms/conditions are met.

For more information, please visit our website finpolicy.georgetown.edu or email cfmp@georgetown.edu